The University of Calgary and the University of Alberta collaborated to host the 2023 Research Security Conference: Mitigating Risk in a Changing World from 26-27 October 2023. The conference was attended by representatives from 54 post-secondary institutions, 12 Government of Canada departments and agencies, 3 provincial or territorial governments and 26 other civil society and research organizations. Attendees from the U15 and Canada’s smaller and mid-sized universities met in advance in workshops to identify common challenges and opportunities for collaboration. Partnerships and professional support networks were established at this conference and we hope to see this capacity building continue in our Canadian research ecosystem.

**Key Takeaways & Questions for Further Action:**

**A Canadian Approach to Research Security**
- Recognition of the need for uniquely Canadian approaches to research security challenges that take into consideration Canadian values, principles, commitments, laws, and regulations.
- Need for a collaborative approach to research security and to building national resilience and capacity and an overwhelming sense of collegiality and a desire to work together.
- Research security is a competency that we will develop. In this regard, we should look to possible models such as research ethics which was once a new lens and competency but is now integrated into the research process.

**Supporting World-Class Research & Researchers**
- There is a shared desire to protect researchers from the misuse of their research – from the theft of their research, data, and knowledge; from intimidation, harassment, coercion, and other forms of foreign interference or transnational repressions; and from an unreasonable burden of administrative effort associated with implementing requirements.
- Canada and Canadian universities approach research security in a way that doesn’t jeopardize our capacity to attract and retain top global talent. We should identify areas where we need to collaborate with countries of concern, and find ways to do so securely to advance our interests.

**Engaging with Scholars from the Social Sciences & Humanities**
- To date research security in Canada has been focused primarily on STEM fields given the importance of protecting sensitive research and technology; however there are also risks to the Social Sciences to be addressed.
Clarity on Sanctions, Export Controls, & Dual-Use Research

- Current levels of awareness and capacity to implement sanctions and export controls on Canadian campuses are risks to be addressed, particularly in light of extra-territorial application of related legislation in the United States.
- There are limits to our current understanding of terms like ‘dual-use’ and ‘dual-use research of concern’. Guidance is needed on how to best work with researchers to help them understand the possible dual-use of their research.

The Importance of Equity, Diversity, & Inclusion in Research Security

- How can we avoid approaches to research security that could create a ‘chill’ on research, contribute to inequity, racism and discrimination, and lead to loss of vital talent in Canada? How do we ensure that EDI considerations are integrated into our research security frameworks and not as an afterthought? And how can we involve those most directly impacted by research security policies – particularly those from traditionally marginalized and equity-denied groups – in the construction of our research security frameworks?

Human Intelligence as the Greatest OSINT Asset

- There are real limits to technological tools – particularly in the absence of expert human guidance, review, and validation of information. Tools are always a reflection of the humans who created them and the design parameters. It is important to be cognizant of the problem that the creator of a tool was trying to solve.

Pre-Conference Workshops

Smaller & Mid-Sized Universities Working Group

On Wednesday October 25th, 2023 a workshop was held for small and mid-sized universities with the goal of bringing the community together to figure out the best way to navigate research security with limited funding. The workshop groups were asked to identify the key challenges and issues facing small & medium sized institutions, as well as solutions and next steps.

Summary:

- Smaller & mid-sized universities emphasized that they do not have the resources to meet many of the federal requirements and require additional funding and/or support.
- It was noted that collaboration between institutions, with the U15 universities playing a big role, is key to addressing the differences in capabilities between institutions.
- Attendees underscored that clarity from the federal and provincial governments in terms of research security requirements for small and medium-sized universities is needed.
- Challenges to building research security capacity were discussed, including limited resources but also reduced volume of risk assessment forms.
- There is the potential to outsource certain due diligence tasks or consortia to pool funds for tool access.
- It was suggested that a ‘buddy system’ be put into place by province to support capacity-building and consistency.
• It was asserted that there is a need for shared training and capacity-building (possible hub-and-spoke approaches).

Next Steps:

• Continue with capacity building engagement with the U15 Research Security group, as well as provincially between institutions.
• Further discussion about resources and the possibility of sharing information, best practices, and resources.
• A survey will be sent to small & medium sized institutions following the conference.
• A follow-up meeting to discuss the points raised will be scheduled (virtually) for all small & medium sized institutions in November.

**U15 Research Security Director’s Forum**

On Wednesday October 25th, 2023 a workshop was held for Research Security Directors from the U15 institutions to discuss the unique challenges facing large research-intensive universities. Agenda items included maximizing efforts through the U15 forum and conveying priorities for government engagement to the U15 representative, capacity building and support for smaller and mid-sized universities, and the future of the ‘Team Canada’ informal network of research security directors across the country.

