Council of the
European Union

Brussels, 7 March 2024
(OR. en)

7267/24

Interinstitutional File:
2024/0012(NLE)

LIMITE

POLCOM 82
COMER 41
RELEX 270
DUAL USE 22
RECH 98
ENER 115
ENV 240

NOTE

From:	General Secretariat of the Council
To:	Delegations
No. Cion doc.:	5788/24
Subject:	Proposal for a COUNCIL RECOMMENDATION on enhancing research security - Presidency text

Delegations will find attached a Presidency text on the Proposal for a Council Recommendation on enhancing research security, with a view to the Research Working Party meeting on 14 March 2024.

Changes in comparison to document 6598/24 are marked in **<u>bold and underlined</u>** for addtions and in ~~strikethrough~~ for deletions.

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, **the** Union's researchers and academics are increasingly exposed to risks to research security when cooperating internationally, resulting in European research and innovation being confronted with malign influence and being misused in ways that affect **the** Union's security or infringe ~~its~~ **EU values and fundamental rights as defined in the Treaties**[1] ~~ethical norms~~. It is therefore vital that **the** European **research and innovation sector** ~~research performing organisations~~ **is** ~~are~~ supported and empowered to address these risks. Precise and proportionate safeguarding measures are needed to keep international cooperation open and safe.

(1a) The changing geopolitical context urgently requires a joint response from all Member States and the Commission to strengthen and exploit the research and innovation potential across the Union. Only collective efforts can ensure the enhancement of research security.

[1] **Article 2 TEU; Charter of fundamental rights of the EU.**

(2) Open science ensures that **scientific research** ~~science~~ is made as accessible as possible for the benefit of science, the economy and society at large. International cooperation in research and innovation is vital for finding solutions to pressing global challenges for the benefit of our societies and drives scientific excellence, while international mobility of research talent enriches scientific enquiry and is essential for fostering innovation and achieving scientific breakthroughs. 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, ~~in parallel with academic responsibility~~ **taking into account that with academic freedom comes academic responsibility.**

(3) Growing strategic competition and the return to power politics are leading to increasingly transactional ~~interstate~~ **international** relations. This shift has resulted in threats that are diverse, unpredictable, and oftentimes hybrid.[2] Given the pivotal role of **critical knowledge and** technology for political, economic, **intelligence** and military pre-eminence, some of the EU's competitors are increasingly **advancing their capabilities in this respect** ~~seeking global primacy~~ ~~in critical knowledge and technology~~ ~~while~~ **or** 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 ~~are~~ **may be** targeted to **obtain** ~~capture~~ state-of-the-art knowledge and technology, at times using methods that are deceptive and covert, or through outright theft or coercion, but more often exploiting seemingly *bona fide* international academic cooperation. Next to jeopardising our security **and welfare**, hybrid threats could affect academic freedom and research integrity in the Union.

[2] **Joint Framework on countering hybrid threats a European Union response**, JOIN(2016)18.

(5) **The r**~~R~~esearch **and innovation sector** ~~performing organisations~~ and ~~Union~~ researchers **from EU countries** working in third countries are thus navigating an increasingly challenging international context for research **and innovation** collaborations, with risks of undesirable transfer of critical knowledge and technology to **third** countries ~~of concern,~~ which might be used to strengthen the**se countries'** military capabilities and intelligence services, affecting the security of the Union and its Member States, or for purposes that are in violation of EU values **and fundamental rights**. While not always legally prohibited, these collaborations **can** ~~are undesirable~~ ~~as~~ ~~they~~ pose significant security ~~and ethical~~ concerns.

(6) In accordance with institutional autonomy and academic freedom, research performing **organisations and research funding** organisations are primarily responsible for developing and managing their international cooperation. Public authorities at all levels should consider providing them with assistance and support, empowering them to take informed decisions and **to** manage the risks to research security involved.

(7) In recent years, discussions on strengthening research security have been ongoing in several Member States and at EU level, where **various** ~~several~~ initiatives have ~~also~~ been undertaken:

- In May 2021, the Commission published its communication on the Global approach to research and innovation, outlining a new European strategy for international research and innovation policy. The Council responded in September 2021 through the adoption of Council conclusions[3] emphasising the Union and Member States commitment to strengthen measures for countering foreign interference.
- 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.

[3] 12301/21.

[4] OJ L 170, 12.5.2021, p. 1–68, in particular Art. 20, 22(5), 22(6), and 40(4).

[5] 14308/21.

