University of Regina

Newsline	Research Security	**Week**	August 31 – September 4, 2026
Editor	Alaa Dabboor	Research Security Manager	
	Research Security Centre (Public Safety Canada)		

Executive summary: This week's coverage focuses on artificial intelligence (AI), cyber threats, research disclosure, military-linked partnerships, strategic technologies, and supply chains. It also shows the importance of responsible digital infrastructure, careful screening, and continued support for open research. Closer attention may be needed when sensitive data, foreign affiliations, connected systems, or dual-use technologies are involved.

Key Points:

1. **Responsible AI and digital infrastructure need stronger planning:** Canada launched its Responsible Data Centre Development Principles for infrastructure supporting artificial intelligence, cloud computing, research, and digital services. The framework sets five expectations related to local benefits, electricity costs, water and environmental impacts, transparency, and strategic value to Canada. It also aims to strengthen Canadian control over important digital infrastructure and data and help municipalities assess proposed data-centre projects. An advocacy group warned that Canada's national AI strategy does not adequately address possible superintelligent AI risks. The group urged Canada to prohibit the domestic development of superintelligent AI and lead international efforts to negotiate and enforce a global ban. Separate research recorded more than 300 incidents in July, nearly double the number reported in June. These incidents included AI systems reportedly ignoring instructions, bypassing approvals, misleading users, or impersonating them.

   What this means: AI tools and data-centre services should be reviewed for security, data protection, environmental impact, Canadian control of sensitive information, human oversight, and loss-of-control risks. Important decisions should not be fully delegated to AI systems.

2. **Espionage and surveillance concerns can involve students, researchers, and activists:** A University of Waterloo student was arrested in Michigan and accused of making false statements during an investigation into suspected intelligence-gathering activities. Investigators alleged that he photographed aircraft and airport facilities at the direction of a contact in China, received payment for some images, and used Chinese subscriber identity module (SIM) cards and encrypted communications. No espionage charge had been laid at the time of reporting. In Taiwan, a former government contract researcher was indicted for allegedly leaking confidential documents, transferring funds, and gathering information for individuals linked to a Chinese espionage network in exchange for monthly payments. Prosecutors also alleged that she helped arrange payments to military personnel involved in the broader network. Citizen Lab confirmed that Pegasus spyware infected the phone of a Serbian student activist through a zero-click exploit. The case was part of broader spyware targeting in Serbia, where at least 14 student activists, civil-society members, and opposition figures received similar warnings ahead of the 2026 elections.

   What this means: Foreign direction, payment, unusual information requests, and concealed communications may indicate higher risk. Requests to photograph facilities, collect information, or transfer documents should be treated carefully. Secure devices and reporting processes should be used, especially during travel or politically sensitive research.

3. **Foreign affiliations and military-linked research are receiving closer review:** Australia's research funding agency is adding stronger foreign-interference screening to approximately one billion Australian dollars in grants. Researchers who fail to disclose foreign scientists, institutions, affiliations, or support could lose access to funding. Ohio State University agreed to pay $2.1 million to settle allegations involving undisclosed China-related ties. The

case involved a professor who participated in China's Thousand Talents Program while conducting research funded by the National Aeronautics and Space Administration and the National Science Foundation. An Australian professor also defended robotics research with Chinese military-linked universities, stating that there was no evidence of transfer to the Chinese military.

What this means: Foreign affiliations, funding, support, appointments, talent-program participation, and partner roles should be fully disclosed. Research involving military-linked institutions, robotics, autonomous systems, or other dual-use areas should receive early review, even when the stated purpose is civilian.

4. **Strategic technology and supply-chain security are becoming more connected:** The Group of Seven (G7) called for faster preparation for quantum-safe cybersecurity by identifying critical systems, reviewing current encryption, developing phased migration plans, and adding quantum-safe requirements to future procurement. South Korea and Japan discussed cooperation on artificial intelligence, semiconductors, energy, and critical-mineral supply chains. China reportedly surpassed the United States in clinical trials, biomedical research output, and research and development investment, raising concerns about genetic data security, dependence on Chinese manufacturing and medicines, and research and innovation moving to China.

   Another report stated that more than 50,000 sensitive or potentially dual-use goods reached Russian defence entities through Indian supply chains since 2022 and identified expanding Russia–India research and talent networks. In Canada, federal and provincial organizations, including the Royal Canadian Mounted Police and the Department of National Defence, awarded more than $2 million in contracts to companies operated by an Edmonton businessman under national security investigation. According to declassified Canadian Security Intelligence Service documents, he was investigated over allegations that he supported Iran's military technology and missile-development efforts before immigrating to Canada.

   What this means: Before procurement or collaboration, critical systems, biotechnology suppliers, contractors, research partners, end users, and technology dependencies should be identified. Sensitive research and genetic data should be protected, current encryption reviewed, and quantum-safe procurement planned. Research relationships and higher-risk goods should also be monitored for sanctions, end-use, and technology-transfer risks.

5. **Research capacity should be strengthened without weakening academic freedom:** Nunavut Arctic College received $600,000 to expand parasite detection, improve its research-licensing portal, and provide training that supports ethical research and stronger relationships with Indigenous communities. The investment will also help Nunavummiut participate more fully in research and support responsible collaboration with visiting researchers. The institute also supports Arctic public health through wildlife parasite testing, mercury monitoring, and environmental research. In Kazakhstan, the arrest of Uzbek professor Ikboljon Qoraboyev on espionage charges created concern about due process, academic freedom, and self-censorship. His recent research used public information and focused on critical minerals and regional cooperation.

   What this means: Community-led research capacity, local participation, and responsible international collaboration should continue to be supported. Visiting researchers should follow community and licensing requirements. Security concerns should be assessed using clear evidence and fair processes so legitimate academic work is not discouraged.

Conclusion: This week's coverage shows that research security includes AI oversight, cyber protection, disclosure, partner review, procurement, and academic freedom. Clear and practical checks can help protect sensitive work while responsible research and international cooperation continue.