



Newsline	Research Security	
Week	March 16 - 20, 2026	
Editor	Alaa Dabboor	Research Security Manager
Reference Package		
	1	Research Security Centre

Executive summary: Recent developments highlight the growing intersection between research, national security, and geopolitical dynamics. Governments are increasing investments in sovereign capabilities and strategic research areas, including space, artificial intelligence, quantum technologies, and nuclear research. At the same time, concerns are emerging around foreign influence, international partnerships, and the protection of sensitive information, including risks related to surveillance, economic dependence, and data aggregation. Regulatory coordination challenges are also becoming apparent as governments work to align innovation with commercialization. These trends reinforce the importance of research security awareness in managing collaborations, technologies, and data.

Key Points:

- Foreign influence and strategic dependence:** Inuit communities may face increasing exposure to foreign surveillance and economic influence linked to Chinese investment proposals in mining, infrastructure, and research collaboration, particularly in the Arctic where local capacity to assess such proposals is limited.

What this means: Foreign investment in strategic regions may introduce risks related to influence, long-term dependency, and access to sensitive resources or information.
- Expansion of research infrastructure and sovereign capabilities:** Canada is investing in sovereign capabilities through a \$200 million space launch facility and \$552 million in research infrastructure, alongside targeted investments in neutron beam research and translational genomics.

What this means: As research infrastructure becomes more strategically valuable, protecting sensitive technologies, data, and facilities becomes increasingly important.
- Advanced research ecosystems and innovation networks:** The University of Waterloo’s Vision and Image Processing Lab highlights Canada’s strength in AI through extensive collaboration across academia, industry, and government, supporting commercialization and applied research.

What this means: Highly collaborative research environments may increase exposure to risks related to intellectual property protection and technology transfer.
- Defence-oriented and dual-use research:** Switzerland is expanding defence-related research in areas such as cyber operations, robotics, autonomy, and space technologies in collaboration with academic institutions.

What this means: Research involving dual-use or defence-related technologies may require increased awareness of security implications and collaboration risks.

- **International collaboration risks:** Partnerships between European universities and Chinese institutions linked to defence research are raising concerns, while countries like New Zealand continue to emphasize the value of international education ties with appropriate safeguards.

What this means: International collaborations may present risks related to foreign interference, unintended knowledge transfer, and access to sensitive research.
- **Strategic technology competition and national initiatives:** The United Kingdom and South Korea are advancing national strategies in quantum and other strategic technologies, while the European Union is investing €330 million through its Euratom programme to strengthen nuclear research.

What this means: Global competition in strategic technologies is increasing the value and sensitivity of research outputs, requiring greater awareness of associated security and economic risks.
- **Policy and regulatory challenges:** The European Commission has delayed its Innovation Act to allow for further coordination, as the proposal aims to address barriers between research, regulation, and market deployment.

What this means: Delays or gaps in regulatory frameworks may create uncertainty in how emerging technologies are governed and deployed.
- **Information exposure and data aggregation risks:** Foreign actors may exploit open information systems, such as Freedom of Information requests, to collect and combine data that reveals sensitive insights related to defence, infrastructure, and research.

What this means: Seemingly low-risk or publicly available information may be aggregated to expose sensitive insights, highlighting indirect data disclosure risks.
- **Declining academic freedom:** Academic freedom has declined in multiple countries due to political pressure, restrictions on expression, and interference in research and institutional governance.

What this means: Changes in academic freedom may affect research environments, collaboration decisions, and the integrity of research activities.

Conclusion: The global research landscape is increasingly shaped by technological competition, geopolitical dynamics, and evolving national security considerations. While investments in strategic capabilities continue to grow, so do risks related to foreign influence, collaboration, and information security. At the same time, regulatory challenges highlight the complexity of translating innovation into practice. Maintaining strong research security awareness remains essential to supporting open, responsible, and secure research.