EUROPEAN
COMMISSION

Brussels, 24.1.2024
COM(2024) 26 final

2024/0012 (NLE)

Proposal for a

COUNCIL RECOMMENDATION

on enhancing research security

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

As outlined in the European economic security strategy, published in June 2023[1], a global increase in geopolitical tensions and hostile economic actions, cyber and critical infrastructure attacks, foreign interference and disinformation have exposed risks and vulnerabilities in our societies, economies and companies. In some cases, it became clear that Europe should be better prepared for evolving, new and emerging risks that have arisen in this more challenging geopolitical context.

Critical and dual-use technologies play a pivotal role in this context, with some of our competitors to use emerging and disruptive technologies to boost their political, economic, and military positions. This may result in European research and innovation being affected by malign influence and being misused in ways that affect our security or infringe our ethical norms.

The research and innovation sector is particularly vulnerable due to its openness and internationalisation, which is in its DNA. Therefore, a tailor-made approach strongly rooted in academic freedom and institutional autonomy, principles that are fundamental to research and innovation, is needed to enhance research security in the research and innovation sector across Europe.

Higher education institutions and research performing organisations must navigate an increasingly complex and tense international landscape. It is the EU's duty to assist them in traversing this terrain responsibly and securely in full respect of academic freedom and institutional autonomy.

The proposed Council recommendation offers, for the first time, a joint definition of the problem and a shared sense of urgency. It provides political guidance on what an effective policy response could look like, while taking into consideration that much of the work on research security is about navigating 'grey zones' where certain forms of international research and innovation cooperation may not be forbidden but are nevertheless undesirable because they pose risks to the security of the Union and its Member States or are unethical.

• Consistency with existing policy provisions in the policy area

The European economic security strategy follows a three-pillar approach: promotion of the EU's economic base and competitiveness; protection against economic security risks; and partnership with the broadest possible range of countries to address shared concerns and interests. Its aim is to provide a framework for a robust assessment and management of risks to economic security at EU, national and business level while preserving and increasing our economic dynamism.

In the strategy the Commission made a commitment to 'propose measures to improve research security ensuring the systematic and rigorous enforcement of the existing tools and identifying and addressing any remaining gaps, while preserving openness of the innovation ecosystem.' The proposal for a Council recommendation delivers on this commitment by formulating guiding principles for responsible internationalisation and key policy actions at

[1] Joint communication of the Commission and the High Representative on the European economic security strategy, JOIN(2023)20 of 20.06.2023 (link).

national and sectoral level to enhance research security and listing initiatives at EU level to support the efforts of the Member States and the sector.

The proposal for a recommendation complements and builds on work ongoing since the Commission published its communication on the Global Approach to research and innovation in May 2021[2]. In that communication, it presented a strategy to preserve openness in international research and innovation cooperation, while promoting a level playing field and reciprocity underpinned by fundamental values.

Through its Council conclusions of September 2021 on the Global Approach, the Council gave a mandate to work on tackling foreign interference in research and innovation.[3] On this basis, important follow-up initiatives were undertaken, notably the Commission's adoption in January 2022 of a staff working document on tackling R&I foreign interference.[4] The document is used by Member States and R&I stakeholders as a basis to discuss research security and as a source of inspiration to develop their own tailor-made guidelines and tools. The European Parliament welcomed the document in its resolution of 6 April 2022 on the Global Approach.[5] The Commission also facilitated peer learning among Member States through a mutual learning exercise and is developing an online one-stop shop that will bring together all relevant documents, reports and tools on research security.

Additionally, a policy debate on 'Knowledge security and responsible internationalisation' took place in the Competitiveness Council of May 2023, which provided invaluable insights and guidance for the proposal.

- **Consistency with other Union policies**

The proposed recommendation is part of a comprehensive package of measures following up on the European economic security strategy of 20 June 2023. As such, the proposal forms a building block in an overarching effort to enhance the EU's economic security at large. On 3 October 2023, the Commission adopted a recommendation in which it identified critical technology areas for the EU's economic security for further risk assessment with Member States[6]. The outcome of this risk assessment could inform other measures to implement the European economic security strategy, including measures to enhance research security. The public consultation launched with the White paper on outbound investment will be considered, in particular when it comes to elements relevant for research and innovation.

Additionally, the proposed recommendation is complementary to and consistent with a number of other EU initiatives, notably:

– the work done on countering hybrid threats, in the framework of the EU Security Union strategy[7] and the Strategic Compass for Security and Defence[8];

---

[2] Commission communication on the Global approach to research and innovation: Europe's strategy for international cooperation in a changing world, COM(2021) 252 of 18.05.2021 (link).

[3] Council conclusions on the Global approach to R&I of 28.09.2021 (link), notably paragraphs 3, 11 and 23.

[4] European Commission, Directorate-General for Research and Innovation, *Tackling R&I foreign interference – Staff working document*, Publications Office of the European Union, 2022 (link).

