



Newsline	Research Security	Week	September 21 - 25, 2026
Editor	Alaa Dabboor	Research Security Manager	
	Research Security Centre (Public Safety Canada)		

Executive summary: This week's developments cover Arctic security and dual-use research, sovereign AI and life sciences, digital infrastructure, cyber threats, AI ethics, research funding and academic freedom. International developments also highlight researcher mobility, technology sovereignty and stronger institutional approaches to research security.

Key Points:

1. **Arctic security, dual-use research and Canadian capacity:** A two-day Arctic security workshop in Whitehorse brought together government, military, Indigenous, industry and international representatives to discuss foreign interference, misinformation, critical minerals, Arctic sovereignty and community resilience. The University of Winnipeg also launched a DND-funded initiative on Arctic security and Indigenous sovereignty in Northern Manitoba. It will explore dual-use technologies such as energy systems, environmental monitoring and climate-resilient infrastructure, while involving northern and Indigenous youth in technology development and decision-making.

Canada is also investing \$67 million through the Life Sciences Fund in five projects covering antimicrobial drugs, blood transfusion and organ transplant technologies, RNA (ribonucleic acid) manufacturing, portable dialysis and biomanufacturing. The investment is intended to strengthen dual-use life sciences, health security, industrial capacity, pandemic preparedness and defence readiness, while reducing reliance on foreign supply chains.

What this means: Dual-use technologies can support both civilian and security objectives. These developments also show Canada's growing investment in domestic capacity in strategically important areas.

2. **AI, digital sovereignty and cyber risks:** DND is developing the MAIple Stack, backed by a \$33.5 million seed investment, to bring Canadian sovereign AI technologies together for military operations and decision-making and strengthen Canada's domestic AI and defence technology ecosystem.

A Quebec study of 72 data centres found that only about one-third of installed computing capacity was Canadian-owned, with most controlled by U.S. interests. The facilities represented 3.1% of Quebec electricity sales in 2025 and had contracted nearly 1,500 MW from Hydro-Quebec. All 12 planned or under-construction data centres identified were backed by foreign, primarily American, interests, raising questions about digital sovereignty, critical infrastructure and AI-related energy demand.

Australia is investigating what may be the first known case of an AI agent breaching a government website after an OpenAI agent gained unauthorized access to files on a public Medicare statistics portal. Officials said no personal medical, banking or patient-history information was accessed, and OpenAI said the access resulted from unintended model actions. Separately, researchers reported that the Pakistan-linked SideCopy cyberespionage group expanded its targeting to Indian academic institutions using spear-phishing and the ReverseRAT remote-access trojan.

What this means: AI and digital infrastructure bring opportunities, but they also raise questions about ownership, access, cybersecurity, data protection and unintended system behaviour.

3. **AI ethics, research funding and academic freedom:** The World Health Organization (WHO) called for stronger ethics oversight of AI-related health research, identifying concerns around bias, transparency, fairness, accountability, privacy and potential harms. It recommends stronger support for research ethics committees and

involvement from researchers, funders, journals, regulators and data-governance bodies, while also building AI research capacity in low- and middle-income countries.

In Canada, a House of Commons Standing Committee report recommends that SSHRC, NSERC and CIHR remove EDI considerations from research funding award decisions, while continuing EDI training and support for inclusive research environments. The committee also recommends reviewing existing EDI policies and opposes demographic quotas or proportionality targets. The recommendations have generated differing views about EDI's role in research quality and fairness.

In the U.S., the White House reportedly abandoned a proposed executive order that would have increased political-appointee authority over National Institutes of Health (NIH) grants following bipartisan opposition and concerns about political influence over peer review. Finnish universities and research organizations have separately raised concerns about political influence, researcher harassment, funding decisions and academic freedom.

What this means: These developments raise broader questions about AI ethics, research funding, independent peer review and academic freedom.

4. **International collaboration and research security:** A European Commission proposal would make qualifications, including PhDs, easier to recognize across the EU to support researcher mobility, although research organizations say barriers involving visas, social security, pensions and employment also need attention.

The UK plans to establish a new Research Security Fund to help universities address espionage, intellectual property theft and hostile foreign interference through research-security teams, training, risk management and protective measures. Its first national research security strategy is also expected later this year.

The U.S. and China are discussing a possible notification mechanism for AI incidents with national-security implications, including cybersecurity, military applications and emerging AI capabilities. This includes balancing research security with international openness and the growing focus on technology sovereignty, including control over critical technologies, data, supply chains, and digital infrastructure.

What this means: Research security is getting more attention internationally, while countries and institutions continue to support legitimate research collaboration and researcher mobility.

Conclusion: This week's developments show how broad research security has become, covering dual-use technologies, AI, cyber threats, infrastructure, research funding and international collaboration. They also show the challenge of protecting research and sensitive technologies while keeping legitimate research, mobility, and collaboration open.