CSIS Research Security Quarterly (RSQ)

Fall 2023

Research Security Quarterly (RSQ) is a quarterly publication produced by the Canadian Security and Intelligence Service's Academic Outreach & Stakeholder Engagement program. The product provides a curated overview of resources and developments in research security, from a range of perspectives and across a variety of jurisdictions and platforms, in order to enhance research security in Canada. Inclusion of a document, source, expert or event does not constitute endorsement by, or affiliation with, CSIS.

UPDATES

This section of RSQ provides updates on major developments on research security in Canada. Earlier this year, the department of Public Safety Canada established a Research Security Centre to serve as a resource for universities and the research community on research security. A policy announcement in relation to the February 14, 2023 Statement from Minister Champagne, Minister Duclos and Minister Mendicino on protecting Canada's research - Canada.ca is expected in fall 2023.

The focus of the Centre is to provide guidance on the implementation of the *National Security Guidelines for Research Partnerships*, including coordinating national security advice to granting agencies on sensitive applications; raising awareness through programs like Safeguarding Science, symposiums, and tailored bilateral engagement; and serving as the main point of entry for the research community to access Government of Canada services. The Centre consists of two teams: one team based in Ottawa that is responsible for policy and tools development, and the implementation of the National Security Guidelines for Research Partnerships, and another team of Regional Advisors who are located across Canada who act as liaisons with universities, the research communities, and the Provinces/Territories on behalf of the Centre.

The Safeguarding Your Research portal has been updated to include International Research Security Resources and an online course on Safeguarding Research Security with Open Source Due Diligence which is a complement to the previously published Guide on Conducting Open Source Due Diligence.

FEATURE READS

01 The Unanticipated Consequences of Technology

One of the challenges of conducting research, particularly in a sensitive area, is the complexity of anticipating possible uses and consequences. This article examines the phenomenon of unanticipated consequences of technology and discusses ethical implications of actions in this context, societal response, and the obligation to accept responsibility for those actions, *Markkula Center for Applied Ethics*. Read here.

See also: **IN CASE: A behavioural approach to anticipating unintended consequences**, *UK Cabinet Office*. Read here.

02 Reducing Insider Risk Through Positive Deterrence

This article proposes the approach of 'positive deterrence' as a complement to traditional 'command and control' programs for reducing insider risk. Positive deterrence is defined as a set of workforce practices that promote the mutual interests of the employee and employer in a way that reduces insider risk. These practices bolster employee support for, trust in, and loyalty to the employer – thereby reducing the risk of insider threats – while simultaneously improving organizational performance, *Counter-Insider Threat Research and Practice*. Read here.

03 State-sponsored economic cyber-espionage for commercial purposes: tackling an invisible but persistent risk to prosperity

The authors analysed publicly-available data on cyber-enabled thefts of intellectual property in the period since 2015 when G20 members committed not to engage in such activities. The report describes the growing scale and severity of economic cyber-espionage and shares findings that companies and universities in advanced economies are the main targets of these cyber operations. The authors also offer recommendations for increased resilience and government action, *Australian Strategic Policy Institute*. Read here.

UPCOMING EVENTS

25-26 October 2023
InCyber Forum Amérique du Nord

InCyber
REGISTER HERE
(Montreal)

26-27 October 2023
2023 Research Security Conference: Mitigating Risk in a Changing World

University of Calgary
and University of Alberta
REGISTER HERE
(Calgary)

13-15 November 2023
CSPC Conference - Science and Innovation in a Time of Transformation

Canada Science
Policy Centre
REGISTER HERE
(Ottawa)

10-14 December 2023
SRA Annual Conference

Society for Risk Analysis (SRA)
REGISTER HERE
(Washington)

FEATURE READS (CONTINUED)

04 Open Gates – Technology Transfer from Chinese Universities to the Defense Industry Through Joint Ventures

The author of this report used publicly-available bulk data to analyse and map university investment networks (joint ventures) in order to provide insights into China's civil-military fusion approach and specific entities of concern. The report is intended to offer a tool for differentiating academics and labs at civilian universities in China with ties to the Chinese defence industry from those with no such ties, *C4ADS*. Read here.