[5] Resolution of the European Parliament on a global approach to research and innovation, P9_TA(2022)0112 of 06.04.2022 (link).

[6] Commission recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States, C(2023) 6689 of 03.10.2023 (link).

[7] Commission communication on the EU Security Union Strategy, COM(2020)605 of 24.07.2020 (link).

[8] Council of the EU: A Strategic Compass for Security and Defence, ST 7371/22 of 21.03.2022 (link).

– the European rules for the export outside the EU of dual-use goods and technology as laid down in the EU's Export Control Regulation.[9] To help higher education institutions and research performing organisations the Commission published in September 2021 a recommendation on compliance programmes for research involving dual-use items[10];

– the Defence of Democracy package, adopted by the Commission in December 2023 ahead of the European elections of June 2024. The package aims to tackle foreign interference threats through increased levels of transparency of interest representation activities, while at the same time encouraging civic engagement and citizens' participation in our democracies[11].

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

• Legal basis

The initiative falls under the 'research and technological development' policy area, where the EU and its Members States share competences in line with Article 4(3) of the Treaty on the Functioning of the European Union (TFEU). The proposed Council recommendation is based on Article 182(5) in conjunction with Article 292 TFEU.

Article 182(5) TFEU opens up the possibility of complementing the activities planned in the multiannual framework programme by allowing the European Parliament and the Council, acting in accordance with the ordinary legislative procedure and after consulting the Economic and Social Committee, to establish necessary measures for implementing the European Research Area.

Article 292 TFEU provides the legal basis for the Council to adopt recommendations based on a proposal from the Commission.

The initiative does not propose any extension of EU regulatory power or binding commitments on Member States. It is the Member States who will decide, based on their national circumstances, how they implement this Council recommendation.

• Subsidiarity (for non-exclusive competence)

The present proposal is in conformity with the principle of subsidiarity as provided for in Article 5(3) of the Treaty on the European Union (TEU).

While national governments are best placed to reach out to their universities and other research performing organisations and support them in taking the necessary measures, EU-level cooperation and coordination is needed to ensure the proper functioning of the European research area and to reduce disparities caused by differences in national research security measures.

Currently, awareness of the risks is not evenly spread across the EU. An increasing number of Member States and R&I actors are developing and introducing dedicated safeguarding measures, while others still seem largely unaware, creating vulnerabilities that could easily be exploited. A minimum level of consistency of approach across the EU is therefore essential.

---

[9] Regulation (EU) 2021/821 setting up an EU regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (link).

[10] Commission recommendation on internal compliance programmes for controls of research involving dual-use items […], 2021/1700 of 15.09.2021 (link).

[11] Commission communication on Defence of Democracy, COM(2023) 630 of 12.12.2023 (link).

- **Proportionality**

The present proposal is in conformity with the principle of proportionality as provided for in Article 5(4) TEU. Neither the content nor the form of this proposed Council recommendation exceeds what is necessary to achieve the objective of achieving a minimum level of consistency of approach across the EU.

The legal status of this initiative should ensure ownership and endorsement by the Member States. At the same time, it should rely predominantly on self-governance by the R&I sector, in line with academic freedom and institutional autonomy.

The recommendation helps Member States and research performing organisations to develop and implement policies and measures that are both effective and proportionate. It underscores the importance of international cooperation and openness following the principle 'as open as possible, as closed as necessary'. It also shows which risk management measures could be introduced, fully respecting academic freedom and institutional autonomy, while avoiding discrimination and stigmatisation.

- **Choice of the instrument**

The proposed Council recommendation provides guidance to Member States about how to identify and address research security risks effectively. It recommends that Member States support their research and innovation sector, taking appropriate steps to raise awareness and build resilience. Building on the staff working document on tackling R&I foreign interference, a Council recommendation would ensure that all Member States are actively involved and committed at political level.

Alternatively, a Commission recommendation or communication could be considered. In terms of content, these could in principle cover the same issues as a Council recommendation. However, what these instruments have in common is that they do not actively involve or commit the Member States. There is no guarantee that the addressees share the proposed approach and the sense of urgency.

A legally binding initiative, such as a directive or regulation, regulating international research and innovation cooperation in such a way that risks are properly identified and addressed by Member States would guarantee legal consistency across the Union. However, the main downside of a binding instrument in this specific context is that it would be very difficult to conceive it in such a way that the division of competence between the EU and the Member States as well as the principles of academic freedom and institutional autonomy are respected.

For these reasons, a proposal for a Council recommendation is considered to be the appropriate policy instrument to address the issues at hand.

3. RESULTS OF EX-POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

- **Ex-post evaluations/fitness checks of existing legislation**

Not applicable.

- **Stakeholder consultations**

The proposed Council recommendation builds on the Commission's staff working document on tackling R&I foreign interference of January 2022. Throughout 2023, a mutual learning

exercise on tackling R&I foreign interference took place, with experts from 13 Member States exchanging national experience and expertise. In addition, three dedicated meetings on research security with Member State experts took place in the context of the EU Knowledge Network on China (EUKNOC).

