



EUROPEAN RESEARCH SECURITY: THREAT PERSPECTIVES AND THE RESPONSES OF POLICY MAKERS AND RESEARCH PERFORMING ORGANISATIONS

DOI:

[10.71535/d5993826-83d6-4aa2-8e23-4195ad92b629](https://doi.org/10.71535/d5993826-83d6-4aa2-8e23-4195ad92b629)

Document Version

Final published version

[Link to publication record in Manchester Research Explorer](#)

Citation for published version (APA):

James, A., Flanagan, K., Naisbitt, A., & Rigby, J. (2025). *EUROPEAN RESEARCH SECURITY: THREAT PERSPECTIVES AND THE RESPONSES OF POLICY MAKERS AND RESEARCH PERFORMING ORGANISATIONS*. Manchester Institute of Innovation Research. <https://doi.org/10.71535/d5993826-83d6-4aa2-8e23-4195ad92b629>

Citing this paper

Please note that where the full-text provided on Manchester Research Explorer is the Author Accepted Manuscript or Proof version this may differ from the final Published version. If citing, it is advised that you check and use the publisher's definitive version.

General rights

Copyright and moral rights for the publications made accessible in the Research Explorer are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

Takedown policy

If you believe that this document breaches copyright please refer to the University of Manchester's Takedown Procedures [<http://man.ac.uk/04Y6Bo>] or contact openresearch@manchester.ac.uk providing relevant details, so we can investigate your claim.



EUROPEAN RESEARCH SECURITY: THREAT PERSPECTIVES AND THE RESPONSES OF POLICY MAKERS AND RESEARCH PERFORMING ORGANISATIONS

ANDREW D JAMES

KIERON FLANAGAN

ALICE NAISBITT

JOHN RIGBY

MAY 2025

MANCHESTER
1824

The University of Manchester

European research security: threat perspectives and the responses of policy makers and research performing organisations

Professor Andrew D James¹

Professor Kieron Flanagan¹

Dr Alice Naisbitt¹

Dr John Rigby²

¹ Manchester Institute of Innovation Research, University of Manchester, UK

² Bibliometrica Ltd, UK

MAY 2025

DOI: 10.71535/d5993826-83d6-4aa2-8e23-4195ad92b629

ISBN 978-0-946007-40-0

MANCHESTER INSTITUTE OF INNOVATION RESEARCH,
ALLIANCE MANCHESTER BUSINESS SCHOOL, UNIVERSITY OF MANCHESTER, M13 9PL, UK
Web: www.mioir.manchester.ac.uk
Email: mioir@manchester.ac.uk

ACKNOWLEDGMENTS

The study was undertaken by a team from the Manchester Institute of Innovation Research, University of Manchester, UK with subcontractor Bibliometrica Ltd and was commissioned by the UK Government's Science & Technology Network (STN). STN leads on developing science partnerships and deploying science diplomacy around the world and is a joint initiative of the Foreign, Commonwealth & Development Office (FCDO) and the Department for Science, Innovation & Technology (DSIT). We wish to thank all the participants across the seven countries, the UK and European organisations for their time in agreeing to be interviewed for this study. All analysis, interpretation and recommendations are solely those of the authors and do not reflect the views of any institution to which the authors are affiliated nor those of the FCDO or DSIT.

DATA ACKNOWLEDGEMENT

Any primary bibliometric analysis in this report was enabled by The Lens <https://www.lens.org/> [[lens.org](https://www.lens.org/)]



CONTRIBUTORS' BIOGRAPHIES

Dr Andrew D. James is Professor of Innovation Management and Policy at the Manchester Institute of Innovation Research, Alliance Manchester Business School, University of Manchester.

Dr Kieron Flanagan is Professor of Science and Technology Policy at the Manchester Institute of Innovation Research, Alliance Manchester Business School, University of Manchester.

Dr Alice Naisbitt is Research Associate at the Manchester Institute of Innovation Research, Alliance Manchester Business School, University of Manchester.

Dr John Rigby is Director at Bibliometrica Ltd and Honorary Senior Fellow at the Manchester Institute of Innovation Research, Alliance Manchester Business School, University of Manchester.

THE MANCHESTER INSTITUTE OF INNOVATION RESEARCH

The [Manchester Institute of Innovation Research](#) is a centre of excellence in the field of innovation studies, building on a more than 50-year tradition of innovation and science studies in Manchester. With around 50 full members, approximately 40 PhD researchers, and a range of associated academics and practitioners, it is one of the world's leading research centres in these fields.

Suggested citation: James, A.D., Flanagan, K., Naisbitt, A. and Rigby, J. (2025). *European Research Security: Threat Perspectives and the Responses of Policy Makers and Research Performing Organisations*. Manchester, UK: Manchester Institute of Innovation Research, University of Manchester. ISBN 978-0-946007-40-0

EXECUTIVE SUMMARY

Modern science is a global enterprise and international research collaboration is a key feature of scientific and technological knowledge production. However, there is a growing concern that it faces challenges from those who seek to illegitimately acquire academic research and expertise or interfere with academic discourse. This has implications for national security, economic competitiveness and the integrity of research collaboration. This impacts researchers in STEM subjects, dual-use technologies, emerging technologies and commercially sensitive research areas, from AI and data science to mathematics and materials science. Equally, foreign interference can have consequences for the conduct of social sciences and humanities.

The report

This report examines perceptions about threats to European research security and the policies and practices in response to those perceived threats. We examine the policies and practices of governments, universities and public research institutes (“research performing organisations”) in the Czech Republic, France, Germany, Italy, the Netherlands, Spain and Sweden. We also assess developments in policies by the European Union.

The study was commissioned by the UK Government’s Science & Technology Network and was conducted by the Manchester Institute of Innovation Research (University of Manchester, UK) between September 2024 and March 2025. This report discusses the situation as of 28 February 2025.

The study used a mixed methods approach, combining quantitative insights from bibliometric data and qualitative data through the collation of policy documents and media reports. The core of the study was a programme of interviews with more than 85 policy makers, research funders, senior leaders of research performing organisations, administrators and managers in research performing organisations, representatives of sector organisations, and independent experts.

Our key findings

- The European countries studied have **similar perceptions of the threats** posed by international research collaboration.
- There are concerns about **threat vectors** associated with the hostile activities of threat actors and poor risk management practices of research performing organisations or individual researchers.
- The **same threat actors are typically identified in the discourse of the countries that we studied**, namely China, Russia and Iran.
- There is a **growing awareness** about research security and policies and risk management practices are being put in place.
- There is **diversity of policy and practice between research systems** with countries at very different stages in their response to research security challenges. We found that some countries have mature research security policies and practices. Other countries are at an early stage in their response to research security threats. However, no country can be said to have institutionalised research security practices across its whole research system.

-
- There is **diversity within the research systems** of individual countries and research performing organisations within research systems are adopting research security policies and practices at different rates. Almost all countries have a core of research performing organisations that have mature research security practices and a tail of organisations with less developed practices. The less engaged ones are often smaller and less internationalised organisations, or those that find the costs of implementing research security measures prohibitive.
 - **A range of non-legislative research security measures exist.** A variety of means are being used to promote awareness and create forums for dialogue between government, security agencies, research funders and research performing organisations although we found no equivalent to the UK's Trusted Research Campaign.¹ A range of written guidance exists on research security written by sector bodies, government or through co-development by stakeholders. Central advice teams for information sharing by government exist in only a few countries and perform a similar role to the UK Government's Research Collaboration Advice Team (RCAT).² Risk management and due diligence processes are being developed and implemented.
 - **Legislative measures exist that have implications for research performing organisations.** EU and national export controls govern certain technologies and research fields but there are concerns about awareness, institutional oversight and capacity especially regarding intangible knowledge transfer. Visa control and vetting procedures focused on foreign researchers and students are being considered by some countries (although none of the countries studied currently has an equivalent of the UK Academic Technology Approval Scheme - ATAS³). Foreign direct investment controls have implications for university spin-offs and in some cases foreign research funding. Unlike the UK, France and Sweden have statutory protective security requirements for research performing organisations engaged in certain sensitive activities.
 - The focus of research security policy and practice is moving **from awareness raising to capacity building and broadening the adoption of good practice** across the research system.
 - There is recognition of the need to increase capacity for risk management, due diligence and export control compliance. **Action remains challenging due to a range of barriers** including resource constraints, a lack of suitably skilled individuals and limited training programmes.
 - **There are opportunities for mutual learning amongst governments, research funders and research performing organisations.** There is a growing body of knowledge and practice in the field of research security and there is a very real appetite to find forums and mechanisms for sharing these experiences and lessons learned.
 - **Striking the right balance between research security and openness to international research collaboration is a key concern for universities, research funders and governments.** The countries remain committed to scientific openness and collaboration with the best scientific partners wherever in the world they reside. We found that countries and organisations that exhibited the most sophisticated responses to perceived research security threats are also clearest about the need to continuously balance research security concerns against the social and economic benefits of participating in open international scientific collaboration.

Our recommendations

Drawing on the findings of our study, we make the following recommendations for the UK and European governments, research funding organisations, research sector organisations and individual universities.

- **Governments** should broaden and deepen their support for capacity building and promote greater information sharing to build an evidence base that can assess what risk management practices are effective as well as the costs of poor practice. Critically, like-minded governments should work together to create sector-wide research security standards and quality assurance to support research performing organisations. Since research security is a crowded policy space there is a need for careful coordination between like-minded countries and, if this initiative is to have the maximum impact, they should seek a forum that engages the widest grouping of countries who are engaged in international research collaboration.
- **Research funders** should broaden and deepen mutual learning exercises with like-minded organisations. Research funders should consider how to include security requirements in grant funding and balance that against the huge benefits of scientific openness.
- **European associations of universities and research professionals** have an important role in facilitating mutual learning activities and professional bodies should be supported by governments to deliver capacity building activities.
- **Universities and research institutes** should leverage their strategic partnerships to conduct mutual learning exercises and agree expectations and minimum standards for research security in their joint activities.

TABLE OF CONTENTS

1. INTRODUCTION	9
1.1 International research collaboration is a key feature of scientific knowledge production ..	9
1.2 There are concerns that international research collaboration is threatened by hostile actors	11
1.3 This report examines research security threats, policies & practices in seven European countries and the EU	12
2 RESEARCH PERFORMING ORGANISATIONS & THEIR INTERNATIONAL RESEARCH COLLABORATIONS	13
2.1 Countries differ in the organisation & governance of their universities & the importance of public research institutes.....	13
2.2 International research collaboration plays an important role in each country	14
3 EUROPEAN PERSPECTIVES ON RESEARCH SECURITY: THREATS & RESPONSES	18
3.1 Countries define research security in different ways.....	18
3.2 Countries have similar perceptions of the research security threats that they face	20
3.3 Responses to research security threats differ between countries & within countries	30
3.4 A variety of factors are influencing responses	35
3.5 Differing governance models have emerged in response to these factors	40
3.6 The focus is turning to capacity building & adoption of good practice	40
4. NON-LEGISLATIVE RESEARCH SECURITY MEASURES	42
4.1 Various means are being used to promote awareness & create forums for dialogue	42
4.2 A range of written guidance exists	45
4.3 Central advice teams exist in some countries	46
4.4 Mature risk management processes have been developed by some research performing organisations.....	47
4.5 Some countries provide public funding for capacity building	50
5 LEGISLATIVE MEASURES WITH IMPLICATIONS FOR RESEARCH SECURITY	52
5.1 Export control practices vary between & within countries	52
5.2 Some countries are considering vetting of visiting researchers & foreign students	56
5.3 Foreign investment controls have implications for research performing organisations ...	57
5.4 Statutory protective security requirements exist in France & Sweden	58

6 RECOMMENDATIONS & CONCLUSIONS 61

6.1	Research security policies & practices are maturing but areas of weakness remain	61
6.2	Recommendations	62
6.3	Limitations of the study & directions for future research	64
6.4	Attention needs to move towards capacity building & convergence of research security practices	65

APPENDICES 67

Appendix 1: Research methodology	68
Appendix 2: Country case study - Czech Republic	72
Appendix 3: Country case study - France	83
Appendix 4: Country case study - Germany	94
Appendix 5: Country case study - Italy	103
Appendix 6: Country case study - The Netherlands	111
Appendix 7: Country case study - Spain	121
Appendix 8: Country case study - Sweden	127
Appendix 9: Case study – the European Union	142
Appendix 10: Interview codes	149

REFERENCES AND NOTES 150

1. INTRODUCTION

- International research collaboration plays a central role in scientific and technological activity.
- There is a growing concern that international research collaboration faces challenges from those who seek to illegitimately acquire academic research and expertise or interfere with academic discourse.
- There is an anxiety that, without attention and effective management, such threats may have implications for national security, economic competitiveness and the integrity of research collaboration.
- This matters for researchers in STEM subjects, dual-use technologies, emerging technologies and commercially sensitive research areas, from AI and data science to mathematics and materials science. Equally, foreign interference can impact the conduct of the social sciences and humanities.
- In response, European governments, research funders and research performing organisations are increasingly thinking about how to strike the right balance between openness and research security in their international research collaborations.
- This report examines research security policies and practices in seven European countries and the EU.

1.1 International research collaboration is a key feature of scientific knowledge production

- **Modern science is a global enterprise** and international research collaboration is a key feature of scientific and technological knowledge production. For example, more than two-

Key terms

International research collaboration.

International research collaboration refers to relationships between researchers or institutions across different countries to jointly conduct research, share knowledge, and achieve common scientific goals. This may include joint research funding, sharing of scientific infrastructure, co-publication, foreign lab visits or presentations at international conferences.

Research security. Countries define research security in different ways. We follow the G7's definition of research security agreed in June 2022: "the actions that protect our research communities from actors and behaviours that pose economic, strategic, and/or national and international security risks. Particularly relevant are the risks of undue influence, interference, or misappropriation of research; the outright theft of ideas, research outcomes, and intellectual property by states, militaries, and their proxies, as well as by non-state actors and organized criminal activity; and other activities and behaviours that have adverse economic, strategic, and/or national security implications".

Research integrity. The concept of research integrity also appears in some discussions, and we follow the G7's approach, seeing research integrity as a separate but related concept. We did not specifically seek to examine research integrity but considered it when it proved to be directly linked by any country in its treatment of research security.

thirds of all UK scientific outputs (excluding arts, humanities and social sciences) are internationally co-authored.⁴

- **There are different types of international research collaboration.** Relationships between researchers or institutions across different countries can take different forms as they seek to jointly conduct research, share knowledge, and achieve common scientific goals. This may include research funding, sharing of scientific infrastructure, co-publication, foreign lab visits or presentations at international conferences.⁵

- **Policy makers have actively encouraged international research collaboration.** Co-authored publications tend to be more highly cited (generally interpreted as a measure of quality) and international research collaboration can be an element of soft power. This has led research policymakers, funders and the leaders of research performing organisations to actively promote international research collaboration in recent decades.⁶

- **Sharing the costs and risks of research has also been an important driver of international research collaboration.** The desire to share the costs and risks of large-scale research projects has led to the promotion of international research collaboration, especially via joint funding initiatives or the development of inter-governmental research organisations such as CERN.⁷

- **Researchers participate in international research collaborations to access knowledge, equipment, data or materials not available domestically.** Such collaborations allow access to

Key terms

Foreign interference. This report discusses foreign interference and here we follow the OECD definition that “foreign interference is carried out by, or on behalf of a foreign actor and is contrary to national sovereignty, values, and interests. It is coercive, covert, deceptive, or corrupting. This is in contrast to foreign influence, which is part of normal diplomatic relations and is normally conducted in an open and transparent manner” (OECD, 2022: p.18). As the OECD notes, the line between interference and influence is not always clear.

Research security maturity. We refer in this report to the maturity of research security at the national and institutional level. We define maturity as the extent to which a research system or research performing organisation has developed and implemented policies, processes and capacity to manage research security risks effectively while maintaining academic freedom and openness to international research collaboration.

Research security capacity. Capacity in research security refers, at the national or organisational level, to the ability to protect the research system from foreign interference, espionage, cyber threats, and intellectual property theft while maintaining an open and competitive research environment. This involves legal, institutional, technological, and human resources dedicated to safeguarding research.

unique datasets, like population health records or climate data, as well as knowledge and specialised expertise.⁸

• **Researchers also have personal career motives.** Individual researchers may pursue international research collaborations to access funding, gain advantage from the greater reputation or visibility of international collaborators, and to publish in higher quality academic journals.

1.2 There are concerns that international research collaboration is threatened by hostile actors

• **There is a growing concern** that international research collaborations face challenges from those who seek to illegitimately acquire academic research and expertise or interfere with academic discourse.⁹

• **Impact on national security:** When sensitive research is exposed to hostile actors, it can accelerate their technological capabilities in areas critical to defence and national security. This may erode a nation's strategic edge, weaken its ability to deter threats, or even compromise critical infrastructure or defence systems. The overall result would be a reduced capacity to protect national interests and respond to emerging security challenges.¹⁰

• **Impact on economic competitiveness:** Theft or misappropriation of research outputs can result in direct economic losses. All research can be at risk, but applied research is argued to be particularly vulnerable, especially where there is a specific commercial application. In these cases, the consequence of research outcomes being exploited may be substantial and may result in loss of economically valuable intellectual property.¹¹

• **Impact on the integrity of collaborative**

research: These issues can undermine confidence in the integrity of the scientific enterprise amongst scientists, funders and the public. When affiliations or funding sources are undisclosed, or when research appears influenced by external interests, it damages the credibility of findings. Reduced transparency and weakened peer accountability diminish public trust, strain international collaboration, and compromise the perceived legitimacy and reputation of research performers.¹²

-
- **Impact on research.** There are consequences in STEM subjects, dual-use technologies, emerging technologies and commercially sensitive research areas, from AI and data science to mathematics and materials science. Equally, foreign interference can impact the conduct of social sciences and humanities.¹³
 - Attention is being paid to effective research security and risk management practices.¹⁴ European universities, research funders and governments are increasingly thinking about **how to strike the right balance** between openness and research security in their international research collaborations.

1.3 This report examines research security threats, policies & practices in seven European countries and the EU

We start from this growing awareness of the importance of research security and the desire for mutual learning on the part of policy makers and research performing organisations.

- **This report examines perceptions of threat to European research security and the policies and practices in response to those threats of governments, universities and public research institutes (“research performing organisations”) in seven European countries.** We do not consider the research security threat in business and industry, except where it impacts universities or public research institutes.
- We examine **the Czech Republic, France; Germany; Italy; the Netherlands; Spain and Sweden.** We also consider **the European Union**, and we provide some information on the United Kingdom.
- The study used a mixed methods approach, combining quantitative insights from bibliometric data and qualitative data through the collation of policy documents and media reports. The core of the study was a programme of interviews with more than 85 policy makers, research funders, senior leaders of research performing organisations, administrators and managers in research performing organisations, representatives of sector organisations, and independent experts. The study was conducted between September 2024 and March 2025. This report discusses the situation as of 28 February 2025. (See Appendix 1 for detailed explanation of our choice of countries and our data collection method).

In doing so, the aim of this study was to:

- **Understand perceptions** of research security threats in selected European countries.
- **Examine research security policies and practices** of governments, universities and public research institutes in those countries and at the EU level, in response to those threats.
- **Consider opportunities for enhanced resilience to research security threats including the scope for cooperation** between European partners.

2 RESEARCH PERFORMING ORGANISATIONS & THEIR INTERNATIONAL RESEARCH COLLABORATIONS

- The countries differ in the organisation and governance of their universities and the importance of public research institutes.
- International research collaboration plays an important role in each country, and is particularly important to the Netherlands, Sweden and France.
- International co-publication and training of foreign PhD students are both important features of their international research collaborations.

We begin our report by examining the features of the research systems of the countries that we studied, and the role played by international research collaboration.

2.1 Countries differ in the organisation & governance of their universities & the importance of public research institutes

- **There is a diversity of arrangements for the conduct, funding and governance of publicly funded research.** The countries that we studied include federal and semi-federal countries (Germany and Spain) as well as countries with more unitary government systems. In some of the science systems most research happens in research-intensive universities and non-university public sector research institutes (the Netherlands and Germany), there are systems where there is a prominent research-performing national research council (France, Italy, Spain) and one with a prominent Academy of Sciences (Czech Republic).
- **The organisation and governance of higher education and research differs between countries.** University or national research council academics have civil servant status in countries such as France, Germany, Italy or Spain. Many universities in Germany and Spain have “civil clauses” precluding them from conducting military or dual-use research.¹⁵ There are legal and constitutional protections for academic freedom in several countries, including the Czech Republic, Spain and Sweden.¹⁶
- **Business engagement differs between countries.** There are differences in the extent to which universities and public research institutes conduct or collaborate in commercial research.^{17 18}

2.2 International research collaboration plays an important role in each country

2.2.1 International co-publications show the particular importance of international research collaboration to Sweden and the Netherlands

The standard metric for international research collaboration is the publication of scientific papers with co-authors based in another country.

- **Sweden and the Netherlands stand out with a particularly high share of internationally co-authored outputs.** Table 1 (below) provides detail from two recent studies using Scopus data for 2018 and 2022 respectively and including the UK for comparison purposes. Both Sweden and the Netherlands represent small but highly mature research systems and researchers working in smaller research systems may be expected to look outside the system for collaborators more often¹⁹. Spain and Italy have the least share of international co-authorship but even here half of all outputs are internationally co-authored.
- **Co-authorship with non-EU member state researchers is also increasing for each of our case study countries.** The figures quoted above include research collaboration within the EU, which is a significant part of the international research collaboration of these countries and partly driven by Horizon and other European funding. Therefore, we also examined co-authorship with non-EU member states (see Figure 1). Again, Sweden and the Netherlands stand out for the intensity of their international co-authorship with scientists outside the EU.

We also undertook a simple bibliometric analysis of international co-publication to find the most important partner countries for co-authorship with our study countries.²⁰ Our bibliometric analysis used *The Lens*, an open-source tool providing data on scholarly publications.²¹ Our analysis found that:

- **The United States** is the leading partner for the countries that we studied with the UK generally coming second. **Switzerland, Australia and Canada** also frequently appear in the top ten collaborating countries by count of publication.
- **China is present in the top ten for each of our case study countries and has risen in the ranking over time for most of them.**
- **Multi-author partnerships.** We used *The Lens* to look at co-authored papers with authors having an affiliation in one of our case study countries and authors with an affiliation in China²². This is important since many collaborative articles include authors from more than two countries, and these multi-co-author international research collaboration patterns can demonstrate interdependencies between national research systems. We found that where three or more countries are present amongst the author affiliations of these papers, in almost every case the most frequent additional partner country seen is the US, followed by the UK.²³

Table 1: International research collaboration measured by co-publication

Country	IRC % Scopus data for 2018 ²⁴	IRC% Scopus Data for 2022 ²⁵
Sweden	67	69
Netherlands	65	68
<i>UK</i>	<i>61</i>	<i>66</i>
France	60	60
Czech Republic	51	56
Germany	56	56
Spain	51	51
Italy	51	50

2.2.2 International PhD students are important to the Netherlands, France and Sweden

We also examined the relative importance of foreign PhD students to the national research base. We provide OECD data on the number of each country's PhD students who come from abroad and as a proportion of all PhDs studying in the country. Table 2 (below) shows that almost half of Dutch PhD students are from abroad (48%). France (37%) and Sweden (36%) are the next ranked countries. By contrast, international students account for 40% of UK PhD students. Germany (6742), France (2543) and Sweden (941) had the largest number of Chinese PhD students. The countries that had the largest proportion of their PhD student body from China were Sweden (4.9%), the Netherlands (4.7%) and France (3.9%). By contrast, the UK percentage was 8.7%. ²⁶

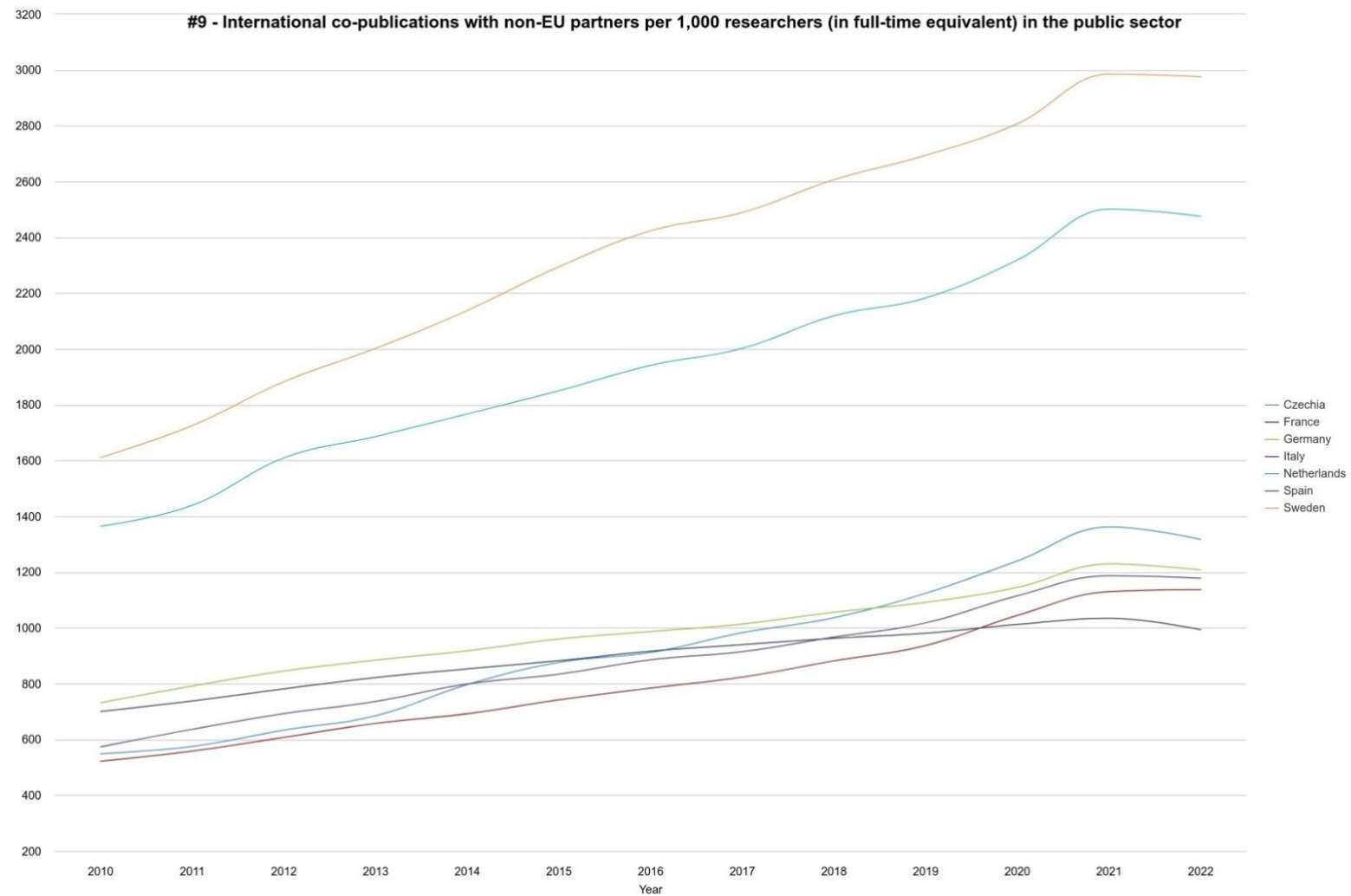


Figure 1: International co-publications with non-EU partners per 1,000 researchers (FTE) in the public sector (European Commission's European Research Area Performance Monitor)²⁷

Table 2: Numbers of international PhD students and as percentage of all PhD students

Country	All PhDs 2021	International 2021	International 2022	% International 2021	% of all PhDs from China 2021
Czech Republic	21,847	5,327	5,594	26%	0.6%
France	65,088	24,176	24,013	37%	3.9%
Germany	192,270	43,230	45,647	24%	3.3%
Italy	33,315	3,205	4,490	13%	0.7%
Netherlands	16,866	8,151	n/a	48%	4.7%
Spain	95,797	18,646	19,693	21%	0.8%
Sweden	19,120	6,845	6,897	36%	4.9%
UK	113,877	46,598	46,113	40%	8.7%

3 EUROPEAN PERSPECTIVES ON RESEARCH SECURITY: THREATS & RESPONSES

- Countries define research security in different ways.
- Countries have similar perceptions of the research security threats that they face.
- Research systems are at very different stages of maturity in their response to these research security threats.
- A variety of factors are influencing the responses of governments and research performing organisations.
- Differing governance models have emerged in response to these factors.
- The focus of research security policy is moving from awareness raising to capacity building and the widening of the adoption of good practice.

3.1 Countries define research security in different ways

- **Different terms are used to characterise research security.** Whilst the term “research security” tends to be used by the UK (alongside the concept of ‘trusted research’), other Anglophone countries, and G7 members, we note that other terms are used by some European countries and international organisations. The Netherlands uses the term ‘knowledge security’, whilst in Germany we see the use of ‘research security’, ‘security-relevant research’ and ‘knowledge security’.²⁸ The Czech Republic talks about foreign interference. Sweden uses the term ‘responsible internationalisation’. The European Council/European Commission’s definition of research security differs from that used by the G7 and the term ‘responsible internationalisation’ is also used.
- **Research integrity is typically considered alongside research security.** Although we did not focus on issues of research integrity, we found that most countries considered research integrity in their assessment of international research collaboration. The Swedish idea of “responsible internationalisation” places considerable emphasis on issues of ethics and integrity in international research collaboration. Research integrity is also seen in the definitions used by the Czech Republic, Italy and the Netherlands and it is also considered by German organisations. We observed differences in the balance of emphasis given to research security and research integrity between countries but also within countries. Thus, some research security officers in Sweden felt that more attention should be paid to security threats within the concept of responsible internationalisation.
- **There are competing views about the impact of these different definitions on communication between countries.** A previous study noted: “These terms are often used

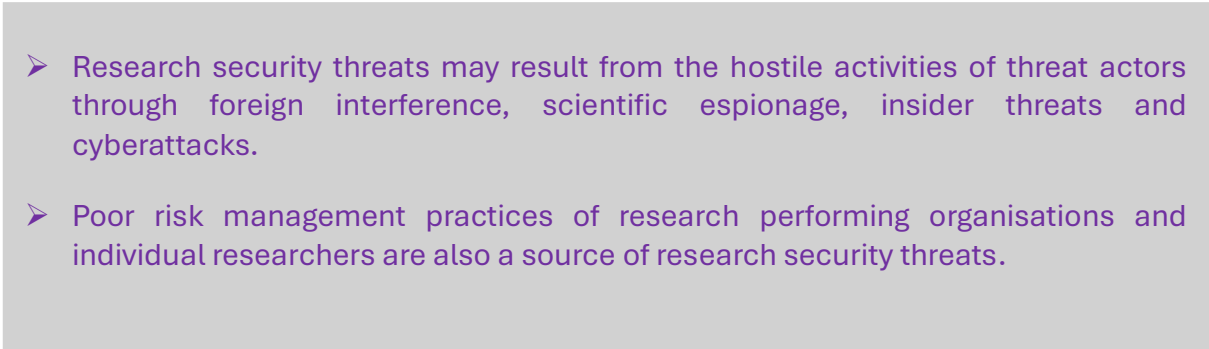
Table 3: Definitions of research security

Country	Definition
Czech Republic	“Organisational and systemic procedures for evaluating and managing security risks in the area of research and education, which reduce the risks associated with illegitimate interference in the higher education and research environment. The primary goal of research security is the comprehensive protection of the research ecosystem, which also encompasses the protection of national and economic interests” ²⁹
France	Research security is framed in terms of the protection of the nation's scientific and technical potential, specifically the most "sensitive" knowledge, expertise and technologies of public and private establishments (research laboratories, companies, etc.), the diversion or capture of which could: harm the economic and scientific interests of the nation; strengthen foreign military capabilities or weaken French defence capabilities; contribute to the proliferation of weapons of mass destruction and their means of delivery; or be used for terrorist purposes on national territory or abroad. ³⁰
Germany	Most documents do not use the term research security. For instance, the DFG guidelines talk about ‘risks in international research collaboration’. Because of the evolution of the debate this is part of the broader notion of ‘security-relevant research’, defined as “scientific work that has the potential to produce knowledge, products or technologies that can be misused by third parties to harm human dignity, life, health, freedom, property, the environment or peaceful co-existence”. ³¹
Italy	Definition as used in the European Council Recommendation. ³²
Netherlands	“...knowledge security refers primarily to preventing the undesirable transfer of sensitive knowledge and technology with negative implications for our national security and ability to innovate. It also involves covert activities aimed at influence and interference activities on the part of state actors within the context of higher education and science. Such foreign interference can lead to forms of censorship (including self-censorship), thereby resulting in the impairment of academic freedom. Finally, knowledge security concerns ethical issues relating to collaboration with individuals and institutions from countries in which fundamental rights are not respected”. ³³
Spain	Definition as used in the European Council Recommendation. ³⁴
Sweden	“Responsible internationalisation covers the aspects that a national actor in higher education, research and innovation needs to take into account in order to responsibly establish, nurture and follow up a relationship with one or more actors in other countries.” ³⁵
European Union	“‘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”. ³⁶

interchangeably, and each term comes with its own focuses, connotations, and subtleties than can hinder communication”.³⁷ We observed differences in emphasis, not least in Sweden’s focus on responsible internationalisation. At the same time, several interviewees said that, in practice, governments and research performing organisations recognised that they faced similar issues and were able to overcome these differences.

- **More mature systems tend to explicitly consider the balance between openness and research security.** Interviewees in those national research systems where research security has been a topic of attention for some time, such as the Netherlands and Germany (but also in our pilot interviews in the UK) tend to talk more directly about mitigating risks and balancing different goals and values for research, recognising that the blanket application of strict research security measures itself poses a direct or indirect risk to the quality, productivity, integrity and therefore the societal and economic value of the national research system.

3.2 Countries have similar perceptions of the research security threats that they face

- 
- Research security threats may result from the hostile activities of threat actors through foreign interference, scientific espionage, insider threats and cyberattacks.
 - Poor risk management practices of research performing organisations and individual researchers are also a source of research security threats.

We examined perceptions of research security threats. Many interviewees were cautious about discussing concrete examples of the threats faced by their institutions. Therefore, we supplemented our interviews with an analysis of public domain sources from government reports and the media.

3.2.1 Threat perspectives

- **There were similar views about the research security threats that countries face.** The perception of threats was similar to those of the UK.³⁸
- We identified two broad types of threats. First, **threats associated with hostile activities threatening research** through the direct or indirect efforts of a threat actor to interfere with research activities or access research or intellectual property. The second we characterise as **threats associated with poor practices of research performing organisations or individual researchers**. Figure 2 sets out our typology.

- **The emphasis placed on particular threats varied between countries.** Thus, foreign interference was a particular concern in the Czech Republic and cybersecurity has been a prominent issue in the Netherlands and Spain.
- **Threats to economic security and national security were treated in a similar way.** None of the countries in our study made a formal distinction between them in their research security policies and processes. The Czech Republic defines the primary goal of research security as the comprehensive protection of the research ecosystem, which also encompasses *the protection of national and economic interests*³⁹ (our emphasis). In France, the *Protection du Potentiel Scientifique et Technique de la Nation* (PPST) seeks to prevent the capture or misappropriation of sensitive knowledge, know-how and technologies regarding harm to national economic competitiveness as well as their potential to strengthen foreign military arsenals, proliferation of weapons of mass destruction and their means of delivery or contribution to terrorist acts at home or abroad.⁴⁰
- **Research security threats are not limited to STEM disciplines in the thinking of several countries.** Foreign interference in the social sciences and humanities is identified as a threat in some countries. This is addressed explicitly in the research security policies of the Czech Republic and Sweden. Likewise, Italy considers all subjects open to threat.⁴¹



Figure 2: Typology of research security threats

3.2.2 Research security threats may result from the hostile activities of threat actors

Our interviews and analysis of public domain sources lead us to characterise a series of threats stemming from the hostile activities of threat actors. Here threat actors, either directly or indirectly, aim to interfere with research operations or gain unauthorised access to research outputs and intellectual property. Table 4 describes four threats and provides examples. Figure 3 and Figure 4 identifies the threat vectors associated with each threat.

Foreign interference

Threat actors may seek to interfere with research priorities or academic discourse in several ways, including:

- **Use of funding or research grants as an interference mechanism.** We found few instances of universities who regarded themselves as over-dependent on specific foreign actors for research funding.⁴² However, there were concerns about funding being used as an interference mechanism. In the Czech Republic, Charles University faced a major crisis in 2019 related to covert funding by the Chinese Embassy of conferences at the Czech-China Centre at the university.⁴³
- **Direct interference by Chinese embassies and Confucius Institutes.** In France, a 2021 Senat Report highlighted the role of the Confucius Institutes and criticised the Chinese Embassy for its attempts to influence academic activity.⁴⁴ In Germany, there have been debates about the role of the Confucius Institutes in interfering with university activities.⁴⁵
- **The recruitment of key researchers through talent programmes, undisclosed dual employment or personal incentives from foreign entities** is another vector for foreign interference. The role of Chinese talent recruitment programmes, notably the Thousand Talents Plan, in actively targeting European academics have been widely discussed.⁴⁶ The Czech security service has reported the recruitment of academics via business social media platform LinkedIn to provide paid reports and provide a pretext for the development of deeper relationships.⁴⁷ In France, the security service has highlighted the case of a foreign company that had recruited a scientist to manage its French subsidiary and used his reputation and network to facilitate the recruitment of other researchers from the same research centre.⁴⁸

Table 4: Research security threats associated with the hostile activities of threat actors

Category	Threat description	Reported Example
Foreign interference	Covert or overt actions by foreign governments or entities to interfere with research priorities or institutional policies.	Covert funding by the Chinese Embassy of conferences at the Czech-China Centre at Charles University, Czech Republic. ⁴⁹
Scientific espionage by foreign actors	Unauthorised acquisition of research data, intellectual property, or emerging technologies by foreign intelligence agencies, corporations, or affiliated actors.	In Sweden, the security service has reported Russian state espionage as part of efforts to evade sanctions on particular technologies. ⁵⁰
Insider threats	Individuals within the institution (staff, researchers, students, or staff) who intentionally or unintentionally compromise security through unauthorised disclosures or conflicts of interest.	In Germany, a Russian scientist working at a German university was arrested for spying for Russia and receiving payments in exchange for information on his scientific research. ^{51 52}
Cyberattacks	Targeted hacking, phishing, malware, and ransomware attacks aimed at accessing research data or results.	In Spain, cyberattacks on research infrastructure at CSIC and INIA ^{53 54}

Scientific espionage by foreign actors

Another threat that was highlighted was targeted efforts by foreign governments, or other institutions, to steal research data, intellectual property or emerging technologies. This included such threat vectors as:

- **Unauthorised access to laboratories, covert access to data and the theft of intellectual property.** In France, there are concerns about the theft of intellectual property during and after the COVID pandemic. In Sweden, the security service has reported Russian state scientific espionage as part of efforts to evade sanctions on particular technologies.
- **The use of compromised foreign visiting researchers or students with undisclosed affiliations or intelligence ties.** In Germany, the role of the Confucius Institutes has been debated in this context.⁵⁵ In the Czech Republic, the security service has reported the role of Chinese students in gathering research and technology⁵⁶.
- **The use of obscured institutional ties.** In Germany, an agent of the Chinese intelligence service procured information on innovative technologies that could be used for military purposes, including using owners of a German company to enter a cooperation agreement with a German university for the transfer of science through their company.⁵⁷

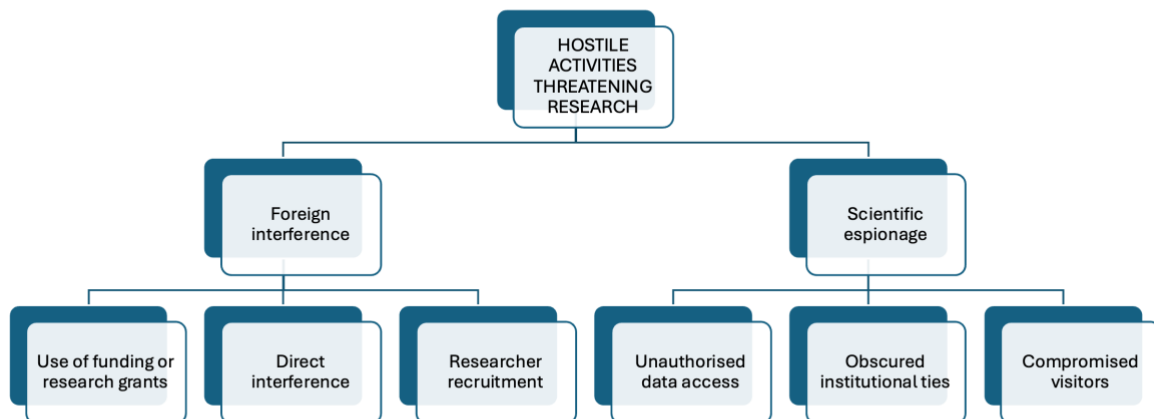


Figure 3: Hostile activities threatening research - foreign interference & scientific espionage

Insider threats

We also noted concerns about threat actors using insiders by coercing or incentivising them to gather research data or intellectual property. This may arise from foreign government pressure, financial incentives or the personal ideological alignment of the insider. “Insiders” may be university employees, foreign students, researchers or visitors.

- **Coerced or incentivised disclosure.** In Germany, a Russian scientist working at a German university was arrested for spying for Russia and sharing information about the European Ariane space rocket programme. He allegedly received 2,500 euros (£2,125) in cash in exchange for the information he shared, which also included details about his scientific research.⁵⁸ In the Netherlands, and other countries, there have been concerns about doctoral students funded under the China Scholarship Council.⁵⁹
- **Insider threats can also result from the coercion of foreign national researchers.** This may include the threat posed by foreign students some of whom may be coerced into inappropriate behaviours by pressures from their national governments, leveraging threats against their family, funding or themselves. This was mentioned as a concern by a Dutch university research security officer.^{60 61}
- **Undeclared foreign ties.** In France, the security service (DGSI) has issued several warnings about French nationals with covert foreign ties. A 2023 DGSI report provided the example of a foreign military university that initiated a formal partnership in fundamental research. After access was limited, it used its existing connections to facilitate informal collaborations in applied research that were not declared by the French scientists concerned.⁶²

Cyberattacks

The threat of hacking or data breaches is a common experience for all the universities that we interviewed. One recent survey of more than 100 academic leaders and funders found that 82% identified cyber security as a top priority, but only 45% felt well prepared to manage the risks.⁶³ In the Netherlands, a 2024 study found that cybersecurity maturity of universities had grown over the last 10 years but there are still persistent weaknesses.⁶⁴ Many research performing organisations that we interviewed reported significant efforts to improve their cybersecurity. Threat vectors that were mentioned include:

- **A lack of guidance/protocols for researchers travelling abroad for work, and how data/research can be accessed by various digital means.**⁶⁵
- **Phishing and credential theft.** Threats vectors such as social engineering, deceptive emails and compromised conference websites were mentioned as common means used in cyberattacks.
- **Cloud and network vulnerabilities** were another vector highlighted by some research performing organisations not least concerns about the complexity of cloud data server locations and the possibility that they might be in potentially hostile states.

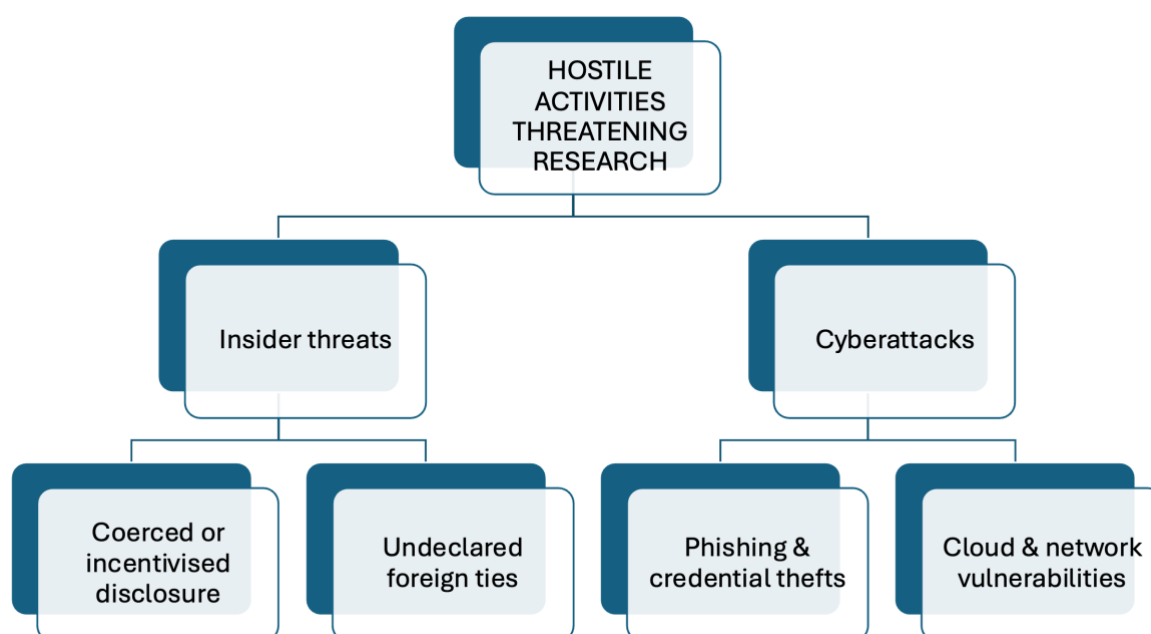


Figure 4: Hostile activities threatening research – insider threats & cyberattacks

3.2.3 Research security threats may also result from poor risk management practices

We also identified a series of research security threats that are the result of poor risk management practices of research performing organisations or individual researchers. Table 5

describes four threats and provides examples. Figure 5 and Figure 6 identify the threat vectors associated with each threat.

