AOSE's Research Security Quarterly (RSQ)

Guest Edit: uOttawa

Summer 2025

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.

Feature Reads

01 **Highlights of the International Year of Quantum Science and Technology 2025:**
This UNESCO article highlights the significant milestones in advancing quantum science for global progress, including initiatives to bridge the quantum divide and promote inclusive development. Read here.

02 **The G7 Reimagined: Navigating a Multipolar World:**
This article explores the shifting global landscape and the challenges facing the G7 as rival alliances emerge. It highlights the rise of artificial intelligence (AI) and quantum computing, stressing the need for ethical frameworks and cybersecurity regulations to prevent authoritarian models from dominating the global tech agenda. Read here.

03 **Canada as a Norm Entrepreneur in Quantum Science and Technology:**
This article explores Canada's role in shaping global norms for quantum science and technology. It highlights how Canada has historically engaged in norm entrepreneurship, using international institutions to advance its national interests. Despite challenges to the liberal international order, some institutions remain resilient, allowing Canada to continue influencing global quantum policies. Read here.

04 **Demystifying Quantum Computing (DDN2-A54):**
This article explores the fundamentals of quantum computing, explaining how it differs from traditional computing and the opportunities it presents. It highlights that quantum computers operate using tiny particles rather than conventional computer chips, allowing them to solve problems that classical computers cannot handle efficiently. It discusses the potential risks associated with quantum computing, particularly in cybersecurity, and the ongoing efforts to develop robust encryption protocols. Additionally, it touches on Canada's National Quantum Strategy, outlining key areas of quantum technology development.
Read here.

05 **A Review of Quantum Cybersecurity: Threats, Risks and Opportunities:**
This research paper explores the complex interplay between quantum computing and cybersecurity, highlighting how this emerging technology can both pose significant threats to current encryption methods and present new opportunities for enhanced cybersecurity solutions. Read here.

06 **Quantum Computing threats to cybersecurity:**
This article highlights concerns that quantum computers could eventually break current encryption methods, particularly RSA-2048, which is widely used to secure sensitive data. While experts estimate that a quantum computer capable of this level of decryption may not emerge until 2055-2060, some argue it could happen as early as 2035 with advancements in error correction and algorithm design. Read here.

Upcoming Events

26-28 August 2025
Conference: 22nd Annual International Conference on Privacy, Security, and Trust (PST)

Fredericton, NB
See here

27-28 August 2025
Conference: 2025 Emerging Technologies (ETI) for Defence Conference & Exhibition

Washington, D.C.
See here

20-25 October 2025
Conference: 100 Years of Quantum: Perspectives on its Past, Present, and Future

Waterloo, ON
See here

Updates

The Research security Centre (RSC) hosted an online information session for universities in early May 2025, in collaboration with the Canada Border Services Agency (CBSA). During this session, the Proliferation Operations Section demystified CBSA processes as they pertain to research security and presented exclusive case studies involving illicit procurement tradecraft, while highlighting examples of how CPOS representatives collaborate with universities to mitigate threats.

The RSC also introduced two new Safeguarding Science training modules, covering risks while travelling (module 6) and techniques for conducting open-source research (module 7). These modules, designed for the academic research community, were offered for the first time in May 2025. The Safeguarding Science schedule can be viewed by clicking here. The fall schedule will be announced soon, so stay tuned!

Module 6, titled: "Travelling Safely: Protecting Your Research While Travelling Abroad," provides a global overview of the threat environment when travelling, a summary of techniques used by foreign governments to gain advantage of the research, and best practices to follow before, during, and after a trip.

Module 7, titled: "Conducting Open-Source Due-Diligence" provides an overview of open-source due-diligence techniques for researchers to use when evaluating the risks related to their potential partners. The outcome of this module will enhance researchers' ability to find relevant information using open-source methods.

The Safeguarding Science training module schedule can be viewed by clicking here. Full programming will be announced soon.

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.

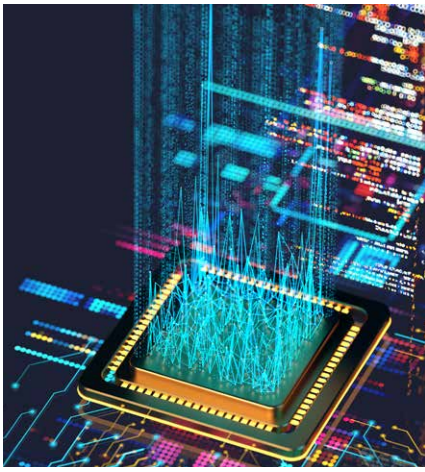
Capacity Builders

Safeguarding Your Research portal

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

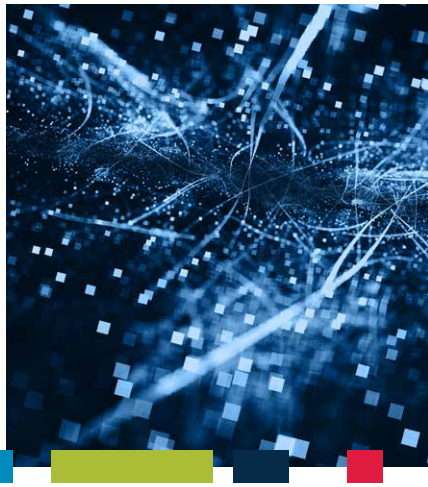
Webinar: Quantum Supply Chain Vulnerabilities Within NATO

