University of Regina

Newsline	Research Security		
Week	Oct. 20-Oct. 24, 2025		
Editor	Alaa Dabboor	**Position**	Research Security Manager
Resource Package			
1	Research Security Centre		

Executive summary: Canadian research faces simultaneous opportunity and risk: significant federal funding opens space for infrastructure and cybersecurity investment, but it raises compliance expectations. This occurs within an aggressive international threat environment, including state-level cyber-attacks and tightly contested strategic technologies. Rapid technology shifts, especially AI, are amplifying cyber and misinformation threats, while ocean and Arctic research and critical-tech collaborations present dual-use, supply-chain, and foreign-ownership vulnerabilities. Priorities are clear: strengthen baseline cyber hygiene and AI-aware training; audit and protect dual-use datasets; and tighten procurement, vendor due diligence, and publication-integrity processes.

Key Points:

- **Federal investment package:** More than $690M announced to strengthen research capacity (Research Support Fund, Canada Research Chairs, infrastructure and cybersecurity priorities).
- **Ocean science vulnerability:** Review warns marine datasets and technologies are dual-use and currently lack tailored research-security safeguards.
- **AI-enabled cybercrime:** AI is scaling and personalizing phishing, producing deepfakes, and automating attacker workflows, increasing risk to researchers and administrative staff.
- **Arctic detection gaps:** Small drones and low-altitude UAVs expose surveillance blind spots in the Arctic, and foreign vessels could gather sensitive data clandestinely.
- **Scholarly integrity threat:** Investigations reveal commercial “paper mills” and fabricated identities; publishers are tightening identity and authorship verification.
- **China accuses U.S. of cyberattack:** China accuses the U.S. NSA of hacking its National Time Service Center, claiming the 2022-2024 attacks targeted critical infrastructure. It alleges the NSA exploited mobile messaging vulnerabilities and used dozens of cyber tools, but no evidence. The U.S. rebutted by pointing to China’s own cyber threats.
- **A U.S. court sets a precedent against Israeli-Made Spyware:** A U.S. judge issued a court order prohibiting Israeli firm, NSO Group, from targeting WhatsApp users, finding its

Pegasus spyware used missed-call and zero-click exploits and caused “irreparable harm” to Meta. The court reduced damages from $168 million to $4 million.

- **Quantum and geopolitical funding:** U.S. moves to bolster quantum capabilities highlight strategic competition and likely tighter export and IP controls affecting partnerships.
- **AI chatbots and misinformation:** High error rates in AI-generated news and content mean outputs must be cross-checked against primary sources before use.
- **Supply-chain and ownership tension (Nexperia):** Disputes over foreign ownership and regulatory oversight in semiconductor supply chains underscore procurement and collaboration risks.

Conclusion: Federal funding creates openings for infrastructure and cybersecurity upgrades, but rising AI-enabled threats, dual-use risks in marine and Arctic research, and integrity and procurement challenges demand immediate, coordinated action: strengthen cyber hygiene and AI-aware training, secure dual-use datasets, and tighten procurement and publication-integrity controls to protect research and preserve funding access.