05 Europe In The Crosshairs – The PRC's United Front is Boosting Efforts to Target the Semiconductor Sector

This report uses specific case studies to explain the ways that the government of China has leveraged international talent, research collaboration and foreign investment to seek an economic and technological advantage in the semiconductor sector. Information on specific government tactics, techniques and procedures used to obtain intellectual property from entities in Europe are offered as a case study in China's efforts to leapfrog competitors in this critical technological competition, *Strider Technologies*. Read here.

CAPACITY BUILDERS

The **Safeguarding Your Research** portal is the primary resource provided by the *Government of Canada* to support research security efforts in Canada. Access here.

Trusted Research Guidance for Academia

The information on this website of the *UK's National Protective Security Authority* has been specifically tailored to the academic community and provides guidance and additional resources on a range of research security topics, including the threat and risk mitigation. Access here. Guidance is also available for Industry here.

5 Insights & Actions to Enhance Compliance Programs

This article offers recommendations derived from behavioural science and cultural psychology relevant to compliance programs. The points are broadly applicable to anyone seeking to influence behaviour and organizational culture. The recommendations include simplifying processes, improving communications, and incorporating nudges, *The Behavioural Insights Team*. Read here.

Country Reports

These country reports, developed by *The Swedish Foundation for International Cooperation* (STINT) in Research and Higher Education provide an overview of various states as prospective partners for research collaboration. Types of information provided include an overview of the higher education sector and areas of past research collaboration. STINT's website also offers a number of reports and analysis on responsible internationalisation. Access here.

Sanctions Explorer

This searchable tool draws on over 30 years of sanctions data to provide comprehensive information on current and historic sanctions, *C4ADS*. Access here. You can also find current information on sanctions imposed by Canada here.

Countering Unwanted Foreign Influence in Department-Funded Research at Institutions of Higher Education

The US Department of Defense published new guidance in June 2023 on risk-based security reviews of fundamental research. The guidance contains a number of elements which may be useful in a Canadian context including a decision matrix, key definitions, factors for assessing risk, and a list of foreign institutions confirmed by the US Government as engaging in problematic activity. See here.

EXPERT SPOTLIGHT

One of the most effective and efficient means of bolstering research security at your organization is to learn from others facing similar challenges. In this section of RSQ, we feature interviews with research security practitioners, sharing lessons-learned and best-practices.

For this issue, we spoke to **Philip Landon, *Interim President and CEO*, Universities Canada.**

Q1. What strategy have you found most effective for engaging those at your organization on research security?

Ensuring that those who need to know are well informed of the evolving situation. I've found that increasing the frequency of dialogue between policy makers, security experts and researchers at our member institutions has helped to limit speculation and build a more informed community. Many of the challenges in research security can be addressed by raising awareness of how to identify risks and providing clear guidance on how to safeguard Canadian research.

It is equally important to ensure dialogue moves in both directions. The best policy is developed when multiple perspectives are considered; research security is no different. By listening to each other, government and the research community can form a greater mutual understanding of each other's concerns and the risk environment. They can also determine how to approach research security in a way that respects the principles of academic freedom and the values at the heart of scientific inquiry.

These conversations also provide greater clarity to the research community on proposed risk mitigation processes, so that administrative burdens can be avoided. Our member universities have taken important steps to strengthen their research security practices and it's important that new measures complement these efforts in a way that avoids slowing down the pace at which Canadians researchers can establish secure partnerships.

Q2. What resources have been the most valuable to you in your role?

The National Security Guidelines for Research Partnerships, developed in partnership between the Government of Canada and universities, has been an important resource for me as I work with our member institutions. Universities are using the guidelines to develop additional measures that safeguard Canadian research, while also respecting institutional autonomy and fitting well into the institutions' existing structures. I believe the collaborative approach taken to develop these guidelines should serve as a model for addressing security challenges moving forward.

The people around me have also been an important resource. I am pleased to have a strong team working to stay abreast of the updates on this file and understand its intricacies.

Q3. What is your top professional priority in the coming months

My focus is on strengthening Canadian research. This is a difficult time for Canada, but I believe research is key to revitalizing our economy and setting us up as leaders in emerging fields.

I hope to address the stagnation of core research funding that is threatening Canada's future prosperity. Other countries have recently made significant investments in their research sectors, and Canada must take a similar approach to stay competitive.

