University of Regina

Newsline	Research Security	Week	Nov. 09 - 13, 2026	Source(s)	Research Security Centre
Editor	Alaa Dabboor	Research Security Manager			

Executive summary: This week's developments highlight growing concerns about foreign interference, cybersecurity, sensitive technology transfers, and international research partnerships. Canada has reimposed sanctions against Iranian entities, while investigations involving university researchers, advanced AI technologies and suspected foreign intelligence activities have raised further security concerns. At the same time, governments and research institutions are working to strengthen research security while protecting academic freedom, scientific collaboration, and research competitiveness.

Key Points:

1. **Canada reimposes sanctions against 11 Iranian entities:** On November 10, Canada announced the reimposition of sanctions against 11 Iranian entities previously removed from its sanctions list in 2016. The measures took effect on November 5 and target organizations involved in Iran's nuclear and ballistic missile programs or related financing. The sanctions restrict specified financial transactions and access to sensitive technologies.

   Reflection: Screening international partners, funding sources and technology transfers against current sanctions lists is important as previous eligibility does not guarantee that an organization remains eligible today.

2. **Foreign interference and intelligence activities raise security concerns:** A University of Waterloo student pleaded not guilty in a U.S. court to making false statements during an FBI investigation involving allegations of photographing aviation facilities for a suspected Chinese government contact. Separately, a Safeguard Defenders report alleged links between Chinese authorities and at least 18 overseas police-related organizations in Canada. In the UK, two men were convicted of assisting Iranian intelligence through surveillance of dissident journalists, with one also convicted of preparing for serious violence.

   Reflection: These cases highlight the importance of recognizing potential foreign interference, protecting university communities from intimidation, and ensuring that suspicious activities can be reported through appropriate channels. Allegations should be assessed carefully without presuming wrongdoing.

3. **York University reports personal data theft:** York University disclosed a cybersecurity incident involving unauthorized access to departmental online forms. Stolen information included contact details, university identification numbers, and, in some cases, financial and government identification information. The university reported no evidence that its core systems were compromised and offered identity protection services to certain affected individuals.

   Reflection: Cybersecurity controls must extend beyond central IT systems. Departmental forms, research data, access permissions, and information retention practices deserve regular review.

4. **Advanced AI technologies and dual-use research face greater scrutiny:** Reuters reported that Northwestern Polytechnical University, a Chinese institution with military links and subject to U.S. restrictions, obtained Nvidia H200 AI chips through domestic suppliers. The findings raise questions about technology access and export control enforcement. Separately, Nvidia CEO Jensen Huang resigned amid reports of personal relationships, including one involving a woman suspected by U.S. intelligence of links to China. A separate Al Jazeera analysis examined the wider intelligence and semiconductor concerns. Nvidia stated that it had found no evidence of compromised sensitive information. Meanwhile, Japan plans to establish university-based defence research hubs focusing on AI, quantum technology, cybersecurity and space.

Reflection: Research involving advanced computing and dual-use technologies requires careful assessment of partners, end users, export controls and potential military applications. Sensitive technologies can present security risks even when their intended applications are civilian.

5. **Research security culture and academic freedom remain priorities:** Witnesses before Canada's House Science and Research Committee described the country's research security framework as a leading model but emphasized the need for stronger awareness, training and information sharing. The European Commission also held discussions on implementation challenges and stronger EU-level coordination. In Quebec, university professors raised concerns about political interference in teaching and research, calling for greater protection of academic freedom and institutional autonomy.

   Reflection: Effective research security depends on more than policies and screening. Universities need a shared security culture, clear responsibilities, and proportionate controls that protect research without unnecessarily limiting academic freedom or legitimate collaboration.

6. **International research funding and scientific priorities continue to shift:** Canadian research leaders are advocating for access to European Research Council grants beyond Canada's existing participation in Horizon Europe. European lawmakers have also supported a proposed €200 billion budget for Horizon Europe for 2028-2034, subject to further negotiations. In Africa, ministers endorsed stronger scientific leadership, research sovereignty, and the Science Granting Councils Initiative. Meanwhile, U.S. researchers filed a lawsuit challenging plans to dismantle the National Science Foundation's Social, Behavioral and Economic Sciences Directorate.

   Reflection: Changes in international research funding and government priorities may affect collaboration opportunities and research continuity. Monitoring these developments, diversifying partnerships, and supporting responsible and equitable international research are important.

Conclusion: This week's developments reinforce the need for a practical and proactive approach to research security. Protecting sensitive research, maintaining cybersecurity, screening partnerships and recognizing foreign interference are increasingly connected responsibilities. Strong institutional coordination and researcher awareness remain essential to managing risks while supporting open, responsible, and internationally competitive research.