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."***

**VIDEO CONFERENCE with CUCCIO**

**7 July 2020**

- Good afternoon, bonjour tout le monde, I am a member of the Academic Outreach & Stakeholder Engagement team at the Canadian Security Intelligence Service, CSIS.

- Avec mes collègues du Service et nos partenaires du Centre canadien pour la cybersécurité (CCCS), nous sommes très heureux d'avoir été invités à vous parler aujourd'hui. CSIS has been working very closely in collaboration with our counterparts at the Canadian Centre for Cyber Security and with the Communications Security Establishment (CSE) to protect Canadians and Canadian interests against threats to our national security and prosperity.

- CSIS investigates threats to the security of Canada, including foreign interference and espionage emanating from hostile state actors and their proxies. Our role is to advise the Government of Canada of these threats so it can take action where appropriate, and in some cases to counter those threats directly.

- We are grateful for this opportunity to share with you some of our concerns related to threats of foreign interference and espionage targeting Canada's research and development community, including within all disciplines of academia.

- Since mid-May, CSIS has been deploying our intelligence and liaison officers from Regional offices across Canada to meet with individuals and organizations involved in the Canadian effort to respond to COVID-19. These outreach efforts have included engagement with the academic community and its IT experts, the life sciences sector, the private sector and provincial governments.

- We know that Canada's academic community is facing complex and unprecedented challenges in an era of virtual learning and funding constraints, in parallel with this changed threat landscape. For some within the research community, requirements to apply a national security lens in considering which research partnerships, collaborations or funding arrangements to pursue may clash with an ethos of open science or seem at odds with objectives of global advancement.

- Our objective in conducting this outreach is not to hamper international scientific and research collaboration, but rather to ensure that the interests of Canada's research community, its human talent, its R&D and IP, its publications and investments are protected against hostile actors seeking to exploit Canadian knowledge and our open research environment in pursuit of their own geopolitical ambitions.

- Collectively, this response aims to help protect Canada's human talent, its public investments in R&D, and the future of higher learning in Canada.

- With those opening remarks, I am happy to pass things over to two of our expert cyber analysts to brief you further on the threats and trends that we are seeing.

# Introductory Remarks for Supply Chain Canada Webinar

## 2020 11 05

Hello, Bonjour. I'm a member of the Academic Outreach & Stakeholder Engagement team at the Canadian Security Intelligence Service or CSIS. I would like to express our appreciation to and all of for providing us with the opportunity to present to you today.

It is my pleasure to deliver introductory remarks as context for this joint presentation by CSIS and our colleagues at the Canadian Centre for Cyber Security.

The mission of CSIS is the protection of Canada's national security interests and the safety of Canadians. CSIS is mandated to achieve this mission through collection and analysis of intelligence, provision of advice to government and also through threat reduction measures.

Our vision is a safe, secure and *prosperous* Canada, through trusted intelligence and advice. Achieving this vision means combatting national security threats such as espionage and foreign interference which is what we're here to discuss with you today.

As a response to the current threat environment, we have been conducting outreach with Canadian businesses, associations, and institutions to ensure that

their research and development, intellectual property and business interests are protected.

While the initial focus of this outreach was speaking to entities directly involved in COVID-19-related research, our attention has now turned to the complex network of organizations working to procure, manufacture, and distribute vaccines, therapeutics and other vital goods that support the economic and health security of Canadians.

At a time when global supply chains are already under extraordinary pressure due to the pandemic, we seek to ensure that our supply chains are not exploited by hostile foreign actors for their own national advantage. We know that reliability and security are guiding principles for your industries. These actors seek to disrupt supply chains and compromise security. We want to support you in preventing foreign actors from jeopardizing your businesses and Canada's economic interests.

You know your businesses better than anyone. You will be the first to identify unusual or suspicious activities - *if you know what to look for*. In briefing you today, we want to be sure that you have the information you need to identify and mitigate against the risk that foreign threat actors could exploit vulnerabilities in your supply chains.

Your industry facilitates multi-modal movement of goods across international borders with diverse cargo under

extreme time pressures, and through vast network of logistics, transportation, freight forwarders, customs brokers, warehousing and authorities. Not to mention the weather!