Collaboration with a foreign entity of concern

A significant threat that was highlighted to us was unintended collaboration with an foreign organisation that poses national security, ethical, or strategic risks due to its affiliations, activities, or government ties. There is widespread concern about European academic collaboration with the Chinese universities collectively known as the Seven Sons of National Defence.⁶⁶ In Sweden, several leading Swedish universities are said to have collaborated on hypersonic technologies with military institutions including the Chinese National University of Defence Technology (NUDT) and others who have close relationships with the People's Liberation Army and the Chinese military-industrial complex.⁶⁷ In France, the security service (DGSI) has warned of the danger that French institutions may unknowingly contribute to foreign military programmes, damaging their international reputation and scientific standing.⁶⁸ Here threat vectors include:

- **Failure to conduct appropriate due diligence** on the part of the research performing organisation.
- Researcher **lack of awareness or failure to comply** with organisational research security processes.
- **Hidden foreign ties.** At the same time, collaborations with a foreign entity of concern may arise because the ties to the foreign entity are hidden as a result of funding through intermediaries or failure of the foreign research collaborator to disclose institutional linkages. Universities expressed concern about the difficulty of identifying such intermediaries during the due diligence process.

Collaborator misuse of shared research

Another threat that was mentioned was unintentional misuse by a research partner of shared research, including repurposing for military applications, misattribution of research results or commercial exploitation, including patent filing without consent. In France, several interviewees from government and research performing organisations mentioned instances of loss of IP, including patent filing without consent. Threat vectors mentioned include:

- **The use of collaboration on one project to access data and knowledge from other** projects and sources due to poor project management and information security practices.
- **Repurposing of research for military or strategic use because of poorly structured research agreements** that lack contractual safeguards, where the research agreements are ambiguous or where dual-use technology applications are not recognised. In the Czech Republic, Interior Ministry officials have worked with universities to increase their awareness of intellectual property protection and provide advice on writing stronger contracts.

Table 5: Research security threats related to the poor risk management practices of organisations or individual researchers

Category	Threat description	Reported Example
Collaboration with a foreign entity of concern	Partnerships with institutions or researchers linked to foreign military, intelligence, or state-sponsored surveillance programmes.	Research collaboration with the Chinese “Seven Sons of National Defence”
Collaborator misuse of shared research	Intentional misuse of shared research, including repurposing for military applications or commercial exploitation without proper disclosure.	Commonly mentioned concern in all countries
Unintentional knowledge leakage	Unwitting transfer of knowledge or intellectual property due to poor data management, misunderstanding of open science policies, or insufficient awareness.	Subject of guidelines in the Czech Republic and Sweden.
Violations of export controls & sanctions	Non-compliance with international laws restricting the transfer of sensitive technologies, data, or expertise to sanctioned entities or in violation of export controls.	Compliance with sanctions following the Russian invasion of Ukraine has been a significant concern

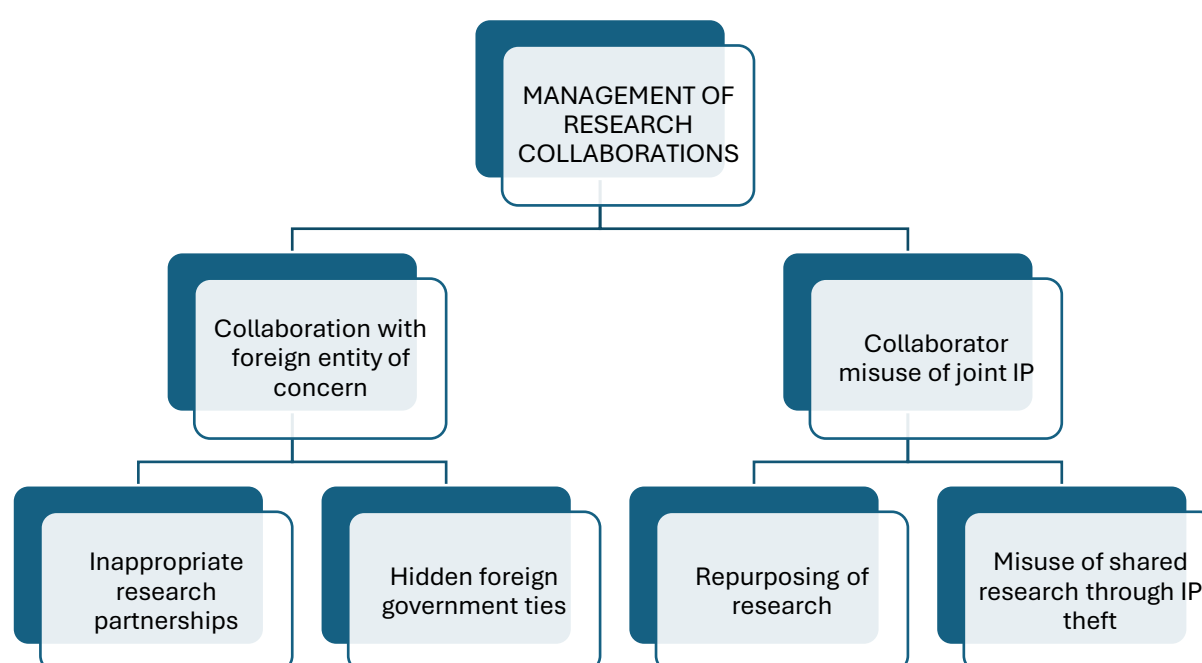


Figure 5: Poor risk management as a research security threat - collaboration with foreign entities of concern & collaborator misuse of joint IP

Unintentional knowledge leakage through collaboration

The unwitting leakage of data, knowledge or intellectual property as an unintended consequence of an international research collaboration was also identified as a threat with several associated threat vectors, including:

- **Poorly structured research collaborations or collaborations that ceded jurisdictional control to an organisation in a potentially hostile country.** This has been the subject of guidelines both in the Czech Republic and Sweden.
- **Foreign visits and presentations at foreign academic conferences.** These were widely recognised as a potential threat vector by governments and research performing organisations. Social engineering is another vector and the Czech security services have reported on foreign organisations using invitations to prominent academics for official visits followed by approaches by intelligence services.⁶⁹ In France, the DGSi has also highlighted the threats associated with travelling abroad, the need to use “burner” computer equipment dedicated to stays abroad, the need to limit the information taken on foreign visits and to maintain a posture of vigilance when interacting with “foreign interlocutors”.⁷⁰
- **Misunderstanding of good practice in open science.** Open science promotes transparency and accessibility in research through open data, publications, and collaboration. At the same time, it has also generated a debate about the potential tensions with research security and the appropriate balance between “as open as possible, as closed as necessary”. Mitigation strategies include a risk-based approach to openness, controlled access to sensitive data, and balancing open science with intellectual property protections.⁷¹
- **Poor research data management.** Negligence in handling data and research results is another threat through threat vectors such as poor awareness of data security issues and unsatisfactory data management practices. Many research performing organisations in our case study countries reported that they had invested considerable time and effort in strengthening research data management awareness and practice. However, there is some way to go, and this is a vector for unintentional knowledge leakage. For example, a Swedish National Audit Office report concluded that higher education institutions do not have effective information security to manage research data that requires protection. The NAO observed that higher education institutions often lack knowledge both about which data needs protecting and how it should be protected.⁷²

Violations of export controls and sanctions

Research collaboration that unintentionally violates export controls, sanctions regimes or international non-proliferation treaties is another threat associated with poor risk management. Threat vectors that we identified include:

- **A lack of export control processes, governance and researcher awareness leading to unauthorised collaborations.**
- **Failure to vet foreign partners and conduct satisfactory due diligence.**
- **Unintentional export through lack of compliance training, misclassification of research or intangible transfer of knowledge through conversations, emails and conference presentations.**

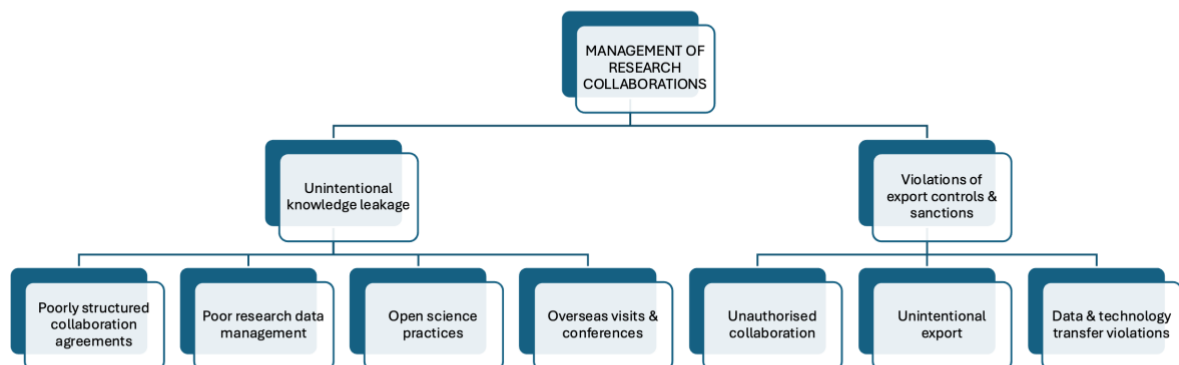


Figure 6: Poor risk management as a research security threat - unintentional knowledge leakage & violations of export controls & sanctions

3.2.4 Policies are state agnostic, but the same state threat actors are highlighted

Policies and processes in all the countries that we studied are in principle state agnostic. However, China, Russia and Iran are identified in official statements from security agencies in Sweden and the Czech Republic, and in the broader discourse around the need for research security in most of the countries that we studied.⁷³ The primary actors of concern are states, but some countries identify terrorist organisations (e.g. French PPST) and organised crime and smuggling networks.^{74 75}

3.3 Responses to research security threats differ between countries & within countries

- Research systems are at very different stages of maturity in their response to research security challenges.
- There is a diversity of policy and practice *between* research systems.
- There is a diversity of policy and practice *within* research systems.

In the previous section, we sought to understand the perceptions of research threats, threat vectors and threat actors in the countries that we studied. In this section, we will examine the research security policies and practices that are being introduced in each country and at the EU level, in response to those threats.⁷⁶

3.3.1 There is diversity of policy & practice between research systems

We developed a simple three-stage model to characterise the maturity of research security policies and practices in each country. We examined public policy and the practices of research performing organisations in terms of awareness, risk management and due diligence, and capacity.

Stage 1: Realisation

During the realisation stage, research security emerges on to the policy agenda of the government and sector. Responses to risk by government and research performing organisations are largely ad hoc and capacity is limited.

We characterise two of the study countries as being at the realisation stage. **Spain** is at a very early stage of awareness and lacks formal guidance on research security. The European Council Recommendation (2024) has led government and some universities to begin consideration of research security policies and practices. Some universities have processes in place for export control and feel that they are ahead of their governments with respect to research security policies.⁷⁷ **Italy** has begun developing policies at national level. Italy's Presidency of the G7 combined with the European Council Recommendation (2024) appear to have stimulated Italian work on research security. Government is consulting universities with a view to introducing a pilot scheme for research security in selected universities in 2026.

The realisation stage can be characterised as follows:

- **Awareness is rising:** There is rising awareness of research security issues and increased pressure on government to respond. There is limited attention to research security threats in the research system beyond the intelligence and defence communities and no coordinated strategy for research security. There is growing interest in international practice.
- **Risk management and due diligence processes are ad hoc:** There are few or no national or sector-led policies guiding universities and research institutions on research security. Due diligence or risk assessment frameworks for international collaborations or foreign funding are ad hoc. Institutions rely on voluntary compliance or react to risks as they emerge.
- **Capacity is limited:** There is uncertainty about roles and responsibilities within the research system. There is limited knowledge and expertise among policymakers and research administrators on research security. Some institutions may have some capacity for research security, others do not.

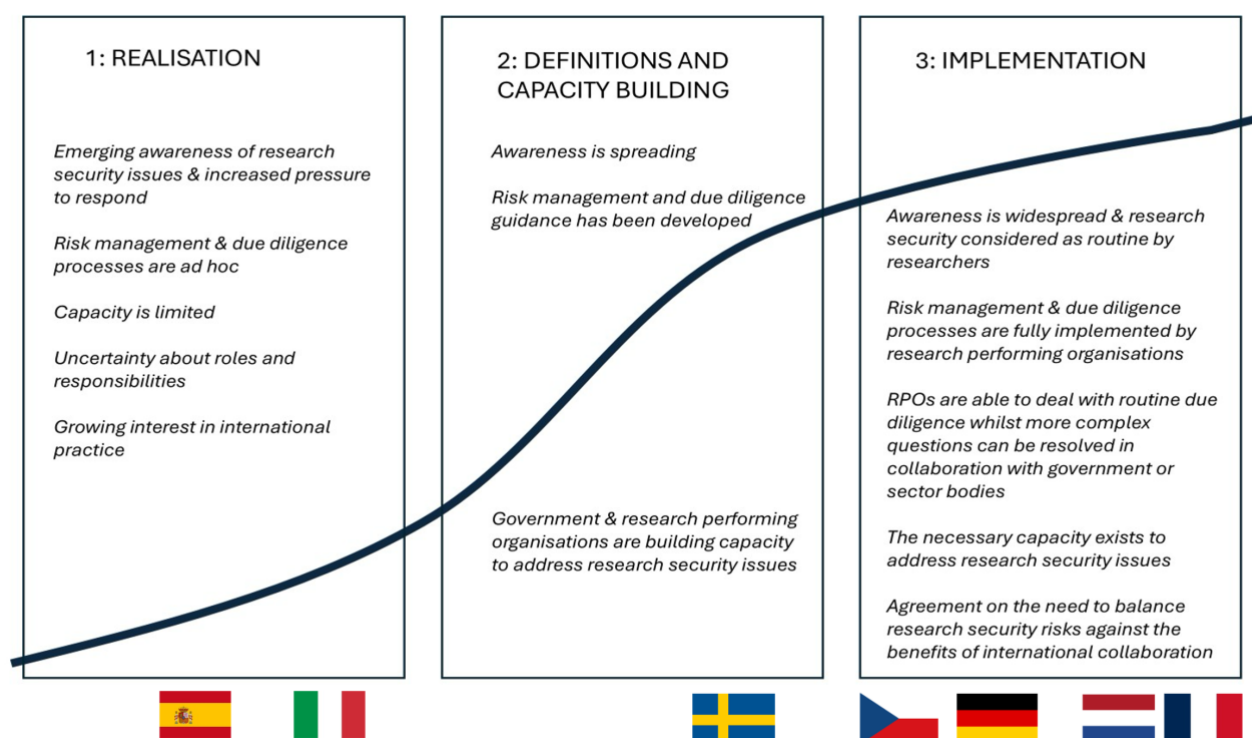


Figure 8: Stylised maturity curve for national research security policies and practices

Stage 2: Definitions and capacity building

During the definitions and capacity building stage, a national research security framework begins to take shape. Awareness of research security issues becomes more widespread in government

and research performing organisations and a broadly agreed conceptualisation of research security emerges (although this may be contested by some organisations). Formal guidance emerges and there are efforts focused on building capacity.

We characterise **Sweden** as being at the definitions and capacity building stage. In 2024, the government asked the Swedish Council for Higher Education, the Swedish Research Council and Vinnova to undertake an assignment to develop national guidelines on responsible internationalisation and make recommendations for a national support function for responsible internationalisation. The assignment submitted two reports that are being considered by the Minister for Education and Research. Draft guidelines on responsible internationalisation have been published that are focused on research security policies and practices.⁷⁸ Recommendations have also been published for a support structure that may include a central advice function.⁷⁹ This builds on existing sector-led activity focused on responsible internationalisation and the development of university processes and capacity in response to the requirements for protective security measures contained in the Protective Security Act (2021).⁸⁰

The definitions and capacity building stage has certain features, as follows:

- **Awareness is spreading:** Government recognises research security as a policy priority and establishes official guidance. There is increased engagement between research institutions, funding bodies and intelligence agencies. Government, sector bodies or individual institutions may undertake targeted awareness campaigns on research security risks in international research collaboration.
- **Risk management and due diligence guidance has been developed:** Written guidance on research security and due diligence is developed by sector bodies or co-created with government. Sector-wide risk assessment tools may be developed to help institutions evaluate research security risks. Sector bodies share good practice.
- **Government and research performing organisations are building capacity to address research security issues:** Government may establish an inter-departmental body to coordinate policy. Research institutions develop their internal research security capabilities, appointing research security officers, establishing risk management and due diligence processes and conducting training programmes for researchers and administrative staff.

Stage 3: Implementation

During the implementation stage, research security becomes embedded within the national research system with proactive risk management and better mutual understanding of goals and values on the part of government and research actors. There is agreement on the need to balance the risks of knowledge leakage against the benefits of international collaboration. Awareness of research security is widespread across government and research performing organisations, risk management and due diligence processes are regarded as standard practice, and the necessary capacity exists for research issues to be addressed by government and research performing organisations.

We characterise several of our study countries as being at the implementation stage. **France** and **the Netherlands** have relatively mature policies, guidelines and processes that have been adopted to a greater or lesser extent by research performing organisations.^{81 82} The **Czech**

Republic and Germany have developed detailed policies, guidance and processes and are at the beginning of the implementation stage.^{83 84}

The main features of the implementation stage are as follows:

- **Awareness is widespread:** Within government, research security is integrated into national science, technology, and innovation (STI) policy and practice. The research community has well developed awareness of research security as a consideration in international research collaboration.
- **Risk management and due diligence processes are fully implemented by research performing organisations:** Risk management and due diligence is standard practice and is proportionate to the potential risk.
- **The necessary capacity exists to address research security issues:** Government has the capacity to advise research performing organisations on complex issues and this may include a national advice team with dedicated resources and cross-sectoral coordination mechanisms. Research performing organisations have dedicated research security offices that can deal with routine risk management and due diligence whilst more complex questions can be resolved in collaboration with government or sector bodies.
- **Research security is considered in the context of the benefits of open international scientific collaboration.** The countries and organisations where we see the most sophisticated responses to perceived research security risks, also tend to be clearest about the need to balance research security concerns against the social and economic benefits of participating in open science. This is encapsulated by the concept of ‘responsible internationalisation’, which can be seen as part of the fundamental question of ensuring responsibility and integrity in research.

3.3.2 There is diversity of practice within research systems

We also found that research performing organisations *within* research systems are adopting research security policies and practices at different rates.

Most countries have a core of universities and research institutes with mature research security practices and a tail with less developed practices

- **The core** comprises universities and public research institutes whose research security practices met or exceeded those of UK peer institutions. These were often technical universities or public research institutes at the more applied and technological end of publicly funded research.
- **Some research performing organisations have been proactive in the development of research security policies, practices and capacity.** The activity of some organisations has been ahead of government policy in some countries. In Sweden, universities like KTH, Lund, the Karolinska Institutet and Uppsala have strong senior leadership direction, resourcing of substantial capacity, well developed processes for risk management, due diligence and risk mitigation as well as significant efforts to promote awareness amongst research and administrative staff. In Germany, the Helmholtz Association and the Fraunhofer Society are seen as leaders in research security, the former because of the work of the DLR Project Management

Agency in formulating guidelines and promoting awareness, and the latter because of its predominantly applied orientation.

- **Some organisations have been reactive.** The response of these organisations may have been because of a lack of senior leadership attention, concerns about resources and capacity or because they do not believe that their research activities are of interest to hostile actors. Some organisations have only responded to specific government or research funder requirements or after suffering reputational damage due to highly publicised incidents – e.g. inappropriate research collaborations with organisations or researchers engaged with the military-scientific complex of a potentially hostile foreign country.
- **Every country had a “tail” of research performing organisations with less mature practices.** Typically, these were smaller universities or institutes with a focus on basic research, little or no engineering or technological development activities and/or limited international collaboration. They often find the costs of research security measures prohibitive.

Research funders recognise research security as an issue, but many are yet to put processes in place.

- **Funding criteria rarely include research security requirements.** We found few examples of research funders changing their funding criteria in ways like UK Research and Innovation (UKRI).⁸⁵
- **The European Council’s Recommendation is influencing thinking.** Some research funders are considering introducing requirements for awareness of research security to be included in the application process and the European Council Recommendation includes that Member States should engage with research funding organisations to develop procedures to assess research security risks. The most significant likely development is the inclusion of such requirements in the European Union Horizon/FP 10 programme. Whilst how and when this will be done is unclear, anticipation of such developments is already driving behavioural and process change amongst some policy makers and research performing organisations. For example, the potential inclusion of such requirements is explicitly emphasised in the Czech Methodologies documents.⁸⁶
- **Some research funders regarded research security as an issue that should be addressed primarily by research performing organisations and individual researchers.** At the same time, research funders are increasingly aware of research security as an issue and the implications of the European Council’s Recommendation.
- **Many research funders expressed concerns about capacity constraints.** Several research funders said that they were anxious about the capacity implications should they begin to assess research security risks in research proposals. Both funders and other research system actors expressed concerns that funders lacked insight on security threats, and funders also worried about the consequences for the peer of research proposals, not least the availability of appropriately qualified peer reviewers with knowledge of research security issues.

Public research institutes are often ahead of universities in terms of their awareness and implementation of research security practices

Public research institutes are diverse in their activities, size and position in national research systems. Accordingly, generalising across all research institutes is problematic. Nonetheless, we found that public research institutes are often ahead of universities in terms of their awareness of research security and implementation of research security practices. There are several reasons for the difference between public research institutes and universities:

- Public research institutes often focus on fields of research where research security has traditionally been an issue (e.g. aerospace or nuclear) or where research security concerns are clear (e.g. quantum).
- Public research institutes often engage in activities at higher Technology Readiness Levels (TRLs) than those typical for university research. Thus, constraints on open science such as intellectual property protection and commercial confidentiality, but also physical and cybersecurity, may be more familiar and accepted.
- Public research institutes are often part of a larger network or organisation with strong central governance and the ability to pool capacity and support.
- Public research institutes often have a close relationship with government, including providing science for policy advice, and this means that they have a greater awareness of research security issues. Public research institutes often receive funding directly from government ministries, national research agencies, or industry collaborations. By contrast, universities are characterised by a funding mix of government grants, tuition fees, and competitive research grants and typically have greater autonomy in setting their research agendas.
- Public research institutes often have a clear focus on applied research, on strategic national priorities, or on a mission of long-term scientific advancement in a particular discipline or field, or work on government-funded or industry-partnered projects with clear policy, economic, or societal impacts. In contrast, universities combine broad research and education missions, the research is investigator-driven and spans a wide range of disciplines.

3.4 A variety of factors are influencing responses

In the previous sections, we observed the differences in policy responses and the adoption of research security practices between and within research systems. Naturally, this leads to the question of what factors lead to these differences. To address this question, we examined the factors influencing governments and research performing organisations. We identified different governance models for the development of research security policies and practices.

We found that the factors influencing policy responses can be considered as the interaction of driving forces and restraining forces. These may influence the behaviours of government or research performing organisations (or both) and they are summarised in Figure 8 below. The remainder of this section expands on each of these points.

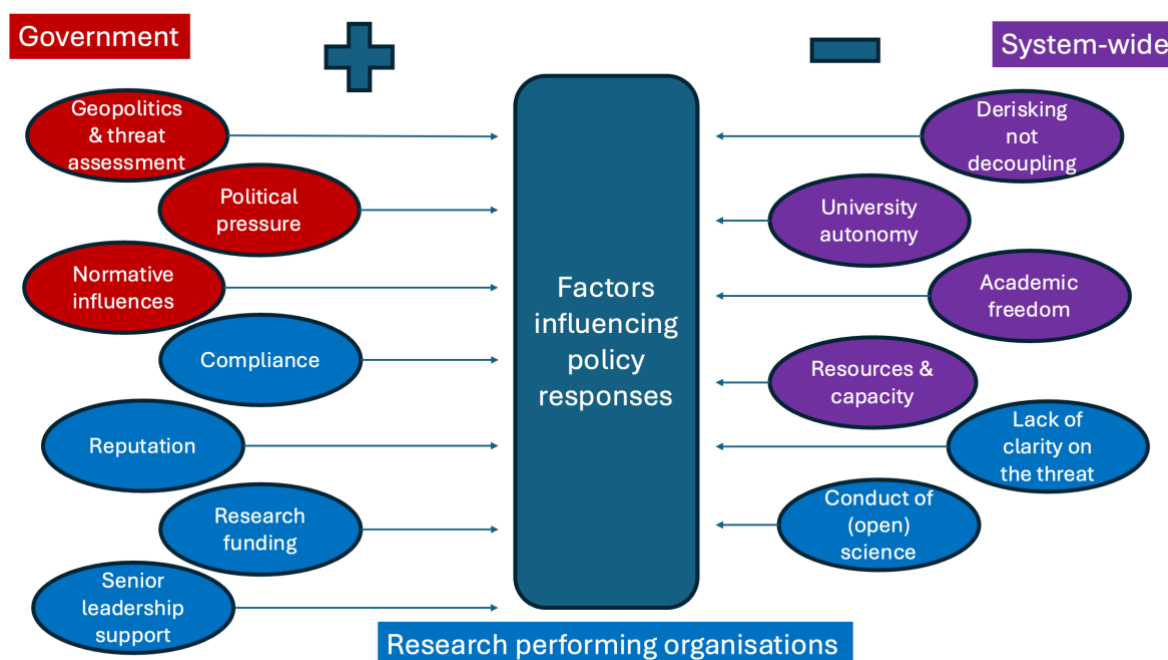


Figure 8: Factors influencing policy responses

3.4.1 Factors driving research security responses

We identified a range of factors that influenced the policy responses of governments and research performing organisations.

Factors driving governments to introduce research security policies

- **Geopolitical change and threat perceptions:** An important factor drawing attention to the issue is the inclusion of elements of research security in national security strategies and threat assessments by defence or security bodies. Several security services have explicitly addressed the national and economic security threats posed by scientific espionage.⁸⁷ The National Security Strategy of the Czech Republic notes a variety of research security threats.⁸⁸
- In many countries there is a widespread **feeling that a turning point has been reached in global affairs and relations that requires a change in attitude** to research security. For instance, in Germany the federal science ministry (BMBF) talks about a turning point (Zeitenwende) in terms of geopolitical and technological relations symbolised by the Russian invasion of Ukraine and the recognition of China as a systemic rival. This is said to require new responses including a more strategic and considered approach to research security.⁸⁹ The Russian invasion of Ukraine has had a similar impact on thinking in Sweden, expressed most dramatically by its decision to join NATO.
- Recognition of a geopolitical turning point has been accompanied by **a new preoccupation with the military and defence dimensions of national security**, and several governments are seeking to strengthen civil-military research relationships and reconsider restrictions on military-related research, such as the ‘civil clause’ present in the statutes of more than 70 German universities⁹⁰. Sweden is expecting universities to become more directly engaged in its “total

defence” and VINNOVA has launched a research programme to encourage civil (university) research engagement in defence technologies.⁹¹ There has also been discussion about the introduction of dual-use research into the European Union framework programme.⁹² These developments are likely to heighten the demands on research security in universities and public research institutes.⁹³

- **Domestic political pressure:** In most countries, the recognition of a geopolitical turning point has both accompanied and been partly driven by growing domestic political pressure on policymakers. Politicians, think tanks and the media have paid growing attention to risks or actual incidents associated with international research collaboration. Examples here are critical commentary on collaborative research with institutions affiliated with the Chinese military as well as broader perceived threats posed by the Confucius Institutes or other aspects of China’s international influence operations.⁹⁴
- **Normative influences from other governments and multinational organisations:** We found that the thinking of some policy makers has been influenced by initiatives undertaken by the G7, OECD and particularly the European Union. The policies and practices of other countries have influenced policy development, not least the US, UK, the Netherlands, Canada and Australia. Several policy makers noted that initiatives by the UK Government’s Science & Technology Network⁹⁵ and various US organisations have contributed to awareness raising and learning.⁹⁶

Factors driving research performing organisations to adopt research security policies and practices

- **Compliance:** We found that compliance with legal requirements, not least export controls and sanctions regimes, was a powerful factor in the adoption of research security practices.⁹⁷ University rectors and the directors of public research institutes also felt themselves under direct or indirect pressure from government to adhere to non-statutory guidance.⁹⁸
- **Reputation:** The reputational consequences of public disclosure of research security incidents or controversial relationships with foreign research organisations was an important consideration. Many respondents recognised the potential severity of the national security consequences of a research security incident that infringed export controls, arms control treaties or sanctions regimes. However, the most common concern amongst universities in particular was reputational risk, unfavourable media and political attention and the potential consequences for research partnerships, especially with business.⁹⁹
- **Actual or anticipated research funder requirements:** We found that the demands of research funders had a very significant impact on the behaviours of research performing organisations and individual researchers. The anticipated introduction of research security requirements into the European Union Framework Programme is already influencing behaviours. The actual or anticipated future requirements of U.S. funders are important, not least the National Institutes of Health and the Department of Defense.¹⁰⁰ Those research performing organisations who received funding from industry emphasised that this generated significant requirements to demonstrate research security practices for IP protection. Growing defence and dual-use research funding is also driving the adoption of strengthened research security practices.
- **Senior leadership support:** We interviewed research security officers and administrators in a range of research performing organisations. They all agreed about the importance of senior leadership support in the adoption of research security practices. They said that senior

leadership support was crucial because it helped establish clear priorities, ensured resource allocation and supported a culture of compliance.¹⁰¹

3.4.2 Factors restraining research security responses

System-wide factors restraining responses

We identified several factors that were common restraining forces for government and research performing organisations as follows:

- **The relative importance of international research collaboration to the national research system influences attitudes and responses to research security.** In those smaller research systems with greater need to look abroad for collaboration, this may have a moderating effect on research security policies (for example, Sweden). However, the extent of the trade-off here may be perceived differently within government (for instance between ministries of education/ research/ science, foreign ministries and security agencies) and between government bodies and research system actors.
- **The need for derisking not decoupling:** Across research systems, there is a recognition of the importance of international research collaboration and a concern that overregulation may have a chilling-effect on that collaboration. All the government officials that we spoke to made clear that they wished to engage in a de-risking rather than de-coupling strategy. This was in recognition of the importance to remain competitive for the best staff and students and at the global leading edge of research. Indeed, in the systems where we see the most sophisticated responses to perceived research security risks we generally see the clearest recognition of the need to balance research security concerns against the social and economic benefits of participating in open international scientific collaboration.
- **There is a concern about the risk appetite of research performing organisations.** Research performing organisations are increasingly cautious about entering international research collaborations where risks have been identified. This potential for an unintended and risky chilling effect of research security measures is seen in part to be a function of asymmetric knowledge. Research performing organisations feel that they are given insufficient information from security services to make informed judgements (and some of our policy-maker interviewees shared this concern) and this may be having a chilling-effect on international research collaboration. For example, in Italy, the Ministry of Universities and Research (MUR) is leading the development of an “Italian Model” that will cover both safety and integrity of research, but concerns exist that the proposed approach will place too high a level of responsibility upon principal investigators who will not have the information they need to make a reliable judgement of risk.¹⁰²
- **Academic freedom and institutional autonomy:** Several of the countries that we studied have constitutional or other legal provisions regarding academic freedom or institutional autonomy. This has contributed to governments in Germany, the Netherlands and Sweden preferring to leave many of the decisions on research security to the researchers themselves within the requirements of the law. In Spain too this is likely to be a factor, although as in Germany, this has to be balanced against the civil servant status of public researchers and university academics. Research performing organisations also face pressure from their own staff and students and obligations to their own statutes, values and ethical positions.

- **Resources and capacity:** Research performing organisations must build the internal capacity to develop institutional research security policies, develop risk management and due diligence processes, appoint research security officers, and promote awareness of research security amongst researchers and administrative staff. All this capacity has typically to be built within the limits of existing funding and in a labour market where there is a scarcity of individuals with knowledge of research security or export controls. Governments face similar capacity constraints as research security places increasing demands on ministries and security agencies. For example, the French government has experienced capacity constraints in its process for establishing protective security zones (ZRRs) and reviewing proposals for international research collaborations because of a lack of reviewer knowledge in emerging technologies like AI and quantum.

Restraining factors for research performing organisations

- **Lack of clarity regarding the threat:** Many universities and sector organisations observed that they were being expected to invest in capacity and manage risk with insufficient information about the nature, source and severity of threats. We asked research officers, administrators and rectors about the threat. Universities found it difficult to assess their vulnerability to a research security incident and many respondents from universities noted that they did not have sufficiently detailed and clear assessments of risk or threat vectors from government or security services.
- **Research performing organisations in most of our case study countries are looking to governments, sector bodies, or their international networks, for clearer insights as to potential sources of risk, and for case studies to illustrate those risks.** In France and the Netherlands there are centralised sources of advice and Germany and Sweden are considering this as well.¹⁰³ In large national research organisations or networks/societies such as the German Max Planck, Helmholtz or Fraunhofer, it may be easier to provide central guidance and support. In some cases, pan-sector bodies are pulling together commonly developed guidelines, training and resources, or are pointing to commercial providers of intelligence for due diligence. For instance, in Germany the HRK is developing an audit service for universities to receive advice about their research security measures and processes, whilst the DAAD, the German academic exchange service, has developed a competence centre for international co-operation, KIWi, which offers guidelines, targeted advice and support to member organisations on knowledge security.
- **Concerns about the implications for the conduct of (open) science.** Many sector organisations, university rectors and research administrators expressed concerns about the actual or potential impact of research security measures on the conduct of science. They worried about the chilling-effect on international research collaboration and the imposition of “bureaucratic burdens” on researchers. Concerns were expressed about tensions between research security concerns and the movement towards open science, with its emphasis on transparency, collaboration, and unrestricted access to research data and findings. It is worth noting that most of our policy maker interviewees also raised, understood and accepted such concerns.

3.5 Differing governance models have emerged in response to these factors

The interaction of these factors has led to the emergence of different governance models for the development of research security policies amongst the study countries, and we can characterise those governance models as follows:

- **Laissez-faire:** There is minimal government or sector attention given to research sector issues. Some research performing organisations have introduced research security measures on their own initiative but there is no consistency of response across the research system and no government initiatives. (e.g. Spain and Italy until 2024).
- **Sector-led:** Research security initiatives are led by the sector with the encouragement of government. Research performing organisations and sector bodies such as national rectors' conferences develop the research system's approach to research security, including the publication of guidance documents, relying on self-regulation and voluntary initiatives and leveraging sector expertise on international research collaboration. (e.g. Sweden until 2023; Germany today).
- **Collaborative approach:** Government works with research performing organisations and their representative bodies to develop and implement research security policies and processes. There is an emphasis on partnership, shared responsibility, and consensus-building (e.g. Czech Republic; Italy today; the Netherlands; Sweden today).
- **Top-down:** This hierarchical approach involves decisions being made by a central authority and imposed on lower levels. It is characterised by strong control, clear command structures, and centralised policy implementation with criminal penalties.¹⁰⁴ France follows this governance model.

3.6 The focus is turning to capacity building & adoption of good practice

- The focus of research security policy is moving from awareness raising to capacity building.
- Awareness of research security threats and practices has grown.
- Risk management practices are being put in place, but no country has institutionalised those practices across its whole research system
- Resources allocated to research security measures vary considerably.
- The cost of research security measures is a significant concern for the leadership of some research performing organisations.
- Capacity is a major concern across the sector.

Our assessment of the current state of play amongst the countries is as follows:

- **Awareness of research security threats and practices has grown.** Most governments and research performing organisations are now aware of research security, not least because of the 2024 European Council Recommendation. There is scope for further awareness raising, especially in countries who are at the early stage in their development of research security policy and practice. There is also scope for awareness raising amongst the tail of research performing organisations in each country who are less engaged with research security.
- **The focus of research security policy is moving from awareness raising to capacity building.** The focus of research security policy and practice in Europe is moving from awareness raising to capacity building with the aim of broadening the adoption of good practice across the research system. There is recognition of the need to increase capacity for risk management, due diligence and export control compliance but this is challenging due to resource constraints, a lack of suitably skilled individuals and limited training programmes.
- **Resources allocated to research security measures by research performing organisations vary considerably.** Some leading universities, especially technical universities, have made significant investments in personnel, processes and awareness raising activities. In others, research activities are ad hoc, responsibility is distributed across a variety of functions and the number of dedicated staff is limited.
- **The cost of research security measures is a significant concern for the leadership of some research performing organisations.** In the Czech Republic, the government has allocated some funding through the EU Cohesion Fund for research performing organisations to develop research security activities, especially awareness raising and training. Likewise, in Sweden, funding has been made available as part of the government assignment on responsible internationalisation to support university development of research security measures. The support function is initially proposed to be financed with SEK 7 million annually (£520,000). The recommendations note that this should also allow for the funding of awareness raising and training activities by research funders and universities.
- **Capacity is also a major concern across the sector.** Universities noted that individuals with the necessary skills to support research security (especially knowledge of export controls) were in short supply and that they were in competition with government and the private sector for suitably skilled individuals. Some universities in Sweden and the Czech Republic are seeking to share resources as a way of reducing costs, especially where the scale or character of the international activity of the university does not merit dedicated resources. In France, even where there is an established system that is of long-standing, it was acknowledged that there may be a shortage of personnel to fill institutional roles in research performing organisations and in central government.¹⁰⁵ In Italy it is thought likely that there will be capacity constraints in filling emerging security roles in universities.^{106 107}

4. NON-LEGISLATIVE RESEARCH SECURITY MEASURES

- A variety of approaches are being used to promote awareness & create forums for dialogue between government, security agencies and research performers.
- A range of written guidance exists on research security.
- Central advice teams for information sharing by government exist in only a few countries.
- Some but not all research performing organisations have mature risk management and due diligence processes.
- Some countries provide public funding for capacity building.

This section considers the measures being adopted by our study countries to address perceived research security risks. Specifically, we examine non-legislative measures focused on increasing awareness, providing written guidance on good practice in research security, government advice teams and the risk management and due diligence processes used by research performing organisations. These non-legislative research security measures are summarised in Table 6 (below). In Section 5 we will examine legislative measures.

4.1 Various means are being used to promote awareness & create forums for dialogue

- **There are many examples of awareness raising activities.** Awareness raising activities include workshops and training activities led by government security agencies, research sector organisations or individual research-performing organisations. In France, the security service (DGSi) offers awareness raising workshops that explain threats, threat vectors and good risk management practice. The Czech government is funding activities aimed at promoting awareness through training of researchers and administrators. The Helmholtz in Germany has undertaken training and awareness raising and provided funding for small scale projects. In Sweden, the government assignment has included the funding of small-scale projects to promote awareness raising in universities. We did not find any examples of communication campaigns equivalent to the UK's Trusted Research Campaign.

Table 6: Non-legislative research security measures

Country	Awareness raising & forums	Written guidance	Government advice	Risk management & due diligence
Czech Republic	Seed funding of awareness activities Interdepartmental Working Group for Combating Illegitimate Interference	Methodologies documents	Informal	Guidance in place Practice limited by capacity & awareness
France	Through the HFDS in ministries & network of FDNs DGSi awareness raising workshops & monthly Economic Interference bulletin	Le dispositif de protection du potentiel scientifique et technique de la nation – Foire aux questions	Formal through the SGDSN, HFDS in ministries & network of FDNs	Centralised
Germany	Through the DFG-Leopoldina joint committee, the DAAD and HRK for universities Through the umbrella associations and societies for public research institutes	DFG-Leopoldina Joint Committee guidelines HRK guidelines on international co-operation. DAAD KiWi www.safeguarding-science.eu	Continued debate about the need for a central team	Decentralised
Italy	Government consultation Work of Italian Association of Research Managers	Very limited guidance present in organisations	Subject of government consultation	Ad hoc and variable, small number of more advanced universities
The Netherlands	UNL, KNAW, NWO, NFI, TO2 and the Ministry AWTI	2022 National Guidelines	National Contact Point for Knowledge Security	Centralised advice and support (NCP) but decision at the institutional level
Spain	Limited/none	None	Informal/none	None
Sweden	Seed corn funding for awareness raising Government is considering recommendations for a national support function	2024 proposed guidelines on responsible internationalisation 2024 Rectors conference guidelines 2020 & 2022 STINT guidelines	Government is considering recommendations for a national support function	Leading universities have mature risk management & due diligence processes

European Union	Dialogue through the ERA Biennial Conference on Research Security	Council Recommendation Staff Working document	Proposal for a Centre of Expertise	Guidance through Council Recommendation & Staff Working document
----------------	--	--	------------------------------------	--

- **Some security services communicate research security related threats.** In France, the DGSI publishes a monthly “Economic Interference Flash”, in which it provides guidance based on real cases of interference.¹⁰⁸ Since 2021, the DGSI has devoted one edition per year to foreign threats to academic research. The publications can be consulted on the DGSI website and on its LinkedIn page.^{109 110} The Czech security service has included university research risks in its annual reports.¹¹¹ Likewise, the Swedish security service discusses research security related threats in its annual report.¹¹²
- **There are some international initiatives aimed at information sharing.** The G7 has established its Virtual Academy and the OECD’s STIP Compass has collated policy documents from OECD members. However, neither of these initiatives were mentioned during our interviews, except to criticise their accessibility and currency. The European Council’s Recommendation includes a proposal for a repository of documents as part of the proposed Centre of Expertise.
- **Some countries have promoted awareness raising activities as part of wider science diplomacy.** The UK government’s Science & Technology Network (STN) has sponsored study visits for delegations from several countries, including the Czech Republic and Sweden. These were seen as highly valuable by participants, as was the STN sponsored virtual workshop series organised by the UK’s Association of Research Managers & Administrators (ARMA).^{113 114} Under the Biden administration, the United States sponsored awareness raising activities in several countries, with a particular focus on Central & Eastern Europe. At the time of writing, the future of such initiatives was unclear.
- **Some countries have established forums for dialogue between actors within the sector.** German research organisations have facilitated information sharing through forums. In the Czech Republic, the Ministry of Education, Youth, and Sports established a platform called the Interdepartmental Working Group for Combating Illegitimate Interference in Higher Education and Research comprising government departments, the Academy of Sciences and universities. The Interdepartmental Working Group has played a key role in promoting dialogue within government and across the sector and was key to the development of the Czech Methodologies documents.¹¹⁵ Sweden has lacked a forum for dialogue between government, research funders and research performing organisations. This is addressed by the government assignment and its proposed support function. Amongst the roles of the proposed support function would be to provide meeting places by facilitating and hosting physical and digital meetings where higher-education institutions and other actors can share experiences.¹¹⁶

4.2 A range of written guidance exists

- **There is an extensive catalogue of written guidance on research security available to governments and research performing organisations.** Table 7 provides a list of some of those guidance documents.
- There are three types of guidance:
 - **Sector-led:** For countries like Germany and Sweden, the guidance on research security and due diligence has been sector-led for instance by the DLR Project Management Agency or DFG in Germany, or by the STINT foundation (with leading universities) and the Swedish Rector's Conference in Sweden.
 - **Co-produced:** the Czech Republic's Methodologies documents were co-produced by the Interdepartmental Working Group which is comprised of government departments, universities and the Academy of Sciences. The Netherlands national guidelines were also developed in collaboration between research system actors including the universities association and national academies, and the government.
 - **Government-led:** In France, government produced guidance on the application of the PPST which represents a detailed explanation of the implementation of the law.
- There is also **multilateral guidance** from the G7 and European Union.
- **Several research managers said that the volume of national and international guidance was confusing.** They called for simpler, more digestible and quality assured guidance and expressed the view that standardised guidance would help collaboration within and between countries.¹¹⁷

Table 7: Examples of written guidance on research security

Title	Author	Content
Responsible Internationalisation	STINT, Sweden (2020, 2022)	2022 has a more explicit focus on research security
Staff Working Document on Tackling R&I Interference	European Commission (2022)	Guidance on values; governance; partnerships; and cybersecurity
Methodologies Documents	Interdepartmental Working Group for Combating Illegitimate Interference, The Czech Republic (2024)	3 documents on rationales for research security policy; conducting due diligence; institutional issues
Council Recommendation for Enhancing Research Security	European Union (2024)	Recommendation for actions by Member States and the European Commission ¹¹⁸
Le dispositif de protection du potentiel scientifique et technique de la nation – Foire aux questions	General Secretariat [of the French Government] for Defence National Security [SGDSN].	Widespread guidance on the PPST, purpose & implementation

4.3 Central advice teams exist in some countries

- The Netherlands & France have central advice teams that provide research performing organisations with a formal means of seeking advice from government and security agencies.
- Each central advice team has unique features, but they play a similar role to the UK government's Research Collaboration Advice Team (RCAT).
- Sweden and Germany are considering the creation of similar functions.

- **In France, there is a centralised system of guidance for research performing organisations.** This is provided by the Secrétariat général de la défense et de la sécurité nationale (SGDSN). The SGDSN has an officer in each ministry, called the Senior Defence and Security Officer (HFDS). Six ministries have an HFDS, these are: agriculture, defence, the economy, ecology, research and health. The HFDS provides guidance directly and via a network of Fonctionnaires de Sécurité de Défense (FSDs) located in research performing organisations.
- **The Netherlands has the National Contact Point for Knowledge Security.** This is a collaboration between different Dutch ministries and offers help to anyone connected to a knowledge institution with questions about opportunities, risks and practical matters concerning international cooperation.
- **The Swedish government is considering recommendations for a national support function.** The proposed national support function would handle questions including general questions about responsible internationalisation and specific questions that may require input from relevant security agencies.¹¹⁹
- **In Germany, there is continued debate about the need for such a central team.** At the time of writing, the national “stakeholder dialogue” was ongoing and some of our interviewees speculated that a central office, team or advice point might emerge out of this process. There has been some discussion in the media, especially after the meeting of the DFG president with US representatives, about Germany creating a new research security organisation modelled after the proposed US NSF SECURE Center. This would serve as a central focus for information on research security risks.¹²⁰

4.4 Mature risk management processes have been developed by some research performing organisations

- Some research performers have well developed risk management processes to identify, assess and mitigate research security risks.
- This includes due diligence to assess potential partners and funding sources before engaging in research collaborations.
- Due diligence includes the use of databases and open-source intelligence techniques, but some research performers felt that these had limitations.
- Institutional oversight differed between universities with central administration, dedicated research security officers and compliance teams playing an important role in mature systems.
- Lack of capacity and skills sometimes limit risk management.