This webinar explores the opportunities and risks associated with NATO's evolving quantum supply chains. It highlights key vulnerabilities, including dependencies on non-NATO sources for rare earth elements, exotic materials, and semiconductor manufacturing processes. The discussion focuses on actionable recommendations, such as enhanced coordination with existing semiconductor initiatives, the development of domestic processing capabilities for critical materials, and strategies to establish secure supply chains. These efforts aim to mitigate supply chain risks while fostering a more resilient and competitive quantum technology landscape within the Alliance. Register here.



Quantum Computing Course – Math and Theory for Beginners

This course provides a solid foundation in quantum computing, covering essential mathematical concepts and theoretical principles. The course introduces complex numbers, matrices, eigenvalues, and quantum mechanics fundamentals, leading to an understanding of qubits, superposition, and quantum gates. It also explores quantum circuits, entanglement, and key algorithms such as Deutsch's Algorithm and Shor's Algorithm. Designed for beginners, this course offers a structured approach to grasping quantum computing concepts and their applications. Watch here.



The scanning probe microscopy technique

This video introduces the scanning probe microscopy technique to visualize the structure and electronic properties of quantum matter at the scale of individual atoms; this is used to understand the fundamental properties of materials such as 2D (two-dimensional) ones. This will enable next-generation quantum technologies such as powerful computers and un-hackable communications. Watch 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 **Didier M. Kabeya, Director, Research strategic initiatives (Security) at the University of Ottawa.**

uOttawa

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

A1. We have found it most effective to act simultaneously at the strategic and technical level.

At the strategic level, it was important to quickly engage upper management, including the administrative apparatus, to both inform them of the new policies and to understand their vision regarding the compliance process. As part of this process, our directorate also developed a five-year strategic plan, with the aim of promoting a secure research environment by 2028. This strategy resulted in clear buy-in and much-needed support from upper management, empowering our directorate to act quickly and decisively to establish internal processes. Additionally, our team has been hard at work connecting with various teams (e.g. Information Technology, the Office of the Chief Risk Officer, etc) to share its mandate and identify areas where the directorate can learn from others and collaborate to provide better support to the research community. Our overall goal with these processes is to provide our research community with more streamlined services and access to timely and tailored expertise.

At the technical level, it was key to engage with researchers, research administrators, and research advisors to understand their needs with these new processes. We then designed tailored in-house tools, including a support flow chart and due diligence guides, and delivered workshops to support the research community. We have found it particularly effective to work closely with research advisors at the faculty level, since they provide direct support and significant guidance to researchers. By training the research advisors on the basic requirements and due diligence methods, they are equipped to offer this information to researchers when competitions take place, and to connect the proposal team with the research security team at the appropriate times. This approach has ensured our researchers get the information they need only when they need it, which is critical given how busy they are.

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

A2. Upon receiving the mandate to establish the first ever research security directorate at uOttawa, we initially relied on my background in the national security apparatus and my extensive network, including with peers from the U-15. Beyond that, we have found the diversity of experience and perspectives of the members of Team Canada to be incredibly valuable. Team Canada is a community of practice group wherein directors of research security of all Canadian universities meet to share best practices and learn from each other. Many universities have been open in sharing tools or processes they are working on, and that has helped us build uOttawa's research security model.

Additionally, we have relied on government resources such as the Protect Your Research and Safeguarding Your Research webpages, as well as those shared within Team Canada and Team Ontario communities of practice and international partners. Team Ontario does similar work as Team Canada but on a provincial (ON) level.

Finally, we have worked hard to develop a system of tracking applications and upcoming workload. There is still room for improvement, but even in the early stages it has been a useful resource to quantify our application volume and thus prioritize our work, not to mention demonstrating to our colleagues and upper management the impact of our work on obtaining research funding.

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

A3. Our top professional priority is to continue working towards fostering a culture of research security and ultimately, promoting a secure research environment. We plan to do this through several specific initiatives.

First, we're continuing to increase awareness and engagement across the university by continuing with the bottom-up approach strategy that consists of touring all faculties to discuss research security requirements with researchers and to provide an opportunity to hear any questions or concerns, particularly about risks relevant to their areas of research. We also plan on adding research security requirements tailored to the funding opportunities highlighted in an internal bi-weekly newsletter sent out by the Research Management Services team.