This complexity will only increase as the supply chain sector begins to fully employ and integrate technologies such as robotics, big data analytics, artificial intelligence, quantum computing and the Internet of Things into its infrastructure. While these new technologies hold great promise for transforming your industry, they bring their own challenges and risks. Technology can and has been used to target, exploit and disrupt supply chains around the world.

While your industry is already aware of the threat of cyber attack, we want to be sure that you are also alert to other avenues or gates through which foreign actors could target you or your partners.

What kinds of activities are we talking about? My expert colleagues will be able to discuss in greater detail, but activities could include theft of intellectual property, valuable data and proprietary technology; cyber techniques to disrupt, degrade or surveil a component or system; theft or reverse-engineering of goods; or infiltration of your business or supply chain by a hostile insider threat.

During the pandemic, Canadians are increasingly aware of our reliance on our supply chains for the provision of

vital goods necessary for the health and safety of our nation. We appreciate all you are doing to keep things running smoothly!

As nations ramp up espionage efforts in the race to acquire and distribute a COVID-19 vaccine, it is imperative that we ensure the integrity of our supply chains, including through dialogue and engagement with important stakeholders like you.

With that context, I am very pleased to pass it over to our expert CSIS briefer . is a Senior Analyst Thanks very much for your attention and please don't hesitate to reach out to our organization with your concerns and questions following this event either through the organizers or through the contact information available on our website. Over to you

**VIDEO CONFERENCE with UNIVERSITIES CANADA**

**19 June 2020**

- Good afternoon, bonjour tout le monde, my name is Tricia Geddes; I am the Assistant Director for Policy and Strategic Partnerships with the Canadian Security Intelligence Service, CSIS.

- Avec mes collègues du Service et nos partenaires du Centre canadien pour la cybersécurité (CCCS), nous sommes très heureux d'avoir été invités à vous parler aujourd'hui. CSIS has been working very closely in collaboration with our counterparts at the Canadian Centre for Cyber Security and with the Communications Security Establishment (CSE) to protect Canadians and Canadian interests against threats to our national security and prosperity. My colleague from CCCS will be speaking more to you about cyber security later during this briefing.

- CSIS investigates threats to the security of Canada, including foreign interference and espionage emanating from hostile state actors and their proxies. Our role is to advise the Government of Canada of these threats so it can take action where appropriate, and in some cases to counter those threats directly.

- We are grateful for this opportunity to share with you some of our concerns related to threats of foreign interference and espionage targeting Canada's research and development community, including within all disciplines of academia.

- Since mid-May, CSIS has been deploying our intelligence and liaison officers from Regional offices across Canada to meet with individuals and organizations involved in the Canadian effort to respond to COVID-19. These outreach efforts have included engagement with the academic community, the life sciences sector, the private sector and provincial governments.

- We know that Canada's academic community is facing complex and unprecedented challenges in an era of virtual learning and funding constraints, in parallel with this changed threat landscape. For some within the research community, requirements to apply a national security lens in considering which research partnerships, collaborations or funding arrangements to pursue may clash with an ethos of open science or seem at odds with objectives of global advancement.

- Our objective in conducting this outreach is not to hamper international scientific and research collaboration, but rather to ensure that the interests of Canada's research community, its human talent, its R&D and IP, its publications and investments are

protected against hostile actors seeking to exploit Canadian knowledge and our open research environment in pursuit of their own geopolitical ambitions.

- Before I turn it over to our senior analyst to provide more information on why Canadian research is of interest, and the methods used to target that work, I would like to thank you all, on behalf of my colleagues at CSIS, for the work you are doing and for the personal sacrifices you are making in these trying times.

- J'aimerais vous remercier tous, au nom de mes collègues du SCRS, du fond de mon cœur pour le travail que vous accomplissez et pour les sacrifices personnels que vous faites en ces temps difficiles.

- As you well know, Canadians are placing a great deal of hope and faith in the work you are doing to respond to the pandemic and ensure continued academic excellence in the future. We know that many of you are investing heavily of your time, your considerable skill and, indeed for some, your life's work into this global effort. Your passion for discovery and innovation, and your commitment to sharing knowledge and working with partners around the world in the interest of humanity is truly an inspiration.

