BRIEFING

European Parliament

Enhancing research security

SUMMARY

On 24 January 2024, the European Commission tabled a proposal for a Council recommendation on enhancing research security. The procedure does not require the European Parliament's involvement.

Research security refers to the safeguarding of scientific activities against misuse and undue influence by third countries or non-state actors. Risks to research include the illicit transfer of knowledge or technology resulting in a threat to the EU's security or undermining its values. Competence for identifying and managing these risks lies with several public bodies, including national authorities and academic institutions. Research security is therefore distinct from research integrity, which seeks to safeguard the reliability and honesty of knowledge creation by individual scientists and academic institutions in line with scientific standards.

Against a backdrop of global challenges, including climate transition and geopolitical tensions such as Russia's war on Ukraine, the current economic situation is highlighting the risks inherent in international cooperation in science and technology and the need for the EU to build resilience by reducing vulnerability to foreign interference. While research and innovation (R&I) are an EU asset, in that they can generate knowledge and solutions to global challenges, they also require an appropriate framework to balance the benefits of openness with the need for safeguards regarding research integrity and the dissemination and exploitation of knowledge, technology and know-how.

The proposed recommendation, adopted as part of the economic security package, is expected to help establish an EU-wide level playing field in research security in line with the objectives set by the Treaty on the Functioning of the European Union for the European research area (ERA): developing the EU's scientific and technological base and ensuring the free circulation of knowledge. With the inclusion of an EU definition of research security, the proposal seeks to prevent the fragmentation of the ERA that could result from diverging national approaches on research security. This approach, empowering the main academic and industrial actors in research creation, should also comply with the principles underpinning research in the EU, such as academic freedom.

IN THIS BRIEFING

EPRS | European Parliamentary Research Service

Author: Clément Evroux
Members' Research Service

PE 760.387 – March 2024

EN

Introduction

International openness, an important feature of research and innovation (R&I), has always been instrumental in facilitating the exchange both of ideas and of talented scientists, technicians and engineers. Science and technology are key to addressing global challenges, such as the climate transition or the COVID-19 pandemic. International cooperation in science is a driver of knowledge creation, as scientists endeavour to equal or surpass each other through emulation. International cooperation also offers opportunities to harness research and innovation (R&I) policies so as to promote multilateralism, with the aim of disseminating new knowledge faster, or for other scientific diplomacy purposes. However, openness to international cooperation is not immune to geopolitical tensions: research staff, infrastructure, proceedings and results can be subject to undue influence and misappropriation by or on behalf of foreign authorities or non-state groups. Scientific and research institutions can mitigate these risks through their governance systems, founded on principles such as academic freedom, research integrity and self-governance. However, self-governance systems alone cannot provide the preparedness and response capacity needed to mitigate the risks associated with the further internationalisation of science and technology.

The European Commission's proposal for a Council recommendation on research security builds on its joint communication with the High Representative of the Union for Foreign Affairs and Security on a European economic security strategy, adopted in 2023. Among the four sets of risks identified in the strategy, those associated with technology security and technology leakage are linked directly to research security.

Existing situation

In 2020, the COVID-19 pandemic illustrated the central role of international cooperation in science when it comes to overcoming the health and socio-economic impacts of crises. In 2022, following the onset of Russia's illegal war of aggression against Ukraine, the EU Heads of State and Government adopted the Versailles Declaration, which stresses the need 'to take further decisive steps towards building our European sovereignty', including strengthening the EU's R&I capabilities, fostering synergies between civilian, defence and space R&I, and investing in critical and emerging technologies and innovation for security and defence. Research and innovation have thus taken centre stage among the EU's political priorities, further reinforcing the importance of safeguarding knowledge and its main drivers: scientific and technological staff, and the infrastructure and networks necessary to advance the EU's scientific and technological base.

EU initiatives relevant to safeguarding research security

Several recent EU legislative initiatives (adopted or still under examination) seeking to safeguard EU strategic autonomy include provisions to improve research security.

