CSIS Research Security Quarterly (RSQ)

Summer 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. On 24 March 2023, the Government of Canada published an updated version of the National Security Guidelines for Research Partnerships' Risk Assessment Form, taking into consideration the feedback received during the pilot phase of Guideline implementation. Also in March 2023, the Canada Foundation for Innovation published its Policy and program guide 2023 which included a dedicated section on Research Security and intellectual property. Similarly, Mitacs published consolidated guidance in the form of a Research Security Plan document in April 2023. On 28 April 2023, in conjunction with the announcement of the recipients of the Canada First Research Excellence Fund, Minister Champagne released a statement reiterating the shared responsibility for research security and expectations of a rigorous approach to research partnerships in sensitive areas. In May 2023, the University of Waterloo announced that it would end all partnerships with Huawei to safeguard scientific research, paving the way for similar announcements from a number of other Canadian universities. At this time, further details with regard to the implementation of the 14 February 2023 policy statement are expected in June.

Canadian Security Intelligence Service | Service canadien du renseignement de sécurité

Canada

FEATURE READS

01 The Contribution of Intangible Technology Controls in Controlling the Spread of Strategic Technologies

This paper provides an analysis of the potential effect of intangible technology controls on the spread of the manufacturing base for strategic dual-use technologies. To this end, the author develops a "Capability Acquisition Model" which has its conceptual groundings in the knowledge management discipline. This model is applied to China's efforts to indigenise carbon fibre production. While the is work is advanced in the context of efforts to counter the proliferation of chemical, nuclear, biological and radiological weapons, readers may draw additional insights into the use of knowledge management techniques to advance broader-research security objectives, *Strategic Trade Review*. Read here.

02 The Brilliant Inventor Who Made Two of History's Biggest Mistakes

This feature article on American inventor Thomas Midgley Jr. offers a cautionary tale in describing the long-lasting negative impacts of his inventions of leaded gasoline and commercial application of chlorofluorocarbons. As the author asserts, Midgley's story puts into sharp relief the question of how to advance innovation given the unknowability of the long-term consequences of those innovations, *New York Times*.
Read here.

03 Chinese Military-Civil Fusion: Sino-Italian Research Cooperation

This paper provides an overview of China's military-civil fusion strategy, using a case study of cooperation between an Italian Remote Sensing Laboratory and institutes closely linked to the Chinese defence sector toillustrate the possible unintended transfer of technology and knowledge from a civilian research partnership to China's military, *International Centre for Defence and Security*. Read here.

UPCOMING EVENTS

24-29 June 2023
CICan Leadership Institute for Leaders in Applied Research and Innovation

Colleges and Institutes Canada (CICan)
REGISTER HERE
(Winnipeg)

21 August 2023
20th Annual International Conference on Privacy, Security & Trust (PST2023)

Privacy Security Trust (PST) (University New Brunswick/ Canadian Institute for Cybersecurity is a sponsor)
REGISTER HERE
(Denmark/ Hybrid)

11 September - 2 October 2023
Research Compliance, Ethics and Integrity Intensive

Society of Research Administrators International (SRA)
REGISTER HERE
(Online)

22 September 2023
SANS OSINT Summit

SANS Institute
REGISTER HERE
(Online)

FEATURE READS (CONTINUED)

04 Sino-European joint ventures and the risk of technology transfer

This report provides insights into the ways that joint ventures can serve as conduits for technology transfer, drawing specifically on a sample of European-Chinese joint ventures. In addition to exploring linkages between China's Made in China 2025 strategy and the joint ventures, the authors identify areas for additional consideration including the identity and nature of parent companies in joint ventures and the scale of transfers in joint ventures compared to other commercial or scientific means, *Clingendael China Centre*. Read here.

05 The Precarious Balance Between Research Openness and Security

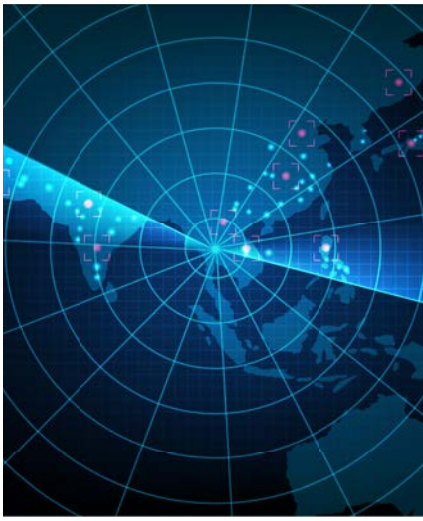
The author advocates for continued scientific collaboration with China on pressing global issues and suggests increased dialogue between leaders of scientific disciplines in the US and China to agree new rules for international collaboration which address national security concerns, scientific integrity and ethical standards, *Issues in Science and Technology*. 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.

ASPI's Critical Technology Tracker

This interactive dataset developed by the *Australian Strategic Policy Institute* allows users to track 44 foundational technologies and to compare rates of technological progress in different countries to understand areas of technological vulnerability and advantage. This understanding can inform risk assessments, offering insights into which technologies are highly sought after by specific countries and why. Access here.



Catalogue of Case Studies on Intangible Technology Transfers from Universities and Research Institutes

Of utility from a training and awareness perspective, this global catalogue of case studies published by the *Centre for Science & Security Studies at King's College London* covers countries with some of the world's most advanced research capabilities and technological expertise (including Canada – see Case Study 12). These case studies outline the challenges universities and research institutes face as hubs for technology development and the wide range of intangible technology transfer scenarios. The authors offer recommendations with a view to averting recurrence of similar scenarios. Read here.

