University of Regina

Newsline	Research Security	Week	June 15 - 19, 2026
Editor	Alaa Dabboor	Research Security Manager	
Reference Package			
1	Research Security Centre		

Executive summary: This week highlights a research security environment increasingly shaped by technological sovereignty, quantum innovation, cybersecurity threats, strategic international partnerships, and the growing security implications of artificial intelligence (AI). Across Canada and internationally, governments, research institutions, and industry are investing in advanced technologies, critical research infrastructure, and collaborative innovation networks while simultaneously strengthening efforts to protect sensitive knowledge, intellectual property, and strategic capabilities. At the same time, growing concerns regarding cyber espionage, dual-use research, export controls, and trusted access to emerging technologies continue to reinforce the close connection between research excellence, economic competitiveness, and national security.

Key Points:

1. **Technological sovereignty and strategic innovation capacity continue to grow:** Developments in Canada's rapidly expanding technology sector, Ottawa's leadership in quantum computing, and growing concerns regarding reliance on foreign-controlled AI technologies highlight increasing efforts to strengthen domestic innovation ecosystems and reduce strategic dependencies. Investments in advanced research infrastructure, including the Vaccine and Infectious Disease Organization's (VIDO) international partnership on high-containment pathogen research, further demonstrate a growing emphasis on technological resilience, biosecurity, and national research capacity.

   What this means: Governments increasingly view AI, quantum technologies, advanced research infrastructure, and innovation ecosystems as strategic assets. Research institutions may face growing expectations to strengthen resilience, diversify partnerships, and protect critical research capabilities and knowledge assets.
2. **Research security and cybersecurity are becoming increasingly interconnected:** Reports revealed that a Chinese-linked cyber espionage campaign targeted academic, medical, military, and research institutions in Canada and the United States for more than a year, seeking access to sensitive information related to artificial intelligence, defence, cyber operations, and medical research. The campaign reportedly exploited vulnerabilities in REDCap and employed credential theft and email monitoring techniques to support intelligence collection activities. Recent investigations involving suspected academic espionage at European universities further highlight the growing security challenges facing research institutions. At the same time, emerging technologies such as quantum computing and AI continue to create both opportunities and new security considerations.

   What this means: Cybersecurity remains a foundational component of research security. Institutions should expect continued efforts by foreign actors to acquire sensitive knowledge, research outputs, data, and strategic technologies through cyber-enabled and other means.
3. **Strategic competition is increasingly centred on AI, emerging technologies, and dual-use research:** Debates surrounding trusted-partner access to advanced AI models, export controls, and concerns

regarding companies identified as national security risks demonstrate the growing intersection between technological innovation and geopolitical competition. Questions surrounding dual-use applications, including AI and drone technologies, continue to challenge traditional research funding and oversight frameworks.

What this means: Strategic competition increasingly extends beyond traditional defence sectors to encompass AI, advanced computing, telecommunications, and emerging technologies. Due diligence, export control awareness, and understanding downstream applications remain important components of research security.

4. **International collaboration remains important but increasingly strategic:** New partnerships involving Canada, France, VIDO, European research networks, BRICS member countries, and global university alliances demonstrate continued demand for international research collaboration. Community-based and Indigenous-led research initiatives also highlight the importance of inclusive and collaborative approaches to knowledge creation. At the same time, concerns regarding academic espionage, reciprocity, trusted partnerships, and research security governance highlight growing expectations that international collaborations be conducted with appropriate safeguards.

   What this means: International collaboration remains essential to research excellence and innovation. However, institutions may face growing expectations to assess partnership risks, understand geopolitical contexts, and ensure collaborations are founded on transparency, reciprocity, and responsible research practices.

5. **Research security governance continues to mature:** Several developments highlighted increasing attention to oversight, accountability, and responsible stewardship of research activities, particularly in areas involving dual-use technologies, emerging technologies, and international partnerships. Research organizations continue seeking ways to balance openness, innovation, and collaboration with appropriate security safeguards.

   What this means: Research security is increasingly evolving from a compliance activity into an institutional governance function. Universities may face growing expectations to strengthen due diligence processes, partnership reviews, and risk-informed decision-making while maintaining open and collaborative research environments.

Conclusion: This week's Newsline reinforces that research security is increasingly connected to technological sovereignty, cybersecurity, AI governance, strategic competition, and international collaboration. As advanced technologies and research institutions themselves become more central to economic competitiveness and national security, governments and institutions are placing greater emphasis on protecting sensitive knowledge, strengthening trusted partnerships, and building resilient research ecosystems. Proactive risk assessment, cybersecurity preparedness, partnership due diligence, and responsible stewardship of research data remain important components of responsible research growth and innovation. A recurring theme across multiple jurisdictions is the growing effort to balance openness with protection. Whether through AI access restrictions, export controls, cybersecurity measures, trusted-partner frameworks, or international research collaborations, governments are increasingly seeking to preserve the benefits of global innovation while safeguarding critical technologies, research assets, data, and national interests.