MINISTERUL EDUCAȚIEI ȘI CERCETĂRII

2025

POLICY RECOMMENDATION ON RESEARCH SECURITY IN ROMANIA

CONCEPT NOTE

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

Str. D.I. Mendeleev nr. 21-25, Sector 1, 010362, București
Tel: +40 21 302 38 50, Fax: +40 21 311 59 92 E-mail: office@uefiscdi.ro
www.uefiscdi.gov.ro

As defined by **the National Science and Technology Council in the United States (NSTC, 2022)**, research security refers to the efforts undertaken to "safeguard the research enterprise against behaviours aimed at misappropriating R&D to the detriment of national or economic security, related violations of research integrity, and foreign government interference." Thus, research security encompasses a wide range of actions aimed at:

- **Protecting Intellectual Property (IP):** Safeguarding inventions, research findings, and methodologies that can provide competitive advantages.
- **Data Protection:** Ensuring the security of sensitive data, including personal information, trade secrets, and classified information.
- **Research Integrity:** Maintaining research outputs' authenticity and accuracy is crucial for public trust and policy-making.
- **Preventing research misuse:** Ensuring the use of research data and RDI end results for the proposed purposes, avoiding the involvement in, among others, criminal purposes, the development of chemical, radiological, and biological or nuclear (CBRN) capabilities, and civilian surveillance.

Policymakers across the globe use a range of terms - such as trusted research, knowledge security, responsible internationalisation, and protection against foreign interference in research - to address emerging challenges in the research landscape. While these concepts are not interchangeable and reflect important semantic and policy differences, they all share a common goal: to safeguard the security and integrity of research ecosystems, ensuring that innovation and international collaboration can continue in a responsible and resilient manner. Ensuring that R&D results are protected and that the benefits of innovation are accredited to those who do the work motivates researchers to continue their work, thus supporting scientific advancement. Moreover, developing and implementing measures addressing research integrity and security prevents bad-faith actors from misappropriating knowledge and technology to advance their goals and use this knowledge in military contexts (SIGRE, 2022).

Over the past decade, research security has gained significant attention due to the growing complexity of external risks, including cyber-attacks and intellectual property theft. However, threats to research security and integrity also include interfering with academic discourse and attempts to improperly influence the direction of research or to have an impact upon the behaviours of individual researchers or whole institutions. Such actions can impact reputation, either of individual institutions (with well known universities such as Cambridge University and Imperial College suffering reputational and political damage due to engaging in work with foreign research performing organisations related to the military) or whole research systems, and even the safety of people on campuses (Jones, 2025).

New challenges and threats are constantly emerging as governments and non-state actors (e.g., private companies) make substantial efforts to improperly exploit and distort research outputs for their interests (OECD, 2022).

At present, geopolitical tensions are bringing research security risks to a new level; furthermore, there are increasing concerns related to the dual use of the same technology for civilian and military purposes (Dixson-Declève et al., 2022). The US competes with China for high-tech dominance (Tiffert, 2024), and the over-reliance on a single source for critical technologies (e.g., semiconductors) has created significant vulnerabilities in markets and supply chains (Diamond et al., 2023). In response to emerging challenges, the United States has made significant efforts to strengthen research security through national policies like the NSPM-33 Memorandum, linking government funding for research projects to compliance with security protocols. Similar initiatives have been adopted in other nations, including Canada and Australia, reflecting a broader global commitment to safeguarding research integrity and security. At the European Union level, The Commission (DG R&I) issued (2022) a Staff working document entitled "Tackling R&I Interference", specifying possible mitigation measures that could be taken by Research Performing Organizations (RPOs) and Higher Education Institutions (HEI).

In Europe, the Russian invasion of Ukraine is putting additional pressure on EU countries, especially in terms of energy production and distribution. Moreover, European cities and states are increasingly committed to fighting climate change and achieving climate neutrality; while such efforts are necessary, the out-of-control climate crisis requires new resources and technologies and putting boundaries on material consumption. All these create disruptions in the research ecosystem and generate concerns over strategic dependencies[1], challenging the EU's vision of "openness", which has been central to European democracy (Dixson-Declève et al., 2022).

An independent expert report published by the Directorate-General for Research and Innovation (2022) puts forward a series of measures for "de-risking" potential national and European security threats. These include the protection of confidential data (for science in general), avoiding strong dependencies on key technologies (especially in the case of technologies addressing global challenges), and decoupling from actors and regions in relevant activities and areas (in the case of goods and knowledge with national security concern) (Dixson-Declève et al., 2022).

The EU's focus on research security has intensified with the publication of the **Council Recommendation on enhancing research security** and the launch of the new Competitiveness Compass (2025). While the Council Recommendation emphasizes the necessity for EU member states to adopt robust frameworks for research security that encompass risk assessment, management strategies, and institutional regulations, the Compass outlines actions to boost economic growth in the EU over the next five years, placing research, innovation, science, and technology at the heart of the EU economy. By embedding research security within a broader economic and strategic framework, Europe can protect its scientific excellence while fostering a research environment that is both open and resilient to emerging threats. Overall, both documents (the Recommendation and the Compass) pave the way for enhanced research security requirements to be integrated in the future framework programme from 2028-2035.