The development of the proposal was also informed by a call for evidence, which was open for public feedback on the 'Have your say' webpage from 6 December 2023 until 3 January 2024. The Commission received 56 contributions, almost 40% came from academic or research institutions. In addition to the call for evidence, a targeted consultation meeting took place on 15 December 2023, with participation of representatives of the main EU-level stakeholder organisations in research and innovation.

- **Collection and use of expertise**

In addition to the input received during the consultation process, the proposal is underpinned by extensive evidence, reports and studies collected over recent years. Key sources of evidence include a large and still growing body of guidance documents on research security developed by Member States and sectoral organisations[12], as well as reports on the issue by think tanks, stakeholder organisations and advisory councils.

Due consideration has also been given to the research security policies that some of our international partners have implemented over the past years, and to the insights and experience they gained while doing so. This includes the policies of countries such as the United States, the United Kingdom, Australia and Canada[13]. In the context of the multilateral dialogue on values and principles[14], a workshop on research security took place in December 2023, in which international partners actively participated.

- **Impact assessment**

An impact assessment has not been carried out, given the complementary approach of the activities to Member State initiatives and the non-binding and voluntary nature of the proposed activities.

The impact of the recommendation largely depends on the engagement and the readiness to act of Member States and sector organisations and is therefore impossible to assess in advance. Provided that the Council adopts the proposal and Member States commit to implementing its recommendations with the support of the sector, the proposal has the potential to enhance research by raising awareness and building resilience throughout Europe.

- **Regulatory fitness and simplification**

The proposal is not linked to the Commission's REFIT legislative simplification programme. Nonetheless, every effort is made to make efficient use of scarce resources, including by using existing European research area governance structures and by relying on existing reporting structures. Also, the proposed recommendation emphasises that unnecessary administrative burden for the sector should be avoided when introducing safeguarding measures and that in the context of research funding the time-to-grant should not be unnecessarily delayed.

---

[12] See for instance the 'annotated collection of guidance for secure and successful R&I cooperation' (2022) that DLR-PT compiled at the request of the Commission (link).

[13] More information can for instance be found on the following websites: for the US (link), for the UK (link), for Australia (link), and for Canada (link).

[14] More information on the multilateral dialogue on values and principles can be found here: link.

- **Fundamental rights**

One of the proposal's main objectives is to support Member States and research performing organisations in ensuring that international research and innovation cooperation does not violate fundamental values and human rights. The recommendation has protecting fundamental academic values, notably academic freedom and research integrity, at its core.

4. BUDGETARY IMPLICATIONS

While this initiative will not require additional resources from the EU budget, the measures in this recommendation will mobilise sources of funding at EU, national and sector level.

For the 'European Centre of Expertise on Research Security' that the Commission intends to establish, the existing Horizon Europe budget would be mobilised. In terms of organisational set-up several options are under consideration, which the Commission will further explore taking into account the Member States' and stakeholders' preferences as regards its functionalities.

5. OTHER ELEMENTS

- **Implementation plans and monitoring, evaluation and reporting arrangements**

To support Member States and stakeholders as they implement the recommendation, full use will be made of the existing European research area governance structures. It is expected that research security will be reflected in the next European research area policy agenda for 2025-2027, which is currently under preparation in dialogue with Member States and stakeholders.

Commission reporting will rely on the already existing biennial reporting on the Global Approach to Research and Innovation. The next report is envisaged for mid-2025. Member States are invited to submit national action plans on how they intend to implement the recommendation within 9 months of its adoption.

- **Explanatory documents (for directives)**

Not applicable.

- **Detailed explanation of the specific provisions of the proposal**

The overall aim of the initiative is to help Member States, higher education institutions and research performing organisations, both public and private, address research security risks. This will ensure that research, innovation and higher education activities are not misused or captured in a way that affects the security of the EU and its Member States or are unethical. To this end, the proposed Council recommendation contains the following sections:

– After introducing the issue at stake and the political background of the proposal in the recitals, its scope is explained. A definition of 'research security' is proposed, which draws on the main elements of the various definitions in use internationally. It is also clarified which organisations and stakeholders are primarily addressed in the context of the recommendation.

– Then, principles for responsible internationalisation are proposed. These principles are conceived in such a way that they can be used to underpin the formulation and design of a policy response to research security at any level (EU, national or individual research performing organisations). The principles draw on the approaches taken in national and sectoral guidance on responsible

internationalisation. From the response to the call for evidence, it can be concluded that these principles clearly resonate with the stakeholder community.

– The following section contains the actual recommendations to the Member States. It is divided in four subsections. The first subsection formulates what public authorities are recommended to do for the research and innovation sector in terms of creating a support structure and providing guidance. The second subsection addresses the pivotal role national funding organisations have in enhancing research security. The third subsection elaborates on what Member States are recommended to do to support higher education institutions and research performing organisations when introducing safeguarding measures and policies.

