

Newsline	Research Security	Week	June 29 – July 3, 2026
Editor	Alaa Dabboor	Research Security Manager	
Reference Package			
1	Research Security Centre (Public Safety Canada)		
2	Huntress (reported by The Hacker News)		
3	TechCrunch		
4	U.S. Department of the Treasury / U.S. Department of State		
5	The Wall Street Journal		

Executive summary: This week highlights a research security landscape increasingly shaped by trusted international partnerships, technological sovereignty, defence innovation, AI, quantum technologies, cybersecurity, and economic security. Canada and its allies continue strengthening trusted collaboration while investing in sovereign digital and industrial capabilities in AI, semiconductors, quantum technologies, and defence-related research. At the same time, cyber threats targeting cloud platforms and software supply chains, along with expanding sanctions, export controls, outbound investment restrictions, and other economic security measures continue to reshape the global research environment. The key theme is the growing convergence of research, technology, economic security, and national security.

Key Points:

- Trusted international collaboration increasingly supports technological sovereignty and economic resilience:** Western University and Dalhousie University expanded collaboration in AI, defence, and research security, while Canada and Germany strengthened semiconductor cooperation. McMaster also expanded partnerships with Baltic institutions in AI, cybersecurity, robotics, and health technologies, reinforcing Canada's focus on trusted international collaboration and resilient innovation ecosystems. These initiatives collectively strengthen Canada's trusted technology ecosystem across AI, semiconductors, defence innovation, and cybersecurity.

What this means: Trusted research partnerships are increasingly influenced by national security, economic security, and technological sovereignty. Partner due diligence and proportionate safeguards remain essential for strategic research.
- Defence innovation and dual-use technologies continue to accelerate:** The Netherlands established a defence innovation hub at Delft University of Technology (TU Delft) focused on drones, quantum technologies, sensors, space systems, and advanced materials. The U.S. launched the QuantumEAGLe initiative to strengthen sovereign quantum supply chains, while continued investment in fusion energy research and Canada's Mitacs Defence and Security Call demonstrate growing support for defence-related innovation.

What this means: Emerging technologies increasingly have both civilian and defence applications, reinforcing the importance of identifying dual-use considerations early in the research lifecycle.
- AI, quantum technologies, and advanced computing are becoming strategic capabilities:** Canada's semiconductor partnership with Germany, Alberta's leadership in quantum innovation, expanding AI education and workforce development, and Communications Security Establishment (CSE)'s continued investment in AI-enabled cyber defence and quantum-resistant security demonstrate increasing competition to develop sovereign digital capabilities.

What this means: AI, quantum technologies, semiconductors, and advanced computing are becoming strategic assets that require responsible governance, secure research environments, and protection of emerging technologies.

4. **Cybersecurity and software supply chain security continue to emerge as major research security priorities:** CSE's Annual Report highlights Canada's evolving cyber threat landscape and growing cyber resilience. Separately, Huntress reported an Azure password spraying campaign involving more than 81 million authentication attempts that compromised at least 78 Microsoft accounts. In a separate incident, Microsoft disrupted a software supply chain compromise affecting dozens of GitHub repositories after attackers inserted credential-stealing malware into open-source tools used by Azure and AI developers.

What this means: Cloud identities, software supply chains, and AI development environments are increasingly attractive targets for cyber-enabled attacks, reinforcing the importance of strong cyber hygiene, secure development practices, and identity protection.

5. **Economic security measures continue to influence international research collaboration:** China strengthened oversight of outbound investments in strategic technologies and expanded export restrictions affecting Japanese organizations involved in dual-use technologies. Separately, the United States imposed sanctions targeting organized crime networks in Mexico and Brazil, procurement and recruitment networks supporting the conflict in Sudan. In addition, The Wall Street Journal reported that China is developing legal mechanisms allowing domestic organizations to seek compensation for losses caused by foreign sanctions.

What this means: International research collaborations are increasingly influenced by export controls, sanctions, outbound investment restrictions, and other economic security measures. Understanding partner affiliations, regulatory obligations, and geopolitical context remains important for informed decision-making and responsible international collaboration.

6. **Science diplomacy and talent security are becoming increasingly important to trusted research collaboration:** Stephane Dion argues that Canada needs a coordinated science diplomacy strategy to strengthen international collaboration while protecting national interests. At the same time, the National Science Foundation (NSF) Secure advisory highlights continued concerns regarding China's foreign talent recruitment programs and the risks of intangible technology transfer. Together, these developments emphasize that maintaining international collaboration increasingly requires strategic awareness alongside appropriate research security measures.

What this means: International collaboration remains essential to research excellence, but growing geopolitical competition continues to increase expectations for due diligence, awareness of foreign talent recruitment programs, and protection of sensitive knowledge while supporting open science.

Conclusion: This week's Newsline highlights the growing convergence of research, technology, cybersecurity, defence innovation, and economic security. As advanced research and emerging technologies become increasingly strategic, trusted collaboration and proportionate safeguards will remain essential to supporting innovation while protecting Canada's research ecosystem.