[1] e.g. European dependency on China for solar panels, as documented by Garcia Herrero (2023)

The critical importance of research security for the next Eu Framework Programme for Research and Innovation is highlighted in Science Europe's recent position paper, entitled "10 Key Messages For the 10th EU Framework Programme" (Science Europe, 2024). The paper calls for a cautious approach to dual-use research, and a balanced approach to knowledge security, while advocating for renewed investment in peace research.

It is therefore expected that the next framework programme will strike a balance between research security and openness, ensuring that international collaborations continue to thrive while addressing growing geopolitical risks. While research and innovation (R&I) investments are more critical than ever to tackle global challenges like climate change, competitiveness, and technological progress, heightened security concerns call for a more structured approach to safeguarding research integrity. A key priority for FP10 should be to preserve international research collaboration, despite increasing demands for stricter security measures. Research security policies should not undermine the openness of scientific exchange, which remains vital for global progress. The programme should promote responsible and reciprocal openness in international R&I cooperation, ensuring that partnerships respect fundamental European values as outlined in the Pact for Research and Innovation.

Furthermore, Science Europe's position paper (2024) undescores that while risk assessments are necessary, they should be conducted at the project level rather than applying blanket restrictions that could hinder scientific progress. Instead of imposing rigid barriers, FP10 should support research institutions and individual researchers by providing the necessary tools, funding, and guidance to navigate security challenges. This includes fostering responsible dual-use research management while maintaining academic freedom, open science, and knowledge integration as foundational principles.

It is thus clear that EU policies and FP10 in particular should enhance research security without compromising the openness and collaborative nature of European science – de-riskrather than de-couple[1]. By taking a balanced, risk-aware, and institutionally supportive approach, the EU can ensure that research remains a driver of global innovation and societal progress while mitigating emerging threats in an increasingly complex geopolitical environment.

A recent study funded by the UK Science and Innovation Network (SIN) aims to investigate research security policies and practices across Europe, focusing on perceptions of threats, governmental and RFO practices already in place in European countries, and opportunities for cooperation (James, 2025).

The study examined seven European countries—Czech Republic, France, Germany, Italy, Netherlands, Spain, and Sweden—alongside the European Union's evolving stance on research security, particularly following the European Council recommendations issued in 2023. Its methodology included:

- Bibliometric analysis using co-publication data to identify patterns of collaboration and key international research partners.
- A review of policy documents from governments, research funders, and sector organizations to understand national approaches to research security.
- Around 70 interviews with policymakers, research funders, university leaders, research managers, and sector organizations to gain insights into practical challenges and policy implementation.

Key findings highlighted that research security risks vary by country but commonly include foreign interference, collaborations with entities of concern, export control violations, cyber threats, and insider threats. The study emphasizes the importance of de-risking rather than decoupling research relationships, particularly concerning China and Russia, which are often viewed as high-risk due to concerns over intellectual property theft, civil-military integration, and geopolitical tensions.

It is important to recognize that many research security risks emerge from activities that are entirely legal and often conducted in good faith - such as fundamental research or international collaborations conducted under the umbrella of academic freedom. These activities do not necessarily violate export controls, intellectual property laws, or criminal statutes, yet they may still expose research ecosystems to strategic vulnerabilities. As such, treating research security primarily as a matter of compliance - by creating lists of sensitive technologies, identifying high-risk partners, or tightening regulations - addresses only part of the challenge. A more holistic and proactive approach is needed, one that emphasizes behavioral change and cultivates risk awareness across the research community.

The study underscores the importance of national research security frameworks, cooperation between governments and academia, and targeted risk assessments at the project level to balance openness with security in international research collaborations. It also points out that existing policies and practices at national levels, albeit different, create opportunities for mutual learning among governments, research funding organisations and research institutions. To support a secure yet collaborative research environment, it is essential not only to share best practices through guidance documents, cross-border forums, and case studies, but also to work toward interoperable standards. Such standards can help build communities of trust and facilitate secure, responsible international collaboration - strengthening, rather than restricting, cross-border scientific cooperation.

MITIGATING RISKS

To tackle threats to research security, several recommendations have been put forward in the scientific literature and included in reports published by international organizations (OECD, G7), National Governments (Germany – BMBF's Position paper on Research Security, UK - National Security and Investment Act: guidance for the higher education and research-intensive sectors), think tanks, and associations (The Higher Education Export Control Association, Universities UK, DFG - German Research Foundation), that include both (1) institutional guidelines and protocols, as well as (2) the integration of research security into broader national policies.

