



Newsline	Research Security	Week	September 28 - Oct 2, 2026
Editor	Alaa Dabboor	Research Security Manager	
	Research Security Centre (Public Safety Canada)		

Executive summary: This week's coverage looks at cyber threats targeting researchers, foreign-funded collaborations, dual-use technologies, and AI use in research assessment. It also covers international investment, restrictions on researcher travel, funding dependence, academic freedom, and damage to research institutions during war.

Key Points:

1. **Cyber threats and targeted approaches to researchers:** Translucence reported unsuccessful attempts by autonomous AI agents to access the Library and Archives Canada website in May and June 2026. Responsibility could not be confidently attributed, and the Canadian Centre for Cyber Security reported no evidence that government systems were compromised. Separately, a Chinese-linked group allegedly impersonated U.S. AI experts and former officials through collaboration invitations that led to credential-stealing websites. The campaign targeted fewer than 10 people working on AI policy, export controls, and national strategy, suggesting a focused intelligence-gathering effort. ShinyHunters also claimed it stole sensitive personal and employment records from the FBI's employment portal. Experts warned that stolen data could be sold or exploited even without being publicly released.

What this means: Researchers should verify unexpected collaboration invitations before opening links, signing in, or sharing information. Targeted approaches may seek access to policy discussions and professional networks as well as research.

2. **Foreign-funded collaborations and researcher mobility:** MI5 urged UK universities to end ties with the China General Technology Research Institute, alleging that it is a front for China's Ministry of State Security. It reported that more than 100 UK-linked academics had worked on projects involving AI, cybersecurity, covert communications, and techniques for hiding information. MI5 warned of possible legal consequences under UK legislation; China rejected the allegations. Another report described travel restrictions requiring some Chinese AI and semiconductor researchers, executives, and their immediate families to obtain approval before travelling abroad. Observers warned that these controls could discourage talent retention and international collaboration.

What this means: When reviewing partners, it is important to check who funds them, who they are connected to, and how they may use the research. Travel restrictions can also affect visits and project schedules.

3. **Dual-use research, investment, and national technology priorities:** University of Alberta researchers are helping Sentinel Advanced Military Solutions develop a containerized drone factory for remote locations, including the Arctic. The system could manufacture, repair, and deploy drones, with civilian uses such as emergency response and communications. Draganfly received \$10 U.S. million from Unusual Machines, backed by Donald Trump Jr., and an unnamed U.S. asset management firm. The report also noted scrutiny of potential conflicts of interest involving Trump family defence investments.

European research ministers called for civilian and defence applications to be considered in the next Horizon Europe programme. Japan plans to recruit overseas dual-use technology specialists to support partnerships and investment. India is preparing a \$25 U.S. billion deep-tech initiative amid concerns about foreign technology dependence, export controls, and supply chains. Xi Jinping encouraged Chinese universities to support national innovation priorities through interdisciplinary research. In Quebec, Fonds de solidarité FTQ and France's AdBio Partners are supporting biotechnology growth through a new 120-million EUR fund and a Montreal office.

What this means: These developments bring opportunities for research and investment, alongside questions about end use, technology transfer, and partner interests. Civilian research may also have defence or strategic applications.

4. **AI screening and confidential research information:** Crane, a UK cybersecurity research network, defended its use of multiple AI models to screen grant applications after researchers raised privacy and confidentiality concerns. Roughly half of the applications were rejected at the initial stage. The network said its AI services were securely ring-fenced, confidentiality was protected, and final funding decisions involved human assessment. A separate opinion article focused on AI's current social effects, including surveillance and information control by authoritarian governments, automation, misinformation, and social fragmentation.

What this means: Using AI with proposals or unpublished research raises questions about both confidentiality and assessment. Researchers should understand how their information is handled and where human review takes place.

5. **Funding dependence, academic freedom, and research continuity:** Following major U.S. funding cuts in 2025, South Africa released a report calling for stronger domestic research investment. It proposed a sovereign risk advisory council and innovation fund, with attention to protecting health and biotechnology research. A study discussed in the Newsline argues that decades of influence from fossil fuel companies, conservative think tanks, and donor networks weakened U.S. university autonomy and helped enable the Trump administration's research funding cuts and investigations into academic institutions. The authors warned about self-censorship and called for greater transparency and safeguards against external influence.

In Ukraine, a Russian drone strike severely damaged the National Academy of Sciences headquarters and killed at least two people. The academy contributes to civilian and defence research, including drones, AI, materials science, and medicine. The attack adds to the damage sustained by Ukrainian universities and scientific institutions since 2022.

What this means: Funding changes, external pressure, and damage to facilities can affect research independence and continuity. Transparent funding relationships and planning for disruptions remain important.

Conclusion: This week's reports show how research security concerns can arise through collaboration invitations, funding relationships, technology development, and everyday use of AI. Early review of these issues can help protect research information and support informed collaboration.