

Science Europe Report on

RESEARCH

SECURITY

Key Messages and Actions

from the January-June 2025 Workshop Series



NATIONAL SCIENCE CENTRE
POLAND



UK Research
and Innovation



fwo



Colophon

October 2025

'Science Europe Report on Research Security: Key Messages and Actions from the Workshop Series'

DOI: 10.5281/zenodo.17433203

This report reflects the outcomes of a series of workshops on research security that took place between January and June 2025. The series was co-organised by:

- UK Research and Innovation (UKRI)
- Dutch Research Council (NWO)
- National Science Centre, Poland (NCN)
- Research Foundation Flanders (FWO)
- Science Europe

For further information, please contact the Science Europe Office:
office@scienceeurope.org

© Copyright Science Europe 2025.

This work is licensed under the Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original authors and source are credited, with the exception of logos and any other content marked with a separate copyright notice. A copy of this license is available at creativecommons.org/licenses/by/4.0/

Lead Author: Theodora Famprikezi (Science Europe)

Co-authors: Ruhena Begum, Hannah Feakes, Benjamin Sharman (UKRI), Berry Bonenkamp, Joyce Kuipers (NWO), Magdalena Dobrzańska-Bzowska (NCN), Isabelle Verbaeys (FWO)

Editors: Lidia Borrell-Damián (Science Europe), Berry Bonenkamp (NWO), Isabelle Verbaeys (FWO), Benjamin Sharman (UKRI), Justyna Woźniakowska (NCN)

Editing and design: Iwan Groeneveld (Science Europe)

Acknowledgements: Science Europe thanks the members of the Organising Committee of the Task Force for their active engagement and for kindly hosting the workshops, and to the Members of the Task Force on Research Security for their contributions and valuable insights throughout the workshop series.



Table of Contents

Executive Summary

Key policy messages on research security	4
Next steps for Science Europe and its Member Organisations	5

Introduction and Context

Policy Context	6
Activities of the Science Europe Task Force on Research Security	7

Roles and Responsibilities of National RPOs and RFOs

8

Key Policy Messages on Research Security

9

Actions by Science Europe Member Organisations

13

Ways Forward for Science Europe

14

Annex I: EU Initiatives

16

Annex II: Definition of Research Security

18

Executive Summary

International co-operation is a main component of scientific excellence in research and innovation. However, in recent years, there has been an increased focus on understanding of risks to national or economic security, with a number of different approaches and policies that aim to mitigate risks associated with research security starting to emerge across national governments, research funding and research performing organisations (RFOs and RPOs).

Between January and June 2025, Science Europe Member Organisations convened a series of workshops to discuss these different approaches and their impact in national R&I ecosystems.

Key policy messages on research security

1. International co-operation must be safeguarded.

Research security measures should encourage and promote international co-operation that is open and safe. Although risk is unavoidable with bold and innovative research, it should be managed and mitigated rather than eliminated, to avoid impacting science.

Balancing openness, security, and academic freedom is therefore the ongoing challenge as well as the overall objective. Researchers should be equipped with the relevant awareness and decision-making tools.

2. Defining boundaries is essential.

There is no 'one size fits all' solution for adopting research security measures. Approaches need to be tailored and adjusted to national context and research sensitivity.

However, to establish 'good practice' in research security, an agreement on common principles, definitions and terminology are required. Clear guidelines and 'red lines' for security practices are essential for RPOs and RFOs in defining their specific responsibilities.

3. Measures and due diligence should be proportionate.

Proportionate risk mitigation, preparedness and due diligence should be encouraged, rather than the complete elimination of risk.

This could include developing targeted questions to help identify and manage risks appropriately, raising awareness of potential risks amongst researchers and staff, and incorporating clear and flexible mechanisms to facilitate the resolution of issues in a timely manner.

4. Research security should be embedded through awareness-raising and culture change.

RPOs and RFOs must embrace a cultural shift, embedding these concerns into their ethos, wider policies and approaches. Researchers

should be encouraged to develop a more critical mindset at the earliest stage of the collaborations' development and throughout the research lifecycle.

Tools alone are not sufficient without properly trained staff capable of interpreting and analysing the data and red flags identified. RFOs can help manage problematic applications by having clearly articulated policies and supporting guidance, reducing further cost and administrative burden on the sector.

