



|                   |                                                 |                           |                    |
|-------------------|-------------------------------------------------|---------------------------|--------------------|
| Newsline          | Research Security                               | Week                      | August 4 – 7, 2026 |
| Editor            | Alaa Dabboor                                    | Research Security Manager |                    |
| Reference Package |                                                 |                           |                    |
| 1                 | Research Security Centre (Public Safety Canada) |                           |                    |

**Executive summary:** This week's coverage shows that research security is increasingly connected to Canada's defence, health, democratic resilience, economic security, and international research relationships. New investments in quantum and pandemic research are being supported, while foreign influence, cyber threats, surveillance, export controls, and supply-chain concerns continue to grow. Secure partnerships, clear disclosure, proportionate review, and continued support for open research remain important.

#### Key Points:

1. **Strategic research capacity is expanding:** Canada launched its first Quantum Defence Innovation Secure Hub, led by the University of Calgary with \$20.3 million over two years. A new \$267-million Medical Countermeasures Laboratory is also planned in Winnipeg to strengthen vaccine, therapeutic, and diagnostic capacity. At the same time, commentary called for sustained investment in fundamental science and a national approach to support scholars at risk.

**What this means:** Opportunities in defence, quantum, health security, and fundamental research may increase. Early review of funding conditions, sensitive technologies, facilities, data, personnel, and partner access should be built into project planning. Support for scholars at risk should also be considered through coordinated academic, security, immigration, and well-being processes.

2. **Research partnerships are becoming more strategic:** Concordia's international climate partnership brings environmental humanities, social sciences, natural sciences, museums, policymakers, and communities together. Vietnam is also positioning science diplomacy as a way to obtain knowledge, talent, and research networks while building domestic control of strategic technologies.

**What this means:** International and interdisciplinary partnerships should continue to be supported, but objectives, roles, funding, data use, intellectual property, publication rights, and technology transfer should be clearly documented. Reviews should be proportionate to the sensitivity of the research and the partners involved.

3. **Foreign influence and democratic resilience require attention:** CSIS warned that Alberta's October 19 referendum could be targeted through misinformation or disinformation. Canada also brought the Foreign Influence Transparency Registry into force, requiring certain activities conducted on behalf of foreign principals to influence public decision-makers to be publicly registered. Japan's new centralized National Intelligence Bureau reflects similar concern about espionage, cyberattacks, foreign interference, and information sharing.

**What this means:** Activities involving foreign governments or entities, public policy engagement, political decision-makers, or influence-related communications should be assessed for possible disclosure obligations. Guidance, records, and escalation routes should be kept clear, while legitimate international engagement should not be treated as interference without evidence.

4. **Technology controls and mobility are shaping global research:** China introduced tighter controls on exports of drones, components, and related technologies to the United States and sanctioned six U.S.

entities. U.S. student visas issued to Indian and Chinese nationals also declined sharply in 2025, which may affect universities, talent pipelines, and research capacity.

**What this means:** Export controls, sanctions, and visa changes may affect research partnerships, technology transfers, travel, and international recruitment. These changes should be monitored, and additional time should be planned where approvals or access may be delayed.

5. **Personal data can be used for surveillance and targeted operations:** Reporting on China's surveillance of foreigners described the aggregation of camera, facial-recognition, government, and travel data into detailed profiles. A breach involving South Korean diplomats showed how names, emails, roles, and affiliations can support AI-enabled profiling, phishing, social engineering, and influence operations. Separate commentary on Uyghur forced-labour evidence highlighted attempts to discredit the evidence and renewed calls for accountability, stronger import controls, and greater scrutiny of supply chains.

**What this means:** Personal and professional information can become sensitive when combined with other data. Access should be limited; researchers should be prepared for phishing and travel risks, and higher-risk research suppliers should be reviewed.

**Conclusion:** This week's coverage shows the need to balance open research and international collaboration with stronger protection of sensitive technology, data, people, and institutional relationships. Early, proportionate review and clear guidance will help support research while managing emerging security and compliance risks.