University of Regina

Newsline	Research Security	**Week**	September 14 - 18, 2026
Editor	Alaa Dabboor	Research Security Manager	
	Research Security Centre (Public Safety Canada)		

Executive summary: This week's news covers international research partnerships, AI and biosecurity, sensitive technologies, researcher travel, cyberespionage, influence operations, and academic freedom. The developments highlight opportunities for international collaboration as well as concerns related to affiliations, technology transfer, cybersecurity, and researcher safety.

Key Points:

1. **Research partnerships, AI, and research capacity in Canada:** Canada is looking to deepen research and education links with the European Union, including expanded participation in Horizon Europe and possible membership in Erasmus+. Cooperation could also expand in AI, quantum, cybersecurity, research infrastructure, economic security, and student mobility, although details are still to be defined.

   Canada is also investing $150 million in LawZero, with Germany contributing another €100 million, to develop "safe-by-design" AI. Its Scientist AI model could potentially safeguard other AI systems, although experts caution that technical measures alone may not address misinformation, unpredictable behaviour, and loss of human oversight.

   Canadian biomedical researchers also raised concerns about research capacity after only 13% of CIHR applications were funded in spring 2026. Stagnant funding, more applications, and inflation are affecting laboratories, staff retention, and international collaboration, while researchers called for broader investment alongside the new Eddie Goldenberg Canada Research Chairs.

   What this means: Canada is expanding international research opportunities while also facing questions around domestic research capacity and safe development of emerging technologies.

2. **Researcher travel, international partnerships, and academic freedom:** China's new rules allow exit bans for national security or technology-related reasons, potentially without prior notice, creating risks for academics and researchers working on sensitive topics, despite the recent decision to allow Canadians visa-free visits for up to 30 days. Separately, U.S. scholar Min Zin was detained after travelling to China for an academic workshop on espionage allegations rejected by his family and the U.S. government. U.S. officials suspect his past involvement in Myanmar's pro-democracy movement and U.S.-funded academic research may have attracted the attention of Chinese security services. He has been designated as wrongfully detained by Washington.

   The Australian Strategic Policy Institute reported extensive links between universities in Hong Kong and Macau and Chinese military, aerospace, space, AI, state laboratory, and defence research, including contributions to lunar missions. Another report examined Michigan State University relationships with Chinese institutions involved in propaganda and public-opinion management, noting potential dual use of digital communications, audience analysis, and AI. It did not allege deliberate support for Chinese government objectives.

   At the same time, the International Science Council announced a science diplomacy initiative to support international cooperation during geopolitical tensions. Scholars at Risk also documented 382 attacks on higher education communities across 59 countries and territories, including violence, arrests, restrictions on expression, job losses, and government interference in university autonomy, research, and funding.

   What this means: International activities may require consideration of institutional affiliations, research areas, local laws, travel risks, and researcher safety while supporting legitimate international collaboration.

3. **Sensitive technology, AI, and cyberespionage:** South Korea expanded its espionage law for the first time since 1953 to cover foreign-linked theft of state secrets, including potentially sensitive semiconductor and AI technologies. China accounted for more than half of detected overseas technology-transfer cases in 2025, although prosecutors must still prove the information is a state secret.

   U.S. intelligence also raised concerns that a proposed US$24-billion sale of 48 F-35 aircraft to Saudi Arabia could expose sensitive technology to China through military relationships, Chinese access to Saudi facilities, and the use of Huawei and Zhongxing Telecommunication Equipment (ZTE) telecommunications equipment.

   China announced plans to expand AI cooperation among BRICS countries (Brazil, Russia, India, and China) through open-source AI, large language models, a shared cloud platform, training, technology exchanges, an engineering talent alliance, and youth innovation programs. Separately, a Chinese hacking-for-hire firm allegedly used AI to analyze and increase the intelligence value of stolen information.

   U.S., U.K., and Dutch authorities also warned that Iranian state-linked actors are using "CHOSEN BRICK" spyware against dissidents, activists, and journalists through spear-phishing on WhatsApp and Telegram, often impersonating trusted contacts, to steal emails, messages, contacts, and other sensitive data.

   What this means: Sensitive information and technology can be exposed through people, partnerships, infrastructure, technology transfer, and cyberattacks. Access, technology transfer, and potential end use are important considerations.

4. **AI biosecurity and influence operations:** Anthropic reported five cases where scientists used Claude for biological research with potential dual-use applications, including virus mutation and toxin research that the company argued could potentially support bioweapons development. Some researchers reportedly attempted to bypass restrictions. Experts disagreed on the level of concern, with some seeing serious biosecurity risks and others viewing the work as similar to legitimate biomedical research.

   Citizen Lab also reported that BlackCore, an Israeli "influence-for-hire" company, allegedly used fake personas, social media campaigns, content amplification, and AI-generated content. A case in Angola reportedly included a supervised influence campaign as part of training for government communicators.

   What this means: AI and digital tools can support legitimate research but may also have dual-use, cyber, biosecurity, and influence-operation applications.

Conclusion: This week's developments highlight research security issues related to international partnerships, institutional affiliations, researcher travel, AI, sensitive technologies, cyberespionage, biosecurity, influence operations, and academic freedom. They also show the ongoing challenge of supporting international research and innovation while protecting sensitive research, technologies, and information.