University of Regina

Newsline	Research Security	**Week**	September 7 - 11, 2026
Editor	Alaa Dabboor	Research Security Manager	
	Research Security Centre (Public Safety Canada)		

Executive summary: This week's news covers AI security, cyberespionage, sensitive technologies, intellectual property (IP), and international research collaboration. Several developments also show more attention to AI, quantum, semiconductors, defence, biotechnology, and other technologies that may have national or economic security importance.

Key Points:

1. **AI security and misuse:** Google reported that Chinese-linked cyber actors are using AI in cyberespionage activities. One group targeted academic, medical, and military research organizations in North America, with interest in proprietary AI research. Attackers were also seen running open-source AI models on compromised cloud systems to avoid safeguards used by commercial AI platforms. Anthropic also reported misuse of Claude by criminal and state-linked actors for cyberattacks, surveillance, propaganda, weapons development, and potentially dual-use biological research.

   University of Toronto researcher Nicolas Papernot called for independent testing of powerful AI models. His research showed how publicly available AI tools could be used to create a self-adapting computer worm. He sees universities as a possible bridge for independently testing these systems. Current and former Anthropic employees also raised concerns about AI safety. Anthropic's alignment science lead said he believes there is more than a 10% chance AI could cause human extinction within the next decade.

   What this means: AI research can itself be a target, while AI tools can also be used to support cyber activities. Independent testing, cybersecurity, and appropriate controls should be considered when working with powerful AI systems.
2. **Sensitive technology and IP:** Belgian authorities are investigating alleged Chinese-linked industrial espionage involving BelGaN, a semiconductor company working with gallium nitride chips used in electric vehicles, aerospace, and military applications. A former senior researcher is suspected of transferring IP and trade secrets to a Chinese company. He denies the allegations.

   The CIA deputy director said U.S. intelligence collection concerning China is expanding into areas such as AI, semiconductors, and biotechnology. He also raised concerns about acquisition of advanced technologies and cyber threats to critical infrastructure. In Canada, RBC launched a C$1.4-billion fund for Canadian technology companies in areas including AI, cybersecurity, quantum, aerospace, health technology, energy, and agriculture. One objective is to help these companies grow while remaining headquartered in Canada.

   What this means: Research results, IP, and sensitive technologies can have value beyond their original research purpose. Their protection should be considered when working with external partners or moving toward commercialization.
3. **International research collaboration:** Australia terminated two university collaborations involving the Australian National University and Shandong University, and the University of Queensland and Chinese Academy of Sciences. Officials cited the protection of sensitive research and sovereign capabilities. The decisions also created debate about the impact of security measures on international scientific collaboration.

   Ireland published its first national Research Security Guidelines. They focus on protecting sensitive knowledge, data, and IP while keeping research open and international. Lithuania also revoked the residence permits of 22

Belarusian technology workers connected to a company involved in an EU-funded space project. The company allegedly received nearly €500,000 while concealing links to Russian and Belarusian military industries. The workers were expelled and banned from Lithuania and the Schengen Area for five years.

What this means: International collaboration should remain open where possible, but the organization, individuals, affiliations, access, and type of research may need additional review when concerns are identified.

4. **Defence and strategic technologies:** Canada was the lead nation at the MSPO, International Defence Industry Exhibition in Poland, with more than 230 Canadian companies and organizations participating. The effort is part of Canada's move to diversify beyond reliance on the U.S. Through the Security Action for Europe initiative, Canadian firms can also access European defence contracts in areas such as drones, military vehicles, and defence technologies.

   The European Commission launched a Security Research and Innovation Campus covering space and quantum technologies, border management, crisis management, defence, internal security, and nuclear security. South Korea and France also agreed to expand cooperation in AI, semiconductors, quantum technologies, nuclear energy, defence, joint R&D, startup cooperation, supply chains, and military cooperation.

   What this means: Research involving sensitive or dual-use technologies may need additional attention to who receives the technology, how it may be used, and what information or IP is being transferred.

5. **Sanctions, trade secrets, and academic mobility:**

   Huawei has gone to trial in the U.S. over allegations related to its business activities in Iran and U.S. sanctions. Prosecutors allege that Skycom was used to conduct transactions through the U.S. financial system and obtain embargoed goods and services. The case also includes allegations of trade-secret theft, money laundering, racketeering, and obstruction. Huawei has pleaded not guilty and denies wrongdoing.

   A University of Ottawa professor also called for Canadian academics to boycott conferences in the U.S. during the current trade dispute. He cited concerns about academic freedom, international mobility, and the use of Canadian public funds, while supporting continued collaboration with U.S. researchers through virtual and international channels.

   What this means: International research activities can also be affected by sanctions, geopolitical issues, academic mobility, and trade-secret concerns.

Conclusion: This week's news shows that research security is not only about international partnerships. AI, cybersecurity, IP, commercialization, personnel, technology transfer, and international travel can also create research security considerations. Most international collaboration is legitimate and beneficial, but additional review may be needed when the research, technology, partner, or access presents a higher risk.