Council of the European Union

Brussels, 27 February 2026
(OR. en)

6856/26

RECH 88
POLCOM 74
COMER 34
RELEX 300
DUAL USE 19
ENER 97
ENV 180

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	27 February 2026
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	SWD(2026) 69 final
Subject:	COMMISSION STAFF WORKING DOCUMENT Research Security Monitor 2025: raising awarness and building resilience

Delegations will find attached document SWD(2026) 69 final.

Encl.: SWD(2026) 69 final

EUROPEAN
COMMISSION

Brussels, 27.2.2026
SWD(2026) 69 final

COMMISSION STAFF WORKING DOCUMENT

Research Security Monitor 2025: raising awarness and building resilience

Contents

FOREWORD

In October 2025 the first European Flagship Conference on Research Security took place in Brussels, co-organised by the European Commission and 12 prominent European research and innovation (R&I) associations, representing a significant share of the EU's R&I sector. Around 500 policymakers, experts and practitioners from Europe and beyond took part in the conference, which took stock of progress made in the field of research security, one and a half years after the Council had adopted its Recommendation on enhancing research security ([1]).

The conference demonstrated that the Council Recommendation has given powerful political impetus to ongoing efforts to raise awareness and build resilience across the European Union, and that a lot of progress has been made at all levels.

Presented as a key element of the EU's economic security strategy, launched in June 2023, the Council Recommendation complements policies that primarily target a variety of economic actors. Academia, and publicly funded research and innovation more generally, required a targeted, tailor-made approach due to its reliance on openness and international cooperation.

The EU's approach to research security is one that, in full respect of academic freedom, is built on strengthened self-governance by the R&I sector in combination with support from public authorities, by sharing information and providing guidance and advice.

The broad range of debates and discussions that took place at the flagship conference showed that this approach resonates with the sector, that there is commitment to act and that the need to do so is felt broadly.

It also showed that there is demand for case examples and insight into how to design policies and how to implement them in a way that is both effective and proportionate.

This first edition of the European Research Security Monitor, which is a report on the implementation of the Council Recommendation and is published alongside the second implementing report on the global approach to R&I, seeks to answer the call for practical examples from across the EU and offers guidance on where to start. It takes a qualitative approach, showcasing interesting examples and initiatives at different levels and contributing to debates that are currently taking place in many EU Member States.

By doing so, the Commission aims to support Member States and the R&I sector implementing the Council Recommendation on enhancing research security by keeping European R&I open and secure.

([1]) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C_202403510

EXECUTIVE SUMMARY

There is growing awareness that researchers need to take the security implications of their work carefully into account in today's international context. In 2024 the EU took important steps to address this issue by adopting the Council Recommendation on enhancing research security. The Recommendation is a reference point for research security with common definitions, shared principles and guidance on what an effective and proportionate policy response might look like. Subsequently, the European Commission launched a process with the Member States and the sector to promote and support the Council Recommendation's uptake and implementation.

Research security is about managing risks related to the undesirable transfer of critical knowledge and technology, malign influence on research, and violations of ethics and integrity. When designing and implementing research security measures, principles of responsible internationalisation should be applied. These include promotion of academic freedom, reliance on self-governance, taking a risk-based, country-agnostic approach and avoiding all forms of discrimination and stigmatisation.

Any research security policy or measure should be based on an appraisal of the risks. A research security risk appraisal should take into account several key risk factors: the institution's own risk profile, the knowledge domain's risk profile and the risk profile of the international partner and of the country where it is based. It is the combination of these factors that defines the project's risk level.

The first Research Security Monitor 2025 report provides a qualitative baseline for research security policies and measures across the EU and aims to inform and inspire policymakers and practitioners who are in the process of developing or strengthening such policies and measures.

The threat landscape for the R&I sector

In today's world there are countries that combine authoritarian regimes and the near absence of academic freedom with eminence in research and innovation. This means that researchers should take into account the potential security implications of their research when collaborating with partners in such countries. Risks must be managed and mitigated, not avoided ('de-risking, not decoupling').

Enabling research performers to take risk-informed decisions about their international collaborations requires solid threat and risk analysis. Member States are finding ways to organise such exchanges of information between their intelligence agencies and the research community. In addition, it should be noted that a considerable number of publications on the threat landscape are made publicly available.

Generally speaking, countries to which relevant sanctions apply, which have an authoritarian regime and lack academic freedom pose a high risk of political and military exploitation of research and innovation collaborations. When assessing state-actor threats, a country-agnostic, risk-based approach is advisable. Country-specific policies may lead to discrimination and stigmatisation and to current and future threats from other countries being overlooked.

National approaches to research security

Owing to their responsibility for national security, national authorities have a key role to play in enhancing research security. In line with the Council Recommendation, Member States are currently in the process of developing or strengthening their national approach to research security.

A policy maturity model can be applied to capture the dynamism of the policy process, from the initial phase – through exploration, implementation and integration – to the maintenance phase. While reaching higher levels of policy maturity is advisable, the model does not define the robustness of the measures that are needed.

Among Member States there is clear readiness to get involved in peer-learning and capacity-building activities, at both national and EU level. In recent years there has been a proliferation of such initiatives.

Although Member States differ and no universal blueprint can be prescribed, some general observations can be made about where to start. As a first step, Member States put in place dedicated internal cooperation structures, involving all relevant public authorities ('whole-of-government approach'). Responsibilities, expectations and needs should then be clarified in dialogue with the research and innovation sector. This is the basis for the development of a national approach which ideally includes a road map with deliverables and a timeline ('who does what and when?'). Guidelines and support structures can be put in place as part of the national approach.

The absence of explicitly defined policy frameworks and structures does not necessarily mean that there are no safeguards. Although managing risks on an ad hoc basis may in certain cases seem appealing, it is recommended to move towards a structural approach and to avoid risk mitigation depending on chance and reactive responses to incidents.

→ Case studies presented from FR, NL, CZ, DK, SE, DE, IT, AT, BE, RO and ES

The role of research funders

Research funders also have a crucial role to play when it comes to enhancing research security. Funders can encourage their beneficiaries to assess and mitigate risks through their funding procedures. They can also apply eligibility restrictions to exclude certain types of projects considered high-risk.

Funding organisations across the EU differ in terms of their scope of activities, mandate and autonomy, which determines their risk profile and ability to act. In some cases, the funder's mandate or strategic plan needs to be updated to include research security considerations.

There are a variety of 'safeguarding tools' that research funders can apply. These include safeguards at project level, where each project selected for funding goes through a security screening process. At the level of calls for proposals, the funder can apply eligibility restrictions to rule out certain categories of projects that are considered particularly risky.

Another possibility is that the beneficiary is asked by the funder to demonstrate that it has a credible risk management system in place to address the risks related to a project selected for funding. Lastly, funders can set transparency obligations, requiring beneficiaries to

disclose any relevant (non-EU) funding sources and (non-EU) affiliations of staff involved in the project.

Across the EU, research funders are introducing such safeguards, while there are still bottlenecks which are often related to mandates and resources.

→ Case studies presented from BE, FI, DE, SI, NL, FR and LU

The research and innovation sector

Research performing organisations are at the heart of any effective research security policy. In line with academic freedom and institutional autonomy, they are primarily responsible for assessing and addressing potential risks of their cooperation with international partners.

Across the EU there is a vast variety of research performing organisations, with differences in size, specialisation and types of research – and thus in risk profiles. Many are in the process of working on research security initiatives and are introducing internal procedures to assess and sign off partnerships and projects with a high-risk profile.

Given the differences between research performing organisations, it is important to underline that any risk appraisal should start with a self-assessment of the organisation's risk profile. The question of *what* to protect precedes the question of *how* to do so.

Research performing organisations are then recommended to assign responsibility for research security within the organisation and to work on devising an internal risk management process to identify 'red flags' and act on them.

In practice, it may be possible to build on existing processes, such as those for compliance with export control rules or for the review of ethics in research projects and cooperations. Measures to protect social safety may also be relevant.

Research and innovation stakeholder associations, both at European and national level, are actively contributing to the debate on research security. They offer platforms for peer learning and the formulation of positions as input for EU and national policymaking.

→ Case studies presented from DK, EE, ES, NL, SE, DE, CZ, FI, SI, IE and PT

EU-level initiatives

EU-level initiatives support Member States and the research and innovation sector to develop their approaches to research security and to promote consistency across the EU, thus contributing to the effectiveness of safeguarding measures and a level playing field within the EU.

The EU's approach to research security is part of a broader effort to raise awareness and build resilience against threats to the security of the Union and its Member States, in particular the European economic security strategy ([2]). As such, research security initiatives complement policy instruments such as export control, foreign direct investment screening and sanctions.

([2]) https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3358

Following the adoption of the Council Recommendation on enhancing research security, the Commission launched dedicated networks of Member State experts, national research funding organisations and European stakeholder associations. Research security is a priority action of the European Research Area (ERA) policy agenda 2025-2027 enabling the ERA governance structures to be fully exploited.

In October 2025 the Commission, together with the R&I sector, organised the first European Flagship Conference on Research Security, bringing together around 500 policymakers, practitioners and experts from Europe and beyond. At the same time, preparatory work is being done to set up a European Centre of Expertise on Research Security, which will strengthen the evidence base and create a community of practice around the topic.

As requested by the Council in its recommendation, several key initiatives are being launched, including developing a resilience-testing methodology, a secure due diligence platform, interpretative guidance and critical technology risk assessments and ensuring that the right safeguards are applied in the framework programme for R&I Horizon Europe. The Commission has also stepped up its engagement on research security with international partners, both bilaterally and multilaterally, to share experiences but also to seek alignment of approaches.

Concluding remarks

The work started in 2024 through the Council Recommendation on enhancing research security has provided the Member States and the research and innovation community with a reference point with guidance on what an effective and proportionate policy response might look like. It has created political momentum for Member States and the sector to introduce or strengthen research security measures.

There is broad support for what may be called the European approach to research security, one that is about keeping international research and innovation both open and secure. This is an approach based on the notion that research performers bear primary responsibility for ensuring research security in their international engagements (‘with academic freedom comes academic responsibility’). To shoulder this responsibility in a meaningful way, research performers need help from public authorities, who should share (threat) information and provide guidance and support. Respect for core academic values, such as academic freedom, is essential for continued support from the sector.

Policy maturity levels differ greatly between and within Member States. More action must therefore urgently be taken at all levels by national authorities, research funders and research performers. The Commission will continue to support the Member States and the sector through a range of key initiatives. This will allow the EU and its Member States to reach higher levels of policy maturity more quickly. This is a shared commitment and responsibility.

1. INTRODUCTION

In today's international context, researchers need to take the security implications of their work carefully into account. In 2024 the EU took important steps to address this, by developing a reference point for research security with common definitions, shared principles and guidance on what an effective and proportionate policy response enhancing research security looks like. It subsequently launched a process to promote and support the implementation.

This first Research Security Monitor 2025 provides a qualitative baseline of research security policies and measures across the EU and aims to inform and inspire policymakers and practitioners who are in the process of developing such measures and policies.

1.1. Research and innovation in a volatile geopolitical context

In an international context with growing tensions and increasing geopolitical relevance of research and innovation, all parts of the economy and society are exposed to risks related to international cooperation. However, the research and innovation sector is particularly vulnerable to such threats, because it has openness and borderless cooperation in its DNA.

Moreover, while academic freedom may be a cornerstone for research performers in the EU, there are also countries where academic freedom hardly exists, with research being instrumentalised for political and military purposes. This is a factor that must be considered when collaborating with researchers in those countries.

It is in this dynamic and challenging context that universities and other research performing organisations are navigating grey areas: cooperation with a specific international partner may not be prohibited, but is it desirable? How do we ensure that international research and innovation cooperation is open *and* secure?

The development and adoption of the Council Recommendation on enhancing research security ('the Council Recommendation') in 2024 was an important step, creating additional momentum across the EU to take measures to raise awareness and build resilience against risks related to international research and innovation collaboration.

The European Commission ('the Commission') tabled its proposal for a Council recommendation in January 2024 ([3]) as part of a package of proposals presented in the context of its European economic security strategy, which it launched in June 2023 ([4]). After negotiations between the Member States, the Council Recommendation was unanimously adopted by the Council of the European Union ('the Council') in May 2024 ([5]).

The Council Recommendation builds on the global approach to research and innovation, the EU's strategy for international cooperation presented in 2021 ([6]) – with its principles

([3]) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52024DC0026
([4]) https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3358
([5]) https://eur-lex.europa.eu/eli/C/2024/3510/oj/eng
([6]) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021DC0252

of preserving openness, promoting a level playing field and reciprocity and pursuing modulated bilateral cooperation internationally – and subsequent work done to safeguard European research and innovation, such as the publication of the Commission staff working document 'Tackling R&I foreign interference' in 2022 ([7]).

1.2. Key elements of the Council Recommendation

Although the Council Recommendation is not legally binding, it has clear political significance. With it, the EU has a politically endorsed common reference point agreed by all 27 Member States with definitions, shared principles and guidance on what an effective and proportionate policy response enhancing research security looks like.

It is built on enhanced self-governance: research performers are primarily responsible – 'with academic freedom comes academic responsibility' – but in combination with public authorities that empower the sector to take informed decisions by providing information, guidance and support.

At national level, public authorities, research funders and research performers are specifically addressed, underlining the fact that this is a collective endeavour where each governance level has a specific contribution to make.

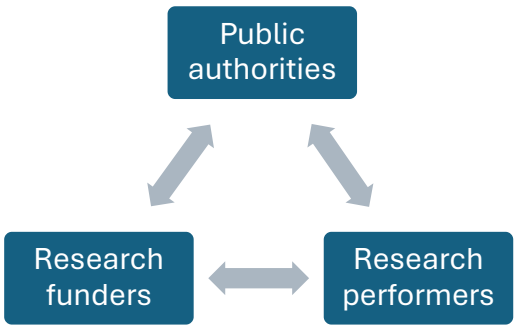

Figure 1: Main actors for research security at national level

The Council Recommendation also addresses the Commission, requesting it to support the implementation of the Council Recommendation by facilitating peer learning between Member States and by developing a number of EU-level initiatives.

In terms of definitions, the Council Recommendation describes research security as a broad phenomenon, covering risks related to international cooperation:

What is research security?

