University of Regina

Newsline	Research Security		
Week	March 9 - 13, 2026		
Editor	Alaa Dabboor	**Position**	Research Security Manager
Reference Package			
1	Research Security Centre		

Executive summary: Recent developments highlight the increasing intersection between scientific research, national security, and geopolitical competition. Governments are investing in strategic technologies such as artificial intelligence, drones, quantum technologies, and advanced maritime systems while strengthening oversight of research collaboration and intellectual property protection. At the same time, cyber espionage, economic espionage, and foreign interference continue to target research institutions and emerging technologies. These developments illustrate the growing importance of research security awareness when engaging in international collaborations and emerging technology research.

Key Points:

- **Investment in strategic and dual use technologies is expanding:** Canada announced a $900 million investment through the National Research Council to establish a drone innovation hub supporting defence related innovation in aerospace, autonomous systems, and quantum technologies. Similarly, Japan has prioritized investments in artificial intelligence, robotics, and quantum technologies. Partnerships such as the University of Toronto collaboration with Hanwha Ocean also illustrate increasing connections between academic research, industry innovation, and national capability development.

  What this means: Research conducted in academic environments may contribute to technologies with strategic or security implications. Awareness of potential dual use considerations and appropriate research risk assessment practices can support responsible innovation.
- **Global competition in science and innovation is intensifying:** China plans to increase research and development spending by at least 7 percent annually between 2026 and 2030 while expanding investment in artificial intelligence and national laboratories. European organizations are also proposing new funding mechanisms to strengthen institutional research networks. In response to growing geopolitical complexity, some institutions are exploring science diplomacy initiatives that connect research collaboration with international policy engagement.

  What this means: Increasing global competition in science and technology may influence international research partnerships and collaboration patterns. Awareness of geopolitical context may help inform research security considerations in global collaborations.
- **Strengthening oversight of international research collaboration:** Universities in New Zealand have supported stronger export control measures to address risks related to foreign interference and unintended technology transfer. These proposals emphasize the need for safeguards that reduce proliferation risks while remaining proportionate and not placing unnecessary burdens on fundamental research.

What this means: International policy discussions highlight the importance of transparency and due diligence when engaging in research collaborations involving sensitive technologies or intellectual property.

- **Persistent cyber espionage targeting research environments:** Finland's intelligence service reports ongoing cyber espionage and influence operations conducted by Russia and China targeting government systems, research institutions, and advanced technology organizations. These activities combine cyber intrusions, traditional intelligence methods, and political influence campaigns aimed at obtaining sensitive research and technological information.
  What this means: Research data and emerging technologies can make research environments attractive targets for cyber and intelligence activities. Awareness of cybersecurity practices and protection of sensitive research information remain important considerations.
- **Increasing scrutiny of research partnerships:** A U.S. lawmaker has called for a pause on a $17 million research security agreement with Texas A&M University due to concerns about safeguarding federally funded research from entities linked to the Chinese military. The case reflects broader concerns about foreign involvement in research related to sensitive or dual-use technologies.
  What this means: Research partnerships involving strategic technologies may face increasing scrutiny and accountability requirements.
- **Emerging risks from AI enabled economic espionage:** Artificial intelligence is enabling new forms of economic cyber espionage, including automated reconnaissance, model extraction attacks, and AI driven phishing targeting valuable technological assets.
  What this means: Emerging technologies may create new pathways for the exploitation of research outputs and intellectual property.
- **Changing dynamics in global scientific publishing:** China is investing heavily in strengthening its scientific journals with the goal of becoming a leading global publishing force by 2035, potentially increasing its influence over global research dissemination.
  What this means: Changes in the global research publishing landscape may influence how scientific knowledge is disseminated and evaluated internationally.

Conclusion: The global research environment is increasingly shaped by technological competition, geopolitical dynamics, and evolving national security concerns. Governments are investing in strategic technologies while strengthening oversight related to international collaboration, cybersecurity, and intellectual property protection. These developments highlight the importance of maintaining awareness of research security considerations while supporting open and collaborative research.