- As you continue to focus on that critical work, please know that we are doing our best to look out for you, your colleagues and Canadian research. We want to make sure you're sensitized to some of the activity of state actors that we've witnessed so you can take appropriate steps to protect your universities, you research, and your staff and students. Taking these steps can also help to ensure reciprocal international partnerships and academic freedoms globally by ensuring cooperation is built on transparency and trust.

- Collectively, this response aims to help protect Canada's human talent, its public investments in R&D, and the future of higher learning in Canada.

- With those opening remarks, I am happy to pass things over to one of our Senior Intelligence Analyst to brief you further on the threats and trends that we are seeing.

- Etant donné la composition de cette audience, nous allons entreprendre la majorité de cette presentation en anglais, mais sommes certainement prêt à clarifier nos commentaires et de répondre à vos questions en francais aussi.

**VIDEO CONFERENCE WITH**
**4 June 2020**

- Good morning, bonjour tout le monde, I am Director General of the Intelligence Assessments Branch with the Canadian Security Intelligence Service, CSIS.

- Avec mes collègues du Service et nos partenaires du Centre canadien pour la cybersécurité, nous sommes très heureux d'avoir été invités à vous parler aujourd'hui. CSIS has been working very closely in collaboration with our counterparts at the Canadian Centre for Cyber Security and with the Communications Security Establishment (CSE) to protect Canadians and Canadian interests against threats to our national security and prosperity. My colleague from CCCS will be speaking more to you about cyber security later during this briefing.

- We are grateful for this opportunity to share with you some of our concerns related to threats of foreign interference and espionage targeting Canada's research and innovation sectors, ultimately compromising your business and proprietary interests. Will do our best to answer any questions you may have.

- CSIS investigates threats to the security of Canada, including foreign interference and espionage emanating from hostile state actors and their proxies. Our role is to advise the Government of Canada of these threats so it can take action where appropriate, and in some cases to counter those threats directly.

- I'll note that since mid-May, CSIS has been deploying our intelligence and liaison officers from Regional offices across Canada to meet with companies and entities such as yours. This effort continues, and if there are participants on this call that would like to meet with us for more in-depth discussions, please get in touch with us. We will send our contact information to pass along to all of you.

- Before I turn it over to our senior analyst to lead the briefing, I would like to first thank you all, on behalf of my colleagues at CSIS, from the bottom of my heart for the work you are doing and for the personal sacrifices you are making in these trying times.

- J'aimerais vous remercier tous, au nom de mes collègues du SCRS, du fond de mon cœur pour le travail que vous accomplissez et pour les sacrifices personnels que vous faites en ces temps difficiles.

- As you well know, Canadians are placing a great deal of hope and faith in the work you are doing to help stem the spread and reduce the impact of this deadly virus. We know that many of you are investing heavily of your time, your considerable skill and, indeed for some, your life's work into this global effort. Your passion for discovery and innovation, and your

