University of Regina

Newsline	Research Security		
Week	Oct. 14-Oct. 17, 2025		
Editor	Alaa Dabboor	**Position**	Research Security Manager
Resource Package			
1	Research Security Centre		

Executive summary: This week's Newsline highlights rapid defense-tech investment in Arctic surveillance, a federal AI funding boost for Manitoba, a major research-integrity fabrication case at UBC, increasing cyber threats affecting research networks, and several international policy moves that could affect collaborations and export-control posture.

Key Points:

- Dominion Dynamics raised $4M pre-seed to develop an Arctic sensor mesh; dual-use sensor technology may trigger export-control and procurement reviews.
- Federal $2.3M investment to expand AI adoption and upskilling in Manitoba; raises data governance and bioscience AI adoption questions.
- A UBC researcher was found to have fabricated clinical-trial data in the Meshfill study; the case exposed gaps in disclosure and oversight and warrants a review of trial audit trails and reporting policies.
- Hydro-Quebec espionage-trial developments: a former employee was charged under the Security Information Act over unauthorized battery/energy publications, underscoring the need for robust IP and publication-authorization controls.
- Canada ranked third globally for malware infections (Jan 2024–Jul 2025): phishing and malicious file vectors remain high; research networks are exposed.
- Drop in francophone Quebec international student enrolment; potential medium-term impact on research funding and graduate talent pipelines.
- Simon Fraser University's advances in silicon spin qubits and plans for a national quantum institute accelerate national quantum capability and introduce heightened collaboration, IP, and security risks; recommend reviewing partnership vetting, IP clauses, and data-sharing controls.
- Recent international cyber and policy developments include the Jewelbug supply-chain intrusion attributed to a Chinese state actor, a U.S. Espionage Act charge involving the retention of classified documents, and emerging national rules on AI and biotech funding. These trends highlight cross-border supply chain and regulatory risks and warrant updates to vendor-risk assessments and research-compliance guidance.

- Other notable risks: national security takeover of chipmaker (Nexperia), unencrypted satellite traffic findings, and MI5 (United Kingdom's Security Service) foreign-espionage guidance for Members of Parliament; all relevant to procurement, data handling, and visitor vetting.

Conclusion: All in all, this week's items indicate rising operational and strategic risks across data governance, export controls, insider disclosure, and cyber hygiene; Mitigation measures to be enhanced and prioritized.