CSIS Research Security Quarterly (RSQ)

Spring 2023

Research Security Quarterly (RSQ) is a quarterly publication produced by the Canadian Security 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 and globally. Further to Budget 2022, a new Research Security Centre has been established at Public Safety Canada. Other recent developments in Canada include the completion of the initial pilot phase of implementation for the National Security Guidelines for Research Partnerships. Feedback received during the pilot phase will be reflected in a new version of the Risk Assessment Form as well as in an initial Progress Report on Implementation. New information on eligible research security expenses has been made available on the Research Support Fund website here. The Safeguarding Your Research portal has also been updated to include new resources including new Guidance on Conducting Open Source Due Diligence. This guidance will be complemented by an online course which will also be offered on the Safeguarding Your Research website. Finally, the University of Waterloo hosted a conference 27-28 February 2023 on Research Security in Today's Geo-Political Era.

FEATURE READS

01 **Research at risk: Global challenges, international perspectives, and Canadian solutions**

This article situates Canadian research security efforts within a broader global and historical context, with comparisons to measures taken in other liberal democracies, specifically the USA, Australia, Japan, and Israel. Recommendations are provided along the themes of centralization, collaboration, controls, and cybersecurity, and with a lens of safeguarding traditional Canadian notions of open science, *International Journal: Canada's Journal of Global Policy Analysis*. Read here.

FEATURE READS (CONTINUED)

02 University Engagement with China: An MIT Approach

This report, while written for the MIT context, contains a number of recommendations applicable to all institutions dealing with China. The authors identify red-lines and principles for all international engagements, as well as actions to strengthen risk-management capabilities. Specific guidance is provided on topics including licensing, data governance, travel, visiting students and faculty and more, *MIT China Strategy Group*. Read here.

03 The Current State of Research Data Management in Canada

The report summarizes the Research Data Management (RDM) landscape in Canada, and documents challenges and opportunities for the current RDM ecosystem. As the authors note, the growth over time of initiatives, partnerships, networks, and supporting organizations has given rise to an increasingly mature, albeit complex, Canadian RDM landscape. From a research security perspective, understanding the current status of data management is vital to ensuring effective protections and maintaining public trust. The report also provides a useful overview of Canadian and International data management efforts, *Digital Research Alliance of Canada*. Read here.

04 The Role of Hostile States in Britain's Academic Institutions: A Data Summary

This research brief provides a statistical analysis of research collaborations between UK universities and China, Russia and Iran. The author sought to emulate the risk assessment approach utilized by the Australian Strategic Policy Institute in its China Defence Universities Tracker, applying it to institutions in Russia and Iran to facilitate an overall risk assessment of UK university collaborations, *Henry Jackson Society*. Read here.

05 China's State Key Laboratory System – A View into China's Innovation System

This report describes the importance of State Key Laboratories for China's overall innovation strategy and offers comprehensive insights into their locations, priorities, and activities – including international academic exchange and collaborations, *Center for Security and Emerging Technology*. Read here.

UPCOMING EVENTS

5 April 2023
2023 Science & Security – Facilitating Compliance.

Society of Research Administrators International

REGISTER HERE

1 May 2023
EDUCAUSE Cybersecurity and Privacy Professionals Conference.

EDUCAUSE (US)

REGISTER HERE

9-10 May 2023
2023 AUECO conference.

Association of University Export Control Officers (AUECO) (US)

REGISTER HERE

14-17 May 2023
Canadian Conference on Research Administration 2023.

CARA

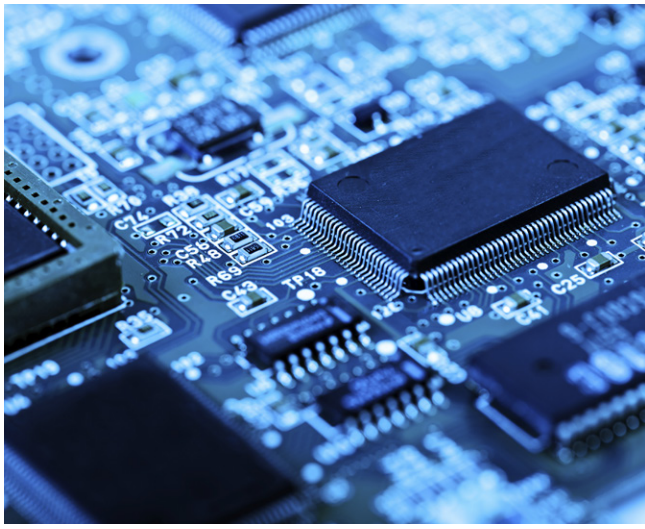
REGISTER HERE

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.