– The final subsection outlines a number of supporting actions and initiatives of the Commission for which the Member States' facilitation is needed.

– The final section specifies how the follow-up to the recommendation is facilitated and monitored.

2024/0012 (NLE)

Proposal for a

COUNCIL RECOMMENDATION

on enhancing research security

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 292, first and second sentence in conjunction with Article 182(5) thereof,

Having regard to the proposal from the European Commission,

Whereas:

(1) Openness, international cooperation, and academic freedom are at the core of world-class research and innovation. Yet, with growing international tensions and the increasing geopolitical relevance of research and innovation, our researchers and academics are increasingly confronted with risks to research security when cooperating internationally resulting in European research and innovation being affected by malign influence and being misused in ways that affect our security or infringe our ethical norms. It is therefore vital that European higher education institutions and research performing organisations, both public and private, are supported and empowered to address these risks. Precise and proportionate safeguarding measures are needed to keep international cooperation open and safe.

(2) Open science ensures that science is made as accessible as possible for the benefit of science, the economy and society at large while international cooperation contributes to tackling global challenges effectively. Academic freedom implies that researchers are free to conduct their research and choose the research methods as well as their research partners from around the globe, while international mobility of research talent enriches scientific enquiry and is essential for fostering innovation and achieving scientific breakthroughs.

(3) Growing strategic competition and the return to power politics are leading to increasingly transactional relations between States. This shift has resulted in threats that are more diverse, unpredictable, and oftentimes hybrid[1]. Given the pivotal role of technology for political, economic, and military pre-eminence, some of the EU's competitors are seeking global primacy in emerging and disruptive technologies to enhance their military and intelligence capabilities while actively pursuing civil-military fusion strategies.

(4) Hybrid threats may affect all relevant sectors, however, owing to its openness, academic freedom, institutional autonomy and worldwide collaboration, the research and innovation sector is particularly vulnerable. EU-based researchers and innovators

[1] Hybrid threats refer to when, state or non-state, actors seek to exploit the vulnerabilities of the EU to their own advantage by using in a coordinated way a mixture of measures (i.e.: diplomatic, military, economic, technological) while remaining below the threshold of formal warfare (link).

are targeted to capture state-of-the-art knowledge and technology, at times using methods that are deceptive and covert or through outright theft, but more often exploiting seemingly *bona fide* international academic cooperation. Next to jeopardising our security, these hybrid threats could affect academic freedom in Europe.

(5) Higher education institutions and other research performing organisations are thus navigating an increasingly challenging international context, with risks of undesirable transfer of critical knowledge and technology to countries of concern, where it may be used to strengthen the capabilities of their military, or for purposes that are in violation of fundamental values. While not always legally prohibited, these collaborations are undesirable as they pose significant security and ethical concerns.

(6) In accordance with institutional autonomy and academic freedom, higher education institutions and other research performing organisations are primarily responsible for developing and managing their international cooperation. Public authorities at all levels should provide them with assistance and support, empowering them to take informed decisions and manage the risks to research security involved, ensuring that international cooperation in research, innovation and higher education remains both open and secure.

(7) In recent years, discussions on strengthening research security have been ongoing at the EU level, where several initiatives have also been undertaken:

– In May 2021, the Commission published its communication on the Global approach to research and innovation[2], outlining a new European strategy for international research and innovation policy. The Council responded in September 2021 through the adoption of Council conclusions[3] giving a political mandate to working jointly on research security.

– Several safeguards were introduced in the EU's framework programme for research and innovation 2021-2027, Horizon Europe[4], giving effect to the EU's distinctive responsibility as one of Europe's largest research funders.

– In November 2021, the Council adopted the ERA policy agenda 2022-2024 as part of its conclusions on Future governance of the European Research Area (ERA)[5], in which tackling foreign interference is included in one of its priority actions.

– In January 2022, following up on its commitments stemming from both the Global approach and the ERA policy agenda, the Commission published its staff working document on tackling R&I foreign interference[6]. Additionally, to

---

[2] Commission communication on the Global approach to research and innovation: Europe's strategy for international cooperation in a changing world, COM(2021) 252 of 18.05.2021 (link).

[3] Council conclusions on Global approach to R&I of 28.09.2021 (link), notably paragraphs 3, 11 and 23.

[4] The Horizon Europe regulation, EU 2021/695 of 28.04.2021 (link), provides *inter alia* for a security appraisal of all projects selected for funding (Article 20), the possibility to exclude entities based in or controlled by third countries from certain calls (Article 22(5)), as well as to add eligibility criteria to those set out in paragraphs 2 to 5 to take into account specific policy requirements or the nature and objectives of the action (Article 22(6)) and the right for the Commission or the relevant funding body to object to transfers of ownership of results, or to grants of an exclusive license regarding results (Article 40(4)). Similar provisions are included in the European Defence Fund and the European Space Programme.

