Newsline	Research Security		
Week	Nov. 24 -Nov. 28, 2025		
Editor	Alaa Dabboor	**Position**	Research Security Manager
Reference Package			
1	Research Security Centre		
2	URegina Safety Advisory		

Executive summary: Research security is now a central strategic priority as nations secure critical technologies and supply chains while preserving open collaboration. Researchers are increasingly targeted, including cyber intrusions, espionage, and ideologically motivated harassment, which makes people-centred protections as important as data controls. This week's items highlight four priorities: couple conditional foreign investment with domestic capability-building, strengthen academic integrity and AI literacy, embed dual-use and supplier risk assessments into research governance, and protect both researchers and data.

Key Points:

- **The "sovereign AI" test: investment or dependency?** The federal government highlighted Nokia's planned $340 million Ottawa campus expansion, noting roughly $72 million in government support and forecasts of about 1,900 jobs by 2028. Critics say that the subsidies may chiefly benefit a foreign multinational and risk undercutting domestic firms.
  What this means: Onshore facilities can reduce exposure to foreign supply-chain constraints and some forms of interference, but relying on foreign corporate hubs still creates vulnerabilities for IP, governance, and personnel. Policy should combine conditional investment with technology-transfer expectations, trusted-partner criteria, and measures that strengthen domestic research and development of talent.
- **Academic integrity strain from AI, an early warning for research misuse:** The University of Manitoba reports a large uptick in AI-related academic misconduct that is overwhelming its integrity system, delaying hearings and diverting faculty time from teaching; the university is initiating committees, workshops, and policy discussions in response.
  What this means: Normalizing dishonest or opaque AI use at the student level risks seeding behaviours that can scale into research misappropriation, falsified results, and erosion of reproducibility. Strengthening academic integrity now, through clear policies, scalable investigation workflows, and AI-responsibility education, acts as an upstream defence for research credibility and security.
- **Dual-use research with scientific and defence implications:** A University of Calgary northern sensor array, originally deployed for space-weather science, was found to detect GPS disruption and jamming. This capability has drawn interest from Canada's military, the U.S.

Navy, and NATO, and the research team is also working with Defence Research and Development Canada.

What this means: Curiosity-driven projects often have unanticipated defence relevance. Institutions should embed early dual-use screening, apply tiered access controls, and adopt partnership playbooks that preserve open science while protecting IP and meeting export-control obligations.

- **Global partnerships and opaque supply chains: a transparency gap:** International collaboration continues to grow, such as the UAE's Technology Innovation Institute establishing a lab within Mila in Montreal, but procurement transparency remains a concern. Hydro-Quebec and its partners have declined to disclose the Chinese turbine manufacturers involved in a major wind project, citing contractual confidentiality despite ongoing forced-labour concerns.

  What this means: Cross-border partnerships accelerate innovation but introduce ethical, geopolitical, and procurement risks when supplier transparency is limited. Institutions and funders should require supplier disclosure clauses, conduct human-rights and security screens for partners, and mandate periodic risk reassessments of collaborative agreements.
- **Threats to people, harassment, espionage, and operational response:** An institutional safety advisory outlines a range of threats facing researchers, including ideologically motivated harassment such as death threats, cyber intrusions, advanced persistent threats linked to foreign actors, and covert attempts at illicit influence. The advisory also provides practical guidance for reporting incidents and preserving evidence, including saving screenshots, retaining emails, and contacting local police or protective services.

  What this means: Protecting people is central to operational research security. Practical measures include well-publicized reporting channels, coordinated incident response with security services, mental-health supports, training in digital evidence preservation, and scenario-based drills that combine cyber and physical threat response.

Conclusion: This week's developments underline four priorities: pairing conditional foreign investment with domestic capability-building, reinforcing academic integrity and AI literacy, embedding dual-use and supplier risk assessments into research governance, and protecting both researchers and data. Practical next steps include publishing partner-vetting criteria, expanding an AI-integrity framework and student education, and running a cross-disciplinary exercise that tests responses to combined cyber and in-person threats. Together, these measures will strengthen Canada's research ecosystem while sustaining responsible international collaboration.