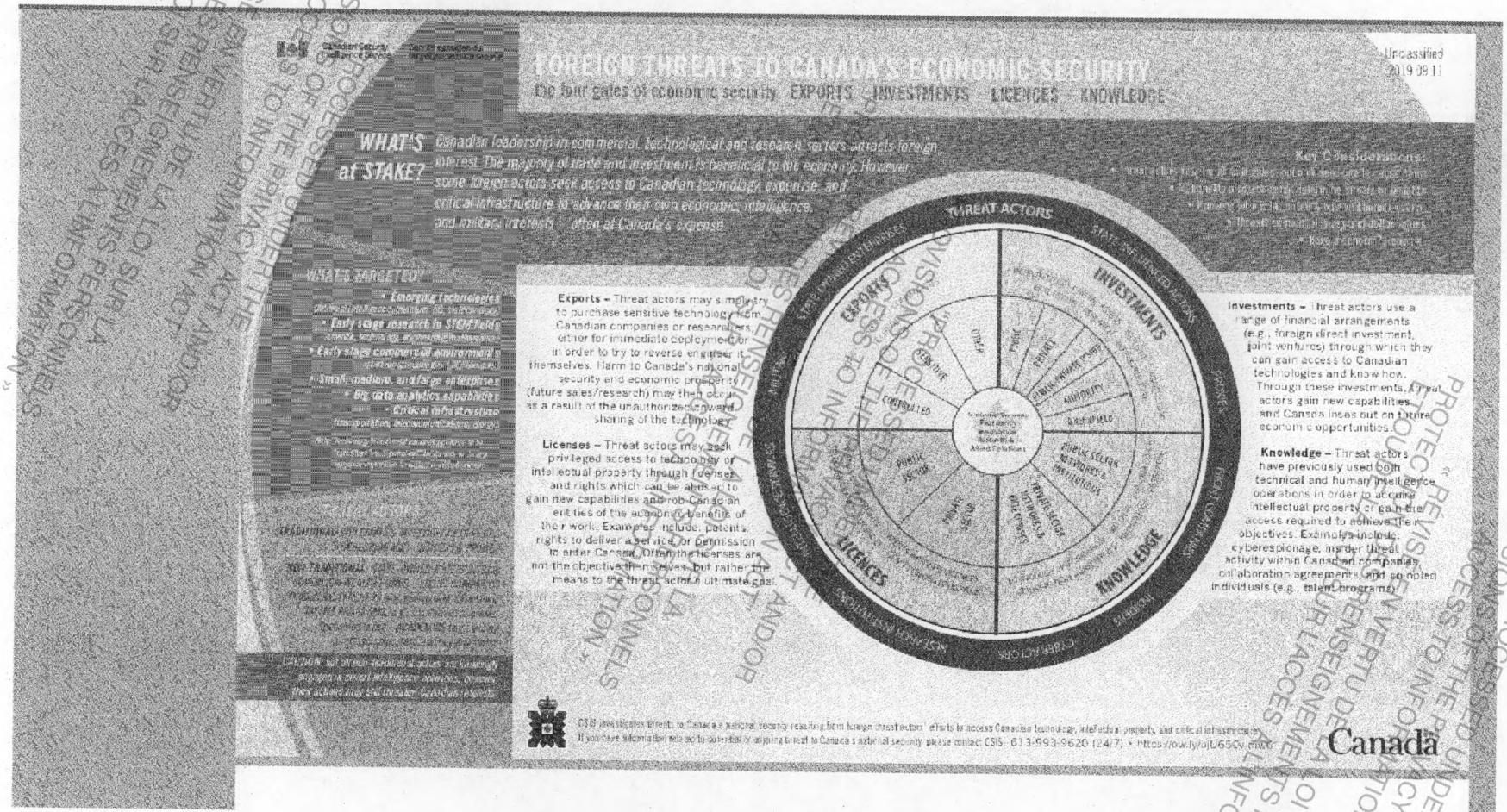
commitment to sharing knowledge and working with partners around the world in the interest of humanity is truly an inspiration.

- As you continue to focus on that critical work, please know that we are doing our best to look out for you and your R&D, and to help to secure the work you do as it relates to Canada's national interests. We want to make sure you're sensitized to some of the activity of state actors that we've witnessed so you can take appropriate measures to protect and secure your research and innovation.

- Collectively, this response aims to help protect Canada's human talent, its public investments in R&D, and your contribution to the global effort to combat COVID-19.

- With those opening remarks, I am happy to pass things over to one of our Senior Intelligence Analysts with an expertise in espionage and economic security who will brief you further on the threats that we are seeing.

- Etant donné la composition de cette audience, nous allons entreprendre la majorité de cette presentation en anglais, mais sommes certainement prêt à clarifier nos commentaires et de répondre à vos questions en francais aussi.