5. National R&I ecosystems require capacity-building.

Investment should be made in dedicated in-house research security expertise and skills, and assign research security responsibility at the appropriate organisational levels. RPOs and RFOs may also benefit from independent national (or regional) advisory services to raise standards more widely.

6. Research security requires systemic support and a collaborative approach.

Identifying opportunities for establishing communities of support and practice should be encouraged to account for the potential discrepancy in available resources and capabilities to address security concerns in larger and smaller institutions. National governments and the EU should also promote consistent messaging, actionable guidance, legal frameworks and clearly defined roles and responsibilities.

Facilitating dialogue for stakeholders such as intergovernmental partners and the wider R&I sector is crucial to build trust as well as share information and increase awareness and capability.

Next steps for Science Europe and its Member Organisations

1. **Continue to facilitate dialogue within Science Europe** in order to convene, discuss common challenges and exchange best practices. A dedicated taskforce will convene bi-annually and practical workshops on selected thematic areas will be organised *ad hoc*.
2. **Create a repository of cases, good practices and tools** mapping research security initiatives to allow Member Organisations to benefit from their collective intelligence and exchange of good practice.
3. **Establish a Science Europe Centre of Support for Member Organisations** that will focus on competence-building and learning through knowledge exchange, with the facilitation of workshops.
4. **Continue collaboration and dialogue with the European Commission**, with Science Europe continuing to be an active R&I stakeholder participating in all relevant consultations.

Introduction and Context

Policy Context

International co-operation is a cornerstone of scientific excellence in research and innovation. However, there have been cases in recent years where projects were shut down, bilateral agreements terminated, and international collaboration halted due to real, potential, or perceived risks to national or economic security, or the undesirable transfer of knowledge and technology. There have also been cases where new co-operations did not take place because of research policies and changing conditions for academic research.

At the same time, potential military application of the results of R&I projects originally conceived for civilian purposes (so-called 'dual use') is receiving growing attention, as reported in two [independent expert reports](#) on dual-use research and innovation (June, 2025). The European Union foresees adopting a 'dual-use by design' approach, integrating dual-use¹ research into the next EU Framework Programme and aligning it with the European Defence Fund.

As a result, national governments and both research funding and research performing organisations (RFOs and RPOs) have started to develop a variety of different policies that aim to mitigate these types of risks. This brings increased constraints on international collaboration with certain actors or in certain research areas. There is a risk that researchers may choose to avoid potentially sensitive international partnerships due to the real or perceived risks involved or potential additional administrative burdens, while others may ignore these considerations altogether.

Legal frameworks, clear policies, and guidance are needed to ensure effective and proportionate approaches to research security. For RFOs and RPOs, challenges lie in the limited existing legal frameworks and the ambiguity of relevant policies, especially when trying to balance values of openness and academic freedom with security. An additional challenge also comes from national governments, who may be inclined to approach security risks as a binary scenario and adopt disproportionate measures, or leave the risks unaddressed. To help navigate the (unavoidable) risks associated with international collaboration, a proactive 'due diligence' research security culture should be adopted across the research ecosystem, following proportionate measures such as risk appraisals, investment in capacity building and information-sharing amongst all involved stakeholders. This requires

1 European Union export control rules for dual-use goods and technology and [Regulation \(EU\) 2021/821](#) of the European Parliament and of the Council (20 May 2021) are highly relevant to research security.

collaboration between all stakeholders, including RPOs, RFOs, industry, and governments.

According to the [Council recommendation](#) on enhancing research security,² Member States should engage with RPOs and RFOs when setting up measures to enhance research security. Safeguards can be introduced at different levels, from the project level to top-down restrictions, based on the risk category. At EU level, a series of initiatives is taking place, mostly co-ordinated by the European Commission (see Annex I). Enhancing research security is an ERA Action in the [ERA Policy Agenda 2025–2027](#), under the priority for ‘a truly functioning internal market for knowledge’, towards an efficient and inclusive European R&I system.

Activities of the Science Europe Task Force on Research Security

The Member Organisations of Science Europe, comprising both RFOs and RPOs, have distinct yet complementary responsibilities to navigate, and their collaboration is essential in this regard.

To facilitate this discussion, a series of workshops was held among a number of Science Europe Member Organisations between January and June 2025, initiated by Science Europe’s Task Force on Research Security:

■ Workshop 1A	28 January	<i>Online</i>
■ Workshop 1B, hosted by FWO	18 February	<i>Brussels (BE)</i>
■ Workshop 2, hosted by UKRI	28 March	<i>London (UK)</i>
■ Workshop 3, hosted by NCN	12–13 June	<i>Kraków (PL)</i>

This report presents the main elements of discussion during the workshops. In this context, the report is not a formal position of Science Europe and/or its Member Organisations, due to the heterogeneity of their individual policies on research security.