[5] Council conclusions on Future governance of the European Research Area (ERA) of 26.11.2021 (link).

[6] European Commission, Directorate-General for Research and Innovation, *Tackling R&I foreign interference – Staff working document*, Publications Office of the European Union, 2022 (link).

facilitate peer learning among Member States, a Mutual Learning Exercise (MLE) took place throughout 2023.

– The Commission's communication on 'A European Strategy for Universities'[7] recalls that higher education institutions have a unique position at the crossroads of education, research, innovation, thus playing a critical role in achieving the European Education Area[8] and the European Research Area, identifies foreign interference in higher education institutions as a threat and supports the implementation of the guidelines on foreign interference. The role of higher education institutions in protecting European democratic values is at the core of the strategy.

– The European Parliament adopted on 9 March 2022 a resolution on 'Foreign interference in all democratic processes in the European Union, including disinformation' in which it calls for strengthening academic freedom, improving transparency of foreign funding as well as mapping and monitoring of foreign interference in the cultural, academic and religious spheres[9].

– From a broader security and defence perspective, work is ongoing in the framework of the EU Security Union strategy[10] as well as the Strategic Compass for Security and Defence[11] aiming at a shared assessment of threats and challenges and greater coherence in actions in the area of security and defence, including through different instruments to detect and respond to hybrid threats in an EU Hybrid Toolbox.

– In the domain of EU export control rules for dual-use goods and technology, the EU's Export Control Regulation[12] is of significant importance to research security. To help higher education institutions and research performing organisations, the Commission published in September 2021 a recommendation on compliance programmes for research involving dual-use items[13].

(8) The Commission and the High Representative adopted a joint communication on European economic security strategy[14] which aims to ensure that the Union continues to benefit from economic openness, while minimising risks to its economic security. The Strategy proposes a three-pillar approach: promotion of the EU's economic base and competitiveness; protection against risks; and partnership with the broadest possible range of countries to address shared concerns and interests. In each of the pillars, research and innovation have a key role to play.

(9) Following up on this joint communication, the Commission has identified critical technology areas for the EU's economic security for further risk assessment with

---

7 Commission communication on a European strategy for universities, COM(2022)16 of 18.01.2022 (link).
8 Commission communication on achieving the European Education Area by 2025, COM(2020)625 of 30.09.2020 (link).
9 European Parliament resolution on Foreign interference in all democratic processes in the European Union, including disinformation, P9_TA(2022)0064 of 09.03.2022 (link).
10 Commission communication on the EU Security Union Strategy, COM(2020)605 of 24.07.2020 (link).
11 Council of the European Union: A Strategic Compass for Security and Defence, ST 7371/22 of 21.03.2022 (link).
12 Regulation (EU) 2021/821 setting up an EU regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (link).
13 Commission recommendation on internal compliance programmes for controls of research involving dual-use items […], 2021/1700 of 15.09.2021 (link).
14 Joint communication on European economic security strategy, JOIN(2023)20 of 20.06.2023 (link).

Member States in its recommendation of 3 October 2023[15]. Risk assessments have already been launched as a matter of priority on four of the ten identified critical technology areas, namely advanced semiconductors, artificial intelligence, quantum and biotechnologies. The outcome of risk assessments, when finalised, could inform other measures to implement the European economic security strategy, including measures to enhance research security.

(10) The joint communication on the European economic security strategy furthermore announced that the Commission would propose measures to enhance research security by ensuring the use of the existing tools and identifying and addressing any remaining gaps, while preserving the openness of the research and innovation ecosystem.

(11) In terms of gap identification referred to in the previous point, discussions with Member States and stakeholder organisations demonstrate an urgent need among policymakers and practitioners for more conceptual clarity, a shared understanding of the issues at hand as well as of what constitutes a policy response that is both proportionate and effective.

(12) An increasing number of Member States has developed or is in the process of developing policies aimed at enhancing research security. While these efforts generally contribute to raising awareness and boosting resilience, an uncoordinated multiplication of national measures would result in a patchwork of national policies, disparities among Member States, and thereby fragmentation of the European Research Area. EU level coordination is therefore needed to provide for a level-playing field and to protect the integrity of the European Research Area.

(13) It should be emphasised that research security safeguards can only be truly effective if consistently applied at all levels, including EU, national, regional as well as the level of individual public and private research performing organisations, so as to avoid loopholes and circumvention.

(14) In specific cases, compliance to relevant EU legislation and rules could benefit from interpretative guidance. This applies in particular to export control rules, notably the intangible transfer of technology (ITT), the visa requirements for foreign researchers[16], as well as the interpretation of certain open science and intellectual asset management requirements from a research security perspective.

(15) It is important that hybrid threats affecting the research and innovation ecosystem are structurally assessed, enhancing situational awareness among policymakers by relying on the Single Intelligence Analysis Capacity (SIAC), in particular the Hybrid Fusion Cell, the work of the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE)[17] as well as ENISA in relation to cybersecurity threats[18]

(16) Taking into account that a significant share of research and innovation takes place in the private sector, it is key to develop targeted guidance and tools for business, notably research-intensive start-ups and small and medium sized companies. While the risks to

---

[15] Commission recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States, C(2023) 6689 of 03.10.2023 (link).