'Research security' refers to anticipating and managing risks related to:

(a) the undesirable transfer of critical knowledge and technology that may affect the security of the Union and its Member States, for instance if channelled to military or intelligence purposes in third countries;

([7]) https://data.europa.eu/doi/10.2777/513746

(b) malign influence on research where research can be instrumentalised by or from third countries in order to inter alia create disinformation or incite self-censorship among students and researchers infringing academic freedom and research integrity in the Union;
(c) ethical or integrity violations, where knowledge and technologies are used to suppress, infringe on or undermine Union values and fundamental rights, as defined in the Treaties ([8]).

It should be noted that this definition goes beyond the issue of 'leakage' of sensitive technologies, a domain it shares with export control ([9]), to also include issues that could affect academic freedom (e.g. foreign interference leading to self-censorship), research integrity (e.g. due to overdependence on a single funding source or partnership) and ethics.

Taken together, these aspects lead to a comprehensive concept of research security, one that calls for a variety of security aspects to be taken into account in international cooperation and the internationalisation of European research and innovation. It is also a concept for which the mere application of the law is insufficient: certain international collaborations may be legally permissible, but still undesirable from a research security perspective.

Framework conditions for research security policies

Another key element of the Council Recommendation is that it lists principles for responsible internationalisation, which are to be read as framework conditions for designing and implementing policy actions to enhance research security.

These principles include ([10]):

- promotion and defence of academic freedom and institutional autonomy, taking into account the fact that research performing organisations are primarily responsible for their international research and innovation cooperation;
- promotion and encouragement of international cooperation in research and innovation that is both open and secure;
- proportionality of safeguarding measures, with the understanding that the objective is to manage rather than to avoid risk;
- promotion of self-governance in the research and innovation sector ('with academic freedom comes academic responsibility'), while empowering its actors to take risk-informed decisions;
- adoption of a whole-of-government approach, bringing together relevant expertise, ensuring a comprehensive approach and fostering coherence of governmental actions;
- adoption of policies that are country-agnostic, identifying and addressing risks to research security wherever they emanate from (risk-based approach);
- avoidance of all forms of direct and indirect discrimination and stigmatisation of groups or individuals;

([8]) Recital 18(1).
([9]) EU control system for the export of dual-use items (i.e. goods, software and technology): https://policy.trade.ec.europa.eu/help-exporters-and-importers/exporting-dual-use-items_en
([10]) Recommendation 1.

- adoption of a learning approach, acknowledging the dynamic nature of research security shaped by new insights, evolving risks and geopolitical context.

Application of these principles should result in policy measures that are not only effective and proportionate, but also legally viable and tailor-made for the scientific community.

How to perform a research security risk appraisal

Carrying out a risk appraisal of an activity, be it a research project or international partnership, is fundamental to any research security policy or measure. Given its prominence, the Council Recommendation provides a detailed explanation of what is meant when we recommend that our researchers assess risks.

In essence, 'risk appraisal' refers to a process that takes into account a combination of four main risk factors. It is the combination of those risk factors that determines the risk level of any given international cooperation ([11]).

Box text: Main risk factors to be assessed in a risk appraisal

1. the **risk profile** of the Union-based organisation entering into the international cooperation: consider the organisation's strengths and vulnerabilities, including financial dependencies, relevant to the research project;
2. the **research and innovation domain** in which the international cooperation is to take place: consider whether the project focuses on research domains involving critical knowledge and technology, methodologies, data or research infrastructures considered particularly sensitive from a security or Union values and fundamental rights perspective, also taking into account its technology readiness level (TRL);
3. the **risk profile of the third country** where the international partner is based or from where it is owned or controlled (for example, whether the country is subject to restrictive measures or whether it has a flawed rule-of-law or human rights protection track record, an aggressive civil-military fusion strategy or limited academic freedom);
4. the **risk profile of the international partner organisation**, namely – to perform due diligence on the organisation to be cooperated with to determine inter alia whether it is subject to restrictive measures or has links to the military, the affiliations of the researchers or of staff involved, as well as the partner's intentions regarding the end-use or application of the research results.

In addition to its fact sheet on building blocks for risk appraisal ([12]), the Commission is developing a practical guidance note on research security risk appraisal, which is expected to be published in 2026, to provide further clarification to those involved in assessing risks of international R&I cooperation.

1.3. About this publication

The publication of the Research Security Monitor follows a request by the Council, which invited the Commission to monitor the progress made in implementing the Council Recommendation and to report to the Council every two years as part of its biennial

([11]) Recital 18(5).
([12]) https://research-and-innovation.ec.europa.eu/document/c0c0dbae-c7d7-45d8-b59b-413f54aa8983_en

reporting on the global approach to research and innovation ([13]). Member States are in turn invited to share information about their national approach to research security with the Commission, as input for its monitoring and reporting activities ([14]).

The objective of this first Research Security Monitor is to provide a qualitative baseline for research security policies and measures across the EU. In addition to a detailed update on initiatives at EU level (recommendations 16 to 26), the report will give an overview of measures taken or planned by national administrations (recommendations 2 to 13), national research funders (recommendation 14) and the R&I sector (recommendation 15).

The Research Security Monitor aims to inform and inspire policymakers and practitioners in the EU and beyond who are in the process of developing measures and policies. The focus is on highlighting interesting initiatives and actions, rather than on exposing remaining gaps and vulnerabilities. Its objective is to give visibility to the fact that across the EU, national authorities, research funders and the R&I sector are taking steps to address the issue of research security and that many interesting initiatives already exist. By doing so, its publication helps to maintain political momentum around the topic.

As a Commission staff working document, the Research Security Monitor is a descriptive, policy-based document, not a scientific study. Whereas the Council recommendation outlines a desirable way forward, the Research Security Monitor aims to be factual, descriptive and explanatory, with the Council Recommendation serving as its basis and defining its scope. The Monitor does not announce any new policy initiatives.

In preparation for the Research Security Monitor, qualitative information about the state of play regarding research security policies and practices in all 27 Member States was collected ([15]). This data was collected from each Member State on the basis of desk research supplemented with input from a limited number of interviews with national experts and policymakers. An important consideration for the choice of methodology was also the explicit wish of the Member States to keep their reporting burden low.

It should be borne in mind that this publication comes only one and a half years after the adoption of the Council Recommendation and that in many Member States a national approach to research security is still being developed. This means that, by the time of its publication, parts of this Research Security Monitor may already be outdated or superseded by new initiatives. If the current pace of policy development is maintained, it is likely that a more quantitative in-depth methodology may be applied in a subsequent edition of this publication.

1.4. Structure of the text

Rather than presenting national approaches country by country, this Research Security Monitor seeks to present good practices and initiatives by governance level. This corresponds to the approach taken in the Council Recommendation, which addresses the different stakeholders (national authorities, national research funders and research performing organisations as well as the European Commission) separately.

([13]) Recommendation 27.
([14]) Recommendation 28.
([15]) Information collected during first half of 2025. No input/feedback was received from Croatia.

First, Chapter 2 gives an outline of the threat landscape of the research and innovation sector. In Chapter 3, the development of national approaches by Member States – as defined by national authorities – is depicted. Chapter 4 zooms in on the role of national research funders within the national R&I system. Chapter 5 then focuses on initiatives by the research and innovation sector itself, with initiatives from both EU and national stakeholder organisations as well as individual research performing organisations. After this, Chapter 6 presents the initiatives at EU level to support Member States and the sector implement the Council Recommendation. Lastly, the Research Security Monitor's main findings and conclusions are set out in Chapter 7.

2. THREAT LANDSCAPE FOR THE R&I SECTOR

In today's world there are countries that combine authoritarian regimes and the near absence of academic freedom with eminence in research and innovation. Researchers should take into account the potential security implications of their research.

Enabling research performers to take risk-informed decisions about their international collaborations requires solid threat and risk analysis. Member States are finding ways to organise such exchanges of information between security analysts and the research community.

2.1. Why cooperate with researchers in high-risk countries?

In its Recommendation, the Council observes that growing strategic competition and the return to power politics are leading to increasingly transactional international relations. Critical knowledge and technology play a pivotal role in political, economic, intelligence and military pre-eminence. This combination has led some of our competitors to 'increasingly [advance] their capabilities in this respect or actively [pursue] civil-military fusion strategies.' ([16]) It stresses the importance of systematically assessing hybrid threats affecting the research and innovation ecosystem in order to enhance situational awareness among policymakers ([17]).

The Council recommends that Member States strengthen the evidence base for research security policymaking through analysis of the threat landscape ([18]) and that the Commission enhance situational awareness among policymakers by structurally assessing hybrid threats affecting the Union's research and innovation ecosystem ([19]).

This raises the question of whether such risks should be taken at all. In his 2024 report ([20]), Manuel Heitor explains that 'In a changed and complex world, European companies and researchers need to operate in key markets and cooperate with the best scientists even when they are in countries with which the EU competes politically, economically, technologically or militarily.'

This is not a new idea and there are valid reasons for pursuing it. It is best for the advancement of science. Science thrives when talents from around the world can work together, unhindered and with full openness and academic freedom. In addition, there are important (science) diplomacy considerations to 'keep doors open' and continue the dialogue also with countries that may not share the European Union's views and values.

While this continues to hold, recent developments have brought about what may be considered a paradigm shift, with consequences for international research and innovation.

([16]) Recital 4.
([17]) Recital 14.
([18]) Recommendation 5.
([19]) Recommendation 19.
([20]) *Align, act, accelerate* – Publications Office of the EU (2024) – Recommendation 11: Adopt a nuanced, granular and purpose-driven approach to international cooperation.

At the end of the Cold War, there was widespread confidence that the world was on an inevitable path towards democracy and a free market economy ([21]). Academic cooperation was expected to speed up this process. In recent years, however, it has turned out that this belief in 'democratic change through cooperation' had been overly optimistic as authoritarian regimes consolidated and became more assertive, challenging the western model of democracy. The combination of having an authoritarian regime that curtails academic freedom while at the same time being an innovative and scientific front runner was previously inconceivable – but it happened, nevertheless. This has led the EU to rethink its approach to international R&I cooperation, as evidenced by the global approach to research and innovation, published in 2021.

Accordingly, the matter of how to cooperate with partners in such countries emerged as an important consideration. It cannot be academic business as usual, because the partner has limited academic freedom, which could undermine the research integrity of the joint work, to begin with. In addition, there are security concerns too. The key here is that we should de-risk, not decouple, and that we manage and mitigate risk, rather than avoiding risk altogether. We must be open *and* secure.

To do this effectively and proportionally, it is crucial to have a clear-eyed view of the risks and threats posed by different countries. The better able we are to assess the potential impact and the likelihood of the occurrence of those risks, the more targeted and proportionate our safeguards can be. A dedicated and country-specific, or even actor-specific, analysis of the threat landscape is called for.

2.2. Cooperation between security and intelligence agencies and the R&I sector

Having detailed insight into the threat landscape may require access to sensitive information, which may be classified. At national level, it requires cooperation between intelligence agencies, on the one hand, and research policymakers and practitioners, on the other, to be established or strengthened.

The Council recommends that Member States 'facilitate information exchange between research performing organisations and research funding organisations on the one hand and intelligence agencies on the other hand, for example through classified and non-classified briefings or dedicated liaison officers' ([22]).

Establishing or strengthening a working relationship between the research ministry (and by extension the R&I community) and the national intelligence services is a crucial step, as it brings the expertise needed to assess and address security risks and a deep understanding of how the R&I sector works together. Such cooperation exists in several Member States. Some examples:

Portugal: In March 2025 a dedicated Unit for Science, Technology and Emerging Areas within the Portuguese Security Intelligence Service (SIS) was set up. This new unit monitors risks associated with international partnerships, misappropriation of intellectual property and the undue transfer of sensitive research results. It also supports research

([21]) *Risky Business: Rethinking Research Cooperation and Exchange with Non-Democracies* – GPPi (2020) – 'Introduction', 'Paradigm Lost'.

([22]) Recommendation 6.

institutions in identifying and responding to threats such as espionage, sabotage and foreign interference. Furthermore, exploratory discussions involving SIS, the Council of Rectors of Portuguese Universities (CRUP) and the Council of Associate Laboratories (CLA) are being held to draw up shared guidelines and promote a more coherent and consistent approach to managing research security risks.

Czechia: In Czechia the Security Information Service (BIS) publishes annual reports that includee, among other things, information relevant to research security. Since 2023 the Ministry of Education, Youth and Sports (MŠMT) has invited BIS, along with other actors from the security sector, to participate in a series of events aimed at raising awareness of risks associated with the research environment. In addition, BIS organises educational and outreach activities specifically designed for research institutions to strengthen security awareness.

Denmark: A defining feature of the Danish approach to research security is the proactive collaboration between universities, ministries and national intelligence services. Regular engagement with intelligence services helps universities assess threats effectively, while cooperation with ministries supports the development of common procedures and shared legal interpretations. Recognising that geopolitical tensions increasingly impact academia, the Danish Security and Intelligence Service (PET) has stepped up its advisory efforts targeted at Danish universities and research institutions. To facilitate ongoing dialogue, PET has set up a partnership called 'Dialogforum', bringing together administrative and leadership representatives from all Danish universities, the Ministry of Higher Education and Science (UFM) and the organisation Danske Universiteter. This platform allows institutions to receive intelligence-based guidance and share best practices for protecting research from foreign interference.

Finland: In Finland the Security and Intelligence Service (SUPO) plays a vital supporting role by providing national security intelligence, including analysis of foreign influence operations, espionage risks and hybrid threats that affect Finnish institutions. Its insights inform government-wide assessments of the research sector's exposure to strategic threats, such as foreign state actors' attempts to access sensitive data or critical technologies. This intelligence is used to guide strategic policy documents, such as the *Security Strategy for Society* (2025) ([23]).

France: The General-Directorate for Internal Security (DGSI), the French special intelligence service under the authority of the Ministry of Interior, maintains regular relations with the research community to detect and prevent attempts at interference. DGSI's economic security mission for the research sector has been strengthened since 2021. Interministerial coordination is carried out under the authority of the General Secretariat for Defence and National Security (SGDSN), which reports to the Prime Minister.

The Netherlands: As part of a comprehensive national approach to research security, the Dutch general and military intelligence and security agencies (AIVD and MIVD) actively contribute to the National Contact Point for Research Security (see also Section 3.4), set

([23]) https://julkaisut.valtioneuvosto.fi/handle/10024/166026

up in 2022, where researchers can obtain guidance on security-related issues in foreign collaborations.