4.4.1 Risk identification & categorisation

- **Research performing organisations considered a range of risks in international research collaboration.** Those risks included intellectual property theft, foreign interference, cybersecurity threats and dual-use research concerns. Reputational risk is also an important concern for universities.
- **Universities typically considered other risks as well that were beyond those narrowly related to research security.** Most universities included issues of “responsible internationalisation” in their consideration of risk, including issues of ethics, integrity and issues related to engagement with authoritarian regimes. A major concern for many universities is the safety and security of staff and students when travelling abroad, heavily influenced by the concerns represented by organisations like the Scholars At Risk Network.¹²¹
- **The scope of due diligence was wide.** The scope of due diligence includes assessing collaborations and partnerships to verify the background and affiliations of research collaborators, particularly those from foreign entities, to ensure compliance with export controls, sanctions, and national security regulations. Due diligence also reviewed funding sources to establish the origins of financial support for research projects to ensure alignment with ethical guidelines, transparency requirements, and institutional policies and to identify and address any conditions tied to funding that could create conflicts of interest or compromise academic freedom.
- **Some fields are subject to higher scrutiny.** Certain fields are subject to higher scrutiny, especially when they are recognised as dual use. The European Commission’s list of critical technologies has in many cases become a reference point for research performing organisations. The Commission has identified ten critical technology areas and recommended, as an initial step, that Member States together with the Commission assess four technology areas: advanced semiconductors; artificial intelligence; quantum; and biotechnologies.¹²²

-
- **Some countries also provide specific guidance.** For example, the Dutch Contact Point for Knowledge Security identifies knowledge areas at increased risk including knowledge that has been developed specifically for military applications or dual-use technologies and emphasises that knowledge areas that fall outside the scope of export control can also be sensitive. Examples include the domains (or sub-domains) of artificial intelligence, advanced robotics and quantum technology. The Dutch guidance also emphasises the risks for domains in which the Netherlands occupies a unique knowledge position or for technologies that affect the continuity of vital processes in the Netherlands, such as transport, the internet and gas production or on which the Netherlands is dependent, due to a lack of viable alternatives.¹²³

4.4.2 Due diligence & screening processes

- **Some public research institutes have well developed due diligence processes.** In Germany, the Fraunhofer Society of applied research institutes has a system that considers issues of responsible collaboration, information security and IP protection, research integrity and compliance with legal requirements such as export controls¹²⁴. Some Helmholtz institutes, such as the Germany Aerospace Centre [the 'DLR'], have long experience with research security considerations and not only have detailed due diligence processes but have promoted due diligence in the system more broadly.
- **Some universities engage in formal due diligence for potential research partners and funders whilst others are more ad hoc.** Some universities undertake formal due diligence processes as a centralised activity and as part of the wider research management process of their institution. In others, due diligence is more ad hoc. In some, it is regarded as the responsibility of individual principal investigators to review funding sources and verify that financial support aligns with the expectations of their university.
- **Research performing organisations have access to an extensive range of formal guidelines and checklists for assessing risks in international collaborations.** There are a range of guides on due diligence. Some of these guidelines and check lists have been generated by the sector such as the Swedish Rectors Conference Guidelines and the Swedish STINT guidelines.¹²⁵ In Germany, the DLR Project Management Agency has produced a host of tools and guidance for use by researchers and research-performing organisations in Germany and elsewhere, including a Due Diligence Manual, a collection of guidelines from research performing organisations in other countries, and the established OPERATE tool for risk assessment¹²⁶. The Czech Methodologies include a document focused on due diligence.¹²⁷
- **Research performing organisations also look to international guidelines.** The European Commission staff working document on *Tackling R&I Interference* is widely used. The UK's Trusted Research guidelines were frequently mentioned as was Universities UK's publication on *Managing Risks in International Research and Innovation*. This guidance is used by many universities, in whole or in part.
- **Research performing organisations use open-source intelligence techniques.** Many research performing organisations reported that they used open-source intelligence (OSINT) techniques to collect, analyse, and interpret publicly available information to assess potential risks. OSINT was used to assess whether a potential research partner had links to military or high-risk entities like defence universities and government-sponsored research programmes and checking whether potential partners are on sanctions or export control lists.

- **Various databases and other sources are used but some felt that these had limitations.** Publication databases such as Scopus were used to analyse researchers' co-authorship networks as well as LinkedIn, institutional websites, and conference records to detect undeclared affiliations. Several research performing organisations reviewed the Canadian government's list of Named Research Organizations.¹²⁸ The Australian Strategic Policy Institute (ASPI) Chinese Defence Universities Tracker was frequently mentioned and was regarded as a valuable tool for understanding research security risks. However, several respondents said that it must be used with caution as it may overgeneralise risks by categorising some universities as "high-risk" even where research areas were unrelated to military applications. Several universities were seeking commercial open-source alternatives or were looking to the European Commission to support the development of a software package.
- **Some research performing organisations engaged with government agencies as part of the due diligence process, but this was often based on informal relationships rather than formal processes.** In the absence of central advice teams, some research performing organisations used informal relationships with government agencies to supplement their own due diligence. Some Swedish universities noted that the Swedish security services were seeking to increase their relationship with universities.

4.4.3 Institutional oversight, capacity & governance

- **In-house capacity in research security has often emerged out of existing capacity in relation to compliance or internationalisation.** Research performing organisations such as universities have extensive experience in conducting ethical reviews and developing data security protocols (including research data management plans) and cybersecurity processes. In some cases, these have been adapted to consider research security issues.
- **Central administration and research offices play a key role in some institutions but in others risk management is decentralised.** Responsibility for risk management differs between institutions. In some institutions, central administration and research offices played a key role in the risk management process, acting as a central resource of advice and guidance and undertaking due diligence. In other institutions, responsibility is devolved to faculties or individual principal investigators.
- **Responsibility typically lies with Principal Investigators.** Some research performing organisations in the Czech Republic and Sweden noted that the outcomes of their due diligence processes were only advisory and that ultimate responsibility lay with the Principal Investigator. In Germany's diverse research system, the practice is different in different institutions but in the end the emphasis is on the responsibility of the scientist within the law. Many universities reported tensions between central administrative teams and faculties, departments and individual researchers who saw centralised advice on research security as a challenge to academic freedom.
- **Institutions with mature research security practices often have formal processes for decisions about high-risk research projects.** Some institutions have formal processes to escalate decisions on high-risk collaborations. In Sweden, KTH has an Advisory Group on Responsible Internationalisation (RAI). If necessary, this group escalates questions to a Steering Group for Responsible Internationalisation (SAI), which is responsible for issues of international cooperation that are strategic in nature, and which may affect KTH's activities and reputation. In 2024, the RAI reviewed around 25 cases, of which 3-4 were escalated to the SAI.¹²⁹ In other

institutions, high-risk collaborations are escalated to Deans of Faculty, Vice Rectors for Research or the Rector. In France, decisions on high-risk collaborations are referred to the institution's FSD and in turn to the HFDS in the relevant government ministry.

- **Many but not all research performing organisations have dedicated research security officers or compliance teams.** Some organisations have dedicated research security officers. The research security officers may be part of the institution's security office, compliance team, research contracts team or research internationalisation team. In at least one case, the research security officer was part of the Rector's office. Some large research performing organisations (especially technical universities) had significant resources with several staff dedicated to research security and/or export controls. In Sweden, for example, some universities have developed comprehensive research security measures, especially technical universities like KTH and universities with substantial international research collaborations. Since the introduction of the Protective Security Act in 2021, these universities have been establishing research security structures and processes, including the development of internal guidance, awareness raising and training activities and risk management processes. By contrast, in other countries, universities reported a single person was sometimes responsible for research security, even in large institutions, and in some cases that person might have other related responsibilities, for example on research ethics.¹³⁰ One respondent noted that they conducted due diligence after work or on weekends.
- **Lack of capacity and skills were widely reported problems that sometimes limit risk management.** A lack of staff dedicated to research security and export controls, and a lack of appropriately skilled staff was frequently mentioned during our interviews. The lack of suitably trained individuals to conduct due diligence was regarded as a constraint on risk management.

4.5 Some countries provide public funding for capacity building

- **Several countries are providing seed-corn funding from public funds for capacity building.** This is in recognition of capacity issues and university concerns about the implementation costs of research security measures, including the costs of training and awareness programmes for staff.
- **In the Czech Republic,** the government has allocated some funding through the EU Cohesion Fund for research performing organisations to develop research security activities, especially awareness raising and training.
- **In Sweden,** funding has been made available as part of the government assignment on responsible internationalisation to support university development of research security measures. The recommendations note that the funding should also allow for the funding of awareness raising and training activities by research funders and universities.
- **In Germany,** the central office of the Helmholtz system of public research performing organisations funds a programme of research security related projects into which Helmholtz institutes bid for funding.
- **In the Netherlands,** there is debate about whether part of the block funding for universities is meant to cover the costs of research security advice and compliance.

-
- **Seed corn funding catalyses further activity.** Several of those universities that had received seed corn funding noted how it had initiated a ripple effect, fostering the mobilisation of additional resources and initiatives that increase awareness and capacity.

5 LEGISLATIVE MEASURES WITH IMPLICATIONS FOR RESEARCH SECURITY

- Export control practices vary between and within countries.
- Several countries are considering the vetting of visiting researchers and foreign students.
- Foreign investment controls have implications for research performing organisations.
- Statutory protective security requirements are a feature of the French and Swedish systems.

In the previous section we examined the non-legislative measures introduced to enhance research security. In this section, we consider legislative measures and Table 8 (below) provides a summary of legislative measures that have implications for research security.

5.1 Export control practices vary between & within countries

- Controls on tangible & intangible exports have implications for research performing organisations.
- Awareness of export controls varies between & within countries.
- Some universities have dedicated export control officers & compliance teams.
- There are capacity & skills issues regarding export controls.
- Universities reported distinctive challenges related to project complexity & volume.
- Intangible knowledge transfer presents particular issues for university export control.

5.1.1 Scope of export control regulations

- **Export controls are governed by EU regulations and national export control laws.** In Europe, export controls are implemented through a combination of European Union regulations (such as the EU Dual-Use Regulation) and national export control laws.¹³¹ The EU also follows international agreements such as the Wassenaar Arrangement conventional arms and dual-use goods), the Nuclear Suppliers Group, and the Australia Group (biological and chemical controls). In addition, most research performing organisations with mature export control processes are conscious of the requirements of US export control regulations, specifically the International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR) that have extraterritorial effects on global technology transfers.
- **Controls on tangible and intangible exports have implications for research performing organisations.** The physical transfer of controlled materials, equipment, or prototypes to non-EU countries requires an export licence (e.g., advanced materials, semiconductors, biological agents or chemical precursors). At the same time, intangible exports can have significant implications for universities. Non-physical knowledge transfers, such as sharing controlled research data via emails, cloud storage, online learning, delivery of teaching abroad or presentations at international conferences, also fall under export controls. Teaching foreign nationals within European institutions about restricted technologies can also be considered an export. Some countries (e.g. the Netherlands) have produced specific guidelines on export controls for academia.
- **Awareness of export controls varies between countries.** We spoke to several experts on export controls. One noted that while the EU Dual-Use Regulation (EU) 2021/821 provides a common legal framework, national authorities interpret and enforce these laws differently. Some countries, like Germany, France and Sweden, have strict national controls and additional licensing requirements, leading their universities to develop more comprehensive compliance programmes. Some countries have less stringent enforcement, leading to a lighter touch approach by universities.
- **Awareness of export controls varies within countries.** We found that the awareness of export controls amongst institutions and researchers varied not only across the countries studied but also within the countries studied. We found that some research performing organisations had a high awareness of export controls, mature policies and practices and well-resourced export control offices. These were typically technical universities and leading research universities with significant government or defence-funded projects. Equally, we found that there were some universities who seemed to have less awareness of export control issues. These tended to be smaller universities or those focused on social sciences and humanities who believed that their research activities were less likely to involve controlled technologies. The pattern of mature practice in leading institutions and a tail of less aware and less resourced institutions that we saw for research security also held for export controls.

Table 8: Legislative measures with implications for research security

Category	Description	Implications for Research Performing Organisations (RPOs)	Examples
Export controls	EU level and national regulations that restrict the transfer of sensitive technologies, dual-use items, and knowledge to foreign entities.	Limits on international research collaboration involving controlled technologies Licensing requirements for sharing certain research findings.	EU Dual-Use Regulation (Regulation (EU) 2021/821) National legislation and export control lists
Visa controls & vetting	Policies governing the entry, residency, and employment of foreign researchers, including security vetting for access to sensitive research.	Restrictions on hiring international researchers in certain fields.	France & Sweden requires vetting of all researchers & administrators covered by PPST and Protective Security Act Dutch government's Knowledge Security Act has entered public consultation before beginning the Parliamentary process and proposes screening for researchers and masters students in certain listed research domains regardless of nationality. ¹³²
Foreign investment controls	National screening mechanisms that assess foreign investments in research institutions or critical technology sectors.	Restrictions on partnerships with foreign firms or entities with implications for foreign investment in university spin-offs. Mandatory government approval for certain collaborations.	EU FDI Screening Regulation (Regulation (EU) 2019/452) France's Decree 2019-1590 on foreign investment in sensitive sectors German Foreign Trade and Payments Ordinance (AWV) Dutch economic security national contact point (OLEV) for investment controls provides a functional equivalent to the NCP for research security.
Statutory protective security requirements	Legal obligations requiring research institutions to implement physical, cyber, and personnel security measures for sensitive research.	Need for dedicated processes and research security officers	<i>Protection du Potentiel Scientifique et Technique de la Nation</i> (PPST) ¹³³ Swedish Protective Security Act (2021) ¹³⁴

5.1.2 Controlled technologies and research fields

- **Researchers in some fields have a disciplinary awareness of export controls.** There are some fields where most researchers are aware of the export control implications of their research, not least nuclear physics and nuclear engineering. Likewise, the life sciences have paid considerable attention to dual use research of concern and have pursued initiatives to promote academic awareness on this issue.¹³⁵
- **The EU critical technologies list has created greater awareness.** Although not all of the technologies covered by the EU critical technologies list are governed by export controls, the publication of that list has increased awareness amongst universities and focused greater attention on fields such as AI, quantum computing and biotechnology.

5.1.3 Compliance infrastructure, institutional oversight and capacity

- **Some organisations have dedicated export control officers and compliance teams.** We found that some organisations have dedicated export control offices or designated compliance officers who are responsible for interpreting regulations, advising researchers, and ensuring that the institution's activities conform to both EU, national, international and US laws. Others, particularly those with fewer international collaborations or limited exposure to sensitive technologies, often rely on general legal offices with little dedicated expertise in export controls.
- **Export control officers, compliance teams and legal departments advise, review and train researchers and administrative staff.** Many organisations undertake training and awareness raising through workshops and seminars and some institutions have developed internal guidelines that detail the steps to take when dealing with controlled technologies, data, or collaborations with foreign entities. In other cases, there is little support for export controls and there is a particular concern about the awareness of academic staff when it comes to export controlled technical data and know-how that could be transmitted electronically or shared in collaborations, including during foreign visits. Organisations in countries like Germany, the Netherlands and Sweden often train researchers and administrative staff on export control laws, recognising the potential legal consequences of non-compliance. In contrast, some institutions lack structured awareness programmes, leading to inconsistent understanding among researchers about their legal obligations when sharing information, travelling abroad, or collaborating with international partners.
- **There are capacity and skills issues regarding export control.** Organisations face capacity issues and those that we interviewed noted that recruiting and training staff with the necessary knowledge of export controls is a challenge. Export control is a specialist field and there is direct competition between organisations, government and the private sector for individuals with knowledge of export control processes.
- **Several respondents felt that there was a lack of suitable training programmes on export controls.** There are some sector leaders who are engaging and advocating across Europe to raise awareness, capacity and capability, not least through the European Export Control Association for Research Organisations (EECARO). EECARO was established in 2022 by research organisations in Belgium, Netherlands and Germany to bring together knowledge and experiences on export control practice and to engage with regulators.¹³⁶

- **Research performing organisations reported distinctive challenges with export controls:** Organisations reported distinctive, though not entirely unique, challenges with export controls related to project complexity and volume. They engage in numerous research projects, each potentially requiring separate export control reviews. This differs from a manufacturing company, which may apply for a single export licence covering the production and export of a specific product to a specific customer. The administrative burden on universities is therefore significantly higher. Organisations, especially universities, frequently host international researchers who may have access to export-controlled materials. Managing compliance in these situations requires clear institutional policies and awareness among staff.
- **Intangible knowledge transfer presents a particular challenge,** particularly through teaching abroad, online learning, and research collaborations. Challenges arise for universities when teaching export-controlled material to international students, whether in-person or virtually, as well as when supervising postgraduate researchers from different jurisdictions.
- **The 2024 EU Council Recommendation identifies export control rules as an important issue for research security in Europe,** notably those that attempt to regulate the intangible transfer of technology. Compliance has been identified as an issue, not least with respect to the transfer of intangible knowledge. The Commission is considering the development of a document on this topic which would be undertaken between DG RESEARCH and DG TRADE.

5.2 Some countries are considering vetting of visiting researchers & foreign students

- There is an ongoing debate about the need for vetting, especially of PhD students.
- The Netherlands has announced a draft screening law for graduate students working in “sensitive” subject areas.
- Germany is also considering potential measures.

- **There is ongoing debate about the need for vetting, especially of PhD students** within many of the countries. The processes for vetting that are in place (or which may be put in place in the future) differ from country to country.
- **There is no equivalent to the UK Academic Technology Approval Scheme (ATAS) in any of the countries studied.**
- **The countries studied are in the Schengen Agreement and short-term visa arrangements are done at that level.** These might cover short-term research visitors who are not employees. On the other hand, working visas (National D-type Work visas) and long-term student visas are issued

by individual states with their own criteria, and incoming researchers from outside the EU would also typically need a residence permit in most EU member states.

- **France and Sweden have protective security measures to control access to certain facilities or systems.** The French PPST system requires the vetting of all personnel entering a controlled zone (Zones à Régime Restrictif, 'ZRR') and this includes French citizens as well as foreign nationals. Sweden's Protective Security Act places similar requirements on operators with sensitive technologies and those operators include some universities.
- **The Netherlands has announced a draft screening law for graduate students working in "sensitive" subject areas.** There is concern across the sector about how this will be implemented in practice.
- **Germany is engaged in a very large national dialogue with all stakeholders in the system that will produce collectively agreed upon guidance about a future vetting process.** It is thought that universities rather than government will be responsible for the vetting.

5.3 Foreign investment controls have implications for research performing organisations

- Awareness of the implications of foreign direct investment controls differs between research performing organisations.
- Foreign direct investment controls can limit foreign investment in university start-ups and spin-offs.
- In Sweden, it appears as if its FDI Act may also be employed to review foreign research funding in some fields.

Although public attention regarding foreign investment controls often focuses on large corporate mergers and acquisitions, they can also have implications for research performing organisations.

- **Awareness of the implications of foreign direct investment controls differs between research performing organisations.** National authorities reported their efforts to raise awareness of these issues.
- **The EU and national governments have strengthened the screening of foreign direct investments.** For example, in December 2023, Sweden introduced the Screening of Foreign Direct Investments Act which gives the Inspectorate of Strategic Products power to screen investments in security sensitive areas including biotechnology, nuclear, military, dual use, emerging and other security sensitive technologies.¹³⁷

-
- **These laws have implications for research performing organisations.** Foreign direct investment controls can impact research performing organisations by influencing their funding, international collaborations, and technology transfer activities. FDI controls can limit foreign investment in university spin-offs and startups, particularly if their innovations fall under "strategic" sectors. In Sweden, it appears as if they may also be employed to review foreign research funding in fields covered by the Protective Security Act (2021).¹³⁸
 - **Foreign investment controls focus on sectors deemed critical for national or economic security.** Fields such as artificial intelligence, quantum computing, semiconductors, and biotechnology are typically subject to FDI controls. In addition, areas deemed important to national security including critical national infrastructure.

5.4 Statutory protective security requirements exist in France & Sweden

- Statutory protective security measures are a feature of research security in France and Sweden.
- They impose legal requirements on organisations to implement physical, personnel and cybersecurity security measures for certain sensitive activities.
- In France, the *Protection du Potentiel Scientifique et Technique de la Nation* (PPST) requires a *Zone a Regime Restrictif* (Restricted Access Area) to be created and applied in all or part of a public or private laboratory engaged in sensitive research.
- The Swedish Protective Security Act (2021) imposes similar requirements for physical and virtual access to designated facilities.
- Security requirements apply to French and Swedish citizens as well as foreign nationals and unauthorised entry can lead to criminal sanctions.

5.4.1 Statutory protective security measures

- **France and Sweden have statutory protective security requirements that apply to research performing organisations.** These statutory protective security requirements cover all research performing organisations, private and public, and apply to research performing organisations in the public research system. The requirements have implications for many universities in France and Sweden.
- **In France,** the PPST system requires protective security measures for laboratories engaged in certain defined research and technology areas, specifically those that may have application to

weapons of mass destruction, the development of military capability, terrorism or economic competitiveness. A protective *Zone à Régime Restreint* (Restricted Access Area) can be created and applied in all, or part of a public or private entity and access control must be managed, with physical and virtual access to a ZRR subject to authorisation by the head of the entity after ministerial permission has been granted. This applies to French citizens as well as foreign nationals and unauthorised entry can lead to criminal sanctions.

- **In Sweden**, the Protective Security Act (2021) obliges all “operators”, including universities, to identify sensitive technologies and put in place practices to protect them.^{139,140} The Protective Security Act, *säkerhetsskyddslagen*, stipulates that every government agency, public organisation, private company and NGO must assess whether there is anything within its operations that is crucial – in any way – for the security of Sweden. A designated Head of Protective Security in the organisation is responsible for the vetting of all people accessing designated activities, both foreign and Swedish nationals. Research performing organisations are expected to undertake a protective security assessment (*säkerhetsskyddsanalys*) every 24 months. If the assessment concludes that there are operations, data or knowledge in the organisation that are relevant for the security of Sweden (“security sensitive operations”), the organisation must report this to its relevant supervisory authority and the Swedish Security Service, *Säkerhetspolisen*.¹⁴¹ The security service can require a further audit at any time if they have concerns about the protective security practices of an organisation.
- **There are legal obligations to report security incidents.** In France, the role of the institution’s FSD (Fonctionnaire de Sécurité de Défense) is to monitor and report any incidents. In Sweden, this is the responsibility of the Head of Protective Security.

5.4.2 Capacity, monitoring, and enforcement

- **Protective security requirements have resource implications for research performing organisations.** There are significant compliance costs in terms of requirements for security infrastructure and training. In France, the PPST system is supported in each academic or research institution by a Fonctionnaire de Sécurité de Défense (FSD). The FSD reports to the HFDS of the Ministry of Higher Education and Research, creating a network of security-aware individuals. These officials may be full-time in larger organisations, and part-time in smaller organisations. In Sweden, the requirements of the Protective Security Act mean that universities that have security sensitive operations must appoint a dedicated Head of Protective Security. This person reports directly to the Rector and is authorised by law to make far-reaching executive decisions regarding all aspects of protective security in the organisation.
- **The Swedish Protective Security Act describes the proactive security measures that need to be enforced in the organisation.** These measures must be set out in a protective security plan and authorised by the Rector of the university.
- **Personnel security clearances are required.** In France, French citizens or foreign nationals who wish to access the ZRR are subject to vetting which is led by government. Likewise, in Sweden any individual who wishes to access security sensitive operations, data or knowledge is subject to security clearance. The security clearance is conducted by the Head of Protective Security in cooperation with the Swedish Security Service.
- **Legal penalties exist for breaches or non-compliance.** In France, a person who enters a ZRR without authorization may be liable to a sentence of 6 months imprisonment and a fine of €7,500 (£6,400). A theft or misappropriation of documents or equipment within a ZRR may be subject to

up to 20 years of criminal detention and a fine of €300,000 (£256,000). A member of staff may be fined if they participate directly or indirectly in the circumvention of the regulations.¹⁴² **In Sweden,** the Protective Security Act allows the supervisory authority (the Swedish Security Service) to impose an administrative fine on any operator that fails to comply with key obligations under the Act. The administrative fine is set at a minimum of SEK 25,000 (£1965) and a maximum of SEK 50 million (£3.93 million).

6 RECOMMENDATIONS & CONCLUSIONS

- This report has examined perceptions of threats to European research security and the policies and practices in response to those threats in seven European countries. We have also examined developments in policies by the European Union.
- Our findings emphasise that research security policies and practices are maturing but areas of relative weakness remain.
- We note that there is a diversity of policy and practice *between* and *within* research systems.
- Our findings lead to recommendations for governments, research funders and research performing organisations.
- Our study has some limitations, and these suggest directions for future research.
- Attention needs to move towards capacity building and the convergence towards good research security practices across countries.
- The appendices to this report provide case studies of the seven countries and the European Union.

6.1 Research security policies & practices are maturing but areas of weakness remain

The main findings of our study are as follows:

- **The countries studied have similar perceptions of the research security threats that they face.** There are concerns about **threat vectors** associated with the hostile activities of threat actors and poor risk management practices of research performing organisations or individual researchers. The **same threat actors are typically identified**, namely China, Russia and Iran.
- **There is a growing awareness of research security and research security policies and risk management practices are being put in place.** However, no country can be said to have institutionalised research security practices across its whole research system.
- **There is diversity of policy and practice *between* research systems** with countries at very different stages in their response to research security challenges. We found that some

countries have mature research security policies and practices. Some are at an early stage in their response.

- **There is diversity *within* the research systems of individual countries and universities and public research institutes within research systems are adopting research security policies and practices at different rates.** Almost all countries have a core of research performing organisations that have mature research security practices and a tail of organisations with less developed practices. The less engaged organisations are often smaller and less internationalised or find the costs of implementing research security measures prohibitive.
- **A range of non-legislative research security measures exist.** A variety of means are being used to promote awareness and create forums for dialogue between government, security agencies, research funders and research performing organisations although we found no equivalent to the UK's Trusted Research Campaign. A range of written guidance exists on research security and some research managers find the volume of national and international guidance confusing. Central advice teams for information sharing by government exist in a few countries and some countries are considering their introduction. Risk management and due diligence processes are being developed and implemented.
- **Legislative measures exist that have implications for research performing organisations.** EU and national export controls govern certain technologies and research fields but there are concerns about awareness, institutional oversight and capacity especially regarding intangible knowledge transfer. Visa control and vetting procedures focused on foreign researchers and students are being considered by some countries (although none of the countries studied is currently operating a system equivalent to the UK's ATAS).¹⁴³ Foreign direct investment controls have implications for university spin-offs and in some cases foreign research funding. Unlike the UK, France and Sweden have statutory protective security requirements for research performing organisations engaged in certain sensitive activities.
- **The focus of research security policy and practice is moving from awareness raising to capacity building and broadening the adoption of good practice across the research system.** There is recognition of the need to increase capacity for risk management, due diligence and export control compliance but this is challenging due to resource constraints, a lack of suitably skilled individuals and limited training programmes.

6.2 Recommendations

Drawing on the findings of our study, we make the following recommendations for governments, research funders, research sector organisations and individual universities.

6.2.1 Governments

- **Governments should promote greater information sharing** to build an evidence base that can evaluate what risk management practices are effective as well as the costs of poor practice.

- **Like-minded governments should work together to create sector-wide research security standards to support universities and research institutes.** Standards setting and quality assurance for risk management processes and due diligence would increase mutual confidence in research security practices between research performing organisations. Furthermore, it would reduce the administrative costs and complexity of research security in large multi-partner research collaborations and the need for due diligence in research collaborations between organisations in like-minded countries. In addition, it would provide quality assurance of practices for organisations who currently face a confusing array of national and international guidance.
- **Governments should seek a forum that engages the widest grouping of countries.** Research security policy is a crowded space and has been a focus of attention for the Five Eyes intelligence alliance, the Group of Seven, the European Union and the Organisation for Economic Cooperation & Development. However, each (apart from the OECD) represents a sub-set of countries with important scientific capabilities and excludes others who play key roles in international research collaboration.¹⁴⁴ Standard setting will be more effective if it engages the widest range of like-minded countries and achieving coordination and coherence between these different forums should be a key consideration for like-minded governments.¹⁴⁵
- **Governments should broaden and deepen their support for capacity building.** There is an urgent need for capacity building through training and skills development for the leaders of research performing organisations, researchers and administrative staff. Individual governments should increase their support for sector-wide and institution level initiatives to increase capacity whilst reinforcing awareness raising, especially in countries who are at the early stage of research security policy development.¹⁴⁶

6.2.2 Research funders

- **Research funders should consider how best to incorporate research security considerations in grant funding.** Risk assessment criteria and security measures should be considered for funding applications, particularly for sensitive technologies and dual-use research. Grant applications should require transparency about international partnerships and funding sources and ensure that policies are in place for data storage, sharing, and protection in research projects.¹⁴⁷ Research funders should balance such developments against the huge scientific, economic and cultural benefits of scientific openness to international research collaboration.
- **Research funders should broaden and deepen mutual learning exercises with like-minded organisations.** Mutual learning can support research funders through the sharing of good practice, written guidance and templates for due diligence as well as case studies of success (and failure).¹⁴⁸

6.2.3 European associations of universities and research professionals

- **European associations of universities and research professionals have an important part to play.** European associations can develop information sharing networks and have

a key role in advocating for balanced policies to ensure that security measures do not stifle international collaboration and academic freedom.

- **European associations of universities should continue with their mutual learning activities.** These have an important role in information sharing and the diffusion of good practice.
- **Professional associations should be supported by governments to deliver capacity building activities.** Professional associations, such as those related to export controls and research administration and management, can play an important role in capacity building through on-line and face-to-face training courses. However, these activities can be costly for those running such activities and they should be supported financially by governments.

6.2.4 Individual universities and research institutes

- **Universities and public research institutes should leverage their strategic partnerships with their peers.** Existing strategic partnerships between research performing organisations can be used to conduct mutual learning exercises and agree expectations and minimum standards for research security in their joint activities.

6.3 Limitations of the study & directions for future research

The study has some limitations that should be noted, not least because they suggest opportunities for future research.

- **Research security in Europe is a dynamic policy space.** One limitation of this study is that some aspects may date quickly. Research security is a dynamic policy space with a series of emerging initiatives and developments by national governments, research performing organisations and research funders as well as developments at the European and international level. The study focused on seven countries and was conducted between September 2024 and March 2025. This report discusses the situation as of 28 February 2025. We are confident that this study provides a strong body of evidence regarding the picture at the time, but this will need to be updated regularly as policies and practices develop.¹⁴⁹
- **There is a challenge around quantitative measures of policy and practice.** Our comparison of the policies and practices of countries and individual research performing organisations is primarily qualitative and based upon published documents, the opinions of our respondents, subject to systematic analysis and our own expert judgement. We used bibliometrics to highlight patterns of international research collaboration, but we were unable to develop satisfactory quantitative and more structured qualitative measures of threat perceptions and adoption of research security policies and practices. To allow deeper comparison between countries and between institutions, there is a need for the development of robust quantitative metrics to assess the adoption of policies and practices, but we do not underestimate the challenge of doing this. One promising avenue

for quantitative research is around the perception and behaviour of individual researchers on the ground.

- **Our study can say little about the awareness of individual researchers.** There is an important difference between the existence of policies and processes and their implementation. Furthermore, the introduction of policies and processes by research performing organisations does not necessarily signify awareness and use by researchers. Our study design deliberately included interviews with managers and administrators responsible for research, research security and internationalisation since they are more likely to have a sense of the on-the-ground reality than do senior leaders. Interviews with those responsible for research security policies and practices give a sense of the challenges. However, our approach did not allow us to assess the awareness of individual research groups, principal investigators or researchers regarding research security and research measures. There is need at institutional, national and European level for studies of researcher awareness. Manchester Institute of Innovation Research is beginning work on this topic, and we encourage others to do so as well.

6.4 Attention needs to move towards capacity building & convergence of research security practices

- **Research security policies and practices are at different levels of maturity.** Our study has emphasised that the countries studied have similar perceptions of research security threats, threat actors and threat vectors of concern. There is a growing awareness of research security, and a range of policies and risk management practices are being put in place. Countries are at different stages of maturity, and some have high levels of awareness, well developed policies and widely implemented research security practices. However, like the UK, no country can be said to have institutionalised research security practices across its whole research system.
- **Awareness of the importance of research security has grown amongst governments and research performing organisations.** The European Council Recommendation and consultation process has played an important part in awareness raising. Likewise, initiatives by the UK Government's Science & Technology Network and various U.S. organisations have contributed to awareness raising and learning exercises alongside the efforts of individual governments, sector-wide organisations and individual advocates.
- **Most of the countries are now at the implementation stage.** The key issues that they face include capacity building and the creation of a culture of research security awareness with proportionate engagement of the "tail" of research performing organisations in each country.
- **Activity should now focus on support for sector-wide and institution level initiatives to increase capacity.** Governments should also reinforce awareness raising, especially in countries who are at the early stage of research security policy development.
- **There is a need and an opportunity for greater convergence of research security practices.** Research performing organisations are at different stages of maturity and have many different guides and protocols to choose from to inform their risk management

practices. The EU Council Recommendation is likely to encourage a convergence of practice across Member States, especially if new research security requirements are introduced under a future framework programme.

- **There is a strong case for the creation of sector-wide research security standards to support universities and public research institutes.** Like-minded governments should work together to establish common standards and quality assurance for risk management processes and due diligence. This would increase mutual confidence in research security practices between research performing organisations. In addition, it would provide quality assurance of practices for organisations who currently face a confusing range of national and international guidance.

How we strike the right balance between research security and openness to international research collaboration is a key question for the global scientific and technological enterprise. International research collaboration is critical to scientific and technological activity and has underpinned the growth of the research base in recent decades. There is a clear and pressing need to balance research security concerns against the social and economic benefits of participating in open international scientific collaboration.

Like-minded governments and research performing organisations should work together to de-risk those collaborations and address the threats as they see them. We found extensive examples of good practice across the countries that we studied, and this speaks to the huge opportunities for mutual learning between governments, research funders, research performing organisations, and professional associations.

The challenge ahead is to build capacity and support convergence towards good research security practices across countries.

APPENDICES

Appendix 1: Research methodology

This appendix describes the research approach that we employed for our study. We emphasise the focus of the study was on research security in universities and public research institutes. We explain why we chose the seven countries for our study. We describe how we collected quantitative and qualitative data through bibliometric analysis, desk research and a programme of interviews.

1.1 The study focuses on research security in universities and public research institutes

The focus of the study was the publicly funded basic and applied research base, in which Europe's universities and public research institutes are the key elements. We examined research security policies and practices for universities and public research institutes ("research performing organisations"). We did not consider research security in business and industry, except where it impacted universities or public research institutes.

We were aware from the outset that different terms are used related to research security, and this was one of the issues that we explored in the study. On the matter of definitions and scope of the study, we chose to begin from the G7's definition of research security agreed in June 2022, that is:

"the actions that protect our research communities from actors and behaviours that pose economic, strategic, and/or national and international security risks. Particularly relevant are the risks of undue influence, interference, or misappropriation of research; the outright theft of ideas, research outcomes, and intellectual property by states, militaries, and their proxies, as well as by non-state actors and organized criminal activity; and other activities and behaviours that have adverse economic, strategic, and/or national security implications".¹⁵⁰

The concept of research integrity also appears in some discussions, and we followed the G7's approach, seeing research integrity as a separate but related concept.¹⁵¹ We did not specifically seek to examine research integrity but considered it when it proved to be directly linked by any country in its treatment of research security.

1.2 We examine seven European countries and the EU, selecting them because of the importance of their publicly funded research bases

We examined research security threats, policies and practices for seven European countries plus the European Union. We selected France; Germany; Italy; the Netherlands; Spain and Sweden because of the importance of their publicly funded research base to the overall European research base. We chose them by using data from the Nature Index of country scientific outputs as our measure for scientific output and international co-authorship.¹⁵² We chose the Czech Republic as an example of policy and practice in Central & Eastern Europe (CEE) and as a European science system that represents the National Academy of Sciences-type model most associated with CEE. We included the European Union given its normative influence on European research policy, its policy coordination role for Member States and its position as a leading funder of science and technology through the HORIZON programme and European Research Council.

1.3 We collected quantitative and qualitative data through bibliometric analysis, desk research and a programme of interviews

We used a mixed methods approach and collected quantitative and qualitative data. Our data collection approach followed the following steps:

- 1 We began by reviewing existing research, analysis and guidance created by the UK government and UK organisations.
- 2 We undertook a scoping exercise in the UK as a means of focusing the study. This comprised sixteen interviews with representatives of the UK government, research security organisations, universities (including Vice Chancellors and senior research managers and administrators), research sector organisations, and selected independent experts.
- 3 For our seven selected European countries, we generated quantitative measures of their international scientific collaboration, specifically the main countries with whom their scientists collaborate and the most important scientific fields for that collaboration, focusing on natural and physical science and engineering fields which are relevant to the UK's five critical technologies.¹⁵³ We undertook a simple bibliometric analysis of international co-publication and funding, a proxy measure of the internationalisation of the academic research base for each country and therefore at least a partial indicator of the extent of the attack surface, that is the potential exposure of that national research system to research-related risks. Our bibliometric analysis used *The Lens*¹⁵⁴, an open-source tool providing data on scholarly publications.¹⁵⁵
- 4 We conducted desk research to collate policy documents and news coverage of research security issues in each selected case country where it existed in English and where necessary we also translated selected key texts. We mapped the research base of each selected country to identify appropriate organisations and individuals for our interview programme. We also analysed the 56 responses to the European Commission call for evidence on its proposal for a Council Recommendation on enhancing research security in Europe.¹⁵⁶
- 5 The core of the study was a programme of interviews with key informants in each of the selected countries and European organisations. We undertook video or face-to-face interviews with 73 key informants from:
 - National government ministries responsible for research funding and policy
 - Research funding bodies
 - Government organisations responsible for research security
 - Senior university leaders (Rectors and Vice-Rectors) and their equivalents in public research institutes
 - Research managers in universities and public research institutes
 - Research sector organisations (national and international associations for universities, including Rectors Conferences and professional bodies)

We also attended three conferences relevant to our study, either as speakers or delegates, these were: the Helmholtz Association conference on research security (November 2024, Berlin); Charles University conference on “Institutional Resilience as a Tool for Safeguarding Academic Freedom” (November 2024, Prague); and the Nordic

Council of Ministers Conference “Nordic Approaches to Responsible Internationalisation” (December 2024, Stockholm).

1.4 Details of the interviews

Country	Policy makers	Research funders	Research security organisations	Research performing organisations		National academy or learned society	Research sector organisations	Independent experts	Total
				Leaders	Managers/ administrators				
Czech Republic	2	0	1	0	2	1	0	1	7
France	0	0	2	3	0	0	1	0	6
Germany	1	2	0	2	1	1	2	0	9
Italy	0	0	1	1	1	0	0	1	4
The Netherlands	2	0	0	0	3	0	0	0	5
Spain	3	0	0	4	0	0	0	0	7
Sweden	4	6	0	0	11	0	1	3	25
European Union	3	0	0	0	0	0	7	0	10
UK	0	0	4	4	3	0	4	1	16
TOTAL	15	8	8	14	21	2	17	6	89

Appendix 2: Country case study - Czech Republic

1. INTRODUCTION

The Czech Republic has paid considerable attention to foreign interference in universities and academic research following several high-profile incidents at Charles University in 2019. The Czech Republic is at the early part of the implementation stage for research security policies and practices. The Czech Republic has published a series of guidance documents, most recently three “Methodologies” documents in 2024, that set out Czech policy, guidance on conducting due diligence, and guidance for university leaders on institutional resilience.^{157 158} However, research security is far from institutionalised in universities and the focus of government has moved towards ensuring widespread implementation of good practice. The Czech government has provided seed-corn funding for capacity building and the Higher Education Act will require universities to report their progress with research security measures from 2025.

Timeline of initiatives and guidelines publications:

- 2019 – Charles University is the focus of foreign interference efforts with accusations of covert funding of the Czech China Centre.
- 2021 – Centre Against Hybrid Threats (Ministry of the Interior) publish the ‘Counter Foreign Interference Manual for the Czech Academic Sector’ and the Financial Analytical Office publish the ‘Handbook: Technical Assistance and Intangible Transfer of Knowledge’.^{159 160}
- 2022 – European Values Centre for Security Policy and other think tanks publish a series of guidelines.¹⁶¹
- 2024 – “Methodology Documents” published by the Interdepartmental Working Group for Combating Illegitimate Interference in Higher Education and Research.
- 2025 – Higher Education Act introduced that requires universities to report progress on the implementation of research security measures

2. THE NATIONAL SCIENCE SYSTEM, UNIVERSITIES AND PUBLIC RESEARCH BASE

The Czech Republic has a well-developed national science system, underpinned by a mix of public and private research institutions, universities, and government support mechanisms. The system has undergone significant reforms since the 1990s, transitioning from a centrally planned model to a more competitive and internationally connected system.

The science and research system is primarily overseen by the Ministry of Education, Youth and Sports (MŠMT) and the Czech Science Foundation (GAČR), which funds basic research. Applied research is largely supported by the Technology Agency of the Czech Republic (TAČR). Additional funding comes from European programmes such as Horizon Europe and structural funds. The Research, Development, and Innovation Council (RVVI) advises the government on national science policy, and the National Research, Development, and Innovation Policy sets long-term priorities.

The Czech Republic has a university sector comprising public universities, a few private institutions, and state-run technical universities. The Academy of Sciences (AV ČR) is the key public research organisation, comprising over 50 research institutes covering physics, chemistry,

life sciences, social sciences, and other fields. It plays a central role in conducting fundamental research and international collaboration.

3. ENGAGEMENT IN INTERNATIONAL RESEARCH COLLABORATION

The Czech science system is increasingly integrated into global networks, following a decades long process of Europeanisation and research and higher education internationalisation. The country hosts research facilities such as the Extreme Light Infrastructure (ELI Beamlines), one of the world's leading laser research centres. It also collaborates with the European Space Agency (ESA) and is active in CERN projects.

In the tertiary sector, OECD data shows that around 15% of enrolments were accounted for by international students in 2022. The majority of these (12% of all enrolments) were from other European countries of origin (the majority from neighbouring Slovakia) with Asia accounting for almost all of the remaining international students.¹⁶² The share of masters and doctoral student enrolments is higher, at 18 and 26% respectively. We could not obtain data on the internationalisation of research and teaching staff in the Czech Republic's tertiary sector as a whole, but Charles University reports around 16% of their academic and research staff as of international origin, although again it might be that many of these international workers are Slovakian.¹⁶³

According to a 2021 study (using 2018 data), the Czech Republic stood in the middle rank of European countries with regard to international research collaboration as proxied by co-publication. 51% of all papers in 2018 were internationally co-authored.¹⁶⁴ A more recent analysis of 2022 data by the US National Science Board provides a slightly higher figure, at 56%¹⁶⁵. When we correct for the scale of the science system and look at only extra-EU collaborations, in 2022 the Czech Republic produced 1316 internationally co-authored publications with non-EU countries per 1000 researchers, well behind Sweden and the Netherlands, but in line with Germany.¹⁶⁶

Our own study of co-publication, using *The Lens*, identified the Czech Republic's nine leading collaborators. This shows that the US, UK and Germany are the main source of collaborators, and their respective rankings have remained the same between 2015-2023. China has emerged as a source of scientific collaboration and now ranks sixth (with Poland and Spain) but only accounts for co-authorship of 5% of Czech scientific papers. Russia features in 2015 but is no longer an important source of co-authorship.

Table 1: Top nine international collaborating countries measured by co-publication, three years

Top Nine International Collaborating Countries, Three Years, By Count of Documents [Publications]						
Country	Document Count 2015	Country	Document Count 2020	Country	Document Count 2023	
Czech Republic	16176	Czech Republic	19386	Czech Republic	18755	% in 2023
US	2098	US	3107	US	2206	12%
Germany	1394	Germany	2114	Germany	1821	10%
UK	1238	UK	1847	UK	1471	8%
France	962	Italy	1408	Italy	1279	7%
Italy	812	France	1337	France	1056	6%
Poland	681	Poland	1087	Poland	1027	5%
Spain	657	Spain	1008	China	1015	5%
Switzerland	572	China	956	Spain	1001	5%
Russia	555	Switzerland	929	Switzerland	733	4%

Source: enabled by the <https://www.lens.org/> [lens.org]



4. PERSPECTIVES ON RESEARCH SECURITY

Here we consider perspectives on research security: how the Czech Republic defines research security, the research security threats and threat actors that it identifies, and the factors influencing the responses of government and research performing organisations.

4.1. Definition of research security

The term “illegitimate interference” is frequently used in Czech discussions of research security issues and there is a strong emphasis in Czech policy on institutional resilience. Czech policy and practice places considerable weight on the implications of foreign interference for the humanities and social sciences as well as STEM disciplines.

The 2024 Methodologies Reports, define research security as follows:

“Organisational and systemic procedures for evaluating and managing security risks in the area of research and education, which reduce the risks associated with illegitimate interference in the higher education and research environment. The primary goal of research security is the comprehensive protection of the research ecosystem, which also encompasses the protection of national and economic interests” ¹⁶⁷

Illegitimate interference is defined as:

“[U]nwanted interference on people, decisions, or processes. This includes foreign malign influence as well as criminal (e.g., corrupt) behaviour and undesirable lobbying.

