University of Regina

Newsline	Research Security	**Week**	May 11 – 15, 2026
Editor	Alaa Dabboor	Research Security Manager	
Reference Package			
1	Research Security Centre		

Executive summary: This week highlights a research security environment shaped by talent mobility, AI infrastructure, dual-use innovation, foreign interference, and growing pressure on academic autonomy. Canada is investing in domestic research capacity through graduate talent programs, AI compute infrastructure, and medical research recruitment, while also facing risks tied to sanctions evasion, controlled technologies, and foreign interference. Internationally, universities are navigating funding instability, national security investigations, defence-linked partnerships, quantum security gaps, and geopolitical competition. Overall, research security continues to sit at the intersection of innovation, talent, infrastructure, partnerships, and national security.

Key Points:

1. **Talent mobility is becoming both an opportunity and a risk:** Canada is investing in Talent Innovation Canada to embed graduate researchers with companies and strengthen innovation, productivity, and talent retention. Toronto's University Health Network is also recruiting global scientists through its Canada Leads program, positioning Canada as an attractive destination for medical research talent.
   What this means: Talent attraction can strengthen Canada's research capacity, but it also requires clear visibility into affiliations, funding, intellectual property, and sensitive research areas.
2. **AI infrastructure and domestic compute capacity are becoming strategic priorities:** Canada is aiming to build an AI supercomputer that could rank among the world's top systems, supported by federal investment to expand domestic compute capacity for researchers and businesses.
   What this means: AI compute is increasingly part of research sovereignty and competitiveness. Institutions should expect more attention to secure compute access, technological sovereignty, and responsible use of advanced AI infrastructure.
3. **Dual-use research and defence integration are gaining momentum:** Witnesses before the House Science and Research Committee emphasized the need to reform procurement and better integrate research, industry, and defence ecosystems to support dual-use technology development.
   What this means: Dual-use innovation can create major opportunities, but it also increases the need for early risk assessment, export control awareness, and clear partnership due diligence.
4. **Academic autonomy and research freedom are under pressure globally:** Argentina's university funding cuts, European warnings about threats to university autonomy, the U.S. National Science Board dismissal, and the lockdown of university labs in Indiana all point to growing pressure on research environments.
   What this means: Research security must be balanced with academic freedom, transparency, and institutional autonomy. Security-driven decisions can significantly affect research continuity, trust, and international collaboration.
5. **Foreign interference and transnational repression remain active risks:** Court documents in Canada indicate individuals were targeted through Chinese anti-corruption initiatives, raising concerns about

intimidation, surveillance, and pressure on Canadian residents. The source also highlights risks faced by highly skilled researchers operating within national security-driven environments.

What this means: Foreign interference is not limited to research partnerships. It can also involve pressure on individuals, diaspora communities, researchers, and institutions.

6. **Sanctions evasion and controlled technology diversion remain difficult to manage:** CSIS visited a Quebec company after Canadian-made sniper rifles appeared in Russia despite export bans. The case raises concerns about how restricted military goods can be diverted through illicit channels.

   What this means: Institutions and companies working with controlled goods, defence-related technology, or sensitive partners need documented due diligence, supply chain awareness, and escalation pathways.

7. **Emerging technologies are creating new security gaps:** The Netherlands leads in quantum technology but is lagging in quantum security readiness. The Newsline also highlights Five Eyes Project Arcadia, Chinese solar technology security concerns in Europe, and China's strategic focus on AI, semiconductors, manufacturing, and military-civil fusion.

   What this means: Research security must anticipate risks before technologies mature. Quantum, AI, energy systems, defence data integration, and critical infrastructure technologies require proactive safeguards.

8. **International partnerships require stronger ethical and reputational review:** Cambridge University's potential work with Saudi Arabia's defence ministry highlights the tension between international engagement, human rights concerns, academic freedom, and reputational risk.

   What this means: Partnership reviews should consider not only technical or legal risk, but also ethics, institutional values, reputational exposure, and defence-sector implications.

Conclusion: This week's Newsline reinforces that research security is becoming a broader institutional capability. Talent, AI infrastructure, dual-use research, sanctions evasion, foreign interference, quantum readiness, and academic autonomy are increasingly interconnected. Earlier risk identification, stronger due diligence, and closer coordination across research services, partnerships, compliance, privacy, IT, and leadership are important to support secure and responsible research growth.