Canadian Security Intelligence Service | Service canadien du renseignement de sécurité

PROTECT YOUR RESEARCH

YUKON

A SAFE, SECURE AND PROSPEROUS CANADA THROUGH TRUSTED INTELLIGENCE AND ADVICE.
DES RENSEIGNEMENTS ET DES CONSEILS FIABLES POUR UN CANADA SÛR ET PROSPÈRE.

/ As a core part of its mandate, the Canadian Security Intelligence Service (CSIS) investigates and advises the Government of Canada on threats posed by espionage and foreign-influenced activities. As the world becomes more competitive, states are seeking every advantage. In order to fulfil their economic and security or military priorities, some foreign states engage in espionage. This foreign espionage has significant ramifications for Canada, including lost jobs, corporate and tax revenues, as well as diminished competitive and national advantages.

In 2019, Yukon contributed approximately $2.7 billion to Canada's GDP, primarily attributable to traditional economic sectors including mining, quarrying, oil & gas, construction, transportation & warehousing and public administration. The knowledge sectors of the Yukon economy are also strong and growing, building in part on the government's science strategy with its commitment to stimulate private sector research, innovation and commercialization activities. The territory has a solid research base centred around Yukon University and the Yukon Research Centre - which has a strong focus on climate change, cold climate innovation, environmental science, and technology innovation. Innovative research and investment in renewable energy is also important to realizing development objectives for the territory. In addition, the region's telecommunications infrastructure is improving, supporting strong efforts to grow the Information Communications and Technology (ICT) sector in the Yukon.

A strong innovation culture gives the territory a competitive edge, and positions Yukon for sustainable economic growth and diversification, fostering a robust and resilient economy. CSIS has identified several of these promising sectors as, unfortunately, being of significant interest to hostile foreign actors. Sectors of the knowledge economy are particularly vulnerable to state-sponsored espionage and interference by hostile actors seeking to exploit the openness and collaborative environment that allow Canadian innovation to thrive.

As difficult as it is to precisely measure, this damage to our collective prosperity is very real. As a result, it is important that Canadians are better-informed about the threat so that they can continue to innovate, collaborate, partner and prosper with a clear understanding of the risks and the knowledge they need to protect themselves. CSIS is engaging with stakeholders in targeted sectors to increase awareness of the current threat context in Canada and in your province. This information is provided to support those in industry, academia, government, and non-governmental organizations in taking the necessary actions to protect their information, the fruits of their research and intellectual property, and their investments. The government, business, and academic communities have a shared interest in increasing awareness of state-sponsored espionage targeting Canada to mitigate the potential negative impact on our economic growth and ability to innovate. We want to work with you to protect your organization's assets, reputation and people.

Canada

/ WHICH SECTORS ARE TARGETED?

- Technology
- Biopharmaceuticals
- Health
- Transportation (Aerospace, Rail, Green Vehicles, Maritime Equipment, Supply Chain)
- Academia
- Energy
- Manufacturing

/ WHAT IS TARGETED?

- Advanced research and equipment in STEM fields
- Intellectual property
- Critical infrastructure assets
- Personally identifiable information (e.g. financial or health information)
- Government information
- Communications capabilities

More specific examples could include: designs; test results; manufacturing or marketing plans; proprietary formulas or processes; employee information; vendor and supply information; software; investment data; corporate strategies; access protocols; and patent or funding applications.

/ WHAT METHODS ARE USED?

- Cyber Espionage
- Human Espionage
- Theft and Illicit Transfer of Technology & Know-How
- Acquisition and Exploitation of Sensitive Canadian Data
- Foreign Access and Control over Critical Infrastructure
- Insider Threats
- Hostile Foreign Investment
- Reverse Engineering
- Sabotage and Disruption
- Exploitative Licensing Agreements
- Elicitation

Please note this list is not exhaustive.

/ HOW CAN I PROTECT MYSELF?

- Identify your most valuable information and protect it – don't share unless essential
- Enhance and regularly test or audit your cyber-security policies and practices
- Do your due diligence
- Vet your vendors, funders, partners, employees and visitors
- Promote a security-conscious culture
- Take a risk-management approach
- Employ strong physical security protocols
- Ensure agreements, such as contracts or partnership agreements, are equitable and reciprocal, and that conflict resolution provisions are enforceable
- Protect your assets
- Beware of unknown solicitations
- Contact authorities if you have concerns

/ WHAT IS HOSTILE FOREIGN INVESTMENT?

While the vast majority of the foreign investment in Canada is carried out in an open and transparent manner, a number of State-Owned Enterprises (SOEs) and private firms with close ties to a foreign government and / or intelligence services can pursue corporate acquisition bids in Canada or other economic activities. Corporate acquisitions by these entities pose potential risks related to vulnerabilities in critical infrastructure, control over strategic sectors, espionage and foreign influenced activities, and illegal transfer of technology and expertise. The involvement of SOEs or state-linked enterprises in these investments may be covert or concealed.

/ WHAT ARE INSIDER THREATS?

Threat actors can use trusted insiders (employees, contractors, suppliers, partners, etc.) to gain access to your organization's most valuable information. You can also hear these individuals referred to as "non-traditional collectors". These insiders can also be coerced, manipulated, compelled or incentivized to provide information or access. Behaviours that could indicate a possible insider threat risk include: irregular hours; attempted computer intrusions; showing unusual interest in information outside the scope of the individual's responsibilities; concealment of foreign affiliations or contacts; and unexplained absences or affluence. You know your organization best. Be alert to unusual or suspicious activities and behaviours.

/ WHAT IS CYBER-ESPIONAGE?

Threat actors can use cyber means such as phishing attacks or installation of malware to clandestinely obtain confidential information or steal intellectual property.

/ WHAT IS ELICITATION?

A threat actor may try to elicit information by using flattery, indicating interest, asking leading questions, claiming a mutual interest or feigning ignorance. These techniques may be employed in both professional and personal settings.

CONTACT US:

Canada.ca

General inquiries: 613-993-9620 | **Reporting National Security Information:** 1-800-267-7685

ISBN: 978-0-660-39463-3
Catalogue number: PS74-14/13-2021E-PDF
Aussi disponible en français sous le titre : *Protégez vos recherches - Yukon*