These are usually activities that are covert, deceptive, coercive or corrupt and which the perpetrator of illegitimate interference (foreign power, corruption, lobbying in violation of the law or generally accepted social ethical rules) carries out himself or through a third party and which threaten or damage the interests of higher education and research institutions. Alternatively, the term foreign interference is also used”.¹⁶⁸

4.2 Research security threats

4.2.1 Threats and threat vectors

Research security threats of concern to the Czech Republic span economic security and national security. The Czech Republic places a particular emphasis on foreign interference with universities and academic research through funding and the actions of foreign agents on campuses.¹⁶⁹

Espionage and the actions of organised crime are also highlighted. Czech guidelines highlight the threat posed by foreign intelligence services, think tanks and NGOs who act as fronts for government agencies and foreign “front” companies and organised criminals, including smuggling networks. There is a long history of hostile intelligence services seeking to recruit academics at Czech universities and insider threats are exacerbated by personal or financial problems. Threat actors are said to be looking for a broad spectrum of data including scientific knowledge.¹⁷⁰ Czech think tanks have emphasised the threat to Czech universities posed by collaboration with Chinese actors such as the Seven Sons of National Defence, the Confucious Institutes and the Thousand Talents Programme.¹⁷¹

Recruitment of Czech academics by foreign intelligence services or criminal organisations using financial incentives or other external pressures is highlighted as a significant concern, particularly in relation to academics being approached by threat actors at foreign conferences or during visits to high-risk countries.¹⁷²

There are concerns about research collaboration with potentially hostile foreign actors and knowledge leakage through legitimate research collaborations that have poorly structured cooperation agreements or cede legal jurisdiction to a potentially hostile state.¹⁷³ Cyber threats and poor research data management have also been highlighted as concerns.¹⁷⁴

Sensitive areas of research and education that carry an increased risk of illegitimate interference and for which enhanced protection is deemed necessary, are identified in the 2024 Methodologies Reports as:

- Critical technologies for the economic security of the EU. These include AI, semiconductors, quantum and space technologies (given the Czech Republic’s strength in this field).¹⁷⁵
- Dual-use goods and technologies, and military material.
- Selected fields of research and education and selected cooperation with third parties.¹⁷⁶
- Any other area that an academic institution chooses to classify as sensitive.¹⁷⁷

4.2.2 Threat actors

Czech guidelines on research security are country-agnostic. However, the 2023 Czech National Security Strategy explicitly identifies the threat posed by both China and Russia.

The National Security Strategy argues that China poses a fundamental systemic challenge globally and also in terms of direct influence operations in the Czech Republic. It also argues that China fails to adequately protect intellectual property rights and misuses the instruments of scientific and academic cooperation.

The National Security Strategy also notes that the threat posed by Russia. Indeed, Russia plays a more prominent role in Czech discussions about national security – and thus research security – than perhaps any of the other countries examined in this study apart from Sweden. The National Security Strategy comments that Russia acts deliberately against the Czech Republic’s political, economic, and social stability and poses a fundamental threat to the country’s security through its use of a broad range of hybrid operations targeting Czech interests. Its non-military activities attempt to undermine confidence in democratic institutions and destabilise the Czech Republic’s society and economy.¹⁷⁸

4.3 Factors influencing the policy responses of government

Several factors can be identified as influencing government policy responses on research security:

- **Political pressure, including from the media and NGOs:** Perhaps more so than in other countries it seems that high profile media cases and public awareness of foreign interference have spurred government responses. The issue of foreign interference in Czech universities has been a subject of attention since the high-profile incidents at Charles University in 2019, when it was revealed that several academics had accepted money from the Chinese Embassy, routed through a private firm, to facilitate conferences at the Czech-China Centre.¹⁷⁹ This has led to pressure on the government from politicians, the media and several NGOs to address the issue of foreign interference in academia.¹⁸⁰ The Counter Foreign Interference Manual was a direct response to requests from Charles University after the 2019 foreign interference scandal.¹⁸¹ High-profile media criticism and reports that Czech universities (e.g. Czech Technical University in Prague and University of Pardubice) have links to the Seven Sons of National Defence, have exacerbated concerns over China’s influence.¹⁸²
- **University autonomy:** Constitutional provisions and the country’s experience under Communism play an important role in its response.¹⁸³ Academic rights and freedoms, institutional autonomy, self-governance, and freedom of research or action have been recognised as specific freedoms enshrined in Czech law and in the Constitution as well as statutes of universities. Thus, the government has emphasised that universities are responsible for the development and management of their international cooperation. The Czech government emphasises that it is interested in providing support to higher education and research institutions through relevant tools to make informed decisions and help them manage risks related to illegitimate interference. However, in the end, and in relation to institutional autonomy, the responsibility and implementation of specific measures lie fully with the higher education and research institutions themselves.¹⁸⁴

- **The importance of international research collaboration:** Government policy has emphasised the importance of international research collaboration and its desire to facilitate a derisking strategy rather than decoupling and this has influenced government policy towards research security.
- **Importance of open science:** The government has emphasised the importance that it places on open science and stresses the need to balance research security needs against this desire for open science.¹⁸⁵
- **Practices of other countries:** Government policy has been influenced by the practices of others, including close relationships with the UK and US. The UK government's Science & Technology Network (STN) has provided advice to the Czech research sector, including organising a fact-finding visit to the UK by a delegation of representatives of government, universities and the National Academy of Sciences. The U.S. State Department and the Stanford University Hoover Institution has been closely involved in Czech developments. The Czech guidance documents refer positively to the practices of the UK, Australia, the Netherlands and Belgium.
- **European Union initiatives and anticipated requirements of FP10:** The Czech government's approach has been influenced by European Union initiatives, engagement in the European Research Area and especially the 2024 EU Council Recommendation.¹⁸⁶ The anticipated requirements for EU research funding under FP10 are strongly emphasised in the Czech Methodologies Reports. The report explicitly argues that: "it is not out of place to be inspired by the motivational saying "fortune favours the prepared mind" in the coming years" in the context of potential research security requirements under HORIZON or FP10.¹⁸⁷

4. 5. Factors influencing responses of research performing organisations

Several factors are influencing the response of research performing organisations:

- **Recent incidents of foreign interference:** Universities have experienced high profile incidents of foreign interference and espionage themselves or are aware of the experience of Charles University. The Academy of Sciences has also had examples of undesirable cooperation and concerns about being targeted by foreign intelligence services.¹⁸⁸
- **New legal and regulatory requirements:** The introduction of requirements since 2025 for reporting research security practices within the university's annual activity report, as well as the proposed new Act on Research, Development, Innovation, and Knowledge Transfer (currently under discussion in Parliament), are causing university leaders to pay increased attention to research security. This has led to the appointment of research security managers and greater responsibility and accountability within senior leadership teams.¹⁸⁹
- **Capacity constraints:** A number of universities reported capacity constraints either because of limited university investment or due to a lack of suitably skilled staff. One university noted that research security had been added to the responsibility of an existing Head of Security

role which already included responsibility for cybersecurity, information security and physical security.¹⁹⁰ Another noted that there was only one full-time equivalent staff member for research security in a very large university and was waiting for an additional appointment.¹⁹¹

- **Disciplinary fields:** There is more awareness of research security issues in some disciplines, especially nuclear physics and engineering, biomedical research and other STEM disciplines. Social sciences and humanities have less awareness although some are conscious of their vulnerability to foreign interference.¹⁹²

5. RESEARCH SECURITY MEASURES

The Czech Republic is at the early part of the implementation stage for research security policies and practices. Whilst the Czech Republic has very well-developed guidance, research security is yet to be institutionalised across the sector.

5. 1. Extent of response to research security challenges

A few universities have engaged with the issue but there is a long tail of universities who have made only modest progress.¹⁹³ The limited adoption of research practices is recognised in the 2024 Methodologies documents, which comment:

“The task for academic institutions will be to implement the agenda of institutional resilience according to their specific needs at their respective departments, and to tailor individual measures to their field of activity and the specific needs of ongoing research projects”.¹⁹⁴

The Academy of Sciences began addressing research security in 2021, establishing a research security contact point for institute managers and holding awareness-raising workshops. In 2022, the Academy of Sciences cooperated with the Ministry of Interior to create a specific Academy of Sciences Manual for Research Security that includes a due diligence check list for international research collaborations. However, there are differences in rate and extent of adoption between its research institutes.¹⁹⁵

5. 2. Promoting awareness and forums for dialogue on research security

5. 2. 1. Awareness raising

The government has provided seed-corn funding through the EU Cohesion Fund to support awareness raising and training activities in universities. Charles University, Palacky University and the Academy of Sciences have undertaken a joint project to develop audio-visual and training packages. Training has been directed at the senior leadership of universities and has been expanded to include academics and administrators. A sector wide website on research security is under development and is being led by Charles University.

The Ministry of Interior has supported a programme of training of senior leaders, researchers and administrative staff. The Czech government under its Resolution No 794 (October 2023) has expanded Ministry of the Interior training on illegitimate interference to include training for higher education and research institutions.

5. 2. 2. Forums for dialogue

In the spring of 2023, the Ministry of Education, Youth, and Sports established a platform called the Interdepartmental Working Group for Combating Illegitimate Interference in Higher Education and Research. The main goal of this platform is to examine more deeply the issue of illegitimate interference and to create a system of appropriate measures that will contribute to strengthening and protecting the higher education and research environment at the national level and in the context of EU policy.

The group's members represent the Ministry of Education, Youth, and Sports; the Ministry of the Interior; the Ministry of Industry and Trade; the National Cyber and Information Security Agency; the Financial Analytical Office; the Research, Development, and Innovation Council; and the Office of the Minister for Science, Research, and Innovation. Representatives of the Czech Academy of Sciences and higher education institutions also participate in the group's meetings. This is to address issues of coordination across the sector.¹⁹⁶

In addition, to the Interdepartmental Working Group, there is a sector-led initiative to increase coordination across Czech universities to coordinate responses to foreign interference.¹⁹⁷

5. 3. Written guidance on research security

The Czech Republic has published several written guides on research security.

- **The Counter Foreign Interference Manual for the Czech Academic Sector (2021):** This was developed by the Ministry of the Interior in 2021 and provides a summary of advice and recommendations, as well as guidelines on how to deal with situations involving influence by foreign powers, and how to react and proceed.¹⁹⁸
- **Technical Assistance and Intangible Technology Transfer Handbook (2021):** Developed by the government's Financial Analytical Office this provides a methodological tool primarily intended for higher education and research institutions, which addresses restrictive measures within the framework of international sanctions and the related issue of intangible technology controls.¹⁹⁹
- **CAS Manual for Counter Foreign Interference (2022):** this was developed by the Ministry of the Interior in cooperation with the Academy of Sciences in response to further cases of foreign interference this document was developed for the Czech Academy of Sciences' internal use.
- **2024 Methodologies Documents.** In 2024, the Czech Republic published three so-called "Methodologies" documents with the aim of promoting a coherent approach to illegitimate interference across research performing organisations. The documents were co-developed by the Interdepartmental Working Group for Combating Illegitimate Interference in the Higher Education and Research Environment, with contributions from the Ministry of Education, Youth, and Sports, the Ministry of the Interior, and the Czech Academy of Sciences, and in consultation with representatives of other Czech higher education and research institutions. The three documents are:
 - **Strengthening Resilience against Illegitimate Interference in the Higher Education and Research Environment:** This sets out the rationale for research

security and the approach of the Czech government towards strengthening research security. The document explicitly aligns itself with EU policy developments and stresses the potential introduction of research security requirements for EU research funding. The report explicitly argues that: “it is not out of place to be inspired by the motivational saying “fortune favours the prepared mind” in the coming years” in the context of potential research security requirements under HORIZON or FP10. The report identifies “pillars” supporting the system: Risk Management; Due Diligence and Risk Management in Collaboration with Third Parties; Communication, Education, and Sharing Experiences; and Cybersecurity.²⁰⁰

- **Methodological Recommendation Defining the Minimum Scope of Due Diligence and Risk Management in Cooperation with Third Parties within the Context of Strengthening the Resilience of the Higher Education and Research Environment against Illegitimate Interference (Methodological Recommendation for Cooperation with Third Parties)** This defines the minimum scope of due diligence and risk management in cooperation with third parties, the scope and purpose of due diligence, the “know your partner” principle, how to conduct due diligence, and how to collaborate with third parties using NDAs and good practice for foreign travel.²⁰¹
- **Methodological Recommendation for Risk Management in Research Security at the Institutional Level:** This document provides guidance to the leadership of academic institutions and to professionals in the field of research security, including advice on how to integrate strengthening of resilience and protection against illegitimate interference into institutional agendas, the development of resources and capacity and communication, educational, and awareness-raising activities.²⁰²

5. 4. Mechanisms for advice and information sharing by government

There is no formal mechanism for advice and information sharing like the UK’s RCAT or the Dutch National Contact Point for Knowledge Security. Interviewees emphasised the importance of informal networks in providing advice and the Interdepartmental Working Group also provides a role in building an advice network. Research performing organisations can approach the Ministry of Interior or the intelligence services but there is an emphasis on universities as ultimate decision makers.²⁰³

5. 5. Due diligence processes employed by research funders and universities

Several guidance documents on due diligence have been published including the 2021 Counter Interference Manual and the 2024 Methodologies document defining the minimum scope of due diligence. Universities also mentioned the 2022 European Commission Staff Working Document on Tackling Foreign Interference in R&I.

The use of due diligence appears to be inconsistent. We found that due diligence is undertaken especially regarding research collaborations with China and Iran. This uses open-source intelligence techniques. However, there are a limited number of staff engaged in due diligence in any one university. Furthermore, university administrators emphasised that the results were only advisory, and the ultimate decision on research collaborations rests with heads of faculty and principal investigators.^{204 205}

5. 6. Funding for capacity building

A notable feature of the Czech approach is the availability of public funding for capacity building. EU Cohesion Funds are being used by the Ministry of Education, Youth, and Sports for a funding programme called “Setting up a System to Increase Institutional Resilience to Illegitimate Influence”. This provides seed corn funding to support the development of capacities, knowledge, and skills of managerial, research, and other staff of research organisations. Raising awareness of this issue and ensuring the education of employees is a mandatory part of implementing the programme.²⁰⁶

6. LEGISLATION AND REGULATIONS

6.1. Export controls

Export control in the Czech Republic is the responsibility of the Ministry of Industry & Trade. Universities are conscious of export controls and particularly sanctions, although the extent of formal mechanisms within universities is unclear.

6. 2. Visa controls and vetting procedures

Visa controls are seen by universities as the responsibility of government agencies. Universities will provide information on students if required. There is no mandatory process within universities regarding the vetting of visitors. Some universities do review visitors on behalf of the Dean of the faculty who will then make the final decision.

6. 3. Investment controls

The Czech Republic has FDI controls. Attention has been paid to university spin-offs and some awareness raising activities have been undertaken by the Ministry of Industry & Trade responsible. Attention is paid to technologies that are regarded as sensitive and not only those formally defined as “dual use”.

6. 4. Formal reporting requirements

Higher education institutions, in accordance with the obligation given by Act No 111/1998 Coll., on Higher Education Institutions and Amending and Supplementing Other Acts, must submit an annual report on the activities of the university and an annual report on the management of the university to the Ministry of Education, Youth, and Sports. Starting in 2025, the outline of the annual report on the activities of the university will also include a section related to the issue of strengthening resilience against illegitimate interference.

6. 5. Research, Development, Innovation, and Knowledge Transfer Act

From November 2023, the Research, Development, Innovation and Knowledge Transfer Act introduces the concept of “institutional resilience” and the obligation of “precautionary principle or precautionary approach” aimed at ensuring research security and protection against illegitimate interference, with obligations on the side of funding providers and recipients. At the end of 2023, a draft of a new Act on Research, Development, Innovation, and Knowledge Transfer

was presented to Parliament. It also mentions issues related to research security and the need to strengthen institutional resilience against illegitimate interference in the research environment.²⁰⁷

7. CONCLUSIONS

Amongst countries in Central and Eastern Europe, the Czech Republic stands out for the attention that it has paid to research security, not least in the context of foreign interference in leading Czech universities. The Czech “Methodologies” documents published in 2024 are impressively detailed and compare favourably against anything produced globally. However, research security is far from institutionalised in universities and the focus of government has moved towards ensuring widespread implementation of good practice. The Czech government has provided seed-corn funding for capacity building and the Higher Education Act will require universities to report their progress with research security measures from 2025.

The introduction of research security measures for Czech research funding is likely to be considered to ensure that it is considered in international Memorandums of Understanding and in evaluation of projects. A methodology has been developed for the evaluation of bilateral projects by the Ministry of Education, Youth & Sports who is currently working on pilot projects on this topic. The rate and character of adoption of research security measures in Czech universities is likely to be influenced by the availability of funding as well as capacity although the new reporting requirements mean that research security has been raised on the agenda of university leaders.

Appendix 3: Country case study - France

1. INTRODUCTION

France has a long-standing tradition of treating science and technology as matters of strategic national interest and this strongly shapes its approach to research security. The French government plays a central role in a top-down system where the state defines research security threats and manages a centralised system to respond to them.

France has the most mature research security system of the countries in this study. Dating back more than a decade, the *Protection du Potentiel Scientifique et Technique de la Nation* (PPST) framework provides the legal and administrative foundation for safeguarding sensitive knowledge, strategic technologies, and digital data. The PPST is a statutory protective security requirement that governs all research performing organisations conducting particular activities. This includes the designation of certain premises as *Zones à Régime Restrictif* (ZRR), where access is legally restricted to prevent unauthorised intrusions and espionage.

In addition, France has a centralised system for the screening of international research collaborations. The screening approach applies to all international research collaborations, and this is done by the Ministry of Universities and Research and the Ministry of Foreign Affairs.

The PPST has been in place for several decades but has been subject of recent reforms, including the introduction of legal penalties for non-compliance. Furthermore, we heard of issues regarding the capacity of the actors involved with the process as well as concerns about its focus and levels of compliance.

Developments in the French approach to research security include:

- 2012 – establishment of the current PPST system.²⁰⁸
- 2021 – Senat Report on research security and government review and enhancement of the PPST.
- 2025 - Criminal penalties introduced for non-compliance with the PPST, including fines and imprisonment for breaches of the rules concerning ZRRs.^{209 210 211}

2. THE NATIONAL SCIENCE SYSTEM, UNIVERSITIES AND PUBLIC RESEARCH BASE

In 2020 France spent 2.3% of its GDP on R&D, slightly above the EU average but below the OECD average.²¹² Public research, which accounts for one third of total R&D spending in France, is carried out in public research organisations, universities, higher education and research institutions (engineering schools) and university hospital and cancer research centres.

Of the public research organisations, the Centre National de la Recherche Scientifique (CNRS) is the most important, employing some 33,000 staff of which 28,000 are scientists. CNRS has 1100 research laboratories in France and abroad, and collaborates closely with the university system in France, external research systems, and the private sector. Another important body is INSERM, the National Institute of Health and Medical Research. INSERM conducts a wide range of health and medical research and develops technology. INRAE, the French national centre for research on agriculture, food and the environment.

France also has more than 3,500 public and private institutes of higher education, of which 72 are universities. Universities are public institutions and financed by the state.²¹³ The Agence Nationale de la Recherche (ANR), created in 2010, is a grant funding agency for France and provides funds to researchers through open – bottom up- applications and top-down programmes that predefine a research topic.²¹⁴

3. ENGAGEMENT IN INTERNATIONAL RESEARCH COLLABORATION

In 2020-21, there were 16,938 foreign academic staff and researchers employed in French higher education and public research institutions²¹⁵. The share of international students as a proportion of all those registered on undergraduate programmes is low, at around 6.8% of all students in 2022. The share of international students is greater for postgraduate masters and doctoral studies, at 13.5% and 36% respectively²¹⁶. The majority of international students in the French system come from Africa, almost 5% of all students in tertiary education, reflecting historic colonial and linguistic links. At doctoral level, Africa accounts for 11.5% of all 2022 enrolments versus 11.9% for Asia and only 8% for Europe outside of France.

As a large, mature research system, France has a relatively high level of international co-authorship of research publications by global standards (although somewhat below the level of the UK and much lower than smaller mature European research systems like Sweden and the Netherlands). In common with most other European countries, recent increases in scientific outputs all seem to be accounted for by growth in internationally co-authored publications. According to a 2021 study (using 2018 data), 60% of the French research system's published research output is internationally co-authored.²¹⁷ A more recent analysis of 2022 data by the US National Science Board provides a similar estimate.²¹⁸ However, when we correct for the size of the French science system and look at extra-EU collaborations, in 2022 France produced 993.3 internationally co-authored publications with non-EU countries per 1000 researchers, the lowest proportion for any of our seven countries.²¹⁹

Our own analysis using *The Lens* shows that the United States is France's main international collaborating partner as measured by co-authored publications. The UK is ranked second, a little ahead of other European countries. China is ranked eight and its rank fell slightly between 2020-2023.

Table 1: Top collaborating countries measured by co-publication, three selected years

Top Nine International Collaborating Countries, Three Years, By Count of Documents [Publications]						
Country	Document Count 2015	Country	Document Count 2020	Country	Document Count 2023	
France	98235	France	110595	France	106707	% in 2023
US	14258	US	18746	US	14512	14%
Germany	8045	UK	11002	UK	8431	8%
UK	7980	Germany	9914	Germany	7389	7%
Italy	5457	Italy	8092	Italy	6690	6%
Spain	4507	Canada	5682	Spain	6230	6%
Canada	4431	Spain	5479	Switzerland	5784	5%
Switzerland	4051	China	5477	Belgium	4825	5%
Netherlands	2963	Switzerland	5230	China	4716	4%
Belgium	2894	Netherlands	4255	Canada	4665	4%

Source: enabled by the <https://www.lens.org/> [lens.org]



4. PERSPECTIVES ON RESEARCH SECURITY

4.1. Definition of research security

France adopts an approach to research security that considers such questions under a wider conversation about national and economic security. The French legal framework for dealing with threats to research focuses on the protection of national interests, of national defence capabilities and of economic competitiveness. The PPST employs a fourfold test, these are: risks related to the misappropriation of sensitive scientific or technical information for the purposes of terrorism, the proliferation of weapons of mass destruction and their means of delivery, or to prevent the growth of military arsenal. It also covers knowledge, know-how, or technologies whose ‘undue capture or misappropriation’ could ‘significantly harm’ the economic competitiveness of France.

4. 2. Research security threats and threat actors

Here we consider French perspectives on research security threats and threat actors. We draw primarily on secondary sources, including statements published by the France's domestic intelligence agency (the DGSI).

4. 2. 1. Threats and threat vectors

In 2021, the French Senat published a report entitled *Mieux protéger notre patrimoine scientifique et nos libertés académiques* (Better Protection for our Scientific Assets and Academic Freedoms).²²⁰ The report observed the significant growth in interference actions initiated by foreign states or economic actors driven by economic interests or aimed at using or diverting French knowledge or technologies to fuel conventional weapons or weapons programs of mass destruction.²²¹

The report identified two categories of objectives for threat actors:

- Shaping a state's image or reputation or promoting an official “narrative” by instrumentalising human and social sciences.
- Intrusion and the theft of scientific data that is sensitive to the national interest or protected by intellectual property, in order to obtain a strategic, economic or military advantage.²²²

The Senat report observed that three factors made the academic world particularly vulnerable to foreign interference: a lack of budgetary resources that make researchers increasingly dependent on foreign funding, governance arrangements that were not well suited to taking into account the risk of interference, and the culture of open research based on the sharing of knowledge.²²³

France's domestic intelligence agency (DGSI) and the Defence Intelligence and Security Directorate (DRSD) have issued multiple warnings about growing foreign interference in French academia, particularly in STEM and strategic sectors. Intelligence reports highlighted risks including IP theft, technology transfer, and undue influence through joint labs, funding, or researcher mobility.²²⁴

These warnings have identified several threats and threat vectors.

- **Foreign interference through funding and attempts to recruit French researchers.** In 2024, the DGSI and DRSD issued a warning that foreign actors were targeting researchers who had won scientific awards.²²⁵ One of them, “[the] winner of a high academic distinction in France” had *received a transfer of a large sum of money from the organisers* of a symposium in which he was participating abroad. He had also questioned on political subjects during his stay. DGSI and DRSD also highlighted the case of a foreign company that had recruited a scientist to manage its French subsidiary. The researcher accepted “because of the possibility of working on an innovative subject which, due to a lack of resources, was no longer part of the fields of study in his laboratory”. The recruitment allowed the foreign company to use his reputation and network to facilitate the poaching of other researchers from the same research centre.
- **Threats related to fundamental research.** The DGSI has also emphasised how foreign actors - particularly state-linked or military-affiliated institutions – seek to exploit partnerships in fundamental research to gain access to sensitive knowledge,

equipment, and dual-use technologies. In June 2023, the DGSi published a report that noted that while fundamental research is often viewed as low risk compared to applied research, it is increasingly vulnerable to covert exploitation, especially due to its potential for long-term strategic applications.²²⁶ The report argues that fundamental research is often underestimated as a target for foreign capture, yet it can lead to applications in military or dual-use technologies. These applications may emerge years after initial collaborations, making the risks less visible or immediate. In the same report, the DGSi notes what it calls “strategic and persistent foreign tactics” where foreign entities - especially those linked to military institutions - employ long-term strategies including sending researchers on secondment, attempting to acquire technical blueprints or know-how and proposing official partnerships as cover for ulterior motives. The DGSi emphasises that these tactics often shift from official to informal or unofficial channels, making them harder to monitor or control. Fundamental research may be used as a gateway to access applied research. Thus, a foreign military university initiated a formal partnership in fundamental research. After access was limited, it used existing connections to facilitate informal collaborations in applied research. The French lab's efforts to restrict sensitive access were circumvented through indirect cooperation.

- **Threat from foreign travel.** The DGSi has also highlighted the threats associated with travelling abroad, the need to use “burner” computer equipment dedicated to stays abroad, limit the information taken abroad and maintain a posture of vigilance when interacting with “foreign interlocutors”.
- **Engagement with inappropriate entities.** French institutions may unknowingly contribute to foreign military programmes, damaging their international reputation and scientific standing.
- **Inappropriate use of IP from legitimate collaborations.** These risks are exacerbated when foreign partners misuse research outputs for military or strategic gains, without the knowledge or consent of French collaborators.
- The Senat Report highlighted the specific threat of the **Confucius Institutes** for their potential to disseminate harmful Chinese propaganda.²²⁷

4. 2. 2. Threat actors

The PPST is country-agnostic and the DGSi reports are careful not to name specific countries, speaking instead about the threats posed by “authoritarian states”. Indeed, this aligns with the observation of a 2024 report from the European Think Tank Network on China, that France is characterised by a broader, more country-agnostic concept of economic security that extends beyond specific concerns about China and reflects a general assessment of the global economic order and the direction of the international system which is increasingly evolving towards one driven by power politics at the expense of liberal international rules.²²⁸

Nonetheless, French actors concerned with research and economic security have placed particular attention on China as a threat actor. The 2021 Senat Report noted that China currently appears to be the country most able to conduct a global, systemic strategy of influence due to both its power and its ability to implement long-term policies. In the future, other countries that are already deploying more offensive policies, such as Russia, Turkey or certain Persian Gulf countries, could replicate this scheme.²²⁹

In a 2023 report for the French Institute for International Relations (IFRI), Alice Pannier identifies China and Russia as the biggest threats to the balance between open and closed research ecosystems in France (and Europe). Pannier highlights that Russia is more of a threat to ‘Open Science’, whilst Chinese research espionage and exploitation of dual-use technologies means they are a bigger threat to economic and military competitiveness.²³⁰

4. 3. Scale of attention and response to threats

In recent years, research security has been subject to greater attention from the French government and security services. The 2021 Senat Report noted that foreign influence in the academic field had long been ignored and poorly documented, but it now constitutes an essential facet of international relations that had become increasingly aggressive in recent years. The 2021 Senat Report called for the issue of foreign interference to be made a political priority to assess the current situation and develop appropriate responses in cooperation with the university sector.

We were told that, until 2021, the topic of research security received little attention in France but the COVID crisis and subsequent state-sponsored attempts to access vaccine research had brought a change. One respondent considers that the French had been “very naïve” about the topic. There had been little awareness in universities and while there may have been a sense that knowing the background of a foreign PhD student or researcher might be appropriate, “open science dominated”. At this time, the PPST system formally existed but was not considered important by many labs, unless they worked directly with the defence industry. The FSD [security officials] were not seen as important nor were their opinions considered or taken seriously.

The same respondents told us that the situation had now changed. Within universities there is an understanding of the scale of threats. There is an awareness of scientific espionage, IP theft and dual use concerns. The awareness has grown not least because a lot of labs have seen that they lost patents or IP and saw that many research results were stolen.^{231 232} Compliance was a significant problem and, even now, there is some resistance to the introduction of the new PPST measures.

4.4 Factors affecting the responses of government and research performing organisations

We identified several factors that were affecting the responses of government and research performing organisations.

- **Geopolitics and threat assessment.** The 2021 Senat Report reflects broader concerns that foreign interference is growing, and foreign state and economic actors are seeking access to French scientific knowledge and technologies for military and economic advantage. The French intelligence agencies have issued repeated warnings about the threat posed by scientific espionage.
- **Concerns about compliance.** Government concerned about weak compliance with the PPST has led to reforms. At the same time, universities have become increasingly aware of the requirement to comply with national directives.
- **Tensions between academic freedom and research security.** While many researchers support the principle of protecting sensitive research, there is concern about overreach and the potential stifling of international cooperation, particularly with non-Western partners. However, we found the lack of public debate in the academic community as noteworthy as was the caution of academics and independent experts about discussing such matters with us.

-
- **Resources and capacity are a concern.** Major institutions have begun developing internal policies on partnership due diligence, data governance, and export control compliance and technical and defence-oriented institutions tend to be more advanced. However, there is concern about the lack of capacity in the system, both for universities and government. Moreover, we were told that one consequence of the highly centralised system was that many academics and institutions saw research security as a matter for the state rather than them.
 - **Universities face contradictory demands.** The Senat Report noted that universities were expected to welcome foreign students and pursue more rigorous controls. At the same time, the culture of openness of the university sector means that it is by nature reluctant to view its activity in a context of conflict and national interest.²³³

5. LEGISLATION AND REGULATIONS

The key legislation in France is the Protection du Potentiel Scientifique et Technique de la Nation (PPST).²³⁴ The PPST is a statutory protective security measure for public and private laboratories and manufacturing facilities that contribute to the scientific and technological potential of France. The PPST has been in place in its current form since 2012 and governs physical security, personnel security and the security of information systems.

5.1 Scope

The French approach is governed by the concept of the scientific and technical potential of the nation. This is made up of all the tangible and intangible assets specific to the scientific activity (fundamental or applied) and the technological development of the nation. The mechanism for the protection of the nation's scientific and technical potential (PPST) aims to protect the most "sensitive" knowledge, expertise and technologies of public and private establishments (research laboratories and companies) located in France, the diversion or capture of which could:

- harm the economic and scientific interests of the nation;
- strengthen foreign military capabilities or weaken French defence capabilities;
- contribute to the proliferation of weapons of mass destruction and their means of delivery;
- be used for terrorist purposes on national territory or abroad.²³⁵

5.2 Implementation of the PPST

The PPST is coordinated on an inter-ministerial level by the General Secretariat for National Defence and Security (SGDSN). The SGDSN has an officer in each ministry, called the Senior Defence and Security Officer (HFDS). Six ministries have an HFDS, these are: agriculture, defence, the economy, ecology, research and health. Each Ministry implements PPST in a manner considered appropriate to its specific field.

Each academic or research institution has a Security and Defence Officer (FSD), who reports to the HFDS of the Ministry of Higher Education and Research, creating a network of security-aware individuals. These officials may be full-time in larger organisations, and part-time in smaller organisations.

5.3 Participation in the PPST

Membership of the PPST scheme is based on consultation between the security services and the entity concerned. Whether a research establishment is determined by whether the capture or misappropriation of knowledge, know-how and technologies developed or implemented in its research or development unit can significantly damage its own competitiveness, that of its industrial or scientific partners or the country as a whole, enables the development of a conventional weapon, promotes the development of a weapon of mass destruction or its delivery system or generates a threat due to possible use for terrorist purposes on national territory or abroad.

An establishment can obtain an assessment of the sensitivity of its activities through engagement with security services (DGSi). This consultation aims to consider the specificities of each entity and to consider appropriate protection on a case-by-case basis, according to the risks, and according to the means available.

5.4 Les zones à régime restrictif (ZRR)

The system of restrictive regime zones (ZRR) is the heart of the PPST. A facility covered by the PPST is required to establish a ZRR. The ZRR may cover a laboratory in whole or (more likely) in part. The ZRR is governed by requirements for physical, personnel and information system security.

With regards to **physical security**, the provision requires that the ZRR be an enclosed space with signage at each of its external accesses informing them of the status of ZRR and the criminal consequences to which persons who enter it without authorisation are exposed. Each entity decides, according to its means and needs, whether to deploy additional means of protection (badge reader, surveillance camera, etc.).

Personnel security requires anyone who wishes to enter the ZRR to undergo a vetting procedure, whether they are French citizens or foreign nationals. Only people authorised by the head of the school have the right to physically or virtually access the ZRR, under penalty of being criminally sanctioned. This governs doctoral students, researchers, those following a course that is not part of initial university training, providing a service, carrying out an audit or inspection mission on behalf of a third country, or carrying out a professional activity. Permission to access the ZRR is subject to the authorisation of the head of the department, who in turn must seek permission from the relevant Ministry. The approval system to work in a ZRR should take as little as two weeks, presently, the average response time is shorter period, around 5 days. The problematic cases taking longer, which can cause disruption and complaints to arise^{236 237}. The refusal rate is presently low, at around 2%.

The ZRR also has requirements for information system security. Institutions must implement an information systems security policy (ISSP). The ISSP is an internal document of the institution that disseminates good practices, procedures and sets the objectives of the institution in terms of IT security. This document helps ensure that every user adopts the right IT hygiene habits in order to reduce security incidents and associated costs. The head of the institution must also appoint an information systems security officer (CISO) who is the main point of contact for all questions relating to IT security and is responsible for the implementation of the ISSP.

5.5 Limitations of the PPST system

The 2021 Senat Report noted certain limitations with the PPST system and some of these have been addressed in subsequent reforms.²³⁸

- **The threshold for vigilance is too high.** The PPST only applies to the very high risks of stealing knowledge and expertise (economic and military interests, proliferation and terrorism) and focuses on “hard” sciences and technologies for high-risk. The Senat report argued that the PPST was not suited to new strategies of influence targeting the human and social sciences.²³⁹
- **“A public policy that still lacks full commitment”.** The Senat report characterised the PPST as too weakly coordinated with poorly shared and institutions and researchers who are too often left to fend for themselves. The Report argued that the system suffered from a general lack of resources, coordination and awareness of these new threats by the academic community. This it saw as a sign that detecting and handling foreign influence was still not a priority for public authorities.²⁴⁰
- **Over reliance on the centre.** More generally, we note that the centralised system has the unintended consequence of reducing the feeling of responsibility of academics and institutions. There is a tendency for research performers to see research security as the responsibility of central government.

5.5 Revisions to the PPST

The criticisms expressed in the 2021 Senat report as well as government concerns about lack of compliance with the PPST have led to reforms and especially the introduction of legal sanctions. Criminal penalties have been introduced for non-compliance with the PPST, including fines and imprisonment for breaches of the rules concerning ZRRs.^{241 242 243}

A person who enters a ZRR without authorisation may be liable to a sentence of 6 months imprisonment and a fine of €7,500 (£6,400). A theft or misappropriation of documents or equipment within a ZRR may be subject to up to 20 years of criminal detention and a fine of €300,000 (£256,000). In the event of intrusion into a ZRR, only the offender is likely to be sanctioned. Under no circumstances can the head of the school be sanctioned because of the capture of his knowledge and know-how contained in his ZRR. However, a member of staff may be fined if they participate directly or indirectly in the circumvention of the regulations.

5.5 Screening of research collaborations,

The French system also includes centralised scrutiny of international cooperations and partnerships.

If a research unit is part of a protected scientific and technical sector, the head of the institution must submit all international collaboration projects (framework agreements, memorandum of understanding, etc.) for an opinion from the relevant Ministry. Similarly, the competent departments of the Minister concerned must also be informed of any project for conferences and seminars and registration for training courses relating to the protected scientific and technical sector.

The screening process is established under Education Law. Screening is the responsibility of the Senior Defence and Security Official (Haut Fonctionnaire de Défense et de Sécurité [HFDS]) at the Ministry of Higher Education and Research (HFDS-MESRI). At the university level, an officer

of the Ministry of Defence is meant to be responsible for delivering the contracts for screening to the HFDS. Intelligence services are consulted in the screening process for input on the risks. According to the Leiden report, which refers to the Senate report of September 2021, the screening process has led to 912 files being submitted for revision since 1 January 2019, with a negative review rate of 6.5%.²⁴⁴

This centralised system of review has experienced some capacity issues, not least as an increasing number of projects on emerging technologies such as AI and quantum have emerged. Government has found it increasingly difficult to find sufficient technically competent individuals to review research collaborations. This has led to delays. Moreover, capacity issues are also impacting the HFDS capability to review PPST/ZRR applications and this has led to some unnecessary ZRR designations. Some universities are engaging with HFDS to enhance the capability of central government to more accurately review ZRR applications and research collaboration proposals.²⁴⁵

6. RESEARCH SECURITY MEASURES

6.1 Promoting awareness and forums for dialogue on research security

France conducts **awareness campaigns** at the local level in universities, schools, and research labs, often built with the help of security services. The DGSi emphasises its awareness-raising actions. The DGSi organises, on request, free workshops to raise awareness of the protection of strategic information, during which it describes the most frequent interference actions and the means of protecting oneself from them, in particular by adapting its behaviour and adopting certain simple rules of digital hygiene. The security services also provide awareness raising about the proliferation of weapons of mass destruction and the legal and regulatory framework and best practices aimed at strengthening their protection and preserving their reputation.²⁴⁶

The HFDS and network of FSDs play a key role as a mechanism for knowledge transfer. The DGSi emphasises its regular contacts with French research actors to detect interference attempts and its regular relations with all the players in the world of research and its environment. In particular, the Service collects concerns or reports from researchers, directors of research units or institutions or business leaders concerning possible malicious foreign approaches. Faced with suspicions or proven cases of interference initiated by foreign actors, the DGSi supports the targeted establishment, in conjunction with the defence and security unit and the supervisory authority, in order to identify the best remediation solution. It has significant resources, which are conferred on it by law, allowing it to identify the origin of the attack and the intentions of its perpetrators.²⁴⁷

6.2 Written guidance on research security

There have been several initiatives taken by the Government to increase awareness in the sector and there is guidance provided by universities and the government. The PPST is explained in a wide range of government documents online and each government department provides extensive coverage of the way in which the HFDS operates in relation to that department's activities.

In 2021, the DGSi formulated specific recommendations to safeguard French research institutions from foreign influence, highlighting the exploitation of funding vulnerabilities by malicious actors.²⁴⁸ This included seven key recommendations for institutions, focusing on due diligence, researcher training, and stronger internal vetting procedures. The DGSi and DRSD

jointly issued seven key recommendations to protect French research institutions from foreign interference:

1. **Raising awareness** among researchers about espionage risks.
2. **Implementing due diligence** for international collaborations.
3. **Screening foreign partners**, especially in sensitive fields.
4. **Training personnel** in security and data protection.
5. **Monitoring access to laboratories and data**.
6. **Improving institutional coordination** with national authorities.
7. **Reporting suspicious approaches or contacts**.

The SGDSN provides an online question and answer briefing on the PPST.²⁴⁹

6.3 Mechanisms for advice and information sharing by government

France utilises guidance provided by its Directorate for Defence and National Security, distributed through different Ministries to the research community via the FSDs in each research institution. Importantly, the centralised system advises on personnel vetting for the ZRR and on research collaborations.

The DGSi publishes a [monthly Economic Interference Flash](#), in which it provides recommendations based on real cases of interference. Since 2021, the DGSi has devoted one edition per year to foreign threats that specifically weigh on research structures. The publications can be consulted on the DGSi website and on its [LinkedIn](#) page.²⁵⁰

7. CONCLUSIONS

France has a mature research security system characterised by its centralisation and importance of the PPST and central review of research collaborations. France's system for research security is now being implemented with increasing strictness after a period in which compliance with it was inconsistent.

Appendix 4: Country case study - Germany

1. INTRODUCTION

Germany has a large, complex and mature public research system, with an unusually diverse landscape. In keeping with this large, mature, diverse and decentralised research system the German response to research security has been decentralised and bottom up, with an emphasis on responsibility in science and on ethics and values in collaboration, rather than on top-down rules and compliance.

Germany is at the implementation stage, with widespread awareness of the issue of research security and the introduction of a range of risk management and due diligence processes by a diverse range of universities and public research institutes. Beyond export controls, visa regulations and the existence of investment screening, there is no research security legislation or top-down regulation in Germany. There is not even a single set of national guidelines. However, there appears to be well-developed processes in the research system and a high degree of awareness at least on the part of research leaders.

- Germany is currently undergoing an extended stakeholder dialogue process on research security. The recent election and change of government may slow down this process and may create new demands.
- The direction of travel for German policy seems to be in favour of clearer common guidelines and the creation of a single office or contact point for intelligence and advice.

2. THE NATIONAL SCIENCE SYSTEM, UNIVERSITIES AND PUBLIC RESEARCH BASE

Germany has Europe's largest and most complex mature public research system, and one of the most productive research systems in the world. The German research system has an unusually diverse landscape which is also complicated by the federal nature of the state. Germany was the originator of the modern notion of the research university but is also characterised by mature and very extensive networks of non-university basic and applied public research institutes and facilities. It also has large and well-endowed private foundations that fund and support research. There is a federal research and education ministry (BMBF – since May 2025 succeeded by the Federal Ministry of Research, Technology and Space BMFRT) and an autonomous national funding agency (DFG) which provides project funding for university and public research institutes. However, the universities and universities of applied science are governed by the governments in each of the federal states/Länder. Another unique feature of the German system is the importance of the DAAD, the national organisation for promoting international exchange of students and researchers.

3. ENGAGEMENT IN INTERNATIONAL RESEARCH COLLABORATION

In 2021, there were 75,223 full-time foreign academic staff and researchers employed at German higher education and public research institutions²⁵¹. Since 2017 the number of international academic staff in German universities has increased by around a third²⁵². The key countries of origin for international academic staff at German universities are India, Italy, China, Austria, Iran, Russia, the US, Spain, France and Turkey. Table 1, sourced from Wissenschaft Weltoffen and based on data from Scopus, shows the country of origin of internationally mobile authors with affiliations in Germany for two periods, 2017-19 and 2020-22.

Table 21: Country of origin of internationally mobile authors with German affiliations

	2017-2019		2020-2022	
	Number	%	Number	%
US	3,148	16.3	2,970	14.6
United Kingdom	1,847	9.6	2,123	10.4
Switzerland	1,214	6.3	1,254	6.2
China	944	4.9	1,087	5.3
France	1,084	5.6	1,062	5.2
Austria	993	5.1	914	4.5
Netherlands	883	4.6	912	4.5
Italy	886	4.6	904	4.4
India	569	2.9	713	3.5
Spain	737	3.8	648	3.2
Other	7,027	36.3	7,731	38.1

Source: https://www.wissenschaft-weltoffen.de/content/uploads/2024/11/WWO_2024_EN_aktualisiert_BF.pdf

There were 469,485 international students studying in Germany in 2023-24, up by more than 55% from 2013/14. Roughly two-thirds of these students are registered with universities whilst the other third or so are registered at universities of applied science²⁵³. 31,216 of these students were registered for PhD programmes but the greater proportion (106,306) were enrolled on Masters level degree programmes, with the most popular field of study for international students being engineering - accounting for 43.1% of all international students enrolled in Germany.

Top countries represented among the international student body are India, followed by China, Turkey, Austria, and Iran. International students are attracted to Germany by the high quality of technical education and the low or non-existent tuition fees²⁵⁴. Whilst Turkey is officially the second most important source of foreign students (accounting for around 35,000 students in 2023/24) it should be noted most Turkish students in German higher education are students with Turkish citizenship who took their higher education entrance qualification in Germany and in many cases may even have been born in the country (Bildungsinländer), and that such students have been present as a large group in the German higher education system for several decades.

Much like our other case study countries, Germany has a relatively high level of international co-authorship of research publications by global standards (although somewhat below the levels of the UK and France, and much less when compared to smaller mature European research systems like the Sweden and the Netherlands). According to a 2021 study (using 2018 data from Scopus)²⁵⁵, 56% of the German research system's published research output is internationally co-authored, and more recent analyses of 2022 Scopus data by the US National Science Board provide a similar estimate²⁵⁶. When we correct for the scale of the science system and look at

extra-EU collaborations, in 2022 Germany produced 1207.5 internationally co-authored publications with non-EU partners per 1000 researchers, well behind Sweden and the Netherlands and with a similar level to Spain, Italy and the Czech Republic and somewhat ahead of France.²⁵⁷

Our own analysis using *The Lens* shows that China has become an important partner for co-authorship for German authors. Between 2015 and 2023, the ranking of China as a partner for co-authored research outputs with Germany rose from 8th to 3rd (see Table 2).

Table 2: Top nine international collaborating countries measured by co-publication, three selected years

Top International Collaborating Countries, Three Years, By Count of Documents [Publications]						
Country	Document Count 2015	Country	Document Count 2020	Country	Document Count 2023	
Germany	162160	Germany	195970	Germany	167866	% in 2023
US	22808	US	30517	US	20193	12%
UK	12111	UK	17818	UK	12336	7%
France	8045	China	9917	China	8403	5%
Switzerland	6428	France	9914	Italy	7578	5%
Italy	6259	Italy	9463	France	7389	4%
Netherlands	5692	Switzerland	8942	Switzerland	7317	4%
Spain	4950	Netherlands	8551	Netherlands	6495	4%
China	4717	Australia	6467	Spain	4959	3%
Canada	4554	Spain	6387	Australia	4752	3%

Source: enabled by the <https://www.lens.org/> [lens.org]



4. PERSPECTIVES ON RESEARCH SECURITY

4. 1. Definition of research security

Most German documents do not use the term 'research security' directly, unless they are referencing to or responding to other initiatives, particularly from the European Commission. For

instance, the BMBF's 2024 position paper on research security uses the G7 definition of research security.²⁵⁸

4. 2. Research security threats and threat actors

The approach in Germany as elsewhere is typically threat-agnostic. The initial impetus to consider the ethical aspects of 'security-relevant research' in the context of the dual use dilemma and non-proliferation concerns often emphasised non-state actors such as Al-Qaeda, or states identified as sponsors of terrorism or identified as attempting to develop weapons of mass destruction, such as Iran²⁵⁹.

