University of Regina

Newsline	Research Security	Week	July 27 – 31, 2026
Editor	Alaa Dabboor	Research Security Manager	
Reference Package			
1	Research Security Centre (Public Safety Canada)		

Executive summary: This week's Newsline highlights espionage and unauthorized transfer of research, growing controls on sensitive and dual-use technologies, international partnerships in strategic research areas, security concerns involving advanced AI and virology research, and cybersecurity threats affecting universities and business travellers.

Key Points:

1. **Espionage and unauthorized research transfer remain key concerns:** A Canadian NATO intern was arrested in Belgium on espionage charges and is suspected of working for China. In South Korea, several international students allegedly copied confidential source code and research files before leaving their universities and the country.

   What this means: Appropriate screening, access controls and offboarding procedures for anyone with access to sensitive research or systems are important. Access should be limited to what is required and removed promptly when a role or affiliation ends.

2. **Controls on sensitive and dual-use technologies continue to expand:** Chinese military-linked researchers reportedly used outputs from leading U.S. AI models to develop defence systems. Concerns were also raised about UK defence universities collaborating with Chinese military-linked institutions, while the U.S. restricted new foreign-made humanoid and quadruped robots and power inverters. Russia also continues obtaining controlled Western technologies through India.

   What this means: It is significant to assess the affiliations, end users and potential military applications of international collaborations. Technology-transfer and supply-chain risks may continue even when a restricted entity or country is not directly involved.

3. **International partnerships are creating opportunities but require careful review:** The University of Saskatchewan signed an agreement with the International Atomic Energy Agency to strengthen nuclear research, education and training. Israel is also seeking closer cooperation with Canada in AI, cybersecurity, digital health and smart-city technologies.

   What this means: Strategic international partnerships can provide important research and training opportunities. However, collaborations involving nuclear science, AI, cybersecurity or other sensitive areas should undergo appropriate due diligence and risk assessment.

4. **Sensitive research and advanced AI are raising new security questions:** The U.S. introduced stronger oversight of high-risk gain-of-function virology research and limits on funding in countries or institutions with inadequate biosafety standards. Open-weight AI offers greater transparency and control over data but can be adapted for harmful purposes. An Anthropic model also found weaknesses in reduced versions of encryption algorithms, although current encryption systems are not affected.

   What this means: Sensitive research requires strong governance, testing and independent oversight. Researchers using advanced or open-weight AI should consider possible misuse, access controls and longer-term implications for cybersecurity.

5. **Cyber threats increasingly target universities, legacy systems and travellers:** More than 144,000 credentials linked to education and research organizations were reportedly compromised through infostealer malware, ransomware and other cybercrime. Unsupported technologies remain common in critical sectors, while attackers are compromising hotel and conference Wi-Fi to steal Microsoft 365 credentials, including through fake device-code requests.
   What this means: Institutions should modernize unsupported systems, strengthen account security and monitor compromised credentials. Travellers should use approved VPNs, secure authentication methods and avoid accessing sensitive information through public Wi-Fi.

Conclusion: This week's coverage shows that research security risks can arise throughout the research lifecycle, from selecting partners and controlling access to sensitive information to using emerging technologies and protecting institutional systems. Strong due diligence, clear access controls, secure technology practices and ongoing risk monitoring remain essential for protecting research and supporting trusted collaboration.