University of Regina

Newsline	Research Security	**Week**	June 1 - 5, 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 artificial intelligence (AI) governance, technology sovereignty, cybersecurity, science diplomacy, strategic competition, and foreign influence activities. Across Canada, Europe, China, and the United States, governments are strengthening efforts to secure critical technologies, reduce strategic dependencies, protect research ecosystems, and align innovation with broader economic and national security objectives. At the same time, institutions are facing growing expectations regarding partnership due diligence, research governance, transparency, cybersecurity preparedness, and protection of sensitive knowledge and technologies. Collectively, these developments reinforce the growing integration of research, innovation, technological competitiveness, and national security.

Key Points:

1. **Technology sovereignty is becoming a strategic priority:** Canada's new AI Strategy emphasizes safety, reliability, domestic infrastructure, and technological sovereignty, while Europe is pursuing measures to reduce dependence on foreign-controlled cloud services, AI platforms, and critical technologies. Similar developments in China and elsewhere demonstrate a growing focus on securing strategic technologies, data, and innovation ecosystems.

   What this means: Governments increasingly view AI capabilities, cloud infrastructure, advanced computing, data ecosystems, and critical technologies as strategic national assets. Research institutions may face growing expectations to consider infrastructure dependencies, data sovereignty, resilience, and trusted technology ecosystems when developing research partnerships and technology strategies.
2. **AI security governance is rapidly expanding:** Several developments highlighted the growing intersection between AI, cybersecurity, and national security, including Canada's AI Strategy, research demonstrating AI-enabled cyber threats, concerns regarding AI-powered surveillance, and risks associated with AI-enabled disinformation and influence operations.

   What this means: AI governance is evolving beyond innovation policy into a broader security and risk-management domain. Institutions should expect growing attention on AI governance, cybersecurity, model security, data stewardship, intellectual property protection, and responsible development of advanced AI capabilities.
3. **Science diplomacy and research collaboration are becoming strategic policy tools:** The European Union adopted its first Science Diplomacy Framework, while Europe's inaugural research security conference highlighted the increasing importance of balancing open research with security considerations. Governments are increasingly viewing research collaboration, talent attraction, and scientific engagement as instruments supporting broader geopolitical and innovation objectives.

   What this means: Research partnerships are increasingly being viewed as strategic assets rather than solely academic activities. Institutions may face growing expectations to consider how international

collaborations, talent networks, and research relationships contribute to scientific influence, competitiveness, and national interests while maintaining appropriate security safeguards.

4. **Strategic competition for research ecosystems is intensifying:** Several articles highlighted growing competition surrounding biotechnology, advanced research, technology transfer, foreign funding, and innovation ecosystems. Simultaneously, concerns regarding foreign-linked funding, technology transfers, and acquisition of advanced technologies continue to receive increased attention from governments and security agencies.

   What this means: Competition increasingly extends beyond individual technologies to encompass research ecosystems, talent pipelines, funding relationships, intellectual property, and innovation capacity. Visibility into affiliations, partnerships, funding sources, and strategic dependencies remains an important component of research security due diligence.

5. **Research security governance and foreign influence awareness continue to mature:** Research security discussions are becoming increasingly embedded within institutional governance frameworks. Meanwhile, Five Eyes partners issued warnings regarding foreign intelligence services using professional networking and recruitment platforms to target individuals with access to sensitive information.

   What this means: Research security is increasingly evolving from a compliance function into a broader institutional responsibility. Universities globally are strengthening partnership review, disclosure requirements, due diligence processes, and awareness programs to help protect research assets, intellectual property, and sensitive information.

Conclusion: This week's Newsline reinforces that research security is increasingly connected to AI governance, technology sovereignty, science diplomacy, strategic competition, cybersecurity, and foreign influence awareness. Governments are investing in technological leadership while strengthening governance and security frameworks across research, innovation, and critical infrastructure. As research becomes more closely linked to economic competitiveness and national interests, early risk identification, partnership due diligence, and coordinated institutional oversight remain important components of responsible research growth.