2.3. Using public sources analysing the threat landscape

At the same time, a considerable amount of relevant information and analysis is publicly available. These public sources are also important because they can provide input for the justification for requiring the application of safeguards or the decision not to fund a research project proposal.

Obvious examples are legal obligations such as the EU restrictive measures (sanctions) ([24]). Other open sources such as the academic freedom index ([25]) can help indicate that research and innovation cooperation with a partner in a country requires extra attention or caution. In addition, security and intelligence agencies across the EU publish annual reports and targeted publications that describe the threats confronting the country in some detail.

Box text: Examples of open-source publications on the threat landscape

Examples of national security strategies

- **Germany** (2023): National Security Strategy of the Federal Republic of Germany (EN)
- **Czechia** (2023): Security Strategy of the Czech Republic 2023 | Ministry of Foreign Affairs of the Czech Republic
- **France** (2025): National Intelligence Strategy

Examples of annual reports

- **Belgium**, VSSE (2025): Intelligence Report 2025 in English | VSSE
- **Austria**, Verfassungsschutzbericht (2024): Publikationen (in German)
- **Finland**, SUPO (2025): National Security Overview | Supo
- **Lithuania**, National Threat Assessment (2025): Lietuvos Respublikos valstybės saugumo departamentas

Examples of targeted publications

- **The Netherlands**, AIVD (2025): Threat Assessment of State Actors 2025 | Publication | AIVD
- **France**, DGSI: Conseils aux entreprises : Flash ingérence | Direction Générale de la Sécurité Intérieure ('Flash ingérence', in French)

Also at European level, several resources are available:

- **European External Action Service** (2025): 3rd EEAS Report on Foreign Information Manipulation and Interference Threats | EEAS
- **European Commission**, Joint Research Centre (2022): China 2.0 – Publications Office of the EU
- **Hybrid Centre of Excellence**: Publications – Hybrid CoE – European Centre of Excellence for Countering Hybrid Threats; collection of trend reports, working papers, etc.

In addition, there are relevant strategic policy documents, such as:

- **European External Action Service** (2025): ProtectEU: a European Internal Security Strategy

([24]) For an overview, see the EU Sanctions Map: https://www.sanctionsmap.eu
([25]) https://academic-freedom-index.net

- **European External Action Service** (2022): Strategic Compass and its 2024 annual progress report: 2024 Progress Report on the Implementation of the Strategic Compass for Security and Defence | EEAS

While there are good practices available from several intelligence agencies, with reports that contain substantial R&I-relevant threat analysis, more in-depth threat analysis is needed, at both national and EU level, as recommended by the Council Recommendation.

Further investments in expertise and networks are needed as a basis for developing policies but also as a basis for justifying restrictions and negative decisions.

2.4. Assessing state-actor threats

Geopolitical shifts, such as growing strategic competition and the return to power politics, have resulted in threats that are diverse, unpredictable and often hybrid. A threat is hybrid when an actor exploits vulnerabilities to its own advantage using a mixture of diplomatic, military, economic and/or technological measures, while remaining below the threshold of formal warfare ([26]).

Since, in today's world, critical knowledge and technology play a crucial role in gaining political, economic, intelligence and military pre-eminence, actors are increasingly advancing their capabilities to obtain such knowledge and technology or are actively pursuing civil-military fusion strategies ([27]). It is against this background that the risk profile of a prospective partner should be assessed.

A clear risk indicator or 'red flag' is the existence of EU restrictive measures (sanctions) against the country, especially when these include prohibitions on the transfer of goods, knowledge or technical assistance in certain technology domains.

A more general rule of thumb might be that a country with an authoritarian regime that lacks democracy and rule of law and in which researchers have limited or no academic freedom ([28]) poses a higher risk of political and military exploitation of its research and innovation collaborations. There is a heightened probability of a hidden agenda driving the seemingly bona fide academic cooperation.

It should, however, be emphasised that, while a limited number of threat actors may be most visible and active, this should not give rise to policies that focus exclusively on those countries. In line with the Council Recommendation, a risk-based, country-agnostic approach is advisable.

A country-specific approach, singling out one or more countries, has two important downsides. On the one hand, fixation on one or more countries may result in current and future threats from other countries and sources being overlooked. On the other hand, it could lead to an overreaction: to a general raising of suspicion – which can easily result in stigmatisation of and discrimination against certain groups or ethnicities.

([26]) Communication, Joint Framework on countering hybrid threats – a European Union response, (JOIN/2016/018): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016JC0018

([27]) Recital 4.

([28]) To obtain an indication of whether this is the case, one could consult international indices and rankings, such as the academic freedom index: https://academic-freedom-index.net/

3. NATIONAL APPROACHES TO RESEARCH SECURITY

Owing to their responsibility for national security, national authorities have a key role to play in enhancing research security. They should do so in dialogue with the research and innovation sector. In line with the Council Recommendation, Member States are in the process of developing or strengthening their national approaches to research security. In doing so, they often encounter dilemmas and barriers. Peer-learning and capacity-building initiatives within and between Member States could help address these.

3.1. Recommendations: What is expected of national authorities?

As outlined in the Council Recommendation, national authorities are recommended to develop and implement a coherent set of policy actions and to enter into a dialogue with their R&I sector with the aim of developing a national approach to research security, clarifying the different actors' responsibilities and roles ([29]).

Furthermore, national authorities should put in place support services to help the research and innovation sector take risk-informed decisions about their international collaborations. This support could include providing relevant information, guidance and advice to identify and manage risks as well as awareness-raising activities and training courses ([30]).

It is important that national authorities work closely together across policy areas and invest in the analysis of the threat landscape for the research and innovation sector, as discussed in Chapter 2 ([31]). In that context, they should take national measures to ensure compliance with relevant EU export control rules and EU restrictive measures (sanctions) ([32]).

Regular testing of the sector's resilience and incident simulations are recommended as ways of gaining practical insight into the effectiveness and proportionality of the national measures ([33]).

3.2. Policy maturity model

The Council Recommendation states that enhancing research security requires a sustained effort over a longer period and it involves both cultural and behavioural change to raise awareness and build resilience to research security risks.

To capture such an evolving and dynamic policy process, a policy maturity model which takes the starting points of the different countries and various parts of the ecosystem into account can be applied as an analytical framework. The model describes the development and introduction of research security policies as a phased approach, moving towards higher levels of maturity.

Although differences between maturity models exist, the models broadly distinguish the

([29]) Recommendations 3.
([30]) Recommendations 4.
([31]) Recommendations 5, 6 and 7.
([32]) Recommendation 10.
([33]) Recommendation 8.

following phases ([34]):

1. Initial phase	Limited awareness, incident-driven ad hoc fixes, low consistency, reliance on individuals
2. Exploratory phase	Some awareness, developing a more structural approach, defining concepts and possible responses, establishing new working relations
3. Implementation phase	Project-based approach, introducing measures and support structures, capacity building, investing in resources, awareness campaigns
4. Integration phase	Structurally embedding safeguards in existing processes, continued development, taking a learning approach, broad awareness
5. Maintenance phase	Assessing and auditing effectiveness, stress testing, updating and adjusting and periodic refreshing of awareness

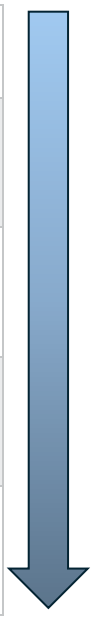

Figure 2: Research security policy maturity model

When applying the maturity levels, there can be differences *between* countries as well as *within* countries, with some governance levels or parts of the R&I ecosystem being more advanced than others.

Another important observation is that while reaching an adequate level of maturity is necessary, it does not define the intensity or robustness of the measures. This means that whereas in some cases a light-touch approach – with minor recalibration of existing systems and practices – should be sufficient, other cases may require the introduction of new dedicated systems and procedures.

3.3. Getting started with research security at national level

Across the EU, a growing awareness of research security risks can be observed. However, important challenges and bottlenecks persist, including, in some cases, a perceived lack of exposure, and more generally a lack of resources and expertise in terms of both funding and human resources.

Among Member States, there is a clear willingness to get involved in initiatives that encourage peer learning and capacity building – be it at national level, organised by public authorities or the sector itself, or internationally, organised by EU-level stakeholder associations, individual Member States, international partners and platforms or the Commission. In recent years, there has been a multiplication of such initiatives.

([34]) ARMA, 2023, Trusted-Report_Booklet_v7.pdf, p. 18; UNL, 2024, UNL Capability Maturity Model Knowledge Security ENG-DEF.pdf, p. 5; University of Manchester, 2025, Manchester_study_2025_EUROPEAN_RESEARCH_SECURITY_THREATS_AND_RESPONSES.pdf, p. 31.

Although the systems and starting positions differ from country to country and no blueprint can be prescribed, some general observations can be made about how Member States tend to start organising their national processes to address research security.

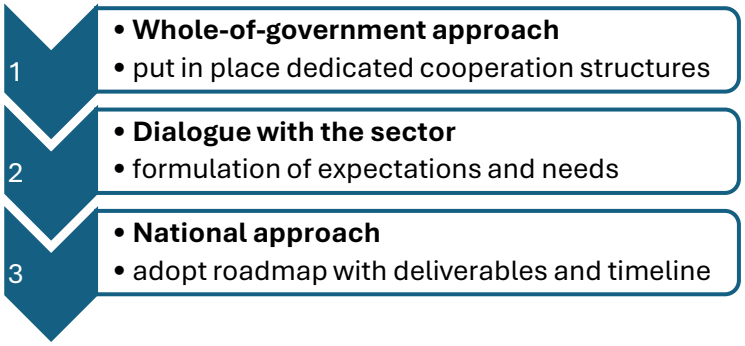

Figure 3: Steps towards the development of a national approach

1. Whole-of-government approach. As a first step, a whole-of-government approach needs to be put in place, involving key policymakers and setting up coordination and an information exchange. In practice it is often the case that the Ministry responsible for Research Policy takes the lead, and that the Ministries of Economic Affairs, Foreign Affairs and Trade and the intelligence agencies are closely involved. Other public authorities may be involved and, depending on national circumstances, variations exist. Giving the Ministry of Research a coordinating role is justified by the fact it has a deep understanding of the sector, which is needed to drive behavioural change effectively.

Given the complexity and multifaceted character of the issue, a programmatic approach based on a temporary structure, such as a task force or project group, may be advisable in a first phase. A more flexible structure also provides the necessary agility and helps to embrace a learning approach.

2. Dialogue with the sector. As a second step, roles and responsibilities need to be clarified between the national authorities and the R&I sector. Research performers have a clear responsibility based on their institutional autonomy and academic freedom. However, they need to accept the public authorities' responsibility to protect national security. At the same time, measures to protect national security should be proportionate and respect academic freedom. In short, a balance should be struck, and this should be done in dialogue.

Expectations and needs can be formulated and addressed in that dialogue. What do authorities expect from research performers? What support is needed for the research performers to take responsibility in a meaningful way? What changes, if any, are needed to the national regulatory framework? What resources and investments are needed and who bears the costs?

3. National approach. These two steps lead to a third step, in which the national approach is developed and agreed. This could take the form of a national road map or action plan containing a set of commitments between the authorities and the sector. Ideally, it includes clear deliverables and a timeline. In essence, it specifies who should do what and by when.

The next steps following this include drawing up (national) guidelines and reflecting and deciding on what support structure is needed to assist the sector. Other issues that might be considered are the conclusion of administrative agreements, changes to the regulatory framework, including mandates of agencies, audits and reporting obligations, the joint development of tools and the setting-up of a community of practice and awareness-raising campaigns.

Although taking such a step-by-step approach to developing and introducing research security policies has evident advantages, the absence of explicitly defined policy frameworks and structures does not necessarily mean that there are no security-related safeguards or risk assessments. It might, for instance, be that risks are identified and managed on an ad hoc basis depending on individual contacts and networks within and between the administration and research-performing organisations.

Notably in smaller Member States with a limited number of research performing organisations and/or limited international exposure this may seem appealing from a proportionality point of view. It is nevertheless recommended to move towards a structural and coherent approach and not make the identification and mitigation of risks that can potentially affect the security of the EU and its Member States dependent on chance and reactive responses to incidents.

3.4. Case studies: Developing a national approach

This chapter presents a couple of examples of how different Member States are working on developing their national approaches. On the one hand, it shows the diversity across the EU and reflects the differences between national political systems and traditions. On the other, it contains a wealth of initiatives and measures that could serve as a source of inspiration to others.

The chapter also shows the differences in terms of policy maturity, with many Member States still in a phase of exploration and implementation (phases 2 and 3 in Table 1) and only a few already having reached the integration and maintenance phases (phases 4 and 5). Among the Member States not referred to in this chapter are countries that are still in the initial phase (phase 1) and that would benefit greatly from peer learning and capacity building.

France: A cornerstone of France's research security architecture is the 'protection of the nation's scientific and technical potential' (PPST) framework, set up in 2011 ([35]). It is a sophisticated, law-based framework to protect sensitive research facilities and activities. Headed and coordinated by the General Secretariat for Defence and National Security (SGDSN), which reports to the Prime Minister, the PPST spans six ministries and involves both public and private research institutions. Within each ministry, a senior defence and security officer service, the High Official for Defence and Security (HFDS), is appointed. This interministerial framework reflects a high level of national oversight. The French Ministry of Higher Education, Research and Space (MESRE) is the main institution for

([35]) https://www.sgdsn.gouv.fr/nos-missions/proteger/proteger-le-potentiel-scientifique-et-technique-de-la-nation

research security in the public sector. It promotes international scientific cooperation while actively safeguarding national interests.

PPST provides legal and administrative protection based on the control of access, both physical and virtual, to sensitive information held within protected areas known as restricted zones (ZRRs). These are defined spaces inside research performing organisations within which sensitive research or production activities take place which must be protected.

A peer review process, involving members of the scientific community and the administration, is used to evaluate the sensitivity of research activities and to recommend the application of the PPST to a lab.

Within each research institution to which the PPST applies there is a Security and Defence Officer (FSD), linked to the HFDS. The General-Directorate for Internal Security (DGSI) maintains regular relations with the research community to detect and prevent attempts at interference (see also Section 2.2).