Establishing institutional guidelines and protocols can safeguard sensitive data, technologies and know-how while promoting openness within international research collaborations. Specific attention should be given to sensitive research areas, including defence, artificial intelligence, and biotechnology, where the risk of misuse of R&D results tends to be higher. Furthermore, dual-use technologies - broadly understood to include not only traditional military-civilian applications but also emerging domains where civilian research may be repurposed for harmful uses - should receive particular attention. As the definition of dual-use continues to evolve, clear and context-specific criteria are needed to help institutions and researchers identify and manage such risks effectively.
Institutional protocols can be adopted at the level of both RPOs and HEIs as well as governmental institutions and may include measures such as (OECD, 2022):

- requiring researchers (in the case of research institutions), evaluators, and public servants to disclose conflicts of interest and conflicts of commitment;
- in the case of governmental institutions, procedures to integrate risk assessment and management into the roll-out of calls for projects and in review/evaluation processes are required;
- adopting tools to systematically assess the risks of malign interference and inform decisions on new research opportunities;
- establishing dedicated structures to manage research security risks and provide research security training to raise awareness among researchers and administrative staff;
- creating the regulatory requirements, institutional procedures, and internal policies necessary to systematically collect, manage, and govern high-quality data that can inform research security risk assessments and decision-making processes.

Risk-based approaches and a due-diligence organisational culture are already in in several countries, such as the UK, Canada and Austrialia, where universities are encouraged to implement detailed checklists and due diligence processes for all international collaborations. Projects involving partners from high-risk countries (e.g., China, Russia, or Iran) are and escalated to dedicated compliance teams for further review.

Developing and implementing national policies on research security is essential to protect the integrity and competitiveness of a country's research ecosystem while fostering international collaboration. Research security policies address threats such as intellectual property theft, unauthorized knowledge and technology transfers, malign interference in research processes, and research misuse.

However, responsibilities for research security do not fall on one category of stakeholders. Still, they are distributed to multiple actors in the international research ecosystem, including national governments, research funding institutions, RPOs, universities, academic associations, and intergovernmental organisations (OECD, 2022). In some countries (notably the USA and Canada), mechanisms are already in place to enhance collaboration and information sharing between intelligence agencies, law enforcement, research institutions, and universities to improve risk management and security in international research collaborations.

EXAMPLES OF POLICY GUIDELINES AND RECOMMENDATIONS ADDRESSING RESEARCH SECURITY

EU LEVEL

a) Council Recommendation on enhancing research security

The need for concrete national policies and measures to protect R&D results from misuse was recently reflected in the European Commision's Proposal for a Council Recommendation on enhancing research security (COM(2024)26, Recommendation ENHANCING RESEARCH SECURITY). The document points out that increasing geopolitical tensions, cyber threats, foreign interference, and hybrid threats have made research security a priority. While Europe must remain an attractive hub for global research cooperation, it must also safeguard its intellectual assets and prevent their misuse for military or coercive purposes. Striking this balance requires a nuanced and proactive approach to research security.

Despite growing awareness, research security policies remain fragmented across EU Member States. Some countries have taken steps to introduce protective measures, while others lag behind, creating vulnerabilities that can be exploited by external actors. Some EU countries have developed research security policies; however, there is inconsistency across Member States, leading to potential vulnerabilities. Thus, a common EU framework is necessary to ensure a level playing field and protect academic freedom.

At the level of individual member states, governments and research funding organisations must provide guidance, training, and institutional support, ensuring that academic institutions can navigate complex security challenges while preserving institutional autonomy. A collaborative effort between policymakers, RPOs, researchers, and funding bodies is necessary to enhance resilience across the sector. Last but not least, measures should be proportionate, avoiding excessive restrictions that could hinder research collaboration.

Overall, **recommendations for member states** focus on:

1. Establishing a national research security framework

- Develop national action plans on research security, aligned with EU principles;
- Create national guidelines for research institutions on identifying and mitigating security risks;
- Establish Research Security Advisory Hubs to provide expertise, training, and resources.

EU LEVEL

2. Strengthening institutional resilience

- Encourage universities and research organizations to implement risk assessment protocols for international collaboration;
- Require due diligence checks on research partners, particularly those from high-risk regions;
- Enhance cybersecurity measures for protecting sensitive research data.

3. Integrating research security in funding policies

- Ensure that research funding agencies include security risk assessments in grant evaluations;
- Require funding recipients to demonstrate compliance with research security best practices;
- Promote transparency in research funding sources and affiliations.

4. Enhancing awareness and training

- Develop training programs for researchers (including PhD and post-doctoral students), laboratory technicians and university administrators on research security;
- Implement awareness campaigns to educate researchers about risks related to foreign interference and knowledge transfer;
- Encourage sector-wide peer learning and knowledge sharing on research security.

5. Strengthening international collaboration safeguards

- Align national policies with EU research security measures to maintain international cooperation while mitigating risks.
- Work with international partners to exchange best practices on secure research collaboration.
- Advocate for reciprocity in international research agreements, ensuring fair and transparent partnerships.

6. Monitoring and evaluation

- Regularly assess and update research security policies in response to emerging threats.
- Introduce resilience testing and incident simulations to identify vulnerabilities.
- Report progress to the EU, ensuring compliance with research security standards.

The recommendations outlined in the Council's proposal provide a comprehensive framework for safeguarding research integrity while maintaining openness, international collaboration, and academic freedom. Striking the right balance between security and cooperation is crucial to ensuring that research remains a driver of innovation while mitigating risks such as foreign interference, cyber threats, and unethical exploitation.