[16] Directive (EU) 2016/801 on the conditions of entry and residence of third-country nationals for the purposes of research, studies, training, voluntary service, pupil exchange schemes or educational projects and au pairing of 11.05.2016 (link).

[17] The Hybrid CoE is an autonomous, network-based international organisation countering hybrid threats, established in 2017, based in Helsinki (link).

[18] The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe (link).

which companies are exposed may be similar, their situation differs from higher education institutions and research performing organisations. In this light, attention should be drawn to the existing rules, including those on the control of exports of dual-use items, the screening of foreign investments as well as the ongoing work on the monitoring of outbound investments.

(17) In the preparation of this recommendation, due attention has been paid to experience from Member States, as well as from the EU's partners, both in bilateral and multilateral settings. It takes into account policy lessons from key partners, while emphasising that an approach should be formulated that suits the unique European context. Continued efforts are being made with our partners to exchange information and experience, share good practices and to seek ways to align safeguard measures, including through the multilateral dialogue on values and principles, as part of association negotiations and joint S&T steering committee meetings in the context of international science and technology agreements, as well as in multilateral fora, such as G7, OECD and NATO, and relevant multilateral export control arrangements.

(18) Research security is a concern that is gaining increasing attention and the ongoing debate on the risks involved and how to best manage them is intensifying. Consequently, there is a need to further raise awareness, facilitate peer learning between Member States and relevant stakeholder organisations, as well as contribute to a learning approach that is both flexible and agile.

SCOPE

1. For the purposes of this recommendation, 'research security' refers to managing risks related to:

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

   (b) malign influence on research, where research can be instrumentalised by or from third countries in order to diffuse certain narratives or incite self-censorship among students and researchers infringing academic freedom and research integrity in the EU;

   (c) ethical or integrity violations, where knowledge and technologies are used to suppress or undermine fundamental values, whether in the EU or elsewhere.

2. For the purposes of this recommendation, 'international cooperation' should be understood as cooperation of public and private research performing organisations and higher education institutions with research and innovation organisations and companies based outside the EU. Research and innovation organisations and companies based in the EU but owned or controlled from outside the EU should be considered on the basis of a risk appraisal.

3. In the context of this recommendation, 'risk appraisal' refers to a process in relation to international research and innovation cooperation in which a combination of main risk factors is taken into consideration. The combination of those factors determines the risk level. The key elements to be assessed can be grouped in four categories:

   – The risk profile of the EU-based organisation entering into the international cooperation: consider the organisation's strengths and vulnerabilities, including financial dependencies, relevant to the research project;

– The research and innovation domain in which the international cooperation is to take place: consider whether the project focusses on a research domain, e.g. a critical technology area, or involves methodology or research infrastructure considered particularly sensitive from a security or ethical/human rights perspective;

– The risk profile of the third country where the international partner is based or from where it is owned or controlled (e.g.: is the country subject to sanctions or does it have a flawed rule of law or human rights protection track record, an aggressive civil-military fusion strategy or limited academic freedom);

– The risk profile of the international partner organisation: perform due diligence into the organisation you envisage to cooperate with to find out whether it has links to the government or the military, the affiliations of the researchers/staff involved as well as the partner's intentions regarding the end-use or application of the research results.

4. For the purposes of this Recommendation, the 'research and innovation sector' covers all research performing organisations and higher education institutions across the Union, both public and private. In light of the importance of other stakeholders, such as technology transfer offices, internationalisation agencies, chambers of commerce and research intensive companies, this recommendation can be equally relevant to all other actors in the EU's research and innovation ecosystem. Where relevant, education-related international cooperation activities could be considered as well.

PRINCIPLES FOR RESPONSIBLE INTERNATIONALISATION

1. Continue to promote and defend academic freedom and institutional autonomy, taking into account that responsibility for international research and innovation cooperation primarily lies with higher education institutions and other research performing organisations;

2. Continue to promote and encourage international cooperation in research and innovation with partners in third countries that is both open and secure, in line with the principle 'as open as possible, as closed as necessary', ensuring that research outputs are findable, accessible, interoperable and reusable (FAIR), with due consideration to applicable restrictions, including security concerns;

3. Ensure proportionality of measures: where safeguards are introduced, these should not go beyond what is strictly necessary to mitigate the risks at stake and avoid unnecessary administrative burden. The objective is to de-risk, not to de-couple;

4. Steer research security measures to safeguarding economic security, including Union and national security, and defending shared values, including academic freedom, while avoiding protectionism and unjustified political instrumentalisation of research and innovation;

5. Promote self-governance within the sector, empowering researchers and innovators to take informed decisions, underscoring the societal responsibilities of higher education institutions and other research performing organisations, building on the principle that 'with academic freedom comes academic responsibility';