Regulation (EU) 2019/452 establishing a **framework for the screening of foreign direct investments into the Union** lays down rules to check such investment on the grounds of security and public order. Article 4 includes foreign direct investment in critical technologies as one of the factors for Member States to take into consideration when assessing the effect of foreign direct investment. Article 8 entitles the Commission to issue an opinion to Member States if it deems a foreign direct investment affects a project funded by the EU framework programmes for R&I on the grounds of security and public order. The third annual report on the screening of foreign direct investments in the Union published in 2023 notes that in 2022, Member States and the Commission handled 1 444 requests for authorisations of acquisition made by the foreign investors and *ex officio* cases (i.e. cases where the screening is activated by the Commission or a Member State on a foreign direct investment planned or completed in another Member States, in line with Article 7 of the regulation), with 1 % of those requests being prohibited, 9 % authorised under conditions or mitigating measures, 86 % authorised without condition, and 4 % withdrawn. The main sectors with the highest number of transactions include manufacturing (27 %), information and communications

technology (ICT) (24 %) and professional activities (12 %) – which include also research and experimental development on biotechnology. The geographical origin of the investors responsible for these requests remains stable in 2022 compared with 2021: United States (US), United Kingdom (UK), China, Japan, Cayman Islands and Canada.

Regulation (EU) 2021/821 setting up a **Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items** is designed to avoid unlawful dissemination of EU knowledge, technology, and know-how that qualify as dual-use items or associated technical assistance. The regulation significantly extends the scope of the technologies subject to an export authorisation. For example, its Article 5 requires an authorisation for the export of cyber-surveillance items not listed in Annex I, for use in connection with internal repression and/or the commission of serious violations of human rights and international humanitarian law. The 2022 report on the implementation of the regulation notes that in 2020, the total value of dual use export applications reached €38.4 billion, and controlled dual-use exports thus represented 2.3 % of total extra-EU-27 exports. Denials of applications amounted to some 1.4 % of the value of controlled dual-use exports in that year, which correspond to 0.03 % of total extra-EU-27 exports.

On 12 December 2023, the Commission adopted a proposal for a directive on **establishing harmonised requirements in the internal market on transparency of interest representation carried out on behalf of third countries**. Without affecting the principle of scientific freedom as enshrined in Article 13 of the EU Charter of Fundamental Rights, any interest representation activity conducted on behalf of a third-country authority in the context of research would be conditional on a registration of information such as the identity of that authority and the purpose of the activity.

The EU institutions do not own a significant share of EU scientific and technological infrastructure, and assets, nor do they employ a relevant share of EU scientific staff. However, through its framework programmes for R&I, the EU invests in transnational research activities designed and conducted by EU R&I actors. In its 2021 communication on a **global approach to R&I**, the Commission revealed its intention to provide for an investment strategy based on a differentiated approach, to ensure an international playing field that is as open as possible and as closed as necessary. Moreover, in 2022, the Commission adopted a staff working document on **tackling foreign interference** meant to provide EU academic institutions with good practices to help them mitigate the risks of interference across their missions and roles. In 2023, this publication was followed up by a mutual learning exercise among 12 Member States coordinated by the Commission. The exercise focused on three main points: (i) awareness raising and stakeholder engagement; (ii) understanding and identifying foreign interference threats; and (iii) measures to counter these threats. A dissemination event on the outcome of the exercise is expected to be organised during the first half of 2024.

While the rules for participating in the EU's funding programme for R&I Horizon Europe, laid down by Regulation (EU) 2021/695, retain the principle of openness for the participation of legal entities regardless of their jurisdiction (Article 22(1)), the regulation also includes **new obligations intended to safeguard research security through reciprocity**.

Article 20 on security provides for actions funded by the programme to comply with the applicable security rules. In particular, research conducted outside the EU using or generating classified information requires the EU to conclude a security agreement with that third country; non-compliance may lead to the action being terminated.

