Canadian Security Intelligence Service

Service canadien du renseignement de sécurité

Research Security Blitz – University of Calgary

February 2023

A safe, secure and prosperous Canada through trusted intelligence and advice.
Des renseignements et des conseils fiables pour un Canada sûr et prospère.

Canada

Canadian Security Intelligence Service

Service canadien du renseignement de sécurité

CANADIAN SECURITY INTELLIGENCE SERVICE

CSIS IS DEDICATED TO THE PROTECTION OF CANADA'S NATIONAL SECURITY INTERESTS AND THE SAFETY OF CANADIANS

CORE MANDATE

· Investigate activities suspected of constituting threats to the security of Canada
· Advise the Government of these threats
· Take measures to reduce threats to the security of Canada

THREATS TO THE SECURITY OF CANADA

· Terrorism
· Espionage and sabotage
· Foreign influenced activities detrimental to the interests of Canada
· Subversion of government through violence

DUTIES AND FUNCTIONS

SECTION 13
PROVIDE SECURITY ASSESSMENTS TO THE GOVERNMENT OF CANADA

GOVERNMENT SECURITY SCREENING
✓ Site Access: 91,000
✓ Government: 75,500
✓ Provinces: 240
✓ Foreign: 570

SECTION 14
PROVIDE SECURITY ADVICE RELEVANT TO THE EXERCISE OF THE CITIZENSHIP ACT OR THE IMMIGRATION AND REFUGEE PROTECTION ACT
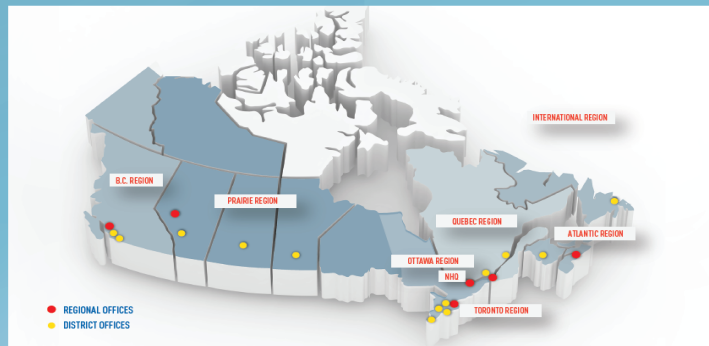
IMMIGRATION SCREENING
✓ Citizenship: 216,800
✓ Perm Resident: 18,000
✓ Temp Resident: 43,300
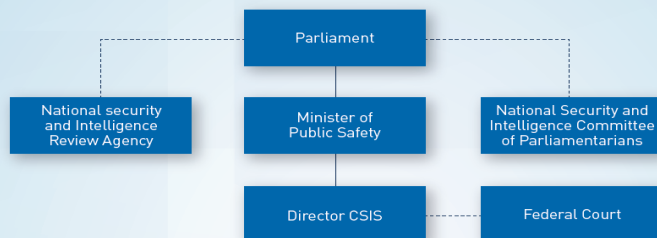✓ Refugees: 46,400

SECTION 16
CONDUCT FOREIGN INTELLIGENCE COLLECTION WITHIN CANADA AT THE REQUEST OF THE MINISTERS OF FOREIGN AFFAIRS AND DEFENCE

· Can only be carried out within Canada
· Must not target a Canadian citizen, permanent resident or corporation

CSIS ACROSS CANADA

INTERNATIONAL REGION

B.C. REGION

PRAIRIE REGION

QUEBEC REGION

ATLANTIC REGION

OTTAWA REGION

NHQ

TORONTO REGION

● REGIONAL OFFICES
● DISTRICT OFFICES

ACCOUNTABILITY MATTERS

Parliament

National security and Intelligence Review Agency

Minister of Public Safety

National Security and Intelligence Committee of Parliamentarians

Director CSIS

Federal Court

PEOPLE OF CSIS

· +3200 employees
· 20% racialized persons
· incl 2% Indigenous persons
· 4% persons with disabilities
· 119 languages and dialects spoken
· 68% speak both official languages