FOREIGN THREATS TO CANADA'S ECONOMIC SECURITY
the four gates of economic security EXPORTS INVESTMENTS LICENCES KNOWLEDGE
Unclassified
2019 09 11
WHAT'S at STAKE?
Canadian leadership in commercial, technological and research sectors attracts foreign interest. The majority of trade and investment is beneficial to the economy. However, some foreign actors seek access to Canadian technology, expertise, and critical infrastructure to advance their own economic, intelligence, and military interests – often at Canada's expense.
Key Considerations
WHAT'S TARGETED
Emerging Technologies
Early stage research in STEM fields
Early stage commercial environments
Small, medium, and large enterprises
Big data analytics capabilities
Critical infrastructure
THREAT ACTORS
STATE-ENHANCED ACTORS
PROXIES
CRIMINAL ENTERPRISES
CYBER ACTORS
RESEARCH INSTITUTIONS
EXPORTS
INVESTMENTS
LICENCES
KNOWLEDGE
Exports – Threat actors may simply try to purchase sensitive technology from Canadian companies or researchers, either for immediate deployment or in order to try to reverse engineer it themselves. Harm to Canada's national security and economic prosperity (future sales/research) may then occur as a result of the unauthorized onward sharing of the technology.
Licenses – Threat actors may seek privileged access to technology or intellectual property through licenses and rights which can be abused to gain new capabilities and rob Canadian entities of the economic benefits of their work. Examples include: patents, rights to deliver a service, or permission to enter Canada. Often the licenses are not the objective themselves, but rather the means to the threat actor's ultimate goal.
Investments – Threat actors use a range of financial arrangements (e.g., foreign direct investment, joint ventures) through which they can gain access to Canadian technologies and know-how. Through these investments, threat actors gain new capabilities and Canada loses out on future economic opportunities.
Knowledge – Threat actors have previously used both technical and human intelligence operations in order to acquire intellectual property or gain the access required to achieve their objectives. Examples include: cyberespionage, insider threat activity within Canadian companies, collaboration agreements (and co-opted individuals (e.g., talent programs).
CSIS investigates threats to Canada's national security resulting from foreign threat actors' efforts to access Canadian technology, intellectual property, and critical infrastructure.
If you have information related to potential or ongoing threat to Canada's national security please contact CSIS: 613-993-9620 (24/7) • https://ow.ly/pJU650v1mCC
Canada

PROVISIONS "PROCESSED UNDER THE ACCESS TO INFORMATION ACT AND/OR PROTECTION OF THE PRIVACY ACT" "RÉVISÉ EN VERTU DE LA LOI SUR L'ACCÈS À L'INFORMATION ET/OU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS"



PROVISIONS "PROCESSED UNDER THE ACCESS TO INFORMATION ACT AND/OR PROTECTION OF THE PRIVACY ACT" "RÉVISÉ EN VERTU DE LA LOI SUR L'ACCÈS À L'INFORMATION ET/OU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS"

PROVISIONS "PROCESSED UNDER THE ACCESS TO INFORMATION ACT AND/OR PROTECTION OF THE PRIVACY ACT" "RÉVISÉ EN VERTU DE LA LOI SUR L'ACCÈS À L'INFORMATION ET/OU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS"

3103(18/09)

**UNCLASS Biopharma Outreach**

**GOAL**: Raise your awareness of espionage risks; answer your specific questions.

We will not prevent espionage in just one discussion. But we can increase awareness – and you can begin to take measures that reduce your risk and to withstand this threat. You are not alone – after today's discussion, I hope that you will talk to your local CSIS representative if you experience security issues or have concerns.

**CAVEAT**: Unconventional for a spy agency to discuss nation security issues beyond our government clients and outside of classified channels.

This is challenging, but necessary. Espionage has evolved beyond covert agents breaking into government safes to steal state secrets. Spies now wear lab coats, not trench coats. Your companies possess things of tremendous value to Canada – and to other nations. You conduct R&D, create valuable IP, and your technology and know-how are the primary espionage targets.

I will go as far as I can to answer your questions and I will tell you when I reach my limits of what I can safely say at an UNCLASS level. Please don't self-censor your questions, but also please accept that I will face some restrictions in how I can respond to them.



**BLUF – Espionage is Real; and Your Sector is a Priority Target**

- 1) **WHAT is happening**: Canadian bioscience now faces significant espionage risk. This threat is no longer hypothetical – Canadian biopharma and health organizations have been targeted.

- 2) **WHY is it happening**: Biopharma and health has become the frontline of international competition. Some countries are aggressively advancing their own national interests, even at the expense of others. Your work is valuable and high-profile; as a result you may be a target.

- 3) **HOW is it occurring and how can you protect yourself**: This state-sponsored espionage will take many forms. However, your organization can also take various measures to reduce your risk, create resilience and protect yourself. The first step is being aware of espionage threats.