Integrity and Security in the Global Research Ecosystem

This *Organisation for Economic Co-operation and Development* (OECD) policy paper published in 2022 provides a useful starting point for those seeking an overview of research security approaches and actions adopted in OECD countries and offers recommendations to help countries develop effective policies to strengthen research security as part of a broader framework of research integrity. Read here.



inCyber is the European media hub of the cyber community, published by the team behind the FIC (International Cyber-security Forum). The group has published a number of their webinars online including this one on **Intellectual Property and National Security: The Challenges of Emerging Technology.**

Targeting U.S. Technologies – A Report of Threats to Cleared Industry

This report from the *US Defense Counterintelligence and Security Agency* can serve as a useful tool for research security practitioners seeking to understand which technologies are being targeted by foreign states, where, and how. Read here.

Academic Security & Counter Exploitation Program

This program at Texas A&M offers a number of useful resources on research security, most notably a weekly media summary and an annual conference. 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'll feature interviews with research security practitioners, sharing lessons-learned and best-practices.

For this first issue, we spoke to **Malcolm Campbell, Vice-President Research** at the **University of Guelph**.

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

Four approaches have proven effective in engaging our community about research security.

The first approach is through institutional governance bodies. Both our Board of Governors and our Senate have been attentive to research security, especially on account of its higher visibility in the press. We have provided briefings to governance bodies on research security, and their engagement has been high.

The second approach has been through representative groups of various stakeholder constituencies, who function as ambassadors for their constituencies. For example, we provide regular briefings for our Research Advisory Board, which comprises representatives for our colleges (faculties) and various research staff offices. They function as conduits for information flow about research security across the university.

The third approach is through education. This has largely been through what might be described as "passive" education - making resources available to people through voluntary information sessions and extensive web-based resources. For example, we constructed a web-based repository of information to help guide researchers on security matters.

The fourth and final approach is through real-world experience. This has largely occurred through the high level of engagement of our researchers in the NSERC Alliance program. With the pilot of research security protocols in NSERC Alliance program, many of our researchers (and our staff that support them) gained significant hands-on experience with navigating research security.

Without a doubt, engagement on research security through institutional governance bodies, particularly with our Board of Governors, and engagement through the NSERC Alliance programs, have been the most effective.

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

The online materials on Safeguarding Research that were created by the federal government have been very useful. These materials are being upgraded and updated regularly and are therefore a very important resource, particularly in terms of providing timely guidance in navigating the evolving research security landscape. Similarly the support provided by people at NSERC and CSIS over the year of the NSERC Alliance research security pilot have been very helpful. This said, perhaps the most valuable resource has been tremendous research support staff in house at our institution. These dedicated individuals who support our institutional research enterprise have dramatically expanded their understanding and navigational skills related to research security. In doing so, they have sustained the momentum of our research enterprise while helping to ensure that Canadian research is secure.

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

As a Vice-President Research my top professional priority has been and will remain providing service leadership in support of Canada's exceptional researchers and innovators, so that they generate discoveries that expand the frontiers of knowledge, that they catalyse the conversion of discoveries into game-changing innovations, and that they mobilise those innovations to generate positive real-world impacts to the benefit of Canadians.

RESEARCH SPOTLIGHT: ARTIFICIAL INTELLIGENCE

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 will provide 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 Service program which also supports Safeguarding Science workshops and briefings.

First up, Artificial Intelligence (AI). AI is an enabling technology with a multitude of applications. This broad category of technology involves the development of computational models and decision-making algorithms to emulate human intelligence for applications including natural language processing and generation; robotics and autonomous systems; computer vision; and data management and data analytics. AI has been identified as a critical technology by global economic and military superpowers. As described by the US National Security Commission on Artificial Intelligence, AI technologies are the most powerful tools in generations for expanding knowledge, increasing prosperity, and enriching the human experience. AI's impacts and applications are social, political, economic, environmental and military.

AI is also the quintessential "dual-use" technology, meaning it has both military and civil applications. The algorithms used to programmatically generate content such as realistic art, photographs and essays could also be exploited in the production of deep fakes and propaganda. Likewise, the development of decision-making algorithms for the gaming industry can have applications for robotics and autonomous systems. As such, AI dominance is anticipated to be a determining factor in ongoing global power competition with critical implications for national security.

CONTACTS

For additional information on research security please contact:

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

Public Safety Canada: ps.safeguardingscience-scienceensecurite.sp@canada.ca

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

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