Research Security and Open Scholarship in Canada

by **Caroline Winter** | 17 November 2023 | **English**, **Observations**, **Observations and Responses**

Lisez-le en français

This observation was written by Caroline Winter, with thanks to Aaron Mauro and John Simpson for their feedback and contributions.

At a glance:

Title	Research Security and Open Scholarship in Canada

Creator	n/a
Publication Date	n/a
Keywords	research security, open data, scholarly communication

Research security—the ability to identify risks to research processes and outputs and take measures to mitigate them—is a longstanding concern for the research community and its stakeholders, from individuals to national governments. Although openness and collaboration are essential for advancing research, greater openness can also lead to greater risks. Securing digital data, knowledge, and other intangible outputs is especially challenging. This was made evident during the COVID-19 pandemic, when the pivot to virtual work environments and unprecedented levels of global collaboration and research sharing was accompanied by increased security threats (see **"Open Scholarship and COVID-19"**).

Research security is a broad issue that relates to all facets of research. For individual researchers and institutions, data theft and other security issues can hamper research, threaten intellectual property, and affect funding eligibility (see **"Intellectual Property Rights and Open Scholarship in Europe"**). Research security is also a national security issue since misappropriated data and knowledge can be used for nefarious intelligence or military purposes. Security is of particular concern for economically valuable and dual-use research—that with potential civilian and military applications—such as in the areas of critical infrastructure and research with human subjects as well as quantum computing and artificial intelligence, both of which are potential tools for cyberattack as well as current target areas (Government of Canada 2023; OECD 2022; Owens 2023a; Science Canada 2021).

The theft of research and/or personal data is a common threat, since data stored on hard drives and USB drives can be stolen or misplaced and cyberattacks can cause data breaches and damage IT systems. Phishing attacks they tend to target individual researchers for whom security may not be top of mind (OECD 2022).

Research security is also at risk from "bad actors," who may be collaborators, visiting scholars, students, or others who aim to misappropriate or tamper with research for their own gain (e.g., in the case of commercial competitors) or for the benefit of others

(e.g., hostile states, organized crime groups, terrorist organizations). These bad actors may act by choice or be compelled or coerced (Science Canada 2021).

Because research security is an increasingly pressing issue, policy development in this area is quite active. The Organisation for Economic Co-operation and Development (OECD) policy paper *Integrity and Security in the Global Research Ecosystem*, published in June 2022, discusses a number of research security policies and initiatives from Australia, Japan, the Netherlands, the UK, and the US, developed by national governments, funding bodies, public research institutions, university associations, universities, international research projects, academic associations, and international political organizations (e.g., the G7, the European Commission, the Global Research Council). Many of these policies address building risk assessments into existing processes (e.g., funding application evaluation), identifying and managing threats and conflicts of interest, and guidelines for due diligence.

The OECD's policy paper acknowledges that the topic of research security can be difficult to discuss, contentious, and polarizing, but stresses that it is vital to consider it nonetheless. It offers seven high-level recommendations for the research community:

1. Underscore the importance of freedom of scientific research and international collaboration as a key element of the global research ecosystem
2. Integrate research security considerations into national and institutional frameworks for research integrity
3. Promote a proportionate and systematic approach to risk management in research
4. Promote openness and transparency in relation to conflicts of interest or commitment
5. Develop clear guidelines, streamline procedures, and limit unnecessary bureaucracy
6. Work across sectors and institutions to develop more integrative and effective policy
7. Enhance international information exchange on research integrity and security (10)

Canada has also developed policy addressing research security. In December 2019, the U15 Group of Canadian Research Universities and Universities Canada released *Mitigating Economic and/or Geopolitical Risks in Sensitive Research Projects: A Tool for University Researchers*. The guide discusses various types of risks in addition to data misappropriation. For instance, it points out that, since not all researchers enjoy the same degree of academic freedom, publishing certain results could put international partners at risk and that risks to human rights must be assessed as part of researchers' travel plans (10).

The Government of Canada has also released a cluster of related research security policy statements:

Joint CSE and CSIS Statement, 14 May 2020: This statement from the Communications Security Establishment (CSE) and the Canadian Security Intelligence Service (CSIS) responds to heightened concerns about research and national security related to the uncertainty generated by COVID-19. It warns against threats to intellectual property as well as personal information, citing an **alert from the Canadian Centre for Cyber Security** and a **statement from Global Affairs Canada** on increased cyber threats to the health sector.

Policy Statement on Research Security and COVID-19, 14 September 2020: This statement from Innovation, Science and Economic Development Canada (ISED) reaffirms the Government of Canada's commitment to open science and reminds the research community to remain vigilant and review their cybersecurity policies and practices in the face of continued security threats.