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

- On 9 March 2022, the European Parliament adopted 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[7]**.**

- In **April 2022** ~~November 2021~~, the Council adopted conclusions on a European strategy empowering higher education institutions for the future of Europe[8] highlighting that deeper European cooperation can be beneficial to support higher education institutions and equip researchers, trainers, students and staff with the necessary tools to deal with the challenges to fair global collaboration, such as inequity, foreign interference and obstacles to open science. It also stresses the need to promote an informed and independent understanding of third-country counterparts.

- On 10 June 2022, the Council adopted conclusions on "Principles and values for international cooperation in research and innovation"[9], underlining the importance of risk management and security, and inviting the Commission and the Member States to develop further good practices.

[6] SWD(2022)12.

[7] P9_TA(2022)0064.

[8] 7936/22.

[9] 10125/22.

– 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 the EU Hybrid Toolbox[12], that brings together different instruments to detect and respond to hybrid threats.

– In the domain of EU export control rules for dual-use goods and technology, the EU's Export Control Regulation[13] 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[14].

(8) The Commission and the High Representative adopted a joint communication on European economic security strategy[15] 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 Member States in its recommendation of 3 October 2023[16]. 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 potential measures to implement the European economic security strategy, including measures to enhance research security.

[10] COM(2020)605

[11] 7371/22.

[12] **10016/22; 15880/22.**

[13] OJ L 206, 11.6.2021, pp. 1–461.

[14] OJ L 338, 23.9.2021, p. 1–52.

[15] JOIN(2023)20.

[16] OJ L, 2023/2113, 11.10.2023.

(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. The present recommendation is part of a package issued by the Commission in January 2024 as follow-up on the joint communication.

(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 all other actors concerned 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 ha**ve**~~s~~ developed or **are** ~~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. **To be truly effective and to avoid loopholes and circumvention, t**~~T~~he development and implementation of safeguards ~~can only be truly effective if~~ **should be** consistently applied at all levels, including EU, national, regional as well as **at** the level of ~~individual higher education~~ research performing organisations and research funding organisations, ~~so as to avoid loopholes and circumvention~~. EU level coordination **and support for capacity building are** ~~is~~ therefore needed to provide for a level-playing field and to protect the integrity of the European Research Area, while respecting the competences of Member States for going further.~~ and setting-up regulatory frameworks.~~

(1**3**~~5~~) 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, in particular the Hybrid Fusion Cell, and taking into account the work of the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) as well as the European Union Agency for Cybersecurity (ENISA) **and the European Cybercrime Centre (EC3) set up by EUROPOL** in relation to cybersecurity threats.

(1**4**~~6~~) Taking into account that a significant share of research and innovation takes place in the private sector, it should be stressed that, while the risks to which companies are exposed may be similar, their nature, needs and capacities differ from those of research performing organisations.

(1**5**~~7~~) Due attention should be paid to the policy experience of **Member States and** key international partners, while emphasising that an approach should be formulated that suits the unique European context. Good practices are **for instance** shared through the Multilateral Dialogue on values and principles for international cooperation in research and innovation, as part of association negotiations and Joint ~~S&T~~ **Science and Technology** Steering committee meetings in the context of international science and technology agreements, as well as in multilateral fora, **such as G7,** and relevant multilateral export control arrangements.

(1**6**~~8~~) 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, **promote and** facilitate peer learning between Member States and relevant stakeholder organisations, as well as contribute to a learning approach that is both flexible and agile.

(1**7**~~9~~) Definitions

For the purpose of this recommendation,

1) ‘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 EU and its Member States, for instance if channelled to military or intelligence 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 and~~ **inter alia** create disinformation 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**, infringe on** or undermine EU values **and fundamental rights, as defined in the Treaties** ~~including human rights~~**;**

2)~~4~~. ‘research and innovation sector’ refers to all research performing organisations across the Union, **including higher education institutions as far as they perform research**, as well as **all** other actors in the EU’s research and innovation ecosystem**.** While elements of this recommendation can be equally relevant to ~~research intensive~~ companies, a dedicated approach geared towards private sector actors to address their research security is needed;

3)~~4 bis~~. ‘research performing organisation’ **means any non-profit organisation that performs scientific research and which employs or supports researchers** ~~refers to universities and other higher education institutions, public and private research and technology organisations, research infrastructures, as well as research funding organisations to the extent that they perform research~~;

4) ~~2~~. ‘international cooperation’ refers to cooperation of ~~EU~~ research performing **organisations** and **research** funding organisations **from the EU** or individual researchers, on the one hand, with entities **including companies** or individual researchers based outside the EU, on the other hand. ~~Where relevant, education-related international cooperation activities could be considered as well~~. **Cooperation** with **r**~~R~~esearch **performing** ~~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.

