University of Regina

Newsline	Research Security	**Week**	April 6 – 10, 2026
Editor	Alaa Dabboor	Research Security Manager	
Reference Package			
1	Research Security Centre		

Executive summary: Recent developments highlight the growing intersection of emerging technologies, geopolitical dynamics, and research security risks. Advances in quantum communication and cybersecurity reflect continued investment in protecting sensitive data, while global events expose supply chain vulnerabilities and the need for domestic resilience. At the same time, international developments point to rising concerns around foreign interference, cyber threats, export controls, and dual-use governance, alongside continued calls for global collaboration. These trends reinforce the importance of research security awareness across technology development, partnerships, and the protection of research data, infrastructure, and compliance obligations.

Key Points:

- **Quantum technologies and secure communications:** Canadian research is advancing quantum-enabled communication security through photon-detection systems enabling interception awareness and ultra-secure transmission, protecting sensitive digital and financial data while modernizing infrastructure.
  What this means: Quantum advancements increase the strategic sensitivity of research outputs, requiring protection of data, IP, and emerging capabilities.
- **Supply chain vulnerabilities and resilience:** Geopolitical conflict has exposed fragile global supply chains, including disruptions to critical resources such as liquid helium used in healthcare and research, highlighting reliance on foreign suppliers and the need for domestic capacity.
  What this means: External dependencies may affect research continuity, emphasizing resilience and secure access to critical materials.
- **International collaboration and geopolitical pressures:** Global developments reflect both the need for stronger collaboration and rising geopolitical complexity, including EU cooperation calls amid funding pressures and concerns over Hungary's engagement with Russia in sensitive areas.
  What this means: International partnerships may carry geopolitical, funding, and regulatory risks, requiring due diligence and policy alignment.
- **Dual-use research and life sciences governance:** Efforts to strengthen dual-use governance, including Malaysia's national initiative, focus on identifying regulatory gaps, improving oversight, and aligning with international biosecurity frameworks.
  What this means: Dual-use research requires oversight to balance innovation with biosafety and biosecurity.

- **Cybersecurity risks and data breaches:** A reported large-scale, petabyte-scale breach involving a Chinese supercomputing centre highlights risks to sensitive defence and research data and vulnerabilities in advanced infrastructure.
  What this means: Cyber incidents may expose sensitive data and IP, reinforcing the need for strong cybersecurity practices.
- **Emerging technology governance and oversight:** International efforts, including quantum cooperation initiatives and increased scrutiny of foreign interference in academia, highlight growing attention to research, investment, and supply chain security.
  What this means: Emerging technologies face increasing oversight, requiring alignment with evolving research security expectations.
- **Geopolitical conflict and research environments:** Conflict-related events affecting research institutions demonstrate how geopolitical tensions can disrupt research operations and infrastructure.
  What this means: Geopolitical instability may impact research continuity, requiring awareness in international engagement.
- **Funding pressures and competitiveness:** Global trends show contrasting funding environments, including increased investment calls in some regions and proposed major cuts to key research agencies in others.
  What this means: Funding shifts may influence collaboration patterns and research priorities.
- **Targeted cyber threats and surveillance:** Advanced threats include targeted malware campaigns against universities and NGOs and AI-enhanced satellite monitoring of military activities.
  What this means: Sophisticated cyber and surveillance capabilities increase risks to research systems, data, and personnel.
- **Legal and compliance risks in research:** Stricter export-control enforcement highlights risks in routine research activities, such as data sharing, with potential for criminal charges, deportation, and long-term career impacts.
  What this means: Research involving sensitive technologies requires strong awareness of regulatory and compliance obligations.

Conclusion: The research landscape is increasingly shaped by technological advancement, geopolitical pressures, and security considerations. While innovation and collaboration remain critical, risks related to cybersecurity, supply chains, foreign interference, and compliance are becoming more prominent. These trends reinforce the need for ongoing research security awareness and responsible practices.