Canadian Security Intelligence Service | Service canadien du renseignement de sécurité

Unclassified
2019 09 11

FOREIGN THREATS TO CANADA'S ECONOMIC SECURITY

the four gates of economic security: EXPORTS · INVESTMENTS · LICENCES · KNOWLEDGE

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:

- 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?

- ***Emerging technologies***
  (Artificial Intelligence, quantum, 5G, biotechnology)
- ***Early stage research in STEM fields***
  (science, technology, engineering, mathematics)
- ***Early stage commercial environments***
  (start-ups, incubators / accelerators)
- ***Small, medium, and large enterprises***
- ***Big data analytics capabilities***
- ***Critical infrastructure***
  (transportation, telecommunications, energy)

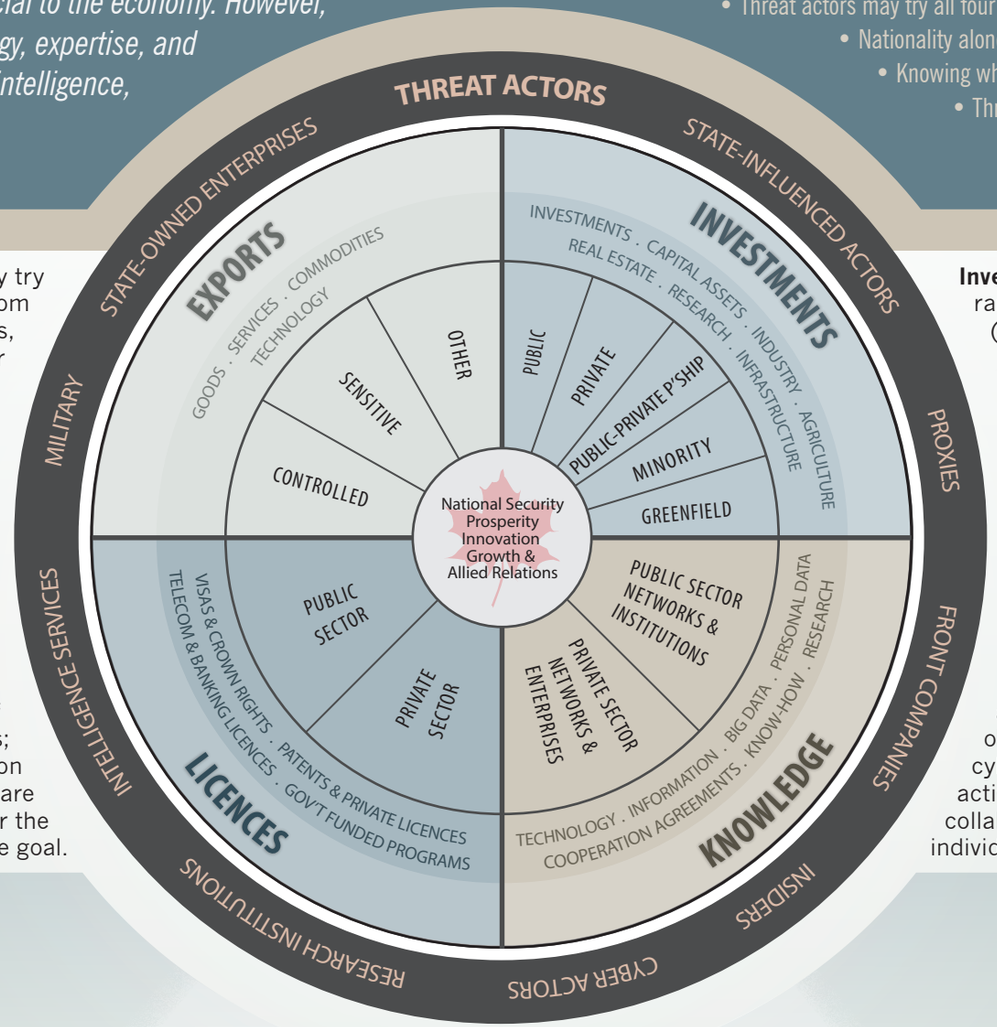
Note: Technology or information does not have to be "classified" or "controlled" for its loss to have a negative impact on Canada's national security.

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.



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/bjU650vImw6

Canada