5)~~3~~. ‘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 research domains involving critical knowledge and technology, methodologies, data or research infrastructures considered particularly sensitive from a security or EU values **and fundamental 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 **restrictive measures** ~~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 i.a. whether it is subject to ~~sanctions~~ **restrictive measures** or has links to the military, the affiliations of the researchers/staff involved as well as the partner's or intentions regarding the end-use or application of the research results**;**

6)~~5~~. 'critical knowledge and technology' refers to knowledge and technology, including know-how, in emerging and disruptive areas and in domains that are key to economic competitiveness, social welfare and the security of the Union and its Member States and in which, as a consequence, overdependencies on third countries are undesirable. This includes but is not limited to ~~dual-use~~ research and innovation **with dual-use potential**[17]**.**

7) ~~2 bis.~~ 'third countries' refers to all non-EU countries.

[17] **Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021, OJ L 206, 11.6.2021, pp. 1–461.**

HEREBY RECOMMENDS THAT MEMBER STATES AND THE EUROPEAN COMMISSION

1. Take into account the following principles for responsible internationalisation when designing and implementing policy actions to enhance research security:

   a) Continue to promote and defend academic freedom and institutional autonomy, taking into account that responsibility for international research and innovation cooperation primarily lies with research performing organisations;

   b) Continue to promote and encourage international cooperation in research and innovation 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;

   c) Ensure proportionality of measures: where safeguards are introduced, these should not go beyond what is necessary to mitigate the risks at stake and avoid unnecessary administrative burden. The objective is to manage rather than avoid risk;

   d) Steer research security measures to safeguard~~ing~~ economic security, as well as Union and national security, and defending **and promoting** ~~shared~~ **EU** values **and fundamental rights**, ~~including~~ academic freedom and research integrity, while avoiding protectionism and ~~unjustified~~ political instrumentalisation of research and innovation;

   e) Promote self-governance within the **research and innovation** sector, empowering ~~researchers and innovators~~ **its actors** to take informed decisions, underscoring the societal responsibilities of research performing organisations, **taking into account** ~~building on the principle~~ that ~~‘~~with academic freedom comes academic responsibility~~’~~ ;

f) 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 necessary steps to upskill and reskill the relevant workforce;

g) 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;

h) Ensure that every effort is made to avoid all forms of discrimination and stigmatisation of groups or individuals, direct as well as indirect, that could occur as **unintended consequences** ~~side-effects~~ of safeguarding measures and ensure full respect of fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union[18];

i) Acknowledge the dynamic nature of research security shaped by new insights, evolving risks and geopolitical context, which requires a learning approach with periodical reviews and updates being carried out to ensure that research security policies and related capacity building efforts remain up-to-date, effective and proportionate, and in line with the above mentioned principles.

[18] OJ C 326, 26.10.2012, p. 391–407.

RECOMMENDS THAT MEMBER STATES,

with full regard to subsidiarity, **proportionality**, institutional autonomy and academic freedom, and in accordance with national specificities, **different starting points** and their **exclusive** competence regarding national security:

2. 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;

3. Engage in dialogue with the research and innovation sector with a view to defining responsibilities and roles and developing a national approach, **if not already in place,** ~~including~~ **for instance** **through** guidelines~~, if not already in place,~~ **or a** list~~ing~~ **of** relevant measures and initiatives to boost research security, together with a timeline for ~~their~~ implementation, while ~~making best use~~ **considering** ~~of~~ Commission guidance and available tools for support.

4. Whe~~n~~**re** relevant, create a new or reinforce an existing support structure~~, e.g. a research security advisory hub~~ or service, to help ~~research performing and funding organisations~~ **actors in the research and innovation sector** to deal with risks related to international cooperation in research and innovation. Bringing together cross-sectoral expertise and skills, it ~~sh~~**c**ould provide information and advice that research performing and funding 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.

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

6. ~~5 bis~~ ~~(former 7)~~ Facilitate information exchange between research performing organisations and intelligence agencies on the aforementioned analysis and research, for instance through classified and non-classified briefings or dedicated liaison officers.

7.~~6~~. **Develop or** ~~R~~**r**einforce cross-sectoral cooperation within government, notably bringing together policy-makers responsible for higher education, research and innovation, **trade**, foreign affairs, and intelligence and security.