**WHAT**: Canadian bioscience now faces significant espionage risk. This threat is no longer hypothetical – Canadian biopharma and health organizations have been targeted.

- CSIS has observed persistent and sophisticated espionage activity aimed at many Canadian economic sectors, for many years now. Regrettably, this threat has harmed Canadian companies. Collectively, it jeopardizes Canada's knowledge-based economy. When our most innovative technology and know-how is lost to espionage, it is our country's future that is being stolen.

- Canada's biopharma and health sector already faced moderate espionage risk before this pandemic. Canadian biopharma companies have been targeted and have lost IP. However, those risks have now become much more significant.

- This is no longer hypothetical. CSIS intelligence and investigations have determined that Canadian companies in your industry have already been targeted and compromised during this pandemic.

- I do not say this to raise undue concern that all organizations here face grave or imminent risk. But a prudential security posture may be warranted.

**WHY**: Biopharma and health has become the frontline of international competition. Some countries are aggressively advancing their own national interests, even at the expense of others. Your R&D is globally valuable and as a result, you may be an espionage target.

- Bioscience has become the new frontline for international competition as nations seek to manage this pandemic, protect their citizens and emerge from this in a position of relative safety, security and prosperity.

- When nations compete and seek to advance their own interests, some of them will resort to espionage. These select nations employ sophisticated and well-resourced intelligence services.

- Over years, these nations have targeted and compromised many Canadian sectors, preying on vulnerable organizations that may be unaware and unprotected against state-sponsored espionage. These countries will even exploit Canada's openness to collaboration, advancement of universal science, and the financing and partnerships in R&D, in order to steal what they desire.

- I will not single out any particular nations in today's discussion. In fact, we should not discount that threat activity can originate from anywhere in the world. Even beyond nation states, non-state actors like organized crime groups may pose a threat to your work.

**HOW**: State-sponsored espionage may take many forms. But your organization can also take various measures to reduce risks and protect yourself. The first step is being aware of espionage threats – that's the reason for today's discussion.

- Note: Refer to Four Gates placemat on screen and BIOTech Canada website. We developed that based on a decade's worth of CSIS intelligence and analysis, to show how certain nations conduct threat activity against Canada, using various threat vectors and tradecraft.

- Sensitive and proprietary Canadian technology, know-how and assets can be accessed in any of four ways: attacks on knowledge, investments, imports/exports, and licenses. I will offer some brief comments on each of those, but we can go further on any of those elements in the Q&A.

**Knowledge**

- Canadian research, IP, as well as personal and corporate data, can be compromised in many ways, such as cyber espionage, insider threats within your organization, and foreign intelligence operations.

- One particular area of concern is what CSIS refers to as "non-traditional collectors". That simply means people without formal intelligence training or tradecraft, but who you engage on research collaboration, investment or financing discussions, and business partnerships. This category includes students, academics, researchers, and investors.

- It starts to make sense if you think of it from the adversary's perspective. I could send a trained spy to compromise your company, but at what risk, and for what reward? I cannot easily train them to become a microbiologist, or a data scientist, or a business person. They may not know what to steal, they will raise suspicion in their actions, and they risk being exposed.

- Instead, I can co-opt or coerce someone that you have invited in the front door, potentially for weeks or months at a time. That offers plausible cover and persistent access – better yet, that individual knows exactly what is most valuable and may even have direct access to it.

- Non-traditional collectors may not even have premeditated intent to cause harm to your organization or to Canada. Instead, they are immensely vulnerable to the coercive demands of another country, if they plan to return there, have family members there, or financial interests. Other countries have powerful national security and intelligence laws that demand cooperation and create severe punishments for anyone who attempted to say no.

**Investment**

- The biopharma sector is attracting significant investment interest these days, from foreign acquisitions to venture capital. However, a small proportion of that investment is state-sponsored and harbours malign intent.

- Especially in this pandemic, foreign governments may pursue investment to gain access and control of Canadian technology and know-how, or even access or control over Canadian critical infrastructure and essential supply chains.

- For years now, CSIS has seen state-sponsored acquisitions aimed at Canada's most sensitive technology, data and critical infrastructure assets. Please realize that what initially appears to be a lucrative foreign investment offer may have hidden strings – and consequences – attached.

