University of Regina

| | | | |
|---|---|---|---|
| **Newsline** | Research Security | **Week** | March 23 - 27, 2026 |
| **Editor** | Alaa Dabboor | Research Security Manager | |
| **Reference Package** | | | |
| 1 | Research Security Centre | | |

**Executive summary:** Research and national security are increasingly interconnected, with growing investments in defence technologies, cybersecurity, and strategic areas such as AI and quantum. At the same time, risks related to foreign interference, transnational repression, and dual-use research are becoming more prominent. Governments are responding with stronger oversight and policy measures, underscoring the importance of research security awareness in high-impact and collaborative research.

**Key Points:**

- **Expansion of defence technology and digital sovereignty initiatives:** Canadian defence startups are collaborating to develop AI-enabled military technologies using Canadian-controlled cloud infrastructure, including drone evaluation, intelligence fusion, and cybersecurity systems tailored to Arctic and long-range defence, while emphasizing digital sovereignty.
  **What this means:** Development of defence-related and AI-enabled technologies reinforces the importance of safeguarding sensitive research, infrastructure, and data within secure and trusted environments.
- **Strengthening secure international research collaboration:** Canada and Norway have renewed collaboration across Arctic science, climate and marine research, artificial intelligence, and quantum technologies, including research security coordination, Indigenous Knowledge integration, increased researcher mobility, and participation in programs such as Horizon Europe and Eureka.
  **What this means:** International partnerships in strategically sensitive areas may require alignment on shared research security risks, including governance, data use, and collaboration structures.
- **Investment in research infrastructure and innovation ecosystems:** Canada is advancing research capacity through investments such as a $3.6 million cybersecurity laboratory at Universite du Quebec en Outaouais, a UBC spinout fund (targeting up to $40 million), and a national biofilm research centre, alongside international funding increases (e.g., Scotland's 8% uplift) supporting institutional stability and innovation.
  **What this means:** Expanded research infrastructure and commercialization pathways may increase the strategic value of research outputs and the importance of protecting intellectual property and sensitive technologies.
- **Rising foreign interference and repression risks:** Risks of transnational and digital repression in Canada are increasing, including surveillance and harassment targeting diaspora communities, with AI and geopolitical dynamics expected to further enable these activities.
  **What this means:** Foreign interference risks may extend into research environments, particularly in sensitive topics, international collaborations, or diaspora engagement.

- **Increasing oversight of foreign influence in research:** In the United States, congressional attention to foreign interference has led to strengthened oversight of international partnerships, laboratory materials, and institutional safeguards, reflecting efforts to balance research openness with national security.
  **What this means:** Research environments may face increasing expectations for transparency, due diligence, and oversight in international collaboration.
- **Strategic technology competition and policy responses:** Global research systems are aligning around advanced technologies such as quantum computing, artificial intelligence, and cybersecurity. Initiatives like Horizon Europe are expanding participation while raising considerations around access to sensitive research and future program direction. In parallel, governments are introducing policy responses, including the U.S. Bureau of Emerging Threats, to address risks across cyber, AI, quantum, and space domains.
  **What this means:** Strategic technology development and evolving policy frameworks may increase research sensitivity and shape expectations for managing risks in international and dual-use contexts.
- **Dual-use research, supply chain risks, and scientific activity:** Some scientific activities, including deep-sea research, may have dual-use implications linked to military or intelligence objectives, with reported operational patterns such as activity beyond declared zones and tracking disruptions. At the same time, restrictions on foreign-made routers highlight broader concerns about vulnerabilities in technology supply chains and digital infrastructure.
  **What this means:** Research in strategic domains and reliance on global technology supply chains may introduce dual-use and security risks, requiring awareness and due diligence across partnerships, infrastructure, and data environments.
- **Researcher exposure and global security risks:** Researchers studying sensitive topics face increasing online harassment and digital targeting, underscoring the importance of institutional support and proactive risk awareness. Concurrently, international initiatives, including a NATO-supported hub linking Euro-Atlantic and Indo-Pacific partners, highlight growing attention to hybrid threats such as cyberattacks, disinformation, and transregional challenges.
  **What this means:** Research security is increasingly shaped by cross-border threats and researcher exposure risks, reinforcing the need for coordinated institutional and individual awareness.

**Conclusion:** The research environment is evolving alongside technological competition and geopolitical shifts, with growing investments and increasing risks related to foreign interference, dual-use research, and cybersecurity. As oversight and policy responses expand, maintaining awareness of research security considerations remains essential to support open, responsible, and resilient research practices.