Summary:

• U15 representatives shared priorities for government engagement and heard from the U15 Representative about efforts undertaken on the research security file. All attendees stressed the need for greater clarity with regard to requirements and greater stability of funding.
• Some U15 representatives urged the U15 to push for a more equitable approach to security clearances across the community, and to seek these at the level of research security directors, not just Vice Presidents of Research. This would be in line with the American approach and facilitate more frequent security briefings.
• U15 representatives heard from the facilitators of the Small and Mid-Sized Working Group and discussed options for offering greater support to those post-secondary institutions to increase the resilience of the community as a whole.
• U15 representatives underscored that research security funding needs to increase in parallel with the increase in the administrative burden placed on universities; there is also a desire for greater stability and certainty of funding given the programs that are being developed.
• Several representatives noted that faculty engagement will be an important part of effecting culture change across institutions and the community and stressed the importance of approaching research security with a view to talent retention.
• It was emphasized that secure data management is critical, and consultations with other institutions and potentially individuals in the defence industry could be of value on this front.
• It was stated that the U15 should push for greater policy harmonization on research security within provinces, and also between the different levels of government.
Conference Summary

*The Geopolitics of Research Security*

**Summary:**
- During the pandemic, security and intelligence agencies witnessed an unmatched spike in espionage efforts targeting vaccine research and therapeutics, leading to the issuance of a threat advisory from CSE and CSIS. Subsequent targeting of Canadian research and innovation led the Government of Canada to take action.
- Academic research must be global and collaborative with an emphasis on attracting talent and research.
- Misinformation and disinformation is being crafted in such a way as to make it more likely to be seen and shared by academics, creating an air of legitimacy. Research by Social Scientists in Canada may also be misrepresented or otherwise misused to advance the objectives of foreign adversaries.
- Foreign influence and interference significantly target STEM fields, but they also target Social Sciences by framing and amplifying (sometimes malign) narratives.
- Safeguarding research practices should be approached as an issue of socio-behavioural change by building awareness and securing buy-in from stakeholders. There may be value in looking to the model of research ethics and the normalization of those considerations.
- Research security training should begin as early as possible, whether it is critical thinking taught in grade school or teaching research security to undergraduates.

*Navigating Sanctions & Export Controls in Academia*

**Summary:**
- Sanctions requirements will have an impact on all postsecondary institutions.
- It is necessary to distinguish between comprehensive sanctions against states (which are coordinated between multinational bodies) and targeted sanctions. The area that is most relevant to universities today is targeted sanctions and their impacts.
- Governments use sanctions to intentionally to discourage collaboration with countries seen as adversarial ("chilling effect") – this can have a very real impact on academia.
- In general, Canadian institutions and individuals are not aware of export controls and sanctions laws and are likely not meeting obligations.
- Universities must be mindful of the extra-territorial dimension of American export control and sanctions legislation.
- Institutions generally implement policies/guidelines to meet sanctions requirements more strictly than the law requires.
- Infrastructure that supports sanctions is well developed in US. However, there are less resources in Canada. Universities typically do not have people within university architecture to track sanctions, but legislature puts the onus on universities to remain compliant.
- Universities need to take a holistic approach and need a leadership commitment to compliance.
- Universities are responsible for having a policy that is made available to researchers.
- There is not much clarity in sanctions law, interpretation, and judicial systems, this leaves universities with a huge legal obligation under various sanctions laws.
OSINT Tools for Identifying & Assessing Risk

Summary:

- Practitioners shouldn’t overemphasize technical tools, as the human element of subjective assessment is what’s important. Tools are useful but not essential and should be verified by other more basic sources and human interfaces.
- Collaboration within and between institutions can be a powerful part of intelligence gathering.
- Adversaries also use OSINT and may use it to reduce their footprint or find potential targets within your institution.
- OSINT practitioners should be clear about what they are looking for and define boundaries at the beginning of the investigation to know when to stop.
- OSINT can be used to engage and educate researchers by clearly demonstrating the potential risks.
- Collaboration with colleagues at other institutions is critical to learning and advancing in the field.
- It is a good practice to conduct a search in the native language of an entity of concern to access additional information.
- There was discussion about the privacy considerations associated with vetting, due diligence and the risks of collection and sharing of personal information without consent. Questions also came up about the legal authority of individuals and institutions to do due diligence and share information about individuals. It was suggested that we look to Europe rather than the US for possible models/tools given their much higher level of consideration for privacy.

