University of Regina

Newsline	Research Security		
Week	Jan. 19 - 23, 2026		
Editor	Alaa Dabboor	**Position**	Research Security Manager
Reference Package			
1	Research Security Centre		

Executive summary: This week's coverage highlights a broad international shift toward protecting strategic research, secure supply chains, and domestic technological capacity. Domestically, Canada saw multiple announcements aimed at strengthening defence and energy research, and commercializing AI. International reporting describes a move toward stricter vetting, procurement preferences for domestic suppliers, and renewed focus on institutional knowledge security. Cybersecurity and espionage reporting — including concerns about connected technologies and targeted recruitment tactics — underscore that research and technology ecosystems face both digital and human-centred threats.

Key Points:

- **Canada strengthens domestic strategic capabilities** An Ottawa defence-tech startup (Dominion Dynamics) will open a Kanata factory; Mila and Inovia Capital announced a US$100M Venture Scientist Fund to commercialize Canadian AI research; the University of Regina received $6.9M to establish a Small Modular Reactor (SMR) safety, licensing and testing centre.
  What this means: Building onshore manufacturing, commercialization funding, and nuclear testing capabilities improves resilience and keeps IP and talent within national ecosystems. These moves reduce near-term dependency on foreign suppliers but also raise the strategic value of the activities, increasing incentives for targeted espionage and supply-chain compromise; security planning must be integrated from project outset.
- **International policy trending toward supply-chain and funding protectionism:** The EU is advancing "made in Europe" procurement concepts for green tech and strengthening oversight of high-risk suppliers; reporting notes US moves to prioritize citizens in certain research funding streams and operational vetting directives.
  What this means: These policy shifts may reduce openness in research partnerships and complicate collaboration patterns. Canadian institutions should reconcile openness with compliance and build robust vetting, procurement due diligence, and legal frameworks to remain interoperable with allies while protecting sensitive work.
- **Cybersecurity concerns tied to connected technologies and procurement choices:** Reporting raised data-security and privacy questions after Canada's decision to allow Chinese EVs into the Canadian market under a tariff agreement; analysts highlighted where vehicle data might be stored and who could access it.
  What this means: Connected consumer or industrial technologies can create unanticipated data-exfiltration and access risks for research networks and partners. Research security

programs must include procurement risk assessments, data-flow mapping, and vendor governance for technology entering institutional environments.

- **Espionage methods remain adaptive and multi-vector:** Investigative pieces in the brief describe recruitment and infiltration techniques used against military and administrative institutions (examples from Taiwan and France) and illustrate financial, social-media and insider-access vectors.
  What this means: Threat actors exploit both technological and human vulnerabilities. Mitigation requires integrated personnel-security processes (vetting, insider-risk monitoring), financial-vulnerability awareness, and cross-sector intelligence sharing.
- **Universities moving toward formalized "knowledge security" frameworks:** Swiss universities (and similar allied initiatives) are proposing coordinated national knowledge-security strategies — secure labs, stricter vetting for sensitive fields, limits on access, and a central liaison hub between universities and security authorities.
  What this means: Institution-by-institution approaches are being replaced by standardized, coordinated frameworks to manage sensitive research consistently. Such frameworks can strengthen resilience but must be calibrated to preserve legitimate academic exchange and not unduly hinder beneficial collaborations.

Conclusion: This week's reporting shows an inflection point where economic policy, procurement choices, and national security considerations converge on research ecosystems. Canada's domestic investments and allied policy shifts both create opportunities to bolster sovereignty and raise new security obligations. Effective research security will require integrating technical, procurement, personnel, and policy measures while preserving the collaborative processes that underpin scientific progress.