Chinese Talent Program Tracker

This tool, developed by the *Center for Security and Emerging Technology*, offers an inventory of initiatives sponsored by the government of China to support strategic civilian and military goals. The evergreen catalogue, derived from primary Chinese sources, is an interactive tool meant to help inform policymakers, researchers/academics, and journalists navigate the array of China's talent programs. Access here.

National Knowledge Security Guidelines

While created by the *Government of the Netherlands* for a domestic audience, this document provides an excellent overview of the challenges to, and possible solutions for, securing international collaborations in an challenging geopolitical context. Guidance offered on risk assessment and management, the role of HR policies, cybersecurity and secure partnerships, collaborations and procurement provides a useful reference point for governments and institutions alike. 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 **Martha Wallace, Director of Research Security** at the **University of Calgary.**

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

Getting out there, talking and being an active listener. It's about finding common ground, building relationships, and using the right language to explain things in a manner that is clear, accessible, and inclusive. We have developed a communications plan that includes an awareness campaign and a website. Our messaging continues to be that no one team or person can be solely responsible for Research Security – we need to work together across the institution to understand potential threats and mitigate risks.

We are finding champions across the University to walk our talk and continually demonstrate the crucial importance of research security. They are using a loaner device when they travel and are coming to see us before building new partnerships.

This year we are focused on building our capacity and team and working with IT to ensure we're centering cyber security. Collaborating with existing teams is part of our approach to ensure we are leveraging the expertise of others and not creating unnecessary barriers. Our goal is to enable research, mitigate risks, and bolster new ways of thinking and finding partners. Having a strong research security program is important for a world-class research university, and we see ourselves as delivering an important service to the institution.

In the short time I have been at the University of Calgary, I have been delighted with how quickly people have adopted new behaviours such as starting a conversation about possible risks at the beginning of a potential collaboration or project, which is beneficial for risk assessment and for strengthening research. I have been well supported by my Senior Leadership team. Having buy-in from the top is crucial and goes a long way in the success of a new program like this.

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

People are always the best resource. I was one of the first Research Security Directors hired in Canada. I quickly met my counterparts across the country, participating in and helping to set up regular Team Canada meetings to discuss how we can collaborate and share best practices to strengthen the security of Canadian research.

I've found information available in open sources to be helpful, especially around the emerging issue of research security and how some of our international partners are approaching it. It's such a new field, resources are limited but we are testing new intelligence (OSINT) tools to build up this competency base.

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

Implementing policy changes related to the Government of Canada's 14 February 2023 statement regarding research security and foreign state actors is the number one priority right now. This statement is what will guide us moving forward.

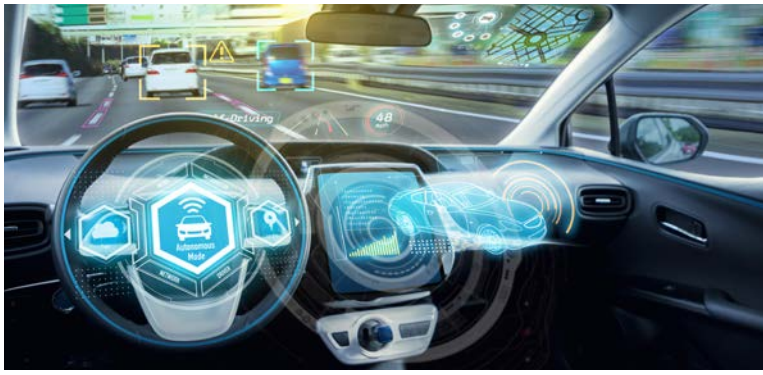
My team and I will continue to build awareness and lay the groundwork for the Research Security Division in terms of framework, roles, and responsibilities. We will take a risk-based approach and ensure appropriate systems are in place.

RESEARCH SPOTLIGHT: AUTONOMOUS SYSTEMS

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.

In the first issue of Research Security Quarterly, we highlighted Artificial Intelligence (AI). In this issue, we discuss Autonomous Systems. According to the US Department of Defense, "autonomous systems can be of two categories, at rest (software) and in motion (robots or autonomous vehicles), and must have the capability to independently compose and select among different courses of action to accomplish goals based on its knowledge and understanding of the world, itself and the situation." Fundamental to these systems is the merging of several critical technologies including sensors for data collection, artificial intelligence for decision making, advanced computing for data computation, and even communications / networking (e.g. swarm technologies). Other priority research areas include human-machine interactions, ethics and policy, trust and other barriers to adoption, and protection against interference and deception.

The diversity of research in this field, and the broad "dual-use" applicability of this technology, makes ensuring research security challenging and performing research forecasting essential. The civilian / military nexus of self-driving vehicles and delivery drone technology is well known, but realizing the applicability of the myriad of other supporting research areas and technologies is also essential; including understanding what it takes for people to trust Autonomous Systems. Research within the fields of cognitive science, neuroscience, psychology, communication, and social sciences that investigate human attitudes and experiences with the technology may provide key advances in this area. Dominance in research, development, deployment and most notably, uptake of Autonomous Systems, is anticipated to be a determining factor in ongoing global power / economic 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) – Été 2023