Interviewees report that the 2018 ASPI report *Picking Flowers, Making Honey* had a big impact in Germany as elsewhere, putting the issue of research collaboration on the political and media agenda²⁶⁰. Then, in 2020, the German Rectors Conference (HRK) produced guidelines on international university co-operation, mainly focused on the need to ensure equal partnerships, adherence to ethical standards and freedom of research and teaching, and a second document which specifically discusses those issues in relation to university co-operation with China.²⁶¹

In 2022 the Joint Committee on the Handling of Security-Relevant Research of the DFG and Leopoldina issued an update to its catalogue of key questions to be used in risk assessments²⁶² and in 2023, in the face of growing media attention regarding ties between German academia and research and China through for instance the Confucius Institutes or through links with the 'Seven Sons'²⁶³, the federal government published its landmark China Strategy, which amongst other things reflected on the threat posed to German research security by China and discussed possible mitigation measures²⁶⁴. Also, in 2023 the DFG produced guidelines on 'Dealing with Risk in International Cooperation', focusing on how risk assessments should be included as part of funding applications²⁶⁵ and the Federal Office for Economic Affairs and Export Control released a manual on export controls and academia²⁶⁶. In parallel to all of this, organisations like the DLR Project Management Agency (part of the German Aerospace Research Centre, one of the Helmholtz system of public research institutes), the DAAD²⁶⁷, and the HRK, continued to develop and share guidance and tools, such as the DLR OPERATE tool for due diligence in research collaboration²⁶⁸.

4. 3. Scale of attention and response to threats

Germany has been grappling with the entwined issues of dual use and research security now for more than a decade. Back in 2014 the German Research Foundation (DFG) and Leopoldina, the national academy of sciences, established a Joint Committee on the Handling of Security Relevant Research and published a set of Recommendations for Handling Security-Relevant Research, an attempt to tackle the 'dual use dilemma'²⁶⁹ which was becoming a point of debate in Germany, mainly in connection with the question of responsibility in science. Article 5 of the German Basic Law protects scientific freedom, and this set of recommendations was framed under the need to balance scientific freedom with scientific responsibility. The guidelines encourage individual researchers to take responsibility by actively risk assessing any 'security-relevant' research and managing those risks appropriately. They also encouraged research organisations to set up ethical committees to advise on such assessments, the Commissions for Ethics in Research, or KEFs.^{270,271}

4. 4. Factors influencing the policy responses of government and research performing organisations

Germany has an unusually mature, diverse and complex research system, with scientific freedom protected in the Basic Law and a ‘civil clause’ in the statutes of many universities which prevents military-related research. Furthermore, Germany is a federal system, and universities are responsible to the Länder²⁷². All of this makes the governance of research security difficult from a top-down perspective even if this was considered politically desirable. At the same time, most actors in the debate have been equally keen to avoid the ‘securitisation’ of research and to avoid any sense of the top-down imposition of ‘red lines’.²⁷³ These concerns arise from sensitivities towards the commitment to scientific freedom and concerns about responsibility in science.

At the same time, research security is being considered in the context of the broader debates about both security-relevant research and the ‘dual-use’ dilemma and about the turning point in geopolitics (Zeitenwende) - symbolised by the Russian invasion of Ukraine and the recognition of China as a systemic rival - which requires new responses including a more strategic and considered approach to research security.²⁷⁴

The federal government itself has shaped the debate through the publication of its China strategy. However, only with the publication of the BMBF position paper on research security in 2024²⁷⁵ has the federal government issued a specific statement of aims regarding research security. Specifically, the BMBF aims to strengthen research security in Germany by reviewing existing instruments and approaches, enhancing awareness, and by critically assessing the traditional separation between civil and military research. The goal is to protect knowledge and technology while maintaining international cooperation under the slogan ‘as open as possible, as secure as necessary’. The paper emphasises eight key considerations: the value of international collaborations for the international competitiveness of German research and innovation, and for overcoming the global challenges of our time; the need to protect scientific freedom; the principle of self-regulation, so that actors in the research system take responsibility for their own informed decision-making; the need for proportionality in research security measures; the need to take a whole-of-government approach, including European and potentially multi-lateral co-operation; the principle of taking a country-agnostic approach; and the need to communicate, monitor, evaluate and learn on an ongoing basis. The paper proposes a debate about the need for clearer national guidelines and a central contact point -type source of advice and support. It also calls for reflection on the division between civil and military research and for a reconsideration of civil clauses, which are present at various levels of the governance system [Land and university]. These and other questions form the basis of an extensive stakeholder dialogue which is ongoing at the time of writing.

5. RESEARCH SECURITY MEASURES

5. 1. Extent of response to research security challenges

Germany has built up a comprehensive but decentralised response to research security. Many different bodies, both on the government and funding side and on the research-performing organisation side of the national research system, such as DAAD and the DLR Project Management Agency, have developed and shared guidelines and advice on the topic of research security²⁷⁶. Germany seems to have caught on to the threats towards research security slightly earlier than other European countries, and the response has been largely bottom-up, from the research system actors themselves.

The Joint Committee of the DFG and Leopoldina can be seen as part of an effort to overcome this lack of coordination, but many actors continue to call for a more central contact point or office to form an interface between the different actors (government, security services, researchers, funding bodies) to improve responses to research security threats²⁷⁷.

Ingrid d’Hooghe and Jonas Lammertink in a report from the Leiden Asia Centre & AWTI (2022) commented that Germany takes:

‘A balanced, comprehensive bottom-up approach that pays attention to the opportunity side and avoids the securitisation of international collaboration. The Federal structures sometimes lead to longer lines of communication, and it lacks one point of coordination for all actions/measures.’²⁷⁸

5. 2. Promoting awareness and forums for dialogue on research security

The Joint Committee keeps track of developments concerning security-relevant research, identifies areas where action is needed and advises researchers and institutions accordingly. It helps researchers/institutions implement research security measures, initially based on the Joint Committee's 2014 recommendations, but since updated in 2022.²⁷⁹ The Joint Committee also supports the local KEFs. By 2022 there were over a hundred KEFs which comprise of interdisciplinary committees within institutions able to provide advice for researchers on security-relevant projects and organise events and awareness raising activities. The local KEFs are able to support researchers quickly and in lieu of institution-specific guidelines but can escalate the issue up the Joint Committee if they need further guidance. However, interviewees felt that KEFs work better in some institutions than others and that more generally some universities were more advanced in their approach than others.²⁸⁰

5. 3. Written guidance on research security

As noted above, there are a range of guidelines and tools available, many developed by funders or research-performing organisations inside of the national research system have developed and shared guidelines and advice on the topic of research security. These include, on the government side, the BAFA Handbook (Export Control and Academia); Handbook of German Export Control (HADDEX)²⁸¹; and on the research system side the DFG-Leopoldina Joint Committee guidelines, revised in 2022²⁸² and the HRK guidelines on international co-operation.²⁸³

5. 4. Mechanisms for advice and information sharing by government

The BMBF has mainly played an informational and awareness raising role²⁸⁴, and hasn’t directly provided national guidelines or formal information briefings but funders and research-performing organisations have been active in doing this.

There has been some discussion in the media, especially after the meeting of the DFG president with US representatives, about Germany creating a new research security organisation modelled after the proposed US NSF SECURE Centre to serve as a central locus for information on research security risks.²⁸⁵

5. 5. Due diligence processes employed by research funders and RPOs

DFG has provided guidelines²⁸⁶ that risk assessments should be written into funding applications, whilst the Humboldt Foundation has published guidelines of its own which follow on from the DFG approach and which apply to Humboldt-funded research²⁸⁷. The non-university basic research institute system, the Max Planck Society, published its own Guidelines for the Development of International Collaborations in 2024, covering specific risk mitigation strategies.²⁸⁸ The applied research institutes system, the Fraunhofer Society, dealing as it does with technological research closer to the market, and working in collaboration with private sector companies, has a very well developed compliance system that considers issues of responsible collaboration, information security and IP protection, research integrity and compliance with legal requirements such as export controls²⁸⁹. It also has its own KEF for the ethical governance of security-relevant research²⁹⁰. The other major system of public research performing organisations, Helmholtz, is a looser network of self-governing institutes. However, some Helmholtz institutes, such as the Germany Aerospace Centre [the 'DLR'], have long experience with research security considerations, and this has prompted the central office of Helmholtz to promote greater consideration of research security across the network, including by funding a programme of research security related projects into which Helmholtz institutes could bid for funding.

The DLR project management agency, as already noted, has developed multiple tools and guidelines for use by research-performing organisations and researchers in due diligence and risk management. The best known of these is the online OPERATE tool, which provides a methodological framework to include scientists in risk assessments and how to weigh up opportunities/risk in cooperations, and it helps to raise awareness and foster exchange amongst stakeholders.²⁹¹ The platform asks the stakeholders to do a self-assessment on risks/opportunities on a sliding scale, and the answers are used to create a matrix which is then used to stimulate a targeted process of opportunity enhancement and risk mitigation.

6. LEGISLATION AND REGULATIONS

6. 1. Export controls

As an EU member state, Germany implements EU legislation and feeds into its future development. It is also a member of various international partnerships and export control regimes centred on particular proliferation issues such as nuclear technology, biological/chemical technology, ballistic-missile and drone technology and conventional military technology. Despite the protection for academic freedom in the German Basic Law and the widespread adoption of 'civil clauses' in German universities, research and academia in Germany must comply with legal obligations.

As already noted, BAFA, the Federal Office for Economic Affairs and Export Control, has produced specific guidance for academia regarding export controls (now in its second edition). This was done in collaboration with research organisations and aims to raise the awareness of individual researchers and universities and RPOs as regards the aims of export controls and to provide advice about how to comply.²⁹² Alongside this sits more specific guidance on export controls and science and research²⁹³.

6. 2. Visa controls and vetting procedures

Germany is a member state of the EU and part of the Schengen Agreement. Visas for short term visits, including potentially by short term research visitors, speakers or conference attendees, are Schengen-wide. On the other hand, working visas (National D-type Work visas) and long-term student visas are issued by individual states with their own criteria, and incoming researchers from non-EU member states would also typically need a residence permit.

6. 3. Investment controls

Investment screening in Germany is governed by the Foreign Trade and Payments Act (Aussenwirtschaftsgesetz, AWG) and the Foreign Trade and Payments Regulation (Aussenwirtschaftsverordnung, AWV). Reviews are carried out by the Ministry for Economic Affairs and Climate Action (succeeded in May 2025 by the Federal Ministry for Economic Affairs and Energy) in consultation with the foreign, defence and interior ministries, but any decision to prohibit an investment would also require the approval of the entire federal government²⁹⁴. Acquisitions carried out through internal restructurings are not subject to FDI screening. On the other hand, asset deals are caught by FDI screening if the acquisition concerns a separable part of a company or all essential operating resources of a company or of a separable part of a company. In common with other EU member states, the German federal government now places greater focus on strategic direct investment by non-EU investors in security-critical European high-tech companies, following the implementation of the regulation on a uniform framework for the screening of foreign direct investment in the EU.

7. CONCLUSIONS

7. 1. Summary

Germany has a large, complex and mature public research system, with an unusually diverse landscape. In keeping with this large, mature, diverse and decentralised research system the German response to research security has been decentralised and bottom up, with an emphasis on responsibility in science and on ethics and values in collaboration, rather than on top-down rules and compliance. Beyond export controls, visa regulations and the existence of investment screening, there is no research security legislation or top-down regulation in Germany. There is not even a single set of national guidelines. However, there appears to be a well-developed debate in the research system and a high degree of awareness at least on the part of research leaders.

7. 2. Future directions for research security in the country

In 2024 the federal government welcomed the European Council recommendation on research security. Many German organisations had responded to the consultation, with a consensus that clearer guidelines and more consistency across the EU would be welcome but that there must always be an element of responsibility on the part of individual researchers to make their own assessments and decisions. Most respondents approved of the country-agnostic approach, but many noted that this also needed to be complemented by country-by-country guidance and by country specific risk assessments. In general, whilst the prevailing approach in Germany is to be country-agnostic, the German discourse has often been about China in the context of the Zeitenwende or turning point.

There has been some discussion in the media, especially after the meeting of the DFG president with US representatives, about Germany creating a new research security organisation modelled after the proposed US NSF SECURE Centre to serve as a central locus for information on research security risks.²⁹⁵ The national ‘stakeholder dialogue’ on research security is still continuing, and some of our interviewees speculated about the creation of a central team or advice point out of this process, although the widespread consensus was that enforced ‘red lines’ remain overwhelmingly unlikely in the German context. In the absence of a central advice point like SECURE or RCAT or the Dutch NCP, there remain multiple sources of guidance and support, and a range of tools offered to support due diligence and risk management, such as OPERATE.

Appendix 5: Country case study - Italy

1. INTRODUCTION

Italy has been a late adopter of research security policies and practices. The country is at what we characterise as the Realisation Stage. There is an emerging awareness of research security issues and some signs of a mixture of top-down initiatives and some sector-led and bottom-up activity. A National Plan is in development and in early 2025 ‘a model for Italy’ was at the consultation stage.²⁹⁶

Major developments in the development of research security are as follows:

- A 2024 national survey of research security practices of universities and public research institutes was conducted by the Ministry of University and Research and underpins the government’s current approach to the development of a plan for research security.
- G7 meeting July 2024 and G7 meeting on research security and research integrity in Bari in December 2024.
- Development of the national plan in 2025 following consultations with university leaders and more broadly in early to mid-2025. It is likely that the plan will be implemented no sooner than 2026.²⁹⁷

2. THE NATIONAL SCIENCE SYSTEM, UNIVERSITIES AND PUBLIC RESEARCH BASE

The Italian Ministry of University and Research database shows 110 higher education institutions in the country.²⁹⁸ There are around 109,000 research and academic staff across the sector.²⁹⁹ Research outside the university system occurs both in public and private laboratories.

The main public research facilities are the Italian Space Agency (ASI), the National Research Council (CNR), the Italian Institute of Technology (IIT). The CNR has 88 research institutes which it funds, and it employs over 9000 staff of whom just over half are researchers³⁰⁰. The CNR also has researchers located in other organisations. Its staff conduct research in many of the EU ten critical technologies.³⁰¹ Likewise the IIT also has satellite research facilities located around Italy. The IIT funds research in several sensitive areas, quantum, nanomaterials, RNA, and robotics. The IIT’s strategic plan for 2024 to 2029 shows around 1500 researchers employed across its activities/sites.³⁰²

3. ENGAGEMENT IN INTERNATIONAL RESEARCH COLLABORATION

The Italian higher education sector lags in internationalisation by European standards. While Italian students are highly mobile to other European countries, and beyond, Italy registers comparatively few international students, and the share has remained stable between 2019 and 2021. International students comprise 3% of undergraduates and around 10% of doctoral students.^{303 304} The share of international academic staff in higher education institutions is also low, at around 4% in the last year for which we could find data (2016)³⁰⁵.

Much like our other case study countries, Italy has a relatively high level of international co-authorship of research publications by global standards (although below the levels of the UK and

France, and much less than smaller mature European research systems like the Sweden and the Netherlands). According to a 2021 study (using 2018 data), 51% of the Italian research system's published research output is internationally co-authored.³⁰⁶ More recent analyses of 2022 data by the US National Science Board provide a similar estimate of 50%³⁰⁷. When we correct for the scale of the science system and look at extra-EU collaborations only, in 2022 Italy produced 1137 internationally co-authored publications with non-EU partners per 1000 researchers, well behind Sweden and the Netherlands but with a similar level to Germany, Spain, and Czech Republic, and somewhat ahead of France³⁰⁸.

Our own analysis using *The Lens* shows that the US remains the most frequent partner for international co-authorship with researchers with Italian affiliations, followed in all three of our snapshot years by the UK. China has become a more important partner over time, though with numbers comparable to collaboration with Switzerland.

Table 13: Top nine international collaborating countries measured by co-publication, three selected years

Top Nine International Collaborating Countries, Three Years, By Count of Documents [Publications]						
Country	Document Count 2015	Country	Document Count 2020	Country	Document Count 2023	
Italy	91799	Italy	130657	Italy	121367	% in 2023
US	15563	US	23481	US	13563	11%
UK	8023	UK	13189	UK	9783	8%
Germany	6259	Germany	9463	Germany	7578	6%
France	5457	France	8092	France	6690	6%
Spain	3941	Spain	6783	Spain	6013	5%
Switzerland	3169	Switzerland	4892	Switzerland	4127	3%
Netherlands	2933	Netherlands	4826	China	4066	3%
Canada	2496	Canada	4497	Netherlands	4065	3%
Australia	2075	China	4160	Canada	3365	3%

Source: enabled by the <https://www.lens.org/> [lens.org]



4. PERSPECTIVES ON RESEARCH SECURITY

4. 1. Definition of research security

There is no widely accepted definition of research security in use in the university sector in Italy. We note that the Ministry of Universities and Research used the European Commission's definition in its survey of Italian research performing organisations.

4. 2. Research security threats and threat actors

4. 2. 1. Research security threats

The Ministry of Education and Research presentations to the G7 conference on research security provide an overview of the country's understanding of current threats to research security. Public reporting of the stance of the government indicates long-standing concern with theft of IP from Italian firms and universities and concerns also on disruption of the activities and infrastructure of research actors including from cyberattacks.³⁰⁹

4. 2. 2. Threat actors

Recent statements by Italian government officials state that the government's approach is 'country agnostic.' As a new report quoting the views of several ministers in late 2024 gives a sense of government thinking.³¹⁰

"When asked about potential adversarial actors, Mantovano responded, "There is no list of unsafe countries; we maintain vigilance across the board."

Minister for Universities and Research Anna Maria Bernini reinforced a neutral stance, stating, "This plan is not against any country; it is a protective measure for our research."

She stressed that there are no inherently good or bad countries, only practices that can be either good or bad.

Bernini highlighted Italy's continued collaboration with China, citing a recent memorandum between her Ministry and its Chinese counterpart focused on artificial intelligence and cultural heritage as evidence of positive engagement."

It remains the case however that the Italian government of Meloni has been clear in its efforts to de-risk in relation to China, however this has been undermined by deepening investment and trade dependencies and a bottom-up approach from industry that has caused ties not to weaken but to growth in strength. The approach outlined by Casarini which indicates an attempt at accommodation between Italy and China until around 2021, indicates that the relationship between the two countries depends significantly upon the position of the Italian government.³¹¹

The Italian academic sector, according to the European Think-Tank Network on China Report has opposed the idea of de-risking, and as the sector currently has autonomy on matters relating to cooperation with international partners, there has been no attempt to introduce guidelines on involvement China either companies or universities.³¹² It was noted by one interviewee that as recently as 2020, Italy and China were collaborating on the development of the international space station.³¹³

4.3 Scale of attention and response to the threat

Research security has not received much political or media attention in Italy. Nonetheless, there is growing awareness of the issue within government and research performing organisations. The Ministry of Universities and Research (MUR) conducted a survey of research performing organisations and found that that around 90 per cent of Italian research institutions and universities acknowledge a growing need for research security, particularly concerning risks tied to foreign interference, ethical violations, and intellectual property threats.³¹⁴

Despite the acknowledgement of this risk, only a very small number of institutions have established protocols and procedures to deal with research security.^{315 316} The survey uncovered strong support for a coordinated national approach and a demand for comprehensive, up-to-date guidelines in view of the European Council Recommendation on research security.

In early 2025, the Italian Government announced plans to implement a National Plan for research security, but it is unlikely that the plan will be fully in operation until at least 2026. At the time of writing, the proposals had reached the representative body of the country's universities, and this body will review the proposals before wider consultations on it begins. A recent report in the national press carries news of the imminent introduction of the system.³¹⁷ The Ministry of Research also outlines the policy process in which it is engaged.³¹⁸

4. 4. Factors affecting the policy responses of government and research performing organisations

We identified several factors that are influencing the Italian approach:

- **Fragmented governance and bureaucratic complexity:** Italy has a historically fragmented research and innovation system, split across multiple ministries. This fragmentation hampers a coordinated national approach to research security although the Ministry of Universities and Research appears to have taken the lead on policy coordination.
- **Membership of the G7 and EU.** Italy's membership of the G7 and EU have shaped its response to research security. Italy's Presidency of the Group of Seven included the Bari Conference on research security in late 2024 and stimulated some activity. Likewise, the process leading to the European Council Recommendation has also required an Italian response.
- **Autonomy and decentralisation.** Italian universities enjoy high levels of institutional autonomy, especially regarding international collaboration. This autonomy makes top-down implementation of national security policy challenging.
- **Lack of awareness and expertise.** Many universities have limited awareness or expertise on research security, particularly outside STEM fields. There are often no dedicated staff or internal policy for managing risks related to foreign interference. There are few controls within universities at research grant application stage and it would appear no controls that compulsorily apply a test of the threat to organisational research security at any stage. This is however set to change as we describe below. Universities participating in Horizon Europe are required to adhere to certain ethical and security standards and these requirements may nudge institutions toward better research security practices, but enforcement is uneven.
- **Priority on internationalisation and funding.** Italian universities are highly motivated to internationalise, particularly due to constrained domestic funding. This leads to openness to partnerships with Chinese and other non-Western institutions, even in sensitive fields.
- **Bottom-up initiatives.** In some cases, research security practices are emerging through bottom-up efforts (e.g., individual researchers flagging concerns, or ethics committees reviewing international partnerships). However, these efforts are patchy and informal.

5. RESEARCH SECURITY MEASURES

5. 1. Extent of response to research security challenges

Our evidence of the response is that universities are waiting for the government initiative from the Ministry of University and Research to take effect, and that awareness and readiness to act by organisations begins from a low base.

5. 2. Promoting awareness and forums for dialogue on research security

The Ministry of University and Research organises awareness and engages with European efforts. At a lower level, the relatively newly created Italian Association of Research Managers [‘RMA’] has begun discussion of research security within university sector. RMA has worked with the European Research Managers Association [‘EARMA’], and engages with it on research security, promoting past events on research security by EARMA, a body with which the UK is closely associated.³¹⁹ The UK government Science & Technology Network supported an event on research security with the RMA.

5. 3. Written guidance on research security

At the moment, the country has no national or sector-based guidelines. Initial responses to the Ministry of University and Research (2024) survey indicate that even on an institutional level, Italian HEIs lack guidelines on risk assessments and how to mitigate research security risks.

For example, 81% of university respondents said their organisation does not have policy/guidelines in place to ensure research security. 71% of university respondents said that their institution did not train relevant personnel on research security issues (i.e. did not do any internal awareness raising). They do however have research integrity guidelines, e.g. the CNR - Research Ethics and Integrity Committee (2019) ‘Guidelines for Research Integrity’. There are some references to research security, e.g. data theft, but they are limited in scope.

5. 4. Mechanisms for advice and information sharing by government

The development of formal mechanisms for advice sharing with universities is anticipated in the plan announced by the Government for the system discussed below under 5.6 which is intended to be implemented some time in 2026.

5. 5. Due diligence processes employed by research funders and universities

The MUR survey showed that 81% of university respondents said their institution does not have a clearly defined process for identifying, documenting, or reporting risk. 88% of university respondents said their institution did not have established international travel policies.

At the moment, action to assess risk from threats to research security is, to our knowledge, undertaken by universities on an ad hoc basis. We note that there are pre-existing mechanisms in the form of university committees to review matters relating to research, mainly ethical issues, and these committees are being used to consider instances of where there are concerns about research security.^{320 321} These interviews provide us with evidence of such ad hoc processes being used, but we do not know about their full extent across the sector, their coverage of actual instances of research security threat or their level of effectiveness.

5. 6. Implementation of risk security management

A press release from the Ministry of University and Research outlines its plans that are to begin operating in 2026, in conformity “with European needs and international best practices”. This system will create an “Italian Model” that will cover both safety and integrity of research. It will have guidelines disseminated through the ministry of university and research portal, where training and capability building materials will also be available.

The press release continues to describe in more detail what the national model will include. It is foreseen that what are termed ‘research activity managers’ are to complete a self-assessment form indicating the level of risk that they believe will arise from the work that is planned. This self-assessment will apply to any research in the 10 sectors identified by the EU.³²²

The origin of any public or private funds supporting the research will also need to be reviewed and any partnerships with external bodies. Those applying for research will use a traffic light system to categorize their research although it is not clear how the categorization will be applied. Three types of research risk level will be used, a green light will identify research that is safe; yellow requires caution and further review; while red light necessitates a thorough risk evaluation which will require referral to a dedicated national reference centre. This centre is not yet operational.

The Ministry of University and Research will convene a national conference prior to the experimental phase which will trial the system. No date has been set for the start of any trial. Attendance at the national conference will be on a voluntary basis.

In bringing forward this plan, the Ministry states that it is ‘working collaboration with the Conference of Rectors of Italian Universities (CRUI) and the Council of Presidents of Public Research Institutions (CoPER)’ and that the outcome of the initiative will strengthen the autonomy and freedom of research, while enhancing international cooperation and competitiveness.’

Where individual universities have internal committees, such as ethical committees to review grant applications, their remit does not necessarily extend to review of applications that might involve dual use technology. In technical universities in Italy, the commercialization route for technology developed from research may lead to spin-off firms. In one university reviewed, it was noted that universities would not then have control over export activities of those spin-off firms.³²³

The measures proposed we have heard from interview and from a documentary source are a bottom-up approach with individuals taking responsibility for compliance with research integrity and research security. Responsibility for assessing the research security threat to a piece of research to be undertaken or a collaboration will be given to the principal investigator [‘PI’] in each case. The PI will then have to assess the level of threat on a tripartite scale. What the levels specifically define is not yet public knowledge. The PI will do their assessment by referring to internal experts. In one university we interviewed, there is a plan to create a committee, which will combine an existing committee membership with a new team that will provide the advice to the PI on the need to assess the planned research. This approach is termed ‘self-assessment’, and the responsibility is with the researcher.^{324 325}

We understand that other universities may adopt a similar system. If the risk is assessed at beyond a certain threshold, it will be necessary for the PI to submit the research proposal and their assessment to the Ministry of University and Research. This will check the proposal and, if necessary, make recommendations. We do not know the form of such recommendations, other than that they may include a ‘revise and resubmit’ option. No sanctions are currently planned in this system, but one interviewee believed that they would be necessary.³²⁶

6. LEGISLATION AND REGULATIONS

6. 1. Export controls

As noted above, Italian universities may engage in commercial activity, but an interview indicated that once a spin-off firm had been created, the responsibility for its activity in the area of export of technologies was then a matter for the company and not for the university. Hence, in the case of one of our university interviews, there are no measures present on export controls.³²⁷ However, in another university, there was clearly a system designed to provide control of exports as in that institution, the export control regulations were considered to apply.³²⁸

6. 2. Visa controls and vetting procedures

Our understanding is that within the visa control process we are unsure as to the extent of checking by the Ministry of the Interior of the potential of a research threat from applicant. In Italy, there is a large number of researcher visa applicants from around the world and a large proportion of applications come from Asia. At present the volumes of applications are significant and hence the time needed to process them is long, causing delays and difficulties in universities and for the applicants.^{329 330 331}

The visa process does not apply to all countries. EU citizens do not require them. Those with residency rights in the EU may not require a visa to work under certain conditions, in Italy, and so therefore may avoid a security check. The visa process applies to both staff and students.

6. 3. Investment controls

There is some awareness of the need to control the ownership and the products [IP – patents, trade secrets etc.] of university spin-off university owned businesses at one of the universities we interviewed.³³² Also, at that university there are arrangements to ensure that legal protections for output are in place to protect IP from the malign intentions of outside investors. To what degree such protections are widespread in Italy we are unaware.

7. CONCLUSIONS

7. 1. Summary

The Italian research system is moving towards the introduction of a national approach to research security which will be operational at some point in 2026 although no definite date has been set. The Ministry of University and Research is leading on research security issues within the Italian government and has discussed the issue with other government ministries. Local approaches within universities are emerging but these wait to some degree upon the creation of a national system, and they are ad hoc.

There is not currently therefore either a large scale formal national system or well-established local organisational systems to raise awareness of threats to research security, to identify such threats, respond to them, to report and monitor them, and to establish sanctions in the instances of breaches of any rules.

Important within universities is the research managers association, which is well connected internationally, including being well-networked into the UK, but its research security role is limited

as it has wide remit, part of which is to establish the role of research management within universities and research security is just one part of its role in establishing the profession.

7. 2. Future directions for research security in the country

Italy will roll out a system for research security during 2025 and 2026 on the current expectation. The relatively slow response of the Italian system is difficult to attribute to one particular cause. It is however clear that the response now being made is the result of needing to act in light of European Union initiatives on research security and the G7.

Appendix 6: Country case study - The Netherlands

1. INTRODUCTION

The Netherlands is a mature, open and highly internationalised research system with a well-developed approach to research security that combines top-down guidance and support through the National Contact Point with an increasingly mature infrastructure for awareness raising, ethical and compliance guidance and support within most research-performing organisations. As in the UK there are concerns about the ability of universities to meet the increasing costs of taking an active approach to research security concerns, there is ongoing debate about the effectiveness of the Dutch approach and there are ongoing calls for clearer guidance and better intelligence. However there appears to be widespread agreement that the approach of trying to understand and reduce risks rather than avoid them is the best way to balance openness and scientific freedom with research security.

2. THE NATIONAL SCIENCE SYSTEM, UNIVERSITIES AND PUBLIC RESEARCH BASE

The Netherlands has a very well established and highly productive public research base, with both strong university research and notable non-university public sector research-performing organisations. More than 60% of directly publicly funded research is conducted within the 14 main research-active universities³³³ whilst the remainder is conducted within non-university research organisations such as TNO, the Netherlands organisation for applied scientific research.

Like the UK the Netherlands has evolved a complex governance arrangement for publicly funded research. There is a Ministry of Education, Culture and Science (OCW) but other ministries also fund research and sponsor research performing organisations, and the Ministry of Agriculture, Nature and Food Quality (LNV) even sponsors its own university, Wageningen. The Dutch National Research Council (NWO) has primary responsibility for funding basic research projects, although most public funding for universities goes directly in block funding from the OCW to the universities. Other key actors are KNAW, the Royal Netherlands Academy of Arts and Sciences, Universities of the Netherlands (UNL) and the Association of Universities of Applied Sciences (VH). Many of these organisations come together in the Netherlands Knowledge Coalition.³³⁴

3. ENGAGEMENT IN INTERNATIONAL RESEARCH COLLABORATION

The higher education system in the Netherlands is one of the more highly internationalised in Europe. Between 2003 and 2023, the share of international scientific personnel in universities increased in all scientific fields, reaching 59% in Engineering (compared with the field with the lowest share, Law, with 28.4% in 2023)³³⁵. Around 61% of international staff come from Europe (EEA and non-EEA)³³⁶. There were 122,287 international students studying on degree programmes at publicly funded universities in 2022-23, 15% of the total student population. 27.7% of these international students came from outside the European Economic Area³³⁷. Meanwhile, the proportion of international PhD students with an appointment at a NL university (the vast majority of PhD students are employees) increased from 37.2% in 2007 to 56.1% in 2023³³⁸, with 54.6% of those coming from outside the EEA.

In terms of international collaboration, the Netherlands again is highly internationalised research system by European standards, ranking second only behind Sweden in the share of international co-publications with non-EU partners per 1,000 researchers. According to a 2021 study (using 2018 data)³³⁹, more than 65% of the Netherlands research system's published research output is internationally co-authored, and more recent analyses of 2022 data by the US National Science Board produce an estimate of 67%.³⁴⁰

Work by the Rathenau Institute shows that the number of Dutch-Chinese co-publications increased by 400% between 2010 and 2020.³⁴¹ Our own analysis using *The Lens* shows that China has become a more important partner for co-authorship for Dutch authors between 2015 and 2023, with the country ranked as the 5th most frequent partner in that year. In 2015 China was not in the top 10 of country partners for international co-authorship with Dutch authors (see Table 1).

Table 1: Top nine international collaborating countries measured by co-publication, three selected years

Top Ten International Collaborating Countries, Three Years, By Count of Documents [Publications]						
Country	Document Count 2015	Country	Document Count 2020	Country	Document Count 2023	
Netherlands	52144	Netherlands	65306	Netherlands	61935	% in 2023
US	9540	US	13809	US	9887	16%
UK	6773	UK	10352	UK	7557	12%
Germany	5692	Germany	8551	Germany	6495	10%
France	2963	Italy	4826	Italy	4065	7%
Italy	2933	France	4255	China	3714	6%
Belgium	2713	Belgium	4190	France	3381	5%
Australia	2352	Australia	4024	Belgium	3276	5%
Switzerland	2091	China	3819	Australia	3142	5%
Canada	2051	Canada	3447	Spain	2812	5%

Source: enabled by the <https://www.lens.org/> [lens.org]

4. PERSPECTIVES ON RESEARCH SECURITY

4. 1. Definition of research security

The Dutch concept of ‘knowledge security’ is somewhat broader than the UK’s concept of ‘research security’. More specifically, the Dutch conception encompasses an explicitly ethical dimension of responsibility in international research collaboration and dissemination in relation to fundamental values such as respect for human rights or the rule of law. Knowledge security is thus seen as comprising three aspects: (1) the undesirable transfer of sensitive knowledge and technology (2) the covert influencing of education and research by state actors (3) ethical issues in collaboration with countries who do not respect fundamental human rights.

The 2022 National Knowledge Security Guidelines³⁴² provide the following definition (in English):

“...knowledge security refers primarily to preventing the undesirable transfer of sensitive knowledge and technology with negative implications for our national security and ability to innovate. It also involves covert activities aimed at influence and interference activities on the part of state actors within the context of higher education and science. Such foreign interference can lead to forms of censorship (including self-censorship), thereby resulting in the impairment of academic freedom. Finally, knowledge security concerns ethical issues relating to collaboration with individuals and institutions from countries in which fundamental rights are not respected”.

The definition appears to be widely accepted throughout the public research system, as evidenced both by our desk research and interviews with actors from across the system. And the commitment to including the ethical and responsibility dimension is strongly evident from our interviews with university actors and from Dutch responses to the European Commission’s 2024 consultation on research security³⁴³. However, the scope of the definition of knowledge security does remain open to debate: for instance, a 2023 KNAW position paper³⁴⁴ notes that the breadth of the concept can cause problems and may risk sidelining consideration of ethical risks in favour of concerns about economic security and dual-use technologies.

4. 2. Research security threats and threat actors

The Dutch National Knowledge Security Guidelines (2022) are country-agnostic in their approach.³⁴⁵ However, there is a broad and explicit acknowledgment in the research system that China poses an increasing risk to both Dutch and European research, and these concerns have been a key driver of the development of thinking around knowledge security. Within the last five years or so the Leiden Asia Centre (2020) and the Hague Center for Strategic Studies (HCSS, 2019) have both produced China-specific guidelines for universities.³⁴⁶ Both are explicit about the perceived threat posed by Chinese actors. A more recent report from Clingendael (2024) focused on the China Scholarship Council (CSC) as a particular threat both to the Chinese students themselves who were subject to monitoring - and thus liable to self-censor - and to Dutch universities who may suffer from undesirable knowledge leakage.³⁴⁷ The report called for clear and specific guidelines for Dutch knowledge institutions in relations to CSC funded students. It is also worth noting here that the National Knowledge Security Contact Point (or Help Desk) has received the most questions about collaborations with Chinese, Russian and Iranian partners.³⁴⁸ This trio of supposed threat actors is repeatedly mentioned in news reports about threats to the Dutch research and tertiary education system.³⁴⁹

4. 3. Scale of attention and response to threats

As noted above, the Dutch debate about research security threats has been developing over the past half decade or more. In 2018, the Leiden Asia Center published its first report into Europe-China educational and research collaboration, following up with a second in 2020³⁵⁰. Unwanted technology transfer in the context of national and economic security and clashes of fundamental values was noted as a risk in the 2019 government strategy on rebalancing the NL relationship with China.³⁵¹ In the same year the Rathenau Institute published ‘Knowledge in the Sights’,³⁵² which raised the issue of the economic, national security and ethical consequences of unwanted knowledge transfer, and the HCSS published the aforementioned checklist for collaboration with Chinese universities and research institutions.³⁵³ At the end of that year the Ministers for Education, Justice and Security and Economic Affairs wrote a joint letter to parliament responding to these concerns and announcing the initiation of a dialogue with research system actors and government bodies to raise awareness and inform the development of workable guidelines that would respect fundamental principles of institutional autonomy and academic freedom, and which would build on the work of Leiden Asia, Rathenau, HCSS and others, and be informed by prior and parallel developments in countries like the Germany, Sweden, the UK, Canada and Australia. The letter also confirmed the creation of what became the National Contact Point, and promised the development of a screening framework for high risk topics and disciplines that would focus on foreign researchers and students who would have access to data, knowledge, technology and infrastructure in those areas, performing a similar function to the UK ATAS system.³⁵⁴

The 2022 National Guidelines were developed in collaboration between research system actors and government - specifically a collaboration of the Dutch central government (Rijksoverheid) with Universities of the Netherlands (UNL), the Royal Netherlands Academy of Arts and Sciences (KNAW), the Dutch Research Council (NWO), the Netherlands Federation of University Medical Centres (NFU) and the federation of applied research organisations (TO2 Federation).³⁵⁵ These actors also serve as initiators and facilitators of the self-regulation of the sector. Alongside the publication of the guidelines came the introduction of the defining feature of the Dutch response to security issues in academia: the National Knowledge Security Contact Point (sometimes referred to as the Knowledge Security Help Desk). The Contact Point stems from a collaboration of various Dutch government ministries and agencies and offers a central point of contact for knowledge institutions and individual researchers who require help on issues pertaining to risk assessments, due diligence and broader knowledge security.³⁵⁶

The National Contact Point is widely and increasingly used within Dutch academic circles. However, queries appear to be becoming more complex: in 2023 *Times Higher Education* reported that the Dutch education minister Robbert Dijkgraaf stated, in a letter to parliament, that there had been “a significant increase in the number and complexity” of questions to the Contact Point from universities, with the implication that this was part of the rationale for the introduction of the new screening legislation (see below). The minister also reportedly noted that the advice of the Contact Point was non-binding, and that there was no mechanism for follow up to see whether universities had taken steps to lessen the collaboration risks they raised in their queries. Meanwhile, the same article reported that some Dutch parliamentarians were concerned about inconsistency in the response of universities to National Guidelines.³⁵⁷ From the perspective of the research performing institutions, the rise in volume may be driven by increased awareness by staff and managers, whilst the change in the balance of workload towards more complex queries may reflect the fact that knowledge security teams (and maybe even researchers and groups) within research organisations are increasingly confident in being able to deal with the more straightforward queries themselves.

4. 4. Factors influencing the policy responses of government and research performing organisations

- Geopolitics and changing threat assessments. The Dutch intelligence service (**AIVD**) has played an active role in shaping public discourse and policy, issuing warnings about foreign interference in academia. Its reports have increased political and institutional awareness
- **High internationalisation and global partnerships.** Dutch universities are among the most internationalised in Europe. This creates tensions between the values of open science and the state's push for strategic caution, particularly in STEM fields.
- **Growing awareness and institutional responses:** Awareness of research security has grown significantly since 2020. Most universities have now appointed knowledge security officers, revised ethics procedures, and implemented due diligence frameworks for international collaborations.
- **Balancing academic freedom and risk:** Dutch universities are vocal about the need to maintain academic freedom and resist overly restrictive policies. The Association of Universities in the Netherlands (UNL) has lobbied for proportionate, evidence-based measures.
- Universities and research performing organisations have had different journeys with respect to research security depending on their research intensity and topic/discipline coverage. As in other countries, universities of applied science and applied RPOs working in areas that might be covered by export controls have had processes for advising researchers and prospective researchers.
- In some cases, institutions had their awareness raised because of specific incidents with individual researchers or prospective researchers whilst others became aware of attempts to coerce staff or students into transferring knowledge or attempts to access data from computer systems.
- Some individuals, research groups, centres and organisations have been exposed to media and/or political criticism when found to be in receipt of funding from countries seen as security or economic competitors or where fundamental human rights are not respected.
- These kinds of experiences and the changing discourse at the national and European level, plus exchange of experience and practice through sector representative bodies such as LERU have raised the awareness of research-performing organisations, whilst the publication of the 2022 Guidelines reinforced the need to take action with respect to establishing or strengthening knowledge security teams within the organisation.
- As with other countries we see knowledge security teams growing out of pre-existing capability regarding matters such as export control compliance, research internationalisation or cybersecurity³⁵⁸. Respondents tended to agree that the technical universities, and especially the larger ones, have tended to be a bit ahead of the game with respect to establishing a team and practices of proactively mapping potential risks, internal awareness raising and guidance³⁵⁹.
- As the national debate evolves and grows in intensity, especially in parliament and the media, research performing organisations become ever more aware of the issues around knowledge security.

5. RESEARCH SECURITY MEASURES

5. 1. Extent of response to research security challenges

The Netherlands appear to have a comprehensive and advanced response to knowledge security issues. They have clearly defined guidelines, consensus on the definition/conceptualisation of ‘knowledge security’, a generally good level of engagement between the research system actors and governmental actors and clearly implemented strategies (e.g. the National Knowledge Security Contact Point) to try to tackle the issues. A CESAER report resulting from a workshop on research security in December 2023, acknowledged that in comparison to other European countries – it names Switzerland and Belgium – the Netherlands is an example of a country in the more advanced stages of ‘the development of approaches, guidelines and tools’.³⁶⁰

This does not mean that the system is perfect either in principle or in practice, and in practice the universities have had a varied response to the National Guidelines, with the uptake being slower for some than for others, whilst as noted above, the advice of the National Contact Point is non-binding and compliance is not tracked.³⁶¹

5. 2. Promoting awareness and forums for dialogue on research security

The Netherlands has a very well developed set of relationships for discussions of issues relating to research and science policy in general, with the an Advisory Council for Science, Technology and Innovation (AWTI) which is functionally equivalent to the UK Council for Science and Technology, along with organisations representing scientists and research-performing organisations, such as the Royal Netherlands Academy of Arts and Sciences, Universities of the Netherlands (UNL) and the Association of Universities of Applied Sciences (VH). The key research system actors also come together in the Dutch Knowledge Coalition³⁶². It is also worth noting that the NL research system has a unique attribute in the presence of the Rathenau Institute, which exists to inform public and political opinion on socially relevant aspects of science and technology by monitoring the research system and organising debates on science, innovation, and new technologies.³⁶³ One illustration of how these bodies and forums help to inform the debate in the NL is the work by the Rathenau Institute on NL collaboration with the China science system³⁶⁴.

5. 3. Written guidance on research security

The 2022 National Guidelines, as noted above, were produced in collaboration between research system actors and the government (specifically a collaboration of UNL, KNAW, NWO, the Netherlands Federation of University Medical Centres (NFU) and the federation of applied research organisations (TO2 Federation).³⁶⁵ It is worth noting that whilst international actors tend to point to the NL as being advanced in relation to the development of ‘approaches, guidelines and tools’,³⁶⁶ the Dutch consultancy firms Oberon and Dialogic suggested in 2023 that more government guidance/regulation was needed to ensure better uptake of knowledge security measures. At the same time, they also note that European and international agreements on knowledge security are needed to ensure that Dutch academia does not lose talented researchers to foreign institutions with less stringent security measures.³⁶⁷

5. 4. Mechanisms for advice and information sharing by government

The principal mechanism for advice and the sharing of insights about specific risks is the National Contact Point or Help Desk, which combines insight and intelligence from different ministries and agencies into a single response to a query from a university or individual researcher.³⁶⁸ As noted above, the Contact Point is widely, and increasingly, used.

5. 5. Due diligence processes employed by research funders and universities

As already noted, research performing organisations differ in their experience with knowledge security, though all have had some response to the 2022 National Guidelines. Some universities have a single full-time equivalent in a knowledge security role whilst others have a small team – the largest we are aware of is 5 FTE. However, in most cases, dedicated officers are combined with other staff members, academic or professional, who have partial responsibilities relating to knowledge security. Importantly, research performing organisations are in effect meeting the increasing costs of knowledge security work themselves. Although our government respondents were under the impression there is some allocation for knowledge security within the general block grant for universities, they also acknowledged that these block grants themselves have been declining³⁶⁹.

In 2023, in response to a request from parliament, OCW (the education and science ministry) undertook a baseline review³⁷⁰ of university responses to the 2022 National Guidelines. According to UNL, this baseline review shows that all universities have carried out risk analysis, identified possible vulnerabilities related to sensitive areas of research, funding sources and country of origin of cooperation partners.³⁷¹ According to UNL, awareness of knowledge security has increased and universities were working to raise awareness further amongst their members, whilst some universities had taken new steps to provide guidance for researchers, to examine ongoing international partnerships, and to take knowledge security into account in recruitment and selection procedures. The review also shows that 12 of the 14 universities had established a Knowledge Security team in response to the Guidelines. Government respondents stressed to us the importance of proportionality in terms of managing the risks around research security, recognising that some institutions are exposed to greater risk than others because of research intensity or subject mix.

Nonetheless, in response to public criticisms that universities are not consistent in their response to the National Guidelines on Knowledge Security, and in response to a report from the Advisory Council for Science, Technology and Innovation (AWTI) in November 2022 entitled ‘Knowledge in Conflict’³⁷², which called on research organisations to strengthen their knowledge security teams and processes, the universities (through UNL and with the support of the consultancy firm Dialogic) took the initiative to develop a Knowledge Security Capability Maturity Model, published by UNL in April 2024.³⁷³ The aim of the model is to support universities in designing and implementing their knowledge security policies, to help them assess the level of maturity of each aspect and work towards increasing the maturity of each aspect, and thus to improve the alignment of knowledge security policies and practices across the universities in terms of conceptualisation and focus areas. The key aspects covered are: protection of academic values; the governance and policy framework around knowledge security; compliance with legal requirements (sanctions and export control); risk assessment; risk management; training and awareness; international partnerships, procurement and contracting; human resources; and cybersecurity.

6. LEGISLATION AND REGULATIONS

In 2022 the aforementioned AWTI report³⁷⁴ called on government to provide more specific guidance whilst respecting the fundamental values and autonomy of research system actors. In 2023, a new Knowledge Security Screening Act was proposed, following up on the intention expressed in the 2020 letter to parliament to introduce a framework for the screening of researchers in certain fields and disciplines from ‘third country nationals’ (uitderdelanders). How tightly these fields are specified has, however, seen pushback from actors within the research system, with a warning from KNAW that the proposed legislation, which would operate at the level of entire disciplines, was not only contrary to the principles of open science but also that it would be too imprecise, impossible to implement and might also generate a false sense of security for researchers that would undermine responsible behaviour towards international collaboration, in that researchers would believe all threats were being screened out, and that this ultimately could actually make research security risks worse.³⁷⁵ Concerns have also been raised about the legality of applying screening to all third country nationals, particularly with respect to the Dutch constitution, Article 1 of which is a strong prohibition against discrimination on any grounds. Some of our interviewees in the research system³⁷⁶ raised both this issue and the practical question of whether government could realistically cope with the volume of screening that would be required, especially with a more expansive conditionality.

