AOSE's Research Security Quarterly (RSQ)

Winter 2024-25

Research Security Quarterly (RSQ) is a quarterly publication produced by the Canadian Security and Intelligence Service's (CSIS) Academic Outreach & Stakeholder Engagement (AOSE) 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

Innovation, Science and Economic Development Canada (ISED) has released new guidance on the Safeguarding Your Research Portal on how to integrate security considerations into the procurement of research goods and services. Supply chains are a known vector for the theft of, interference with, or unauthorized transfer of knowledge or data. Threat actors may seek to offer extremely low-cost, and/or gifted equipment, materials, and services in an effort to gain access to sensitive physical (i.e., facilities, people, materials) or digital assets (i.e., research data, intellectual property, IT systems).

ISED's new guidance offers those purchasing research goods or services aid in identifying risks within a procurement, as well as suggestions for potential security criteria to include in a Request for Proposal to mitigate against identified risks. The guidance was developed in consultation with relevant departments and agencies across the Government of Canada, including the Canadian Centre for Cyber Security.

With the launch in 2023 of the Research Security Centre at **Public Safety Canada (PS)**, the Centre has been hard at work to fulfil its mandate as a resource for the research community on topics of research security. There was a strong desire for Safeguarding Science (SASC) workshops across this community and for the development of appropriate tools tailored to universities' realties in order to raise awareness on research security. As a result, the Centre developed and delivered interactive workshops (under the Safeguarding Science

initiative) for Canadian universities and the broader research community. The Centre leveraged expertise from several government partners to deliver workshops on topics of particular interest to the research community including dual-use technologies, immigration process, export control and sanctions. Since January 2024, the Centre delivered 46 Safeguarding Science workshops, reaching more than 100 academic institutions, totaling to more than 3300 total participants.

The Centre continues to engage with the research community to determine what are new and emerging areas of concern. Therefore, additional workshops are currently being developed to support this need. Direct engagement with research institutes across Canada is a key component of the mandate of the Centre. An interesting example of such an engagement is the recent visit by a Regional Advisor from the Centre to Iqaluit, Nunavut.

This was the first time the Centre had an in-person engagement with the region on the topic of research security. Not only was it an opportunity to meet various institutions faced with same issues of safeguarding research and the chance to deliver an in-person Safeguarding Science workshops, but it facilitated collaboration with the Artic community on topics that were relevant to the North.

Did you know?

The Research Security Centre not only offers Safeguarding Science workshops but is also a resource for researchers and universities if they have questions about research security.

Make sure to reach out to our mailbox researchsecurity-securiteenrecherche@ps-sp.gc.ca if you need support.

Feature Reads

01 **Dual use concerns in artificial intelligence and the neurosciences: How medical research can end up in war**

While Dual Use Research of Concern (DURC) has been fully analyzed as a concept and 'term of art' in the life sciences, there is a gap in applying it in newer fields of research. The authors aim to fill that gap by examining the possible misuse of Artificial Intelligence, neurotechnology and neuroenhancement for military purposes. Drawing on their findings, the authors make a number of important recommendations including the need for an international effort and agency to monitor research and establish appropriate safeguards to cover *all* fields of research. They emphasize the critical need for greater awareness of DURC within the medical research community and for thorough review of research flagged as DURC to ensure appropriate risk mitigation and regulation, *Research Ethics*, Read here.

02 **Undercover Infrastructure: Dual-Use Arctic Satellite Ground Stations**

This research paper delves into the dual-use nature of space assets and infrastructure, highlighting the challenge of managing these technologies by looking at the example of satellite ground stations in the Arctic. The authors clearly explain the dual-use nature of the technology and infrastructure, the value it holds

Upcoming Events

24-28 February 2025
Academic Security & Counter Exploitation Annual Seminar

University Research Security Professional's Association
More Information here

March 18 2025
Safeguarding Canadian Research, Alberta Views

Canadian Association of Research Administrators (CARA)
Register here

in a contested strategic landscape, and the complications of regulation, particularly given that many of these ground stations are owned by private commercial interests, universities, or multinational scientific research consortiums, *Centre for International Governance Innovation*, Read here.