An organising committee that comprised representatives from UK Research and Innovation (UKRI), the Dutch Research Council (NWO), the Research Foundation Flanders (FWO), the National Science Centre Poland (NCN), and Science Europe co-ordinated the organisation of the workshops.

² On 24 January 2024, the European Commission issued a proposal for a Council recommendation (2024/0012(NLE)) on enhancing research security, as part of a package of proposals on economic security. The recommendation was adopted at the Competitiveness Council [meeting](#) of 23 May 2024.

Roles and Responsibilities of National RPOs and RFOs

Research performing and research funding organisations are responsible for developing and managing their international co-operation initiatives, with the support of their national government authorities.

They should seek to introduce proportionate internal risk-appraisal and due-diligence procedures, assign responsibility for research security within the organisation, raise awareness through trainings, protect sensitive knowledge and research facilities, and take physical and virtual safeguards (such as compartmentalisation and robust cybersecurity measures), among others.

This responsibility of RPOs and RFOs guided the internal discussion and sharing of best practices on the topic of research security. The participants' approaches come from a range of positions and national contexts that drive their existing policies and capabilities.

RPOs and RFOs face different challenges. For **RPOs**, the topics of discussion included (but were not limited to): international collaboration (*funding, agreements, and contracts*), research data and infrastructure (*purchase of equipment/software, cyber security, access control*), outgoing activities (*travel, secondments*), and incoming activities (*recruitment, foreign delegations*). Some of the main challenges that RPOs face in research security included the absence of a central information repository, limited institutional capacity, and a need for better training and guidance.

For **RFOs**, challenges related to how requirements on research security are communicated and managed through their national systems and within their organisational remits and contexts. Key considerations include ensuring that measures are applied in a proportionate, consistent, transparent, and effective manner, as well as clarifying the role and responsibilities of RFOs in relation to RPOs, national governments, and other actors within their system (such as technical agencies or other regulatory bodies).

Key Policy Messages on Research Security

From the perspective of both RPOs and RFOs, the main aim is to safeguard international co-operation at a global scale, uphold academic freedom, and promote open science. Risk assessment and due-diligence approaches should build and protect resilient partnerships, while remaining proportionate to the risks and protecting the R&I system. Awareness building, ethical reflection, and balanced policy making are essential.

The key messages for SE Member Organisations, together with the broader principles for responsible internationalisation³ – as set out in the Council recommendation – should be taken into consideration in enhancing research security. These messages included:

1. Safeguard international co-operation.

Cases were reported where, as a response to perceived risks or ambiguity regarding international research partners, research collaboration decreased or sometimes even stopped, leading to missed opportunities for academic and scientific advancement. Research actors should be equipped to responsibly assess and handle the risks that come with collaborating internationally. However, identifying the right level of due diligence is vital, as well as the need for balanced approaches that do not unintentionally discourage global engagement or impact research openness and transparency. Risk management is very complex, and RPOs and RFOs face internal challenges such as uneven awareness, a limited sense of urgency in departments perceiving less exposure to risks and security challenges, and fragmented governance structures that affect the formal authority to implement research security policy.

Research security measures should encourage and promote international co-operation that is open and safe. Although risk is unavoidable with bold and innovative research, it should be managed and mitigated rather than eliminated, to avoid impacting the pursuit of scientific knowledge. Research security measures should respect the institutional autonomy of research performing organisations and recognise the key role of research funding organisations. Balancing openness, security, and academic freedom is therefore the ongoing challenge as well as the overall objective.

³ Responsible internationalisation is a term increasingly used to promote relationship building in a world shaped by the growing impact of global challenges and geopolitical competition ([Council of the European Union, 2023](#)), Shih, T. (2024).

While smooth co-operation in research does not necessarily require full data sharing as a pre-requisite, trust and transparency are nonetheless fundamental. In the case of long-standing research partnerships, monitoring can be more challenging, though it may deepen the co-operation in the long run. In such cases, researchers should be equipped with the relevant awareness and decision-making tools, such as lists of measures and considerations that RPOs should ask their potential research partners.

