Newsline	Research Security		
Week	Jan. 12 - 16, 2026		
Editor	Alaa Dabboor	**Position**	Research Security Manager
Reference Package			
1	Research Security Centre		

Executive summary: This week's coverage reflects an intensifying focus on research security as governments, universities, and industry respond to geopolitical competition. In Canada, attention is growing on sovereign capabilities in defence, nuclear, and microelectronics, while allied countries continue to confront espionage and insider-threat cases. At the same time, implementation challenges and policy spillovers, such as visa reclassifications and UK Academic Technology Approval Schema (ATAS) delays, show how fragmented approaches can create new risks. The key takeaway remains that investment in research capability must be matched with practical, proportionate, and internationally aligned risk management.

Key Points:

- **Defence tech startup with Arctic focus:** Former Defence Minister Harjit Sajjan co-founded Juno Industries, a Vancouver startup developing autonomous systems software for high-risk environments (notably the Arctic). The company has operated in stealth since April 2025 and recently closed a $3M seed round.
  What this means: Strengthening domestic defence tech pipelines reduces reliance on external suppliers and can improve control over sensitive IP and personnel. However, rapid scaling of dual-use startups also requires early security-by-design, export-control awareness, and screening of partnerships to avoid inadvertent technology diffusion.
- **Espionage and insider threats targeting defence research:** A former U.S. Navy sailor received a lengthy sentence for selling ship-system manuals and data to a foreign intelligence officer; Sweden detained a former military IT consultant on spying suspicions; France charged a researcher alleged to have enabled unauthorized access to a secure lab.
  What this means: These are reminders that personnel with access to operational or dual-use data are high value to state actors. The university must prioritize continuous vetting, clear reporting channels, insider-threat awareness training, and technical controls (least privilege, logging, secure collaboration tools).
- **UK ATAS delays expose implementation risk in researcher screening:** MPs report ATAS clearance waits stretching to six months (vs. 28-day target), disrupting legitimate research and livelihoods.
  What this means: Security filters can backfire if they are under-resourced or vague. Long delays harm trust and can push collaborations into ad-hoc or less secure arrangements. Efficient processing, transparency, and escalation mechanisms are essential to retain both security and international research excellence.

- **Commentary: are we shifting risk rather than reducing it?** Analysis argues that uneven national rules create a "waterbed effect" that pushes activity and threats toward more permissive partners, often straining Global South institutions.

  What this means: Fragmented policy increases systemic risk and inequity. Sustainable research security requires harmonized standards, capacity building for partner institutions, and mechanisms for shared responsibility.
- **Australia tightens student visa checks for four countries:** Australia reclassified India, Nepal, Bangladesh, and Bhutan to Evidence Level 3, its highest risk category, effective January 8, 2026. The change increases documentary, financial, and language requirements and is expected to extend processing timelines.

  What this means: The student mobility pipeline is now an explicit risk vector in some jurisdictions. Risk-based immigration measures can help protect integrity, but they also risk reducing legitimate mobility and research capacity unless accompanied by clear criteria, appeals processes, and outreach to affected communities.
- **State-linked cyber-operations target energy, defence and research collaborations (APT28):** APT28 credential-harvesting campaigns targeted energy research, defence collaboration entities and think tanks across multiple countries using realistic phishing pages and free hosting services to obfuscate operations.

  What this means: Technical controls (multifactor auth, phishing resistant keys, domain monitoring), threat-intelligence sharing, and hardening of research collaboration platforms are urgent priorities, particularly for teams working in critical energy and defence Research and Development (R&D).
- **National research ecosystem stories worth noting (concise):**
  - **McMaster and nuclear capacity:** McMaster expanding reactor operations, training and isotope production, signals growth in nuclear R&D and the need for enhanced lab security and export-control processes.
  - **Waterloo IP model:** University of Waterloo's researcher-centric IP approach is influencing commercialization policy internationally, relevant for how institutions balance openness with IP protection.
  - **Quebec microelectronics value chain (PRIMA Quebec):** Report highlights critical materials and strategic niches, securing supply chains and protecting sensitive know-how will be important.
  - **Australia defence research funding:** A $20M to universities for defence R&D shows growing state-university collaboration in sensitive tech areas.

Conclusion: This week's reporting underscores a central tension in global research security. As governments expand sovereign capabilities in sensitive sectors, espionage, cyber threats, and implementation gaps persist. Practitioners must strengthen internal controls while advancing internationally aligned approaches that prevent risk displacement. Balancing domestic safeguards with cooperative global standards remains essential to a secure and open research ecosystem.