Article 22(5) stipulates that for actions relating to EU strategic assets, interests, autonomy or security, the Horizon Europe work programme may provide for the participation to be limited to legal entities established only in Member States, or to legal entities established in specified associated or other third countries in addition to Member States. Moreover, to safeguard the EU's and its Member States' strategic interests, the work programme may also exclude legal entities established in the EU, or in those associated countries directly or indirectly controlled by non-associated third countries, or by legal entities of non-associated third countries, from participating in individual calls for proposals,

or make their participation subject to conditions set out in the work programme. In 2023, the first biennial report on the implementation of the global approach to R&I concluded that the targeted approach to activating Article 22(5) to technological fields such as quantum research, critical raw materials and space did not substantially alter the programme's general openness.[1]

Article 22(6) allows for the inclusion of additional eligibility criteria, to take into account specific policy requirements or the nature and objectives of the action, including the type of legal entity and the place of establishment. On these grounds, the 2023-2024 work programme has banned legal entities established in China from participating in Horizon Europe innovation action.

Member States' policy mixes

In 2022, the Organisation for Economic Co-ordination and Development (OECD) published a report on integrity and security in the global research ecosystem. The report defines the security risks arising from the internationalisation of research as activities by national authorities or non-state groups consisting in distorting research endeavours, and/or in exploiting research results unfairly, for instance through misappropriation. Analysing initiatives from 13 OECD countries, the report stresses that research security calls for the adoption of various measures (e.g. legislative framework, awareness raising activity and capacity building) and their coordination at national and multilateral levels. The report has been followed up by the creation of a repository.

National initiatives cover a wide range of legislative and non-legislative initiatives that all aim to strike a balance between the safeguard of security and that of creativity, including academic freedom. Most of the initiatives that have been adopted seek to increase the awareness and situational judgement of academic and scientific institutions and their staff. For instance, in 2019, the German Academic Exchange Service established a Competence Centre for International Academic Cooperation, based on a 2018 recommendation by the German Science and Humanities Council. The centre provides researchers and academic institutions with guidance allowing them to carry out international cooperation activities or update them, taking into account research security and research integrity. The Dutch government has set up a national contact point for knowledge security, whose business model includes the provision of advice within 48 hours to any request on international cooperation by a researcher and/or an academic institution. Other national initiatives are more prescriptive. With a 2021 decree on protecting the nation's scientific and technical capabilities, the French government has established a regulatory system that introduces a label for sensitive scientific infrastructure, both private and public, designated as 'restricted regime zones'. The attribution of the label to a laboratory or other infrastructure results in strengthened access rules to be enforced. The prime minister's services have been given a coordinating role, as well as the powers to identify the relevant scientific and industrial fields.

Multilateral initiatives

Group of Seven (G7) members are addressing research security through their targeted cooperation on research integrity. In 2023, the Security and Integrity of the Global Research Ecosystem (SIGRE) working group adopted a set of best practices for secure and open research. Reaffirming the role of scientific freedom as a cornerstone of democracy, G7 members stressed the shared responsibility of national authorities and R&I stakeholders to uphold the integrity and security of research activities. Eight principles have been identified: (i) balance between national and global interests; (ii) maintenance of openness and research security; (iii) collaboration and dialogue; (iv) proactive efforts; (v) risk proportionality; (vi) shared responsibilities; (vii) accountability; and (viii) adaptability.

International partners' research security initiatives

In the **US**, Section 10114 of the Chips and Science Act requires the Department of Energy to 'develop and maintain tools and processes to manage and mitigate research security risks, such as a science and technology risk matrix, informed by threats identified by the Office of Intelligence and Counterintelligence, to facilitate determinations of the risk of loss of US intellectual property or threat to the national security of the United States'. A 2023 report by the Congressional Research Service highlights the development of a comprehensive research security strategy, and notes that (as of July 2023), the White House Office of Science and Technology Policy has yet to adopt guidelines to ensure the relevant legislation, included for instance in the Chips and Science Act, is implemented consistently across the federal government. In 2023, **Canada** has adopted national security guidelines on research partnerships. They aim to provide support for researchers, research institutions, federal granting agencies and the government, to help safeguard Canada's research ecosystem from foreign interference, espionage, and unwanted knowledge transfer. **Australia**, too, has taken measures to mitigate risks to research security. In particular, it has established a university foreign interference taskforce, which developed guidelines to safeguard international cooperation by Australian research actors. Moreover, it has adopted a framework on countering foreign interference, which also addresses pre identified critical technologies.