PARTNERSHIPS

· Over 80 arrangements with domestic partners
· Over 300 arrangements with foreign partners in over 150 countries
· Robust information sharing framework ensures conformity to Ministerial Direction

ACCOUNTABILITY

· Federal Court
· Minister of Public Safety
· National Security and Intelligence Review Agency
· National Security and Intelligence Committee of Parliamentarians

DEPARTMENTAL RESULTS

· CSIS obtains relevant information and intelligence to carry out its national security activities.
· CSIS intelligence informs government decisions and actions relating to Canada's security and national interests.
· CSIS threat reduction measures diminish threats to the security and safety of Canada and Canadians.
· The assessments of the Integrated Terrorism Assessment Centre inform Government of Canada decisions and actions relating to the terrorism threat.

Statistics as of end of fiscal year 2019-20.

Canada

Role of CSIS in GoC Research Security Approach

- National security investigations – collect intelligence, conduct analysis, provide advice to GoC

- Intelligence assessments – conduct threat assessments to inform granting agencies funding decisions National Security Guidelines for Research Partnerships

- Liaison – Maintain local operational and tactical relationships, contact to report suspected threat activity

- Academic outreach & Stakeholder engagement – increase awareness of threat and mitigations, conduit to GoC partners and operational colleagues

Current Geopolitical Context

- What's changed?
- Autocracy vs. democracy
- Technology & science critical indicators of power and competitiveness
- Civil-military fusion programs
- New capabilities of threat actors – technological, operational, legal
- Certain adversaries using any and all means, from abroad and within Canada
- Adversary approach requires collective resilience and collaborative response
- War in Ukraine – Threats Against Taiwan – Global Instability
- New opportunities and challenges in Indo-Pacific

R&D and Innovation Critical to Canada's Future

- Economic impact
- Contributions to global development and prosperity
- Technological and scientific advances
- Vehicle of soft power
- Attraction of talented students and workforce
- Opportunities for future generations
- Support for Canadian policies and commitments
- Retaining Canada's place in the world

Canadian Security Intelligence Service
Service canadien du renseignement de sécurité

Research Security
Protecting Canadian Data Science & Technology

Canada is a global research leader, due to our world-class universities, public and private research organizations, and human talent.

Canada's innovative reputation attracts threat actors: they exploit our principles of open science and collaboration; disregard Canada's laws and values; and disguise their role in serving a foreign state agenda to obtain valuable Canadian data, intellectual property (IP) and know-how.

These deceptive and malign activities harm Canada's safety, security and prosperity interests. Canada's research integrity is undermined; our knowledge-based economy is stolen; and threat actors gain powerful and destabilizing surveillance and military capabilities.

MIN   MAX

ENHANCE SECURITY LEVEL

Who & Why

- Hostile state actors, particularly China and Russia, pose the greatest threat.

- In our digital era, threats can arise from anywhere, including from non-state actors.

- The world is increasingly competitive. Hostile states seek advantage at Canada's expense. They look to advance their economic, technological, intelligence and military state interests.

- Policies and practices of Military-Civil Fusion, coercive national security laws, and state capitalism pose a growing threat.

What

Almost all Canadian research domains face some level of risk; but the top five targets are:

- Biopharma & health
- Artificial intelligence (AI), quantum, and big data
- Semiconductors, 5G, and smart cities
- Ocean technology, including sensors
- Aerospace technology, including hypersonics

How

Sophisticated threat actors will exploit vulnerabilities, including via deceptive means, such as:

- Traditional espionage
- Cyber espionage
- Insider threats
- Non-traditional collectors
- Talent spotting
- Research funding
- Unsafe supply chains *(equipment, services)*
- Joint ventures
- Minority investments *(e.g. venture capital)*
- Foreign acquisitions *(foreign direct investment)*

SENSITIVE LABORATORIES — Threat actors seek direct or indirect access to sensitive laboratories.