6. Adopt a whole-of-government approach, which brings together relevant expertise and skills, ensures a comprehensive approach to research security and fosters coherence of governmental actions and messaging towards the research and

innovation sector, including concrete steps to upskill and reskill the relevant workforce;

7. While pursuing a risk-based approach, adopt policies that are country-agnostic, identifying and addressing risks to research security wherever they emanate from, as this is the best guarantee that a balanced approach to opportunities and risks in the research and innovation cooperation is maintained and that evolving developments in the threat landscape, including the emergence of new threat actors, are not overlooked;

8. Ensure that every effort is made to avoid all forms of discrimination and stigmatisation, direct as well as indirect, that could occur as unintended side-effects of safeguarding measures and ensure full respect of fundamental rights and shared values;

9. Acknowledge the dynamic nature of research security shaped by evolving risks, new insights, and geopolitical contexts, which requires a learning approach with periodical reviews being carried out to ensure research security policies remain up-to-date, effective and proportionate.

HEREBY RECOMMENDS THAT MEMBER STATES

with full regard to institutional autonomy and academic freedom, and in accordance with national circumstances and their responsibility for national security:

1. Work towards developing and implementing a coherent set of policy actions to enhance research security, making best use of the elements listed in this section, while taking into account the aforementioned principles for responsible internationalisation;

2. Engage in dialogue with research and innovation stakeholders with a view to defining responsibilities and roles, and developing a national action plan, formulating national guidelines where relevant, and listing relevant measures and initiatives to boost research security, together with a timeline for their implementation.

3. Create a support structure, e.g.: a Research Security Advisory Hub, to help researchers and innovators deal with risks related to international cooperation in research and innovation. Bringing together cross-sectoral expertise and skills, it should provide information and advice that research performing organisations can use to take informed decisions, weighing opportunities and risks of a prospective international cooperation as well as other services for which the research and innovation sector has a clear need, including awareness raising activities and trainings.

4. Strengthen the evidence base for research security policymaking, through analysis of the threat landscape, including from a cybersecurity perspective, as well as through conducting or commissioning policy-relevant research.

5. Pay specific attention to those critical technologies identified by the Commission recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States[19], and to the outcomes of such collective risk assessments.

[19] Commission recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States of 03.10.2023 (link).

6. Reinforce cross-sectoral cooperation within government, notably bringing together policy-makers responsible for higher education, research & innovation, foreign affairs, and intelligence & security.

7. Facilitate information exchange with public and private research performing organisations on the aforementioned analysis and research, including through classified and non-classified briefings or dedicated liaison officers.

8. Gain insight in the resilience of the sector as well as the effectiveness and proportionality of the applicable research security policies, including possibly through regular resilience testing and incident simulations.

9. In order to ensure compliance with the applicable EU's export control rules for dual-use items and the sanctions adopted pursuant to Article 29 TEU and Article 215 TFEU, take national measures notably on intangible technology transfer (ITT), as well as to strengthen the implementation and enforcement of sanctions regimes that are relevant to research and innovation, such as those prohibiting the transfer of certain technologies.

10. Proactively contribute to the EU's one-stop-shop platform on tackling R&I foreign interference by sharing tools and resources developed through public funding with the aim to facilitate the cross-border uptake of these tools and resources and deliver them in a user-friendly and accessible manner.

11. Develop, together with the private sector, targeted information and guidance for business involved in private research and innovation, including for research-intensive start-ups and small and medium size companies.

12. Consider, where relevant, and based on risk-assessment, the application of the measures contained in this recommendation to international cooperation activities in higher education, including to student and staff mobility activities.

Role of research funding organisations

13. Engage with research funding organisations to ensure that:

    (a) Research security is an integral part of the application process that takes into account the different factors that, taken together, define the risk profile of the project. The objective is to stimulate beneficiaries to think through the context in which the R&I cooperation takes place and what motivations and (hidden) agendas could play a role, ensuring potential risks and threats are identified up front with the aim to avoid as much as possible problems at a later stage.

    (b) Research projects selected for funding that raise concerns ('red flags') undergo a risk appraisal proportionate to their risk profile, resulting in agreeing appropriate safeguard measures addressing the identified risks while ensuring that the time-to-grant is not unnecessarily delayed, and avoiding any unnecessary administrative burden.

    (c) When applying safeguarding measures in national funding programmes, those applied in relevant EU funding programmes are taken into account.

    (d) Applicants are seeking assurances, for instance through agreeing a partnership agreement, from prospective partners for projects with a high risk profile that the research results will be used in a manner that upholds fundamental values, including respect of human rights.

(e) Adequate expertise and skills are available within the funding organisation to address research security concerns as well as to have adequate monitoring and evaluation measures in place to oversee projects at different stages, including keeping track of incidents and taking credible measures in case of non-compliance.