**Imports & Exports**

- The purchase and export of advanced and dual-use technologies, which can then be copied or reverse-engineered, is a well-known national security concern.

- What's new in this pandemic is a growing concern over the risk of disruption of vital Canadian supply chains, which could undermine our public health capacity.

- Active pharmaceutical ingredients, personal protective equipment, medical devices, and other critical supplies are the foundation of Canada's sovereign capability to respond to this pandemic. If our supply chains are compromised, it may affect Canada's health security and Canadian lives.

**Licences**



- Finally, licenses may grant privileged rights or access to assets or data, which could be exploited to harm Canada and Canadians. In this category, we typically focus on visas to enter Canada, patents that protect IP, and research and collaboration agreements with foreign partners.

- The licences are not the objective, but rather a means to the threat actor's ultimate goal, such as your IP or the data you hold. For example, if you enter into licensing or contractual arrangement with a foreign partner in the expectation that they will abide by that agreement and Canadian laws and norms, you may face some risks.

**Wrap Up**:

- The espionage threat is real and your sector is a priority target. Threat actors may try all Four Gates, but they only need to succeed in one to significantly harm your company and Canada's national security.

- You are not alone in facing these threats. The fact that my CCCS colleague and I are having today's engagement with you shows that our government wants to work with you to protect your companies and the invaluable work that you do in Canada.



- We have covered a lot of material very quickly – and I do look forward to the Q&A – but please reach out to your local CSIS representatives at any future point if we can be of assistance to investigate security issues or offer additional advice. Thank you.

Canadian Security Intelligence Service / Service canadien du renseignement de sécurité

Unclassified
2020 04 21

# FOREIGN THREATS TO CANADA'S BIOPHARMACEUTICAL AND HEALTHCARE SECTORS

## WHAT'S at STAKE?

*Canadian leadership in biopharmaceutical and healthcare sectors – whether commercial, technological, or scientific – is critical to Canada's ability to manage the healthcare response to, and the economic recovery from, the COVID-19 pandemic. While international collaboration is a feature of this, some foreign actors seek to advance their own interests at Canada's expense.*

**Key Considerations:**

- Threat actors may try all four gates, but only need one to cause harm
- Nationality alone does not determine threats or benefits
- Knowing who is in control & who will benefit is vital
- Threats come in all sizes and dollar values
- Have a concern? Report it.

### WHAT'S TARGETED?

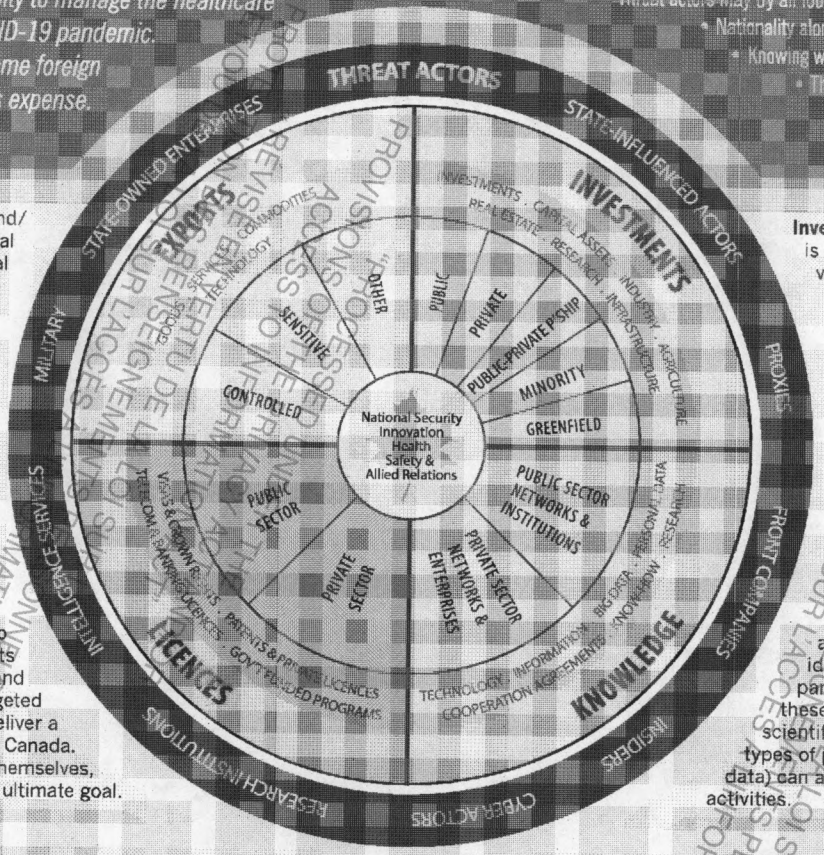
- **Medical Advancements** *(vaccines, therapeutic treatments)*
- **New Technologies** *(diagnostic equipment)*
- **Medical equipment** *(personal protective equipment)*
- **Research & Sensitive Data** *(personal health data; corporate information)*
- **Small, medium, and large enterprises**
- **Academia**