INTELLECTUAL PROPERTY (IP) — Control over IP may be lost, with all gains accruing to foreign states.

DEFENCE & DUAL-USE — Researchers may knowingly or unwittingly contribute to foreign military capabilities

ACADEMIC LEADERSHIP — Leading academics and administrators may be targeted or leveraged.

RESEARCH GRANTS/ FUNDING — Government funding may be subverted, and foreign funding may co-opt Canadian research and IP.

**These threats are real; and Canada is not unique in managing these challenges and risks.
Most importantly, you are not alone in facing these threats.**

Canada

Critical & Emerging Technologies Targeted

CANADA'S PRIORITIZED CRITICAL AND EMERGING TECHNOLOGIES

- Intelligence agencies are increasingly seeing adversaries use any and all means to acquire critical and emerging technologies for competitive advantage.

- As seen in this excerpt from a recent Privy Council Office National Intelligence Assessment, this includes may of the areas in which DTS members work.

- Some of this research is also targeted and known as 'sensitive technologies' due to its possible application in military, intelligence and surveillance programs.

Canada

Ways & Means

- Illicit technology transfer
- Espionage – human and cyber
- Talent and scholarship programs
- Foreign investment
- Licensing
- Joint Ventures, partnerships, agreements, collaboration
- Recruitment – Witting and unwitting
- Non-traditional collectors
- Elicitation
- Coercion
- Travel
- Supply chain

Consider intent and character of activities.

Activities of concern are covert, opaque, coercive

Focus: Insider Threat

'An insider threat/risk is an individual who either wittingly or unwittingly misuses or exploits, or intends to exploit, their legitimate access to the assets of a department of the Government of Canada, causing harm to Canada's national interest through espionage, terrorism, unauthorized disclosure of information, or loss or degradation of a capability to deliver a service or a product.'

Resources:

Resilience to Insider Risk (publicsafety.gc.ca)

The Insider Risk Assessment Tool (publicsafety.gc.ca)

How to protect your organization from insider threats (ITSAP.10.003) - Canadian Centre for Cyber Security

Insider Risk (odni.gov).gc.ca)

Focus: Travel

Risk factors / vulnerabilities:

Visa requests

Hotels & transportation

Communications

Conferences

See: Far_From_Home_2020.PDF (canada.ca) and How can you protect your research during travel? (science.gc.ca)

Laws	Date Passed	Intended Purpose	Implications
National Security Law	2015	• Outlines whole-of-society responsibilities for China's national security • Stipulates that citizens and private organizations must assist the Chinese government and intelligence entities with security issues when ordered	• Able to force Chinese companies and personnel to assist the government on national security issues • May compel locally employed Chinese personnel of U.S. companies to assist in investigations that may expose operating elements of the U.S. company
Cybersecurity Law	2017	• Outlines China's approach to cybersecurity • Mandates that critical infrastructure companies (undefined) retain their data within China's borders	• Must localize certain types of data held within China's borders, including the data of foreign companies working in undefined critical industries
National Intelligence Law	2017	• Stipulates that citizens or private organizations must assist the Ministries of Public Security and State Security in carrying out intelligence work	• Creates "affirmative" legal responsibilities for Chinese and foreign entities to provide access to or collaborate with Chinese intelligence entities • May force locally employed Chinese personnel of U.S. companies to assist in Chinese intelligence operations
Data Security Law	2021	• Classifies data in a tiered system according to the government's interpretation of the data's importance to state security • Positions Beijing to control or deny cross-border data transfers and refuse foreign government data transfer requests • Imposes stricter penalties on China-based businesses for noncompliance	• Expands Beijing's access to, and control of, companies and data within China • Expands China's ability to control the outbound flow of data