In any case a change of minister and government appears to have brought this Act back to the drawing board, with reports³⁷⁷ that the current education minister is working to tighten the focus of the screening framework to be included in the legislation, a commitment made in a letter to parliament in October 2024.³⁷⁸ The letter also promises to consult on what is the appropriate and lawful approach to categorising which nationalities would need to be screened. The government’s aim as stated in the letter is to publish the draft legislation for public consultation in the first half of 2025.

6. 1. Export controls

As an EU member state, the Netherlands implements EU legislation and feeds into its future development. It is also a member of various international partnerships and export control regimes centred on issues such as nuclear technology, biological/chemical technology, ballistic-missile and drone technology and conventional military technology. Decisions taken in the context of these regimes are incorporated into national legislation by the Netherlands, in some cases through EU legislation. Finally, the Netherlands is party to a number of treaties, such as the UN Arms Trade Treaty, the Convention on Cluster Munitions and the Non-Proliferation Treaty³⁷⁹ and adopts international sanctions agreed by the UN and EU (but does not impose sanctions of its own)³⁸⁰. A list of specific topics/programmes at specific institutions (mainly but not only universities of applied science) is published under the ‘knowledge embargo’ of the Dutch implementation of international sanctions, and anyone intending to do training or research in those areas must apply for permission (‘exemption’) from the ministry of education and science (OCW) before commencement.³⁸¹

6. 2. Visa controls and vetting procedures

The Netherlands is a member state of the EU and part of the Schengen Agreement. Visas for short term visits, including potentially by short term research visitors, speakers or conference attendees, are Schengen-wide. On the other hand working visas (National D-type Work visas) and long-term student visas are issued by individual states with their own criteria, and incoming researchers from non-EU member states would also typically need a residence permit. As noted

above, announcements in 2020 and 2023 promised the development of a new Knowledge Security Screening Act to introduce a framework for the screening of researchers in certain fields and disciplines from ‘third country nationals’. There are legal/constitutional reasons why it may be difficult to discriminate against nationals of countries in such a screening system but many of our respondents in the research system expressed skepticism about the practicality of introducing such a wide screening process³⁸².

6. 3. Investment controls

The Investments, Mergers and Acquisitions Security Screening Act (Vifo Act, 2023) provides for security and economic security screening of FDI, mergers and acquisitions, with mandatory notification required for investments in sensitive areas. There is also an economic security contact point (Ondernemersloket Economische Veiligheid - OLEV) to act as a functional equivalent for businesses to the National Contact Point for knowledge security.

7. CONCLUSIONS

7. 1. Summary

The Netherlands is a mature, open and highly internationalised research system with a well-developed approach to research security that combines top-down guidance and support through the National Contact Point with an increasingly mature infrastructure for awareness raising, ethical and compliance guidance and support within most research-performing organisations. As in the UK there are concerns about the ability of universities to meet the increasing costs of taking an active approach to research security concerns, there is ongoing debate about the effectiveness of the Dutch approach and there are ongoing calls for clearer guidance and better intelligence. However, based on the consensus amongst all our interviewees, there appears to be widespread agreement that the approach of trying to understand and reduce risks rather than avoid them is the best way to balance openness and scientific freedom with research security.

7. 2. Future directions for research security in the country

Consultancy firms Oberon and Dialogic suggested in 2023 that more government guidance/regulation was needed to ensure an uptake of research security measures, however at the same time, European and international agreements on knowledge security are needed to ensure that the Dutch system does not risk losing talented researchers to foreign institutions with less stringent security measures.³⁸³ Our respondents, both from within the research system and on the government side, expressed concern about the ‘waterbed effect’ of different interpretations and degrees of implementation of research security in different European nations, leading to the risk that researchers and students of potential concern will simply apply to an institution or programme in a national research system with less developed screening. And although there is much discussion of the benefits of collaboration and sharing of experience and even potentially intelligence between like-minded partner countries, several respondents also noted that which countries can be considered ‘like-minded’ might also be subject to change, either gradually or more suddenly. Several respondents raised the example of collaboration with Israeli partners being raised as a knowledge security issue in their institutions in the light of the War in Gaza.

The draft Knowledge Security Screening Bill is promised to be published for consultation in the first half of 2025. The letter to parliament of October 2024³⁸⁴ also notes that the government is

working to update the 2022 Guidelines in response to the recent analysis of knowledge security practice in the research system that fed into the development of the aforementioned UNL maturity model, and in the light of the advice from the AWTI. The letter also promises further audits of the implementation of the guidelines in the sector (although government respondents stressed to us the importance of proportionality with respect to exposure to risk). The letter also stresses the government's commitment to implementing the EU Council recommendation on research security³⁸⁵ and emphasises and recommits to the strong ongoing collaboration and exchange of practice and information with like-minded countries such as Germany, France, the UK and USA.

Appendix 7: Country case study - Spain

1. INTRODUCTION

In Spain, research security is still an emerging area of policy and practice. While the Spanish government has begun to recognise the risks of foreign interference and intellectual property leakage, responses remain fragmented and less developed when compared to the other countries in this study. Spain can be characterised as being at the realisation stage with an emerging awareness of research security but lack of capacity across the research system and uncertainty about roles and responsibilities within government and between government and research performing organisations.

While there are systems for export control and investment control that are comparable with those of other countries, at the level of the research system, research security awareness and the implementation of measures is much less advanced. For this reason, we can place Spain at the earliest stage of development of its approach and it is too early to tell what the dominant approach will be in terms of top-down versus bottom-up, sector led initiatives. What is however apparent is that the European Union developments in this area will shape what happens in Spain.

There is as we note above, a state implemented and developed export and investment control regime. However, within the research system, it is difficult to note key features of a specific research security approach, although, in terms of awareness, Spain follows the path of other countries in that there is a limited but growing broad awareness of threats, although there is awareness of the threat of cyberattacks – but these are not necessarily considered attributable to activities other than criminality.

The major developments in Spain in this policy area are as follows:

- 2010, University of Barcelona joins the League of European Research Universities [and while this is not a research security organisation as such, it is an important organisation for the development of policies across countries in Europe and increasingly so].
- 2022 cyberattacks attributed to Russian hackers on significant CSIC infrastructure
- 2024 cyberattack on Spain's agricultural research centre INIA [Instituto Nacional de Investigación de Tecnología Agraria y Alimentaria (INIA), the largest research centre operating under the CSIC.

2. THE NATIONAL SCIENCE SYSTEM, UNIVERSITIES AND PUBLIC RESEARCH BASE

Spain has a large university system³⁸⁶ and a number of non-university research performing organisations and funding bodies³⁸⁷ of which the Spanish National Research Council (Consejo Superior de Investigaciones Científicas CSIC) is the most significant with 120 research institutes. CSIC is located organisationally under the Ministry of Science Innovation and Universities of Spain but has some measure of independence from it. Of the 120 CSIC institutes, 51 are joint centres with other institutions, mostly universities. 23 of the institutes are researching in physics, mathematics and sciences, robots and computation. These topics are included the list of the ten key technologies referred to in the European Council 2024 Recommendations.³⁸⁸

In addition, there are several other important research organisations: The Research Centre for Energy, Environment and Technology (CIEMAT); The Carlos III Health Institute (ISCIII); The Institute of Astrophysics of the Canary Islands (IAC). Several other research facilities exist in

Spain and are designated as SOMMa [key centres of excellence] some of which are independent, some under CSIC and others joint.³⁸⁹ There is also public funding of defence through various agencies which include the Spanish National Institute of Strategic Studies (IEEE).

3. ENGAGEMENT IN INTERNATIONAL RESEARCH COLLABORATION

In 2021-22 there were 5,787 foreign academic staff and researchers employed at Spanish higher education and public research institutions³⁹⁰. The percentage of international academic staff in Spanish universities is low compared with many other European countries, at 3.4% in 2022³⁹¹. Spain is one of the most popular destinations for international student visits in Europe, with the universities receiving more than 50,000 student visits each year and many more for language training³⁹². However, the share of international students as a proportion of all those registered on undergraduate programmes is far lower, at around 3.9% of all students in 2019. The share of international students is greater for postgraduate masters and doctoral studies, at 21% and 29% respectively³⁹³. However, international student numbers have been rising over the past decade or so³⁹⁴. Top countries represented among the international student body in 2021-22 are Italy, followed by Ecuador, France, Colombia and China. The majority of international students in Spain are registered in subjects such as Business Administration and Management, Engineering, Languages, Humanities, Law, or Health Sciences.

Much like our other case study countries, Spain has a relatively high level of international co-authorship of research publications by global standards (although somewhat below the levels of the UK and France, and much more so when compared to smaller mature European research systems like the Sweden and the Netherlands). According to a 2021 study (using 2018 data)³⁹⁵, 51% of the Spanish research system's published research output is internationally co-authored (up from only about 10% in the mid-1980s³⁹⁶) and more recent analyses of 2022 data by the US National Science Board provide a similar estimate³⁹⁷.

When we correct for the scale of the science system and look at extra-EU collaborations, (see chart below) in 2022 Spain produced 1178 internationally co-authored publications with non-EU countries per 1000 researchers, well behind Sweden and the Netherlands, somewhat ahead of France, and with a similar level to Italy and Czech Republic³⁹⁸. Spain is unusual in having more citations to its non-internationally collaborative research in two fields, medical sciences, and social sciences³⁹⁹.

Our own analysis using *The Lens* shows that Spain's main international collaborating partner as measured by co-authored publications is the US (see Table 1). Between 2020 and 2023, China has dropped down the list of top collaborating countries whilst Brazil has risen up it, showing a significant increase in the absolute number of internationally co-authored papers with Spain.

Table 1: Top nine international collaborating countries measured by co-publication, three years

Top Nine International Collaborating Countries, Three Years, By Count of Documents [Publications]						
Country	Document Count 2015	Country	Document Count 2020	Country	Document Count 2023	
Spain	76943	Spain	100622	Spain	98195	% in 2023
US	8890	US	12489	US	11498	12%
UK	5736	UK	8679	UK	6737	7%
Germany	4950	Italy	6783	France	6230	6%
France	4507	Germany	6387	Italy	6013	6%
Italy	3941	France	5479	Germany	4959	5%
Canada	2156	China	3165	Switzerland	3632	4%
Netherlands	2036	Netherlands	3051	Brazil	3618	4%
Brazil	1901	Australia	2993	Belgium	3184	3%
Switzerland	1825	Brazil	2977	China	3079	3%

Source: enabled by the <https://www.lens.org/> [lens.org]



4. PERSPECTIVES ON RESEARCH SECURITY

4. 1. Definition of research security

The most recent Spanish National Security Strategy (2021) briefly refers to the risk to economic security of attacks by hostile actors on research and scientific and technological activities, but the concept of research security appears from our desk research to have had little purchase in Spain until recently. The EU dual-use regulation⁴⁰⁰ and the Council's Communication on research security⁴⁰¹ are what respondents refer to when asked for a definition of research security. These documents define the threats currently understood to exist, and in particular the Council document's Recital (18) (1) (a) which focused on the risk of the transfer to malign actors 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'.⁴⁰²

4. 2. Research security threats and threat actors

4. 2.1. Research security threats

The risk of cyberattack upon research actors is the main form of research security threat of which our interviewees were aware in either the university or research institute systems, and this may also be because of the existence of a binding (by royal decree) National Security Framework for

cyber/information security.⁴⁰³ In addition, Spain's export and investment control regime reflects a perception of the risk of theft of or unauthorized or accidental export / flow of research information to other countries. This regime is both more long-standing than the any research security frameworks that might be in development but also subject to recent upgrading and strengthening.⁴⁰⁴

4. 2. 2. Threat actors

In the absence of formal approaches to threat prevention there is no official approach that specifies either countries of concern or a country-agnostic approach.⁴⁰⁵

4. 2. 3. Threat vectors

The principal threat vectors of which Spanish universities and research organisations would appear to be aware is cyberattack upon Spanish research infrastructure. The issue was mentioned in interviews and one respondent had personally been subject to such an attack. The paper by Navajas-Adán et al ⁴⁰⁶ demonstrates the widespread awareness of cyberthreats to research activity. Cybersecurity has a leading role in Spain's National Security Council⁴⁰⁷ and is covered by a dedicated specialist organisation. The web site KonBriefing provides public data on the extent of cyberattacks on universities, Spanish universities feature although far less significantly than France, Germany or the Netherlands but to similar levels as Sweden.⁴⁰⁸ There is also recognition that Spain's economic security, for example in fisheries, depends upon research that is outside the areas noted in the Council's [the EU] list of key technologies⁴⁰⁹.

4. 3. Scale of attention and response to threats

At the senior level in universities there is some awareness of threats to research security but at lower levels there may be far less. According to informants with knowledge of other European countries, there has been far less discussion in Spain than in other countries of this issue.^{410 411}

A further view obtained from interviews^{412 413} is that Spain should now follow other countries' approaches and that it may be able to adopt a system that has been developed elsewhere which could then be implemented in Spain. There is however little understanding of which specific approach to research security of those being implemented elsewhere should be adopted in Spain, although work is now beginning on what this could look like.⁴¹⁴ Respondents to interview confirm that they understand that research security is very important, and the stimulus here is European Council Communication and to a lesser extent the operation of LERU which has one member institution in Spain⁴¹⁵.

4. 4. Factors influencing policy responses of government and research performing organisations

- **Lack of strong threat perception.** There is a perception that the country is less 'at risk' than others, and that action is less necessary and less urgent than that being undertaken by other countries.⁴¹⁶
- **Lack of clear responsibility within government.** Responsibility is split across multiple ministries - mainly the Ministry of Science, Innovation and Universities (MICIU) and the Ministry of Defence - and coordination currently appears limited.

- **Influence of EU guidance and Horizon Europe:** the European Council Recommendation on international research cooperation and foreign interference is beginning to shape national thinking, but this is at an early stage.
- **Decentralised university system with no national guidance:** Spanish universities operate with considerable autonomy and lack national coordination on research security. The CRUE (Conference of Rectors of Spanish Universities) has not issued sector-wide guidance. As the governance of Spanish universities operates at regional level to a great extent⁴¹⁷, there is a further layer of government through which any regulatory structure of the university sector would need to operate. Research funders though, such as CSIC, which are under a ministry [the Ministry of Science Innovation and Universities], are subject to more direct steering from the state – but this works both ways, in that the Ministry seems to see CSIC as a lead actor in helping it to develop a response to the EC recommendations and communications⁴¹⁸.
- **Low awareness and institutional preparedness:** Research security is still a low-salience issue for many Spanish universities. Very few appear to have designated officers or internal policies to assess risks in international collaboration, especially with regard to dual-use research or foreign funding.
- **Bottom-up initiatives and awareness campaigns:** Some awareness of research security risks is emerging at the institutional level, especially in technical universities and those involved in defence or dual-use research projects. Research ethics structures are generally focused on human subjects and scientific misconduct rather than geopolitical risk or foreign interference. Some institutions are beginning to introduce risk assessment procedures, but this is not yet standard. However, these efforts are sporadic and often driven by individual researchers or administrators. (e.g. University of Barcelona).
- **Concerns about academic freedom.** An interviewee noted that university researchers '*Liberdade de cátedra*', [academic freedom] is cited as a reason not to limit the scope of research that academics can undertake. It should be noted that, unlike in many other countries, academic freedom is written into the Spanish Constitution.⁴¹⁹

5. RESEARCH SECURITY MEASURES

There has been very little formal response either from the government or from the research sector in Spain to the issue of research security. There are no formal guidelines or policy document which address the issue of foreign interference in academia, but actors within the sector are beginning to acknowledge that they must act. There is knowledge and awareness of approaches being taken elsewhere in Europe, which appears to be more the result of interaction between actors at the European level rather than as the result of a strategic process. One university is a member of LERU and is actively engaged with it and its committees that cover research security issues. CSIC is a member of the European Association of Research Managers. But there is little evidence that formal awareness raising programmes on the issue are being conducted within Spain or within its university sector.

6. CONCLUSIONS

6. 1 Summary

Spain is at the very earliest stage in the development of awareness of research security, and of systems to address it, and this was widely agreed by our interviewees across the system. There is a lack of formal guidance and very little risk mitigation measures implemented consistently across Spanish universities and research institutions. But the message from our interviewees is that research security will come more to the fore in the coming years as the country aligns itself with the sentiment behind the European Commission Council Recommendation (2024) on Research Security.

6.2 Future directions for research security in the country

Future directions for policy are difficult to assess. While Spain does have awareness of cyber threats and some specific economic security concerns, and has existing IP policies around the value and protection of its commercial and technological knowledge, its research security policies are limited. The country will aim to follow others, but the model / definitions of research security adopted and the structures and procedures that will be implemented are not yet at the design stage.

Appendix 8: Country case study - Sweden

1. INTRODUCTION

Like other Nordic countries, Sweden uses the term “responsible internationalisation” rather than research security. Sweden has pursued a sector-led approach to responsible internationalisation but a government assignment for recommendations on responsible internationalisation undertaken by the University and Higher Education Council, the Swedish Research Council and Vinnova suggests an attempt to delineate between the roles of central government and the sector as well as a more explicit focus on research security.⁴²⁰ Draft guidelines on responsible internationalisation have been published together with recommendations for a support structure.⁴²¹ At the time of writing the proposals were being considered by the Ministry of Education & Research against a background of concerns from some universities and sector organisations about their implications for university autonomy and academic freedom.

We characterise Sweden as being in the Definitions and Capacity Building stage. Awareness of research security is spreading, and risk management and due diligence guidance is being developed. There has been growing government attention to research security and economic security issues. The Swedish government introduced an updated Protective Security Act (2021) and the Foreign Direct Investment Screening Act (2023), both of which have implications for universities. Furthermore, the government has sought to introduce greater research security awareness in universities by imposing new members of university governing bodies.

We identify the following important developments in Sweden:

- 2020 – publication of the first STINT report on responsible internationalisation.⁴²²
- 2021 – introduction of the Protective Security Act.
- 2022 – publication of the second STINT report on responsible internationalisation.
- 2023 – introduction of the Foreign Direct Investment Screening Act.
- 2023 – Government assignment issued to UHR, Swedish research council and Vinnova.⁴²³
- 2024 – publication of the two reports of the government assignment.

2. THE NATIONAL SCIENCE SYSTEM, UNIVERSITIES AND PUBLIC RESEARCH BASE

Sweden is a world leader in scientific research, development, and innovation. The country is widely recognised for its high-quality higher education system and open and excellent research system. Sweden is home to five of the world’s top 200 universities in 2023 according to the Times Higher Education university rankings, with the Karolinska Institutet, Lund, and Uppsala universities at the forefront. The country’s excellence in industrial research has been developed in parallel through leading technical institutes with strong industry-links such as Chalmers Technical University and KTH Royal Institute of Technology.

Key research funders include the Swedish Research Council and Vinnova (the Swedish Government Funding Agency for Innovation System) for applied research, alongside a number of other public/private institutes such as the Wallenberg Foundation.

A Strategic Partnership between the UK and Sweden was signed in October 2023, deepening UK-Swedish cooperation in areas including security and defence, innovation, science, energy and climate, and trade and investment. In May 2022, the UK and Sweden signed a memorandum of understanding in life sciences, to promote cooperation across local, regional, and national healthcare, research, and innovation systems.

3. ENGAGEMENT IN INTERNATIONAL RESEARCH COLLABORATION

Swedish higher education is not highly internationalised as measured by student enrolments, with the exception of doctoral students. In 2022, Sweden enrolled only about 5% of all tertiary students with a country of origin other than Sweden. However, doctoral students from another country-of-origin account for 32% of all enrolled doctoral students in that year, with about half coming from Europe and half from Asia.⁴²⁴ Around 6,704 academics and researchers in the relatively small Swedish system hailed from outside of the country in 2021⁴²⁵ out of a total of about 21,500 researchers⁴²⁶.

In research terms, international research collaboration is seen as critical to Sweden's research base and Sweden has the highest level of international research collaboration amongst any of the case study countries considered in this study. Two studies based on Scopus, 2018 data⁴²⁷ and on Scopus 2022 data by the US National Science Board⁴²⁸ show a share of internationally co-authored publications for Sweden of 67% and 69% respectively.

Our own analysis, using *The Lens*, shows the international co-authorship rate of Swedish papers for the country's leading collaborating countries (see Table 1). This shows that the US, UK and Germany are the main source of collaborators. However, the rise of China is notable, rising from ninth to fourth between 2015 and 2023. In 2023 there was a Chinese co-author on 8% of Swedish publications (1% point lower than Germany).

Table 1: Top nine international collaborating countries measured to co-publication, three years

Top Nine International Collaborating Countries, Three Years, By Count of Documents [Publications]						
Country	Document Count 2015	Country	Document Count 2020	Country	Document Count 2023	
Sweden	37153	Sweden	45764	Sweden	44247	% in 2023
US	6443	US	8967	US	7104	16%
UK	4329	UK	6690	UK	5811	13%
Germany	3465	Germany	5132	Germany	3926	9%
Denmark	1990	China	3491	China	3529	8%
Italy	1964	Italy	3059	Italy	2751	6%
France	1889	Netherlands	2878	Netherlands	2521	6%
Netherlands	1774	Australia	2824	Australia	2401	5%
Australia	1706	France	2720	Denmark	2253	5%
China	1672	Denmark	2709	France	2130	5%

Source: enabled by the <https://www.lens.org/> [lens.org]



4. PERSPECTIVES ON RESEARCH SECURITY

4. 1. Definition of research security

Sweden uses the term “responsible internationalisation” when considering international research collaboration. The term is broader than research security, integrating security concerns with broader issues of research integrity, ethics, mobility, the position of foreign students in the Swedish education system as well as sustainability. A key report emphasises that this perspective cannot be decoupled from other important societal issues with international facets.⁴²⁹ The reports of the government assignment note:

“Responsible internationalisation covers the aspects that a national actor in higher education, research and innovation needs to take into account in order to responsibly establish, nurture and follow up a relationship with one or more actors in other countries.”⁴³⁰

The term emerged in response to several high-profile ethical scandals associated with international research collaboration and these led to two reports on international research collaboration from the Swedish Foundation for International Cooperation in Research and Higher Education.⁴³¹

This broader perspective has pervaded thinking in government and universities. Thus, scientific espionage, cybersecurity, dual use, political interference are discussed alongside issues of

human rights aspects and academic freedom.⁴³² The government assignment has stimulated a debate within Sweden about the appropriate balance between responsible internationalisation and the narrower focus on research security that is seen by Swedes as characterising the UK and Dutch policy approaches. Critics argue that the focus has shifted too far towards research security.⁴³³ Equally, there are those in Sweden who see the broader scope of responsible internationalisation as diverting attention away from research security.⁴³⁴ The Swedish government expresses the view that the focus of responsible internationalisation on openness, ethics, transparency and research integrity and the question of research security should be complementary and not in conflict with issues of research security.⁴³⁵

4. 2. Research security threats and threat actors

4. 2. 1. Research security threats

The Swedish perspective on research security threats spans both national security and economic security as well as wider ethical issues. There are concerns that if knowledge and technology transfer is done inappropriately it can weaken economic competitiveness.⁴³⁶ Sweden takes a similar view of threats to the UK, with concerns about legitimate research collaborations that are poorly structured leading to unwanted knowledge leakage⁴³⁷; cyber threats and poor research data management⁴³⁸; foreign interference on campuses, including through the China Scholarship Council⁴³⁹; insider threats (including from firms, visitors who disguise their identity) and foreign researchers⁴⁴⁰; and the use of foreign direct investment to acquire technologies (especially from SMEs) and increase technological dependencies.⁴⁴¹ There is also some concern about a “waterbed effect” whereby tighter controls on foreign students and researchers in the United States and Canada has led to those students seeking access to Swedish universities.⁴⁴²

The Swedish security service (Säkerhetspolisen) has warned that espionage against Swedish higher education institutions continues to increase and its 2021 annual report it said: “the Chinese government is using Chinese citizens at Swedish colleges and universities with the objective to gather technology and knowledge that is strengthening the Chinese military capacity”.⁴⁴³ The 2023-2024 annual report notes that China acquires technology and knowledge through Chinese researchers at Swedish universities and through collaborations and acquisitions.⁴⁴⁴ The annual report also notes that the war in Ukraine means more pressure for Russia to obtain knowledge and technologies from universities and public research institutes. Sanctions have led to more covert efforts to collect knowledge and technologies through actors who appear legitimate.⁴⁴⁵

4. 2. 2. Threat actors

Like other countries, Sweden has taken a largely state-agnostic approach to responsible internationalisation although the 2022 STINT guidelines do specifically mention China as a threat. At the same time, however, there have been state-specific warnings from the Swedish security services. The Swedish security service annual report identifies Russia, China and Iran as the countries that make up the largest threats against Sweden with all three conducting intelligence activities and security-threatening activities in and against Sweden.⁴⁴⁶

4. 3. Scale of attention and response to threats

4. 3. 1. Response has been sector-led until recently

Initial Swedish responses to responsible internationalisation were driven from the academic sector itself as the government (Swedish Ministry of Education and Research) tried to refrain from being directly involved in an effort to preserve institutional autonomy and academic freedom. Hence the Swedish Foundation for International Cooperation in Research and Higher Education (STINT) took the lead in drawing up guidelines.^{447 448} University rectors have been very clear in their view that decisions on international research collaboration should be left to universities who they argue have more experience and understanding of the topic.⁴⁴⁹ In response to a growing awareness of the issue and some pressure from politicians, the Association of Swedish Higher Education (SUHF) established a network of security officers at universities and there were some contacts between the security services and universities.⁴⁵⁰ In 2024 SUHF (the Swedish Rectors Council) produced its own short guidelines regarding higher education institutions' responsibility for ethics in research abroad.⁴⁵¹

One critic commented that Swedish academe was late to address the issue of research security and has hidden behind the issue of academic freedom. It was suggested to us that Sweden is now trying to turn this into something positive by becoming a “fast follower”⁴⁵²

4.3.2 There are first signs of direct government intervention

The government assignment suggests a turning point for the Swedish approach to research security from the bottom-up sector-led approach with advisory measures to a more formal regulation and compliance process with greater government intervention in which the roles of government and the sector are more clearly delineated.

In 2024, the government mandated the Swedish Council for Higher Education, the Swedish Research Council and Vinnova to develop national guidelines on responsible internationalisation. This is seen as Sweden moving from leaving the task of defining and implementing guidelines on managing risk in international collaborations to the sector towards the national government more involved in the process and has generated significant comments and response from the sector.⁴⁵³

In May 2024, the University and Higher Education Council, the Swedish Research Council and Vinnova released a preliminary report providing guidance for government and universities.⁴⁵⁴ A second report was published in December 2024 that recommended a national support function to help increase the capacity of higher education institutions and public authorities and other stakeholders to act responsibly on internationalisation issues.⁴⁵⁵ At the time of writing, these were being considered by the Ministry of Education and Research in the context of Sweden's desire to implement the EU Council Recommendation on research security of May 2024.

4. 4. Factors influencing policy responses of government

Several factors have influenced the policy response of the Swedish government:

- **Security assessments, geopolitical context and NATO membership:** The Swedish security services have been clear in their view about research security threats to Swedish universities. Furthermore, several interviewees emphasised the impact on Swedish society of Russian aggression in Ukraine and the Baltic as well as the decision to join NATO and these were seen to have changed the environment for research performing organisations.⁴⁵⁶

- **Political pressure, including from the media and NGOs:** There have been several reports in the Swedish media exposing risks with research collaborations, including researchers with connections to the Chinese military having collaborated with Swedish universities, as well as reports about foreign interference in Swedish universities⁴⁵⁷ At the same time, members of the coalition government have raised this as a political issue.⁴⁵⁸
- **University autonomy:** the principle of university autonomy has had a significant influence on the government's approach. University autonomy is enshrined in Swedish law and the government has been very conscious of this in its approach to responsible internationalisation.⁴⁵⁹
- **The importance of international research collaboration:** government is acutely aware of the importance of international research collaboration to the Swedish research base and has consistently emphasised the need to de-risk those relationships rather than de-couple Sweden from collaborations with China and the rest of the world. This is strongly emphasised in the reports of the government assignment which emphasise its support for international activities as openly as possible and as safely as necessary as a prerequisite for excellent science, echoing language which originates in the policy discourse around open science.⁴⁶⁰
⁴⁶¹ The report comments: "Internationalisation is therefore an inalienable value that needs to be safeguarded and nurtured."⁴⁶²

4.5 Factors influencing responses of research funders and universities

Likewise, a range of factors are influencing the responses of research funders and universities, as follows:

- **Geopolitics:** there is an awareness amongst universities that the geopolitical situation has changed, there are demands that universities contribute to societal mobilisation and desire on the part of Rectors not be seen as "naïve".⁴⁶³
- **Demands of funders and industry partners (actual or anticipated):** Universities that have already addressed research security are those with significant relationships with industry, not least technical universities such as KTH. Other universities are responding to actual or anticipated demands from researcher funders, of which the US National Institutes of Health was mentioned by several interviewees, as well as anticipated EU research security requirements under a future Framework programme.
- **Reputation:** There are concerns amongst research funders and universities about the reputational implications of a research security incident.⁴⁶⁴
- **Lack of detailed information on the risk:** The nature and the scale of the risk is not clear to universities and clear case studies are needed to illustrate the security, financial and reputational risks.⁴⁶⁵
- **Academic freedom (and Professor's privilege):** academic freedom is a significant concern and in Sweden an additional issue is the so-called "Professor's privilege", whereby academics own the intellectual property arising from their research, even when it is publicly funded. Consequently, universities can put in places to protect intellectual property but its use is assigned to the academic. The university can only govern that in terms of the conduct of research and then when it comes to downstream outputs from the research that is entirely in the hands of an individual professor.⁴⁶⁶

- **Concerns about the impact on the conduct of science (and open science):** There are concerns about the consequences of the focus on research security for open science and anxiety that enhanced research security measures will have a chilling-effect on international research collaboration, especially with China which is seen as scientific leader in a growing number of fields.⁴⁶⁷
- **The importance of international research collaboration to Sweden:** Like government, the sector is acutely aware of the critical role of international research collaboration to a small country like Sweden, and there is a strong emphasis on the need to engage with China due to China's globally excellent science and importance in addressing many of the world's grand societal challenges.⁴⁶⁸
- **University autonomy:** the desire to retain university autonomy in decisions regarding international research collaboration is a strong factor in the response of universities and sector organisations.⁴⁶⁹
- **Capacity and capacity building:** Some universities have expressed concerns about the costs needed to build their own skills and organisation. This is particularly the case for smaller universities who are struggling to find the resources to set up structures and are exploring ways of pooling capacity and expertise.⁴⁷⁰ Universities commented on the need to adopt operational best practices, including investment in open source intelligence software for due diligence.⁴⁷¹ It is worth noting that a survey of participants at the Nordic Council of Ministers Conference on Responsible Internationalisation found that building capacities and culture was seen as the key need to support responsible internationalisation and was ranked as much more important than national guidelines or a central advisory activity.

5. RESEARCH SECURITY MEASURES

Although Sweden has pursued a sector-led approach until recently, the government has introduced several measures that have implications for research security and the government assignment on responsible internationalisation is an important step in the Swedish approach.

5.1. Extent of response to research security challenges

Research security is yet to be institutionalised across the sector. Some universities have introduced research security measures whilst others have hardly begun implementation. Some universities and university organisations emphasised their progress and the governmental assignment has prompted greater attention to this matter.⁴⁷²

Some universities have developed research security measures, especially technical universities like KTH, and universities with substantial international research collaborations. Since around 2021, these universities have been establishing research security structures and processes, including the development of internal guidance, awareness raising and training activities and risk management processes. The demands of the Protective Security Act (2021) which we will discuss later, have had implications for some universities.

KTH has an Advisory Group on Responsible Internationalisation (RAI). If necessary, this group may escalate questions to a Steering Group for Responsible Internationalisation (SAI), which is responsible for issues of international cooperation that are strategic in nature, and which may affect KTH's activities and reputation brand. In 2024, RAI handled around 25 cases of varying

magnitude, of which 3-4 have been escalated to SAI.⁴⁷³

The government's assignment has accelerated activity in other universities, including through pilot funding. However, there seems to be a long tail of universities where less action has taken place, especially smaller universities.⁴⁷⁴

5. 2. Promoting awareness and forums for dialogue on research security

5. 2.1. Promoting awareness

There has been no formal campaign on security research. There has been some awareness raising through STINT, the Rectors Conference and engagement with foreign and international bodies, such as the EU.

The government assignment has provided funding for pilot projects for some universities to undertake their own internal awareness raising activities, targeting senior leadership, deans and Heads of Department, researchers and administrators.⁴⁷⁵ Senior leaders have highlighted the importance of responsible internationalisation in internal communication.⁴⁷⁶ One university reported establishing an online risk assessment tool that could be used by all members of staff. Most universities have dedicated web resources on responsible internationalisation.

5. 2. 2. Forums for dialogue

Sweden has lacked a forum for dialogue between government, research funders and research performing organisations. This is addressed by the government assignment and its proposed support function. Amongst the roles of the proposed support function would be to provide meeting places by facilitating and hosting physical and digital meetings where higher-education institutions and other actors can share experiences.

5. 3. Written guidance on research security

The STINT guidelines on responsible internationalisation have been influential not only in Sweden but in other European countries as well.

5. 3. 1. STINT Responsible Internationalisation reports

Until recently, Sweden has not had any government guidelines for research security. Instead, the STINT (2020,2022) guidelines are commonly viewed as the key guidance for responsible internationalisation in the country.

- 2020 – STINT: 'Responsible Internationalisation: Guidelines for Reflection on International Academic Collaboration' – set out the core principles of responsible internationalisation, with notably little discussion of research security, scientific espionage and intellectual property management.
- 2022 – STINT 'Recommendations to Higher Education Institutions on how to work with Responsible Internationalisation' this contains a report updating on how the guidelines were adopted in various universities and provides guidelines that all universities are encouraged to follow. These STINT guidelines provide a matrix for research institutions to use to structure their advice/risk mitigation, based on questions regarding the

institution's degree of internationalisation and centralisation. There is emphasis on building the capacity of staff to deal with these issues, emphasis on sharing information and best practices.⁴⁷⁷

- 2023 - The Association of Swedish Higher Education Institutions, SUHF 2023 Global Responsible Engagement: Checklist which includes guidance on questions universities should ask in international research collaborations, including the democratic principles and academic freedom in the partner country; institutional partner reputation and university values; use of data, IPR and patent rights; dangers of misuse of research and negative unintended applications, including for dual-use or military applications; ethical dumping and security around personnel and biological data; and, personal safety of researchers travelling to the foreign country.

5. 3. 2. Proposed guidelines

In April 2024, the Swedish government tasked the Swedish Council for Higher Education (UHR), the Swedish Research Council and Vinnova with preparing a report proposing a system for responsible internationalisation, based on an overall strategic orientation and indicative national guidelines. The purpose of the indicative national guidelines is to provide a framework that could be used by research funders and universities to develop their own tailored guidance. The guidelines are divided into five dimensions: the Swedish context, the context of its own activities, the foreign context, the knowledge of the partner and the design of the cooperation.⁴⁷⁸

The report outlines a proposal for a system for responsible internationalisation with three levels of responsibility:

- Policy: an overarching strategic approach that sets the direction for responsible internationalisation which will be decided by the government or parliament.
- National guidelines: more detailed guidelines for due diligence and risk management.
- Local guidelines: the expectation is that universities and research funding bodies will use the national guidelines as a template to develop their own institutional guidelines.

The report does not set the national policy and guidelines but instead proposes a framework for those guidelines based on five dimensions, where each dimension includes both challenges and opportunities for international collaboration:

- The Swedish context, where the focus is on the importance of understanding and navigating national conditions for international collaboration,
- The local context, where the focus is the need to identify and protect sensitive data and assets at universities, identify threats, risks and vulnerabilities and assess limitations or possibilities associated with funding.
- The foreign context, which focuses on aspects that may affect the room for manoeuvre in international collaborations, such as the nation legislation of the cooperation partner, democracy, rule of law and human rights, academic freedom and the general threat level. Mitigating measures are also considered.
- Gaining knowledge about the collaboration partner(s), which involves using open-source data to assess the status and level of autonomy of the partner(s).
- Planning and organising international collaboration, which concerns commitments within the framework of a partnership, potential dependencies resulting from this and how to

respond to them. This covers issues such as good research practice, research integrity and ethics, open science, and sustainability and equality.⁴⁷⁹

There have been different responses to the draft guidelines. Some (mainly smaller) universities have welcomed clearer guidelines on how to act while others want to trust their own capabilities and experience.⁴⁸⁰ The Swedish Association of University Teachers and Researchers (SULF) has reiterated that universities' autonomy and academic freedom must be the starting point for all decisions regarding internationalisation and is opposed to any imposition of government guidelines. Similarly, the Association of Swedish Higher Education Institutions (SUHF) has stressed the need for universities' independence.⁴⁸¹

5. 4. Mechanisms for advice and information sharing by government

5. 4. 1. Informal relationships with government and agencies

The relationship between research performing organisations and government and its agencies has been mainly informal. The Swedish Security Service, *Säkerhetspolisen* have talked with universities and in some cases have provided training, but SAPO does not have the resources to provide very detailed project-by-project advice and guidance to universities. Furthermore, decision making is seen as the responsibility of universities and individual researchers.⁴⁸² SAPO feels that it has good connections with research security offices in universities.⁴⁸³ Several universities agreed and felt that they could reach out to contacts with the security services should they require advice.⁴⁸⁴ There is no formal process whereby universities report research security incidents, although the same universities said that they would know who to alert should an issue arise.

5. 4. 2. The proposed support function

The government also tasked the Swedish Council for Higher Education (UHR), the Swedish Research Council and Vinnova to propose a suitable support function that would have as its aim the enabling of exchanges of experience between higher education institutions, authorities and other relevant actors in the innovation ecosystem to create a better national capacity to cope with the issues that arise from international research collaboration.⁴⁸⁵ The recommendations for the support function see it as providing:

- A national node for responsible internationalisation that would coordinate and interact with actors in the field and act as a contact point for the Government Offices, the EU, and internationally.
- Provide support to capacity building and culture by providing unified information via a website, seminars, and training courses, including advice on the implementation of the national guidelines and information regarding relevant laws and policies.
- Monitoring of the environment through contacts and collaboration with other actors (national and international) to provide information about developments in the current environment and to provide analysis and data collection.
- Updating and developing the national guidelines as necessary.
- Provide tools including checklists, for example for applications for funding of collaborations.

- Provide meeting places facilitating and hosting physical and digital meetings where higher-education institutions and other actors can share experiences.
- Handle questions including general questions about responsible internationalisation and questions of a security nature that may require input from relevant security agencies.

The recommendations note that the detail needs to be developed in close cooperation with universities, research funders and other authorities to ensure that it meets their needs.

The current proposal is that several organisations (likely to include the Swedish Research Council and VINNOVA) will work together to establish the function. A strategic council composed of representatives of all key actors from the research and innovation sector will be established to provide direction for the support function. Furthermore, it is proposed that relevant authorities with knowledge and missions in civil defence, sanctions, security and defence matters will be tasked with assisting the support function on security matters.

The support function is initially proposed to be financed with SEK 7 million annually (£520,000). The recommendations note that the funding should also allow for the funding of awareness raising and training activities by research funders and universities.

There have been mixed responses to the proposals for a support function. Some universities – mainly smaller universities with limited responses – have welcomed the proposal and have expressed a need to be able to obtain assistance on issues such as security and export controls. Others are sceptical about the ability of a centralised function to provide the detailed advice and guidance that universities would need in order to assess risk. A vocal critic commented: “[Y]ou cannot really delegate this to a central organisation. How would that work? Should we send our contracts to a central body... governments think that they can regulate this in a responsible way without understanding what complexity we are looking at”.⁴⁸⁶ The same person argued that it was universities who need to take responsibility and there was a danger that a central body will mean that they will not responsibility for decisions.⁴⁸⁷ Another sceptic argued that the government assignment had not undertaken a proper needs assessment to fully understand what research funders and universities wanted.⁴⁸⁸ Some leading universities are broadly supportive of the plans for workshops, development of support material and other outreach activities. However, they are sceptical as to whether a central function could provide effective advice and guidance on collaborations.⁴⁸⁹ The small budget proposed for the support function has also been noted.

5. 5. Due diligence processes employed by research funders and universities

Most large universities have some form of risk management and due diligence process. This is often based on the STINT guidelines and the EU report on foreign interference. The due diligence typically examines issues of research integrity as well as research security.⁴⁹⁰ University practice varies and some of the large institutions like KTH are felt to have come a lot further than others.

⁴⁹¹

Attention is paid to compliance issues related to export controls and sanctions. Some universities have specialist export control offices that work with research support offices and grants offices to ensure that they are aware of export control regulations.⁴⁹² In these circumstances, due diligence includes conducting checks on end-users and the existence of any links to the military, checks on the publication records of the collaborators, their CVs and so forth. Particular attention is paid to technologies on the EU critical technologies list.⁴⁹³

Another university coordinated due diligence across its international office and Grants and Innovation Office to consider issues such as ethics, research data management and so forth.

There are a series of checklists related to the university's self-developed framework for responsible internationalisation, and these are questions that the university recommends that all researchers consider before entering a collaboration. There are checklists for a range of matters, including research data management and information security.⁴⁹⁴ In this case, responsibility for export control compliance is decentralised with responsibility for compliance devolved to researchers and their heads of department. The university provides a structure and guidance to aid with compliance.⁴⁹⁵ A major research performing organisation noted that they had developed their own assessment tool to support anyone considering an international research collaboration. The tool covers all aspects of collaboration, including research security, export controls as well as ethics. The tool also directs researchers to additional support as necessary.⁴⁹⁶

Notably, the universities emphasised that these processes were for advice and guidance. In most cases it was ultimately the researcher's responsibility, although where a legal contract is required, their legal advisors would typically expect that a full due diligence has been conducted. One research performing organisation noted that in the case of large and sensitive collaborations, they would engage an external risk advisory firm with knowledge of the particular country.

Swedish research funders have yet to introduce research security clauses. STINT is the only funder that reviews international collaborations as part of the assessment process (although STINT is a minor funder of research). Research funders are concerned about issues of capacity and their capability to make informed decisions.

5. 6. Public funding for capacity building

As part of the government assignment, five pilot projects were funded at universities to implement responsible internationalisation measures.⁴⁹⁷ There is a recognition that further funding may be needed to facilitate the initial implementation of procedures and practices in higher education institutions.⁴⁹⁸

6. LEGISLATION AND REGULATIONS

6. 1. Export controls

Most universities have formal export control processes. Leading universities have full time export control officers working solely on dual use and export control compliance.

6. 2. Visa controls and vetting procedures

Universities are clear that responsibility for vetting of students or visitors is the responsibility of government, specifically the Migration Agency. They are hesitant in taking on any responsibility for background checks.

An important exception is when an activity is covered by the Protective Security Act (2021). If there is a research project or department that is handling classified information, then universities will conduct a vetting process. This would include the vetting of Swedish citizens as well as foreign nationals. The security services play a role in this process which involves an interview process with researchers.⁴⁹⁹

6.3 Protective Security Act (2021)

Sweden is one of the few countries in this study that has statutory and legally enforceable requirements for protective security measures for sensitive technologies (France is the other). The Protective Security Act (revised and updated in 2021) is not focused on international research collaboration per se but universities are classed as “operators” in the same way as businesses and public sector organisations.⁵⁰⁰

Under the Act, all operators are responsible for protecting information and activities that are important for Sweden's security against espionage, sabotage, terrorist crimes, theft and certain other threats. Security protection is also about protecting activities that are covered by an international commitment on security protection that is binding for Sweden. As such, several universities have activities that fall under the Protective Security Act. Support is provided by the security service where requested. In the event of security service concerns about the security practices of an operator, the Act gives the security service the power to conduct an audit.

The Protective Security Act forced universities to consider whether they have sensitive technologies as defined under the Act.⁵⁰¹ The Act requires operators to undertake a protective security assessment (*säkerhetsskyddsanalys*). The protective security assessment must be repeated every 24 months. The purpose of the assessment is to identify activities, capabilities or information that are of importance to Sweden's security. A respondent in one of the universities recalled that this involved a detailed inventory of activities involving all departments in this large university. Each department was examined to identify sensitive technologies, and this was a substantial and resource intensive exercise.⁵⁰²

If the assessment concludes that there are operations, data or knowledge in the organisation that are relevant for the security of Sweden (“security sensitive operations”), the organisation must report this to its relevant supervisory authority and the Swedish Security Service, *Säkerhetspolisen*.⁵⁰³

Where a university has sensitive technologies as defined under the Act, this generates particular requirements for security protection. Security protection includes requirements for Information Security, Physical Security, Personnel Security and Security Protected Procurements, Cooperations or Collaborations. The security protection requirements may be required for a facility in whole or in part.

Universities that have security sensitive operations have to appoint a dedicated Head of Protective Security. This person reports directly to the Rector and is authorized by law to make far-reaching executive decisions regarding all aspects of protective security in the organisation.

The designated Head of Protective Security is responsible for the vetting of all people accessing designated activities, both foreign and Swedish nationals.

The Protective Security Act allows the supervisory authority (the Swedish Security Service) to impose an administrative fine on any operator that fails to comply with key obligations under the Act. The administrative fine is set at a minimum of SEK 25,000 (£1965) and a maximum of SEK 50 million (£3.93 million).

6. 4. Investment controls

In December 2023, Sweden introduced the Foreign Direct Investment Screening Act. The Act gives power to screen investments in security sensitive areas. These areas include biotechnology, nuclear, military, dual use, emerging and other security sensitive technologies.

The Act has implications for Swedish universities. Spin-offs from universities may be subject to scrutiny should they operate in security sensitive field and receive foreign investment. Equally, foreign investment in Swedish research in security sensitive areas may also be subject to the foreign investment screening process

The FDI Screening Act is overseen by the Inspectorate of Strategic Products (ISP). The ISP recognises that one of its challenges is to make researchers aware of the new Act and its potential implications for them.

