



Newsline	Research Security	Week	August 17 – 21, 2026
Editor	Alaa Dabboor	Research Security Manager	
Reference Package			
1	Research Security Centre (Public Safety Canada)		

Executive summary: This week's coverage focuses on research capacity, cyber espionage, foreign influence, international partnerships, critical technologies, and artificial intelligence. It also shows the challenge of protecting research while keeping international collaboration and global talent. For URegina, closer attention may be needed to research access, international affiliations, cyber risks, and the use of AI tools and datasets.

Key Points:

- 1. Research capacity depends on infrastructure, talent, and public trust:** Polytechnique Montreal's federally funded Ramp Up laboratory is supporting vaccine development, domestic biomanufacturing, supply-chain readiness, skilled-worker training, and public trust. Quebec universities warned that lower international enrolment may reduce graduate research capacity and global collaboration. In the United States, a new science and technology strategy seeks global talent and stronger critical-technology leadership, but partnership audits and a proposed four-year visa limit may affect STEM doctoral students.
What this means: Research infrastructure, training, and international talent should continue to be supported. Immigration or policy changes that may affect students, and projects should be monitored early. Public communication should also be included where trust is important to research.
- 2. Universities and researchers remain targets for influence and cyber espionage:** Canadian researchers identified Russian and American sources influencing online discussions about Alberta separatism. North Korean hackers are reportedly using AI for phishing, malware development, stolen data analysis, and fake remote-worker identities. Canadian research and critical infrastructure are among the reported targets. U.S. prosecutors also charged 17 Iranian nationals linked to the Mabna Institute over an alleged cyber-espionage campaign conducted on behalf of Iran's Islamic Revolutionary Guard Corps (IRGC). The campaign reportedly compromised more than 300 universities in the United States and other countries and stole over 31 terabytes of research, intellectual property, and email data. In Australia, a fake consulting website collected resumes and personal information from people with defence, intelligence, trade, and political backgrounds.
What this means: Research accounts, email, and professional information should be treated as valuable targets. Recruitment contacts and online opportunities should be verified, strong account security should be used, and suspicious activity should be reported. Foreign influence should also be separated from legitimate public debate based on evidence.
- 3. International partnerships require disclosure and case-by-case review:** Iran's Sharif University and Indonesia's Institut Teknologi Bandung signed an agreement covering joint research, exchanges, shared resources, emerging technologies, and commercialization. At the same time, the Pentagon directed 30 U.S. universities to review foreign partnerships by August 31 or risk losing funding. In Australia, a former Australian National University (ANU) vice-chancellor defended a cancelled China partnership as low risk and academically valuable. A U.S. professor was also banned from federal funding for six years after findings that Chinese talent-program participation was not disclosed while he helped oversee about \$80 USD million in grants.

What this means: International partnerships should be reviewed according to their actual risk, not only the country involved. Affiliations, funding, roles, research scope, technology access, and conflicts should be disclosed. Grant conditions and changes during the project should also be documented.

4. **Critical technology protection must be balanced with commercialization:** Canada blocked a board appointment at Quebec laser manufacturer CorActive, acquired by China's Han's Laser in 2017, because its specialty-fibre technology could benefit foreign militaries. Reuters also reported that a cryptocurrency venture backed by the Trump family was linked to WorldClaw, a Hong Kong platform where nearly half of the AI models came from Chinese firms flagged by the U.S. government, although the arrangement was legal. Separately, China's Unitree Robotics built successful robot dogs using ideas from openly published U.S. military-funded research. Researchers said this was not theft, but it showed the U.S. challenge in moving research into large-scale manufacturing. The Pentagon now lists Unitree as a contributor to China's defence industrial base.

What this means: Ownership, governance, technology transfer, partner control, and possible military use should be reviewed for critical technologies. AI platforms should also be checked for provider, model origin, licensing, data use, and security. Publication decisions should remain open where possible, while commercialization and protection plans should be considered early.

5. **AI training data can influence how systems understand the world:** China is developing large state-backed datasets and promoting their use internationally, especially in developing countries. The goal is to reduce reliance on English-language and Western data while increasing China's role in global AI development. Critics warn that these datasets may also promote Chinese government positions on issues such as human rights and Taiwan.

What this means: AI datasets should be reviewed for origin, quality, representation, political bias, licensing, and permitted use. Researchers should understand how training data may shape results, and important outputs should be checked through human review and other reliable sources.

Conclusion: This week's coverage shows that research risks can arise from cyberattacks, undisclosed affiliations, technology transfer, and the use of AI data. These risks should be reviewed based on each project, while open and useful research collaboration should continue.