



Newsline	Research Security	Week	July 13 – 17, 2026
Editor	Alaa Dabboor	Research Security Manager	
Reference Package			
1	Research Security Centre (Public Safety Canada)		
2	Radio-Canada Article		
3	Science		

Executive summary: This week highlights a research security landscape increasingly shaped by strategic technologies, defence innovation, cybersecurity, and evolving international research partnerships. Canada and its allies continued investing in artificial intelligence (AI), autonomous systems, and strategic technologies while strengthening measures to protect sensitive research and introducing new restrictions affecting international collaboration. Together, these developments reinforce the growing convergence of research, innovation, national security, and geopolitical competition.

Key Points:

- Strategic technologies continue driving research investment and international partnerships:** Canada expanded AI research through Anthropic's investment, while the European Union (EU), India, and Japan advanced cooperation in AI, semiconductors, quantum technologies, high-performance computing, and research capacity. These developments reinforce growing global competition in strategic technologies.
What this means: Strategic technologies are increasingly central to research competitiveness, technological sovereignty, and trusted international collaboration.
- Defence innovation and dual-use research continue expanding:** Canada announced a new defence innovation hub for autonomous systems, while the United Kingdom (UK) launched the Defence Universities Alliance to strengthen defence research, advanced skills, and academia–government collaboration.
What this means: Defence-related research and dual-use technologies are becoming increasingly integrated into national innovation strategies.
- Research security risks, insider threats, and protection of strategic knowledge remain significant concerns:** Recent cases involving a former Canadian government scientist, a former U.S. Federal Reserve adviser, the detention of a U.S. seismologist in China, and warnings about Chinese activities targeting Dutch strategic sectors highlight continuing concerns regarding insider threats, foreign interference, talent recruitment, and protection of sensitive technologies.
What this means: Protecting research increasingly requires awareness of insider risks, intangible technology transfer, and safeguarding strategic knowledge.
- International research collaboration is increasingly influenced by geopolitical and national security considerations:** The European Union and India expanded cooperation in strategic technologies, while on July 8, the U.S. National Science Foundation (NSF) announced a new research security policy that will ban NSF-funded collaborations with entities on U.S. restricted-party lists. Because these lists include hundreds of leading Chinese universities and research institutions, *Science* reported that the policy would effectively ban almost all collaborations with Chinese scientists on NSF-funded research. Effective October 1, 2026, the policy will also prohibit senior/key personnel from collaborating with, holding appointments at, or receiving research support from those restricted entities on NSF-funded projects.

What this means: Researchers and institutions receiving NSF funding should review existing and planned international collaborations to ensure compliance with the new policy and verify whether prospective collaborators or partner organizations appear on U.S. restricted-party lists.

5. **Cybersecurity remains fundamental to protecting research and critical infrastructure:** Canada, the United States (U.S.), the UK, and other allies jointly warned that Russian state-backed actors are targeting vulnerable networking equipment supporting critical infrastructure through cyber-enabled espionage. Radio-Canada also reported that Chinese state-linked hackers have targeted Canadian university research, reinforcing concerns about protecting sensitive research, intellectual property, and strategic technologies

What this means: Strong cybersecurity practices, secure infrastructure, and timely system maintenance remain essential to protecting research environments and critical infrastructure.

6. **Research funding and innovation ecosystems continue evolving:** Anthropic's AI investment, Japan's strategy to expand doctoral training, and renewed calls to better support Indigenous knowledge-sharing demonstrate continued efforts to strengthen research capacity, innovation, and inclusive research practices.

What this means: Building a resilient research ecosystem increasingly depends on strategic investment, skilled talent, and research approaches that support diverse knowledge systems.

Conclusion: This week's developments demonstrate the growing convergence of strategic technologies, research security, cybersecurity, and national security. As governments expand investment in innovation while introducing new safeguards and restrictions on international research collaboration, institutions must continue balancing trusted partnerships with effective protection of sensitive research and strategic technologies.