University of Regina

Newsline	Research Security	**Week**	August 24 – 28, 2026
Editor	Alaa Dabboor	Research Security Manager	
Reference Package			
1	Research Security Centre (Public Safety Canada)		
2	Office of the Foreign Influence Commissioner of Canada		

Executive summary: This week's coverage focuses on research talent, artificial intelligence (AI)-enabled cyberattacks, connected technology, dual-use research, international partnerships, and new foreign influence reporting obligations. Closer attention may be needed when managing cyber risks, technology suppliers, sensitive collaborations, and arrangements that may require registration under Canada's new law.

Key Points:

1. **Canada is attracting research talent while open partnerships remain important:** Ottawa named 64 inaugural Eddie Goldenberg Research Chairs from 13 countries, with most coming from United States institutions. Germany's largest public research funder also committed to stronger cooperation with the United States despite geopolitical pressures. These developments show continued competition for leading researchers and the importance of maintaining useful international research links.

   What this means: Research recruitment and international mobility should be supported. Affiliations, commitments, access needs, and possible conflicts should still be reviewed when the work involves sensitive research or technology.

2. **AI is increasing the speed and scale of cyber threats:** Canadian organizations are being encouraged to improve cyber resilience as AI supports faster vulnerability discovery, automated attacks, and more convincing phishing. United States authorities disrupted domains linked to QTFY, a hacking group allegedly connected to the Chinese government, after it reportedly targeted government agencies, national laboratories, hospitals, utilities, defence contractors, the National Institutes of Health, and the National Aeronautics and Space Administration. Chinese state-linked groups are also reportedly using DeepSeek and other AI models for reconnaissance and exploitation. State-sponsored actors reportedly attempted to compromise the Signal and WhatsApp accounts of senior European Union officials through targeted phishing and social engineering.

   What this means: Sensitive accounts, cloud systems, and research networks should use continuous verification, multifactor authentication, updated security controls, and careful checks of unexpected messages. AI-assisted cyber risks should be included in security planning.

3. **Connected technology and suppliers may create hidden risks:** Researchers found security flaws in Chinese-made Unitree robot dogs that could allow control through Wi-Fi, Bluetooth, or a mobile app. One study also identified an undisclosed external connection and transmissions to infrastructure linked to China. The United Kingdom is proposing powers to secretly block risky technology suppliers from critical sectors, including health, energy, telecommunications, transport, and data centres.

   What this means: Connected equipment and suppliers should be checked before use in sensitive environments. Data flows, external connections, software updates, vendor ownership, and remote-control functions should be understood and limited where needed.

4. **Dual-use research is receiving closer attention:** Finland's Defence Tech Hub is connecting more than 100 organizations working in quantum, AI, autonomous systems, sensors, space, and drones. New Zealand

warned that public and private research is being targeted for intellectual property and emerging technologies. The warning also noted that international exchanges and foreign talent recruitment programs may be used to obtain sensitive knowledge. China and Russia also began a joint Arctic expedition, while a report identified 131 contacts or collaborations between China's 98 top-tier defence laboratories and foreign institutions.

What this means: Projects involving defence labs, Arctic activity, space, quantum, drones, AI, or other dual-use fields should be reviewed early. Partner background, access, intended use, knowledge transfer, and publication plans should be clearly considered.

5. **International partnerships are facing stronger oversight:** Australia expanded government powers to veto university partnerships, including some researcher-to-researcher collaborations, while universities also paused or restricted doctoral applications from some Iranian students because of unclear sanctions and security guidance. A United Kingdom survey found that many academics still see research security as bureaucracy and have lower confidence in applying relevant laws, especially in unfunded collaborations.

   What this means: International work should be assessed based on the actual level of risk. Clear guidance and early support should be provided so security, sanctions, and reporting requirements can be addressed without applying unnecessary restrictions to low-risk research.

6. **Canada's new foreign influence registry creates reporting duties:** The Foreign Influence Transparency and Accountability Act (FITAA), its regulations, the Office of the Foreign Influence Commissioner, and a public registry came into effect on August 4, 2026. A person or institution that enters an arrangement with a foreign principal to conduct influence activities related to a Canadian political or governmental process may need to register. This includes processes at the federal, provincial, territorial, and municipal levels. Individual researchers are responsible for registering their own arrangements, while the University is responsible for institutional arrangements. New arrangements must be registered within 14 days. Arrangements already in place before August 4 must be registered by October 3, 2026. This may include an institutional agreement with a foreign state-owned university to raise visa-delay concerns with federal officials.

   What this means: Proposed agreements or activities involving a foreign principal and engagement with Canadian government should be identified early. The responsible individual or University office should confirm whether registration is required and keep enough information to meet the deadline. Ordinary international collaboration is not automatically registrable; the arrangement and planned influence activity are the key questions.

Conclusion: This week's coverage shows that research security concerns can arise from people, partnerships, equipment, cyber systems, and government engagement. Each case should be reviewed based on its facts, while open and responsible research should continue.