8.~~7.~~ 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, **considering where appropriate** ~~with~~ the support of the Commission.

9. ~~7 bis (former 5)~~ Pay specific attention to international cooperation in domains involving critical knowledge and technology, including those 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.

10.~~8.~~ In order to ensure compliance with the applicable EU's export control rules for dual-use items and the ~~sanctions~~ **restrictive measures** adopted pursuant to Article 29 TEU and Article**s 207 and** 215 TFEU, take national measures notably on intangible technology transfer, as well as to strengthen the implementation and enforcement **of restrictive measures with relevance for research and innovation** ~~of sanctions regimes that are relevant to research and innovation, such as those prohibiting the transfer of certain technologies~~.

11.~~9.~~ 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.

[19] OJ L, 2023/2113, 11.10.2023.

1**2**~~0~~. ~~Develop, together~~ **Engage** with the private sector~~,~~ **to develop** ~~targeted information and~~ guidance for companies involved in research and innovation, including for research-intensive start-ups, spin-offs and small and medium size companies. In this regard, 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.

1**3**~~1~~. Consider, where relevant, and based on risk-assessment, the application of the measures contained in this recommendation to international cooperation activities **related** ~~in higher education, including to student and staff~~ **to researchers'** mobility ~~activities~~.

Role of research funding organisations

1**4**~~2~~. Engage with research funding organisations to encourage them to ensure that:

(a) Research security is an integral part of the application process that takes into account the different factors **jointly** defining the risk profile of the project. The objective is to stimulate beneficiaries to think through the context in which the **research and innovation** ~~R&I~~ cooperation takes place and what motivations and (hidden) agendas could play a role, ensuring potential risks and threats are identified up front.

(b) Research projects selected for funding that raise concerns undergo a risk appraisal proportionate to their risk profile, resulting in agreeing appropriate **risk management** ~~safeguard measures addressing the identified risks~~ while ensuring that the time-to-grant is not unnecessarily delayed, and avoiding any unnecessary administrative burden. ~~The process could be inspired by the "security appraise~~**a**~~l" process, set up for Horizon Europe.~~

(c) **Whenever entering into research partnership agreements with foreign entities, including through Memoranda of Understanding, consider possible risks related to the international cooperation and include key framework conditions, such as respect for EU values and fundamental rights, academic freedom, reciprocity and arrangements on intellectual assets management, including the dissemination and exploitation of results, licensing or transfer of results and spin-off creation, and provide for an exit strategy in place in case the conditions of the agreements are not complied with;**

d~~(c)~~ When applying safeguarding measures in national funding programmes, those applied in relevant EU funding programmes are taken into consideration;

e(~~d~~) Applicants are seeking assurances from prospective partners, for projects with a high risk profile, for instance through a partnership agreement, taking into account key framework conditions such as those listed in **14**~~13~~(c).

(f)~~(e)~~ Adequate expertise and skills are available within the funding organisation to address research security concerns and that research security is integrated in existing monitoring and evaluation measures, including keeping track of incidents, and taking **timely and** credible measures in case of non-compliance**.**

Support to research performing organisations

1**5**~~3~~. Encourage and support research performing organisations to

(a) ~~Create sectoral platforms of stakeholders at national or regional levels to~~ ~~f~~ **F**acilitate information exchange, peer learning, development of tools and guidelines and incident reporting **among peers**. Consider resource pooling to make best use of scarce and scattered resources and expertise;

(b) Implement internal risk management procedures in a **systematic** ~~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, while avoiding unnecessary administrative burden**;**

(c) Whenever entering into research partnership agreements with foreign entities, including through Memoranda of Understanding, ~~identify~~ **consider** possible risks related to the international cooperation and ~~insist on~~ includ**e**~~ing~~ key framework conditions, such as respect for EU values **and fundamental rights**, academic freedom, reciprocity and arrangements on intellectual assets management, including the dissemination and exploitation of results, licensing or transfer of results and spin-off creation, and provide for 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 **and innovation,** 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) Facilitate access to training programmes, including online courses, for new and existing research staff ~~members~~, as well as develop education and training programmes aimed at training ~~the next generation of~~ security advisers and **other relevant actors** ~~policy-makers~~. Train recruiters **and staff dealing with internationalisation** ~~mobility officers~~ to check and detect, as part of a structural vetting process, elements that raise concerns in applications for research positions, especially those in research domains involving critical knowledge and technology;

(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) Assess risks related to procured or foreign-sponsored equipment, laboratories and research infrastructures, notably focusing on any undesirable obligations imposed on hosting organisations;

(j)(~~i~~) Ensure that all forms of discrimination and stigmatisation, both direct and indirect, are prevented, that individual safety is **protected** ~~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.

