University of Regina

Newsline	Research Security	Week	April 13 – 17, 2026
Editor	Alaa Dabboor	Research Security Manager	
Reference Package			
1	Research Security Centre		

Executive summary: Recent developments highlight the increasing integration of research security into institutional strategy, infrastructure, and international collaboration. In Canada, universities are advancing research security through new portals, dedicated chairs, observatories, and formalized practices, while investments in sovereign AI infrastructure and innovation funding reforms strengthen links between research, security, and domestic capacity. Internationally, concerns are growing around espionage, dual-use research, data trust, academic decoupling, and erosion of critical research capabilities. Together, these trends reinforce the importance of research security across technology development, global collaboration, data governance, and institutional resilience.

Key Points:

- **Canadian-controlled infrastructure and technology sovereignty:** A new AI data centre at Thompson Rivers University is being developed as part of a Canadian-controlled infrastructure network, emphasizing data sovereignty and governance under Canadian law. The facility is designed for sustainability, including hydroelectric power use, closed-loop water cooling, and waste heat recovery. In parallel, Scientific Research and Experimental Development reforms expand support for hard tech and manufacturing by restoring capital expenditure eligibility, increasing funding access, and enabling investment in equipment and production, with the goal of strengthening domestic supply chains.

  What this means: Sovereign infrastructure and domestic innovation investments may reduce reliance on external systems while increasing the importance of secure data governance, infrastructure control, and protection of research outputs.
- **Research security becoming an institutional function in Canada:** Canadian universities are formalizing research security as a core institutional function. Initiatives include a Franco-Canadian observatory and joint chair between University of Ottawa (uOttawa) and Université Côte d'Azur, as well as Université du Québec à Montréal (UQAM)'s research security portal and University of New Brunswick (UNB)'s integration of research security alongside ethics and safety. At UNB, risks are assessed based on project sensitivity rather than nationality and apply across all disciplines.

  What this means: Research security is increasingly treated as a routine governance function embedded across the research lifecycle rather than a reactive or project-specific activity.
- **Northern research, sovereignty, and community partnership:** Universities are playing an expanded role in Arctic and northern regions through Indigenous-led research, infrastructure development, environmental monitoring, and sovereignty-related science, while balancing national priorities with Indigenous knowledge, local needs, and ecological sensitivity.

What this means: Research in strategically sensitive regions may involve heightened considerations related to sovereignty, community partnership, and responsible data stewardship in complex geopolitical contexts.

- **Research security as a national resilience issue:** Research security is increasingly linked to national resilience, digital governance, and alliance credibility. Estonia highlights risks to NATO trust without adequate safeguards, while South Africa's AI policy emphasizes computing infrastructure, research centres of excellence, and responsible governance.

  What this means: As advanced technologies become integral to national resilience, institutional safeguards and governance practices play a growing role in maintaining trust, security, and long-term strategic capacity.
- **Geopolitical conflict, academic decoupling, and critical capacity loss:** Geopolitical tensions are reshaping research collaboration. Australian universities face pressure to sever ties with Iran, raising concerns about academic decoupling, while UK experts warn that funding pressures may erode critical research capacity. Concerns also persist regarding dual-use collaboration, knowledge transfer, and sanctions evasion linked to Russia's Joint Institute for Nuclear Research.

  What this means: Geopolitical pressures and funding changes may influence collaboration decisions and long-term institutional capability, requiring broader risk assessment beyond immediate partnerships.
- **Espionage, dual-use exposure, and industrial security risks:** Germany warns of increasing espionage, sabotage, and hybrid threats targeting defence-related industry and research, including attempts to access sensitive technologies. Broader reporting highlights risks of technology leakage, misuse of dual-use research, and the potential for research environments to face increased security scrutiny or exposure.

  What this means: Research linked to defence or advanced technologies may face heightened exposure to misuse, espionage, and security-related risks, reinforcing the need for proportionate safeguards and institutional awareness.
- **Data trust and digital sovereignty:** Survey data shows low public trust in U.S. and Chinese technology firms handling personal data, with stronger support for domestic alternatives and concerns about foreign data access under external legal regimes.

  What this means: Declining trust in foreign providers underscores the importance of data sovereignty, vendor risk assessment, and confidence in digital systems used to manage research and personal data.

Conclusion: The research environment is increasingly shaped by strategic technology development, institutional research security practices, geopolitical dynamics, and data governance concerns. Across Canadian and international contexts, research security is becoming a more embedded and operational function tied to sovereignty, resilience, collaboration, and trust.