Canada

Threats to Research Security – Institutional Impact

- Financial
- Reputational
- Academic principles, ethics and integrity
- Legal
- Trust deficit
- Data, cyber and infrastructure integrity
- Privacy
- Policies, procedures, agreements
- Future prospects

Threats to Research Security – National Impact

- Economic prosperity
- Military/defence
- Human rights
- Foreign affairs & commitments
- Innovation future
- Trust in government
- Trust in science and academia more broadly
- Impact on democratic institutions
- Attracting immigration
- Reputation and global influence

Mitigation Measures

- Risk-Based Plans
- Capacity-building in due diligence
- Codes, policies, processes, reporting; identify institutional 'red lines' (if any)
- Training, awareness, tools
- Security culture with layered lines of defence
- Oversight mechanisms
- Security screening/vetting
- Data management and research security plans

- Legal review of all agreements
- Diversify funding sources
- Access controls & segregation of most valuable assets
- Seek advice – Government, allied counterparts
- Use of OSINT tools – public and commercial
- Threats evolve – reassess mitigation routinely
- Leverage assets already in your institution (e.g. interdisciplinary expertise)

Elements of a Successful Partnership

Whether in life or research, there are common attributes of a successful partnership. These include:

- Trust
- Respect
- Reciprocity
- Openness
- Honesty
- Transparency

- Common interests, values, ethics
- Shared partnership objectives
- Good communication
- Framework for cooperation
- Dispute resolution mechanism
- Individual autonomy

Government of Canada response – Research Security Highlights

2016 – Creation of Safeguarding Science program

2018 – Establishment of GoC-Universities Working Group

June 2020 – Joint CSIS-CSE statement

March 2021 – Research Security Policy Statement

July 2021 – National Security Guidelines for Research Partnerships and supporting resources (Safeguarding Your Research portal)

April 2022 - Budget 2022: funding for Research Security ($159.6 million, starting in 2022-23, and $33.4 million ongoing), intellectual property regime, Canada Excellence Research Chairs, creation of Canadian Innovation & Investment Agency

Government of Canada response – Research Security Highlights
(continued)

Fall 2022: Release of new OSINT due diligence guide and guidance on developing a research security plan – updates to Safeguarding Your Research. Investments in S&T and research security through Indo-Pacific Strategy.

December 2022: New guidance on research security funding available through the Research Support Fund

February 2023: Statement from Minister Champagne, Minister Duclos and Minister Mendicino on protecting Canada's research - Canada.ca

Forthcoming:
- First meeting of Classified Information Exchange Roundtable (April 2023)
- Publication of *revised* Risk Assessment Form.
- Publication of guide on risk mitigation strategies and progress report on implementation.
- New AOSE publication: Research Security Quarterly.
- Expansion of National Security Guidelines for Research Partnerships to additional funding streams

Ongoing and complementary: sanctions regime, export controls, visa vetting, Controlled Goods Program, Safeguarding Science program

