University of Regina

Newsline	Research Security	**Week**	April 27 – May 1, 2026
Editor	Alaa Dabboor	Research Security Manager	
Reference Package			
1	Research Security Centre		

Executive summary: Recent developments highlight the growing intersection of research security with advanced energy systems, defence and security ecosystems, emerging technologies, and global partnerships. In Canada, activity spans nuclear innovation, quantum strategy, defence industrial expansion, and AI-enabled safety systems. Internationally, trends point to strategic competition in technology supply chains, evolving collaboration risks, institutionalization of research security practices, and increasing cyber-enabled espionage. Together, these developments reinforce the importance of research security across critical infrastructure, dual-use technologies, partnerships, and data-driven systems.

Key Points:

- **Advanced nuclear research and energy innovation:** The University of Alberta is launching a Next Generation Nuclear Energy program focused on small modular reactors, safety, policy, and workforce development through collaboration with industry and government partners.
  What this means: Emerging energy technologies are closely linked to national capability, requiring attention to dual-use risks, regulation, and secure collaboration.
- **Expansion of defence industrial ecosystems in Canada:** Oshawa is emerging as a potential hub for Canada's defence industry, leveraging industrial capacity, workforce, and infrastructure to support growing demand.
  What this means: Defence-related growth in new regions reflects deeper integration between industrial capacity and national security priorities.
- **Canada's role in allied security financing and coordination:** Canada has been identified as the prospective host of a new multinational Defence, Security and Resilience Bank supporting allied projects.
  What this means: Leadership in defence financing signals expanded involvement in allied coordination and long-term security investment.
- **Quantum collaboration and national innovation strategy:** The Prairie Quantum Corridor is strengthening Canada's National Quantum Strategy through regional collaboration in research, talent, and commercialization.
  What this means: Quantum technologies are becoming a strategic domain where research, commercialization, and national security intersect.
- **AI-enabled safety and governance in nuclear systems:** Dalhousie University is advancing AI tools to improve safety, transparency, and decision-making in nuclear energy systems.
  What this means: Integrating AI into critical systems requires secure, explainable, and accountable approaches to support safety and oversight.
- **Strategic technology competition and industrial policy:** European concerns over Chinese green technology highlight tensions between competitiveness and national security priorities.
  What this means: Technology supply chains are increasingly shaped by geopolitical pressures and the need for strategic control.
- **Research collaboration risks in emerging technologies:** China–Iran research ties in aerospace, AI, and nanotechnology demonstrate targeted cooperation in dual-use domains.

What this means: Collaboration risks are becoming more visible, reinforcing the need for due diligence and partner assessment.

- **Institutionalization of research security practices:** South Korea has launched a national Research Security Center to support risk assessment, education, and collaboration oversight.
  What this means: Research security is increasingly formalized as a core institutional function supported by centralized tools and guidance.
- **Academic collaboration on security and resilience:** Nordic business schools are expanding collaboration focused on governance, resilience, and geopolitical risk.
  What this means: Security considerations are extending into leadership, governance, and cross-sector decision-making.
- **Cyber-enabled espionage through academic impersonation:** A spear-phishing campaign targeted NASA and research institutions by impersonating trusted researchers to obtain sensitive software.
  What this means: Trust-based environments remain vulnerable to social engineering, emphasizing the need for awareness and verification.
- **Semiconductor supply chains and strategic partnerships:** Canada–Japan cooperation is being positioned to strengthen semiconductor supply chains through specialization and joint investment.
  What this means: Securing critical technologies increasingly depends on coordinated partnerships within trusted networks.
- **Military innovation ecosystems and dual-use technologies:** China's military innovation model leverages competitions, universities, and industry to advance capabilities in unmanned systems and integrated operations.
  What this means: Military-civil integration highlights how civilian research ecosystems can contribute to defence capabilities.
- **AI-driven surveillance and data ecosystems:** AI-enabled surveillance systems are expanding large-scale data collection and behavioral analysis across society.
  What this means: The scale of data use introduces risks related to privacy, governance, and concentration of control.
- **Autonomous systems and defence innovation in Canada:** Saskatchewan Polytechnic is advancing AI-enabled drone systems for detection and interception of unauthorized aerial vehicles.
  What this means: Autonomous systems are becoming central to defence capabilities, reinforcing the importance of domestic innovation.
- **Research due diligence and institutional risk assessment tools:** The Chinese Academy of Sciences directory provides insights into institutional links to defence-related activities.
  What this means: Accessible tools support due diligence and help reduce risks in international research collaboration.

Conclusion: The research environment continues to evolve alongside advances in energy systems, emerging technologies, global competition, and security-focused collaboration. Research security is increasingly shaped by considerations related to critical infrastructure, dual-use technologies, partnerships, and data governance, reinforcing the importance of maintaining awareness while supporting responsible and secure research.