In 2024 the PPST was reinforced ([36]) with the introduction of sanctions for breaches of the obligations relating to the protection and implementation of restricted areas and any obstruction of the duties of personnel responsible for safeguarding such areas. The procedures for granting authorisation to access restricted zones were also simplified and clarified.

Another important update is the introduction of a dedicated strategic objective for the public research and innovation sector in the *National Strategic Review* ([37]) of July 2025. Contributing to goals of European and national economic and technological sovereignty, the strategic objective contains actions on the protection of research against capture, the supervision of international cooperation and raising awareness of the risks of interference in higher education and research.

The Netherlands: In 2020 the Netherlands started developing a comprehensive national approach to research security, as a joint initiative of the ministries responsible for education and research, economic affairs and justice ([38]). A governance structure for dialogue with the sector was established, through regular dedicated meetings with the main stakeholder organisations representing research universities (UNL), universities of applied research (VH), university medical centres (NFU), applied research institutes (TO2 federation), the national research funder (NWO) and the academy of science (KNAW).

Subsequently, in 2022, national guidelines on knowledge security ([39]) were presented jointly by the government and the sector and a National Contact Point for Knowledge

([36]) Decree No 2024-430 of 14 May 2024 containing various provisions relating to the protection of the nation's scientific and technical potential – Legifrance (https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000049535465).

([37]) http://www.sgdsn.gouv.fr/files/files/Publications/20250713_NP_SGDSN_RNS2025_EN_1.pdf

([38]) Letter to Parliament 'Knowledge security in higher education and research', 27.11.2020: https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2020Z23069&did=2020D48724 (in Dutch only).

([39]) National guidelines on knowledge security, 14.1.2022: https://open.overheid.nl/documenten/ronl-5379d1b4f8b9784bf518251032507a965be9c92d/pdf

Security was launched (see box text). In July of the same year, research security had been included in the 2022 Administrative Agreement (*Bestuursakkoord*) of the ministry with all higher education institutions ([40]). It contains commitments such as that each university must ensure that a board member has responsibility for research security, that there is a research security adviser and that measures are taken to raise awareness and build resilience in line with the national guidelines.

Following a baseline audit of all research performing organisations, reports were published providing assessments of the state of play of research security in the sector ([41]). Most recently, the Netherlands has been working on dedicated research security screening to address risks of the undesirable transfer of sensitive knowledge by individual researchers. The proposed 'Knowledge Security Screening Act' would provide for targeted screening of individuals, regardless of nationality, seeking access to domains of knowledge with a high risk to national security. A public consultation on the Act took place in 2025 ([42]).

Box text: National Contact Point for Knowledge Security, the Netherlands

In 2022 the Dutch government launched its *Loket Kennisveiligheid*, a national contact point to support research performing organisations in the Netherlands take risk-informed decisions about their international cooperation ([43]).

Research performing organisations can turn to the contact point for advice on research security-related questions, for instance on institutional collaborations and partnerships, export control and incoming and outgoing international visits. The contact point cannot deal with queries related to individuals. Queries can be submitted through an online form and will be answered without delay, often within two weeks. Advice is non-binding, and the research performer remains responsible at all times.

The contact point consists of a front office in the Netherlands Enterprise Agency (RVO), an agency that implements a wide range of government policies. It handles most queries by itself in line with national guidelines. In the case of complex questions, the back office gets involved. Here, several ministries and intelligence agencies work together to analyse and provide advice on the matter in hand. This ensures that public authorities speak with one voice.

In addition to its advisory task, the contact point set up a learning community in 2023, which provides training courses and network activities. In 2025 an evaluation of the contact point was launched.

Czechia: The Czech approach to research security has developed rapidly in recent years. Until recently it was based primarily on voluntarism and awareness raising. Since 2025, however, universities have been required to report on research security practices in their annual activity reports, and the new Act on Research, Development, Innovation and Knowledge Transfer ([44]) has further strengthened the focus on this area.

The main policymakers are the Ministry of Education, Youth and Sports (MŠMT) and the Ministry of the Interior, which provide guidance, training and expert analysis to higher

([40]) https://open.overheid.nl/documenten/ronl-fcd6dcb389dae70bfc3f39317ee1cf2672b302ba/pdf p.10 (in Dutch only).
([41]) 'Sectorbeeld Universiteiten', 11.9.2023: https://www.rijksoverheid.nl/documenten/rapporten/2023/09/11/bijlage-1-oberon-dialogic-sectorbeeld-kennisveiligheid-universiteiten-2023 and 'Sectorbeeld Hogescholen', 22.12.2023: https://www.rijksoverheid.nl/documenten/rapporten/2024/03/11/kennisveiligheidsbeleid-in-het-hoger-onderwijs-en-onderzoek-sectorbeeld-hogescholen (in Dutch only).
([42]) https://www.internetconsultatie.nl/screeningkennisveiligheid/b1 (in Dutch only).
([43]) https://english.loketkennisveiligheid.nl/
([44]) https://www.e-sbirka.cz/sb/2025/328?zalozka=text (in Czech only).

education institutions (HEIs) and research-performing organisations (RPOs). MŠMT works closely with other government bodies, including the Ministry of Industry and Trade, the National Cyber and Information Security Agency, the Financial Analytical Office, the Customs Administration, the Research, Development and Innovation Council, the Ministry of Foreign Affairs, the Ministry of Defence and other state security agencies.

Key guidance includes the *Counter Foreign Interference Manual* published in 2021 ([45]), supplemented in 2024 with both methodological recommendations on due diligence, risk management and institutional resilience ([46]) and the *Technical Assistance and Intangible Technology Transfer* handbook ([47]).

Coordination and information exchange are supported by the Interdepartmental Working Group for Combating Illegitimate Interference, set up by MŠMT in 2023. Research security has also been integrated into the Jan Amos Comenius operational programme ([48]), providing financial incentives for institutions to implement security measures and build capacity at institutional level.

Denmark: Denmark's research security framework is centred on the 2022 URIS guidelines on international research and innovation cooperation ([49]), which set out requirements for identifying and protecting vital research, screening partners, complying with export control and investment rules and raising awareness among researchers.

In September 2024 the Ministry of Higher Education and Science (UFM) set up a dedicated Research Security Office (Kontoret for Forskningssikkerhed, Databeskyttelse og Informationssikkerhed) to oversee implementation and monitoring of the guidelines across universities and funding organisations. Coordination is further supported by FIKS, a strategic forum under UFM, and 'Dialogforum', a PET-led platform where universities receive intelligence-based guidance on foreign interference risks.

Universities play a central role in implementation, with future agreements between UFM and universities expected to strengthen the dialogue and support the integration of the URIS guidelines into institutional governance. Alongside this, the Danish Security and Intelligence Service (PET) ([50]) provides direct support through briefings, training, screening advice and dedicated initiatives such as the Quantum Security Forum. Export control and investment screening are managed by the Danish Business Authority ([51]), ensuring alignment with EU regulations.

Sweden: In 2023 the government tasked the Swedish Research Council, innovation funder Vinnova and the Swedish Council for Higher Education with developing proposals on

([45]) https://mv.gov.cz/chh/clanek/protivlivovy-manual-pro-sektor-vysokych-skol.aspx
([46]) https://msmt.gov.cz/vyzkum-a-vyvoj-2/dokumenty-2
([47]) https://www.fau.gov.cz/assets/en/cmsmedia/en/prirucka-technicke-pomoci-a-nehmotneho-p.pdf (2021, updated 2024).
([48]) Jan Amos Comenius OP maintained by the Ministry of Education, Youth and Sports: https://opjak.cz/en/
([49]) https://ufm.dk/publikationer/2022/afrapportering-udvalg-om-retningslinjer-for-internationalt-forsknings-og-innovationssamarbejde
([50]) Danish Security and Intelligence Service. Knowledge Security. Retrieved from https://pet.dk/en/security-advisory-services/knowledge-security
([51]) Danish Business Authority. Legal Basis for Export Control. Retrieved from https://eksportkontrol.erhvervsstyrelsen.dk/lovgrundlag-for-eksportkontrol

responsible internationalisation in higher education, research and innovation. Their assignment included both drafting national guidelines and providing advice on a support structure for the sector.

In 2024 these organisations first presented a proposal for national guidelines ([52]), structured around three levels of responsibility – policies, national guidelines and institution-specific guidelines – with recommendations across five key dimensions, from the Swedish and foreign context to risk assessment of partners and collaboration design. Building on this, the government has given the organisations further assignments on implementing the guidelines.

In a second advice ([53]), it was suggested to create a coordination hub which would provide training and guidance, monitor international developments and supply practical tools such as checklists and risk assessment templates.

Meanwhile, several universities, as well as sector bodies such as SUHF ([54]) and STINT ([55]), have already published guidelines and checklists to support responsible engagement.

Germany: Germany has several relevant policies in place, in particular in the areas of export control (through the Foreign Trade and Payments Act) and ethics, where commissions for the ethics of security-relevant research (KEFs) have been set up at universities and research institutions.

Building on this, a formal stakeholder process was launched in 2024 by the Federal Ministry of Education and Research on the basis of a position paper ([56]), with the aim of developing a national approach to research security, which includes a national risk assessment, a national platform for information and advice and research on research security to strengthen the evidence base for policymaking.

In 2025 several key policy initiatives have reinforced this trajectory. The Conference of Science Ministers, under the aegis of the Standing Conference of the Ministers for Education and Cultural Affairs (KMK), adopted a policy paper explicitly addressing research security ([57]) and the German Science and Humanities Council (Wissenschaftsrat) has published a position paper calling for the establishment of a dedicated federal research security support structure ([58]), while the German Research Foundation (DFG) and

([52]) https://www.uhr.se/globalassets/_uhr.se/publikationer/2024/responsible-internationalisation---interim-report-on-a-government-assignment-2024.pdf

([53]) https://www.uhr.se/globalassets/_uhr.se/english/about-the-council/national-support-function-for-responsible-internationalisation---final-report-2025.pdf

([54]) Global Responsible Engagement: Checklist, RECOMMENDATION 2023:4 (REVISED) https://suhf.se/app/uploads/2023/04/SUHF-Checklist-Global-Responsible-Engagement-REC.-2023-4-230411-REVISED.pdf

([55]) Stint. *Responsible internationalisation: Guidelines for reflection on international academic collaboration*, R20:01, 2020. Stint. *Recommendations to higher education institutions on how to work with responsible internationalisation*, R22:05, 2022.

([56]) https://www.bmftr.bund.de/SharedDocs/Downloads/DE/2024/position-paper-research-security.html

([57]) 'Germany Needs a New Agenda for Science, Research and Innovation' https://www.kmk.org/fileadmin/pdf/PresseUndAktuelles/2025/2025_01_31-Positionspapier-Wissenschaftsagenda.pdf

([58]) https://www.wissenschaftsrat.de/download/2025/2485-25_en

Leopoldina continue to provide guidance through joint reports on handling security-relevant research.

In December 2025 the Federal Ministry of Research, Technology, and Space (BMFTR), the Alliance of Science Organizations, and the state ministries of science agreed on key points for strengthening research security and establishing a National Platform for Research Security ([59]).

Italy: In 2024 the Ministry of University and Research (MUR) conducted a nationwide survey on research security among universities, with over 80% responding. The findings raised awareness and prompted the launch of a comprehensive national framework.

Since then, the ministry has established an Interministerial Coordination Platform and a Scientist Working Group with universities (CRUI) and research institutions (CoPER) to develop guidelines, consult stakeholders and organise workshops.

A draft national action plan for research security was presented in December 2024, featuring a voluntary self-assessment tool for researchers. In April 2025 a Presidential Decree ([60]) created a Directorate-General for Research Evaluation and Security within MUR, which will oversee the roll-out of a national support structure, including a future Research Security Centre, to be implemented across universities and research institutions by 2026. All information on the Italian activities can found on a dedicated website of the ministry ([61]).

Austria: A specific feature of the Austrian approach to research security is the formal integration into the performance agreements concluded by the Ministry of Women, Science and Research (BMFWF) with Austria's public universities for the 2025-2027 period. The 2024-2026 performance agreements with the Austrian Academy of Sciences (ÖAW) and the Ludwig Boltzmann Gesellschaft (LBG) include the topic as well.

In their performance agreements, all 23 public universities committed to develop and implement measures to enhance research security. This includes embedding research security in their international strategies and nominating a single point of contact by 2025, conducting risk analyses by 2026 and implementing and evaluating security measures by 2027 ([62]). Progress will be systematically monitored by the ministry.

The implementation is supported by the BMFWF, for example through its single point of contact and the established network of contact points. More than 70 universities and research organisations under the aegis of the BMFWF participate in the network, which offers training courses, capacity building, information briefings and trusted exchange. Specific questions from network members are answered by the single point of contact within the ministry, providing advice both on the development and implementation of measures and on specific cases.

([59]) https://www.bmftr.bund.de/SharedDocs/Downloads/EN/2025/key-points-research-security.pdf?__blob=publicationFile&v=1

([60]) Presidential Decree No 62 of 4 April 2025.

([61]) https://www.sicurezzaricerca.mur.gov.it/

([62]) All performance agreements are publicly available: https://unidata.gv.at/SitePages/Publikationen.aspx

Another specific initiative has been launched by the Ministry of Innovation, Mobility and Infrastructure (BMIMI), which is developing guidance for funding applicants. Evidence-based policymaking is supported by a 2023-2024 baseline study on foreign interference commissioned by BMFWF ([63]).

Belgium: Research security in Belgium is shaped by its multilayered federal, regional and community governance. To coordinate across these levels, the Interministerial Conference on Science Policy (IMCWB) created in 2023 a Research Security Coordination Group, chaired by the federal research policy agency BELSPO. The group brings together federal services, regional administrations, research councils and security and intelligence actors.

Although there is no specific legislation yet, the 2021 national security strategy ([64]) explicitly recognised research security and the IMCWB has reached an agreement in principle on making research organisations primarily responsible for managing research security risks, with public authorities providing policy coordination and guidance and with specific demand-driven input from the security services in complex cases. To assist the research sector, a national contact point on research security may be set up.