Research Security Policy Statement, 24 March 2021: This statement from ISED reports an increase in threat levels to research and national security and reminds the research community about the September 2020 policy statement. It also notes that it has asked the Universities Working Group to develop risk guidelines to guide researchers in consider national security issues related to their research. These **National Security Guidelines for Research Partnerships** were released in July 2021.

Statement on Protecting Canada's Research, 14 February 2023: This statement from ISED from the ministries of Innovation, Science and Industry; Health; and Public Safety again notes an increased level of threat and announces a change in funding policy for the Tri-Agency: "Grant applications that involve conducting research in a sensitive research area will not be funded if any of the researchers working on the project are affiliated with a university, research institute or laboratory connected to military, national defence or state security entities of foreign state actors that pose a risk to our national security" (ISED 2023).

In addition, Canada's **2022 federal budget** introduced $125 million in funding for the **Research Support Fund** to help post-secondary institutions build capacity for research security, as well as $34.6 million over five years and $8.4 million in ongoing funding to establish a Research Security Centre to advise research institutions.

Although research security is a complex issue, researchers can take action to protect themselves and their work. The Government of Canada's **Safeguarding Your Research** portal includes information about research security as well as tools and guidelines for researchers and institutions. The **Assessing your Risk Profile** and **Mitigating your Research Security Risks** tools provide specific, practical advice to help researchers evaluate and address risks specific to their projects. The resources shared through this portal are from the **Government of Canada–Universities Working Group**, which works towards open, collaborative, and secure research in Canada.

Research Security in the Press

One issue covered in the academic and popular press was a pilot program developed in response to the March 2021 policy statement in which funding applications for **NSERC's Alliance grants** were reviewed by CSIS and the CSE. Articles in ***University Affairs***, ***CBC News***, the *Globe and Mail* (**announcing the pilot in 2021** and its **outcomes in 2023**), and ***ScienceBusiness*** report that, of the approximately 1000 funding applications received by NSERC, 48 were flagged for review and 32 of those were denied funding due to security concerns.

Following this pilot program, security reviews are planned to roll out to all Tri-Agency funding applications. However, some researchers have criticized the program for lacking transparency and clarity (Owens 2023b). The screening cannot prevent potentially risky projects from happening, since projects that are denied NSERC funding can seek equivalent funding from their international partners, and projects that are not seeking federal funding will not be screened (Fife and Chase 2021). In May 2023, the ***Toronto Star*** reported that ISED was developing a policy listing specific research areas and institutions of concern to address some of these challenges.

Another issue addressed in the press is the specific research security threat from the Chinese state. Writing about the screening pilot program, Brian Owens notes that, "[w]hile no specific institutions or countries were mentioned" in the February 2023 Statement on Protecting Canada's Research, "it is widely understood that labs and companies in China are of particular concern due to extensive but often murky links to the military, and suspected abuses of intellectual property rights" (Owens 2023b). China has been widely discussed as a research security threat in the international press, including pieces in ***Global News***, ***Science***, and ***Times Higher Education***.

Although most policies have adopted what the OECD calls a "country agnostic approach" (OECD 2022, 33), concerns have been raised—such as in pieces for the *Atlantic*, the *Chronicle of Higher Education*, *Policy Options*, and *ScienceBusiness*, and *University Affairs*—about the implicit focus on threats from China. David Robinson outlines these risks in a piece for the Canadian Association of University Teachers (CAUT) newsletter:

> There may be legitimate national security risks arising from academic research, but we as a community have to guard against overreach. We must ensure that academics are not targeted because of their ethnicity, and that rules are not so broad as to restrict legitimate research and scholarship. Nor should a foreign influence law be used to target academics who are critical of Canada's military or foreign policy. (Robinson 2023)

As Robinson notes, this focus on threats from China has led to a climate of fear about collaborating with Chinese researchers that is hindering research, harming collaborative relationships, and putting individual researchers at risk.

Responses from the INKE Community

INKE Partnership member Aaron Mauro's research currently focuses on research cybersecurity. His 2022 book *Hacking in the Humanities: Cybersecurity, Speculative Fiction, and Navigating a Digital Future* (2022) discusses a "security-first research approach." His talk of the same name at the Dahlem Humanities Center in 2022 argues that "[d]igital humanities projects must now embrace security best practices in the ways we plan, conduct, and communicate research" and that digital humanists are well positioned to ask the necessary critical questions.

Mauro gave an Institute Lecture at the 2021 Digital Humanities Summer Institute (DHSI) called **"Human Exploits: Cybersecurity and the Humanities,"** and teaches a DHSI course on Cybersecurity for Humanists.