Government of Canada Policy Implementation Update

Summary:

- The Government of Canada is not trying to create a system that determines if someone is a bad actor. The government is looking at specific affiliations and if there is risk.
- Consultation has taken place with the academic community regarding the sensitive technology research list.
- There will be time between the announcement of the implementation of the sensitive technology research and affiliations of concerns lists and enforcement. This will allow time for individuals and institutions to address any potential problematic affiliations.
- The Public Safety Canada Research Security Centre, with its network of Regional Advisors, serves as a resource for awareness building and the implementation of National Security Guidelines for Research Partnerships.

Safeguarding Sensitive Research & Technologies

Summary:

- Technology, research, and tools are all inherently neutral. This means there is a need to better understand the end user and their intentions and anticipated end use.
- Research is a highly competitive environment. If a university chooses not to pursue a type of research, there is nothing to say that type of research is not happening elsewhere.
- Researchers are the top asset at the university. A paperwork/checklist approach is not the ideal way to ensure secure research. Rather, what is needed is regular engagement with the researchers doing the work to really understand the research and what it involves. Also important to build a culture in which researchers have the necessary supports be they mental health, mentorship or safe spaces for disclosure.
- It is important to keep in mind that research security is about risk mitigation, not risk elimination.
- Research is increasingly multidisciplinary and collaborative. Likewise, research security should also involve a multidisciplinary, collaborative approach.
- Need to fully and convincingly explain the ‘why’ of research security in order to win hearts and minds and build a culture in which research security efforts are normalized. The importance of engagement and awareness was underscored.

**Mitigating Risks in Canada’s Research Ecosystem**

**Summary:**

- China is the biggest threat actor in the cyber security space. However, it would be a mistake to think that China and Russia are the only countries that the research community needs to think about and be concerned with.
- Universities must reconcile the dual imperatives of spreading knowledge on the one hand, and mitigating risk on the other hand. Security considerations should not stop the core mission of a university.
- It is important to stop looking at academic freedom and research security as being in opposition. Research security can also protect and support the exercise of academic freedom and be implemented in a way which does not curtail this important principle.
- Data risks should be considered by researchers at the outset. It’s important to be aware of spaces in which you may want to delay publication or hold back information.
- Foreign actors do not always use top of the line tools to access research.
- The academic community is seeking case studies and CSIS is hoping to be able to declassify more information so that it can be more easily shared.

**EDI Lens on Research Security**

**Summary:**

- There is an emphasis in research security on foreign actors (nefarious actors) that are undermining security. We think about threats from abroad, but also have to remember that civil rights leaders were framed as a national security threat. During WWI and WWII religious and ethnic groups were framed as threats. We need to incorporate historical knowledge and awareness as we develop approaches to research security to avoid repeating the mistakes of the past.
• BIPOC colleagues might be more exposed to attention in research security. The research security community needs to be ruthlessly forensic about the outcomes of the research security project to ensure that it is not having a disproportionate outcome equity-deserving groups.
• It is good that the messaging around research security is country agnostic, but the conversations around research security are not just happening at universities. The wider culture is not country agnostic and there is a risk that the concept comes across as “colour blind” – we need to be country conscious instead.
• There needs to be a greater focus on human rights and human dignity in how we think about research security.

A Western Canada Approach to Research Security

Summary:

• There has been growth in security consciousness in past five years along with a growing capacity at Canadian universities in terms of identifying and mitigating risk.
• The entire research ecosystem needs to be secure, including smaller institutions.
• It is important that research security be a facilitator of great research, not an impediment.
• Divergent national security and provincial policies could create preferred systems where similar institutions and provinces align. National security responsibility vs provincial responsibility for post secondary. Complexity of relationship:
  o In Alberta, we have already seen engagement by both levels of government.
  o Look to where the spaces are that the federal govt is concerned and how do we best mitigate these risks.
  o As we look at partnerships inter-institutionally, divergent policies provincially could create preferred systems where similar institutions and provinces align.
  o Will become more restrictive if policies are not aligned.
• How to manage protecting what needs to be protected but not restricting openness?
  o Try to engage faculty as early as possible when considering a project/partnership. Need to mitigate, not create barriers.
  o Dialogue is important. Will continue to provide advice.
  o Whatever we implement cannot be checklists to complete. Cannot be seen as a bureaucratic barrier. Focus on building a research security culture.
  o Understanding the why when it comes to risk assessment. Engaging the researchers at the beginning of the project proposal.

Conclusion & Next Steps

Numerous fruitful discussions took place over the course of a productive 3 days. It was emphasized repeatedly that research security is not something that any one individual, office or institution can successfully do alone. We must work together to achieve our objectives and increase our collective resilience against threats to research security while simultaneously protecting our core principles and the values of academia and democratic society. Next steps will include continued discussions in the informal Team Canada forum – including through new working groups on specific priority areas,
future workshops and conferences, and deepening of support networks across the country, including between larger and smaller institutions to advance capacity-building in research security.