In Flanders the Flemish Research Council (FWO) developed and implemented a risk assessment tool (see also Section 4.3) and discussions are being held with the research performing organisations to see how the tool can be applied more broadly across the sector and whether a duty of care for research performing organisations should be introduced ([65]). French-speaking Belgium has taken a less formalised approach, focusing more on cybersecurity and integrity, with initiatives such as the Walloon CyberExcellence ([66]) programme launched in 2022.

Romania: Research security in Romania is still emerging but important building blocks are in place. Certain national research infrastructures are formally designated as being of 'high national importance' and must follow specific guidance from the National Authority for Research, aimed at preventing unauthorised access.

The authority, operating under the Ministry of Education and Research, also coordinates the national research and development institutes and participates in an interinstitutional group with ministries and intelligence services. The group manages security-related research in line with EU and NATO frameworks and might in future expand its remit to cover research security more broadly.

Romania's legal framework already covers several aspects relevant to research security, including laws on classified information ([67]), the protection of research infrastructures of national interest ([68]) and the law on cybersecurity and cyber-defence ([69]). Together with

([63]) https://www.bmfwf.gv.at/forschung/forschungssicherheit.html
([64]) https://www.premier.be/nl/nationale-veiligheidsstrategie, 1 December 2021.
([65]) Beleidsnota 2024-2029. Economie, wetenschap, innovatie en industrie | Vlaanderen.be
([66]) CyberExcellence – CETIC – Your connection to ICT research
([67]) Law No 182/2002 on the protection of classified information, Official Journal No 248/2002.
([68]) Government Decision No 786/2014 regarding the approval of the list of installations and objectives of special interest financed from the budget of the Ministry of National Education, Official Journal No 690/2014.
([69]) Law No 58/2023 regarding Romania's cybersecurity and cyber-defence, Official Journal No 214/2023.

the national strategy for the defence of the country, these provisions lay down a baseline of protection for critical infrastructures and sensitive research.

Most recently, in 2025, the Ministry of Education and Research published a concept note with policy recommendations on research security, the first forward-looking policy document in this area ([70]). Capacity building is supported through EU- and NATO-linked initiatives, awareness raising programmes run by the intelligence services and training by national institutes in collaboration with international partners. Discussions are also underway on setting up a national research security hub to provide direct support to institutions and researchers.

Spain: In July 2025 the Ministry of Science, Innovation and Universities (MICIU) tasked the Spanish Foundation for Science and Technology (FECYT) with developing a national action plan for research security. To deliver on this task, FECYT is taking a phased approach, starting with a planning phase until the end of 2025. In that phase, working groups are being set up: a strategic working group and working groups for research funders and research performers. Bilateral meetings took place with selected countries, including Italy, the Netherlands, the UK and Germany, to learn from their experience.

In the next phase, in 2026, the action plan will be drafted and developed, including guidelines, a support structure through a national information and contact point and the launch of a national portal on research security. In subsequent years (2027-2030) the action plan will be implemented, with the strategic working group in a coordination and monitoring role.

([70]) UEFISCDI – Executive Unit for Financing Higher Education, Research, Development and Innovation (2025) 'Policy recommendation on research security in Romania. Concept note': https://uefiscdi.gov.ro/resource-865271-Research-Security-Concept-Note_aprilie-2025.pdf

4. THE ROLE OF RESEARCH FUNDERS

Research funders have a crucial role to play when it comes to enhancing research security. Funders can incentivise their beneficiaries to assess and mitigate risks through their funding procedures. They can also exclude certain types of projects considered high-risk through eligibility restrictions. Across the EU, research funders are introducing such safeguards, while bottlenecks remain, often related to mandates and resources.

4.1. Recommendations: What is expected of research funders?

The Council acknowledges the important contribution that research funding organisations can make to enhancing research security by incentivising their beneficiaries to consider research security risks ([71]).

First, research security should be an integral part of the grant application process. This should encourage beneficiaries to identify risks and threats up front and to carry out due diligence into prospective partners. Projects selected for funding that raise concerns should undergo a risk appraisal, resulting in agreement between the funder and the beneficiary on appropriate risk management measures.

This means that adequate expertise and skills should be available in or to the research funding organisation to address research security concerns and that research security is integrated into both existing monitoring and evaluation measures and partnership agreements of the research funder with foreign partners.

To ensure some level of consistency, research funders are recommended to take the safeguards in Union funding programmes into consideration when applying safeguards in their own programmes.

4.2. Getting started with research security as a research funder

A first observation is that the role of national R&I funders differs from country to country, and that it is a very diverse group of organisations.

There are funders that cover a broad range of research and innovation activities and there are those that are specialised, for instance covering only innovation (e.g. Vinnova in Sweden) or targeting specific research domains (e.g. the Health Research Board in Ireland). There are 'hybrid' funders that combine funding research with performing research (e.g. NWO in the Netherlands) and there are organisations that have funding as part of a broader set of activities, for instance the DAAD in Germany, which promotes internationalisation and, as part of that mission, provides research funding.

The distance a research funder has from the government, and thus its independence and autonomy, may vary too. This has implications for the funder's mandate and competence as well as the scope it has to integrate research security into its operations autonomously.

([71]) Recommendation 14.

Such differences determine the risk profile of the activities the funder is funding and also its ability to act.

Therefore, as a first step, it is recommended to check whether the organisation has the mandate and competence to follow up on the recommendations. It may be necessary to explicitly add research security to the funder's mandate or strategic plan. Moreover, a dedicated legal basis may be needed for the funder to require risk assessment and mitigation measures and to have the possibility, in justified cases, of turning down project proposals on security grounds.

As part of this first step, the responsibilities of the funder should be clarified too. As underlined by the Council Recommendation, research funders clearly have their own role and responsibility between the responsibility of the research performing organisation based on its academic freedom, on the one hand, and the responsibility of the national authorities to protect national security, on the other.

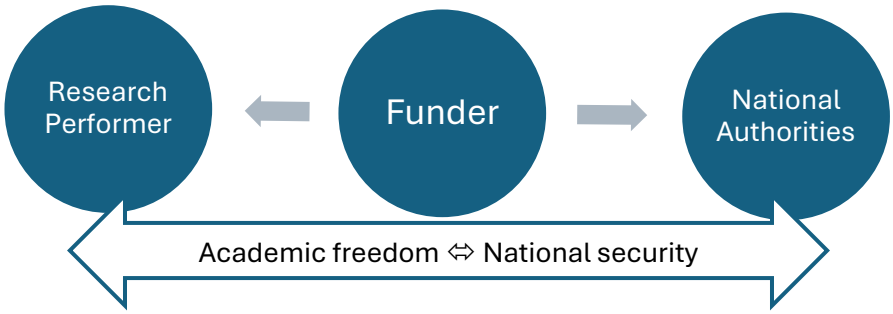

Figure 4: The research funder's responsibility in research security

Once the mandate and responsibilities have been established, there are a variety of instruments that the funder can apply as part of its 'safeguarding toolkit'. These tools can be categorised as follows:

- **Safeguards at project level**: case-by-case risk assessment and due diligence. This could involve self-assessment by the beneficiary of the risks related to the project proposal and some form of verification of the beneficiary's self-assessment. This means that the funder incentivises beneficiaries to assess risk, verifies the self-assessment (usually after the scientific merit review has been successfully completed), agrees mitigation measures and includes them in the grant agreement.
- **Eligibility restrictions**: This means that a combination of risk factors is defined beforehand (e.g. in a call document) and that for those categories, restrictions or exclusions from calls for proposals or parts of funding programmes apply. Such measures should always be proportionate and targeted, taking into account multiple risk factors.
- **Institutional risk management**: In order to carry out high-risk projects, the beneficiary may be required to have a credible risk management system in place.

- **Transparency**: The beneficiary should be open and transparent about relevant (non-EU) funding sources and (non-EU) affiliations of staff involved in the project. In this respect, there is a direct link to research integrity.

As an example of what safeguards may look like in practice, two relevant safeguards in the current Horizon Europe programme are summarised in the text box.

Box text: Examples of safeguards in Horizon Europe, 2021-2027

The framework programme for research and innovation, Horizon Europe ([72]), balances openness to international cooperation with the need to safeguard EU interests in strategic areas, in particular to promote the EU's strategic autonomy and its technological leadership and competitiveness.

Safeguard at project level: Article 20 to protect sensitive and classified information

The security appraisal procedure, based on Article 20, focuses on the identification and protection of sensitive and classified information and consists of three steps:

1. The *security self-assessment*: All applicants complete the security issues table and, if the proposal falls under a *security-sensitive topic* flagged in the work programme, they must also fill in the security section, detailing any classified information to be produced and the security staff foreseen.
2. The *security review*: The purpose of the review is to identify security concerns and verify that they have been properly addressed in proposals selected for funding. It focuses on the compliance of the proposal with security rules, particularly the protection of sensitive and classified information against unauthorised disclosure. It also aims to identify potential security issues arising from the research or the possible misuse of results and to ensure that they are mitigated by taking appropriate measures. The outcome may result in security requirements becoming *contractual obligations* (outcome of the security scrutiny procedure becomes the security section of Annex 1 to the grant agreement).

The security review includes three steps:

- *Security pre-screening* carried out by qualified staff of the granting authority during the scientific evaluation or soon after.
- *Security screening* performed by qualified staff of the European Commission (DG HOME) after the scientific evaluation and before the signature of the grant agreement.
- *Security scrutiny* conducted by the Security Scrutiny Group (SSG), comprised of national security experts, after the scientific evaluation and before the grant agreement is signed.

3. The *security checks* by the Commission or the relevant funding body, where appropriate, during or after the life of the project.

Eligibility restrictions: Article 22 to protect strategic assets, interests, autonomy or security

For actions related to Union strategic assets, interests, autonomy or security, the work programme may provide, on the basis of Article 22(5), that the participation is limited to legal entities established only in Member States and specified associated or other third countries ('eligible countries').

For duly justified and exceptional reasons, the work programme may also exclude the participation of legal entities established in eligible countries that are directly or indirectly controlled by non-eligible third countries, or make their participation subject to conditions set out in the work programme.

In addition, on the basis of Article 22(6), the work programme may provide, where appropriate and duly justified, for additional eligibility criteria to take into account specific policy requirements or the nature

([72]) https://eur-lex.europa.eu/eli/reg/2021/695/oj/eng It should be noted that the programme, in force since 2021, predates both the EU's economic security strategy and the Council Recommendation on research security.

and objectives of the action, including the number of legal entities, the type of legal entity and the place of establishment.

This provision allows for targeted and country-specific measures, such as the exclusion of Chinese entities from innovation actions due to concerns linked to unwanted IP transfer and the stalling of negotiations on the joint road map for the future of EU-China STI (science and technology innovation) cooperation and the exclusion of 'high-risk suppliers' of mobile network communication equipment from certain relevant Horizon Europe calls ([73]).

The Commission will generally seek to prevent access by high-risk entities to Union supported actions in the critical technology sphere, which can potentially be weaponised against the EU ([74]).

Introducing and implementing safeguards may require change at various levels. It usually involves changes to internal working processes and procedures. There are also human resource implications, such as providing training to existing staff members and/or attracting staff with security expertise and know-how. Gaining access to security expertise outside its own organisation could be an alternative or additional way for the funder to have the right expertise and know-how at its disposal.

It also has implications for communication with applicants, who should be informed and supported to deal with these new requirements. Last but not least, one should consider the implications for the regular project monitoring and evaluation cycle: how can research security aspects best be integrated into those processes, ensuring that risk mitigation is actually implemented?

4.3. Case studies: An active role for research funders

The overall picture is that a few front runners have more mature procedures and structures in place and a growing number of funders are taking steps in that direction. However, some funders have not started the process yet.

There is growing awareness of research security among EU-based research funders, but the actual integration of security considerations into funding processes remains at an early and largely exploratory stage in terms of the policy maturity model presented in Section 3.2. Practices vary considerably: some funders have in-house security expertise, or have access to external specialists, while many lack either. At present, security-related safeguards are mostly applied at project level on a case-by-case basis, with predefined eligibility exclusions generally being limited to compliance with sanctions, such as those against Russia and Belarus.

Some funders have embedded security questions in their grant application forms, where applicants are asked to self-assess risk, although the applicants' responses are not always subject to verification. Key challenges include uncertainty over mandate and responsibility (e.g. whether refusal of funding can be justified on security grounds), a lack of resources and expertise, and concerns about adding administrative burden or delaying time to grant.

Generally speaking, research funders take an approach that keeps the assessment of the

([73]) Amendment of the 2023-2024 Horizon Europe work programme.

([74]) Joint communication, Strengthening EU economic security, JOIN(2025) 977 final of 3 December 2025, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52025JC0977&qid=1765793215655

scientific merit of research projects separate from risk-related aspects. The aim for security reviews is 'getting to yes', i.e. setting out conditions under which the project can go ahead. Funders are reticent to flatly refuse scientifically sound research projects.

In addition, funders tend to ensure that research performers retain primary responsibility (in line with academic freedom) and aim to keep the administrative burden on all parties involved as low as possible.

Belgium: Among Belgian funders, the Flemish Research Council (FWO) has taken the lead on research security. Together with universities, it has co-developed a mandatory risk assessment tool for grant applicants, now applied across most calls (see box text). FWO excludes cooperation with Russia and Belarus and also with China's 'Seven Sons of National Defence' universities and has embedded the core values and principles that need to be respected throughout the cooperation in its memoranda of understanding and agreements.

At federal level, the Belgian Science Policy Office (BELSPO) has prepared an internal action plan and intends to integrate a similar risk appraisal tool into its grant application procedure, while the French-Community Fund for Scientific Research FRS/FNRS emphasises awareness raising to responsibilise universities in line with academic freedom.

Box text: FWO's research security appraisal tool

The Flemish research funder FWO developed a research security appraisal (RSA) tool which applicants for funding should use to assess the risk profile of their research projects at the submission stage. The tool was piloted in a call for funding in 2024. Now, after several iterations, it has become an integral part of most funding calls.

In essence, the tool consists of 10 questions with three answer options ('yes', 'possibly' and 'no'). The questions relate to the research topic, the partner's country and the partner institution/researcher itself. To minimise administrative burden, the RSA tool uses automated classifications wherever possible. For instance, countries have been categorised on the basis of several international indices, including the academic freedom index and the rule-of-law index. The assessment of the research domain is in part based on the EU critical technology list.

