Newsline	Research Security		
Week	Jan. 5- 9, 2026		
Editor	Alaa Dabboor	**Position**	Research Security Manager
Reference Package			
1	Research Security Centre		

Executive summary: Research, commercial value, and national security are increasingly intertwined. Accelerating investment in quantum and defence-aligned research, combined with structured foreign funding and persistent cyber-espionage, heightens the risk of IP loss and undue influence for universities. Immediate focus is required on dual-use risk triage, foreign funding vetting, and baseline cyber protections for sensitive research.

Key Points:

- **Major funding accelerates Canadian quantum and dual-use research:** Vancouver-based Photonic announced a C$180 million first closing to commercialize an entanglement-based quantum platform, positioning itself as an anchor for Canada's quantum sector and planning further fundraising and expansion. At the same time, increased federal defence spending is prompting expanded university work on drone applications, Arctic sensors, and other dual-use technologies in partnership with defence programs and industry. These developments increase both opportunity and exposure for academic intellectual property and personnel.

  What this means: High-value dual-use projects should be treated as top priorities for research security triage. We should require formal risk assessments and export-control reviews before accepting foreign partners or sharing sensitive data. Need-to-know access controls and network segmentation should be enforced for sensitive labs and datasets. Research Security should be notified early of defence-aligned or Department of National Defence (Canada)-linked awards to enable coordinated mitigation.
- **NSERC moves to retain intellectual property domestically (valorisation model):** NSERC signed a memorandum of understanding with Quebec's Axelys to align funding and commercialization activity with domestic economic benefit. Inspired by Quebec's valorisation approach, the initiative aims to reduce "IP philanthropy" and ensure research outputs are intentionally assessed and retained for long-term Canadian benefit.

  What this means: Technology transfer and legal offices should provide concise guidance on IP classification, patenting strategy, and export implications. Research offices should identify proposals with potential national economic impact at intake and route them through early commercialization and compliance pathways to align with evolving funder expectations.
- **Structured foreign funding under scrutiny:** Recent reporting highlights very large state donors to universities abroad and continued state-supported recruitment initiatives that channel funding and talent into higher education institutions. While such partnerships are often defended as legitimate,

they can create dependency, reputational risk, and contractual leverage that may affect institutional autonomy.

What this means: We should require full disclosure, legal clause review, and conflict-of-interest screening for large or recurring foreign gifts and contracts. State-linked or structured funding above established institutional thresholds should be escalated to Research Security and Legal for coordinated vetting. Agreements must preserve academic freedom and publication rights.

- **Germany to launch a national research security platform:** Germany plans to establish a National Platform for Research Security to centralize rapid risk assessments of international collaborations and sensitive projects. Planning begins in January 2026, with a launch targeted for autumn 2026. This reflects a broader international shift toward formalized research security governance.

  What this means: This development reinforces the need for standardized risk-assessment tools and centralized advisory services at the institutional level. We should ensure researchers have access to clear consultation pathways when navigating complex international partnerships.
- **APT cyber-espionage campaign again targets universities:** A Pakistan-linked group, APT36, has launched a cyber-espionage campaign using spear-phishing emails with ZIP archives disguised as PDFs. The malware enables persistent access, surveillance, and data exfiltration and has targeted universities and government entities across multiple countries.

  What this means: Mandatory multi-factor authentication, least-privilege administration, and targeted phishing awareness training should be enforced for research groups handling sensitive data. Institutions should prioritize monitoring for archive-based malware vectors and require rapid incident reporting to limit dwell time in the event of compromise.
- **Shifts in multinational research engagement and legal risk to individual researchers:** Executive actions in some jurisdictions have directed withdrawal from international research and technology organizations, creating uncertainty for long-standing data-sharing and collaboration frameworks. Separately, the use of foreign-agent laws and espionage allegations abroad illustrates growing personal legal risk for researchers engaged in international work, as demonstrated by the recent detention and exchange of a foreign researcher in Russia.

  What this means: Researchers should review existing collaboration agreements and data-sharing obligations with Research Security and Legal to assess continuity and compliance. Travel and partnership guidance should explicitly address personal legal risk and mitigation strategies for international engagement.

Conclusion: This week confirms we must manage openness deliberately: growing strategic investment increases both opportunity and exposure. Our priority actions are to embed security triage at project intake for dual-use, defence-aligned, and high-value work; require disclosure and legal review for large or state-linked foreign funding; and enforce baseline cyber and operational safeguards (MFA, least privilege, segmentation, and rapid incident reporting). Taken together, these steps help us continue global collaboration while protecting researchers, IP, and institutional reputation.