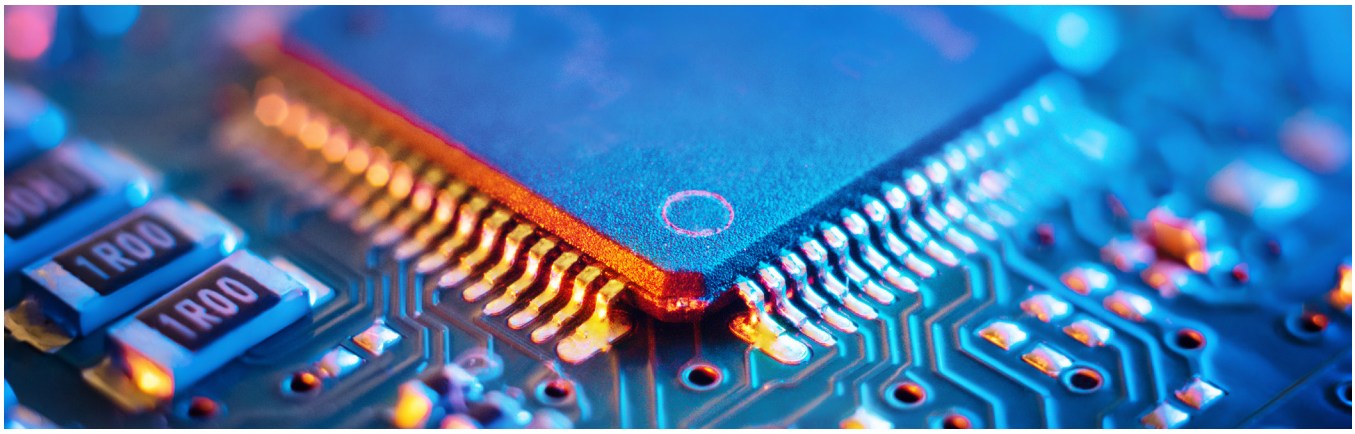
I also want to ensure research collaborations remain a central part of our research ecosystem, as they bring in new ideas and help drive R&D-led economic growth in Canada. To retain these important benefits, any restrictions on existing research collaborations should be complemented with funds to encourage other secure partnerships.

Research collaboration restrictions targeting specific regions could also inadvertently increase prejudice against associated nationalities—an outcome we hope to avoid. We will continue to engage with government to ensure that diversity, equity and inclusion remain important considerations in how such measures are implemented.

RESEARCH SPOTLIGHT: SPACE & SATELLITE TECHNOLOGY

One of the important elements of any research security plan is having full awareness which research, technologies, knowledge and data are most likely to be targeted by threat actors and why. Each issue of RSQ provides a snapshot of a different category of targeted research and information on what makes it a high-value target. This information is provided by the CSIS Scientific and Technical Services program which also supports Safeguarding Science workshops and briefings. In this issue, we discuss Space and Satellite-related technologies.

Canada is a leader in space technology having been successful in designing and building novel satellites, pioneering space robotics and a variety of other space related technologies. Increasingly, space assets are forming part of our critical infrastructure making them vulnerable to the risk of foreign interference. The space sector is growing as the cost to build and launch satellites decreases and new technologies emerge. As well as the risks from interference to space and ground infrastructure, there is the risk to potential economic and opportunity loss resulting from the proliferation of space technology in various forms (Intellectual Property, communications technology such as Quantum Communications, Global Navigation Space Systems (GNSS), etc.). In order for Canada to maintain jobs in this sector and its place on the world stage in space technology, it is critical that steps are taken to protect key Canadian space technology and make the Canadian space economy and infrastructure more resilient.



CONTACTS

For additional information on research security please contact:

CSIS Academic Outreach & Stakeholder Engagement team: SE-CI@smtp.gc.ca

Public Safety Canada Research Security Centre: researchsecurity-securiteenrecherche@ps-sp.gc.ca

Canadian Centre for Cyber Security: contact@cyber.gc.ca

Natural Sciences and Engineering Council: researchsecurity@nserc-crsng.gc.ca

Aussi disponible en français sous le titre : Trimestriel du SCRS sur la sécurité de la recherche (TSR) – Automne 2023