6. 5. Membership of University Boards

The Ministry of Education plays a role in the appointment of external members of University Boards. In 2023, the Swedish government in a rare intervention in the running of universities, cut the terms for university board members and appointed a number of new board members with backgrounds in defence or security in an effort to introduce new security experts on to boards. At this time, they also appointed a special investigator to look into security issues at universities and how university competence in security questions could be increased, including an analyse of the impact of demanding security clearance for external members of a university boards, and the heads of such boards.⁵⁰⁴ These interventions provoked a considerable response from the Swedish Association of University Teachers and Researchers (SULF) and prominent university Rectors who expressed concerns about the impact on university autonomy⁵⁰⁵

6.6. Public funding for capacity building

Another feature of Swedish public policy is that a small sum of public funding has been made available to universities to support awareness raising and capacity building. The funding for five pilot projects was made as part of the government assignment on responsible internationalisation. The government assignment recommends that such funding should continue and at the time of writing that recommendation, along with the other recommendations arising from the government assignment, were being considered by the Ministry of Education and Research.

7. CONCLUSIONS

7.1. Summary

At the time of writing, the Ministry of Education and Research was considering the recommendations of the government assignment on responsible internationalisation. If implemented, in whole or in part, the combination of national guidelines and a central support activity would represent a significant development in research security in the country that tests long-held Swedish principles regarding the balance between university autonomy and government policy. Already, changes have been taking place. Whilst a sector-led approach has been pursued, government intervention has been growing, whether in the form of the Protective Security Act or changes in the composition of university governing boards.

7. 2. Future directions for research security in the country

In large part, the future direction of security research in Sweden will be determined by the Education Minister's response to the recommendations regarding guidelines and the proposed support structure. The response of universities and the rate and character of their engagement with any new guidelines and advisory structure will be critical. Leading universities have already adopted some research security practices, especially where their activities are subject to the

Protective Security Act (2021). However, research security measures are not institutionalised consistently across the sector and as in many countries, there is a tail of universities where research security measures have been less widely adopted as a consequence of their size, degree of internationalisation or perception of their scientific and technological capabilities. Government intervention has prompted debates about university autonomy as well as questions about the adequacy of university responses. As in other countries, the emergence of new research security rules under a future Framework Programme will be a major factor in adoption, although some universities have already responded to actual or perceived requirements from other funders, not least the US National Institutes of Health. There has also been discussion about the potential for closer Nordic and Baltic security cooperation, including in science, science diplomacy and research security within the framework of the Nordic Council of Ministers.⁵⁰⁶

Appendix 9: Case study – the European Union

1. INTRODUCTION

The European Union is an influential actor in the development of research security policies and practices by some Member States. This occurs through the EU's normative influence as a source of policy frameworks and good practice guidance; the influence of research funding requirements through HORIZON and other funding instruments; and the convening power of the EU. In particular, the publication of the 2024 European Council Recommendation for Enhancing Research Security is seen as a key development by the European Commission and most Member States.^{507 508}

There is a view that the political salience of research security has grown within the European Union in the last two years. As well as DG Research & Innovation, several parts of the Commission have an interest in research security, including DG HOME and DG TRADE although some interviewees commented that thinking was not always joined up across the Commission.⁵⁰⁹ However, senior European Commission officials are now paying attention to the issue and there is a growing “whole of government” perspective across the European Commission. Equally, several Member States have been prompted to consider research security because of the discussions that led to the 2024 EU Council Recommendation. These are part of the wider EU focus on economic security.

The timeline of EU actions related to international research collaboration and research security includes:

- 2020: European Commission publish ‘Concept Note on Tackling Foreign Interference in Higher Education Institutions and Research Organisations’ - intended to act as a basis for discussion on a joint response to foreign interference in research following a December 2019 meeting on ‘R&I Cooperation with China’.⁵¹⁰
- 2021: The ‘Global Approach to Research and Innovation’ outlines a new European strategy for international R&I policy.⁵¹¹
- 2021: The Council adopts the recommendations on internal compliance programmes for the control of research involving dual-use items.⁵¹²
- 2022: ‘Staff Working Document on Tackling R&I Foreign Interference’ is published.⁵¹³
- 2023: The Commission and High Representatives adopt a joint communication on a European Economic Security Strategy.⁵¹⁴
- October 2023: The Commission identified critical technology areas for the EU's economic security for further risk assessments with the member states.
- 2024: European Council Recommendation for Enhancing Research Security.⁵¹⁵

2. THE ROLE OF THE EUROPEAN UNION

The European Union has stimulated awareness and interest in research security amongst some Member States. For example, EU initiatives have framed policy developments in a number of our

case study countries, not least the Czech Republic where the “Methodologies” documents published in 2024 explicitly use EU developments as a rationale for action, not least the need to prepare for anticipated research security requirements under a future framework programme. Similarly in Spain, it seems clear from our interviews that the 2024 Recommendation has been key in putting research security on the domestic research policy agenda.

The January 2024 European Commission Proposal for a Council Recommendation on Research Security defines the term as follows:

‘For the purposes of this recommendation ‘research security’ refers to managing risks related to (a) the undesirable transfer of critical knowledge, know-how or technology that may affect the security of the EU and member states (b) malign influence on research, where research can be instrumentalised by or from third countries in order to diffuse certain narratives or incite self-censorship which may impact academic freedom and research integrity in the EU (c) ethical or integrity violations where knowledge and technologies are used to suppress or undermine fundamental values whether in the EU or elsewhere.’⁵¹⁶

This differs in some respects from the G7’s definition (where the Commission has been a partner) and follows a similar three-pronged approach to the Dutch conception of knowledge security, as defined by the Dutch National Knowledge Security Guidelines.⁵¹⁷

Placing research security in its larger political context, EU strategy has sought to sustain its relationship China through derisking of the relationship rather than decoupling. Since 2019, the EU has seen China not only as a ‘cooperation’ and ‘negotiating’ partner but also as an ‘economic competitor’ and a ‘systematic rival’.⁵¹⁸ The current policies aim at mitigating the risks China poses by enacting research and economic security measures whilst avoiding decoupling. Thus, the Commission is still working on its Road Map for R&I with China but within a context in which rules have been changed to limit Chinese participation in HORIZON to research innovation actions only with exclusion from innovation actions.

The European Union can influence Member States policy and the practice of research funders and research performing organisations in three main ways:

- Normative influence as a source of policy frameworks and good practice guidance.
- Influence through actual or anticipated research funding requirements under HORIZON or a future framework programme.
- The convening power of the EU.

3. NORMATIVE INFLUENCE & POLICY COORDINATION

The European Union has sought to exercise normative influence over both Member State governments and research performing organisations through seeking to shape their beliefs, values, and standards of behaviour without using formal legal mechanisms and has done so by promoting norms, best practices, and shared principles as well as taking a policy coordination role. A number of guidance documents are highlighted here

3.1. Staff Working Document on Tackling R&I Foreign Interference

The 2022 European Commission Staff Working Document on Tackling R&I Foreign Interference was published by the European Commission Directorate-General for Research and Innovation.⁵¹⁹

Foreign interference is defined as activities that are carried out by, or on behalf of, a foreign state-level actor, which are coercive, covert, deceptive, or corrupting and are contrary to the sovereignty, values, and interests of the European Union.

The document provides detailed guidance on four aspects of countering actual or potential foreign interference, namely: values, governance, partnerships and cybersecurity. Thus, the scope of the document is wider than “research security” and includes questions of research integrity.

This an important document, also referred to as the EU ‘toolkit’ on foreign interference. Is frequently referenced by other national actors as they construct their own research security guidelines. It places a heavy emphasis on raising awareness and implementing robust risk assessments. The document does emphasise several research security issues including the importance for research performing organisations to consider:

- Raising awareness of potential risks involved in engaging in a partnership and of the ways the institution seeks to mitigate them.
- Developing a risk management strategy.
- Creating awareness and knowledge of export control legislation and Foreign Direct Investment screening.
- Identifying and protecting the institution’s ‘crown jewels’ and understanding the potential technological, security and economic interest from third countries’
- Defining the minimum levels of due diligence for different types of partnerships.
- Establishing a Foreign Interference Committee to develop and oversee a foreign interference strategy and a sound procedure for developing robust partnership agreements.
- Carefully negotiating partnership agreements to ensure transparent delineation of responsibilities including financial commitments, IPR, data management and open science.
- Developing a broad range of cybersecurity processes and information security measures.

3.2. Critical technologies

In 2023, the European Commission published a Recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States.⁵²⁰ The Commission identified ten critical technology areas and recommended, as an initial step, that Member States together with the Commission assess, by the end of 2023, four technology areas: advanced semiconductors; artificial intelligence; quantum; and biotechnologies.⁵²¹

This list is being used as a reference point by Member States and some research-performing organisations. The critical technologies list is viewed as providing more granular detail on areas where particular attention should be paid by research security.⁵²²

3. 3. European Council Recommendation for Enhancing Research Security

The most significant development in EU research security policy is the 2024 Council Recommendation on Enhancing Research Security. The Council Recommendation is part of the wider European Economic Strategy announced in 2023. This is a Recommendation and does not propose any extension of the EU's regulatory powers in this regard or any binding commitments by Member States. Nonetheless it is clear in our interviews with many policy makers and research performing organisations, that it is informing their view of research security.

The Guiding Principles of the Recommendation stress the importance of proportionality of response, self-governance, academic freedom and institutional autonomy and that ultimate responsibility for decisions on international research collaborations lie with universities. The recommendations are country agonistic.

The Recommendation propose policy actions at national/sectoral level and EU level as follows:

- **Recommendation to both Member States and the Commission:**

The Council recommends that the Commission and member states take into consideration key principles for responsible internationalisation when designing and implementing policy actions to enhance research security, such as academic freedom and institutional autonomy. When it comes to international research and innovation (R&I) cooperation with partners in non-EU countries, this should be done in a way that is both open and secure, in line with the principle 'as open as possible, as closed as necessary', and with consideration to applicable restrictions. Other principles to be considered are proportionality of safeguard measures, non-discrimination, and respect of fundamental rights. Measures to safeguard research security should avoid protectionism and unjustified political instrumentalisation.

- **Recommendations to member states:**

There are fourteen recommendations to member states to enhance research security, including:

- the development of national approaches which may include the formulation of national guidelines or a list of relevant measures and initiatives;
- the creation or reinforcement of support services to help actors in the R&I sector to deal with risks related to international cooperation in research;
- the reinforcement of cross-sectoral cooperation within government;
- the development of the evidence base for research security policymaking.
- measures on member states' engagement with research funding organisations and research performing organisations.

- **Recommendations to the Commission:**

There are eleven recommendations for the Commission to explore and assess options for more structural support. Most notably, there is a recommendation to establish a European Centre of Expertise on Research Security.

The European Centre of Expertise on Research Security is regarded by the Commission as “the most feasible action at the EU level”. The exact nature of the centre was being considered at the time of writing and several different options are being considered. One model would follow the U.S. SECURE Centre consortium model which is distributed across several consortium members but equally the Commission could also run the Centre. Whatever is chosen, the Commission has emphasised that it is highly unlikely to take the form of a new Agency with a large staff. The Centre will have two core tasks: investing in the evidence base and creating a community of practice; and providing threat analysis and evidence for academe. The target for establishing the Centre is 2026.

With respect to the question of whether and how the UK might participate in the work of the Centre, it was stressed that this is envisaged as a capability primarily for the European Union and its Member States, and not a capability for the HORIZON programme itself, and thus potentially associate members of HORIZON and third countries. One question being considered is how open the Centre should be to the public and how much it should be closed. The assumption is that there would be close cooperation with international partners such as the US, UK and Canada. Ultimately, however, this will be a decision for the Member States.

There are several other aspects of the Recommendation that may hint at future activities for the European Commission:

- Export control rules, notably those that attempt to regulate the intangible transfer of technology. Compliance has been identified as an issue, not least with respect to the transfer of intangible knowledge. The Commission is considering the development of a document on this topic which would be undertaken between DG RESEARCH and DG TRADE.
- Visa requirements for foreign researchers. The Recommendation also discuss visa requirements and the need for more awareness of the need for possible action in this area.
- Open science and intellectual asset management requirements. The Commission believes that there is a need to explore the relationship between open science and research security since this is an on-going concern of the scientific community and has been raised in consultation on the draft Council Recommendations. There is a need for a document that explains the link between the two. This mirrors similar debates in Member States such as Germany and the Netherlands.
- An inventory of national policy documents. This initiative has begun with the Commission requesting member states to submit a pro forma identifying their research security policies and examples of good practices by universities.

We undertook an analysis of the responses to the Commission’s consultation exercise on its proposal for a Council Recommendation and found that those responses to the recommendations have been broadly positive. The creation of a European Centre of Expertise on Research Security is widely accepted amongst Member States, though the League of European Research Universities noted recently that this should be developed in partnership with the universities to avoid top-down imposition of rules and because universities and researchers know the threats/risks the best.⁵²³ European university organisations have noted positively that in

drafting the Recommendation, their concerns about respect for university autonomy and decision making in international research collaborations has been recognised.⁵²⁴

3. 4. Policy coordination (through the ERA and other mechanisms)

The EU does not have exclusive competence over research but shapes national policies through coordination mechanisms, not least the European Research Area (ERA) that aims to create a single European market for research, promoting joint initiatives, open science, and researcher mobility. Member states voluntarily align policies through ERA roadmaps and the ERA Forum.

At the end of the Council Recommendation, there is a note on reporting and monitoring progress. There is an expectation on the part of the Commission and Member States that Member States will report on their progress through the ERA structure.

4. RESEARCH FUNDING

The most powerful potential mechanism to influence research security policy and practice is through European Union research funding, not least HORIZON/Framework programme and the European Research Council. Already, the anticipation of potential research security requirements under a future Framework Programme is leading some Member States and research performing organisations to address research security (for example, see the Czech Republic case study).

Horizon Europe was established in April 2021 by EU Regulation 2021/695, which defines the rules for participation and dissemination of results.

The European Commission has already used some measures in the regulation to enhance attention to research security. Article 22(5) specifies that “...For actions related to Union strategic assets, interests, autonomy or security, the work programme may provide that the participation can 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.”

The European Commission has excluded entities based in China from the innovation activities of Horizon Europe, in connection with Article 22(6) of the regulation, which states that “...Where appropriate and duly justified, the work programme may provide for eligibility criteria in addition to those set out in paragraphs 2 to 5 to take into account specific policy requirements or the nature and objectives of the action, including the number of legal entities, the type of legal entity and the place of establishment.”

Article 39 regarding the use and dissemination of results, specifically paragraph 6, states: “Unless the work programme provides otherwise, proposals shall include a plan for the exploitation and dissemination of the results. If the expected exploitation of the results entails developing, creating, manufacturing and marketing a product or process, or in creating and providing a service, the plan shall include a strategy for such exploitation. If the plan provides for the exploitation of the results primarily in non-associated third countries, the legal entities shall explain how that exploitation is still to be considered to be in the Union interest.”

Article 20(1) requires security agreements with countries outside the EU: “Actions carried out under the Programme shall comply with the applicable security rules and in particular rules on the protection of classified information against unauthorised disclosure, including compliance with any relevant Union and national law. In the case of research carried out outside the Union using or generating classified information, it shall also be necessary that, in addition to the

compliance with those requirements, a security agreement shall have been concluded between the Union and the third country in which the research is to be conducted.”

There is a very strong belief that the next Framework Programme for Research and Innovation will include more explicit research security measures. Indeed, several senior European Commission officials have made this expectation very clear and there is an assumption that the Commission will take into account the 2024 Council Recommendations when it designs the regulations for the next Framework Programme (noting that those Recommendations which call on Member States to introduce research security measures in their funding programmes). How it will do this is unclear since the Commission does not have the capacity to evaluate every proposal for research security issues, and it would be difficult to find sufficient appropriately qualified peer reviewers.⁵²⁵ There is a view that this is likely to be “a tick box exercise”.⁵²⁶

Most interviewees did not believe that the introduction of new measures would have an impact on Associate Members. UK universities were regarded as being ahead of most of Europe regarding research security and therefore able to address any requirements.

5. CONVENING POWER AND NETWORKS

The EU plays a key role in bringing together national research stakeholders to foster policy convergence. There are two notable developments:

- The Commission proposes to host a 2-day Research Security Conference in Brussels in 2025 with the aim of raising awareness of research security, exchanging knowledge and developing communities of practice.
- The Commission is keen to support networks of practice and peer learning activities, for example, the creation of a network of national research funders

6. CONCLUSIONS

6. 1. Summary

The European Union is emerging as an influential actor in the development of research security policies and practices by some Member States. This is arising out of a combination of normative influence as a source of policy frameworks and good practice guidance; the actual and anticipated role of research security measures in EU research funding instruments, not least the next Framework Programme; and the convening power of the EU. The publication of the 2024 EU Council Recommendation for Enhancing Research Security is seen as key development by the European Commission and most Member States.

6. 2. Future directions for research security

The Council Recommendation are “a reference point” and attention will now turn to implementation. Whilst the Council Recommendation have no legal standing it is likely that Member States will be expected to report their progress via the ERA and the prospect of research security measures being introduced in the next framework Programme is already having an influence on thinking by some Member States and universities. As such, the European Union is likely to be a powerful force for convergence of research security practices in the medium-term future.

Appendix 10: Interview codes

Code	Organisation
IE	Independent expert/think tank/STN
FA	Research funding organisation
NALS	National academy or learned society
PM	Policy maker
RPOL	Research performing organisation leader/leading researcher
RSO	Research security organisation
UA	Administrator or manager at research performing organisation
UL	Senior leader at research performing organisation
UO	Research sector organisation (national or international university association, professional body, etc)

REFERENCES AND NOTES

- ¹ Trusted Research refers to the UK Government's suite of publicly available advice and guidance published jointly by the National Protective Security Authority (NPSA) and the National Cyber Security Centre (NCSC). The Trusted Research Campaign includes guidance for academics on research security, advice when travelling abroad as well as guidance for senior university leaders and a Trusted Research Evaluation Framework to allow organisations to undertake a self-assessment of their research security practices and culture. <https://www.npsa.gov.uk/trusted-research-academia>
- ² The UK's Research Collaboration Advice Team (RCAT) acts as the first point of contact for universities seeking official advice about the national security risks linked to international research collaboration. RCAT is part of the UK government's Department for Science, Innovation & Technology. <https://www.gov.uk/government/groups/research-collaboration-advice-team-rcat> partners with organisations such as the National Protective Security Authority (NPSA), the National Cyber Security Centre (NCSC) and research funders UK Research and Innovation (UKRI), as well as representatives of the academic community. <https://www.gov.uk/government/groups/research-collaboration-advice-team-rcat>
- ³ The Academic Technology Approval Scheme (ATAS) applies to certain foreign students and researchers who want to study or conduct research in specific sensitive technology-related fields in the UK. The Foreign, Commonwealth & Development Office (FCDO) administers the scheme and issues ATAS certificates. Applicants must be in possession of an ATAS certificate before they apply for a visa.
- ⁴ In 2019, more than two-thirds (64.5%) of all UK scientific outputs (excluding arts, humanities and social sciences) indexed in Scopus were internationally co-authored, up from 57.6% in 2015. (Scopus is a leading bibliographic database of peer reviewed scientific journals and conference proceedings).
- ⁵ Chen K, Zhang Y, Fu X, (2019), 'International research collaboration: An emerging domain of innovation studies?', *Research Policy*, 48(1), pp. 149-168, <https://doi.org/10.1016/j.respol.2018.08.005>.
- ⁶ Royal Society. (2011). *Knowledge, Networks and Nations: Global Scientific Collaboration in the 21st Century*. The Royal Society.
- ⁷ Galison, P. and Hevly, B. (eds) (1992). *Big Science. The Growth of Large-Scale Research*. Stanford University Press, Stanford, CA.
- ⁸ Wagner, C. S. (2008). *The New Invisible College: Science for Development*. Brookings Institution Press: Washington DC.
- ⁹ Group of Seven (2022) *G7 Common Values and Principles on Research Security and Research Integrity*; OECD (2022) *Integrity and Security in the Global Research Ecosystem*, OECD Science, Technology and Industry Policy Papers No. 130, OECD: Paris; European Union (2024) *Council Recommendation on Enhancing Research Security*.
- ¹⁰ A. Joske (2018). *Picking Flowers, Making Honey: The Chinese Military's Collaboration with Foreign Universities*. Policy Brief Report No. 10/2018. Australian Strategic Policy Institute. <https://www.aspi.org.au/report/picking-flowers-making-honey/>
- ¹¹ Council of the European Union (2024). Council Recommendation on Enhancing Research Security (2024/0012(NLE) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024H03510>. National Protective Security Authority (2024). *Trusted Research Guidance for Academia*. <https://www.npsa.gov.uk/trusted-research-academia>
- ¹² OECD (2022) *Integrity and Security in the Global Research Ecosystem*. OECD Science, Technology and Industry Policy Papers, June 2022 No. 130. Paris: Organisation for Economic Cooperation and Development.
- ¹³ UK Trusted Research, *Guidance for Academics*. <https://www.npsa.gov.uk/trusted-research-academia>
- ¹⁴ *G7 Best Practices for Secure and Open Research*. Security and Integrity of the Global Research Ecosystem (SIGRE) Working Group, February 2024 <https://science.gc.ca/site/science/en/safeguarding-your-research/general-information-research-security/international-research-security-resources/g7-best-practices-secure-and-open-research>.
- ¹⁵ The German civil clause is a voluntary prohibition on military research which appears in the statutes of more than 70 universities. "List of current civil clauses sorted by date of their existence", Universities for Peace – Yes to the Civil Clause, <http://zivilklausel.de/bestehende-zivilklauseln>

- ¹⁶ Faber, S. (2022). Blocking Access to the Recent Past: Threats to Academic Freedom in Post-dictatorial Spain. *Copyright American Association of University Professors*, p.13.
https://www.aaup.org/sites/default/files/Faber_JAF13.pdf
- ¹⁷ Polt, W., Rammer, C., Schartinger, D., Gassler, H., & Schibany, A. (2001). Benchmarking industry-science relations: The role of framework conditions. *Science & Public Policy - SCI PUBLIC POLICY*, p.28.
<https://doi.org/10.3152/147154301781781453>
- ¹⁸ European Patent Office. (2024). *University research generates over 10% of all inventions in Europe, new EPO report finds*, <https://www.epo.org/en/news-events/press-centre/press-release/2024/1252722>
- ¹⁹ A tendency already noted in the foundational study on international research collaboration: Frame, J.D., & Carpenter, M. P. (1979). International Research Collaboration. *Social Studies of Science*, 9(4), pp. 481-497. <https://doi.org/10.1177/030631277900900405>
- ²⁰ Data tables available on request from the authors. Analysis enabled by the <https://www.lens.org/> [lens.org]
- ²¹ The Lens is an informetric database comprising both bibliometric and patent data which was established in 1998. The Lens compares favourably with the more established databases of publication data, providing high levels of data coverage and structured query facilities making it suitable for a variety of science mapping activities. More details are available in Velez-Estevez, A., Perez, I. J., García-Sánchez, P., Moral-Munoz, J. A., & Cobo, M. J. (2023). New trends in bibliometric APIs: A comparative analysis. *Information Processing & Management*, 60(4), 103385.
<https://doi.org/https://doi.org/10.1016/j.ipm.2023.103385>
- ²² It should be noted that in this simple analysis we have made no attempt to control for those individuals who might have affiliations in multiple countries.
- ²³ We also reviewed data published by the open-source intelligence company Datenna in their report on China-European university collaboration. Datenna examined current and historical collaborations between European universities and twenty selected Chinese universities. The 20 leading Chinese universities comprised the top 13 universities in academic rankings, and the Seven Sons of National Defence (7S) universities known for their established position in military research in China. Datenna divided Sino-European programmes into “joint study programmes” and “joint research centres”. Datenna identified 379 collaborations: 267 joint study programmes and 112 joint research centres. There are some limitations to the Datenna report that means we decided not to use it in our report. First, Datenna notes that these are current and historical collaborations, so we have no way of knowing whether they continue to operate or whether they exist but are inactive. Datenna does not provide disaggregated data for research centres so the figures that we report here include joint study programmes. Finally, we have no sense of the scale of the collaborations. Datenna (2024). *Navigating Challenges and Risks in Sino-European Academic Collaborations*. <https://www.datenna.com/wp-content/uploads/2024/08/Datenna-Report-Navigating-Challenges-and-Risks-in-Sino-European-Academic-Collaborations.pdf>
- ²⁴ Kwiek M. (2021), ‘What large-scale publication and citation data tell us about international research collaboration in Europe: changing national patterns in global contexts’, *Studies in Higher Education*. 46(12): 2629-2649. <https://doi.org/10.1080/03075079.2020.1749254>
- ²⁵ National Science Board (2023), *Science and Engineering Indicators: Publications Output: U.S. Trends and International Comparisons. Supplementary Table SPBS-33*. Available at: <https://nces.gov/pubs/nsb202333/table/SPBS-33>
- ²⁶ OECD Data Explorer: <https://data-explorer.oecd.org/> [data-explorer.oecd.org]
- ²⁷ European Research Area Platform (n.d). *ERA Performance Indicators*. Available at: https://european-research-area.ec.europa.eu/scoreboard-reports?countries%5B0%5D=42&countries%5B1%5D=46&countries%5B2%5D=25&countries%5B3%5D=50&countries%5B4%5D=55&countries%5B5%5D=60&countries%5B6%5D=61&edit-countries-42=on&edit-countries-46=on&edit-countries-25=on&edit-countries-50=on&edit-countries-55=on&edit-countries-60=on&edit-countries-61=on&field_related_sb_indicator_target_id=123
- ²⁸ In Germany, the term “security-relevant research” (sicherheitsrelevante Forschung) typically refers to research that may pose risks to public safety, national security, or international peace—either because of the potential misuse of results (e.g., dual-use technologies) or due to connections with military applications. This can include work in areas like biotechnology (e.g., synthetic biology, pathogens), artificial intelligence, cybersecurity and encryption, aerospace and drone technologies and nuclear

research. The German debate around this topic has become more structured in response to global developments in dual-use research and increasing concerns about technological misuse or geopolitical tensions.

²⁹ Czech Government, (2024), *Strengthening Resilience against Illegitimate Interference in the Higher Education and Research Environment*.

https://msmt.gov.cz/uploads/311/STRENGTHENING_RESILIENCE_AGAINST_ILLEGITIMATE_INFLUENCE/INTERFERENCE_IN_THE_HIGHER_EDUCATION_AND_RESEARCH_ENVIRONMENT.pdf pp.3-4

³⁰ Secrétariat Général de la Défense et de la Sécurité Nationale (2025) Protéger le potentiel scientifique et technique de la nation <https://www.sgdsn.gouv.fr/nos-missions/proteger/proteger-le-potentiel-scientifique-et-technique-de-la-nation>

³¹ DFG & Leopoldina. (2022). *The Handling of Security-Relevant Research in Germany – An Overview*. [https://www.leopoldina.org/fileadmin/redaktion/Ueber_uns/Kooperationen/Information/The_Handling_of_Security-Relevant_Research_in_Germany - An_Overview_web.pdf](https://www.leopoldina.org/fileadmin/redaktion/Ueber_uns/Kooperationen/Information/The_Handling_of_Security-Relevant_Research_in_Germany_-_An_Overview_web.pdf); DFG (2023). *Recommendations on dealing with risks in international research cooperation*. <https://www.dfg.de/resource/blob/289704/585cb3b48bb8e9f5b6e57e0e0a0d700e/risiken-int-kooperationen-en-data.pdf>

³² Council of the European Union (2024). Council Recommendation on Enhancing Research Security (2024/0012(NLE) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024H03510>

³³ Universiteiten van Nederland (2022), *National Knowledge Security Guidelines: Secure International Relations*, <https://open.overheid.nl/documenten/ronl-5379d1b4f8b9784bf518251032507a965be9c92d/pdf>

³⁴ Council of the European Union (2024). Council Recommendation on Enhancing Research Security (2024/0012(NLE) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024H03510>

³⁵ UHR (2025), *National Support Structure for Responsible Internationalisation*, https://www.uhr.se/globalassets/_uhr.se/english/about-the-council/national-support-function-for-responsible-internationalisation---final-report-2025.pdf

³⁶ Council of the European Union. (2024). *Council Recommendation on Enhancing Research Security*, 2024/0012(NLE), https://research-and-innovation.ec.europa.eu/document/download/e82a2fd9-ac12-488a-a948-87639eef10d4_en

³⁷ Universities UK (2022) unpublished study on *Research Security in Europe and the UK*.

³⁸ Universities UK (2020). *Managing Risks in Internationalisation: Security Related Issues*. London: Universities UK. UK Trusted Research, *Guidance for Academics*. <https://www.npsa.gov.uk/trusted-research-academia>

³⁹ Czech Government, (2024), *Strengthening Resilience against Illegitimate Interference in the Higher Education and Research Environment*

https://msmt.gov.cz/uploads/311/STRENGTHENING_RESILIENCE_AGAINST_ILLEGITIMATE_INFLUENCE/INTERFERENCE_IN_THE_HIGHER_EDUCATION_AND_RESEARCH_ENVIRONMENT.pdf, pp.3-4

⁴⁰ The *Protection du Potentiel Scientifique et Technique de la Nation* (PPST) is a statutory protective security measure that provides the legal and administrative regulation of covered public and private research performers and is designed to safeguard sensitive knowledge, strategic technologies, and digital data. This includes the designation of certain premises as *Zones à Régime Restrictif* (ZRR), where access is legally restricted to prevent unauthorised intrusions and espionage. <https://www.sgdsn.gouv.fr/nos-missions/proteger/proteger-le-potentiel-scientifique-et-technique-de-la-nation>

⁴¹ Interview IT UL-1.

⁴² European Commission, *Tackling R&I Foreign Interference: Staff Working Document*, January 2022, p.2. Fears of economic dependency also include worries about dependencies on foreign student fees that could lead to uncomfortable situations in the future, where foreign state actors could leverage this income to shape research agendas or in cases where geopolitical tensions cause big shifts in the number of students universities would be left without huge sources of income. Whilst this may be a concern for the UK, we found few instances of such dependence in the countries that we studied. For documents that mention student fee dependencies, see: A. Baykal and T. Benner, 'Risky Business: Rethinking Research Cooperation and Exchange with Non-Democracies. Strategies for Foundations, Universities, Civil Society Organisations and Think Tanks', GPPi, October 2020. I. d'Hooghe and J. Lammertink, 'Towards Sustainable Europe-China Collaboration in Higher Education in Research', Leiden Asia Foundation,

October 2020; R. Seeley & R. Clark, 'Living with the Dragon: What does a coherent UK Policy towards China look like?', Civitas, 2024, p.3.

⁴³ K. Hille and J. Shotter (2019) 'Czech university mired in Chinese influence scandal: Secret payments to academics renew concerns about Beijing's encroachment', *Financial Times*, 11 November 2019; I. D'Hooghe., J. Lammertink. (2020). 'Towards Sustainable Europe-China Collaboration in Higher Education in Research'. *Leiden Asia Centre*. <https://leidenasiacentre.nl/wp-content/uploads/2020/10/Towards-Sustainable-Europe-China-Collaboration-in-Higher-Education-and-Research.pdf>

⁴⁴ Mieux protéger notre patrimoine scientifique et nos libertés académiques, (Better Protection for our Scientific Assets and Academic Freedoms) Rapport d'information n° 873 (2020-2021), déposé le 29 septembre 2021 <https://www.senat.fr/rap/r20-873/r20-87329.html>

⁴⁵ H. Boytchev, (2023), 'Frankfurt university ends deal with Confucius Institute', *Research Professional News*, <https://www.researchprofessionalnews.com/rr-news-europe-germany-2023-3-frankfurt-university-ends-deal-with-confucius-institute/>

⁴⁶ D. Plášek. (2022). 'Czech Republic: Chinese influence at universities as a clearly rising threat'. CEIAS [Online]. <https://ceias.eu/czech-republic-chinese-influence-at-universities-as-a-clearly-rising-threat/>

⁴⁷ Czech Security Information Service Annual Report, (2023) <https://www.bis.cz/public/site/bis.cz/content/vyrocní-zpráva/2023-vz-aj.pdf>

⁴⁸ [DGSi et DRSD alertent sur les ingérences étrangères dans le milieu scientifique - Next](https://next.ink/143159/dgsi-et-drdsd-alertent-sur-les-ingerences-etrangeres-dans-le-milieu-scientifique/?utm_source=chatgpt.com) DGSi and DRSD warn of foreign interference in the scientific community) (https://next.ink/143159/dgsi-et-drdsd-alertent-sur-les-ingerences-etrangeres-dans-le-milieu-scientifique/?utm_source=chatgpt.com)

⁴⁹ K. Hille and J. Shotter (2019) 'Czech university mired in Chinese influence scandal: Secret payments to academics renew concerns about Beijing's encroachment', *Financial Times*, 11 November 2019; I. D'Hooghe., J. Lammertink. (2020). 'Towards Sustainable Europe-China Collaboration in Higher Education in Research'. *Leiden Asia Centre*. <https://leidenasiacentre.nl/wp-content/uploads/2020/10/Towards-Sustainable-Europe-China-Collaboration-in-Higher-Education-and-Research.pdf>

⁵⁰ Säkerhetspolisens årsbok 2023-2024 (sakerhetspolisen.se) (Security Service Yearbook 2023-2024) <https://sakerhetspolisen.se/download/18.5cb30b118d1e95affec37/1708502268494/L%C3%A4gesbild%202023-2024.pdf>

⁵¹ D. Matthews (2021), 'German police arrest Russian 'spy' at university', *Times Higher Education*, <https://www.timeshighereducation.com/news/german-police-arrest-russian-spy-university>

⁵² 'German prosecutors charge Russian spy with sharing details of European space rocket programme', (2022), *News Wire: France24*, <https://www.france24.com/en/europe/20220127-germany-accuses-russian-spy-of-sharing-details-of-european-space-rocket-programme>

⁵³ INCIBE (2022). 'Cyberattack on the Spanish National Research Council (CSIC)'. *Spanish National Cybersecurity Centre*, <https://www.incibe.es/en/incibe-cert/publications/cybersecurity-highlights/cyberattack-spanish-national-research-council-csic>

⁵⁴ J. Conejo del Cerro (2024). 'Cyberattack on Spain's INIA: Scientific Research Under Attack', *Thousand Guards*, <https://www.thousandguards.com/post/cyberattack-on-spain-s-inia-scientific-research-under-attack>.

⁵⁵ H. Boytchev, (2023), 'Frankfurt university ends deal with Confucius Institute', *Research Professional News*, <https://www.researchprofessionalnews.com/rr-news-europe-germany-2023-3-frankfurt-university-ends-deal-with-confucius-institute/>

⁵⁶ Note that the report notes this as a general threat vector experienced by several countries, rather than a threat vector seen in the Czech Republic specifically. Czech Security Information Service Annual Report, (2023) <https://www.bis.cz/public/site/bis.cz/content/vyrocní-zpráva/2023-vz-aj.pdf>

⁵⁷ German Federal Prosecutor General (2024), 'Arrests for suspected secret service agent activity', <https://www.generalbundesanwalt.de/SharedDocs/Pressemitteilungen/DE/2024/Pressemitteilung-vom-22-04-2024.html?nn=478184>

⁵⁸ D. Matthews (2021), 'German police arrest Russian 'spy' at university', *Times Higher Education*, <https://www.timeshighereducation.com/news/german-police-arrest-russian-spy-university>; 'German prosecutors charge Russian spy with sharing details of European space rocket programme', (2022), *News Wire*. <https://www.france24.com/en/europe/20220127-germany-accuses-russian-spy-of-sharing-details-of-european-space-rocket-programme>

-
- ⁵⁹ I. D’Hooghe, X. Martin. (2024). ‘Dutch collaboration with PhD students sponsored by the China Scholarship Council’, *Clingendael and CKN*. https://www.clingendael.org/sites/default/files/2024-03/Report_Dutch_Collaboration_with_CSC_PhD_students_final.pdf
- ⁶⁰ European Commission, *Tackling R&I Foreign Interference: Staff Working Document*, January 2022; I. d’Hooghe and X. Martin, (2024), ‘Dutch collaboration with PhD students sponsored by the China Scholarship Council’, *Clingendael*, p.23
- ⁶¹ Interview NL UA-1.
- ⁶² FLASH DGSi #95 June 2023. The risks associated with know how acquisition in fundamental research. Foreign Interference Risks in Fundamental Research (DGSi Report).
- ⁶³ Elsevier (2024), ‘View from the Top: Academic leaders’ and funders’ insights on the challenges ahead’, [HYPERLINK "https://www.elsevier.com/en-gb/academic-and-government/academic-leader-challenges-report-2024"](https://www.elsevier.com/en-gb/academic-and-government/academic-leader-challenges-report-2024) <https://www.elsevier.com/en-gb/academic-and-government/academic-leader-challenges-report-2024>
- ⁶⁴ SURF (2024) ‘Cybersecurity’, <https://www.surf.nl/en/themes/cybersecurity>
- ⁶⁵ UUK, (2020), *Managing Risks in Internationalisation: Security Related Issues*, pp.31-33.
- ⁶⁶ The “seven sons” are Beihang University, Beijing Institute of Technology, Northwestern Polytechnical University, Nanjing University of Aeronautics and Astronautics, Nanjing University of Science and Technology, Harbin Institute of Technology, and Harbin Engineering University. The ASPI Chinese defence universities tracker is a frequently used source in due diligence by European universities and provides a detailed list of universities with links to the People’s Liberation Army (<https://unitracker.aspi.org.au/>)
- ⁶⁷ G. Chambers and M. Bruzzese (2023), *Hypersonic Research Collaboration between Sweden and People’s Republic of China*, China Aerospace Studies Institute, <https://www.airuniversity.af.edu/Portals/10/CASI/documents/Research/Infrastructure/2023-03-06%20PRC-Sweden%20Hypersonic%20Collaborations.pdf>
- ⁶⁸ FLASH DGSi #95 June 2023. The risks associated with know how acquisition in fundamental research. Foreign Interference Risks in Fundamental Research (DGSi Report)
- ⁶⁹ Czech Security Information Service Annual Report, (2023), <https://www.bis.cz/public/site/bis.cz/content/vyrocní-zpráva/2023-vz-aj.pdf>
- ⁷⁰ “Des acteurs malveillants cherchent à instrumentaliser la recherche française”: la DGSi formule sept préconisations”
- ⁷¹ Helmholtz (2024), ‘The Perceived Tension between Open Science and Research Security’, *Helmholtz Open Science Office*, <https://os.helmholtz.de/en/newsroom/news/article/the-perceived-tension-between-open-science-and-research-security/> ; NWO (2025), ‘Why knowledge security enables open science’, <https://www.nwo.nl/en/cases/why-knowledge-security-enables-open-science>
- ⁷² Riksrevisionen, (2023), ‘Information security at higher education institutions – management of research data requiring protection’ (2023), Audit Report, <https://www.riksrevisionen.se/en/audits/audit-reports/2023/information-security-at-higher-education-institutions---management-of-research-data-requiring-protection.html>
- ⁷³ For instance, the German Rectors Conference (HRK) has published China-specific guidance: HRK - German Rectors Conference. (2020). *Guiding Questions on University Cooperation with the People’s Republic of China*. https://www.chinazentrum.uni-kiel.de/de/aktuelles/datei-aktuelles/2023/info-china-kooperation/01_handreichungen-leitfaeden/03_HRK_Guiding-question-on-university-cooperation-with-the-PR-China_2020.pdf/
- ⁷⁴ Leopoldina’s guidelines also mention Al-Qaeda and the ‘so-called Islamic State’; Leopoldina, (2022) *The Handling of Security-Relevant Research in Germany – An Overview*. https://www.leopoldina.org/fileadmin/redaktion/Ueber_uns/Kooperationen/Information_The_Handling_of_Security-Relevant_Research_in_Germany_-_An_Overview_web.pdf p.15
- ⁷⁵ Interview: CZE RSO1
- ⁷⁶ To examine research security policies and practices, we used as our framework the G7’s *Best Practices for Research Security & Integrity* which emphasises the importance of establishing resources to promote awareness and forums for dialogue and information sharing on research security and integrity across all research stakeholders; the identification and sharing of information on which research areas are at risk; identification areas of risk activity by conducting due diligence and ensuring transparency and the disclosure of relevant information; and, the implementation of risk mitigation measures at the

organisational and project level. *G7 Best Practices for Secure and Open Research*. Security and Integrity of the Global Research Ecosystem (SIGRE) Working Group, February 2024

<https://science.gc.ca/site/science/en/safeguarding-your-research/general-information-research-security/international-research-security-resources/g7-best-practices-secure-and-open-research>.

⁷⁷ Interview ES UL-2.

⁷⁸ UHR (2024) *Responsible Internationalization. Partial Report of a Government Assignment* (Ansvarsfull internationalisering. Delrapportering av ett regeringsuppdrag, UHR:s rapportserie 2024:1)

https://www.uhr.se/globalassets/_uhr.se/publikationer/2024/ansvarsfull-internationalisering_uhr-2024_1.pdf

⁷⁹ UHR (2025), National Support Structure for Responsible Internationalisation,

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

⁸⁰ The Protective Security Act (2021) requires organisations with sensitive technologies to implement physical, personnel and information security measures to control access to certain facilities or systems. Those operators include universities.

⁸¹ France has the *Protection du Potentiel Scientifique et Technique de la Nation* (PPST) and a network of security and defence officials (FSDs) in most research institutions.

⁸² The Netherlands has a very developed policy framework for knowledge security and a central advice team in the form of the Contact Point for Knowledge Security

⁸³ The Czech Republic has paid considerable attention to the issue of foreign interference in its universities. The Czech Republic has published a series of guidance documents, most recently in 2024 the three so-called “Methodologies documents”. The Czech Republic has a cross government and cross research sector forum for research security matters called the Interdepartmental Working Group for Combating Illegitimate Interference in the Higher Education and Research Environment. Furthermore, the government has provided public seed corn funding to develop awareness and capacity in its universities.

⁸⁴ Germany has a complex and devolved system that has generated a wide variety of guidance documents, advisory networks and support structures.

⁸⁵ UK Research and Innovation (UKRI) is the national funding agency investing in science and research in the UK with a combined budget of more than £6 billion. In 2021, UKRI updated its terms and conditions for research grants to require recipients of UKRI funding to ensure that appropriate due diligence is undertaken on their collaborative activities. In April 2024, two new conditions were added to outline TR&I expectations for organisations in receipt of UKRI funding. Amendments have also been made to clarify adherence to statutory requirements, all UK legislation and sanctions, with specific reference to including export controls, the UK National Security and Investment Act and the Academic Technology Approval Scheme (ATAS). To support recipients when considering their approaches to ensuring trusted research and innovation, UKRI has published a document on UKRI Trusted Research and Innovation Principles.

<https://www.ukri.org/manage-your-award/good-research-resource-hub/trusted-research-and-innovation/>

⁸⁶ In 2024, the Czech Republic published three guidance documents on research security. The three so-called “Methodologies documents” published by the Interdepartmental Working Group for Combating Illegitimate Interference in the Higher Education and Research Environment are: *Strengthening Resilience Against Illegitimate Interference in the Higher Education and Research Environment*; *Methodological Recommendation for Risk Management In Research Security at the Institutional Level*; and *Methodological Recommendation Defining the Minimum Scope of Due Diligence and Risk Management in Cooperation with Third Parties within the Context of Strengthening the Resilience of the Higher Education and Research Environment against Illegitimate Interference (Methodological Recommendation for Cooperation with Third Parties)*

https://msmt.gov.cz/uploads/311/METHODOLOGICAL_RECOMMENDATION_FOR_RISK_MANAGEMENT_I_N_RESEARCH_SECURITY_AT_THE_INSTITUTIONAL_LEVEL.pdf

⁸⁷ See the Czech Security Information Service Annual Report, (2023)

<https://www.bis.cz/public/site/bis.cz/content/vyrocní-zpráva/2023-vz-aj.pdf> ; Swedish Security Service Sakerhetspolisens årsbok 2023-2024 (sakerhetspolisen.se) (Security Service Yearbook 2023-2024)

<https://sakerhetspolisen.se/download/18.5cb30b118d1e95affec37/1708502268494/L%C3%A4gesbild%202023-2024.pdf>; France's domestic intelligence agency (DGSI) publishes monthly security alerts and

one each year focuses on the research security threats facing universities

<https://www.dgsi.interieur.gouv.fr/dgsi-a-vos-cotes/contre-espionnage/conseils-aux-entreprises-flash-ingérance>

⁸⁸ Czech Government, (2023), 'Security Strategy of the Czech Republic 2023',

https://mzv.gov.cz/file/5161068/Security_Strategy_of_the_Czech_Republic_2023.pdf

⁸⁹ BMBF. (2024). *Position paper of the German Federal Ministry of Education and Research on research security in light of Zeitenwende*. https://www.bmbf.de/SharedDocs/Downloads/DE/2024/position-paper-research-security.pdf?__blob=publicationFile&v=4

⁹⁰ See for instance: R. Nestler, (2025) 'Germany slowly rethinks defence and security research', *Science Business*, <https://sciencebusiness.net/news/germany-slowly-rethinks-defence-and-security-research>

⁹¹ Vinnova (2024) Civil innovations will strengthen Sweden's defense capabilities, published: 17 June 2024 <https://www.vinnova.se/en/news/2024/06/civil-innovations-must-strengthen-swedens-defense-capabilities/> and interviews: SWE FA3-5.