03 Critical Dual-Use Technologies: Commercial, Regulatory, Societal and National Security Challenges (Draft)

This paper makes the case for a more comprehensive NATO framework for regulating trade in sensitive technologies with competitor nations, including better enforcement tools, risk assessments, sanctions, export controls and scrutiny of investments. It also argues for a coordinated technology development program to ensure NATO allies remain competitive, particularly as AI speeds the pace of technological development. The authors note *"Dual use technologies pose a particularly daunting challenge…as their military potential as well as their capacity to facilitate human rights violations is not always evident. Allied governments need forward looking criteria to make these assessments, and the reflection process should engage government, the military, universities, and the private sector"*, *NATO Parliamentary Assembly, Economics and Security Committee*, Read here.

04 Dual-use Research and Trade Controls: Opportunities and Controversies

This article makes an important contribution in identifying the meaning of 'dual use' in various contexts and offering a working definition for the export control context. The author presents measures presently governing dual-use research that could be applied in combination with trade controls for greater impact, drawing on European and US case studies. They also explain the nexus between research and export control, noting that researchers have a responsibility for applying for an export authorization when they export controlled items in the context of their research. The author further asserts that one function of trade controls, in an era where much strategic research happens outside government, is they can act as a lever to force research institutes and industry to conduct research responsibly, *Strategic Trade Review*, Read here.

05 AI and Biorisk: An Explainer

This brief paper breaks down the reality behind growing concerns - as reflected in the media and government directives - about the impact that Artificial Intelligence could have on the existing biorisk landscape. The authors suggest that while important barriers to bioweapons development are unlikely to be removed for scientifically naive users, the application of AI to Biological Design Tools could be used by malicious actors to pathogens with more severe, targeted, or dangerous phenotypes, or that evade screening and detection measures. The authors recommend clearly defining the threats of concern and developing targeted mitigation measures, *Center for Security and Emerging Technology*, Read here.

12-15 May 2025
46th IEEE Symposium on Security and Privacy

IEEE ComputerSociety Technical Committee on Security and Privacy

Register here

On Demand
Dual Use and High Risk - Navigating the Challenges of Export Controls for Financial Institutions

Global Affairs Canada and Certified Financial Crime Specialists

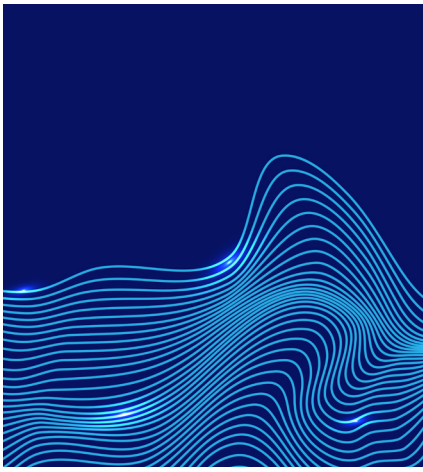
Register here

Capacity Builders

Safeguarding Science Module 2: Dual-Use Technologies: Know Your Research – Know your Partners - Assess the Risk

The module elaborates on dual-use technologies and research with specific examples. These examples highlight the complex nature of dual-use technologies, and ways to recognize their sensitivities. The outcome of the module will enhance understanding of the dual-use nature of any research, whether in STEM or social sciences, and give frontline researchers and institutions tools to perform their due diligence and evaluate risks appropriately.
Register here.

Capability Maturity Model - Knowledge Security



This guidance document was developed cooperatively by universities in the Netherlands. It provides an invaluable starting point to understand the key elements of a research security framework at an institution, and a path to gaining greater research security capability and maturity.
Read here.

Dual Use Research: A Dialogue

This educational video was produced by the National Institutes of Health (U.S. Department of Health and Human Services) to raise awareness and understanding about the issue of dual use life sciences research. The video offers a conceptual introduction to the issue and features interviews with leading American experts .
Watch here.

Dual-Use Quickscan of the Netherlands Biosecurity Office

Researchers can enter data into this tool to identify potential dual-use aspects. The tool can also be used to support related consultations and decision making.
Access here. See also this guidance on the dual-use assessment process.