2. Defining the boundaries or 'red lines'

Across RPOs and RFOs, there are significant disparities on how research security is assessed, managed, and interpreted. At the same time, the risk tolerance of each organisation varies (often also across an organisation), and self-evaluation of the risk might pose a challenge, especially for RPOs. When it comes to adopting research security measures, there is no 'one size fits all': approaches need to be tailored and adjusted to the national context and sensitivity of the research activity being conducted. Legal definitions do not always cover the full scope of concern, and compliance frameworks alone may be insufficient.

To establish what is considered 'good practice' in research security to secure international collaboration, an agreement on common principles, shared definitions, and terminology is required. Some institutions may apply rigorous controls, while others are more lenient, leading to inconsistent practices and potential points of weakness in the wider system. Such discrepancies may in turn shape international collaboration: researchers tend to gravitate towards environments that are seemingly less demanding when it comes to research security. This creates a so-called 'waterbed effect' and hinders progress towards ensuring a level playing field. Clear guidelines and minimum baselines, or 'red lines', for security practices are therefore essential for RPOs and RFOs in defining their specific responsibilities.

3. Proportionality of measures and due diligence approach

To safeguard academic freedom and encourage international collaboration, it is essential to avoid over-securitising the R&I system. That is one of the key concerns regarding the potential unintended consequences of overly risk-focused frameworks. Instead, the focus should be on preparedness, due diligence, and proportionate risk mitigation, rather than the complete elimination of risk. In this context, the misuse of the security rhetoric by national authorities should be prevented.

Commonly agreed principles and research security measures should transcend geopolitical barriers, and avoid protectionism and political instrumentalisation of R&I. RFOs should also ensure appropriate focus

on the complexities of 'grey zone' areas (areas not traditionally seen as the highest-risk areas, including ones that might have potential dual-use application). The current geopolitical context increases the importance of managing risks related to protectionism. Contributing to this cycle of escalation should be avoided; a thoughtful, proportionate, and dialogue-driven approach to research risks and responsibility should be taken. Some existing good practices include guiding RFOs and RPOs through targeted questions to identify and manage risks appropriately, such as following a country-aware approach and focusing on building good security practices and behaviours, as well as on raising self-awareness of potential risks. Finally, the incorporation of flexible mechanisms, such as specific and clearly defined withdrawal clauses, can facilitate the resolution of issues in a timely manner.

4. Embedding research security through awareness-raising and culture change.

To proactively incorporate research security, RPOs and RFOs must embrace a cultural shift and embed these concerns into their ethos, wider policies, and approaches. Researchers should be encouraged to develop a more critical mindset throughout the entire pipeline, from the earliest stage of the proposed collaboration, through submitting proposals, and ultimately during the implementation of the agreed research activities. Research security considerations should be built in from the outset and not viewed as an afterthought when a proposal is successful. The same approach should be applied by support staff and research managers. Emphasis should also be put on effective project monitoring at all stages of the research life-cycle, rather than relying on final reporting on projects.

While EU-level lists and guidelines exist, tools alone are not sufficient without properly trained staff capable of interpreting and analysing the data and identifying red flags. Emphasis should be placed on embedding security into the mindset of researchers; RPOs in particular play a key supporting role. This should apply at all stages of researchers' careers, including for established researchers who may have been trained in a different environment and are not always aware of current risks or eager to adapt existing practices. RPOs and RFOs should encourage their researchers and wider staff to think more critically and at an earlier stage, even before submitting proposals. Funding organisations can help prevent problematic applications from entering the system to begin with, by having clearly articulated policies and supporting guidance, reducing further cost and administrative burden on the sector.

Some organisations provide general training to all staff in the organisation and more specialist training to the roles who require it, or

even develop training materials and guides. Training should be discipline-specific and target different audiences (such as PhDs, senior leaders, research managers).

5. Capacity-building is required for RFOs and RPOs.

While awareness of research security has generally increased, there is concern about the way in which organisations implement measures and necessary safeguards, translating strategic knowledge into practical support.

RPOs, RFOs, and the broader R&I sector should invest in dedicated in-house research security expertise and skills, and assign responsibility to the appropriate organisational levels. In some cases, this has been done through the creation of a committee for research security within a research organisation. Its functions could include maintaining institutional policies and practices for research security; advising staff on international collaboration; providing training; preparing the organisation's research security plan; ensuring compliance with security requirements for national and international calls; and, taking an advisory role in the negotiation of international agreements, protocols, and contracts. However, as resources amongst organisations vary, RPOs and RFOs may also benefit from independent national (or regional) advisory services that could work closely with institutions to raise standards sector-wide.

