University of Regina

Newsline	Research Security		
Week	Nov. 10 -Nov. 14, 2025		
Editor	Alaa Dabboor	**Position**	Research Security Manager
Resource Package			
1	Research Security Centre		

Executive Summary: This week's Newsline shows growing research-security pressure worldwide and at home: increased espionage and influence activity (notably in Canada's Arctic and on campuses), shifting international partnerships and U.S. funding cuts under the Trump administration, and rising supply-chain and dual-use technology concerns (AI models, telecoms, equipment). High-profile legal and policy items (criminal cases, parliamentary inquiries, EU/UK moves on China) reinforce the need for earlier, clearer security gating (STRAC/RAF) and stronger post-award monitoring.

Key Points:

- **Rising espionage in Canada's Arctic:** CSIS reports increased spying and influence activity (recruitment, data access, interference) in the North. **What this means**: Arctic-related research and partnerships should be treated as high-sensitivity and routed for early review.
- **Multiple-state threat landscape:** Russia, China, Iran, and India present varied risks (espionage, transnational repression, influence). **What this means**: Risk assessments must consider multiple threat vectors, personnel vulnerabilities, and partner/supplier exposure.
- **U.S. funding cuts under Trump disrupt Canada–U.S. science ties:** National Oceanic and Atmospheric Administration (NOAA), National Aeronautics and Space Administration (NASA), and National Institutes of Health (NIH) reductions have paused long-running collaborations and data streams (e.g., Great Lakes, atmospheric projects). **What this means**: Canadian teams may need new funders or partners—an opportunity that also brings risk if replacements are less vetted or disrupt data continuity.
- **Targeted tech partnerships and recruitment:** Canada's quantum deals and university hiring drives boost capacity but raise export-control, IP, and onboarding issues. **What this means**: Screen partnerships early for export-control exposure and contractual safeguards.
- **Pressure on academic freedom from incentives:** Funding and reporting demands can narrow basic research and shape what gets funded.

What this means: Design security processes that protect national interests without unduly restricting legitimate academic inquiry.

- **Criminal and procurement risks are real:** Cases of material smuggling and concerns about foreign-made equipment reveal operational vulnerabilities.
  What this means: Strengthen lab controls, material transfer oversight, and vendor due diligence to reduce accidental or illicit transfers.
- **EU/UK moves to limit China in sensitive areas:** Policymakers are excluding or narrowing Chinese participation in high-risk research (civil security, health, digital/space).
  What this means: Canadian institutions should proactively review collaborations in sensitive domains to avoid sudden policy shocks.
- **AI and supply-chain vulnerabilities:** Adoption of low-cost foreign AI models and remote-accessible hardware raises data-access and control risks.
  What this means: Enforce provenance checks, cybersecurity reviews, and procurement vetting for AI, cloud services, and hardware.
- **Rising public and political scrutiny of universities:** Inquiries, media coverage, and protests increase pressure on governance and compliance.
  What this means: Maintain clear records, transparent decision trails, and robust compliance to respond quickly to scrutiny.
- **Trend to earlier screening and monitoring:** Coverage favors STRAC/RAF attestation at intake, structured triage (internal committee to PSC), and conditional monitoring for funded projects.
  What this means: Make STRAC/RAF mandatory at intake, tag high-sensitivity projects for immediate review, and require mitigation plans and monitoring.

Conclusion: This week's developments make clear that research security must be proactive and systematic: implement STRAC/RAF gating at application intake, automatically flag high-sensitivity proposals (Arctic, dual-use tech, foreign partnerships), and document fast, auditable triage paths to internal committees and Public Safety Canada. Strengthen procurement and laboratory controls, require mitigation plans for conditional funding, and prepare for increased public and governmental scrutiny. These steps preserve academic collaboration and innovation while reducing the real, growing risks to national security and research integrity.