EU LEVEL

At the European level, a coordinated approach is essential to avoid fragmentation and inconsistencies in research security policies. Establishing a European Centre of Expertise on Research Security, fostering peer learning, and ensuring alignment with critical technology protection efforts and export control policies will enable Member States to address emerging threats proactively.

b) Tackling R&I foreign interference, Staff Working Document

EU Higher Education Institutions (HEIs) and Research Performing Organisations (RPOs) can benefit from a comprehensive strategy for tackling foreign interference that covers key areas of attention grouped into the following four categories: values, governance, partnerships, and cybersecurity. A non-exhaustive list of possible mitigation measures that can help HEIs and RPOs develop a comprehensive strategy tailored to their needs is included in the document.

G7: Best practices for secure and open research

This framework of principles, guidelines, and best practices is based on the vision that respecting freedom in scientific research is an indispensable cornerstone of democracy and a common core value for trustful and open research cooperation with international partners.

Although it is not a policy-binding document, it is intended to inform and inspire collaborative efforts among G7 nations. The framework focuses on shared values and principles, such as transparency, academic freedom, and proportional risk management, to address emerging challenges in the global research environment.

The document includes a list of best practices to provide high-level information on practices that contribute to secure and open research, addressed to various stakeholders: governments, research funders, research institutions, and researchers.

EXAMPLES OF NATIONAL POLICY FRAMEWORKS AND INSTITUTIONS IN PLACE TO STRENGTHEN RESEARCH SECURITY

USA

The US National Security Presidential Memorandum-33 (NSPM-33) serves as a cornerstone policy to enhance research security in the United States. It provides a model for balancing openness in research with robust protections against undue foreign influence. NSPM-33 mandates that institutions receiving substantial federal research funding implement research security programs to address key areas such as cybersecurity, foreign travel security, research security training, and compliance with export control regulations. It also sets the framework for standardizing disclosure requirements for researchers to address conflicts of interest and commitment and prohibiting participation in malign foreign talent recruitment programs.

The National Science Foundation (NSF) plays a critical role in complementing the measures outlined in the NSPM-33. Actions implemented by NSF include emphasizing compliance with disclosure rules both for NSF staff and the institutions and researchers funded by NSF, requiring research institutions funded by NSF to submit financial disclosure reports, requiring annual science and security training for all its staff and developing and providing broader training on research security for the research community[3].

However, unlike some other national systems, the U.S. does not currently provide centralized, government-operated advisory services outside of law enforcement or intelligence agencies. Responsibility is largely decentralized, falling to individual institutions to interpret and implement security requirements. While agencies like the National Science Foundation (NSF) play a complementary role by offering guidance and requiring compliance with disclosure and training mandates, institutions often operate with limited access to dedicated, publicly supported advisory bodies. This lack of a unified advisory mechanism creates a fragmented environment where implementation practices may vary widely across research-performing organizations.

To help organizations protect international science research, the National Institute of Standards and Technology (NIST) launched the "Safeguarding International Science Research Security Framework" (Strouse et al., 2023), offering guidelines and best practices to help institutions balance openness with appropriate levels of protection. Despite these tools, U.S. institutions must often navigate research security requirements independently, which may serve as a cautionary point for Romania regarding the importance of centralized advisory support.

[3] The online modular training is intended to enhance awareness and to provide recipients of federal research funding with knowledge on the existing and emerging risks and threats to the global research ecosystem and resources necessary to protect against such risks and threats (NSF, 2024)

Canada has adopted a more integrated and proactive approach to research security. To ensure the Canadian research ecosystem is as open as possible and as secure as necessary, the Government of Canada introduced the National Security Guidelines for Research Partnerships.

The guidelines aim to integrate national security considerations into developing, evaluating, and funding research partnerships. Developed in consultation with the Government of Canada-Universities Working Group, these guidelines are intended to provide clear information on the specific national security considerations for research partnerships (including who researchers partner with and what areas of research are at higher risk) to support researchers, research institutions, and funding agencies to identify and mitigate potential security risks to research.

To protect their work, all researchers are encouraged to use the National Security Guidelines for Research Partnerships to assess all research partnerships with any partner or funder.

Furthermore, starting from 2024, in line with the new Policy on Sensitive Technology Research and Affiliations of Concern, research-performing organisations submitting funding applications involving research that advances a sensitive technology research area are required to ensure that researchers involved in activities supported by the grant are not affiliated with universities, research institutes or laboratories connected to the military, national defence, or state security entities that could pose a risk to Canada's national security.

To support this, Canada released two lists[4] that provide clear, defined, and transparent guidance so that researchers can quickly and efficiently determine if these new requirements apply to their research.

The Canadian model illustrates the value of clarity and operational guidance. Its centralized tools could serve as a useful reference point for Romania, especially in terms of designing mechanisms that provide researchers and institutions with practical decision-making support.

CANADA

[4] (1) List of Sensitive Technology Research Areas that support the development and advancement of new technologies, and (2) List of Named Research Organizations connected to military, national defence, or state security entities that could pose a risk to Canada's national security.

UNITED KINGDOM

The UK does not currently have a single overarching national research security policy, but it has developed a decentralized institutional ecosystem to manage research security risks.

