



Newsline	Research Security	Week	Oct. 5 - 9, 2026
Editor	Alaa Dabboor	Research Security Manager	
	Research Security Centre (Public Safety Canada)		

Executive summary: This week's coverage looks at international research partnerships, foreign influence, dual-use technologies, AI-related cybersecurity threats, and competition for research talent and funding. It also includes an update on the Foreign Influence Transparency and Accountability Act (FITAA), clarifying when researchers and URegina may need to register. Other developments highlight technology transfer, academic mobility, and the protection of research infrastructure.

Key Points:

- 1. FITAA and foreign influence registration:** An update on the Foreign Influence Transparency and Accountability Act (FITAA) clarifies when researchers and URegina may need to register. Receiving foreign research funding, independently publishing findings, participating in international collaborations, exchanges or conferences, providing independent expert advice without policy advocacy, and routine government communications about grants or project administration generally do not require registration on their own.

Registration is required when all three conditions apply together: (1) an arrangement exists with a foreign principal, such as a foreign government or state-controlled institution; (2) the arrangement involves influence activities, such as advocacy, publications, communications, or providing services or facilities; and (3) the activities are intended to influence Canadian political or governmental processes, including laws, policies, regulations, or government decisions. URegina registers institutional arrangements through an authorized representative, while researchers register their own independent arrangements. Registration is required within 14 days of entering into a registrable arrangement.

What this means: Foreign funding and international collaboration alone do not automatically require registration. Researchers should consider who they are working with, the activities involved, and whether the arrangement is intended to influence Canadian government decisions or policies.

- 2. Open science, international partnerships, and foreign influence:** Canada's Chief Science Advisor, Mona Nemer, emphasized that open science and research security can work together. She encouraged stronger safeguards against espionage, foreign interference, and misuse of research while maintaining international collaboration. Queen's University Belfast is reviewing partnerships linked to the China General Technology Research Institute following MI5 allegations of connections to Chinese intelligence services. More than 100 UK-affiliated academics reportedly contributed to projects funded by the institute, sometimes unknowingly, in areas including AI and cybersecurity. In Italy, a new partnership between the University of Bari and Chengdu Normal University involving STEM research and academic exchanges has raised questions about technology protection. Separately, Global Affairs Canada withdrew sponsorship of an international disinformation conference over concerns about how certain sessions described the United States and foreign interference.

What this means: International collaboration remains important, but researchers should understand who funds their partners, their affiliations, and how research may be used. Appropriate partner reviews can help identify potential foreign interference and knowledge transfer risks.

- 3. Dual-use technologies and strategic research collaboration:** Halifax hosted NATO's Innovation Continuum, bringing together up to 600 researchers, industry representatives, and defence organizations to demonstrate technologies involving drones, autonomous systems, AI, cybersecurity, and Arctic operations. In New Zealand, the

growing overlap between civilian and military satellite applications is raising concerns about space security and dependence on foreign owned infrastructure.

Canada and India are also exploring a talent and innovation strategy that would establish Canadian-standard training centres in India, covering AI, aerospace, critical minerals, clean energy, and nuclear technology. The initiative aims to strengthen bilateral cooperation and workforce development.

What this means: These developments offer opportunities for research and international collaboration, alongside questions about technology transfer, potential end uses, and partner interests. Research intended for civilian purposes may also have military or strategic applications.

4. **AI governance, cybersecurity, and sensitive information:** Canada established a 13-member National AI Council, including Yoshua Bengio, to advise on AI adoption, safety, technological sovereignty, and protecting democratic institutions.

In South Korea, hackers allegedly used Artex, a Chinese AI-powered cybersecurity tool originally designed for authorized security testing, to breach at least seven financial institutions and expose personal information belonging to more than 68,000 people. The incident raised concerns about AI making sophisticated cyberattacks easier to carry out. Canada's Get Cyber Safe guidance also highlights five practical measures: assigning cybersecurity responsibility, developing a plan, protecting sensitive data, maintaining backups, and budgeting for security needs.

What this means: AI tools can support research and cybersecurity but may also introduce risks. Researchers should understand how their information is handled, who can access it, and what safeguards are in place, particularly when working with sensitive or unpublished research.

5. **Research talent, funding, and infrastructure security:** The University of Toronto announced a \$100-million scholarship program to attract doctoral researchers, offering selected students \$80,000 annually for four years beginning in 2027. China continues efforts to recruit international AI researchers through new visas and financial incentives, although attracting foreign talent remains challenging. In the United States, legal proceedings continue over the Trump administration's efforts to prevent Harvard from enrolling international students. Students remain enrolled while the case proceeds.

In Europe, the Netherlands launched a new innovation agency with €500 million planned over ten years to support breakthrough technologies and commercialization. The European Commission is proposing to reduce the number of EU funded research partnerships by approximately half, raising concerns about disruption to existing collaborations. Separately, the EU committed €65 million to strengthen critical biotechnology databases, including GENCODE, UniProt, and Europe PMC.

What this means: Changes in research funding, international mobility, and access to research infrastructure can affect collaboration and research continuity. Understanding funding relationships and planning for potential disruptions can help protect ongoing research.

Conclusion: This week's reports show how research security concerns can arise through international partnerships, foreign influence arrangements, emerging technologies, cybersecurity, and funding relationships. Reviewing these issues early can help protect research information, meet applicable requirements, and support responsible international collaboration.