University of Regina

Newsline	Research Security		
Week	Feb. 9 - 13, 2026		
Editor	Alaa Dabboor	**Position**	Research Security Manager
Reference Package			
1	Research Security Centre		

Executive summary: This week's reporting shows growing securitization across quantum, energy, health, agriculture, and AI, plus shifting funding and institutional policies and rising state-level cyber activity. Together these trends expand risks to intellectual property and people and reinforce the need for research security measures that go beyond traditionally classified programs to include foundational and community-led work.

Key Points:

- **Quantum and cryogenics scaling—new domestic deep-tech hub:** Zero Point Cryogenics is scaling commercial production of dilution refrigerators that support lab and commercial quantum work, leveraging local expertise and industrial capacity.
  What this means: Quantum hardware and supply chains are dual-use and strategically sensitive. The value lies not only in equipment but in research data, techniques, and expertise. Identify projects using specialized components, review export/controlled-goods requirements, and align procurement, IP, data, and access controls with technical sensitivity.
- **Advanced energy and health-tech research:** Teams at the University of Saskatchewan are advancing perovskite solar research, while Montreal's School of Technology is developing medical and health technologies through a new health-technology research institute.
  What this means: Early-stage commercialization increases exposure to partnerships, contracts, and investor-driven timelines, which can compromise careful risk screening. IP protection should be strengthened, standardized industry agreements adopted, and material transfer, licensing, and sponsor vetting for sensitive technologies reviewed.
- **Defence-tech boom and domestic Research and Development opportunity:** The Financial Post reports that increased defence spending is fueling investment in drones, AI, cybersecurity, sensors, and advanced manufacturing, creating opportunities for startups and universities to supply the Canadian Armed Forces.
  What this means: Applied defence research will grow. Universities must ensure compliance with controlled-goods and export rules (e.g., U.S. export controls and similar regimes), tighten subcontract and partner vetting, and prepare for security requirements in procurement and facilities.
- **First Inuit-led university — community and sovereignty:** Inuit Tapiriit Kanatami selected Arviat as the main site for Canada's first Inuit-led university, backed by major funding including a gift from the Mastercard Foundation.
  What this means: Research security must protect Indigenous knowledge and community control. Develop data-governance models and partnership agreements that respect sovereignty while securing sensitive data and IP.

- **Domestic policy and funding shifts reshape priorities:** Provincial funding changes and debates over hiring policies (and their ties to federal chair programs) are altering institutional priorities and talent flows.

  What this means: Funding incentives can push research toward strategically sensitive areas. Monitor policy changes for clauses that affect international collaboration, and update guidance on foreign affiliations, disclosures, and conflict-of-interest processes.
- **Securitization of agriculture — defence-research nexus expands:** The US US Department of Agriculture and the Department of Defense formalized cooperative steps treating agriculture as a defence domain.

  What this means: Agricultural and veterinary research will be viewed increasingly through a security lens. Review collaborations, data sharing, and materials management to protect sensitive techniques, genetic data, and supply-chain information.
- **International partnerships with China — risk management test case:** Some Canadian universities are formalizing long-standing ties with major Chinese institutions.

  What this means: Refresh partnership risk assessments and ensure agreements clarify IP ownership, publication rights, student and staff safety measures, and data handling obligations.
- **Campus foreign-interference reporting and government engagement:** The UK has instructed universities to report suspected interference directly to the UK Security Services and provided a secure reporting channel.

  What this means: Though Canada currently differs, the UK precedent signals potential policy shifts. Review institutional reporting pathways, legal support, and senior-leader briefing protocols to ensure timely escalation of suspected interference.
- **State-level cyber operations increasingly target individuals:** Reports show a surge in state-sponsored "direct-to-individual" attacks that use phishing, fake recruiting, and personal-device exploitation; Google Threat Intelligence highlights this trend.

  What this means: Perimeter controls alone are insufficient. Prioritize role-specific cyber training, multifactor authentication, separation of sensitive accounts from personal devices, and stronger HR/IT checks during recruitment and onboarding.
- **AI industry turnover highlights ethics and governance gaps:** High-profile departures from major AI firms signal tensions between rapid commercialization and safety/ethical commitments.

  What this means: Universities should strengthen governance of AI research: enforce provenance and consent for datasets, limit commercial reuse through contract terms, and train researchers on dual-use and misuse risks.

Conclusion: This week underscores how research, economic priorities, and national security are converging across quantum, energy, agriculture, health, and AI. As geopolitical interest grows, universities face greater partnership, cyber, data, and materials risks.