The Research Collaboration Advice Team (RCAT) is a collaboration between the government and academia, providing research institutions with advice about national security risks linked to international research (2024). RCAT provides non-enforcement-based advisory services to research institutions. RCAT operates through five regional offices, offering tailored advice to universities and research organizations about national security risks linked to international collaboration. It serves as a key point of contact for universities seeking risk assessments, helping institutions interpret and apply existing guidance in specific collaboration contexts.

The Trusted Research and Innovation (TR&I) work programme was developed by the UK Research and Innovation (UKRI); it aims to protect the UK's intellectual property, sensitive research, people, and infrastructure from potential theft, manipulation, and exploitation, including as a result of interference by hostile actors. In line with this programme, UKRI published a set of Trusted Research and Innovation Principles (2021) to set out expectations of UKRI-funded organisations concerning due diligence for international collaboration.

This combination of regional advisory services (via RCAT) and strategic principles (via UKRI) offers a highly user-oriented model. In addition, the National Protective Security Authority (NPSA) and the National Cyber Security Centre (NCSC) have developed a suite of Trusted Research guidance materials in consultation with academic and public sector experts. These include tailored guidelines for researchers, university leadership, and industry partners, alongside a series of scenario-based videos illustrating real-world cases from the UK higher education sector.

To support institutional self-assessment and capacity-building, NPSA and NCSC also introduced a Trusted Research Implementation Framework and a Collaboration Checklist, which research institutions and offices can use to evaluate the level of risk in proposed international collaborations.

Together, these resources form a coherent support system that encourages informed decision-making at the institutional level—an approach that could provide a valuable model for Romania as it develops its own national framework and advisory infrastructure.

THE NETHERLANDS

The Dutch model for research security is structured around the concept of knowledge security, which encompasses not only the prevention of undesirable knowledge and technology transfer but also the protection of academic freedom and ethical standards in international cooperation. The system is supported by the National Contact Point for Knowledge Security, ensuring tailored guidance based on the specific needs and regulatory environments of both academic as well as business entities. The offices of the National Contact Point assist institutions in risk assessments, partner due diligence, and the application of screening mechanisms for foreign researchers and visiting scholars.

The guidance provided covers both legal compliance (e.g., export control and sanctions) and broader risk awareness, including reputational and ethical dimensions. Additionally, the National Knowledge Security Guidelines can help ensure that international collaboration can occur safely.

This model encourages early engagement in the research lifecycle, helping users flag and mitigate potential risks before formal partnerships are established. For Romania, this approach offers a useful example of how institutional support services can be embedded within a dedicated, government-supported framework while maintaining a strong focus on safeguarding openness and collaboration.

GERMANY

Germany's approach to research security is shaped by its federal governance structure, which distributes authority over higher education and research between the federal government (Bund) and the individual states (Länder). This decentralization creates both strengths and challenges: while it allows regional tailoring of research governance, it also complicates the development of nationally unified research security frameworks.

The German Federal Ministry for Education and Research (BMBF) issued a Position Paper on Research Security in 2024 in light of geopolitical shifts. The paper calls for increased awareness and safeguards related to international research collaboration, especially concerning dual-use research, civil-military cooperation, and knowledge transfer risks.

However, Germany lacks a centralized advisory body comparable to RCAT in the UK or the contact points in the Netherlands. Instead, research security implementation varies across institutions, with some universities developing internal risk assessment protocols and training programs, while others rely on guidelines and ad hoc advice from federal and Länder-level bodies.

This fragmented but maturing system underlines the importance of coordination mechanisms between state and federal levels. For Romania, Germany's experience offers a valuable lesson on the need for cohesive governance and capacity-building, especially in contexts where authority over research is shared among multiple entities. A national advisory hub or working group could help bridge institutional gaps and foster harmonized implementation.

In the Czech Republic, a set of documents for enhancing resilience against illegitimate interference in the higher education and research environment has been developed by the Interdepartmental Working Group for Combating Illegitimate Interference in the Higher Education and Research Environment, with support from the Ministry of Education, Youth, and Sports, the Ministry of the Interior, and the Czech Academy of Sciences, and in consultation with representatives of other Czech higher education and research institutions.

These documents include:

- Methodological recommendations for risk management in research security at national level, providing universities and research institutions with standardized best practices for identifying and mitigating risks, ensuring their resilience against external interference;
- Handbook on Technical Assistance and Intangible Transfer of Technology, which further supports research institutions in complying with export controls and international sanctions. The Handbook provides guidelines on managing controlled technologies and international research cooperation, screening procedures for foreign researchers and partners to mitigate security risks, and legal requirements regarding dual-use technologies and strategic research exports;
- The Counter Foreign Interference (CFI) Manual - a comprehensive guide designed to help academic institutions identify and mitigate risks associated with foreign interference. The manual was developed in response to increasing concerns over covert influence, espionage, and knowledge security threats within Czech universities and research organizations. The manual provides practical recommendations for universities, research institutions, and individual researchers to enhance resilience against foreign interference.

The CFI manual covers:

- Risk management strategies to identify and address vulnerabilities within academic institutions.
- Due diligence processes for assessing international research collaborations, financial partnerships, and external funding sources.
- Guidelines for protecting intellectual property, research data, and sensitive information.
- Cybersecurity measures to safeguard digital assets from cyber threats and espionage.
- Countermeasures against covert foreign influence techniques, such as recruitment, coercion, and financial manipulation.