The process ensures that the applicant, i.e. the host research performing organisation, remains responsible at all times, in line with its institutional autonomy. Once the applicant has completed the RSA tool, it will be validated by the project selection panel. The host research performing organisation receives an overview of high-risk projects, conditionally approved for funding, which need additional research security approval.

Once the host institution has formally confirmed to FWO that it is aware of the risks involved and will take appropriate steps to mitigate them, the research project can be launched.

Finland: The Research Council of Finland (RCF) has adapted its mandate to integrate research security more systematically. Following the 2025 amendment to the Act on the Research Council of Finland (AKA) ([75]), the RCF must now explicitly consider the safety of research and potential risks in projects, collaborations and applications of results, while safeguarding academic freedom. Although the Act was amended in the context of

([75]) https://valtioneuvosto.fi/paatokset/paatos?decisionId=3698

fundamental research, it is well aligned with the 2025 *Security Strategy for Society* ([76]) drawn up by the Security Committee.

RCF had already embedded research ethics and integrity in its grant procedures. It has now also included research security in its grant applications through a concise self-assessment template ([77]). Risk awareness is thus gradually becoming part of assessment, while responsibility for managing risks (including dual-use, export control and data protection risks) remains with the universities, in line with Finland's strong principle of institutional autonomy.

Germany: Two of Germany's major research funders, the German Academic Exchange Service (DAAD) and the German Research Foundation (DFG), have integrated research security into their funding practices in response to geopolitical developments and EU-level recommendations. Both DAAD and DFG are in close exchange with ministries, security agencies and initiatives like the Network for International Research Security.

At organisational level, DAAD has set up the Competence Centre for International Scientific Cooperation (KIWi) as its dedicated research security unit ([78]). KIWi provides guidance to universities on compliance systems and due diligence, operates a global expert network with regional specialisation (e.g. China, Middle East) and runs awareness programmes, including event series on dual-use, position papers on cooperation with sensitive countries ([79]) and a self-assessment tool for structured risk assessment ([80]).

At programme and call level, DFG and DAAD require institutions to assess and address risks before submitting funding applications. Applicants must raise awareness, analyse partnerships, assess risks related to topics, partners, data protection and IP, and prepare mitigation measures. In 2023 DFG published recommendations for international cooperations, which also set out what is expected of applicants ([81]).

While the funders provide guidelines and advice, responsibility for risk management lies with the funded institutions. Universities must demonstrate that they have compliance systems in place and, in sensitive cases, consult KIWi or other advisory structures.

Since Russia's invasion of Ukraine, both funders have suspended cooperation with Russia (except individual mobility grants), and security considerations now weigh more heavily in internationalisation strategies.

Slovenia: The activities of the Slovenian Research and Innovation Agency (ARIS) are based on its 2024-2027 strategy. Given the newly emerging landscape of research security-related challenges, ARIS is updating this strategy. The process of updating the current strategy explicitly follows a long-term orientation and aims for a holistic perspective on the topic of research security.

([76]) https://julkaisut.valtioneuvosto.fi/server/api/core/bitstreams/aff0ba13-4037-43e8-8b85-e138215ce3ac/content
([77]) https://www.aka.fi/en/from-research-to-society/responsible-science/research-security/
([78]) https://www.daad.de/en/information-services-for-higher-education-institutions/kiwi/
([79]) https://www.daad.de/kiwi-kompass/no-red-lines/
([80]) https://static.daad.de/media/daad_de/pdfs_nicht_barrierefrei/infos-services-fuer-hochschulen/kompetenzzentrum/dokumente/kiwi_checkliste_wissenssicherheit_en.pdf
([81]) https://www.dfg.de/en/basics-topics/basics-and-principles-of-funding/security-relevant-research/risks-inter-cooperation

Part of this process is a dialogue with the ministries on jointly defining criteria for future research security-sensitive funding calls. The goal is to lay down criteria that enable effective assessment of potential research security risks without being overly restrictive, so as not to unduly limit research processes or hinder opportunities for innovation breakthroughs.

The Netherlands: The Dutch Research Council (NWO) combines its role as a funder with its role as a research performer, through several research institutes. It has developed a research security strategy for both.

Efforts are being made throughout NWO (both for all staff involved in the funding process and for all those working at one of the nine NWO institutes) to raise awareness of knowledge security. NWO has set up two advisory teams for both parts of the organisation.

Applicants for funding are required to follow the national guidelines on knowledge security ([82]), to which NWO is a party. In case of doubt, it can ask the applicant for further clarification. In addition, NWO may decide to include further conditions in the award letter to protect research security.

In 2025 NWO launched a EUR 6.6 million call for proposals on 'Knowledge security: scientific research in a geopolitical context' to strengthen the knowledge base on research security-related issues ([83]).

France: The French National Research Agency (ANR) integrates research security into its funding framework through the protection of the nation's scientific and technical potential (PPST), presented in more detail in Section 3.4. Applicants are encouraged to consult their institution's Security and Defence Officer (FSD) before submitting their project proposals, and ANR may request the opinion of the High Official for Defence and Security (HFDS) at the Ministry of Higher Education and Research.

In 2022 a systematic security check procedure was introduced: projects with either non-EU public partners or foreign private partners are reviewed by the High Official for Defence and Security (HFDS) at the Ministry of Higher Education and Research, following guidelines of the General Secretariat for Defence and National Security (SGDSN). Negative opinions exclude projects from funding.

Through these measures, ANR balances its role of supporting international collaboration with the need to protect sensitive research, making security oversight a standard element of its funding practice.

Luxembourg: Given its central position within Luxembourg's research ecosystem, FNR plays a critical role in implementing measures designed to ensure research security. Although it does not yet possess a dedicated research security policy, FNR integrates relevant elements through its broader frameworks related to research integrity, ethics, dual-use research and data protection. A working group on research security has recently been set up with representatives of all public research institutions and the Ministry of Research and Higher Education. A risk assessment tool for grant applicants is being developed and will be tested as part of a pilot call in 2026.

([82]) https://www.rijksoverheid.nl/documenten/rapporten/2022/01/14/nationale-leidraad-kennisveiligheid
([83]) https://www.nwo.nl/en/calls/knowledge-security-scientific-research-in-a-geopolitical-context

At programme level, specific security-related eligibility criteria are implemented only in certain cases, such as the Defence-BRIDGES Call. In this call, eligibility is restricted to nationals of NATO, EU/EEA/EFTA countries and select Indo-Pacific partners. Furthermore, researchers affiliated with institutions in some countries are currently excluded from FNR's peer review processes.

The FNR also requires consortium and IPR agreements for international projects as a risk mitigation step. Compliance with security standards is ensured through eligibility checks and project follow-ups. The requirement for a data management plan (DMP) for all funded projects indirectly supports research security by addressing data storage, access control and preservation issues.

5. THE RESEARCH AND INNOVATION SECTOR

Research performing organisations are at the heart of any effective research security policy. Although no one-size-fits-all approach exists, each organisation needs to take certain steps to ensure an adequate level of security. Across the EU a wide variety of initiatives are being developed, including procedures to assess and sign off partnerships and projects with a high risk profile.

5.1. Recommendations: What is expected of research performers?

The EU's approach to research security is based on the notion that research performing organisations are primarily responsible for ensuring research security. This is in keeping with academic freedom and their institutional autonomy. This means that they are expected to introduce and apply internal measures to ensure that research security is adequately addressed. For that reason the Council Recommendation contains several recommendations addressed to research performing organisations ([84]).

Research performing organisations should assign research security responsibility at the appropriate level in their organisation. They should also introduce internal risk management procedures, with risk appraisal, due diligence on prospective partners and escalation to higher levels of internal decision-making when a project raises concern.

When concluding partnership agreements (such as MoUs) with foreign partners, research performing organisations should consider possible risks and include key framework conditions in the agreement, such as respect for values and fundamental rights, academic freedom, reciprocity and intellectual assets management. The agreement should provide for an exit strategy if its conditions are not complied with. By the same token, the organisations are also recommended to assess risks related to foreign government-sponsored talent programmes in research and innovation.

Implementing such safeguards requires investment in dedicated in-house research security expertise and skills and the provision of access to training programmes for new and existing research staff. Recruiters should be trained to check and detect, as part of a structural vetting process, elements that raise concern in applications for research positions.

Research performing organisations should ensure full transparency of funding sources and affiliations of research staff in scientific publications, avoiding undesirable foreign dependencies and conflicts of interest or commitment.

5.2. The contribution of sectoral stakeholders

The Council encourages research performing organisations to 'engage in information exchange, peer learning, development of tools and guidelines and incident reporting among

([84]) Recommendation 15.

peers, as well as to consider resource pooling to make best use of scarce and scattered resources and expertise' ([85]).

The sector has indeed taken several initiatives to support peer learning, awareness raising and capacity building. There are a great variety of activities and events at which participants discuss the topic, learn from each other and formulate positions and responses. There are activities at Union level, at national level and at the level of individual research performing organisations.

European R&I stakeholder associations have been particularly active on the topic of research security. The Council Recommendation has been hotly debated and there is broad support for its approach, with respect for academic freedom as a key element.

Several associations have launched dedicated working groups and task forces for their members, such as Science Europe ([86]), CESAER ([87]), EECARO ([88]), ALLEA ([89]) and LERU. Dedicated events and thematic sessions have been organised, for instance by LERU ([90]) and EU-LIFE ([91]), and the topic was added to the agenda of their summits and general assemblies.

There have also been (position) papers and reports, such as those of CESAER ([92]), The Guild ([93]), ALLEA ([94]), EECARO ([95]) and Science Europe ([96]), and contributions to the call for evidence launched by the Commission in preparation for its proposal for the Council recommendation (EUA, EARTO, EECARO, LERU, The Guild and YERUN ([97])).

The Commission organises regular meetings with representatives of more than 15 European R&I stakeholder associations to discuss updates on research security ([98]). In addition, there has been close cooperation and, indeed, co-organisation on the European Flagship Conference on Research Security that took place in October 2025 (see also Section 6.3). The fact that 12 European stakeholder associations – and through them their respective members – were involved in the organisation contributed significantly to the relevance and impact of the event.

([85]) Recommendation 15(a).
([86]) https://scienceeurope.org/our-priorities/cross-border-collaboration/research-security/
([87]) https://www.cesaer.org/task-forces/task-force/?id=11825
([88]) https://eecaro.eu/working-groups/
([89]) https://allea.org/research-security/
([90]) https://www.leru.org/news/improving-research-security-in-european-universities
([91]) https://eu-life.eu/newsroom/events/BT-research-security
([92]) 'Research security as a collective responsibility: empowering universities, enabling Europe' (2025) https://doi.org/10.5281/zenodo.17453941 and 'Keeping science open' (2023) https://www.cesaer.org/news/keeping-science-open-current-challenges-in-the-day-to-day-reality-of-universities-1556/
([93]) https://www.the-guild.eu/news-and-blog/news/2023/research-universities-emphasise-the-need-for-responsible-internationalisation.html
([94]) https://allea.org/portfolio-item/allea-statement-on-research-collaboration-and-research-security-in-a-shifting-geopolitical-landscape/
([95]) Feedback on the Factsheet Research Security: Building blocks for risk appraisal https://eecaro.eu/publish/pages/6178/october-2024_eecaro-contribution-to-research-security-risk-appraisal-building-blocks.pdf
([96]) Science Europe 'Report on Research Security: Key Messages and Actions' (2025).
([97]) Call for evidence (2023), feedback received: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14056-Boosting-research-security-in-the-EU-guidance-/feedback_en?p_id=32434562
([98]) This refers to the work in the context of the ERA action on research security. See also Section 6.3.

At national level, a similar trend can be seen in a growing number of Member States: national umbrella organisations, rectors' conferences and academies of science are providing platforms and working groups for the sector at national level to discuss among themselves (i.e. in addition to the groups and meetings for which the national administration takes the lead). In some cases, such initiatives work on the pooling of resources so that research performers (in particular smaller ones) can make best use of their limited resources.

5.3. Getting started with research security in a research performing organisation

What are the implications of these recommendations – and where to start? It is important to underline that the research and innovation sector consists of a very wide variety of actors. It includes major applied research institutes involved in dual-use research and smaller universities focusing on fundamental research. There are research performers that have deep involvement in a large number of international partnerships and there are those whose exposure to the world is fairly limited.

It is for these reasons that any risk appraisal (see Section 1.2) starts from an assessment of the risk profile of one's own organisation: what are the organisation's assets or 'crown jewels', which parts or domains deserve particular attention? This step is about defining *what* should be protected, which precedes the question of *how* to do so.

Once this has been clarified, next steps can be taken. Here are some basic steps that are often mentioned by research performing organisations that have research security policies in place.

Assigning responsibility for research security may involve nominating someone at board level to oversee the development of an in-house strategy and implementation plan. Depending on the size and profile of the organisation, they may be assisted by one or more expert(s) in preparing such internal policies and answering questions from research staff about the issue. Access to relevant national authorities is key for the effectiveness of such experts.

A process may then be devised to determine how projects or partnerships that raise concern ('red flags') are to be identified. This may be a new internal procedure, but it may also be an add-on to an existing one.

It could, for instance, be added to a procedure for compliance with export control and sanctions, with elements that go beyond legal compliance to avoid technology leakage through export. Another option is adding a security dimension to an existing ethics reviews procedure or taking into account forms of transnational repression as part of social safety policies.

At the same time, awareness-raising activities for new and existing staff may be organised, for instance through articles on the internal website, lunch discussions for staff or targeted in-house campaigns.

5.4. Case studies: research performing organisations

It is impossible to make general statements on the basis of the qualitative information collected for this publication. From the information available, a heterogeneous picture emerges, with a large difference both between and within countries.

One observation is that front runners are often (but not always!) institutes for applied research, which are closer to the market, and universities of technology, which often deal with critical knowledge and technology. Another observation is that, alongside security and research integrity considerations, the avoidance of reputational damage is an important driver for action for research performing organisations.

Rather than trying to reflect the situation in each country, a couple of case studies will be presented here. It should be noted that, due both to the sensitivity of the topic and to the fact that this is about organisation-internal matters, the information that may be disclosed in the public domain is limited.