Tools for Innovation Monitoring, TIM Dual-Use

The European Union Joint Research Centre developed this tool which can assist researchers and research security administrators in navigating research results and identifying those that could potentially be used in ways that contribute to the proliferation of weapons of mass destruction. The web-based platform can be used to search a database of over 70 million documents including abstracts and patents. The user can visualize the results of the queries in detailed lists and graphics, including powerful visualizations of knowledge maps and cooperation networks.
Access 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 **Jacqueline Littlewood, Director, Research Security, University of Alberta**

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

A1. Our most effective engagement strategy has been the provision of information tailored to the needs of recipients at the time they were most interested in receiving that information. We know that researchers are extremely busy, so finding ways to deliver the information they need, when they need it, and in an accessible manner is our priority. We now offer the option for members of our community to book specific types of consultations or support through our website or they can also contact us through a central email address. We have found that the University of Alberta community really values tailored support and appreciates the premium we place on building relationships. We have also found that building on the existing networks and knowledge of our research administration colleagues has been a significant advantage in realizing our engagement objectives. In addition, one important engagement focus is building research security capacity as a professional competency in early career researchers and graduate or postdoctoral students.

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

A2. Coming to this role from outside of academia, the support offered by my colleagues and leadership within the institution has been invaluable. The culture and organizational structure of the University of Alberta are very different from the federal government and colleagues' assistance in navigating that landscape was crucial. My team has also been essential to achieving Safeguarding Research Office objectives - each of them brings unique experiences, knowledge and dedication and together we're achieving some significant milestones in our vision for safeguarding research. The members of the 'Team Canada' research security group, and particularly Martha Wallace at the University of Calgary, have been an important source of information and support. Finally, Martha and I are working together to advance the Alberta Research Security Community of Practice and we hope it will also be a resource to all Alberta post secondary institutions, particularly those in the early stages of developing a research security approach.

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

A3. My top priority is continuing to implement our vision for making the University of Alberta a secure ecosystem for innovative research, including by integrating research security throughout the research lifecycle. We recently welcomed two additional members to the Safeguarding Research Office who will be focused on assisting researchers in implementing their risk mitigation plans. Getting these Implementation Support Leads out into our community is a major focus area for me right now. I'm also looking forward to seeing some communications and engagement initiatives come to fruition, including launching a podcast, delivering more great newsletter content, and holding our first annual Research Security Day. In addition, we are in the process of standing up a travel security program, building on the great models developed by counterparts at other Canadian universities.

Research Spotlight:
Marine tech – acoustic surveillance and underwater sensors

One of the important elements of any research security plan is having full awareness of 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 Services Program, which also supports Safeguarding Science workshops and briefings.

This issue of Research Security Quarterly, we highlight underwater sensors and sensor networks.

In January 2024 the Government of Canada released its Policy on Sensitive Technology Research and Affiliations of Concern (STRAC), aimed at balancing the principles of openness and collaboration in the research ecosystem with safeguards to protect Canadian innovation. Included in the STRAC policy was the Sensitive Technology Research Areas list – a list of advanced and emerging technologies that are of particular interest to foreign states, state sponsored actors, and non-state actors. Underwater sensors and sensor networks feature prominently on this list.

The ocean environment poses a unique challenge for common sensing technologies based on optics or electromagnetic radiation, as electromagnetic waves rapidly attenuate in water due to scattering and absorption. On the other hand, sound propagates through water at very long distances, especially at lower frequencies, making acoustics ideal for sensing and communications in the marine environment.

Hearkening back to a Hollywood Cold War-era thriller, SONAR (sound navigation and ranging) and hydrophones (underwater microphones) may be the two underwater acoustic sensing technologies that immediately come to mind for most readers. While these techniques have a clear nexus to military and national security applications, the underwater sensing landscape is much more varied and the security implications increasingly complex.

