University of Regina

Newsline	Research Security		
Week	Dec. 8-12, 2025		
Editor	Alaa Dabboor	**Position**	Research Security Manager
Reference Package			
1	Research Security Centre		

Executive summary: This week highlights Canada’s push to attract global research talent and strengthen trusted tech partnerships amid rising research security threats. Ottawa launched a $1.7B Canada Global Impact+ Research Talent Initiative to recruit over 1,000 international and expatriate researchers, including Francophones, and concluded G7 agreements, notably the Canada–Germany Digital Alliance, to align AI, quantum, and digital standards. Internationally, state driven espionage, export control circumvention, and ethical concerns over Chinese surveillance linked AI collaborations emphasize the need for robust research security and human rights due diligence in recruitment, funding, and partnerships.

Key Points:

- **Canada launches major global research talent initiative:** The Government of Canada announced the $1.7 billion Canada Global Impact+ Research Talent Initiative. It has four streams: $1.0B for Impact+ Research Chairs (salaries and infrastructure), $120M for Emerging Leaders, $400M for infrastructure, and $133.6M for doctoral and postdoctoral training awards. The program targets rapid, flexible recruitment of more than 1,000 leading international and expatriate researchers, explicitly including Francophone candidates.

  What this means: The scale and speed boost Canada’s competitiveness but create research security pressure. Institutions must scale proportionate, timely security screening and onboarding controls so rapid hiring does not exceed protective measures.
- **Canada deepens digital and tech alliances at G7 meeting:** Canada signed Memoranda of Understanding with the EU, UK and Germany to deepen cooperation on AI regulation, quantum technology, digital sovereignty and secure public digital systems. The Canada–Germany Digital Alliance includes AI strategy alignment, a joint quantum commercialization funding call planned for January 2026, and cooperation on large language models and generative AI.

  What this means: These agreements build shared standards and trusted supply networks, reducing single point dependencies. Harmonized approaches to responsible AI, secure procurement, and interoperable credentials strengthen collective research security.
- **Former CSIS chief warns of “industrial-scale” espionage targeting academia:** Former CSIS director David Vigneault warned that hostile states, prominently China, are conducting industrial-scale efforts to acquire advanced technology via universities and private sector research using cyber intrusions, agent recruitment and covert influence tactics. He urged mandatory security reviews for sensitive programs and closer academia security agency cooperation, while cautioning against racial profiling.

What this means: The warning confirms persistent, sophisticated threats to open research ecosystems. Universities and funders should adopt risk proportionate mandatory reviews for dual use or defence relevant projects, strengthen threat awareness training, and formalize rapid liaison channels with security partners.

- **Export control breaches and smuggling schemes expose supply chain vulnerabilities:** The U.S. Justice Department charged individuals alleged to have conspired to smuggle about $160M in advanced Nvidia H100 and H200 chips to China. Separately, reporting found that ASML (a Dutch multinational and a key player in the global semiconductor supply chain) supplied sensitive chip making components in 2024 to Chinese institutes, including a military research arm and a quantum research academy, revealing gaps in export controls and screening.

  What this means: Actors exploit legal and logistical loopholes to move foundational technologies. Research security needs tighter export control compliance at universities and industry partners, stronger supplier due diligence, and rapid incident reporting to detect diversion.
- **Report alleges Western university links to surveillance linked Chinese AI labs:** The "Shared Labs, Shared Harm" report documents extensive co-authorship and project ties between leading Western universities, including MIT, Oxford and McGill, and Chinese labs tied to surveillance systems. Many collaborations received U.S. agency funding and produced work on facial recognition, tracking and biometric imaging.

  What this means: Ethical and human rights risks must be part of due diligence. Funders and institutions should require collaborator transparency, human rights risk assessments for surveillance relevant projects, and oversight of co-authorship and data sharing.
- **Ukraine offers dual use military technology cooperation:** Ukraine signaled willingness to share or co-produce drones and other military technologies with Canada. Reporting highlights Ukraine's high volume drone production and ongoing defence cooperation, aligning with Canada's goal to diversify defence supply chains while the U.S. remains the dominant supplier.

  What this means: Access to combat tested dual use innovations could speed up capability development, but collaborations must include strict IP safeguards, aligned export controls and lifecycle risk management to prevent technology leakage.

Conclusion: This week highlights the tradeoff between advancing investment and partnerships to secure talent and technology and managing persistent threats to research openness. Key steps include timely risk reviews, stronger export control and supplier due diligence, human rights assessments in collaborations, and enhanced interagency and international coordination. These transparent, non-discriminatory measures will help Canada and partners safeguard research while preserving collaborative openness.