Denmark: The Technical University of Denmark (DTU) takes a structured, risk-based approach to research security, particularly in fields involving critical and emerging technologies. Since 2020 it has required the use of a tailored risk assessment questionnaire before entering international collaborations, ensuring that ethical, economic and security risks are addressed early in the process. DTU runs a system-supported mapping process to identify high-risk research collaborations, with a focus on projects in dual-use and emerging technologies. Collaborations with high-risk countries undergo stricter controls, including detailed risk documentation and departmental approval. In addition, DTU has extended its risk assessment procedures to new employees and guest researchers.

DTU has set up a coordinating committee for security in research, innovation and education activities (SiFI), which clarifies matters of principle and supports and prioritises the development of a stronger security organisation. In line with the new agreements on research security for 2026-2029, DTU is preparing an annual report on research security management for the Danish Agency for Higher Education and Science ([99]).

Box text: Security assessment during hiring process at Aalborg University

Another case from Denmark is Aalborg University, which has introduced a screening procedure that applies to both new employees and guests ([100]). Danish universities have been granted hiring authority under Danish law, which allows them to consider all relevant criteria, including security, in the hiring process. For the background checks, the applicant's CV and open-source intelligence (OSINT) are used.

Checks focus on countries identified as threat actors by the Danish intelligence agency (PET) and countries against which EU sanctions apply. Assessments are made on a case-by-case basis. There are questions related to the candidate's background, employment history and publication history as well as questions about the access the candidate will be given to labs and research infrastructure and the research domain in which he or she will be involved. For the latter, it is for instance relevant to know whether the domain has dual-use potential or ethical implications.

The process consists of a template containing risk assessment questions to be answered by the recruiting department followed by a risk analysis performed by the grants and contracts representative that will provide the basis for a recommendation by the Head of Department, taking into account whether the

([99]) https://www.dtu.dk/english/about/strategy-policy/sustainability-report

([100]) https://www.security.aau.dk/security-rules-and-policies/security-handbook#3.1-pre-employment

level of risk is acceptable and if proper risk mitigation initiatives have been implemented. The final decision is taken by the Dean.

Experience has shown that the procedure effectively raises awareness of security risks and that it is an effective tool for dialogue within the institution about balancing risks and benefits.

Estonia: TalTech, Estonia's technical university, addresses research security through a mix of established practices rather than formal guidelines. TalTech collaborates closely with the Estonian defence sector, NATO and EU programmes such as Horizon Europe – Cluster 3 and the European Defence Fund, which require strict security compliance. A dedicated security expert oversees cybersecurity, data protection, partner vetting and dual-use technologies. Staff engaged in international collaboration must attend training on risks such as foreign interference and partner vetting, reflecting the university's strong focus on awareness and responsible decision-making in sensitive research areas.

Spain: The Spanish National Research Council (CSIC), with its 120 research institutes, has moved away from a fragmented, decentralised approach to research security and towards a structured institutional framework. Central to this transformation is the creation of a Research Security Committee, which unites representatives from across disciplines and institutional levels and consults external experts when necessary.

The committee is tasked with producing standardised documentation and risk assessment templates, advising leadership and research centres on security-sensitive cases and delivering training for researchers, technical staff and project managers.

By embedding security in risk assessments, collaboration reviews and staff awareness programmes, CSIC is turning research security into an enabler of international cooperation, aligned with EU economic security goals and national strategies.

The Netherlands: Delft University of Technology has implemented research security policies that are managed both centrally and decentrally within the organisation, and there are various tools available with information and tools for employees ([101]). It has a guidance document that can be used by any staff member to assess whether a collaboration – which can both be institutional and involve employment or hospitality – is permissible and desirable. Furthermore, it has developed 'partnering tools' with checklists and guidelines for entering into, implementing and evaluating international collaborations.

Like other Dutch universities, Delft University of Technology has set up an in-house advisory team for research security, which handles around 700 queries annually, and it has research security contact persons in all faculties. Training courses and symposia are organised to increase knowledge and awareness. Delft University of Technology participates in the inter-university Universities of the Netherlands (UNL) working group on research security and, at European level, it plays an active role in both EECARO and CESAER.

Sweden: Stockholm's KTH Royal Institute of Technology has created a structured framework for managing international collaboration risks through its Advisory Board for Responsible Internationalisation (RAI) ([102]). Chaired by the university's Security

([101]) https://www.tudelft.nl/en/about-tu-delft/strategy/knowledge-security

([102]) https://intra.kth.se/en/styrning/kths-organisation/beredande-organ/styrgrupp-och-radgivande-grupp-for-ansvarsfull-internationalisering-1.1369382

Manager, RAI provides expert advice on issues such as recruitment, guest researchers, external funding and innovation partnerships. Only cases pre-assessed by schools or divisions may be submitted, ensuring a targeted and efficient process. Unresolved or complex cases are escalated to the Governing Board for Responsible Internationalisation (SAI), reflecting a multi-tiered model of oversight.

This structure is complemented by initiatives like Campus Total Defence ([103]), which links academia with national security stakeholders, and training efforts supported by the Swedish Defence University and SUHF. Together, these measures embed research security in governance, decision-making and awareness raising across the institution.

Germany: The University of Hamburg has put in place internal processes for project approval and risk assessment, consisting of a systematic review process for international collaborations, ensuring that projects comply with export control regulations and safeguarding academic freedom.

Security-sensitive research is evaluated by the Central Committee for Ethics in Security-Relevant Research (ZKEF), which advises researchers on dual-use risks, data protection and ethical concerns. Dedicated departmental responsibilities further ensure accountability and consistency in decision-making so that robust internal structures and clear responsibilities support compliance and risk mitigation, without compromising academic openness.

Czechia: In 2024 a memorandum of understanding (MoU) was signed between the Czech Academy of Sciences, Charles University (CUNI) and Palacký University Olomouc (UPOL) with the aim of pooling and sharing relevant knowledge of research security and promoting awareness of the importance of risk assessment and due diligence. Beyond these initial signatories, several other universities and research institutions, both within Czechia and internationally, have expressed interest in joining and expanding the MoU, reflecting a growing commitment to collaboration in this field.

Most Czech higher education institutions and research performing organisations have approached research security proactively, gradually integrating it into their daily practices. This includes measures such as appointing dedicated staff, developing internal guidelines, raising awareness, organising training activities and, in some cases, incorporating research security topics into PhD curricula to ensure early education on these issues.

Finland: The University of Helsinki has introduced a web-based risk assessment tool to evaluate potential risks in international research collaborations, with particular relevance for sensitive fields such as biotechnology. Piloted in 2024 and launched in 2025, the tool is expected to become mandatory during project preparation, ensuring systematic assessment of security risks before research begins.

The university has also aligned its practices with national security priorities, including by suspending collaboration if a review by Finland's Security and Intelligence Service gives rise to concerns. These measures are part of a broader national effort coordinated by Universities Finland (UNIFI), embedding research security in everyday academic practice while maintaining openness and international engagement.

([103]) https://campustotalforsvar.se/om-campus-totalforsvar/

Slovenia: Following the 2024 LERU-CE7 seminar, the University of Ljubljana set up a Research Ethics and Integrity Unit that now also covers research security. Working with the international, legal and knowledge transfer offices, the unit developed a research security due diligence form for staff considering cooperation with certain partners or countries.

The form raises awareness among researchers by prompting them to reflect on potential risks, such as dual-use concerns, and propose mitigation measures. At the same time, it provides university leadership with a structured basis to evaluate risks and benefits before approving projects.

Ireland: Munster Technological University (MTU) has put in place a comprehensive approach to managing institutional risks, including those linked to research security. The university maintains an information security policy to protect its information assets from unauthorised access, disclosure or misuse, supported by internal monitoring and third-party audits.

Risk management is embedded institutionally: MTU conducts risk analyses at least twice a year using structured criteria and maintains an Audit and Risk Committee that advises its governing body on governance, compliance and emerging risks. These processes cover more than research security alone and provide a systematic foundation for identifying vulnerabilities and ensuring resilience in sensitive research environments.

Portugal: The University of Porto has taken steps to strengthen its governance structures in areas relevant to research security. Building on frameworks for research ethics, data protection and intellectual property, the university has started to extend those frameworks into a broader discussion about security in international research collaborations.

The university's technology transfer office (UPIN) plays an important role in safeguarding intellectual property and providing advice on contractual clauses in international partnerships, while the ethics committees and the data protection officer oversee sensitive aspects of conducting research.

6. EU-LEVEL INITIATIVES

EU-level initiatives support Member States and the research and innovation sector in developing their national approaches to research security and in promoting consistency across the EU, thus ensuring both effectiveness of the safeguarding measures and a level playing field within the EU. The EU's approach to research security is part of a broader effort to raise awareness and build resilience against threats to the security of the EU and its Member States. Through international cooperation, both bilaterally and multilaterally, experience is shared and alignment of approaches is sought.

6.1. EU added value: why EU-level action is needed

While national authorities are best placed to engage with their research funders and research performing organisations and support them in taking the necessary measures, EU-level cooperation and coordination is needed to promote consistency of approach and a level playing field across the EU so as to ensure proper functioning of the European Research Area.

Consistency in this context has both a horizontal and a vertical dimension, and it serves both external and internal purposes. Horizontally, consistency means that there are similar approaches between EU Member States and that there are no disparities that hinder the EU's level playing field. Consistency in a vertical sense means that different governance levels take similar approaches. This means that the approach of the Commission and those of the Member States should be aligned to the extent possible, and that within the Member States the research funders reinforce those efforts. Individual research performing organisations should apply those policies within their own organisations, taking into account their specific risk profiles.

Why does this matter? In the first place, it matters for external effectiveness reasons. If some Member States do not safeguard their research and innovation or part of their research and innovation ecosystem remains unaware of the risks related to international cooperation, this creates vulnerabilities that could easily be exploited by threat actors. In a borderless European Research Area, the existence of such vulnerabilities, or 'weakest links', may put the entire EU research and innovation ecosystem at risk.

Box text: The importance of consistency, a hypothetical case

A researcher based in the EU submits a project proposal for funding from Horizon Europe. It concerns a critical technology, such as quantum technology, and it involves a research institute known to be closely linked to the military in a country with an authoritarian system where researchers have limited academic freedom.

The proposal is not selected for funding by the Commission. The researcher then decides to submit the same proposal for funding to the national funder. Even if the national funder were to turn it down too, nothing would prevent the researcher from accepting an offer from a high-risk foreign partner to fully fund the project.

This hypothetical example demonstrates the importance of safeguards that are aligned at all levels: Union level, national level and the level of the research performing organisations themselves.

There are EU-internal reasons as well. The absence of safeguards in one country or part of the sector and the existence of different and diverging approaches and measures in others also has internal implications for cooperation within the European Research Area. If such a situation persists, it may over time reduce trust, with negative repercussions for collaboration between researchers from different Member States.

It could, for instance, mean that researchers from a specific Member State were excluded from consortia because their country lacks research security policies – or, on the contrary, because its safeguarding measures are perceived as too stringent and burdensome. If this happens, it will directly affect the integrity of the European Research Area. A minimum level of consistency of approach across the EU is therefore essential, which is where Union level action can add value.

6.2. A comprehensive EU policy approach

Enhancing research security across the EU is part of a broader effort to strengthen the Union's economic security. The development of a European approach to research security fills a gap in a larger toolbox containing policy instruments such as export control, foreign direct investment screening and sanctions ([104]). How these instruments work together can be explained in a simplified example.

Box text: Technology transfer seen from a threat actor's perspective

Seen from the perspective of a threat actor, there are several methods to acquire the critical knowledge and technology needed to develop its military capability. An actor usually chooses the modus operandi that involves the least risk, cost and time.

Stealing technology through espionage is a sophisticated, time-consuming, costly and high-risk method, and strict counterterrorism laws and frameworks apply in the Member States.

Importing critical knowledge and technology as part of a commercial deal with a private partner in the EU would be easier. To prevent this from happening, the EU and its Member States apply tight export control rules ([105]).

If import is not possible, another option for the threat actor could be to buy the EU-based company and its assets, including the critical knowledge and technology. To counter this threat, the EU introduced foreign direct investment screening ([106]). The FDI Screening Regulation is currently under revision and will be further strengthened ([107]).

([104]) Joint communication, Strengthening EU economic security, JOIN(2025) 977 final of 3 December 2025: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52025JC0977&qid=1765793215655

([105]) EU export control system: https://policy.trade.ec.europa.eu/help-exporters-and-importers/exporting-dual-use-items_en

([106]) EU framework for foreign direct investment screening: https://policy.trade.ec.europa.eu/enforcement-and-protection/investment-screening_en

([107]) Press release on trilogue conclusion: https://policy.trade.ec.europa.eu/news/revision-eus-foreign-investment-screening-mechanism-2025-12-11_en

Until recently the academic cooperation route was the most convenient and low-risk way of acquiring state-of-the-art knowledge and technology. Not only is it legal, but there is also often even funding available to support it.
Research security policies target this vulnerability by taking decisive action to raise awareness and build resilience in the research and innovation sector.

In the broader economic security toolbox, research security adds a dedicated approach for publicly funded research and innovation, a sector that has openness and international collaboration in its DNA and whose governance is characterised by academic freedom and institutional autonomy. A dedicated, tailor-made approach is therefore a necessity.

The Union's economic security strategy, launched in June 2023, addresses four categories of risks:

(1) resilience of supply chains;
(2) physical security and cybersecurity of critical infrastructure;
(3) technology security and technology leakage; and
(4) weaponisation of economic dependencies or economic coercion.

While all four risk categories may have repercussions for the research and innovation sector, the risks related to technology security and leakage are at the heart of the strategy. They are an important component of what the research security approach focuses on.

To address these risks, a combination of actions to promote, protect and partner is proposed:

- Promoting the EU's competitiveness and growth, strengthening the single market, supporting a strong and resilient economy and fostering the EU's research, technological and industrial base.
- Protecting economic security through a range of policies and tools, including targeted new instruments where needed.
- Partnering and further strengthening cooperation with countries worldwide.

Research and innovation are relevant in all three of the economic security strategy's pillars. While this report focuses on the 'protect' side of the strategy, it should be stressed that these efforts complement an ambitious 'promote' agenda.

Significant investments are being made in excellent research and innovation by both the Member States and the EU, through its Horizon Europe programme and its Cohesion Policy support, notably via the European Regional Development Fund (ERDF). Through robust investments in education and training and also initiatives to attract talent from around the globe, such as the Choose Europe for Science initiative ([108]), the EU exploits its potential as a research and innovation leader.