RECOMMENDS THE COMMISSION TO:

1**6**~~4~~. Make full use of the open method of coordination, notably the ERA governance structures, **and support the implementation of this recommendation by**~~, to~~ rais**ing**~~e~~ awareness, ~~to~~ facilitat**ing**~~e~~ **and promoting** peer learning, enabl**ing**~~e~~ capacity building as well as ~~to~~ facilitat**ing**~~e~~ consistency of policies; ~~I~~incorporat**e**~~ing~~ the content of this reccommendation also in the agendas of ~~all~~ relevant strategic platforms and boards. ~~, such as the European Strategy Forum on Research Infrastructures (ESFRI)~~;

1**7**~~5~~. Develop and maintain **a** ~~the~~ EU one-stop-shop platform on tackling **research and innovation** ~~R&I~~ foreign interference, which aims to consolidate all pertinent data, tools, reports, and other resources developed at the EU, national, regional, organisational level, or outside the EU, ensuring they are presented in a manner that is both user-friendly and accessible.

1**8**~~6~~. Support the collection of evidence for policy making in research security and bring together relevant expertise from Member States and stakeholders, as well as explore and assess options for more structural support in this respect, such as through a European centre of expertise on research security, **taking into account existing structures and linking it to the one-stop-shop platform. Additional functionalities to support Member States and the research and innovation sector could be added in due time, if needed.**

1**9**~~7~~. Enhanc**e**~~ing~~, in cooperation with the High Representative, situational awareness among policymakers by structurally assessing hybrid threats affecting the research and innovation ecosystem;

20~~18~~. Develop~~ing~~ a resilience testing methodology **for research performing organisations** that can be used ~~at national level~~ on a voluntary basis **by Member States with their** research performing organisations;

21~~19~~. Continu**e**~~ing~~ its work, together with the Member States and with involvement of the stakeholders, on assessing risks of critical technologies[20], as well as engag**e**~~ing~~ 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;

22.~~20~~. Develop~~ing~~ tools and resources, both country-agnostic and country-specific, to support research performing organisations to perform due diligence into prospective partners;

23.~~21~~. Organis**e**~~ing~~, together with EU-level stakeholder organisations, a biennial **flagship event** ~~Stakeholder Forum~~ on research security, aimed at sharing information and solution-oriented exchanges;

[20] OJ L, 2023/2113, 11.10.2023.

2**4**~~2~~. Prepar**e**~~ing~~ interpretative guidance, where necessary, on the development of risk appraisal procedures as well as on the application of relevant EU legislation. This applies in particular to export control rules, notably the intangible transfer of technology, the visa requirements for foreign researchers[21], as well as the interpretation of certain open science and intellectual asset management requirements from a research security perspective[22].

25~~3~~. Engag**e**~~ing~~ with the research and innovation sector and the Member States to assess how best to increase transparency of research funding sources and affiliations of researchers;

2**6**~~4~~. Strengthen~~ing~~ the dialogue **and cooperation** with international partners on research security ~~for example through the activities of the Multilateral Dialogue on values and principles for international cooperation in research and innovation, facilitating sharing of good practices~~ **through exchanging information and experience, sharing best practices and seeking ways to align safeguarding measures** as well as tak**e**~~ing~~ into consideration the option of bringing about a common EU voice on the topic in multilateral fora.

MONITORING PROGRESS

27~~1~~. **The Commission is invited to monitor the progress made in implementing this recommendation, in cooperation with the Member States and after consulting the stakeholders concerned, using the ERA policy platform, and to report to the Council every two years, as part of its biennial reporting on the Global Approach to Research and Innovation and its existing reporting on the Reseaerch and Innovation Framework Programme.**

28.~~2.~~ Member States are invited to implement this recommendation without delay and to share **with the Commission** information on their national approach ~~and guidelines~~ (referred to in recommendation 3 to the Member States) ~~with the Commission, as soon as practicable~~, ~~taking into account their respective starting positions~~, **as input for the aforementioned monitoring and reporting activities by the Commission.**

[21] OJ L 132, 21.5.2016, p. 21–57.

[22] OJ L 69, 7.3.2023, p. 75–84.

~~2. The progress made in implementing this recommendation should 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 &and Innovation, as well as through its existing reporting on the R&I Framework Programme.~~

29. 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