University of Regina

Newsline	Research Security	**Week**	June 8 - 12, 2026
Editor	Alaa Dabboor	Research Security Manager	
Reference Package			
1	Research Security Centre		
2	Research Data Management – Tri-Agency		

Executive summary: This week highlights a research security environment increasingly shaped by technological sovereignty, defence innovation, research security governance, cyber-enabled espionage, strategic competition, and evolving international research partnerships. Across multiple jurisdictions, governments are investing in advanced technologies, research infrastructure, and innovation ecosystems while strengthening measures to protect strategic research, intellectual property, data, and national interests. Collectively, these developments reinforce the growing convergence of research, innovation, economic competitiveness, and national security.

Key Points:

1. **Technological sovereignty and strategic research capacity continue to expand:** Countries are investing heavily in AI infrastructure, advanced technologies, semiconductors, quantum research, and strategic research facilities. Canada's potential participation in NATO's Innovation Fund and the development of Vaccine and Infectious Disease Organization (VIDO)'s Level 4 containment laboratory further demonstrate growing emphasis on technological resilience, biosecurity preparedness, and national research capacity.
   What this means: Governments increasingly view advanced research infrastructure, AI, biosecurity capabilities, and emerging technologies as strategic assets. Research institutions may face growing expectations to protect critical knowledge, technologies, and data while supporting national innovation priorities.
2. **Research security governance and data stewardship are becoming more formalized:** Governments and funding agencies continue strengthening oversight of sensitive research, foreign funding, and technology protection. Discussions surrounding the Tri-Agency Research Data Management Policy also highlight growing attention to data governance, stewardship, transparency, and responsible management of research outputs.
   What this means: Research security is increasingly evolving into an institutional governance function. Universities may face growing expectations to assess risks, strengthen data governance practices, and implement safeguards while maintaining international collaboration.
3. **Strategic competition is increasingly centred on emerging technologies and defence innovation:** AI, semiconductors, quantum technologies, advanced manufacturing, and dual-use research continue to attract significant government attention. Canada's growing participation in allied defence innovation initiatives and international technology partnerships demonstrates how emerging technologies are increasingly viewed through both economic and national security lenses.
   What this means: Strategic competition increasingly extends beyond traditional defence sectors to encompass research ecosystems, innovation networks, advanced technologies, and commercialization pathways. Partnership due diligence and visibility into affiliations, funding sources, and downstream applications remain important.

4. **Cyber-enabled espionage, AI governance, and intellectual property protection remain significant concerns:** Reports highlighted continued cyber espionage targeting technology companies, intellectual property, AI capabilities, and strategically valuable data. Ongoing discussions surrounding AI governance, copyright, and responsible AI development further demonstrate the growing intersection between cybersecurity, innovation, and research security.

   What this means: Cybersecurity, intellectual property protection, AI governance, and research security are becoming increasingly interconnected. Institutions should expect continued attention on protecting sensitive knowledge, research outputs, and strategic technologies.
5. **International collaboration remains important but increasingly strategic:** New international partnerships continue to support research excellence and innovation. At the same time, geopolitical tensions, foreign influence concerns, researcher travel risks, the detention of academics in sensitive geopolitical environments, and initiatives such as China's Science Silk Road demonstrate how research collaboration is increasingly being shaped by broader economic, geopolitical, and strategic objectives.

   What this means: International collaboration remains essential, but institutions may face growing expectations to understand geopolitical contexts, partnership dynamics, foreign influence risks, researcher safety considerations, and potential security implications while supporting global scientific engagement.

Conclusion: This week's Newsline reinforces that research security is increasingly connected to technological sovereignty, defence innovation, research governance, cybersecurity, AI governance, data stewardship, biosecurity, and international collaboration. As research becomes more closely linked to economic competitiveness and national interests, proactive risk assessment, partnership due diligence, and coordinated institutional oversight remain important components of responsible research growth.