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?

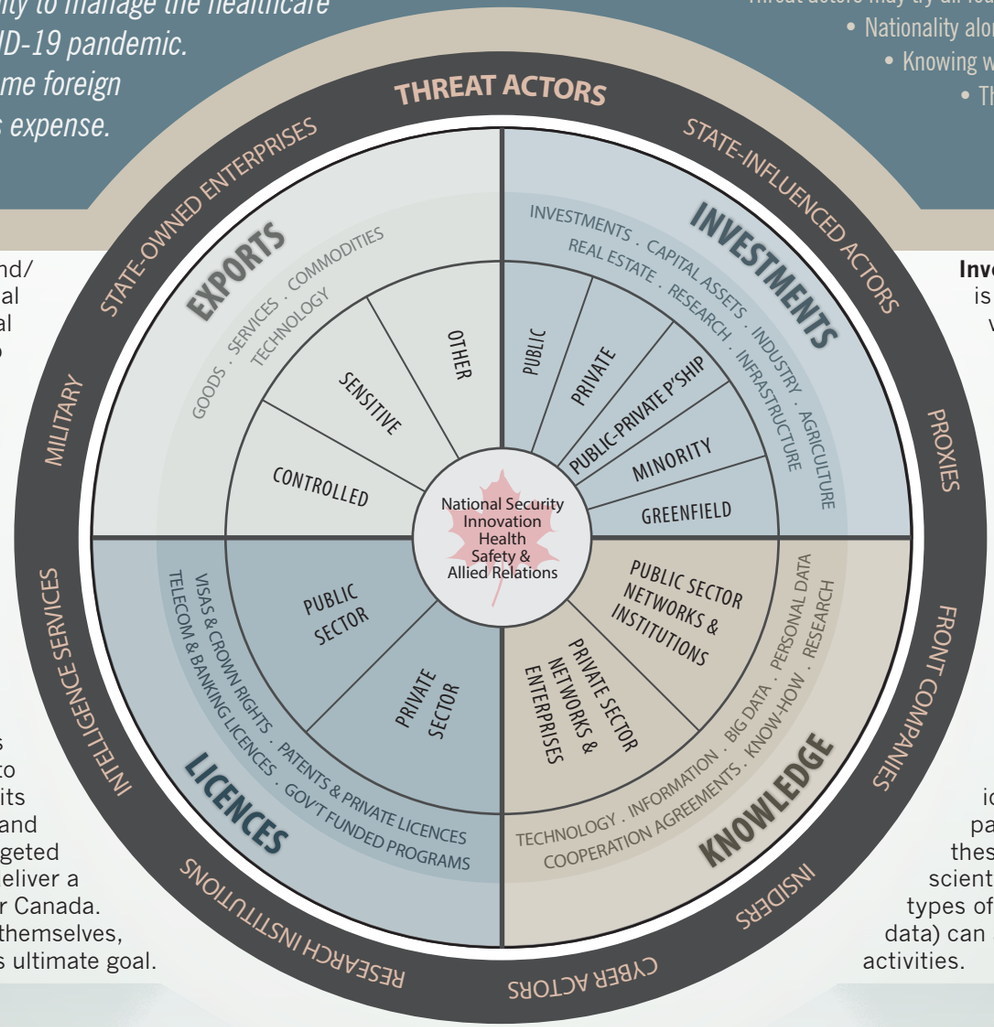
- ***Medical Advancements*** *(vaccines, therapeutic treatments)*
- ***New technologies*** *(diagnostic equipment)*
- ***Medical equipment*** *(personal protective equipment)*
- ***Research & Sensitive Data*** *(personal health data; corporate information)*
- ***Small, medium, and large enterprises***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

## THREAT ACTORS

***TRADITIONAL:*** *DIPLOMATS – 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 professorships, research collaborations)*

*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