6. Systemic support/collaborative approach.

The size of an organisation often dictates the available resources it can dedicate. For that reason, larger institutions generally possess greater resources and capabilities to address security concerns, whereas smaller institutions require assistance, and benefit more from a support ecosystem. Identifying opportunities for establishing communities of support and practice should therefore be encouraged.

National governments and the EU should promote consistent messaging and support RPOs and RFOs through actionable guidance, legal frameworks, as well as clearly defined roles and responsibilities. At the same time, opportunities for wider dialogue that bring together the views of intergovernmental partners (such as the G7, Organisation for Economic Co-operation and Development (OECD), UNESCO, or Council of Europe) and the wider R&I sector would help build trust and could be used to help share information and increase awareness and capability. Facilitating dialogue for stakeholders is extremely beneficial, supporting both RFOs and RPOs that are starting to invest more in the agenda to learn from those that already have policies in place.

Actions by Science Europe Member Organisations

As key stakeholders in the European R&I landscape, Science Europe and the co-organisers of this workshop series have identified several activities and next steps to support the implementation of the Council recommendation.

Science Europe will continue to advocate to the European Commission as its members continue to shape their approach and capability around research security needs. These initiatives are considered complementary to the initiatives already underway at the European level, as well as providing direct support and benefit to the Member Organisations involved and wider national structures.

- 1. Continue to facilitate dialogue within Science Europe:** Member Organisations will continue to convene, discuss common challenges, and exchange best practices, as well as take note of any developments in their research security measures. The Task Force on Research Security will convene twice a year to take stock of national, European, and international developments and practices that directly or indirectly impact research security. Practical workshops on selected thematic areas (such as dual-use, or export controls) will also be organised *ad hoc*, to allow for more in-depth discussion and exploration, bringing together experts and practitioners to share empirical understanding.
- 2. Create a repository of cases, good practices and tools:** This will be a dedicated platform and toolbox for Member Organisations to map their research security initiatives. Such an internal platform would allow members to benefit from their collective intelligence and serve as a space for exchange of good practices.
- 3. Establish a Science Europe Centre of Support for Member Organisations:** Such a centre would focus on competence building and learning through knowledge exchange, through the facilitation of workshops that use real case studies to build knowledge and expertise within the sector and between Science Europe members. It would make use of the resources gathered through the internal repository (see item 2).
- 4. Continue collaboration and dialogue with the European Commission:** Science Europe will continue to be an active R&I stakeholder and participate in all relevant stakeholder consultations. The outcomes from this workshop series and discussions at the European Commission's Flagship Conference on Research Security aim to refine Science Europe's policy and advocacy messages on research security.

Ways Forward for Science Europe

This synthesis of workshop discussions has explored where and how RFOs and RPOs can add value to the development of a common awareness and understanding of research security and identify proportionate and effective approaches that support international collaboration. It also identifies areas for mutual learning, co-development, and co-ordinated approaches.

Overall, in an increasingly complex international environment, research security must be approached not as a constraint on academic freedom or international collaboration, but rather as a protective framework that enables researchers to conduct their work freely, responsibly, and with trust, consistency, and transparency in their output; it should empower them instead of restricting them.

This depends on governments, RFOs, and RPOs defining and implementing research security requirements effectively and efficiently; poorly-designed or -applied measures can be just as harmful to science as the absence of such measures altogether. Restrictions on international collaboration should only apply in the case of real risks, which should be clearly communicated and consistently applied. Ongoing dialogue between these actors, institutional flexibility, and a shared responsibility for research security are essential to making progress for this agenda and ensuring long-term cultural change within the global R&I ecosystem.

Both RFOs and RPOs, as well as national governments and the EU, have distinct yet complementary responsibilities. Within Science Europe, the combination of both perspectives offers a valuable opportunity for mutual learning, alignment, and the development of co-ordinated strategies.

To deal with short-term challenges stimulated by geopolitical turbulence, as well as the need for compliance with evolving legislation and the development of good practices in this space, a deeper cultural and behavioural shift is required. This involves embedding shared values of research integrity and research cultures, such as collegiality, reciprocity, openness, and academic freedom, as well as translating responsibility, thoughtfulness, and critical thinking into actionable measures. In this context, Science Europe incorporates the shared values set out in its [Values Framework](#) (2022), and the [Vision and Framework for Research Cultures](#) (2025) throughout its relevant activities.