### THREAT ACTORS

TRADITIONAL: DIPLOMATS – ILLEGAL INTELLIGENCE OFFICERS – CYBERESPIONAGE – INSIDERS & PROXIES

NON-TRADITIONAL: STATE-OWNED ENTERPRISES & SOVEREIGN WEALTH FUNDS – FRONT COMPANIES – FOREIGN RESEARCHERS (e.g., government, think tanks) – TALENT PROGRAMS (e.g., scholarship schemes, sponsored trips) – ACADEMICS (e.g., visiting researchers, research collaboration)

*CAUTION: not all non-traditional actors are knowingly engaged in covert intelligence activities; however, their actions may still threaten Canadian interests.*




**Imports/Exports –** The manufacture and/or importation of goods (e.g., medical supplies, protective equipment) essential for keeping Canadians safe is critical to Canada's COVID-19 response. In order to secure their own access, some foreign governments have taken actions (i.e. export bans) that threaten to disrupt or manipulate Canada's supply chains for essential goods and/or the materials needed to produce them. The export of sensitive technologies remains a concern as threat actors continue to target them.

**Licences –** Foreign actors may seek privileged access to medicines, technologies, equipment or intellectual property through licences and rights which can be abused to deny access to others and rob Canadians of the benefits of Canada's investments in research and development (R&D). Examples of targeted licences include: patents; rights to deliver a service or product; or permission to enter Canada. Often the licences are not the objective themselves, but rather the means to a threat actor's ultimate goal.

**Investments –** The COVID-19 pandemic is creating financial distress and new vulnerabilities for Canadian companies, especially start-ups and other small businesses. Additionally, increased global competition for access to therapeutics, medical equipment, and other essential materials is elevating the risk of both espionage and predatory investment. Organizations developing vaccines and new technologies, or those holding significant amounts of health data, are at an elevated risk.

**Knowledge –** Threat actors have previously used technical and human intelligence operations to seek access to proprietary knowledge and sensitive data (i.e. personally identifiable information). The COVID-19 pandemic only increases the urgency of these efforts, especially as they related to scientific research and health data. Other types of privileged information (i.e. financial data) can also be used to inform future threat activities.

CSIS investigates threats to Canada's national security. If you have information related to potential or ongoing threat to Canada's national security, please contact CSIS:
613-993-9620 (24/7) • https://www.canada.ca/en/security-intelligence-service/corporate/reporting-national-security-information.html

Canada

PROVISIONS "PROCESSED UNDER THE ACCESS TO INFORMATION ACT AND/OR PROTECTION OF THE PRIVACY ACT"

« RÉVISÉ EN VERTU DE LA LOI SUR L'ACCÈS À L'INFORMATION ET/OU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS »



PROVISIONS "PROCESSED UNDER THE ACCESS TO INFORMATION ACT AND/OR PROTECTION OF THE PRIVACY ACT"

« RÉVISÉ EN VERTU DE LA LOI SUR L'ACCÈS À L'INFORMATION ET/OU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS »

PROVISIONS "PROCESSED UNDER THE ACCESS TO INFORMATION ACT AND/OR PROTECTION OF THE PRIVACY ACT"

« RÉVISÉ EN VERTU DE LA LOI SUR L'ACCÈS À L'INFORMATION ET/OU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS »

3103(18/09)