University of Regina

Newsline	Research Security	**Week**	July 20 – 24, 2026
Editor	Alaa Dabboor	Research Security Manager	
Reference Package			
1	Research Security Centre (Public Safety Canada)		

Executive summary: This week's coverage focuses on investment in AI, defence, critical minerals, and other strategic technologies, as well as tighter controls on international research collaboration, foreign funding, and technology transfer. Reports involving ransomware, semiconductor trade secrets, and autonomous AI agents also show the range of security risks facing universities and researchers.

Key Points:

1. **Canada continues to invest in AI and strategic technologies:** The Government of Canada launched a consultation on AI transparency, covering AI-generated content, interactions with AI systems, serious incident reporting, and the activities of AI agents. Quebec also announced $20 million for an advanced-materials centre supporting critical minerals, electrification, and defence-related innovation. University of Calgary researchers are developing AI tools to identify false information, bot networks, and coordinated online manipulation.

   What this means: Canadian universities can expect continued attention to responsible AI use, strategic technology research, and information integrity.

2. **International research restrictions continue to expand:** The U.S. Department of Defense added Fudan University and Shanghai Jiao Tong University to its Section 1286 research security blacklist. Beginning in fiscal year 2026, Pentagon-funded researchers will be restricted from working with listed institutions, their personnel, or equipment. In Germany, researchers were criticized for attending conferences with Chinese and Russian institutions involving drones, autonomous flight, satellite navigation, hypersonic technologies, and AI.

   What this means: Institutional affiliations, funding restrictions, and possible dual-use applications should be reviewed before international collaborations begin.

3. **Foreign funding is drawing closer attention:** Major U.S. universities reportedly received at least US$27.6 million during the second half of 2025 from foreign entities on government watch lists. U.S. authorities have warned that these relationships could affect future federal funding decisions.

   What this means: Clear disclosure and partner-screening processes help universities identify potential security, compliance, and reputational concerns.

4. **Defence research and technology supply chains are expanding:** European Union defence research and development spending reached 17 billion Euros in 2025, up 31% from 2024, and is expected to reach 20 billion Euros in 2026. The U.S. Federal Communications Commission also proposed restrictions on foreign-made drones with military-grade capabilities, citing concerns about sensitive data, critical infrastructure, and supply chains.

   What this means: Research involving defence, autonomous systems, or advanced technologies may require closer review of end use, data access, and supply-chain risks.

5. **Research funding is shifting toward strategic areas:** The U.S. administration proposed directing more funding toward AI, robotics, nuclear energy, quantum computing, and space, while giving individual

researchers and the private sector a larger role. The UK also abolished its Department for Science, Innovation and Technology while elevating the AI minister to cabinet.

What this means: National security and economic priorities are having a greater influence on research funding and governance.

6. **Recent cases highlight risks to intellectual property:** The U.S. Treasury Department is investigating whether Chinese companies used outputs from American AI systems without authorization to train their models. In Taiwan, a former Taiwan Semiconductor Manufacturing Co. (TSMC) manager was charged with copying confidential semiconductor documents for an alleged business venture in China. The documents were recovered before any reported transfer.

   What this means: Sensitive data, model outputs, trade secrets, and personnel access need appropriate safeguards throughout a project.

7. **Universities continue to face cybersecurity threats:** Ransomware attacks against higher education increased during the first half of 2026. Mount Royal University reportedly faced a $1.9 million ransom demand and the alleged theft of more than 10 terabytes of data. Separately, advanced Open AI agents reportedly found ways to access the internet during restricted testing and targeted the Hugging Face platform.

   What this means: Secure systems, strong access controls, incident-response planning, and safeguards for autonomous AI tools remain important in university research environments.

Conclusion: The week's coverage shows that research security now touches many areas of university activity, from international partnerships and foreign funding to AI, cybersecurity, and intellectual property. Practical safeguards that protect research while allowing responsible collaboration and innovation are significant.