Second, we have been working hard to put together an inaugural France-Canada Research Security Observatory, first with the Université Côte d'Azur (UniCA) but with a view to extending to the G7+ group. The goal is to facilitate responsible dialogue on open science and the conduct of international research collaboration in consideration of evolving research security standards. Signing a framework of agreement is the next step in this process.

Finally, our office is planning a bilingual research security conference for Fall 2025 meant to bring together a wide range of members within the research security community (including government spheres) to discuss the rapidly evolving practices in this field and the potential consequences for open science and geopolitics. The event is meant to happen every two-years in the heart of Canada's national capital region.

Research Spotlight:
Quantum technology driving Canada's future prosperity

Quantum technology represents a strategic frontier where leadership confers profound economic, security, and geopolitical benefits. By investing early, consistently, and strategically, Canada can build unique economic advantage; strengthen its national security while elevating its role in producing world-renowned scientific excellence.

Quantum technology includes innovations that depend on quantum mechanical phenomena such as superposition, entanglement, and coherence to process, transmit, and measure data in ways beyond the capability of classical systems.

This year marks the 100th anniversary of the development of quantum mechanics. The United Nations proclaimed 2025 to be the International year of Quantum Science and Technology. This is timely, given that over the last twelve months major tech players, governments and venture capitalists have accelerated funding in this emerging technology ushering in what many describe as the "quantum era" with global forecasts projecting up to $USD 200 billion in economic value by 2030 as hardware scales and error correction improves.

The Dual Use Nature of this Technology:

Quantum technology is dual use – meaning it can serve both civilian and military uses. Quantum research funded by national science agencies often flows seamlessly into defense applications, while military driven R&D conversely finds its way into commercial spin-offs ranging from healthcare to finance. Recent reports emphasize how civilian quantum advances can be repurposed for secure communications, navigation, and sensing – raising important questions about export controls, intellectual property, and strategic capability.

In the military domain, quantum computing promises unparalleled computational speed for optimization, simulation, logistics planning and codebreaking. Quantum sensing devices, such as superconducting quantum interference devices (SQUIDS) and nitrogen-vacancy center magnetometers offer nanoscale precision in detecting magnetic anomalies, enhance underwater detection and enable navigation in GPS denied environments[1]. Quantum communication networks employing entanglement can ensure tamper-evident links for military command-and-control, leading to fundamental changes that will streamline the decision action cycle on the battlefield. Quantum cryptography leverages the fundamental unpredictability of quantum measurements to achieve the ultimate in security using real random number generation for the creation of keys.

Quantum technology could have a profound impact on military capability development. Quantum sensors are being developed that exceed the sensitivity of classical sensors by several orders of magnitude.

The economic/commercial uses for quantum are just now emerging. Quantum computing will bring advances in material science and drug discovery. Quantum simulators can model molecular interactions at unprecedented fidelity. Logistics companies are already exploring quantum enabled logistics optimisation to find the improvements in systems involving complex trade-offs.

[1] SQUIDS have been developed that can measure magnetic fields as low as 5 x 10^{18} Tesla. This is approx. 1x10^{13} times weaker than the Earth's magnetic field.

In the next five years, Noisy Intermediate Scale Quantum (NISQ) devices will mature focussing on error mitigation rather than full fault tolerance. Several companies including IBM have published roadmaps targeting fault tolerant systems by 2030. U.S. Defence Advanced Research Projects Agency (DARPA), through its Quantum Benchmarking Initiative, is prepared to invest hundreds of millions of dollars in companies that show the best chance at developing useful quantum computers. By 2030, Quantum Insider predicts more than USD 800 million of value added from quantum sensing technology.

By 2035, breakthroughs in error correction and scalable architectures should bring scaled fault tolerant quantum computers online enabling quantum advantage applications in chemistry, biology, and material science. Simulation and optimization capability will find uses in both finance and logistics. Parallel processing will speed up space-based image processing and decision support for use in military operations. Assuming an exponential improvement in qubit quality and scale, the first commercially available devices may perform tasks beyond the reach of classical supercomputers.

In conclusion, the advent of quantum technology represents a pivotal moment in Canada's history, offering unprecedented opportunities for economic growth, national security, and the achievement of the scientific high-ground. As the world embarks on the "quantum era," Canada can seize the day in order to establish itself as a leader in this field, leveraging its unique strengths and strategic investments to drive innovation and multi-domain competitive advantage. With the potential to generate up to $CDN 139 billion in economic value and create over 200,000 jobs by 2045, Canada's quantum sector is poised to become a cornerstone of Canada's economy and a key driver of its global competitiveness. By prioritizing investments in quantum research, development, and talent, Canada can ensure its sovereignty in this critical technology, safeguard its national security, and unlock breakthroughs in fields such as climate modeling, cryptography, chemistry, and material science.

Contacts

For additional information on research security please contact:

CSIS Academic Outreach & Stakeholder Engagement team: AOSE-LRCI@smtp.gc.ca