Alberta as a Target

- Strengths and expertise in artificial intelligence, big data, geomatics, and interactive digital media.
- Emerging and growth sectors in Alberta like agri-tech, biotech/biomanufacturing, clean-tech, quantum, and fintech.
- Important research and development projects in bio-energy applications, carbon capture and storage, and electricity transmission and distribution infrastructure.
- Location of one of Canada's three National A.I. Institutes
- Home to more than 2,800 tech companies, 4 leading universities, and many tech and innovation incubators.
- Universities received approximately $295M in granting council funding in FY 2021-22.
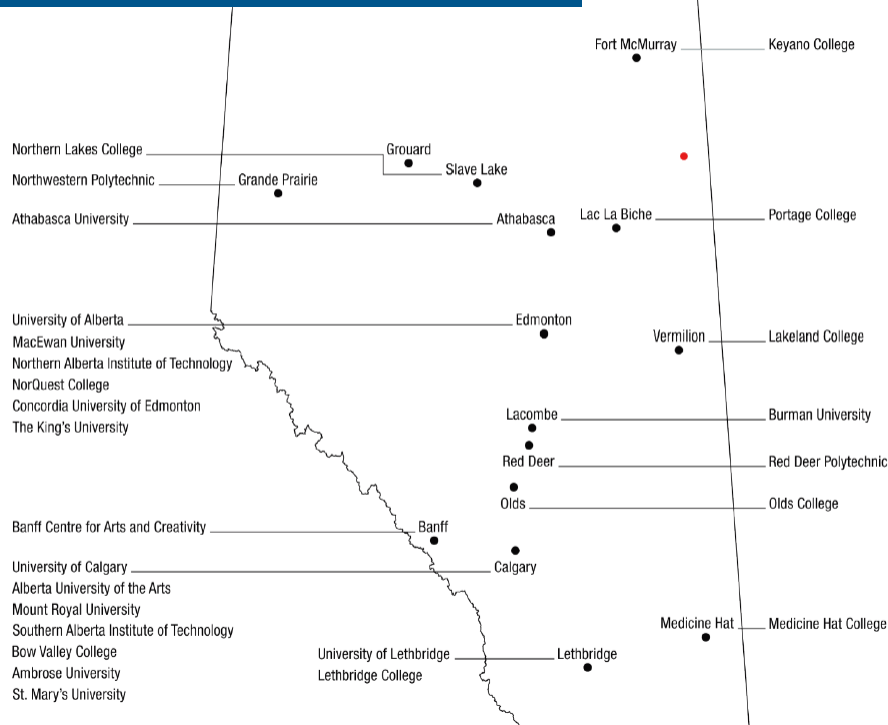- Public post-secondary institutions received approximate $5M in provincial government funding in 2021-22

Alberta Research Security Ecosytem

Post-Secondary Institutions

- Alberta Advanced Education
- Alberta Provincial Security & Intelligence Office
- Public Safety Research Security Centre – Regional Advisor (Prairies)
- RCMP INSET Public Engagement Units
- CSIS Prairie Region
- CSIS Academic Outreach & Stakeholder Engagement

Canadian Security
Intelligence Service

Service canadien du
renseignement de sécurité

Top 10 universities in Canada collaborating with China's National University of Defence Technology, by publication count

Publications from 2005 to 2022   Publications since 2017

University	Publications since 2017	Publications from 2005 to 2022
University of Waterloo	46	113
University of Alberta	57	99
McGill University	25	73
University of Toronto	15	71
University of B.C.	20	57
Simon Fraser University	18	50
University of Victoria	23	44
McMaster University	14	31
Concordia University	19	29
University of Calgary	7	25

THE GLOBE AND MAIL, SOURCE: STRIDER TECHNOLOGIES, INC.

- China-Beijing Institute of Technology
- China-China - Generic
- China-China University of Petroleum East China
- China-Nankai University
- China-Shandong University of Science and Technology
- China-The University of Hong Kong
- China-Xi'an Jiaotong Liverpool University

- China-Beijing Language and Culture University
- China-China Maple Leaf Educational Systems
- China-Harbin Institute of Technology
- China-Huazhong University of Science and Technology
- China-Northeast Forestry University
- China-Shantou University
- China-Tianjin University
- China-Xi'an Jiaotong University