European Parliament position

In its resolution of 6 April 2022 on a global approach to research and innovation: Europe's strategy for international cooperation in a changing world, Parliament stressed that global R&I cooperation is crucial for Europe's competitiveness, while noting that this cannot lead to unconditional openness on the part of the EU. The resolution supports the general approach characterised by the principle of 'as open as possible, as closed as necessary', and calls on the Commission to urgently issue practical guidelines to R&I stakeholders on academic freedom, to ensure the EU's safety and security.

In its resolution of 9 March 2022 on foreign interference in all democratic processes in the EU, including disinformation, Parliament expressed its concern about the increasing financial dependence of European universities on China and other foreign states, given the risk of sensitive data, technologies and research outcomes flowing to foreign states and the implications this dependency could have for academic freedom. It also stressed the importance of academic freedom for addressing disinformation and influencing operations.

Parliament's resolution of 9 May 2023 on critical technologies for security and defence: state of play and future challenges highlighted the growing relevance of research security. By welcoming the Commission's proposal to overcome the current division between civil, defence and security research, development and innovation, and by calling on the Commission to better connect EU civil, defence and security programmes and instruments with the relevant stakeholders, in particular in the field of innovation, Parliament makes it clear that research security is expected to become more central to EU R&I programming and implementation.

A resolution of 17 January 2024 with recommendations to the Commission on promotion of the freedom of scientific research in the EU conveys Parliament's views on how to balance the safeguard of research security with the freedom of scientific research, including academic freedom. The resolution called on the Member States to fully respect and uphold the freedom of scientific research, and to ensure that any measures taken in the name of public interest, for example in the interest of national security, would not unduly restrict the freedom of scientific research. Also, as part of its request to the Commission to submit a proposal for an act on the freedom of scientific research on the basis of Articles 182(5) and 179(1) TFEU, the resolution provides a definition of freedom of scientific research, which includes a security-associated restriction, namely that the 'exercise of the freedom of scientific research, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety'.

Council of the EU position

Since the onset of Russia's illegal war of aggression against Ukraine, the rotating presidencies of the Council of the EU have adopted conclusions and organised discussions on how to optimise security in research policies.

In its conclusions of 10 June 2022 on principles and values for international cooperation in research and innovation, adopted during the French Presidency, the Council recommends that the Commission and the Member States take measures to counter foreign interference and manage the risks inherent in international R&I cooperation. This would include, in particular, the provision of safeguards for the EU's security and for the rights of its R&I actors and citizens, such as intellectual and industrial property rights, and personal data.

On 2 December 2022, during the Czech Presidency, conclusions on research infrastructure were adopted. They invited the Commission, in particular, to prepare an initiative by the end of 2023 to update the European charter for access to research infrastructures, in order to ensure access to this infrastructure also through virtual access modes via secure connectivity.

During the Competitiveness Council meeting of 23 May 2023, the Swedish Presidency organised an exchange of views on knowledge security and responsible internationalisation. The Presidency note, which fed into the discussions, further explains the importance of grounding international cooperation in 'rigorous research ethics', and of striving to ensure complementarity between openness and security. Ministers were invited to discuss good practices of national coordination ensuring the proper involvement of the different actors concerned (e.g. academic institutions, funding agencies and national authorities) across scientific disciplines.

The proposed recommendation in detail

Definition of research security. The proposed Council recommendation would provide for a definition of research security based on the management of three sets of risks: (i) the transfer of knowledge, know-how or technology that may affect the EU's security; (ii) any interference by third countries seeking to leverage research to incite researchers or students to self-censorship, or to breach research integrity or academic freedom; and (iii) any misuse of knowledge and technologies to undermine or cancel fundamental values across the world, including through ethical or integrity violations.

Broad set of recommendations. The proposal invites Member States to design a framework compliant with academic freedom, including institutional autonomy, and encompassing the complementary levels of governance of research ecosystems across the European research area. National authorities:

- are given 12 tasks hinging on the cooperation between national authorities across their sectoral remits (whole-of-government approach), which were enshrined among the main principles to comply with. Member States should reinforce cooperation within government, between authorities in charge of higher education, research, foreign affairs and intelligence, while also liaising with the private sector, in order to raise awareness and provide guidance;
- should work with research funding organisations on the one hand and higher education institutions and research performing organisations on the other, to make sure they include research security in all of their work processes and invest in raising their in-house expertise, while ensuring any direct or indirect discrimination is prevented;
- are invited to cooperate with the EU institutions and Member States, including to enhance situational awareness among policymakers.