Ongoing and future activities mentioned throughout the document, including the two dedicated sessions at the 2025 Flagship Conference on Research Security organised by the European Commission, will be Science Europe's main contribution to Priority 1 of the [ERA Policy Agenda 2025-2027](#), on 'a truly functioning internal market for knowledge'. Science Europe will continue to work closely with its Member Organisations towards the identification and development of appropriate and proportionate measures to advance international collaboration.



Annex I: EU Initiatives

At the EU level, a series of activities are already planned by the European Commission as a follow-up on the Council recommendation:

- 1. Using the European Research Area governance:** the Commission will make full use of the governance structures of the European Research Area (ERA), to support implementation of the Recommendation. The work carried out in this context will support the Member States and the R&I sector in their efforts to develop coherent sets of policy measures and create support structures through peer learning and capacity building. The ERA policy agenda 2025–2027 includes a Priority Action on Enhancing Research Security.
- 2. Research Security Monitor 2025:** A report prepared by the Commission provides a baseline of research security policies and measures. The report highlights interesting initiatives and actions, giving visibility to the R&I sector, through showcasing good practices. The Monitor presents observations on a governance level (EU/national/funders/sector), rather than a country-by-country approach.
- 3. European Flagship Conference on Research Security:** The first European Flagship Conference on Research Security, taking place on 28–30 October 2025, was co-organised by the Commission, together with twelve R&I stakeholder organisations. Science Europe organised two sessions, one on the ‘Needs and responsibilities of RPOs and RFOs’, and a session jointly organised with the European Federation of Academies of Sciences and Humanities (ALLEA) on ‘Integrating academic freedom and research security’.
- 4. Establishing a Centre of Expertise on Research Security:** A Centre of Expertise (as specified by Clause 18 of the Council Recommendation) will i) support the development of an evidence base for research security policy making, and ii) create a community of practice, including experts and practitioners. The Centre will provide analyses, impact studies, awareness-raising activities, and act as a network of experts and practitioners linking national support structures. The expectations of the research community are quite high regarding the Centre of Expertise; it should provide an EU-approved list of sources and databases, create the space to share intelligence, and promote research on research security.
- 5. Building blocks on risk appraisal:** In 2024, the European Commission published a factsheet that addressed in more detail the issue of risk appraisal; it is a valuable resource for many RPOs and RFOs.

A more extensive guidance document will aim to provide concrete guidance to RPOs, particularly for research managers and other research staff involved in international collaboration in third countries.

6. **Collecting data on science, technology and innovation (STI) policies:** In a joint initiative by the European Commission and the OECD, the [2025 edition of the STIP Compass](#) collects qualitative and quantitative data on national trends in STI policy, covering internationalisation policies, and a [thematic portal on research security](#).

Annex II: Definition of Research Security

According to the Council Recommendation, 'Research security' refers to anticipating and managing risks related to:

- a. the undesirable transfer of critical knowledge and technology that may affect the security of the Union and its Member States, for instance if channelled to military or intelligence purposes in third countries;
- b. malign influence on research where research can be instrumentalised by or from third countries in order to inter alia create disinformation or incite self-censorship among students and researchers infringing academic freedom and research integrity in the Union;
- c. ethical or integrity violations, where knowledge and technologies are used to suppress, infringe on or undermine Union values and fundamental rights, as defined in the Treaties.

The text of the recommendation recognises that 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 [...] while preserving an open economy and pursuing a level-playing field and balanced reciprocal openness." Moreover, hybrid threats may affect sectors but the research sector is considered particularly vulnerable, due to its values and practice of openness, academic freedom, institutional autonomy and worldwide collaboration.

Science Europe AISBL

RUE DE LA SCIENCE 14, 1040 BRUSSELS, BELGIUM

Science Europe is the association of major research funding and research performing organisations in Europe.

Our vision is for the European Research Area to have the optimal conditions to support robust education and research & innovation systems.

We define long-term perspectives for European research and champion best-practice approaches that enable high-quality research for knowledge advancement and the needs of society.

We are uniquely placed to lead advancements to the European Research Area and inform global developments through participation in research initiatives where science is a strong and trusted component of sustainable economic, environmental, and societal development.

More information is available at www.scienceeurope.org

 @scienceeurope.org
 @ScienceEurope

 Science Europe
 @science-europe