University of Regina

Newsline	Research Security		
Week	Dec. 15-19, 2025		
Editor	Alaa Dabboor	**Position**	Research Security Manager
Reference Package			
1	Research Security Centre		

Executive summary: This week's reporting underscores intensifying technological competition and rising research security risks. Canadian governments are advancing domestic compute, AI, and quantum capacity to retain talent and IP, while continued exploitation of research collaborations, insider theft allegations, and grey zone tactics heighten cyber and physical threats. Institutions should strengthen partnership due diligence, personnel and IP protections, and security aware of procurement and commercialization practices.

Key Points:

- **National push for technological sovereignty and talent recruitment:** Canadian institutions and governments are pursuing onshore capacity in high performance computing and AI. Reports indicate Queen's University is recruiting external expertise to support a national scale compute bid. Quebec has placed a "digital sovereignty" principle into regulatory text with the stated aim of favoring local technology where appropriate. These moves sit alongside federal investments to expand national compute and AI capabilities.

  What this means: Keeping critical infrastructure and IP onshore reduces exposure to foreign legal regimes and data exfiltration risks, but it also concentrates high value facilities and talent that adversaries may target. Operational measures should include vendor security questionnaires, supply chain review, procurement clauses requiring demonstrable security practices, strengthened physical protection for compute sites, and enhanced insider risk monitoring for newly recruited experts.
- **Canadian Quantum Champions Program (CQCP) clarified scope:** The CQCP's Phase 1 reportedly selects four Canadian firms for awards of up to CA$23 million each. The Phase 1 awards are part of a broader multiyear set of investments associated with Canada's quantum strategy, which has been reported in public materials at an approximate program level envelope of CA$334 million across related initiatives. Phase 1 contains conditions intended to encourage domestic anchoring and benchmarking activities.

  What this means: The CQCP increases Canada's ability to retain quantum IP and build capacity, but institutions and partners should examine contract terms carefully. Legal and tech transfer offices need to review localization clauses, IP ownership or licensing language, and any commercialization commitments tied to government support.

- **Espionage and foreign interference remain high risk for collaborative research:** A U.S. congressional review found cases in which partnerships related to Department of Energy funded research were exploited to transfer sensitive capabilities to foreign entities. Broader reporting continues to show that academic and industry collaborations can be used as vectors for acquiring dual use technologies.

  What this means: Standardized risk assessment procedures should be applied to international collaborations, especially in dual use fields such as nuclear, quantum, AI, and advanced materials. Institutions should ensure pre-award reviews include conflict of interest checks, export control screening, and mandatory security risk mitigation plans. Establish clear incident reporting lines between research offices and institutional security/cyber teams.
- **Insider threats and IP protection, ongoing high consequence cases:** The Florey Institute has filed a lawsuit alleging that a former executive improperly removed and deleted thousands of confidential files related to patented brain research methods and commercialization activities. The filing sets out alleged facts and seeks remedies; the matter is before the courts, and the allegations remain subject to legal process.

  What this means: Institutions should enforce least privilege access, implement robust data loss prevention and audit logging, strengthen offboarding procedures for privileged users, and ensure commercialization agreements include clear confidentiality, injunctive relief, and forensic access provisions. Regular tabletop exercises to simulate data exfiltration scenarios are also recommended.
- **Geopolitical "grey zone" activity and broader security environment:** Adversarial advances were observed in multiple domains, including enhanced drone and surveillance capabilities in polar regions, the use of commercial spyware by state actors to target journalists and researchers, and continued grey zone tactics such as influence operations and covert technology acquisition. Domestic and allied political shifts affecting research funding and organizational structures were also noted.

  What this means: Research security planning must be coordinated with institutional cyber and physical security strategies. Monitor geopolitical indicators that change partner risk profiles, and adapt data sharing, publication, and travel policies for teams working on sensitive subjects. Consider targeted training for researchers on identifying suspicious approaches and secure handling of sensitive material.

Conclusion: Research security spans multiple domains, and while Canada's push for sovereign capacity strengthens resilience, it must be matched by institutional controls that reduce foreign interference and insider risk through stronger IP safeguards, standardized collaboration reviews, researcher awareness, and cross functional coordination.