



Newsline	Research Security		
Week	Feb. 2 - 6, 2026		
Editor	Alaa Dabboor	Position	Research Security Manager
Reference Package			
	1	Research Security Centre	

Executive summary: This week’s reporting highlights the dual nature of contemporary research security: tangible misuse of scientific capability, including illegal labs, weaponizable systems, and explosives, alongside the diplomatic and economic value of secure international collaboration such as Artemis II, France partnerships, and India engagement. Domestic policy shifts, notably deep federal cuts in agricultural research and calls for a national innovation strategy, increase systemic vulnerability by altering incentive structures. Internationally, partners are reprioritizing funds toward commercialization and strategic partnerships, while threats to academic freedom and AI-powered disinformation are emerging as non-kinetic risks to reputations and open inquiry. The University of Regina should strengthen proportional safeguards for high-risk research, reinforce IP and data controls in global partnerships, and expand support systems for faculty targeted by disinformation, while centring Indigenous governance in innovation discussions.

Key Points:

- High-profile investigations show research misuse and diversion:** A CBC investigation links a former B.C. entrepreneur, Jesse Jia-Bei Zhu, to two suspected illegal biolabs in the U.S.; and a separate Ontario explosives investigation found individuals seeking to develop and fund an anti-drone weapons system. Both stories illustrate how research-capable infrastructure and dual-use knowledge can be diverted to illicit or military ends.

What this means: Tighten due diligence on collaborators, spinouts, and contractors. Reinforce export control and controlled-goods awareness among faculty and tech transfer staff, and require risk assessments for applied projects in biotechnology, materials, robotics, and systems that could be repurposed. Ensure clear pathways for reporting suspicious activity and a named internal contact for controlled-goods enquiries.
- Strategic international collaborations continue, with layered risk profiles:** Canada’s role in Artemis II, including Canadarm3 and astronaut participation, and new bilateral programs such as the University of Calgary Visiting Scholars initiative with France, along with a Universities Canada delegation to India, show continued high-value international engagement. These partnerships advance innovation and capacity building.

What this means: Use a balanced approach based on clear principles. Standardize templates for MoUs and visiting scholar arrangements that include IP, data management, and publication safeguards. Implement tiered due diligence by partner country and technology and require security briefings for researchers working in sensitive areas.

- **Domestic funding instability heightens strategic vulnerability:** Large cuts at Agriculture and Agri-Food Canada threaten centres and expertise. Institutions such as Université Laval are exploring ways to preserve critical capacity. Analysts also argue Canada lacks a unified national innovation strategy.

What this means: Funding cuts may push researchers and projects to move or seek new support. The university should identify key research areas at risk, focus on keeping critical labs and talent, and carefully review any urgent funding or partnership offers, especially those that seek quick access to facilities or expertise.
- **Global reprioritization of research funding and pressure on academic freedom:** The UK is restructuring major research funding to favour commercialization. The EU is investing heavily to deepen science ties with Africa, and the UK and Japan have expanded science cooperation. Meanwhile, professors in the U.S. report increased surveillance and political pressure that threaten open inquiry.

What this means: Monitor partner countries' funding orientations when negotiating collaborations. Protect academic freedom by ensuring security controls do not become pretexts for censorship. Balance targeted risk mitigation with clear policies that support open research and academic expression.
- **Emerging threats from AI deepfakes and disinformation targeting scholars:** An American political scientist is facing hundreds of AI-generated deepfakes that falsely attribute controversial statements to him. The case demonstrates how generative AI can rapidly amplify reputational harm and distort public debate.

What this means: University resources should be available to support researchers affected by deepfakes or online disinformation. This includes clear steps for legal and communications support, quick removal requests, basic digital safety training, and a simple process to report incidents and escalate serious cases.
- **Indigenous sovereignty and innovation governance:** Commentary in the source material highlights that Canada's innovation agenda must consider Indigenous sovereignty and governance. Innovation policy is also about place, rights, and long-term stewardship.

What this means: Centre Indigenous research governance within institutional research security and innovation strategies. Strengthen Indigenous-led research programs, ensure benefit-sharing and IP arrangements respect Indigenous rights, and involve Indigenous governance in decisions about strategic partnerships and facilities.

Conclusion: This week's developments reinforce two concurrent priorities for university leadership. First, strengthen operational safeguards around high-risk research and partnerships through improved due diligence, export-control awareness, and clearer IP and data protections. Second, build institutional resilience by supporting researchers targeted by disinformation, safeguarding academic freedom, integrating Indigenous governance, and identifying strategic capacities at risk.