University of Regina

Newsline	Research Security	Week	Nov. 02 - 06, 2026	Source(s)	Research Security Centre
Editor	Alaa Dabboor	Research Security Manager			

Executive summary: This week's updates highlight growing concerns about research security, cyber threats, foreign interference and international research partnerships. Canada has expanded sanctions against Russia, while new reports link Russian scientists to military technologies and expose ongoing cyberespionage activities. Meanwhile, several countries are strengthening research security frameworks, investing in strategic technologies, and expanding international scientific cooperation.

Key Points:

1. **Canada expands sanctions against Russia:** On November 9, Canada announced sanctions against 38 entities and 24 individuals, effective November 5. The measures target ballistic missile development, defence industries, cyber activities and financial networks, including cryptocurrency exchanges supporting sanctions evasion. The amendments also update goods schedules and provide a limited exception for financial services needed to obtain Canadian legal services concerning listed ships.
   Reflection: Research partners, funders and individuals must be screened against updated sanctions lists. The amendments must be read alongside the existing Russia Regulations.
2. **Russian scientists linked to military research:** Ukraine's Defence Intelligence identified 13 Russian scientists and engineers, along with research institutions, allegedly supporting military aviation, drones, robotics, machine vision and other dual-use technologies. Some reportedly maintain international research connections.
   Reflection: Research affiliations and potential military applications require careful review before establishing or continuing collaborations.
3. **Budget 2026 and strategic research priorities:** Canada's budget prioritizes economic growth, defence and strategic technologies, with limited new direct support for universities. Measures include $437.9 million over five years for Indigenous post-secondary students, support for women's health research, commercialization, AI and nuclear research. International student targets remain unchanged.
   Reflection: Increased investment in sensitive technologies calls for stronger protection of research, intellectual property and partnerships.
4. **Canada joins European supercomputing network:** Canada has joined EuroHPC, expanding access to European supercomputing, AI and quantum resources, with further partnerships under discussion. Separately, an OECD-focused report warns that reliance on major U.S. cloud and AI providers raises concerns about digital sovereignty.
   Reflection: International computing partnerships require clear safeguards for data residency, external access, and technology sharing.
5. **University supercomputers targeted by cybercriminals:** Two Canadians are accused of hacking U.S. university supercomputers between 2016 and 2019 to mine cryptocurrency. One was extradited to the United States in October 2026.
   Reflection: Research computing infrastructure needs strong access controls, monitoring, and protection against unauthorized use.
6. **Cyber Centre warns of help-desk phishing:** The Canadian Centre for Cyber Security warned of ongoing voice-phishing attacks, particularly against legal and financial organizations. Attackers impersonate IT staff to steal credentials and MFA responses, potentially compromising Microsoft 365 accounts, stealing data, and enabling extortion.

Reflection: Staff should verify unexpected IT requests independently. Phishing-resistant MFA, account monitoring, and awareness training remain essential.

7. **Chinese software and Russian mobile espionage:** Researchers uncovered a China-aligned cyberespionage campaign exploiting Sogou keyboard software to install a backdoor. Separately, Russia-linked APT29 reportedly targeted iPhone and Android users through compromised websites, including attacks requiring no user interaction.
   Reflection: Unapproved software, unmanaged devices, and mobile vulnerabilities can expose sensitive research information.
8. **Research security frameworks evolving internationally:** Australia is considering research security requirements within university registration standards. A UK parliamentary committee called for faster guidance, clearer risk assessments and a single contact point combining advisory and interference-reporting functions. Germany has launched its National Platform for Research Security.
   Reflection: Effective research security depends on clear responsibilities, timely assessments, and coordinated government support while preserving academic freedom.
9. **Cyber governance and international research mobility:** Quebec has begun transferring cybersecurity and digital responsibilities to the Treasury Board, ahead of legislative approval, raising concerns about oversight and expertise. Meanwhile, Japan and India are strengthening scientific cooperation in food, health and materials, including the LOTUS initiative aimed at bringing 1,000 Indian researchers to Japan in 2026.
   Reflection: Strong governance and early risk screening help institutions manage expanding international research partnerships and researcher mobility.
10. **Alleged Chinese transnational repression in Italy:** Italian prosecutors are investigating alleged surveillance and intimidation of Chinese dissidents, including the commentator known as "Teacher Li." Investigators reported suspected connections to Chinese police and United Front networks.
    Reflection: Foreign interference can threaten academic freedom, researcher safety, and the ability of international scholars and students to express themselves freely.
11. **Research independence and public trust:** A metascience report warns that growing political interest in research performance could affect scientific independence. Separately, an international university conference highlighted concerns about foreign interference, cyberattacks, technology transfer, and political pressure on universities.
    Reflection: Universities need closer coordination between research security, ethics and research integrity while protecting academic freedom, institutional autonomy, and public trust.

Conclusion: This week's developments reinforce the growing connection between research security, cybersecurity, sanctions compliance and international collaboration. Universities must remain open to research opportunities while identifying risks early, strengthening due diligence, and maintaining clear institutional responsibilities. Protecting research and academic freedom must remain central to these efforts.