Support to higher education institutions and other research performing organisations

14. Encourage and support higher education institutions and other research performing organisations to

(a) Create a sector-wide platform of stakeholders to facilitate information exchange, peer learning, development of tools and guidelines, and incident reporting. Consider resource pooling to make best use of scarce and scattered resources and expertise;

(b) Implement internal risk management procedures in a structural manner, including through risk appraisal, due diligence into prospective partners and escalation to higher levels of internal decision-making in case of elements that raise concerns (‘red flags’), while avoiding unnecessary administrative burden;

(c) Whenever entering into research partnership agreements with foreign entities, including through Memoranda of Understanding, insist on including key framework conditions, such as respect for fundamental values, academic freedom, reciprocity and arrangements on intellectual assets management, including the dissemination and valorisation of results, licensing or transfer of results and spin-off creation, and ensure there is an exit strategy in place in case the conditions of the agreements are not complied with;

(d) Assess risks related to foreign government-sponsored talent programmes in higher education and research, notably focusing on any undesirable obligations imposed on their beneficiaries, and guarantee that foreign government-sponsored on-campus providers of courses and trainings abide by the host institution’s mission and rules;

(e) Invest in dedicated in-house research security expertise and skills, assign research security responsibility at the appropriate organisational levels, and invest in cyber hygiene and in creating a culture in which openness and security are in balance;

(f) Develop training programmes, including online courses, for practitioners and new staff members, as part of their on-boarding, as well as curricula aimed at training the next generation of security advisers and policy-makers. Train recruiters to check and detect, as part of a structural vetting process, elements that raise concerns (‘red flags’) in applications for research positions, especially those in critical research domains;

(g) Ensure in scientific publications and all other forms of dissemination of research results full transparency of funding sources and affiliations of research staff, avoiding that foreign dependencies and conflicts of interest or commitment affect the quality and content of the research;

(h) Introduce compartmentalisation, both physical and virtual, guaranteeing that for areas, such as labs and research infrastructure, data and systems that are particularly sensitive, access is granted on a strict need-to-know basis, and, for online systems, robust cybersecurity arrangements are in place;

(i) Ensure that all forms of discrimination and stigmatisation, both direct and indirect, are prevented, that individual safety is guaranteed, with particular attention to coercion of diaspora by the state of origin and other forms of malign influence, which could give rise to self-censorship and may have security implications for the foreign researchers, doctoral candidates and students involved, and that incidents are reported.

Supporting actions at union level

15. Fully cooperate in view of facilitating the actions which the Commission has taken or intends to take to support implementation of this recommendation, and in particular:

(a) Making full use of the open method of coordination, notably the ERA governance structures, to raise awareness, to facilitate peer learning, as well as to facilitate consistency of policies;

(b) Establishing a European Centre of Expertise on Research Security as a focal point, linked to the Commission's one-stop-shop platform on tackling R&I foreign interference, contributing to creating an EU-wide community of practice and maintaining a structural dialogue with stakeholder organisations as well as to policy-relevant research into research security and analysing trends and patterns across the Union;

(c) Enhancing, in cooperation with the High Representative, situational awareness among policymakers by structurally assessing hybrid threats affecting the research and innovation ecosystem;

(d) Developing a resilience testing methodology that can be used at national level on a voluntary basis by higher education institutions and public and private research performing organisations;

(e) Continuing its work, together with the Member States and with involvement of the stakeholders, on assessing risks of critical technologies[20], as well as engaging in a dialogue to ensure information sharing and consistency of approach regarding risk appraisal and research security safeguards in national funding programmes and those in relevant EU funding programmes;

(f) Developing tools and resources, both country-agnostic and country-specific, to support higher education institutions and public and private research performing organisations to perform due diligence into prospective partners; as well as organising, together with EU-level stakeholder organisations, a biennial Stakeholder Forum on Research Security;

(g) Preparing interpretative guidance, where necessary, on the development of risk appraisal procedures as well as on the application of relevant EU legislation;

(h) Engaging with the research and innovation sector to assess how best to increase transparency of research funding sources and affiliations of researchers;

[20] Commission recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States of 03.10.2023 (link).

(i) Strengthening the dialogue with international partners on research security, as well as taking initiatives to bring about a common EU voice on the topic in multilateral fora.

REPORTING

1. It is recommended that Member States implement this recommendation as soon as practicable. They are invited to share their action plan (referred to in point 2 of the recommendations to the Member States) with the Commission by [insert date 9 months after adoption by Council] setting out the corresponding measures to be taken to boost research security, taking into account their respective starting positions.

2. The progress made in implementing this recommendation will be monitored by the Commission, using ERA governance monitoring and reporting frameworks, in cooperation with the Member States and after consulting the stakeholders concerned, and report to the Council every two years, as part of its biennial reporting on the Global Approach to Research & Innovation. After in-depth assessment and in light of the future evolution of the geopolitical situation, further steps and measures can be proposed.

Done at Brussels,

For the Council
The President