Among other writings related to cybersecurity, Mauro has written several pieces for *The Conversation.* In **"Working from Home during the Coronavirus Pandemic Creates New Cybersecurity Threats,"** he outlines how threats such as phishing and ransomware have become increasingly common during the pandemic and the need for more secure

infrastructure and better security habits by users. In **"Ukrainian Cultural Artifacts are at Risk during the Russian Invasion, but Digitizing Them my Offer Some Protection,"** he outlines how Russian cyberattacks and rhetoric threaten Ukrainian cultural heritage as well as its national security. Although digitization can create backups of cultural heritage materials, he notes, it depends on infrastructures that are also under threat (for more on the digitization of cultural heritage materials, see **"Canada's National Heritage Digitization Strategy"**).

Research Security and the Broader Academic Community

Numerous initiatives in the broader Canadian academic community address issues of research security. At a national level, for instance, the Digital Research Alliance of Canada (the Alliance) launched **a cluster of cybersecurity standards and policies** in December 2022 related to national-level infrastructure, addressing **data classification**, **data handling**, **vulnerability management**, and **cybersecurity risk management**. The Alliance is also marking **Cybersecurity Awareness Month 2023** with a series of online workshops held throughout October, each focusing on an issue related to digital research security.

Also at a national level, the **Canadian Shared Security Operations Centre (CanSSOC)**—a collaboration between **CANARIE** and the **National Research and Education Network (NREN)**—coordinates local, regional, and national cybersecurity services across Canada.

Institutions and organizations are also taking action. For example, in September 2021, the U15 released a **Statement on Protecting Canadian Values and Canadian Research** that emphasizes the need for security policies to be clear, transparent, and considered, recognizing that "academic freedom and institutional autonomy are foundational principles that ensure our institutions remain free from political interference, capable of speaking truth to power, and responsive to the social, cultural, and economic needs of Canadians" (U15 2021).

In February 2023, the University of Waterloo hosted a **Research Security Conference** as a way of raising awareness about key issues and encouraging discussion, including about the potential for racial discrimination as a result of security measures. It also

addressed the changing role of research services offices, as many institutions now have dedicated research security divisions, offices, and/or funding.

And, although it is not specifically a research security policy, the First Nations Principles of OCAP® from the First Nations Information Governance Centre address Ownership, Control, Access, and Possession, all of which relate to data integrity and security.

Research Security and Open Scholarship

A key challenge for open and secure scholarship is that the openness, collaboration, and sharing that are foundational to Open movements are precisely what bad actors exploit to undermine research security. Along the same lines, the digital infrastructures and online communication technologies that make open scholarship possible are also particularly vulnerable to attack.

A related security challenge that is also particularly relevant for open scholarship is that the more openly information is shared, the greater the risk that it will be used for nefarious purposes, as Grace Browne discusses in an article for *Wired*. COVID-19 research could be used to develop bioweapons, for example, and generative AI code could be used to spread disinformation. The rise of open pre-print servers, especially for research with dual-use potential, is particularly of concern because that research is not yet peer reviewed and may contain errors or pose potential security risks that have not been identified. Noting that openness magnifies the already existing risk that research will be used in unintended, harmful ways, Browne argues that "it's time for open science to be reckoning with its risks, before the worst happens" (Browne 2022).

In addition to the Canadian efforts described above, efforts are underway worldwide to develop a security-first research culture, often related to issues that intersect with open scholarship. For instance, the TRUST Principles for Digital Repositories (Transparency, Responsibility, User focus, Sustainability, Technology), which recognize that the digital infrastructures that researchers use to deposit and source data must be secure and trustworthy (see "The TRUST Principles for Digital Repositories"). In their joint endorsement of the principles, the Canadian Association of Research Libraries (CARL) and Portage noted that Technology includes "the ability to effectively detect and respond to security threats" (2020).

Educause has a **Security and Privacy Guide** containing information and resources to support policy development and education programs for the higher education community. In January 2022, the European Commission released ***Tackling R&I Foreign Interference***, a working document containing specific guidelines for research organizations for mitigating security risks while advancing open scholarship.

These are just a few examples of initiatives underway across the world to address the complex issue of research security. They reflect the consensus among research security stakeholders that openness must be balanced with security while upholding academic freedoms: a recognition of the benefits of working openly and collaboratively across national borders and of the legitimate security risks involved.

Works Cited

Browne, Grace. 2022. "Making Science More Open Is Good for Research—but Bad for Security." *Wired*, April 22, 2022. https://www.wired.com/story/making-science-more-open-good-research-bad-security/.

CARL (Canadian Association of Research Libraries) and Portage. 2020. "CARL and Portage Endorse the TRUST Principles for Digital Repositories." Canadian Association of Research Libraries. July 31, 2020. https://www.carl-abrc.ca/news/trust-principles-for-digital-repositories/.