Overall, these guidelines encourage Czech institutions to conduct **regular security audits,** enforce **data protection** protocols, and establish **clear incident response mechanisms**. Rather than severing international partnerships, the focus remains on risk mitigation and responsible collaboration, ensuring that research remains secure, ethical, and globally competitive.

The Czech model offers valuable lessons for Romania, particularly in demonstrating how a coordinated, interministerial approach can result in practical tools that empower institutions while maintaining national coherence. The emphasis on detailed manuals, checklists, and implementation guides - rather than solely on regulatory controls - could inform Romania's own development of a national research security framework.

RISK ASSESSMENT AND MITIGATION

Risk assessment in research security and trusted research is a critical process to safeguard intellectual property (IP), ensure the integrity of technology transfer, and protect sensitive innovation processes[5]. With the increasing complexity of global research collaborations and technological advancements, evaluating risks is essential to balance openness in research with the need for security.

Regarding **IP protection in research and development**, risks arise from insufficient contractual protections and/or unregulated information-sharing practices in collaborations, particularly in international settings. Robust IP management policies, including clear ownership agreements and legal safeguards, are crucial for mitigating these risks. Additionally, clearly identifying sensitive research areas, technologies, and projects and implementing enhanced cybersecurity measures can prevent unauthorized access to proprietary data, as recommended in the UK's Trusted Research guidance (NSPA, 2024).

The **technological transfer (tangible and intangible goods and/or services) and innovation process** also demand rigorous risk assessment to prevent misuse or unintended dissemination of sensitive data, know-how and technologies. Similarly, ensuring that **testing environments** are secure from insider and outsider threats is pivotal, particularly in the case of sensitive or dual-use technologies, as vulnerabilities in these areas can lead to significant breaches or exploitation.

Moreover, a structured risk assessment framework must address the use of research infrastructure, mainly when advanced technologies like AI and IoT are involved. Emerging technologies pose unique risks, including vulnerabilities in data integrity and potential misuse in critical infrastructure applications. As highlighted in a report published by RAND (Gerstein & Leidy, 2024), integrating advanced threat and vulnerability analyses can help researchers and institutions navigate these challenges, ensuring research benefits society without unintended harm.

Research partnerships' potential national security implications are considered in project funding decisions in countries such as the US or Canada. In the United Kingdom, risk assessment is not mandatory; however, guidelines, self-assessment frameworks, and checklists are available to researchers and research offices to determine the level of risk incurred by a collaboration.

[5] see recommendations from the German Research Foundation (2023) and an updated study published by the German Aerospace Center (Plé et al., 2024)

These insights underline the importance of creating comprehensive, adaptable risk assessment protocols integrated into research governance at institutional and national levels. However, implementing research security policies and protocols requires enhanced administrative capacity and a knowledgeable workforce. Building and strengthening institutional capacity for research security and integrity requires coordinated efforts across research-performing organizations, research funding bodies, and governmental agencies.

At the institutional level, universities and research institutions play a pivotal role in safeguarding research. They must prioritize establishing robust internal policies and systems for identifying potential risks and ensuring compliance with national and international security standards. Furthermore, dedicated research security committees help in risk evaluation and management, and tools like checklists and risk assessment frameworks allow for better decision-making (OECD, 2022).

Internal procedures and protocols should be backed by relevant guidelines and training programmes to prepare researchers and administrative staff to recognize threats and implement risk mitigation strategies (OECD, 2022). **As the workforce becomes increasingly digital, increasing awareness of research security issues among researchers and providing necessary training to equip them with the skills to identify and mitigate risks effectively are crucial.** If possible, funding bodies should provide ongoing training and resources to researchers and institutions, helping them understand the complexities of research security (e.g., as in the case of NSF in the United States).

Governments should continuously collaborate with academia and industry to share intelligence, develop best practices, and ensure that research security does not come at the cost of academic freedom or international cooperation. Research ecosystems can remain secure, innovative, and trustworthy by aligning policies across these sectors.

RECOMMENDATIONS FOR GOING FORWARD

BUILDING CAPACITY FOR RESEARCH SECURITY IN ROMANIA

Research security is an essential aspect of the current global research ecosystem; as the research landscape evolves, the implementation of comprehensive security frameworks, awareness programs, and international collaboration becomes imperative. By prioritizing research security, nations can ensure the integrity and sustainability of their scientific endeavours while safeguarding national interests.

In Romania, given the current geopolitical challenges and the growing number of research projects and international collaborations, addressing risks to research security is essential for safeguarding the integrity and credibility of the research, development, and innovation system. While research integrity refers to the ethical and professional standards governing the conduct of research, research security focuses on protecting institutions, knowledge, and collaborations from undue influence, misappropriation, or strategic misuse.

Both are vital - and complementary - in maintaining trust in Romanian science. Building national and institutional capacity to address security threats, while fostering critical awareness among researchers, is key to ensuring that Romania can thrive as a competitive player in the international research community. Moreover, as global research security norms tighten, countries without credible safeguards may find their researchers excluded from sensitive or high-value collaborations.

A robust and transparent research security framework could therefore be a prerequisite for continued access to international partnerships and funding opportunities.

