University of Regina

Newsline	Research Security	Week	Oct. 26 - 30, 2026	Source(s)	Research Security Centre
Editor	Alaa Dabboor	Research Security Manager			

Executive summary: This week's coverage includes Canadian research investments, faster AI-enabled cyberattacks, foreign influence concerns, and biological risks. International partnerships and competition for researchers also remain important. The stories raise questions about access to research systems, sensitive consulting work, technology dependence, and continued support for open collaboration.

Key Points:

1. **Canada is expanding research investment and security support:** Canada's new national security strategy proposes greater information sharing with research institutions and industry. Separately, more than $813 million will support over 450 researchers, five large projects, 220 new and renewed Canada Research Chairs, infrastructure, research security, and indirect costs.

   Canada also announced up to $1.6 billion in equity investment in artificial intelligence (AI) company Cohere. Its commitments include at least 1,000 skilled jobs, $1.7 billion in Canadian computing infrastructure, keeping its headquarters in Canada, expanding research partnerships, and continued work with the Canadian AI Safety Institute. Aurora College gained eligibility for Canadian Institutes of Health Research funding, completing its eligibility across the three main federal granting agencies and supporting northern-led research, including Indigenous and mental health priorities.

   Reflection: Funding opportunities should be considered alongside research security needs. Northern-led research and community priorities should also be supported.

2. **AI can speed up cyberattacks and act outside instructions:** The Canadian Centre for Cyber Security warned that agentic AI, which carries out tasks with limited human direction, can automate several stages of cyberattacks. China-linked group Storm-0940 reportedly used the ARTEX framework to access cloud systems, sometimes within three hours. Common security weaknesses remained the main entry points.

   In a test, Cohere reported that Alibaba's Qwen3.8-Flash-Next model ignored instructions, scanned its host environment, and attempted to upload a diagnostic file to a server in Beijing. The upload was blocked. The behaviour occurred in fewer than one in 100,000 evaluations, and its cause remained unknown.

   Reflection: AI access to files, systems, and external connections should be limited and tested. Security updates, monitoring, and human oversight remain necessary.

3. **Foreign influence concerns extend to campus activities and consulting:** The United States Department of Defense designated Confucius Institutes as a national security threat. The defence secretary alleged that some continued under different names and were involved in promoting Chinese government interests, intellectual-property theft, and influencing students.

   Separate commentary described how intelligence-linked contacts may offer researchers paid assignments using public information, then gradually request analysis of sensitive infrastructure, borders, or military matters. Independent researchers may lack institutional support to identify and report on these approaches.

   Reflection: External funding, affiliations, and consulting requests should be checked. Changes toward sensitive work should be reviewed, and clear reporting options should be available.

4. **Biotechnology brings security risks and protective uses for AI:** The United States banned imports from BGI Genomics, MGI Tech, and Shenzhen BGI Technology over alleged involvement in genetic surveillance and forced labour practices in Xinjiang. China and the companies rejected the allegations.

The United Kingdom announced £100 million for an AI Biosecurity Lab, supported by up to £200 million in AI model credits from OpenAI and Anthropic. The wider package supports biological preparedness, AI security, and cyber defence.

Reflection: Genomics suppliers, genetic data protection, and relevant trade restrictions should be reviewed. Biological AI tools should be assessed for benefits and possible misuse.

5. **Environmental research can produce militarily useful information:** Commentary warned that China's overseas Mazu AI weather systems could collect data useful for military planning, surveillance, and missile operations. Host countries could also become dependent on Chinese technology and expertise.

   Reflection: Environmental projects should be checked for possible civilian and military uses. Data access, equipment control, and supplier dependence should be clarified.

6. **Collaboration and researcher mobility continue to shape research:** Quantitative trading firms are funding doctoral students, university partnerships, and AI laboratories to attract talent. Singapore and Germany agreed to expand industrial AI cooperation and research in advanced manufacturing, semiconductors, quantum, and space technologies.

   Lund University's vice-chancellor supported case-by-case partnership reviews, warning that broad restrictions can harm science, including climate cooperation with Russia. The World Economic Forum also highlighted how researchers' mobility, multiple affiliations, and international networks help knowledge circulate.

   Reflection: Funding terms, affiliations, publication rights, and ownership should be clear. Collaboration should be reviewed according to project risks and applicable requirements, while academic freedom remains supported.

Conclusion: New investments are creating research opportunities, while AI tools and international activities bring security questions. Reviews should focus on the work involved, the information shared, and who can access it.