UNIVERSITATEA LUCIAN BLAGA DIN SIBIU

HPI Hasso Plattner Institut
Digital Engineering · Universität Potsdam

CLUJ IT

Sibiu IT Cluster

SID 2025
Sibiu Innovation Days
06 - 07 November, Sibiu - RO

EMERGING DISRUPTIVE TECHNOLOGIES:
Balancing Innovation, Risks, and Societal Impact

Research Security

Prof. Dr. Ing. Razvan Craciunescu

Universitatea Nationala de Stiinta si Tehnologie POLITEHNICA Bucuresti

MINISTERUL EDUCAȚIEI ȘI CERCETĂRII

2025

POLICY RECOMMENDATION ON RESEARCH SECURITY IN ROMANIA

CONCEPT NOTE

uefiscdi UNITATEA EXECUTIVĂ PENTRU FINANȚAREA ÎNVĂȚĂMÂNTULUI SUPERIOR, A CERCETĂRII, DEZVOLTĂRII ȘI INOVĂRII

Contributors:
A. Bahna, O. Buiu, R. Coșcodaru, A. Crăciun, R. Crăciunescu, A. Curaj, A. Dinu, A. Fărcășanu-Răvar, O. Ionescu, M. Mitroi, E. Simion

Acknowledgements to:
British Embassy Bucharest | U.S. Embassy in Romania

28 OCT 2025 - Commission’s first dedicated research security conference in Brussels

New laws on research security are to be included in the forthcoming European Research Area (ERA) Act, according to EU research Commissioner Ekaterina Zaharieva.

This is expected to provide legal backing for measures to protect the EU from risks such as the undesirable transfer of critical technology, malign influence and ethical or integrity violations by foreign countries.

The European Commission had signalled that it might include research security in the Act in a call for evidence published in June, but Zaharieva’s latest statement confirms the move.

Possible measures:
Establishing a European centre for expertise in research security,
creating a platform that helps researchers assess international cooperation risks,
a common methodology for EU member states to test the resilience of their research-performing organisations.

https://sciencebusiness.net/news/european-research-area/eu-embed-research-security-law

Why Research Security Matters

International and European Context

Growing **geopolitical tensions** and **competition in high-tech sectors**

Rising risks of foreign interference, cyber threats, and dual-use misuse

Pressure on universities and RDI institutes to **remain open for cooperation** in the context of talents’ mobility, while protecting knowledge, research outputs, and use of critical infrastructure

Alignment with **EU Council Recommendation (2024), G7 Best Practices, OECD policy recommendations, FP10 priorities and broader international practice**

Research security Scope:

Protecting intellectual property (inventions, data, methods) and sensitive information, maintaining research integrity, and preventing misuse of research outcomes (e.g. preventing civilian research from aiding weapons or criminal activities).

Preserves the benefits of innovation for those who created it and maintains trust in science.

Robust research security discourages bad-faith actors from exploiting research for harmful purposes, helping ensure research advances are used responsibly.

Cyber:
Research institutions face hacking, malware, and espionage attempts targeting their networks and data. Hackers have launched cyber-attacks on labs, databases, and intellectual property repositories to steal sensitive research (e.g. biomedical or aerospace data).

Intellectual Property:
Theft of proprietary research findings and technology for economic or military gain. This can occur through cyber intrusions or insider misappropriation, and it undermines the competitive edge of universities and industries.

Insider:
Trusted insiders (researchers or staff) with malicious intent or undisclosed foreign ties may leak or steal research. Cases have occurred of academics funneling federally funded research to foreign adversaries, highlighting the need for background checks and conflict-of-interest disclosures.

Foreign Interference & Espionage:

Foreign governments or their proxies seek to influence research or obtain data. Tactics include recruiting academics, setting up partnerships or institutes as fronts, and providing funding with strings attached. Such interference can distort research agendas and has led to reputational damage for institutions. In extreme cases it may even threaten campus safety or researchers' independence.

Dual-Use Research Risks:

Research intended for civilian benefit that can be repurposed for harmful uses. Examples include advanced biotechnology, AI, or aerospace research that could be diverted to military or malicious applications. These dual-use technologies require careful oversight. Clear criteria and export control compliance are needed to prevent scientific knowledge from contributing to weapons, surveillance, etc.

Institutional Policies & Protocols:

Develop clear research security guidelines at universities and labs. Establish internal protocols to safeguard sensitive data and technology, especially in high-risk fields (defense, AI, biotech, etc.). Formal policies set expectations for secure data handling, information classification, and visitor or collaboration vetting.

