University of Regina

Newsline	Research Security	**Week**	May 19 – 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 AI talent, sovereign technology capacity, dual-use innovation, trusted international partnerships, foreign interference, surveillance, sanctions evasion, and growing integration between universities and defence-related ecosystems. Canada is investing in AI recruitment, biomedical AI, space launch capability, defence testing infrastructure, and military innovation programs, while governments continue increasing scrutiny on high-risk technologies and foreign-linked partnerships. Internationally, developments involving China-linked espionage allegations, People's Liberation Army (PLA)-affiliated research collaborations, security-based research funding vetoes, allied research cooperation, and secure AI infrastructure demonstrate that research security is becoming increasingly operationalized across research, funding, and governance environments. Overall, research security continues to sit at the intersection of innovation, infrastructure, partnerships, supply chains, talent, and national security.

Key Points:

1. **AI talent and sovereign AI capacity are becoming strategic priorities:** Canada is strengthening AI capacity through the University of Alberta and Alberta Machine Intelligence Institute (Amii)'s $30M recruitment campaign and Cohere's expansion into biomedical AI and European markets, supporting domestic AI capacity, commercialization, and sovereign AI capabilities.
   What this means: AI talent, biomedical data, compute capacity, and international AI partnerships are increasingly part of research security. Institutions should expect growing attention on due diligence, data governance, IS infrastructure, trusted partnerships, and secure AI collaboration environments.
2. **Dual-use research and defence integration are expanding:** Federal and provincial investments are supporting defence testing at Ontario Tech University and Alberta's DEFENDS program, connecting universities, industry, and the Canadian Armed Forces around military and dual-use technologies.
   What this means: Universities are becoming more directly connected to defence and dual-use innovation ecosystems. This increases the need for early risk assessment, export control awareness, partnership review, and clear intake and routing mechanisms for sensitive projects.
3. **Sovereign infrastructure and strategic technology capacity are gaining importance:** Canada's investment in domestic satellite launch capability reflects growing focus on sovereignty, defence, communications resilience, and reduced dependence on foreign providers.
   What this means: Research infrastructure is increasingly viewed as both an innovation asset and a strategic security consideration. Space, aerospace, communications, and advanced technology initiatives may require stronger research security review and oversight.
4. **Trusted international partnerships and allied research ecosystems are becoming increasingly strategic:** This week highlighted growing cooperation among allied and like-minded countries in areas including AI, climate technologies, security, aerospace, defence innovation, and advanced research collaboration.

What this means: Institutions may increasingly need to balance international collaboration opportunities with geopolitical considerations, trusted partnership frameworks, and protection of sensitive technologies and knowledge.

5. **Foreign interference and research espionage remain active risks:** German authorities arrested individuals accused of gathering advanced technology information for China through university and research networks, while a Strider report highlighted extensive collaboration between Australian and New Zealand institutions and PLA-affiliated entities in sensitive Science, Technology, Engineering, and Mathematics (STEM) areas, reinforcing growing emphasis on partnership due diligence, affiliation visibility, and network-based risk assessment.

   What this means: Affiliations of concern, talent recruitment pathways, visiting researchers, joint publications, and institutional partnerships remain central research security considerations, particularly in AI, aerospace, advanced communications, and other dual-use research areas.

6. **Trusted technology and supply chains are under growing scrutiny:** Ontario is moving to ban Chinese-made drones across ministries and police operations due to sensitive data concerns. Reporting also highlighted sanctions evasion networks using intermediaries and shell companies to move sensitive technologies to Russia.

   What this means: Procurement, vendor risk, supply chains, and technology sourcing are increasingly interconnected with research security and institutional risk management. Institutions may require stronger visibility into technology providers, third-party risks, and indirect partnership exposure.

7. **Research funding decisions are increasingly influenced by national security considerations:** Australia vetoed multiple research funding applications on national security grounds, reflecting growing willingness by governments to intervene directly when research is considered strategically sensitive.

   What this means: Research security is becoming increasingly operationalized across funding and governance environments. Earlier screening and coordinated institutional review may help reduce late-stage disruption, reputational exposure, and funding-related risk.

8. **Surveillance and transnational repression risks continue to evolve:** Reporting this week highlighted advanced Chinese surveillance systems targeting foreign nationals and Iran's use of cyber-espionage, intimidation, and digital monitoring against dissidents abroad.

   What this means: Research security extends beyond projects and partnerships. It also includes researcher safety, travel security, digital security, and protection of individuals operating in higher-risk international environments.

Conclusion: This week's Newsline reinforces that research security is becoming a broader institutional capability. AI, defence innovation, trusted technology, space infrastructure, foreign interference, surveillance, sanctions evasion, and strategic partnerships are increasingly interconnected. Earlier risk identification, documented due diligence, and coordinated institutional review across research services, partnerships, privacy, IT, procurement, compliance, and leadership are important to support secure and responsible research growth.