A National Framework for Research Security in Romania

Based on best practices from the Czech Republic and other European and international policies and practices, Romania could benefit from a structured, multi-stakeholder national framework that balances openness and international collaboration with security measures focused on due diligence and risk mitigation. Its development should be based on a comprehensive analysis of data on research projects benefitting from public funding in the past decade to identify sensitive research areas, research infrastructure, and technologies that should be subject to risk assessment and de-risking strategies.

Further, the framework should include:

- National policies and guidelines that provide a structured risk management approach for research security;
- Institutional support structures, such as a Research Security Advisory Hub, to assist researchers in evaluating international collaborations and mitigating risks;
- Integration of research security into funding policies, requiring grant recipients to conduct due diligence and risk assessments;
- Literacy and awareness-raising programme to build institutional and researcher capacity;

To ensure a comprehensive, risk-based, and sustainable approach, the governance and implementation of such a framework should involve key national institutions, funding bodies, and security agencies, including:

- The Ministry of Education and Research;
- Ministry of Internal Affairs;
- Ministry of European Investments and Projects (MIPE);
- Ministry of Economy, Digitization, Entrepreneurship and Tourism (MEDAT);
- Executive Agency for Higher Education, Research, Development, and Innovation Funding (UEFISCDI);
- National Council for Research Ethics (CNER);
- Special Telecommunications Service (STS);
- Authority for Digitalization of Romania (ADR)
- Intelligence Services (SRI, SIE);
- National Council of Rectors in Romania (CNR);
- Council of National Research and Development Institutes in Romania (CINCDR).

By working collaboratively, these entities would ensure the necessary institutional capacity and expertise for designing and implementing a wide range of measures, such as developing evidence-based national guidelines on research security, integrating security protocols into research funding, developing tools to ensure compliance with research integrity standards and ethical guidelines to prevent research misuse, and developing guidelines for cybersecurity and digital research security.

Intelligence services are to play a key role in providing data and expertise on foreign interference, cyber threats, and counterintelligence related to research security, while the involvement of the **National Council of Rectors (CNR)** and the **Council of National Research and Development Institutes (CINCDR)** would support the effective implementation and **institutional adoption of research security policies** across Romania's **higher education and research ecosystem.**

Literacy and awareness programme addressed to academia and peer reviewers/project evaluators

Regular training and awareness campaigns are crucial for cultivating a security-conscious research culture. Courses covering export controls, research security protocols, and intellectual property protection help ensure that researchers and administrative staff understand and comply with security requirements. However, research security is not only a regulatory or procedural issue, but fundamentally a behavioral challenge. Policy documents and guidelines will have limited impact unless they are embedded within a broader cultural shift in how science is governed and practiced. Training programmes should therefore not only deliver information but also foster shared responsibility, ethical awareness, and critical reflection among researchers. Building such a culture requires ongoing engagement, leadership commitment, and integration of security considerations into the daily practice of research-performing organizations.

Tools to build literacy and awareness:

- written guidelines on research security and trusted research, focusing on possible risks in research collaborations and potential de-risking strategies; several de-risking strategies have already been documented in the independent expert report published by the European Commission in 2022 (Dixson-Declève et al., 2022);
- presentations of real-life scenarios based on real events (several cases of misappropriation of dual-use technologies have been documented, particularly in the US and the UK) and best practices on how to mitigate security risks in research collaborations;
- trainings (online and on-site) for project directors and project evaluators.

Development of practical tools for risk identification and assessment

- self-assessment screening - tools for identifying risks (e.g., checklists for academia and industry)
- templates for due diligence in international collaborations (including forms to disclose conflicts of interest and conflicts of commitment)

Integration of research security protocols in the evaluation of public-funded projects

- funding applications should include mandatory risk assessments for collaborations in sensitive research areas, ensuring transparency and mitigation of potential threats
- introducing the requirement to disclose conflicts of interest and commitment concerning external parties.

It should be noted that, despite established practices, many institutions – both research funders as well as research performing organisations - face challenges such as limited resources, shortages of skilled personnel (for example, experts in open-source intelligence), and the risk that burdensome procedures might deter researchers from pursuing valuable international collaborations.

RESEARCH SECURITY ADVISORY HUB

The concept of „**Research Security Advisory Hub**" was first introduced in the European Commission Proposal for a Council Recommendation on enhancing research security; it is defined as a support structure to help researchers and innovators deal with risks related to international cooperation in research and innovation. Bringing together expertise and skills from multiple sectors, such a hub should offer information and guidance that research-performing organizations can use to make well-informed decisions, carefully assessing both the opportunities and risks of potential international collaborations.

Additionally, a Research Security Advisory Hub should provide other essential services tailored to the specific needs of the research and innovation sector, such as designing and deploying awareness-raising campaigns and rolling out training programmes.

Establishing a national hub would serve as a critical step in addressing the need for enhanced national and institutional capacity. Such a structure would act as a centralized platform to provide training, resources, and guidelines to researchers, institutions, and policymakers, ensuring a systematic approach to risk management and fostering a culture of security and integrity. Ultimately, a national Research Security Advisory Hub would contribute to the resilience of the Romanian research ecosystem, enabling it to thrive amidst growing global challenges.