Risk Assessment & Due Diligence:

Integrate security risk checks into research workflows. Before entering international partnerships or projects, conduct thorough due diligence on partners and funders. Require researchers to disclose conflicts of interest and affiliations, and screen for potential foreign interference risks. Funding agencies and grant review processes should include security risk assessments to flag vulnerabilities early.

Cybersecurity

Strengthen IT security for research. This includes access controls, encryption of sensitive research data, and incident response plans. Regular audits and threat monitoring help safeguard digital research assets from cyber-espionage.

Training & Awareness

Provide regular research security training for faculty, students, and staff. Build a culture through workshops on topics like export controls, data protection, social engineering awareness, and ethical conduct in research. An informed research community is better equipped to recognize suspicious approaches and adhere to protocols, thereby reducing human-factor vulnerabilities.

United States

The National Security Presidential Memorandum-33 (NSPM-33) mandates that institutions receiving federal research funds implement research security programs covering areas like cybersecurity, researcher training, foreign travel security, and export control compliance.
Agencies like NSF back this up by requiring disclosures of foreign ties and annual science security training for researchers and staff.

Canada

Follows an “as open as possible, as secure as necessary” philosophy. The government introduced National Security Guidelines for Research Partnerships to embed national security considerations into the evaluation and funding of research collaborations.
Starting in 2024, Canada’s Policy on Sensitive Technology Research and Affiliations of Concern requires that any research grant involving sensitive technologies ensure no participants have affiliations with foreign military or security entities of concern.
To help researchers comply, Canada published clear lists of sensitive research areas and high-risk foreign institutions.

United Kingdom

The Research Collaboration Advice Team (RCAT), a government-academia partnership, offers universities confidential advice on national security risks in international research.

In parallel, UK Research & Innovation (UKRI) rolled out Trusted Research and Innovation principles to safeguard IP, sensitive research, and personnel from hostile interference.

Cyber Espionage on R&D examples:

In 2020, Western governments revealed that Russian intelligence-linked hackers (APT29 “Cozy Bear”) attacked COVID-19 vaccine research in the US, UK, and Canada theguardian.com.
Otherstate actors from China, Iran, and North Korea attempted to steal vaccine data and intellectual property in what was described as an “IP war” over life-saving research theguardian.com.

Insider IP Theft

In 2025, a researcher at the University of Texas MD Anderson Cancer Center was charged with espionage for stealing 90 gigabytes of confidential cancer research data with intent to smuggle it to China texaspolicy.com.
In another case, a Texas A&M professor covertly sent NASA-funded research to a Chinese institution texaspolicy.com.

Charles University (Prague), 2019

Chinese Embassy in Prague secretly financed activities at Charles University’s Czech-Chinese Centre. The funding (≈ €47,000) was routed through a private company co-owned by the centre’s director, Miloš Balabán, and used to underwrite two university-branded conferences (2018–2019).

The same network financed a for-credit course on the Belt and Road Initiative; top student essays were rewarded with embassy-funded trips to China.

University response

After the payments came to light, Charles University fired three staff members involved and closed the Czech-Chinese Centre; audits were initiated.

A subsequent Counter Foreign Interference (CFI) Manual produced for the Czech academic sector documents the episode and notes an estimated loss of ~CZK 5 million tied to the affair.

The National Research Security Hub

one-stop shop

The Hub's Role

Policy informing and coordination, knowledge sharing,
risk identification

Guidance & Support

Provide comprehensive guidance and assistance for research institutions and other key actors throughout the RDI ecosystem to address security challenges

Develop and Provide Practical Tools

Risk evaluation in international R&I collaborations, including due diligence protocols, risk assessment guidelines, checklists etc.

Disseminate know-how on research security

Document and disseminate national and international good practices, develop and deliver awareness raising campaigns and capacity building programmes

Public policy advisory and development

Help embed research security in the governance of publicly funded RDI projects

Initiate interinstitutional dialogue

Explore cooperation models for the National Research Security Hub & policy framework.

Next steps

01

Institutional commitment

Memorandum of Understanding to establish the operational structure for the Hub, including governance model, core functions and responsibilities (possible model: M100 Hub).

02

System mapping & analysis

Who is doing what? Analyze roles, competences, resources and motivations to support the Hub and policy framework

03

Develop instruments

Including procedures for risk assessment, checklists, due diligence protocols.

04

Awareness & training programmes

for researchers, evaluators, and project managers involved in regional, national and international RDI projects.

05

Embed RS in funding process

Gradual integration of research security criteria in project application and evaluation processes.

Policy coherence

Multi Level Governance

Thank you

razvan.craciunescu@upb.ro