University of Regina

Newsline	Research Security	Week	Oct. 13 - 16, 2026	Source(s)	Research Security Centre
Editor	Alaa Dabboor	Research Security Manager			

Executive summary: This week's coverage highlights AI-related cybersecurity threats, targeted attacks on researchers, foreign interference, sanctions compliance, and research security screening. It also examines researcher affiliations and mobility, data sovereignty, confidential research information, institutional security, and international research funding.

Key Points:

1. **AI threats and cybersecurity readiness:** A Cisco report found that 92% of surveyed Canadian organizations experienced a business-disrupting cyber incident in the past year. More than half took over a day to implement security controls after identifying a threat, while 71% needed at least six months to fully deploy new controls. Poor coordination, manual processes, and unclear responsibilities were among the reasons for delayed responses.

   Dozens of Canadian academics joined international scientists calling for stronger AI safety measures, including sandboxing, air-gapping, and international standards. Their warning cited testing involving AI systems from OpenAI, Anthropic, Meta, and Google that compromised external systems, as well as a failed attempt targeting Library and Archives Canada. Separately, Anthropic researchers warned that small AI models could become capable of spreading and replicating across internet-connected devices within months. No current model has reliably demonstrated this capability.

   Reflection: AI-related threats are evolving, while delays in implementing security controls can increase institutional exposure. Clear responsibilities, timely incident response, and appropriate safeguards are important when AI tools interact with sensitive research information or institutional systems.

2. **Targeted cyberattacks, surveillance, and insider threats:** Citizen Lab researchers found that Al Jazeera journalists were targeted with zero-click spyware developed by Candiru and delivered through online advertisements, allowing infection without clicking a link. The investigation also identified the alleged involvement of advertising technology firm Discover-Tech, with related advertisements appearing on nearly 200,000 websites and apps.

   North Korean hacking group Kimsuky reportedly targeted Ukrainian security and policy experts using fake conference invitations, collaboration requests, and malicious documents. The group allegedly sought intelligence about North Korea's involvement in Russia's war in Ukraine. Most observed attempts were unsuccessful.

   In another case, an OpenAI engineer was arrested after a concealed recording device was discovered in an executive conference room. Authorities allege it was intended to capture confidential discussions. OpenAI reported no evidence that source code, model weights, or customer data were accessed or stolen. Separately, Canadian cybersecurity executive Edward Dubrovsky was arrested over alleged involvement with ShinyHunters, a group that claimed responsibility for breaching the FBI's employment portal. The allegations against him remain unproven.

   Reflection: Threats can come through unexpected collaboration invitations, compromised devices, and unauthorized recording or access to confidential discussions. Researchers should verify unusual requests, protect sensitive meetings and information, and report suspicious activities.

3. **Sanctions, foreign partnerships, and researcher affiliations:** Global Affairs Canada published new guidance on "deemed ownership" under Canadian sanctions. Property held by an unlisted entity may be treated as belonging to a sanctioned individual if that person controls the entity through majority ownership, influence over its board, or the ability to direct its activities.

Following an MI5 warning, the Scottish Government urged universities to strengthen due diligence involving the China General Technology Research Institute (CGTRI), which MI5 alleges has ties to Chinese intelligence services and funds research that could support espionage.

A Digital Science report examined more than 3 million U.S. federally funded publications and 1.9 million researchers. It found that 48.2% of researchers affiliated with both a restricted entity and a U.S. institution held their U.S. appointment for two years or less. The report warned that short-term appointments may leave previous affiliations undisclosed and recommended targeted, risk-based screening rather than broad restrictions on international collaboration.

Reflection: Reviewing partner ownership, control, funding sources, and researchers' previous or short-term affiliations can help identify sanctions exposure, foreign interference, and knowledge-transfer risks.

4. **Researcher screening, international mobility, and security compliance:** Danish university leaders supported proposed legislation that would allow institutions to screen and potentially reject undergraduate and master's applicants from countries considered high risk, including China, Russia, and Iran. Supporters argue the measures would protect sensitive technologies, while critics warn about discrimination and the impact on international collaboration.

   In Japan, a study involving 18 Chinese graduate students found that research security concerns are increasingly affecting background screening, conference participation, research topic selection, and access to sensitive projects.

   In South Korea, a review of more than 33,000 state-funded R&D projects found that the only two classified as security-sensitive both involved foreign researchers who had not completed required security reviews. One involved next-generation lithium battery technology, while the other had its security classification changed after project selection.

   Reflection: Consistent, risk-based screening should consider project sensitivity, access to facilities and information, and relevant affiliations while protecting sensitive research without unnecessarily restricting international collaboration.

5. **Data sovereignty, AI confidentiality, and research funding:** A CSIS assessment warned that Canada's expanding data-centre sector faces risks beyond cyberattacks, including foreign ownership, supply-chain vulnerabilities, third-party service providers, and potential foreign-state influence. These concerns are growing as data centres become more important for AI, data sovereignty, and critical digital infrastructure.

   Researchers also raised concerns about sharing unpublished ideas and findings with AI chatbots. A Scientific American article examined disputes over whether AI companies could benefit from information researchers entered into their systems. The companies involved denied using the data for training, but questions remain about confidentiality, intellectual property, and transparency.

   In Europe, university organizations criticized proposed reductions to the next Horizon Europe research programme. Under the proposal, funding would fall to €158.2 billion, nearly 10% below the European Commission's proposed budget. Researchers warned that these reductions could affect research capacity, infrastructure, talent development, and international collaboration.

   Reflection: Researchers should understand where their data is stored, who can access it, and how external services and AI tools handle confidential or unpublished information. Funding changes and dependence on third-party infrastructure can also affect research independence, security, and continuity.

Conclusion: This week’s reports highlight research security risks involving AI, cyberattacks, international partnerships, researcher affiliations, and external services. Early due diligence and appropriate safeguards help protect sensitive research while supporting international collaboration.