University of Regina

Newsline	Research Security	**Week**	June 22 - 26, 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 AI, health data, quantum technologies, cybersecurity, critical infrastructure, nuclear strategy, Arctic security, and geopolitical competition. Across Canada and internationally, governments and research institutions are expanding access to advanced research infrastructure, sensitive data, and emerging technologies while also strengthening controls around national security, dual-use research, foreign interference, and cyber-enabled threats. Particular attention is being given to responsible governance of sensitive research data, trusted international collaboration, quantum technologies, and protection against cyber-enabled and intangible technology transfer risks. The key theme is balance: enabling innovation, collaboration, and technological sovereignty while protecting sensitive knowledge, data, infrastructure, and strategic capabilities.

Key Points:

1. **AI, health data, and advanced computing are becoming strategic research assets:** Canada's AI strategy to expand access to health data, the AI-quantum partnership between Queen's University and *Universite de Sherbrooke*, the modernization of UVictoria's national research cloud, and growing global competition in supercomputing demonstrate increasing investment in digital research infrastructure, technological sovereignty, and advanced computing capabilities. Together, these developments demonstrate how digital research infrastructure is becoming central to scientific leadership, economic competitiveness, and national innovation. They also emphasize the growing importance of privacy, data governance, cybersecurity, and public trust as institutions expand AI-enabled research involving sensitive information.
   What this means: Research data, computing platforms, AI systems, and quantum capabilities are no longer only technical assets; they are strategic assets. Institutions may face growing expectations to strengthen data governance, cybersecurity, access controls, and responsible AI use, especially where sensitive health data or advanced computing infrastructure is involved.
2. **Cybersecurity and research security are increasingly inseparable:** Reports involving alleged hacking of more than 150 U.S. universities, Five Eyes warnings about frontier AI accelerating cyber threats, and concerns that advanced AI could assist in identifying system vulnerabilities reinforce the growing connection between cyber risk and research security. These threats target academic data, credentials, research outputs, and sensitive institutional systems.
   What this means: Cybersecurity is a foundational part of research security. Universities should expect continued attempts by foreign actors and criminal networks to access research data, intellectual property, and sensitive technologies through cyber-enabled means. Strong cyber hygiene, secure platforms, incident reporting, and researcher awareness remain essential.
3. **Dual-use research and intangible technology transfer remain major concerns:** The Ottawa student case involving aerospace research allegedly helpful to Iran's weapons programs highlights the risks associated with international research mobility, sanctioned entities, and knowledge transfer. Similar concerns appear in the ASIO (Australian Security Intelligence Organization)-disrupted AUKUS (a trilateral security

partnership among Australia, United Kingdom, and United States) espionage case, where a foreign intelligence officer allegedly sought sensitive defence information from a cleared individual.

What this means: Research security risk is not limited to physical exports or formal partnerships. Knowledge, expertise, training, software, methods, and technical discussions can also create security concerns. Institutions should continue applying due diligence to affiliations, end-use, end-users, sanctions exposure, and potential military or weapons-related applications.

4. **Critical infrastructure, telecommunications, nuclear energy, and Arctic research are increasingly linked to national security:** Canada's new powers to ban high-risk telecom suppliers, its Nuclear Energy Strategy, and U.S. legislative efforts to restrict Russian and Chinese Arctic research activity all point to the growing security sensitivity of infrastructure-related research and technology. These areas intersect with energy security, communications, uranium production, reactor technologies, critical minerals, secure supply chains, defence, and strategic geography.

   What this means: Research connected to telecommunications, nuclear technologies, Arctic activity, infrastructure mapping, energy systems, and critical minerals may require closer review. Institutions should consider whether projects involve sensitive infrastructure, foreign access, export controls, controlled goods, or strategic data that could support foreign state interests.
5. **Geopolitical competition is increasingly shaping research, trade, and technology access:** China's export controls on U.S. rare-earth firms, new overseas ethnic unity law, and advances in supercomputing highlight how research, technology, supply chains, and state power are increasingly connected. These developments also show how export controls, procurement restrictions, and extraterritorial legal claims can affect universities and international collaborations.

   What this means: Research institutions may need to better understand geopolitical context before entering partnerships or sharing data, equipment, software, or expertise. Due diligence, export control awareness, sanctions screening, and partnership transparency remain important tools for managing risk while preserving open research.
6. **Research security governance and trusted collaboration continue to mature:** The University of Manitoba's role in the 2026 Canadian Research Security Conference, the Team Canada–HERSA (Higher Education Research Security Association) partnership, and expanded discussion of Arctic security, generative AI, foreign interference, and policy development show that research security is becoming a more established institutional function.

   What this means: Research security is moving beyond one-off compliance checks toward ongoing governance, education, and risk-informed decision-making. Universities may face growing expectations to support researchers early, build internal capacity, and maintain trusted international collaboration with appropriate safeguards.

Conclusion: This week's Newsline highlights the growing intersection of research, technology, and national security. As research institutions advance innovation through global collaboration, maintaining trusted partnerships, responsible governance, and proportionate safeguards will remain essential to protecting Canada's research ecosystem.