University of Regina

Newsline	Research Security	**Week**	August 10 – 14, 2026
Editor	Alaa Dabboor	Research Security Manager	
Reference Package			
1	Research Security Centre (Public Safety Canada)		
2	External Research Intelligence (Subscription-Based Source)		

Executive summary: This week's coverage focuses on risks related to dual-use research, AI, intellectual property, international partnerships, and technology supply chains. It also shows how China is working to influence global AI and IP rules. For URegina, early review, clear agreements, and practical safeguards should be included in research planning.

Key Points:

1. **Dual-use research and Arctic activity require closer attention:** Four former Western University students face additional charges in an explosives and firearms case that began after a trespassing incident at an engineering building and included allegations involving weapon-related computer data. Canada and the United States are monitoring Chinese research icebreakers whose sonar and telemetry equipment may also be used for submarine detection and seabed mapping. New Zealand also disrupted a proposed Chinese-linked satellite-tracking site, while a UK Arctic program stressed that local knowledge and public trust are important for responsible research.

   What this means: Access to laboratories, hazardous materials, equipment, and data should be limited to approved personnel and activities. Projects involving Arctic research, satellites, sonar, or other dual-use technologies should be reviewed early. Community or Indigenous engagement should also be considered where relevant.

2. **AI is accelerating research and security threats:** Canadian firm Transformer Lab launched Primus to review literature, develop hypotheses, run experiments, and prepare research papers. At the same time, suspected China-linked actors reportedly used AI agents in an autonomous cyberattack against Taiwan, and North Korea's Kimsuky group is reportedly using AI-generated research documents for phishing. Researchers also demonstrated that AI can design new viruses, creating both scientific opportunities and biosecurity concerns.

   What this means: AI research tools should be reviewed for data protection, research integrity, cybersecurity, and dual-use risks. Human review should be maintained, and AI-generated documents and invitations should be verified. Higher-risk AI or biological research may require additional review.

3. **International research collaboration is facing stronger controls:** Australia is considering powers for intelligence agencies to review university agreements without notice, while South Korea is creating a sensitive R&D category with stronger safeguards for foreign participation. China is expanding exit-ban rules related to industrial and technological security. In the United States, scientists warned that a proposed rule restricting federally funded collaboration with China could weaken U.S. research competitiveness.

   What this means: International collaboration should continue to be supported based on the level of risk. Partners, foreign participation, sensitive information, travel, and government requirements should be reviewed without creating unnecessary restrictions for low-risk research.

4. **Canada faces growing innovation and intellectual-property competition:** Canadian technology firms are often sold to foreign buyers when they reach the scaling stage, moving strategic decisions abroad. China's 2026-2030 Intellectual Property Plan treats IP as a national competitive resource by connecting patents, trade secrets, AI, critical technologies, commercialization, specialized talent, overseas expansion, and international standards. The plan is expected to strengthen Chinese firms from research and patent development to commercialization and overseas expansion.

   What this means: Ownership, licensing, publication, commercialization, and patent rights should be clarified before research begins. Existing and project-generated IP should be protected, particularly when technology may be transferred or commercialized in China or other markets.
5. **China is seeking greater influence over global AI governance:** Through the World AI Conference and the new World AI Cooperation Organization, China is promoting open AI models, training, infrastructure, and technical support, particularly across the Global South. China is also working to influence international AI standards and using its Digital Silk Road presence to expand Chinese AI platforms. The coordinated Kimi K3 release supported this message, although questions remain about foreign technology dependencies and alleged use of U.S. models for training.

   What this means: AI platforms and open models should be reviewed before use. The review should consider where the model came from, how data and IP will be managed, and whether URegina may become dependent on one provider. Changes in international AI standards should also be monitored.
6. **Supply-chain and network security remain practical risks:** Camera components in UK military drones were found transmitting operational status data to an IP address in China, raising concerns about hidden connectivity in technology supply chains. A suspected rogue Wi-Fi network appeared on a Delta flight, raising concerns that travelers could be redirected to fraudulent networks. Delta confirmed that no airline systems were hacked, and no aircraft operating or safety systems were affected. The incident remained under investigation.

   What this means: Equipment, connected components, and technology suppliers should be checked before sensitive use. Unnecessary external connections should be removed. Trusted networks and secure devices should also be used during travel.

Conclusion: Research security is becoming connected to more areas of university research. Early review and practical safeguards will help URegina protect sensitive work while continuing to support responsible collaboration.