By integrating the ethos of corporate digital responsibility, this initiative would also set a benchmark for ethical and secure practices in research and innovation, positioning Romania as a responsible and forward-thinking player in the global scientific community.

Overall, a national framework for research security would provide the platform and tools to balance openness with risk management, ensuring that research remains innovative, collaborative, and secure. Bringing key institutions together as part of a multi-stakeholder working group or task-force on research security and developing a Research Security Advisory Hub will provide a solid foundation for a secure research ecosystem, helping Romania become and remain a trusted partner in international collaborations, despite the rapidly evolving geopolitical landscape.

Additionally, a national-wide literacy and awareness programme would help equip researchers, institutions, and policymakers with the knowledge and tools needed to identify, assess, and mitigate risks, ensuring that scientific advancements remain protected while maintaining an open and collaborative research environment.

REFERENCES

Deutsche Forschungsgemeinschaft (2023). Dealing with Risks in International Research Cooperation. Recommendations from the Deutsche Forschungsgemeinschaf [**Dealing with Risks in International Research Cooperation**]

Dixson-Declève, S., Renda, A., Schwaag Serger, S., Soete, L., Walz, R., Christofilopoulos, E., & Balland, P-A. (2023). Research, innovation, and technology policy in times of geopolitical competition, Publications Office of the European Union [https://doi.org/DOI 10.2777/745596]

Diamond, L., Ellis Jr., J. O., & Schell, O. (Eds.). (2023). Silicon Triangle: The United States, Taiwan, China, and Global Semiconductor Security. Hoover Institution Press

European Commission (2025). An EU Compass to regain competitiveness and secure sustainable prosperity [EU website, https://ec.europa.eu/commission/presscorner/detail/en/ip_25_339]

European Commission (2024). Recommendations on Research Security [EU website, eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52024DC0026]

European Commission (2022) Tackling R&I foreign interference – Staff working document, Publications Office of the European Union [Tackling R&I foreign interference - Publications Office of the EU]

G7 Security and Integrity of the Global Research Ecosystem (SIGRE) Working Group (2023). G7 Best Practices for Secure and Open Research [2023_bestpracticepaper.pdf]

German Federal Ministry of Education and Research – BMBF (2024). Position paper of the German Federal Ministry of Education and Research on research security in light of the Zeitenwende [position-paper-research-security.pdf]

Gerstein, D.M., Leidy, E.N. (2024). Emerging Technology and Risk Analysis. Artificial Intelligence and Critical Infrastructure [Emerging Technology and Risk Analysis: Artificial Intelligence and Critical Infrastructure | RAND]

Government of the Netherlands (2022). National knowledge security guidelines [National knowledge security guidelines | Publication | National Contact Point for Knowledge Security]

Government of the United Kingdom (2021). National Security and Investment Act: guidance for the higher education and research-intensive sectors [National Security and Investment Act: guidance for the higher education and research-intensive sectors - GOV.UK]

Innovation, Science and Economic Development Canada (2023). National Security Guidelines for Research Partnerships [national_security_guidelines_for_research_partnerships_Jan2024.pdf]

REFERENCES

James, A. (2025). Research Security: Reflections on the UK Experience. Presentation held in Bucharest for UEFISCDI staff and research performing organisations on February 28th 2025.

Ministry of the Interior of the Czech Republic (2020). Counter Foreign Interference Manual for the Czech Academic Sector, [UK-11805-version1-cfi_manual_for_the_czech_academic_sector.pdf]

OECD (2022), "Integrity and security in the global research ecosystem", OECD Science, Technology and Industry Policy Papers, No. 130, OECD Publishing, Paris [https://doi.org/10.1787/1c416f43-en]

National Protective Security Authority (NSPA) (2024). Trusted research [https://www.npsa.gov.uk/trusted-research]

National Science and Technology Council (NSTC) (2022). Guidance for Implementing National Security National Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development [NSPM-33 Definitions]

National Science Foundation (2024). Research Security Training [Research Security Training | NSF - National Science Foundation]

Plé, A., Kunkis, M., Droste-Franke, B. (2024). Risks in international research research cooperation. Causes, correlations and effects. German Aerospace Center [Risks-in-international-research-cooperation.pdf]

Science Europe (2024). 10 Key Messages for the 10th EU Framework Programme for Research and Innovation (FP10) [10 Key Messages for the 10th EU Framework Programme for Research and Innovation (FP10) - Science Europe]

Strouse, G.F., Wood, T.R., Saundry, C.M., Bennett, P.A., Bedner, M. (2023) Safeguarding International Science: Research Security Framework. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal Report (IR) [https://doi.org/10.6028/NIST.IR.8484]

UK Research and Innovation (2021). UK Research and Innovation Trusted Research and Innovation Principles [UKRI-170821-TrustedResearchandInnovationPrinciples.pdf]

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

MINISTERUL EDUCAȚIEI ȘI CERCETĂRII

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

Str. D.I. Mendeleev nr. 21-25, Sector 1, 010362, București
Tel: +40 21 302 38 50, Fax: +40 21 311 59 92 E-mail: office@uefiscdi.ro
www.uefiscdi.gov.ro