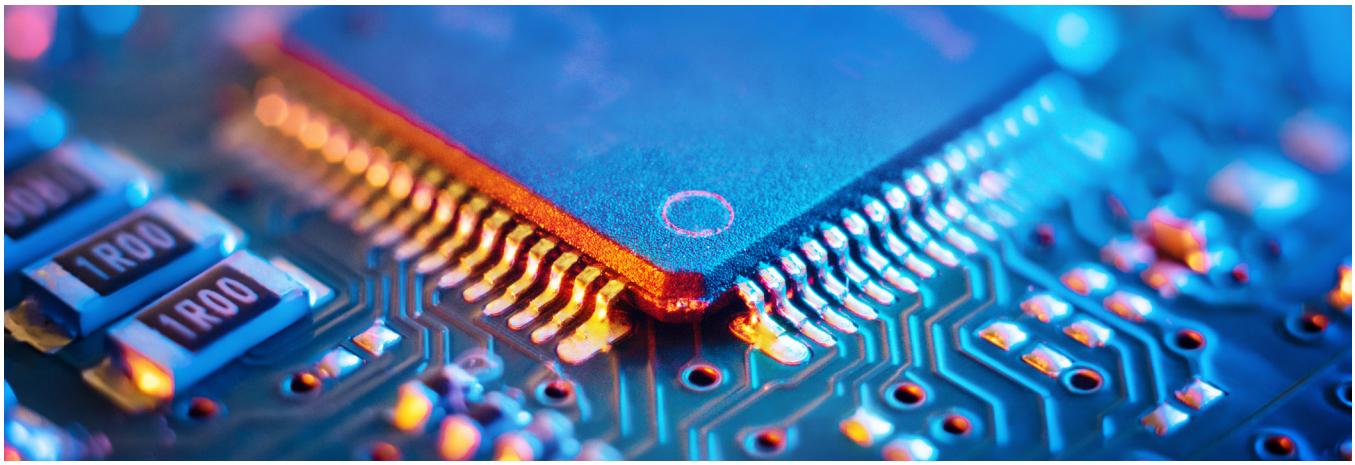
Within the oil and gas sector, for example, acoustic sensors are employed to locate oil reserves, monitor pipeline health, and assess oil platform structural integrity. Meanwhile, researchers and government fisheries management agencies employ sensors and sensor networks to track marine life populations and monitor ocean biodiversity. Environmental scientists utilize these sensors (and others) to detect changes in water temperature and chemistry [density, salinity, oxygen levels, etc.], and map ocean currents, sea ice thickness, and seafloor topography. This latter area is becoming an increasing area of interest as countries grapple with the effects of climate change, which is having are having a drastic impact on the ocean and disproportionately affecting the North. The deployment of sensors and sensor networks within Canada's ocean environment will only continue to increase and become an increasingly important source of information on the global impact of climate change.

So how does commercial and academic related research translate to national security risks? As sensors and sensor networks become increasingly connected to the internet, adversaries are more readily able to undertake cyber attacks to access the networks to monitor and track the movement of Canadian and allied military vessels in Canadian waters; alternatively, they can use the same means mask their own vessel movement. By using existing sensors, adversaries no longer need to deploy their own to detect, identify and communicate with objects that are submerged in water. Adversaries are also interested in understanding Canada's detection and monitoring capability.

Beyond the obvious benefits, our adversaries and strategic competitors are keenly interested in acquiring ocean floor topography data for several reasons. This information can enhance their surface and subsurface navigation capabilities, particularly in the Arctic region. Additionally, it can help them

identify critical undersea infrastructure, such as pipelines and telecommunications cables, which could become targets in a conflict. Furthermore, this data can provide insights into exploitable undersea resources and inform Canada's territorial claims.

However, it's not just about the data itself. The supporting infrastructure, data transmission methods, and algorithms used to process and analyze the information can also be leveraged by adversaries to improve their own marine defense systems and offensive capabilities. As with all dual-use research, it's essential for researchers to consider the potential risks and unintended consequences of their work. They must ask themselves how their methods and data could be used by those who do not share our national interests. By taking a step back and adopting a more nuanced perspective, researchers can better understand the potential implications of their work and take steps to mitigate any potential risks.



Contacts

For additional information on research security please contact:

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

Aussi disponible en français sous le titre : Trimestriel sur la sécurité de la recherche de la Liaison-recherche et Collaboration avec les intervenants – Hiver 2024-25