- China-Beijing Normal University
- China-Capital Medical University
- China-China University of Petroleum Beijing
- China-Harbin Medical University
- China-Jiangsu University of Science and Technology (JUST)
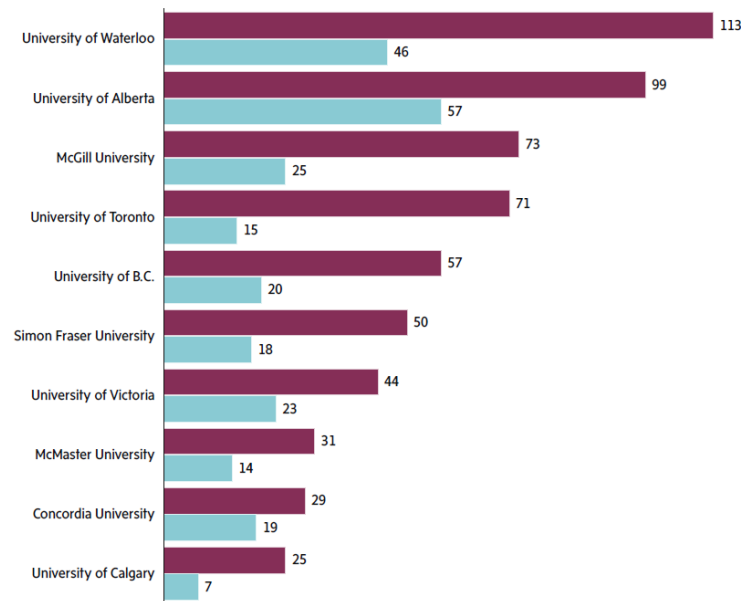- China-Shaanxi Normal University
- China-The Hong Kong Polytechnic University
- China-Wuhan University of Technology
- China-Yangtze University

Canada

Resources - Canada

[International Research Partnerships Framework | Saskatchewan International Education Strategy | Government of Saskatchewan](#)

[Academic Outreach and Stakeholder Engagement - Canada.ca](#)
AOSE's Need to Know bi-weekly newsletter
[Far From Home – A Travel Security Guide - Canada.ca](#)
[China's intelligence law and the country's future intelligence competitions - Canada.ca](#)
[Safeguarding Your Research (science.gc.ca)](#)

[Safeguarding Science (publicsafety.gc.ca)](#)

[Critical Infrastructure (publicsafety.gc.ca)](#)

[Canadian Centre for Cyber Security](#)
[CyberSecure Canada](#)
[CANARIE + CanSSOC – Stronger Together](#)

Additional Resources - Allies

- [Commission publishes a toolkit to help mitigate foreign interference in research and innovation (europa.eu)](#)
- [Trusted Research Guidance for Academia | CPNI](#)
- [Research Collaboration Advice Team (RCAT) - GOV.UK (www.gov.uk)](#) (see partner advice section)
- [Guidelines to counter foreign interference in the Australian university sector - Department of Education, Australian Government](#)
- [Home – Chinese Defence Universities Tracker — ASPI](#)
- [Protection against Foreign Interference | Protective Security Requirements](#)
- [Think before you link | Protective Security Requirements](#)
- [UK-11805-version1-cfi_manual_for_the_czech_academic_sector.pdf (cuni.cz)](#)
- [Actions Taken by Universities to Address Science and Security Concerns | Association of American Universities (AAU)](#)
- [Managing Academic Collaborations with Chinese Institutions at US Universities – YouTube](#)
- [About Foreign Interference | grants.nih.gov](#)
- [DCSA-CI_AcademicSolicitation_2021.pdf](#)
- [The China Threat — FBI](#)
- [Combating Foreign Influence — FBI](#)

Additional Resources - Multinational

- [220812-g7-sigre-paper.pdf (bmbf.de)](#)
- [G7 Information Centre (utoronto.ca)](#)
- [Integrity and security in the global research ecosystem | en | OECD](#)
- [Research security portal | STIP Compass (oecd.org)](#)
- [Commission publishes a toolkit to help mitigate foreign interference in research and innovation (europa.eu)](#)
- [Emerging technologies and dual-use concerns: a horizon scan for global public health (who.int)](#)

Case Studies Resources

Case Studies - Scenarios (science.gc.ca) (Canada)

Case studies – Governance and risk frameworks - Department of Education, Australian Government

Trusted Research for Academia Guidance - Risk Case Studies – YouTube (UK)

About Foreign Interference | grants.nih.gov (US NIH)

Case Studies | TradeCompliance.io (Various, not limited to academia)