Member States are expected to prepare an action plan to implement the proposed recommendation, and to share it with the Commission nine months following the adoption of the proposal by the Council. The Commission would then report to the Council every two years, as part of its reporting exercise on the EU global approach to R&I.

Stakeholder views[2]

European R&I actors, especially those from academia, have welcomed the proposal, and affirmed their support for a balanced approach between the principle of openness to international cooperation and the need to safeguard EU assets, including academic freedom and knowledge protection. Before the adoption of the proposal, the European University Association (EUA) in December 2023 adopted a policy paper in which it called for proportionality in designing responses to risks. It also called for a balance to be struck between the risks of cooperation and those of non-cooperation. In a position paper published in January 2024, the European Association of Research and Technology Organisations (EARTO) insisted in particular on the importance of framing a level playing field for research security across Europe. According to EARTO, research security refers to a wide scope of legislation and practices such as data or dual use export, which call for the design of European guidelines and for consistency among all relevant EU initiatives. EARTO considers that the adoption of a European framework should come before the conclusion of similar guidelines at multilateral level.

Following the adoption of the proposal, the League of European Research-intensive Universities (LERU) adopted a statement where it expresses its delight at the proposed recommendation. In particular, LERU praises the university-centric approach adopted by the Commission, which it says appropriately ensures academic freedom and institutional autonomy. LERU stresses that academic institutions will need to rely on advice and guidance from a wide range of national and EU authorities to perform their due diligence on research security. It also welcomes the establishment of an EU-wide level playing field, and notes its preference for preparing for international harmonisation with like-minded partners. The Guild of European Research-intensive Universities (the Guild) meanwhile adopted an opinion to welcome the adoption of the proposal. While stressing the need to align the research security framework with the overall objectives of the economic security package, including the need to better support research and development-involving technologies with dual-use potential, the Guild highlights the need for investment by Member States to achieve the right degree of capacity building across R&I organisations. However, investment in a European Centre of Expertise on Research Security should not crowd out investment in excellent R&I, according to the Guild.

The industrial actors point to the interactions between research security and EU international partnerships. In a joint statement on business priorities for the fifth ministerial meeting of the EU and US Trade and Technology Council, Business Europe and the US Chamber of Commerce declare their preference for the development of joint roadmaps on emerging technologies, and highlight their concerns regarding the possible adverse impact on security that may stem from data-sharing obligations arising from legislative initiatives. They therefore call for screening of these initiatives, with a view to checking the effective protection of intellectual property.

Next steps

The proposed recommendation has been referred to the Council of the EU. It is being examined in the Working Party on Research. While Article 292 TFEU on Council recommendations provides for the Council only to be involved in the legislative process, Parliament retains its competence to discuss the proposal in line with its Rules of Procedure, in particular Rule 136 and Rule 138 on questions, and Rule 143 on motions for resolutions.

MAIN REFERENCES

Evroux C., Scientific integrity: Handling knowledge as a public good, EPRS, European Parliament, 2022.

Evroux C., The European Union's global approach to research and innovation, EPRS, European Parliament, 2023.

Hoffmeister F. 'Strategic autonomy in the European Union's external relations law', *Common Market Law Review*, Vol. 60(3), 2023, pp. 667–699.

ENDNOTES

[1] According to the report, some 20 % of the topics expressly mention the relevance of international cooperation (under Article 22(5), participation was limited to 49 topics in the 2021-2022 work programme, and 31 topics in the 2023-2024 work programme, amounting to, respectively, 4 % and 3.5 % of these work programmes' budgets).

[2] This section aims to provide a flavour of the debate and is not intended to be an exhaustive account of all different views on the proposal.

DISCLAIMER AND COPYRIGHT

eprs@ep.europa.eu (contact)

www.eprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)