Fife, Robert, and Steven Chase. 2021. "Ottawa Imposes National-Security Risk Assessments for University Researchers Seeking Federal Funds." *The Globe and Mail*, July 12, 2021. https://www.theglobeandmail.com/politics/article-ottawa-imposes-national-security-risk-assessments-for-university/.

Government of Canada. 2021. "Who Are You at Risk From?" July 11, 2021. https://science.gc.ca/site/science/en/safeguarding-your-research/general-information-research-security/who-are-you-risk.

Government of Canada. 2023. "Why Safeguard Your Research?" Government of Canada. March 31, 2023. https://science.gc.ca/site/science/en/safeguarding-your-research/general-information-research-security/why-safeguard-your-research.

ISED (Innovation, Science and Economic Development Canada). 2023. "Statement from Minister Champagne, Minister Duclos and Minister Mendicino on Protecting Canada's Research." Government of Canada. February 14, 2023. https://www.canada.ca/en/innovation-science-economic-

development/news/2023/02/statement-from-minister-champagne-minister-duclos-and-minister-mendicino-on-protecting-canadas-research.html.

Mauro, Aaron. 2022. “Hacking in the Humanities: Cybersecurity, Speculative Fiction, and Navigating a Digital Future.” Dahlem Humanities Center (DHC). June 7, 2022. https://www.fu-berlin.de/en/sites/dhc/videothek/Videothek/908-DHCL-Mauro/index.html.

OECD. 2022. “Integrity and Security in the Global Research Ecosystem.” OECD Science, Technology and Industry Policy Papers, no. 130. https://doi.org/10.1787/1c416f43-en.

Owens, Brian. 2023a. “A New Era of Research Security.” *University Affairs*, June 14, 2023. https://www.universityaffairs.ca/features/feature-article/a-new-era-of-research-security/.

Owens, Brian. 2023b. “Researchers Decry a Lack of Clarity under National Security Risk Assessments.” *University Affairs*, March 21, 2023. https://www.universityaffairs.ca/news/news-article/researchers-decry-a-lack-of-clarity-under-national-security-risk-assessments/.

Robinson, David. 2023. “Academic Freedom and National Security.” *CAUT Bulletin*, June 2023. https://www.caut.ca/bulletin/2023/05/executive-directors-corner-academic-freedom-and-national-security.

Science Canada. 2021. “CSIS Research Security Briefing.” July 9, 2021. https://www.youtube.com/watch?v=LSu5ObwzM8c.

U15 Group of Canadian Research Universities. 2021. “U15 Statement on Protecting Canadian Values and Canadian Research.” U15 Group of Canadian Research Universities. September 28, 2021. https://u15.ca/publications/statements-releases/u15-statement-on-protecting-canadian-values-and-canadian-research/.

U15 Group of Canadian Research Universities and Universities Canada. 2019. *Mitigating Economic and/or Geopolitical Risks in Sensitive Research Projects: A Tool for University Researchers*. Innovation, Science and Economic Development Canada (ISED). https://science.gc.ca/site/science/sites/default/files/attachments/2022/Mitigating_Risks2.pdf.

Search

Archives

Select Year

Categories

- Community News
- English
- French
- Observations
- Observations and Responses
- Policies
- Responses
- Uncategorized

Tags

Berlin Declaration / Déclaration de Berlin Bethesda Statement / Déclaration de Bethesda bibliodiversity / bibliodiversité Budapest Statement / Déclaration de Budapest Canada Canadiana.org Canadian government/le gouvernement du Canada CAPOS CARL / ABRC collaboration Compute Canada / calcul Canada copyright / droits d'auteurs CRKN / RCDR data management / gestion des données digital scholarship / version numérique en français / French english English / en anglais

Federation for the HSS / Fédération des sciences humaines

funding agencies / organismes de financement identity management / gestion de l'identité

implementation / mise en oeuvre INKE international policy / politique internationale

Naylor Report / le rapport Naylor open access / libre accès open data / données ouvertes

open education / éducation ouverte open government / gouvernement ouvert

open infrastructure / infrastructure ouverte open scien open science / science ouverte

open source software / les logicels libres ORCID peer review / critique des pairs PKP

Plan S Plan S update / mise à jour du Plan S policy / politique promotion et titularisation

publishing / édition RDC / DRC RDM RECODE

recommendations / recommandations reports / les rapports repositories / les dépôts

research evaluation / l'évaluation de la recherche

research evaluation / évaluation de la recherche

research libraries / les bibliothèques de recherche

research output / les résultats de la recherche research security / sécurité de la recherche

RPT / révision scholarly communication / la communication savante

SFU Library / Bibliothèque social media / les medias sociaux

Tri-Agency / des trois organismes UK UK / Royaume-Uni UNESCO UVic Libraries

Érudit

INKE
IMPLEMENTING NEW KNOWLEDGE ENVIRONMENTS