Cooperation with our closest partners worldwide is certainly also part of the European approach to research security, as will be explained in Section 6.4.

As well as being a core element of the EU's economic security strategy, enhancing research security also contributes to strategies that aim to improve the EU's resilience to emerging

([108]) https://commission.europa.eu/topics/research-and-innovation/choose-europe_en

threats and crises, the European Preparedness Union Strategy ([109]), protect its internal security, the European Internal Security Strategy ([110]) and strengthen its democratic resilience, the Democracy Shield ([111]).

6.3. EU initiatives to enhance research security

In line with the Council Recommendation, the Commission has launched a variety of initiatives and actions to deliver on the Council's requests. The publication of the Research Security Monitor is part of this endeavour, and it will feed into the different work strands. This section provides an update on the main initiatives.

Working together with Member States and the R&I sector

As requested by the Council ([112]), the Commission is making full use of the governance structures of the European Research Area (ERA) to support implementation of the Recommendation. The work carried out in this context supports the Member States and the R&I sector in their efforts to develop coherent sets of policy measures and create support structures through peer learning and capacity building. It also provides a space to discuss the joint development of EU-level initiatives.

On 28 February 2025 the Commission presented its proposal for the ERA policy agenda 2025-2027, which includes research security as a priority action. After negotiations the Council adopted the ERA policy agenda in May 2025 ([113]), confirming research security as a priority action for further developing the European Research Area in the coming years.

To further this work, the Commission has launched separate strands of policy-related work with the main target groups: (1) Member State national authorities, (2) EU-based national research funding organisations, and (3) research performers through their European stakeholder organisations. For each target group a dedicated network of representatives has been created, and meetings and workshops are being organised throughout the ERA policy agenda's time frame (2025-2027).

Other ERA governance bodies will be kept informed and actively involved, as necessary. This includes bodies such as ERAC (committee at Director-General level), the ERA Forum and in particular its subgroup on the global approach, which covers issues related to international research and innovation cooperation ([114]).

European Flagship Conference on Research Security

Work carried out since the adoption of the Council Recommendation culminated in the first European Flagship Conference on Research Security: for responsible, open and secure

([109]) 26.3.2025: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025JC0130
([110]) 1.4.2025: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025DC0148
([111]) 12.11.2025: https://commission.europa.eu/document/2539eb53-9485-4199-bfdc-97166893ff45_en
([112]) Recommendation 16.
([113]) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CONSIL:ST_8469_2025_INIT
([114]) https://european-research-area.ec.europa.eu/era-governance

research and innovation, which took place from 28 to 30 October 2025 in Brussels ([115]). At the conference around 500 participants of different target groups from across Europe and beyond met in a host of sessions aimed at sharing information, disseminating results of work done so far and paving the way for the next steps in the policymaking process.

The organisation of the event was the result of a unique process. As requested by the Council ([116]), the event was co-organised with sectoral stakeholders. As a clear sign of the sector's active involvement and resolve, 12 European stakeholder organisations committed to co-organise the event: ALLEA, CESAER, Coimbra Group, EARTO, EECARO, EUA, EU-LIFE, G6, LERU, Science Europe, The Guild and YERUN. Together, these organisations represent a significant part of the EU's research and innovation ecosystem. Each organisation contributed by preparing one or more parallel sessions, bringing in their own members, expertise and viewpoints. In addition, groupings of countries (both EU and non-EU) and international organisations presented and discussed their approaches to research security.

The conference showcased the state of the art in research security, the European balanced approach to it and how governments, funders and research performers are teaming up. As such, it offered an excellent opportunity for peer learning, networking and inspiring each other. To the EU's international partners, the conference sent a strong message that the EU is serious about safeguarding its research and innovation.

As stated in the Council Recommendation, the aim is to organise the flagship conference on a biennial basis, with the second edition in autumn 2027.

Setting up a Centre of Expertise on Research Security

Since adoption of the Council Recommendation, the Commission has been exploring options for setting up a Centre of Expertise on Research Security. As specified by the Council ([117]), its core objectives will be: (i) to invest in and further develop the evidence base for research security policymaking; and (ii) to create a community of practice, bringing together experts and practitioners from across Europe. The Preparedness Union Strategy, published on 26 March 2025, which aims to enhance the EU's civilian and military preparedness and readiness for future crises, includes establishing the centre among its key actions ([118]).

Creating a permanent hub for the EU helps pool efforts and allows higher levels of policy maturity to be reached more quickly. The launch of the centre is in keeping with an approach that calls for structural efforts with long-term impact: research security cannot be addressed by a one-off recommendation, report or conference alone. The work done in

([115]) Commission news article of 28.10.2025: https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/commission-announces-new-measures-strengthen-research-security-2025-10-28_en and Commission news article of 21.11.2025: https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/together-responsible-open-and-secure-research-and-innovation-2025-11-21_en

([116]) Recommendation 23.

([117]) Recommendation 18.

([118]) Joint communication on the European Preparedness Union Strategy, 26.3.2025 (link), and its Annex.

the context of the centre will structurally feed into and underpin the policy-related work in the context of the ERA governance structures.

The centre will, inter alia, carry out the following core tasks, each covering various services and deliverables:

- *Research on research security*. To strengthen the evidence base for policymaking different forms of research and analysis will be conducted. This could include analysis of the threat landscape and studies into effectiveness of research security policies and measures.
- *Dissemination*. Information sharing and raising situational awareness will be achieved through active dissemination of information and best practices. An online platform will be developed to underpin these efforts.
- *Tools and guidance*. Under this task practical tools, training modules, webinars, awareness raising campaign toolkits and guidance material will be developed.
- *Peer learning and capacity building*. This task includes bringing together, in a Union-wide community of practice, relevant networks and stakeholders. Workshops, peer-to-peer exchanges and conferences will be organised, and technical assistance can be provided.

The aim is to launch the core functionalities of the centre around mid 2026, i.e. two years after the Recommendation's adoption, after which a period of further development will follow, taking into account feedback from Member States and the stakeholders.

Other EU research security initiatives

In addition to the activities using the ERA governance, the co-organisation of the flagship conference and the establishment of a centre of expertise, the Commission is working on several other initiatives contained in the Council Recommendation.

Resilience testing. How resilient are research performing organisations? To find out, Member States are recommended to gain insight into the resilience of their R&I sector, for instance through resilience testing and incident simulations ([119]). At the same time, the Council asked the Commission to develop a resilience-testing methodology that can be used on a voluntary basis by Member States with their research performing organisations ([120]).

The Commission intends to prepare such a methodology and make it available for Member States in 2026. By applying the same methodology across the EU, a degree of comparability can be ensured. This can help identify vulnerabilities that should be prioritised. Once the methodology has been developed, a structured process for the application of the methodology will be launched among the participating Member States.

Due diligence platform. To facilitate due diligence into prospective third-country partners, the Commission has been asked by the Council ([121]) and the sector to develop tools and resources providing reliable information and data on such partners.

([119]) Recommendation 8.
([120]) Recommendation 20, also included as one of the actions of the Preparedness Union Strategy (Action 41).
([121]) Recommendation 22.

In response to this call, the Commission is working on developing a secure IT platform that will compile reliable information about foreign research institutes to help researchers learn about the potential risks associated with cooperating with foreign research institutes. The due diligence platform is intended to support researchers and research organisations across the EU in making well-informed decisions and strengthening overall confidence in international cooperation.

A first pilot version is expected to be available at the end of 2026.

Interpretative guidance. With regard to the Council's request to prepare interpretative guidance on some key elements of the Council Recommendation ([122]), the Commission is working on practical guidance notes. The aim is to further operationalise such key elements and give guidance to practitioners and policymakers on their application. Work has been started on a note on 'risk appraisal' ([123]). Further topics could include 'risk mitigation' (as a logical next step after risk appraisal), 'safeguarding innovation' (focusing on private R&I) and the concept of 'intangible technology transfer' as defined by the Export Control Regulation.

Critical technologies risk assessment. Following the publication of the Commission Recommendation on critical technologies in October 2023 ([124]), a risk assessment process has been launched, involving the Member States, in 10 technology domains considered critical for economic security.

As a priority, the assessment focused on four technology domains: artificial intelligence technology, advanced semiconductor technology, quantum technology and biotechnology. The process has helped identify those parts of the technology domains that are most sensitive and gain insight into developments in those domains.

Further work, refining the results and formulating policy responses in those four areas, is still ongoing and risk assessments in the remaining six technology domains are being prepared.

Safeguards in EU funding programmes. Whereas the current Horizon Europe programme (2021-2027) already includes a range of safeguards to protect the security and interests of the Union (see also Section 4.2), these need to be updated to take account of geopolitical developments and strategic policy responses to those developments at national and EU level ([125]). In July 2025 the Commission presented its proposals for the next multiannual financial framework (MFF) for 2028-2034, including proposals for the next Horizon Europe programme ([126]) and a new European Competitiveness Fund ([127]).

Where necessary and duly justified, the Commission's proposals provide the legal means to ensure that appropriate measures can be taken. Such measures may include targeted

([122]) Recommendation 24.
([123]) As defined in recital 18(5) of the Recommendation. Alongside the proposal for a Council recommendation, the Commission has already published a fact sheet on building blocks for risk appraisal: https://research-and-innovation.ec.europa.eu/document/c0c0dbae-c7d7-45d8-b59b-413f54aa8983_en
([124]) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202302113 and referred to in recommendation 21.
([125]) As alluded to in recommendation 21.
([126]) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025PC0543
([127]) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025PC0555

restrictions on the scope of participation and place of performance, restrictions on transfers of and access to results, or risk assessments to mitigate threats. Overall, a variety of measures could be applied, at programme, call or project level. The implementation of the Horizon Europe programme should follow a risk-based approach, whereby risks will be detected early on and be addressed through proportionate and effective measures, as necessary.

The two legislative proposals are currently being discussed by the co-legislators (the Council and the European Parliament) and the outcome of these discussions cannot be pre-empted.

6.4. International partnering on research security

In its Recommendation, the Council asks the Commission to strengthen the dialogue and cooperation with international partners on research security ([128]). This involves exchanging information, experience and best practices, seeking ways to align safeguarding measures and endeavouring to speak with one EU voice on the matter in multilateral forums.

That recommendation is fully in line with the EU's global approach strategy for international R&I cooperation ([129]) and the 'partnering' dimension of the EU's economic security strategy ([130]). In the context of that strategy, partnering is about cooperating with countries which share the EU's concerns on economic security and are on similar de-risking paths and also with those which have common interests and are willing to cooperate to achieve a more resilient and secure economy.

With the Council Recommendation as a basis, the Commission has stepped up engagement with international partners both bilaterally and multilaterally on the topic of research security. Bilateral dialogue is ongoing both with European countries such as Norway, Switzerland and the UK and with international partners such as Australia, Canada, Japan, South Korea and the US. Multilateral forums active in the field are the G7, the OECD and NATO.

Among partners there is a notable readiness and commitment to exchange with the EU and to exchange with and learn from each other. Moreover, these interactions reveal a remarkable comparability of approach across partners, with national authorities in those countries developing tools and guidance for the sector and putting in place support structures in some shape or form.

([128]) Recommendation 26.
([129]) For further details, see the second implementation report on the global approach to R&I.
([130]) Joint communication on European Economic Security Strategy, JOIN(2023) 20 final of 20 June 2023: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023JC0020&qid=1687525961309

7. CONCLUDING REMARKS

There is growing awareness among policymakers, experts and practitioners in Europe that the security implications of international research and innovation cooperations should be taken into account.

This first Research Security Monitor 2025 provides a qualitative baseline for research security policies and measures across the EU. Through an overview of selected examples and practical insights derived from real-life examples, it aims to inform and inspire policymakers and practitioners who are in the process of developing such measures and policies.

The monitor clearly demonstrates that the work launched in 2024 through the Council Recommendation on enhancing research security has had added value. It has provided the research and innovation community with a reference point for research security with common definitions, shared principles and guidance on what an effective and proportionate policy response enhancing research security looks like.

The Council Recommendation was also well timed. It created political momentum and accelerated a process that had already started in several Member States and encouraged others to start reflecting on policies and measures. It provided a sense of direction at the right moment, for policymakers and practitioners alike.

One and a half years later, it can be concluded that the Recommendation is impactful and has triggered new initiatives and strengthened existing policies and measures at all levels.

There appears to be a remarkable consensus on what should be the key elements of effective and proportionate research security policies. There is broad support from Member States for what may be called the European approach to research security, one that is about keeping international research and innovation cooperation both open and secure. It is an approach based on the notion that research performers bear primary responsible for ensuring research security in their international engagements: ‘with academic freedom comes academic responsibility’. There is also a shared understanding that research performers need help from public authorities, who should share (threat) information and provide guidance and support.

It should be noted that this approach also clearly resonates with the sector. A clear sign is the active engagement of all leading European R&I stakeholder associations, through dedicated task forces, working groups and events on the topic. This sectoral support is certainly not a given, as measures aimed at enhancing security are easily perceived as affecting or even opposing open science, international cooperation and academic freedom. Designing research security policies and measures in a way that respects these core academic values is a *sine qua non* of sectoral support.

In terms of policies and measures, levels of maturity differ significantly both between and within countries and across the EU. From a security perspective, these differences are potential vulnerabilities, putting the security of the EU and its Member States at risk. From the perspective of the European Research Area, such differences and disparities signify the

lack of a level playing field and thus risk hampering borderless and seamless cooperation within the EU.

More action is therefore urgently needed at all levels: in policy frameworks at national level, in grant application procedures of research funders and in risk management processes within the research performing organisations themselves.

The same is true at Union level, where several key initiatives are still being developed. There is a clear and urgent need to develop and launch initiatives such as the European Centre of Expertise on Research Security and a secure online due diligence platform.

Joint work at Union level supporting Member States and the R&I sector should help all those involved reach higher levels of maturity more quickly and contribute to a level playing field within the European Research Area. However, peer-learning opportunities, training and capacity-building efforts are needed at all levels, from Union to national level to the level of individual research performing organisations. This is a shared commitment and responsibility.

In the meantime, there is scope and willingness to continue and further strengthen cooperation both with international partners, including countries such as Australia, Canada, Japan and South Korea, and within multilateral forums, such as the OECD, G7 and NATO, in order to align policies.