⁹² European Commission (2024). final WHITE PAPER On options for enhancing support for research and development involving technologies with dual-use potential, COMMISSION Brussels, 24.1.2024 COM(2024) https://research-and-innovation.ec.europa.eu/system/files/2024-01/ec_rtd_white-paper-dual-use-potential.pdf

⁹³ Interviews: SWE FA3-5. EU UO1; EU UO3; EU UO4

⁹⁴ See H. Boytchev. (2023). 'Warning over German research with Chinese military', *Research Professional News*. <https://www.researchprofessionalnews.com/rr-news-europe-germany-2023-1-report-warns-of-widespread-work-with-chinese-military/>; P. Charon, & J-B, Jeangène Vilmer, (2021). *Chinese influence operations: A Machiavellian Moment*. Institute for Strategic Research (IRSEM); D. Plášek. (2022). 'Czech Republic: Chinese influence at universities as a clearly rising threat'. *CEIAS* [Online]; Senat (2021) Mieux protéger notre patrimoine scientifique et nos libertés académiques, Rapport d'information n° 873 (2020-2021), déposé le 29 septembre 2021 <https://www.senat.fr/rap/r20-873/r20-87329.html>

⁹⁵ Interviews: CZE PM2; CZE UA2; ITRSO1; FRUL3; SWE FA1; SWE FA2; SWE UA4

⁹⁶ Interviews: CZE PM1; CZE PM2; CZE RSO1; CZE UA2.

⁹⁷ Interviews: CZE UA2; CZE NALS1; ES UL2

⁹⁸ Interview SWE UO1.

⁹⁹ Interviews: CZE UA1; CZE UA2; ES UL2; SW UA1; SWE UA2; SWE UA3; SWE UA4; SWE UA10; SWE UA11

¹⁰⁰ Interview: SWE UA1; SWE UA2; SWE UA3; SWE UA4; SWE UA5; SWE UA8; SWE UA9; SWE UA11.

¹⁰¹ Interview ESP UL2; SWE UA1; SWE UA2; SWE UA4; SWE UA5.

¹⁰² Interview IT UL-1.

¹⁰³ In France, there is a centralised system of guidance for research performing organisations. This is provided by the Secrétariat général de la défense et de la sécurité nationale ['SGDSN'] and certain ministries. The Netherlands has the National Contact Point for Knowledge Security. The Swedish government is considering recommendations for a national support function. In Germany, there is continued debate about the need for such a central team. See Section 4.3 for more details.

¹⁰⁴ Decree No. 2024-430 of 14 May 2024 on various provisions relating to the protection of the Nation's scientific and technical potential, (2024).

<https://www.legifrance.gouv.fr/eli/decret/2024/5/14/PRMD2334561D/jo/texteAlias>

¹⁰⁵ Interview FR RSO-2.

¹⁰⁶ Interview IT UL-1.

¹⁰⁷ Interview IT UA-1.

¹⁰⁸ <https://www.dgsi.interieur.gouv.fr/dgsi-a-vos-cotes/contre-espionnage/conseils-aux-entreprises-flash-ingérance>

¹⁰⁹ (10) DGSi - Direction Générale de la Sécurité Intérieure: Overview | LinkedIn

¹¹⁰ <https://www.dgsi.interieur.gouv.fr/decouvrir-dgsi/nos-missions/protection-economique/mission-de-securite-economique-de-dgsi-au-profit> (Published on 25/10/2021 and updated on 26/11/2024)

¹¹¹ Czech Security Information Service Annual Report, (2023)

<https://www.bis.cz/public/site/bis.cz/content/vyrocní-zpravy/2023-vz-aj.pdf>

¹¹² Security Service Yearbook Säkerhetspolisens årsbok 2023-2024 (sakerhetspolisen.se)

¹¹³ Interviews: CZE UA2; SWE UA4

¹¹⁴ The ARMA virtual workshops took place in Autumn 2024. The *Promoting European cooperation in developing responses to research security challenges: Online Events Series* comprised three workshops covering research security risks: insider threats; resources for managing research security risks; and products to support research security management. There were over 300 sign-ups for the workshop series and an average attendance of 150 participants from across Europe.

¹¹⁵ The three so-called “Methodologies documents” published by the Interdepartmental Working Group for Combating Illegitimate Interference in the Higher Education and Research Environment are: *Strengthening Resilience Against Illegitimate Interference in the Higher Education and Research Environment*; *Methodological Recommendation for Risk Management In Research Security at the Institutional Level*; and *Methodological Recommendation Defining the Minimum Scope of Due Diligence and Risk Management in Cooperation with Third Parties within the Context of Strengthening the Resilience of the Higher Education and Research Environment against Illegitimate Interference (Methodological Recommendation for Cooperation with Third Parties)*

https://msmt.gov.cz/uploads/311/METHODOLOGICAL_RECOMMENDATION_FOR_RISK_MANAGEMENT_IN_RESEARCH_SECURITY_AT_THE_INSTITUTIONAL_LEVEL.pdf

¹¹⁶ In 2024, the government asked the Swedish Council for Higher Education, the Swedish Research Council and Vinnova to undertake an assignment to develop national guidelines on responsible internationalisation and make recommendations for a national support function for responsible internationalisation. The assignment submitted two reports that are being considered by the Minister for Education and Research. The first report was published in December 2024 and provided general guidance on responsible internationalisation. UHR (2024) *Responsible Internationalization. Partial Report of a Government Assignment* (Ansvarsfull internationalisering. Delrapportering av ett regeringsuppdrag, UHR:s rapportserie 2024:1) https://www.uhr.se/globalassets/_uhr.se/publikationer/2024/ansvarsfull-internationalisering_uhr-2024_1.pdf The second report on the national support structure was published in 2025. UHR (2025), *National Support Structure for Responsible Internationalisation*, https://www.uhr.se/globalassets/_uhr.se/english/about-the-council/national-support-function-for-responsible-internationalisation---final-report-2025.pdf

¹¹⁷ Interview: IT RSO1

¹¹⁸ These include recommendations addressing national authorities, national research funders and research performers as well as the Commission.

¹¹⁹ UHR (2025), *National Support Structure for Responsible Internationalisation*, https://www.uhr.se/globalassets/_uhr.se/english/about-the-council/national-support-function-for-responsible-internationalisation---final-report-2025.pdf

¹²⁰ T. Gabel. (2024). ‘Germany mulls new research security organisation’. *Science Business*. <https://sciencebusiness.net/news/germany-mulls-new-research-security-organisation>

¹²¹ Scholars at Risk Network (<https://www.scholarsatrisk.org/>)

¹²² The other technology areas listed included advanced connectivity, navigation and digital technologies, advanced sensing technologies, space and propulsion technologies, energy, robotics and autonomous systems, advanced materials, manufacturing, and recycling technologies.

¹²³ Contact Point for Knowledge Security, (n.d.) ‘Knowledge areas at increased risk’. <https://english.loketkennisveiligheid.nl/risk-analysis/knowledge-areas-at-increased-risk>

¹²⁴ Fraunhofer-Gesellschaft (2019), *Fraunhofer Principles of Cooperation*, <https://archives.greenairnews.com/www.fraunhofer.de/en/about-fraunhofer/corporate-responsibility/governance/declaration-project-cooperation.html>

¹²⁵ STINT (2020). *Responsible Internationalisation: Guidelines for reflection on international academic collaboration*. https://www.stint.se/wp-content/uploads/2020/02/STINT_Responsible_Internationalisation.pdf.

¹²⁶ All of which can be found at their website: <https://www.safeguarding-science.eu>

¹²⁷ Interdepartmental Working Group for Combating Illegitimate Interference in the Higher Education and Research Environment (2024) *Methodological Recommendation Defining the Minimum Scope of Due Diligence and Risk Management in Cooperation with Third Parties within the Context of Strengthening the Resilience of the Higher Education and Research Environment against Illegitimate Interference (Methodological Recommendation for Cooperation with Third Parties)*

https://msmt.gov.cz/uploads/311/METHODOLOGICAL_RECOMMENDATION_FOR_RISK_MANAGEMENT_IN_RESEARCH_SECURITY_AT_THE_INSTITUTIONAL_LEVEL.pdf

¹²⁸ Government of Canada (2024), 'Named Research Organisations', <https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/sensitive-technology-research-and-affiliations-concern/named-research-organizations>

¹²⁹ UHR (2025), *National Support Structure for Responsible Internationalisation*, https://www.uhr.se/globalassets/_uhr.se/english/about-the-council/national-support-function-for-responsible-internationalisation---final-report-2025.pdf

¹³⁰ Interview IT UA-1.

¹³¹ Regulation (EU) 2021/821 of the European Parliament and of the Council Setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast), (2021).

¹³² The proposals have generated considerable controversy in the Netherlands. See Ben Upton (2023) Dutch research security rules 'virtually impossible to implement', Times Higher Education, October 18, 2023. <https://www.timeshighereducation.com/news/dutch-research-security-rules-virtually-impossible-implement>

¹³³ <https://www.sgdsn.gouv.fr/nos-missions/proteger/proteger-le-potentiel-scientifique-et-technique-de-la-nation>

¹³⁴ <https://www.government.se/government-policy/foreign-and-security-policy/protective-security-ordinance-2021-955/>

¹³⁵ See B. Rappert (2007), *Biotechnology, Security and the Search for Limits: An Inquiry into Research and Methods*, Palgrave MacMillan.

¹³⁶ 'EECARO - About Us', (n.d.) EECARO, <https://eecaro.eu/about-eecaro/>

¹³⁷ <https://www.isp.se/eng/foreign-direct-investment/translation-of-the-screening-of-foreign-direct-investments-act>

¹³⁸ The scope of the 2023 Act with respect to foreign research funding remains unclear to some universities who are seeking clarification (Interview: SWE UA10-11).

¹³⁹ When describing *säkerhetsskydd*, which should be functionally understood as national security in a Swedish legal context, every organization – governmental, public, private or NGO, can be divided in two categories. In one category we have every organization that the state already has decided plays a critical role for the defense of Sweden, also known as the Total Defense. The total defense of Sweden is composed of the military and the civilian Swedish defense. The other category is made up of organizations that does not have this sort of task or obligation from the state. However, every organization in Sweden is by law obliged to assess whether or not any aspect of its operations have any sort of relevance, direct or indirect, for the security of Sweden.

¹⁴⁰ <https://www.government.se/contentassets/7d1bd1801f8d46a69ded4cd2a30bb6fe/protective-security-act-2018-585.pdf> [government.se]

¹⁴¹ Personal correspondence with SWE UA1.

¹⁴² In the event of intrusion into a ZRR, only the offender is likely to be sanctioned. Under no circumstances can the head of the school be sanctioned because of the capture of his knowledge and know-how contained in his ZRR.

¹⁴³ In April 2025 (as this report was undergoing its final revisions) the Netherlands announced a draft screening law for graduate students intending to work in "sensitive" subject areas.

¹⁴⁴ We acknowledge that the Group of Seven includes the European Union as a "non-enumerated member" and that EU officials were engaged in the development of the G7's reports on research security. Thus, it could be an alternative forum for standards setting.

¹⁴⁵ This point was raised numerous times by research managers in research performing organisations. The case for standardisation was also put by an Italian respondent who has played an important role in developing research security policy in Italy. Moreover, we note that the 2021 French Senat report *Better Protection For our Scientific Assets and Academic Freedoms* recommended the promotion of a reference document of standards and guidelines nationally, internationally, and in Europe to clarify universities' exchanges based on a requirement of due diligence and compliance with guidelines founded on respect for academic freedom and research integrity in accordance with the Bonn Declaration of 23 October 2020

and the work of the OECD. (Mieux protéger notre patrimoine scientifique et nos libertés académiques, Rapport d'information n° 873 (2020-2021), déposé le 29 septembre 2021 <https://www.senat.fr/rap/r20-873/r20-87329.html>).

¹⁴⁶ Capacity building does not have to begin from scratch. During our study, we identified very many examples of good practice. These include the training provided by the Helmholtz and others in Germany. Lund University in Sweden is offering a course on research security. There are some sector leaders who are engaging and advocating across Europe to raise awareness, capacity and capability, not least through the European Export Control Association for Research Organisations (EECARO). The UK's Higher Education Export Control Association (HEECA) is the sector-led national body of Higher Education Export Control practitioners in the UK and provides on-line training programmes on export controls and research security. The UK's Association of Research Managers & Administrators (ARMA) has delivered an STN sponsored virtual workshop series on research security for European peers and has worked with the European Association of Research Managers & Administrators (EARMA).

¹⁴⁷ An example is provided by the UK's national funding agency UK Research and Innovation (UKRI) that updated its terms and conditions for research grants to require recipients of UKRI funding to ensure that appropriate due diligence is undertaken on their collaborative activities. In April 2024, two new conditions were added to outline TR&I expectations for organisations in receipt of UKRI funding. Amendments have also been made to clarify adherence to statutory requirements, all UK legislation and sanctions, with specific reference to including export controls, the UK National Security and Investment Act and the Academic Technology Approval Scheme (ATAS). To support recipients when considering their approaches to ensuring trusted research and innovation, UKRI has published a document on UKRI Trusted Research and Innovation Principles. <https://www.ukri.org/manage-your-award/good-research-resource-hub/trusted-research-and-innovation/>

¹⁴⁸ These matters are the subject of on-going discussion not least through Science Europe.

¹⁴⁹ One example of the dynamic nature of this policy space is provided by the recent developments in the Netherlands with the Government's announcement of a draft screening law for graduate students intending to work in "sensitive" subject areas.

¹⁵⁰ *G7 Common Values and Principles on Research Security and Research Integrity* (2022). <https://science.gc.ca/site/science/en/safeguarding-your-research/general-information-research-security/international-research-security-resources/g7-common-values-and-principles-research-security-and-research-integrity>

¹⁵¹ The G7 defines research integrity as: "the adherence to professional values, principles, and best practices which uphold the validity, social relevance, responsibility and quality of research – forms the base on which researchers can collaborate in a fair, innovative, open and trusted research environment. Research integrity ensures that individuals can be confident in the advancement of research knowledge and in the dissemination of its results". *G7 Best Practices for Secure & Open Research*, Security and Integrity of the Global Research Ecosystem (SIGRE) Working Group (2024): p.3.

<https://science.gc.ca/site/science/en/safeguarding-your-research/general-information-research-security/international-research-security-resources/g7-best-practices-secure-and-open-research>

¹⁵² See for instance the ranking of per capita share of outputs in the Nature Index, in which these countries join the UK in the European top 10: <https://www.nature.com/nature-index/country-outputs/generate/all/Europe>

¹⁵³ The five critical technologies are artificial intelligence, engineering biology, future telecommunications, semiconductors, and quantum technologies. <https://www.gov.uk/government/publications/science-and-technology-framework/science-and-technology-framework>

¹⁵⁴ Data analysis enabled by the <https://www.lens.org/> [lens.org]

¹⁵⁵ The Lens is an informetric database comprising both bibliometric and patent data which was established in 1998. The Lens compares favourably with the more established databases of publication data, providing high levels of data coverage and structured query facilities making it suitable for a variety of science mapping activities. More details are available in Velez-Estevez, A., Perez, I. J., García-Sánchez, P., Moral-Munoz, J. A., & Cobo, M. J. (2023). New trends in bibliometric APIs: A comparative analysis. *Information Processing & Management*, 60(4), 103385.

<https://doi.org/https://doi.org/10.1016/j.ipm.2023.103385>

- ¹⁵⁶ European Commission. (2024). Ares (2023)8333434, Boosting research security in the EU (guidance): Call for Evidence. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14056-Boosting-research-security-in-the-EU-guidance_en
- ¹⁵⁷ The three reports published in 2024 by the Interdepartmental Working Group for Combating Illegitimate Interference in the Higher Education and Research Environment are: *Strengthening Resilience Against Illegitimate Interference in the Higher Education and Research Environment*; *Methodological Recommendation for Risk Management In Research Security at the Institutional Level*; and *Methodological Recommendation Defining the Minimum Scope of Due Diligence and Risk Management in Cooperation with Third Parties within the Context of Strengthening the Resilience of the Higher Education and Research Environment against Illegitimate Interference (Methodological Recommendation for Cooperation with Third Parties)* https://msmt.gov.cz/uploads/311/METHODOLOGICAL_RECOMMENDATION_FOR_RISK_MANAGEMENT_IN_RESEARCH_SECURITY_AT_THE_INSTITUTIONAL_LEVEL.pdf
- ¹⁵⁸ There have also been a number of related reports, including Ministry of Defence of the Czech Republic. (2021). *National Strategy for Countering Hybrid Interference* <https://www.mo.gov.cz/assets/en/ministry-of-defence/basic-documents/national-strategy---aj-final.pdf>; National Cyber and Information Security Agency. (2015). *Action Plan for the National Cyber Security Strategy of the The Czech Republic for the Period from 2015 to 2020*. <https://nukib.gov.cz/en/cyber-security/strategy-action-plan/>; National Cyber and Information Security Agency. (2021). *National Cyber Strategy of the Czech Republic, for the period 2021-2025*. <https://nukib.gov.cz/en/cyber-security/strategy-action-plan/>; D. Plášek. (2022). 'Czech Republic: Chinese influence at universities as a clearly rising threat'. CEIAS [Online]. <https://ceias.eu/czech-republic-chinese-influence-at-universities-as-a-clearly-rising-threat/>
- ¹⁵⁹ Centre Against Hybrid Threats. (2021). *Counter Foreign Interference Manual for the Czech Academic Sector*. https://cuni.cz/UK-11805-version1-cfi_manual_for_the_czech_academic_sector.pdf
- ¹⁶⁰ Financial Analytical Office. (2021). *Handbook: Technical Assistance and Intangible Transfer of Technology*. <https://www.financnianalytickurad.cz/files/prirucka-technicke-pomoci-a-nehmotneho-prenosu-technologie.pdf>
- ¹⁶¹ D. Toman., J. Famfollet. (2022). 'Protecting Universities and Research from Foreign Interference and Illicit Technology and Transfer: A Comparison of Existing Policies and Lessons Learned from Europe, Japan and Taiwan from Legislative and Policy Updates'. *European Values Centre for Security Policy*. <https://europeanvalues.cz/en/protecting-universities-and-research-from-foreign-interference-and-illicit-technology-transfer/>; D. Plášek. (2022). 'Selected findings from relationship research and cooperation between Czech academic institutions and entities from the People's Republic of China'. *European Values Centre for Security Policy*. https://europeanvalues.cz/wp-content/uploads/2023/01/REPORT_en_How_chinese_entities_influence_academic_institutions_and_how_to_prevent_related_security_threats.pdf; J. Famfollet. (2022). 'Protection of strategic and dual-use technologies: a take on the current situation and various approaches'. *European Values Centre for Security Policy*. https://europeanvalues.cz/wp-content/uploads/2022/08/REPORT_en_Protection_of_Strategic_and_Dual-Use_Technologies-2022.pdf; I. Karásková., F. Šebok., V. Blablová. (2022). 'How to do trusted research: China-specific guidelines for European stakeholders.' *Association for International Affairs (AMO)*. <https://chinaobservers.eu/how-to-do-trusted-research-china-specific-guidelines-for-european-stakeholders/>
- ¹⁶² Data from OECD Data Explorer: Enrolments of mobile students by countries of origin and total enrolments for 2022. <https://data-viewer.oecd.org?chartId=9f81c085-54fa-4476-966a-6f6e47e7431d>
- ¹⁶³ Charles University, (n.d). 'Facts and Figures', <https://cuni.cz/uken-109.html>
- ¹⁶⁴ Kwiek M. (2021), 'What large-scale publication and citation data tell us about international research collaboration in Europe: changing national patterns in global contexts', *Studies in Higher Education*. 46(12) :2629-2649. <https://doi.org/10.1080/03075079.2020.1749254>
- ¹⁶⁵ National Science Board (2023), *Science and Engineering Indicators: Publications Output: U.S. Trends and International Comparisons. Supplementary Table SPBS-33* <https://nces.nsf.gov/pubs/nsb202333/table/SPBS-33>
- ¹⁶⁶ European Research Area Platform, (n.d.), 'ERA Performance Indicators', <https://european-research-area.ec.europa.eu/scoreboard-reports?countries%5B0%5D=42&countries%5B1%5D=46&countries%5B2%5D=25&countries%5B3%5D>

=50&countries%5B4%5D=55&countries%5B5%5D=60&countries%5B6%5D=61&edit-countries-42=on&edit-countries-46=on&edit-countries-25=on&edit-countries-50=on&edit-countries-55=on&edit-countries-60=on&edit-countries-61=on&field_related_sb_indicator_target_id=123

¹⁶⁷ Czech Government, (2024), *Strengthening Resilience Against Illegitimate Interference in the Higher Education and Research Environment*,

https://msmt.gov.cz/uploads/311/STRENGTHENING_RESILIENCE_AGAINST_ILLEGITIMATE_INFLUENCE_INTERFERENCE_IN_THE_HIGHER_EDUCATION_AND_RESEARCH_ENVIRONMENT.pdf, pp. 3-4

¹⁶⁸ Czech Government, (2024), *Strengthening Resilience Against Illegitimate Interference in the Higher Education and Research Environment*,

https://msmt.gov.cz/uploads/311/STRENGTHENING_RESILIENCE_AGAINST_ILLEGITIMATE_INFLUENCE_INTERFERENCE_IN_THE_HIGHER_EDUCATION_AND_RESEARCH_ENVIRONMENT.pdf, p.4

¹⁶⁹ Interview: CZE PM1; CZE PM2; CZE RSO1

¹⁷⁰ Interviews: CZE PM1; CZE PM2; CZE RSO1

¹⁷¹ D. Plášek. (2022). 'Czech Republic: Chinese influence at universities as a clearly rising threat'. CEIAS [Online]. <https://ceias.eu/czech-republic-chinese-influence-at-universities-as-a-clearly-rising-threat/>

¹⁷² Source: presentation by the Ministry of Interior during a conference at Charles University, November 2024

¹⁷³ Interview: CZE RSO1

¹⁷⁴ Interview: CZE UA2

¹⁷⁵ Interview: CZE PM2

¹⁷⁶ The Methodologies Reports do not specify the selected fields.

¹⁷⁷ Czech Government (2024), *Strengthening Resilience Against Illegitimate Interference in the Higher Education and Research Environment*,

https://msmt.gov.cz/uploads/311/STRENGTHENING_RESILIENCE_AGAINST_ILLEGITIMATE_INFLUENCE_INTERFERENCE_IN_THE_HIGHER_EDUCATION_AND_RESEARCH_ENVIRONMENT.pdf, p.4

¹⁷⁸ Czech Government, (2023), 'Security Strategy of the Czech Republic 2023',

https://mzv.gov.cz/file/5161068/Security_Strategy_of_the_Czech_Republic_2023.pdf

¹⁷⁹ K. Hille and J. Shotter (2019) 'Czech university mired in Chinese influence scandal: Secret payments to academics renew concerns about Beijing's encroachment', *Financial Times*, 11 November 2019; I.

D'Hooghe., J. Lammertink. (2020). 'Towards Sustainable Europe-China Collaboration in Higher Education in Research'. *Leiden Asia Centre*. <https://leidenasiacentre.nl/wp-content/uploads/2020/10/Towards-Sustainable-Europe-China-Collaboration-in-Higher-Education-and-Research.pdf>

¹⁸⁰ The Central European Institute of Asian Studies (CEIAS), AMO and the European Values Center have all emphasised the threat posed by China and in a series of reports around 2022 they called for the government to introduce more guidelines and legal frameworks to tackle undue Chinese interference.

¹⁸¹ K. Hille and J. Shotter (2019) 'Czech university mired in Chinese influence scandal: Secret payments to academics renew concerns about Beijing's encroachment', *Financial Times*, 11 November 2019; I.

D'Hooghe., J. Lammertink. (2020). 'Towards Sustainable Europe-China Collaboration in Higher Education in Research'. *Leiden Asia Centre*. <https://leidenasiacentre.nl/wp-content/uploads/2020/10/Towards-Sustainable-Europe-China-Collaboration-in-Higher-Education-and-Research.pdf>

¹⁸² D. Plášek. (2022). 'Czech Republic: Chinese influence at universities as a clearly rising threat'. CEIAS [Online]. <https://ceias.eu/czech-republic-chinese-influence-at-universities-as-a-clearly-rising-threat/>

¹⁸³ Interviews: CZE RSO1; CZE IE1; CZE PM1; CZE UA2

¹⁸⁴ Czech Government, (2024), *Strengthening Resilience Against Illegitimate Interference in the Higher Education and Research Environment*,

https://msmt.gov.cz/uploads/311/STRENGTHENING_RESILIENCE_AGAINST_ILLEGITIMATE_INFLUENCE_INTERFERENCE_IN_THE_HIGHER_EDUCATION_AND_RESEARCH_ENVIRONMENT.pdf,

¹⁸⁵ Czech Government, (2024), *Strengthening Resilience Against Illegitimate Interference in the Higher Education and Research Environment*,

https://msmt.gov.cz/uploads/311/STRENGTHENING_RESILIENCE_AGAINST_ILLEGITIMATE_INFLUENCE_INTERFERENCE_IN_THE_HIGHER_EDUCATION_AND_RESEARCH_ENVIRONMENT.pdf,

¹⁸⁶ Interviews: CZE PM1; CZE IE1.

¹⁸⁷ Czech Government (2024), *Strengthening Resilience against Illegitimate Interference in the Higher Education and Research Environment*

https://msmt.gov.cz/uploads/311/STRENGTHENING_RESILIENCE_AGAINST_ILLEGITIMATE_INFLUENCE_INTERFERENCE_IN_THE_HIGHER_EDUCATION_AND_RESEARCH_ENVIRONMENT.pdf, pp.3-4

¹⁸⁸ Interviews: CZE RSO1; CZE UA1; CZE UA2; CZE NALS1

¹⁸⁹ Interviews: CZE IE1; CZE UA1; CZE UA2

¹⁹⁰ Interview: CZE UA1

¹⁹¹ Interview: CZE UA2

¹⁹² Interviews: CZE UA1; CZE UA2

¹⁹³ Interviews: CZE IE1; CZE UA1; CZE UA2; CZE NALS1.

¹⁹⁴ *Methodological Recommendation Defining the Minimum Scope of Due Diligence and Risk Management in Cooperation with Third Parties within the Context of Strengthening the Resilience of the Higher Education and Research Environment against Illegitimate Interference (Methodological Recommendation for Cooperation with Third Parties)*

https://msmt.gov.cz/uploads/311/METHODOLOGICAL_RECOMMENDATION_FOR_RISK_MANAGEMENT_IN_RESEARCH_SECURITY_AT_THE_INSTITUTIONAL_LEVEL.pdf

¹⁹⁵ Interview: CZE NALS1

¹⁹⁶ Ingrid d’Hooghe and Jonas Lammertink in their comparative report on European responses to knowledge security for the Leiden Asia Centre & AWTI in 2022 commented that the Czech response, though comprehensive, seemed to lack a certain level of coherence. I. D’Hooghe., J. Lammertink. (2022). ‘How National Governments and Research Institutions Safeguard Knowledge Development in Science and Technology’, *Leiden Asia Centre & AWTI*. <https://leidenasiacentre.nl/wp-content/uploads/2022/11/How-National-Governments-and-Research-Institutions-Safeguard-Knowledge-Development-in-Science-and-Technology.pdf> p.16.

¹⁹⁷ Interview UA1; UA2

¹⁹⁸ *National Strategy for Countering Hybrid Interference* <https://www.mo.gov.cz/assets/en/ministry-of-defence/basic-documents/national-strategy---aj-final.pdf>;

¹⁹⁹ <https://fau.gov.cz/files/prirucka-technicke-pomoci-a-nehmotneho-prenosu-technologie-en.pdf>

²⁰⁰

https://msmt.gov.cz/uploads/311/STRENGTHENING_RESILIENCE_AGAINST_ILLEGITIMATE_INFLUENCE_INTERFERENCE_IN_THE_HIGHER_EDUCATION_AND_RESEARCH_ENVIRONMENT.pdf

²⁰¹

https://msmt.gov.cz/uploads/311/METHODOLOGICAL_RECOMMENDATION_FOR_RESEARCH_SECURITY_DUE_DILIGENCE_AND_RISK_MANAGEMENT_IN_COOPERATION_WITH_THIRD_PARTIES.pdf

²⁰²

https://msmt.gov.cz/uploads/311/METHODOLOGICAL_RECOMMENDATION_FOR_RISK_MANAGEMENT_IN_RESEARCH_SECURITY_AT_THE_INSTITUTIONAL_LEVEL.pdf

²⁰³ Interview: CZE PM1; CZE RSO1

²⁰⁴ Interviews: CZE UA1; CZE UA2; CZE NALS1

²⁰⁵ An article from CEIAS in 2022 questioned the extent to which such tools are used in practice and argued that the Counter Interference Manual was underused when universities perform risk assessments or due diligence. D. Plášek. (2022). ‘Czech Republic: Chinese influence at universities as a clearly rising threat’. *CEIAS* [Online]. <https://ceias.eu/czech-republic-chinese-influence-at-universities-as-a-clearly-rising-threat/>

²⁰⁶ Interviews: CZE PM1

²⁰⁷ Czech Government, (2024), *Strengthening Resilience Against Illegitimate Interference in the Higher Education and Research Environment*,

https://msmt.gov.cz/uploads/311/STRENGTHENING_RESILIENCE_AGAINST_ILLEGITIMATE_INFLUENCE_INTERFERENCE_IN_THE_HIGHER_EDUCATION_AND_RESEARCH_ENVIRONMENT.pdf.

²⁰⁸ I. d’Hooghe and J. Lammertink (2022). How National Governments and Research Institutions Safeguard Knowledge Development in Science and Technology. *Leiden Asia Centre*, <https://leidenasiacentre.nl/wp-content/uploads/2022/11/How-National-Governments-and-Research-Institutions-Safeguard-Knowledge-Development-in-Science-and-Technology.pdf> p.64.

²⁰⁹ Interview FR RSO-2.

²¹⁰ Code civil (Civil Code) (2025). Article 413-5 of the French Penal Code.

- ²¹¹ French Government (2024). Decree No. 2024-430 of 14 May 2024 on various provisions relating to the protection of the Nation's scientific and technical potential.
- ²¹² OECD (2024). *OECD Main Science and Technology Indicators Database, March 2024*. <http://oe.cd/mst>
- ²¹³ Campus France. (2024). *The different types of institutes of higher education in France*. <https://www.campusfrance.org/en/institutes-higher-education-France>
- ²¹⁴ ANR. (2025). *Research Projects Funding*. <https://anr.fr/?id=2037>
- ²¹⁵ International academics and researchers at public universities and research institutes in major host countries, (n.d.), *Wissenschaft weltoffen*, <https://www.wissenschaft-weltoffen.de/en/in-focus-selected-findings-of-the-publication/international-academics-and-researchers-at-public-universities-and-research-institutes-in-major-host-countries/>
- ²¹⁶ Data from OECD Data Explorer: Enrolled mobile students in tertiary education and total enrolments in tertiary education for 2022. <https://data-explorer.oecd.org/> [data-explorer.oecd.org]
- ²¹⁷ Kwiek M. (2021), 'What large-scale publication and citation data tell us about international research collaboration in Europe: changing national patterns in global contexts', *Studies in Higher Education*, 46(12) :2629-2649, <https://doi.org/10.1080/03075079.2020.1749254>
- ²¹⁸ National Science Board (2023), Science and Engineering Indicators: Publications Output: U.S. Trends and International Comparisons. Supplementary Table SPBS-33, <https://nces.nsf.gov/pubs/nsb202333/table/SPBS-33>
- ²¹⁹ European Research Area (n.d). *ERA Performance Indicators*, https://european-research-area.ec.europa.eu/scoreboard-reports?countries%5B0%5D=42&countries%5B1%5D=46&countries%5B2%5D=25&countries%5B3%5D=50&countries%5B4%5D=55&countries%5B5%5D=60&countries%5B6%5D=61&edit-countries-42=on&edit-countries-46=on&edit-countries-25=on&edit-countries-50=on&edit-countries-55=on&edit-countries-60=on&edit-countries-61=on&field_related_sb_indicator_target_id=123
- ²²⁰ Mieux protéger notre patrimoine scientifique et nos libertés académiques (Better Protection for our Scientific Assets and Academic Freedoms), Rapport d'information n° 873 (2020-2021), déposé le 29 septembre 2021 <https://www.senat.fr/rap/r20-873/r20-87329.html> The report was the conclusion of a fact-finding mission established in July 2021 at the initiative of the Rassemblement des démocrates, progressistes et indépendants (RDPI) group, chaired by Etienne Blanc with André Gattolin as rapporteur.
- ²²¹ <https://www.dgsi.interieur.gouv.fr/decouvrir-dgsi/nos-missions/protection-economique/mission-de-securite-economique-de-dgsi-au-profit> (Published on 25/10/2021 and updated on 26/11/2024)
- ²²² Mieux protéger notre patrimoine scientifique et nos libertés académiques, Rapport d'information n° 873 (2020-2021), déposé le 29 septembre 2021 <https://www.senat.fr/rap/r20-873/r20-87329.html>
- ²²³ <https://www.aefinfo.fr/depeche/701901-ingerences-les-institutions-academiques-francaises-de-plus-en-plus-dependantes-de-financements-etrangers-parlement>
- ²²⁴ "Des acteurs malveillants cherchent à instrumentaliser la recherche française" : la DGSi formule sept préconisations"
- ²²⁵ [DGSi et DRSD alertent sur les ingérences étrangères dans le milieu scientifique - Next](https://next.ink/143159/dgsi-et-drds-alertent-sur-les-ingerences-etrangeres-dans-le-milieu-scientifique/?utm_source=chatgpt.com) DGSi and DRSD warn of foreign interference in the scientific community) (https://next.ink/143159/dgsi-et-drds-alertent-sur-les-ingerences-etrangeres-dans-le-milieu-scientifique/?utm_source=chatgpt.com
- ²²⁶ FLASH DGSi #95 June 2023. The risks associated with know how acquisition in fundamental research. Foreign Interference Risks in Fundamental Research (DGSi Report)
- ²²⁷ Mieux protéger notre patrimoine scientifique et nos libertés académiques, Rapport d'information n° 873 (2020-2021), déposé le 29 septembre 2021 <https://www.senat.fr/rap/r20-873/r20-87329.html>
- ²²⁸ European Think-tank Network on China (ETNC) (2024). National Perspectives on Europe's De-risking from China. https://www.clingendael.org/sites/default/files/2024-7/ETNC2024_National_Perspectives_on_Europes_De-risking_from_China.pdf
- ²²⁹ Mieux protéger notre patrimoine scientifique et nos libertés académiques, Rapport d'information n° 873 (2020-2021), déposé le 29 septembre 2021 <https://www.senat.fr/rap/r20-873/r20-87329.html>
- ²³⁰ A. Parnier (2023). Balancing Security and Openness for Critical Technologies: Challenges for French and European Research. Paris: Institut Français des Relations Internationales (IFRI).
- ²³¹ Interview FR UL-1
- ²³² Interview FR RSO-2.

-
- ²³³ Mieux protéger notre patrimoine scientifique et nos libertés académiques, Rapport d'information n° 873 (2020-2021), déposé le 29 septembre 2021 <https://www.senat.fr/rap/r20-873/r20-87329.html>
- ²³⁴ <https://www.sgdsn.gouv.fr/nos-missions/protéger/protéger-le-potentiel-scientifique-et-technique-de-la-nation>
- ²³⁵ <https://www.sgdsn.gouv.fr/nos-missions/protéger/protéger-le-potentiel-scientifique-et-technique-de-la-nation>
- ²³⁶ Interview FR UL-1.
- ²³⁷ Pannier, A. (2023). Balancing Security and Openness for Critical Technologies: Challenges for French and European Research. *French Institute for International Relations*. <https://www.ifri.org/en/studies/balancing-security-and-openness-critical-technologies-challenges-french-and-european>
- ²³⁸ Mieux protéger notre patrimoine scientifique et nos libertés académiques, Rapport d'information n° 873 (2020-2021), déposé le 29 septembre 2021 <https://www.senat.fr/rap/r20-873/r20-87329.html>
- ²³⁹ Mieux protéger notre patrimoine scientifique et nos libertés académiques, Rapport d'information n° 873 (2020-2021), déposé le 29 septembre 2021 <https://www.senat.fr/rap/r20-873/r20-87329.html>
- ²⁴⁰ Mieux protéger notre patrimoine scientifique et nos libertés académiques, Rapport d'information n° 873 (2020-2021), déposé le 29 septembre 2021 <https://www.senat.fr/rap/r20-873/r20-87329.html>
- ²⁴¹ Interview FR RSO-2.
- ²⁴² Code civil (Civil Code) (2025). Article 413-5 of the French Penal Code.
- ²⁴³ French Government (2024). Decree No. 2024-430 of 14 May 2024 on various provisions relating to the protection of the Nation's scientific and technical potential.
- ²⁴⁴ I. d'Hooghe, J. Lammertink, (2022). How National Governments and Research Institutions Safeguard Knowledge Development in Science and Technology, *Leiden Asia Centre*, <https://leidenasiacentre.nl/wp-content/uploads/2022/11/How-National-Governments-and-Research-Institutions-Safeguard-Knowledge-Development-in-Science-and-Technology.pdf>
- ²⁴⁵ Interview FR UL-3.
- ²⁴⁶ <https://www.dgsi.interieur.gouv.fr/decouvrir-dgsi/nos-missions/protection-economique/mission-de-securite-economique-de-dgsi-au-profit> (Published on 25/10/2021 and updated on 26/11/2024)
- ²⁴⁷ <https://www.dgsi.interieur.gouv.fr/decouvrir-dgsi/nos-missions/protection-economique/mission-de-securite-economique-de-dgsi-au-profit> (Published on 25/10/2021 and updated on 26/11/2024)
- ²⁴⁸ "Des acteurs malveillants cherchent à instrumentaliser la recherche française": la DGSi formule sept préconisations"
- ²⁴⁹ SGDSN. Le dispositif de protection du potentiel scientifique et technique de la nation – Foire aux questions, <https://www.sgdsn.gouv.fr/nos-missions/protéger/protéger-le-potentiel-scientifique-et-technique-de-la-nation/foire-aux-questions>
- ²⁵⁰ <https://www.dgsi.interieur.gouv.fr/decouvrir-dgsi/nos-missions/protection-economique/mission-de-securite-economique-de-dgsi-au-profit> (Published on 25/10/2021 and updated on 26/11/2024)
- ²⁵¹ International academics and researchers at public universities and research institutes in major host countries, (n.d.), *Wissenschaft weltoffen*, <https://www.wissenschaft-weltoffen.de/en/in-focus-selected-findings-of-the-publication/international-academics-and-researchers-at-public-universities-and-research-institutes-in-major-host-countries/>
- ²⁵² Total international academic staff and international professors, by key countries of origin, since 2013, (n.d.), *Wissenschaft Weltoffen*, <https://www.wissenschaft-weltoffen.de/en/in-focus-selected-findings-of-the-publication/total-international-academic-staff-and-international-professors-by-key-countries-of-origin-since-2013/>
- ²⁵³ Germany International Student Statistics, (n.d.) Study in Germany, <https://www.studying-in-germany.org/germany-international-student-statistics/>
- ²⁵⁴ Germany International Student Statistics, (n.d.) Study in Germany, <https://www.studying-in-germany.org/germany-international-student-statistics/>
- ²⁵⁵ Kwiek M. (2021), 'What large-scale publication and citation data tell us about international research collaboration in Europe: changing national patterns in global contexts', *Studies in Higher Education*. 46(12) :2629-2649. <https://doi.org/10.1080/03075079.2020.1749254>

-
- ²⁵⁶ National Science Board (2023), *Science and Engineering Indicators: Publications Output: U.S. Trends and International Comparisons. Supplementary Table SPBS-33*
<https://nces.nsf.gov/pubs/nsb202333/table/SPBS-33>
- ²⁵⁷ European Research Area (n.d). *ERA Performance Indicators*, https://european-research-area.ec.europa.eu/scoreboard-reports?countries%5B0%5D=42&countries%5B1%5D=46&countries%5B2%5D=25&countries%5B3%5D=50&countries%5B4%5D=55&countries%5B5%5D=60&countries%5B6%5D=61&edit-countries-42=on&edit-countries-46=on&edit-countries-25=on&edit-countries-50=on&edit-countries-55=on&edit-countries-60=on&edit-countries-61=on&field_related_sb_indicator_target_id=123
- ²⁵⁸ BMBF. (2024). *Position paper of the German Federal Ministry of Education and Research on research security in light of Zeitenwende*. https://www.bmbf.de/SharedDocs/Downloads/de/2024/position-paper-research-security.pdf?__blob=publicationFile&v=1;
- ²⁵⁹ Interview DE NALS-1
- ²⁶⁰ Interviews DE FA1, DE FA2
- ²⁶¹ HRK - German Rectors Conference. (2020). *Guidelines and Standards in International University Cooperation*. https://www.hrk.de/fileadmin/redaktion/hrk/02-Dokumente/02-01-Beschluesse/Beschluss_Leitlinien_und_Standards_HRK_Praesidium_6.4.2020_EN.pdf ;HRK - German Rectors Conference. (2020). *Guiding Questions on University Cooperation with the People's Republic of China*. https://www.chinazentrum.uni-kiel.de/de/aktuelles/datei-aktuelles/2023/info-china-kooperation/01_handreichungen-leitfaeden/03_HRK_Guiding-question-on-university-cooperation-with-the-PR-China_2020.pdf/
- ²⁶² DFG & Leopoldina. (2022). *The Handling of Security-Relevant Research in Germany – An Overview*. https://www.leopoldina.org/fileadmin/redaktion/Ueber_uns/Kooperationen/Information_The_Handling_of_Security-Relevant_Research_in_Germany_-_An_Overview_web.pdf
- ²⁶³ See e.g. H. Boytchev. (2023). 'Warning over German research with Chinese military', *Research Professional News*. <https://www.researchprofessionalnews.com/rr-news-europe-germany-2023-1-report-warns-of-widespread-work-with-chinese-military/>
- ²⁶⁴ Federal Government of Germany. (2023). *Strategy on China: Of the Government of the Federal Republic of Germany*. <https://www.auswaertiges-amt.de/blob/2608580/49d50fecc479304c3da2e2079c55e106/china-strategie-en-data.pdf>
- ²⁶⁵ DFG. (2023). *Dealing with Risks in International Cooperation*. <https://www.dfg.de/resource/blob/289704/585cb3b48bb8e9f5b6e57e0e0a0d700e/risiken-int-kooperationen-en-data.pdf>
- ²⁶⁶ BAFA. (2023). *Manual Export Control and Academia*. (2nd Edition). https://www.bafa.de/SharedDocs/Downloads/EN/Foreign_Trade/ec_manual_export_control_and_academia.html?nn=1444524
- ²⁶⁷ e.g. DAAD (2024) *Strengthening International Academic Cooperation*, https://static.daad.de/media/daad_de/pdfs_nicht_barrierefrei/infos-services-fuer-hochschulen/kompetenzzentrum/daad_kiwi_en.pdf; DAAD (2020-) *KiWi Compass: No Red Lines* <https://www.daad.de/kiwi-kompass/no-red-lines/>; DAAD (2024) *Academic cooperation with China: a realistic approach - DAAD recommendations to German higher education institutions*, https://static.daad.de/media/daad_de/der-daad/kommunikation-publikationen/presse/240307_daad_perspektive_china_en.pdf
- ²⁶⁸ OPERATE: Application to assess opportunities & risks of research cooperation: <https://www.safeguarding-science.eu/tools/operate/>
- ²⁶⁹ i.e. the clash of values that can emerge where research has both the potential to advance knowledge and useful technology but also to enable or risk harmful outcomes.
- ²⁷⁰ DFG & Leopoldina. (2014). *Scientific Freedom and Scientific Responsibility: Recommendations for Handling Security Relevant Research*. https://www.leopoldina.org/uploads/tx_leopublication/2014_06_DFG-Leopoldina_Scientific_Freedom_Responsibility_EN.pdf
- ²⁷¹ Interviews DE NALS-1, DE FA-1
- ²⁷² Some interviewees (e.g. DE FA-1, DE FA-2, DE UA-1) discussed the implications for research security policy of the responsibility that the länder have for higher education, but it is worth noting that the newly-
-

established council of research ministers from each federal state will consider matters such as research security: <https://www.forschung-und-lehre.de/politik/wissenschaftsministerkonferenz-gegruendet-6774>

²⁷³ There was clear consensus about this amongst all our interviewees.

²⁷⁴ BMBF. (2024). *Position paper of the German Federal Ministry of Education and Research on research security in light of Zeitenwende*. https://www.bmbf.de/SharedDocs/Downloads/DE/2024/position-paper-research-security.pdf?__blob=publicationFile&v=4

²⁷⁵ BMBF. (2024). *Position paper of the German Federal Ministry of Education and Research on research security in light of Zeitenwende*. https://www.bmbf.de/SharedDocs/Downloads/DE/2024/position-paper-research-security.pdf?__blob=publicationFile&v=4

²⁷⁶ Interview DE PM-1

²⁷⁷ D. Matthews. (2020). 'Hamburg Confucius Split latest sign of German caution over China', *Times Higher Education*. <https://www.timeshighereducation.com/news/hamburg-confucius-split-latest-sign-german-caution-over-china>. H. Boytchev. (2023). 'Warning over German research with Chinese military', *Research Professional News*. <https://www.researchprofessionalnews.com/rr-news-europe-germany-2023-1-report-warns-of-widespread-work-with-chinese-military/>

²⁷⁸ I. D'Hooghe., J. Lammertink. (2022). 'How National Governments and Research Institutions Safeguard Knowledge Development in Science and Technology'. *Leiden Asia Centre & AWTI*. <https://leidenasiacentre.nl/wp-content/uploads/2022/11/How-National-Governments-and-Research-Institutions-Safeguard-Knowledge-Development-in-Science-and-Technology.pdf> p.30.

²⁷⁹ DFG & Leopoldina. (2022). *The Handling of Security-Relevant Research in Germany – An Overview*. https://www.leopoldina.org/fileadmin/redaktion/Ueber_uns/Kooperationen/Information_The_Handling_of_Security-Relevant_Research_in_Germany_-_An_Overview_web.pdf

²⁸⁰ E.g. DE FA-1, DE FA-2, DE UO-1.

²⁸¹ BAFA. (2023). *Manual Export Control and Academia*. https://www.bafa.de/SharedDocs/Downloads/EN/Foreign_Trade/ec_manual_export_control_and_academia.html?nn=1444524; BAFA. (2019). *Export Control in Science and Research*. https://www.bafa.de/SharedDocs/Downloads/EN/Foreign_Trade/ec_awareness_academia.htm

²⁸² DFG & Leopoldina. (2022). *The Handling of Security-Relevant Research in Germany – An Overview*. https://www.leopoldina.org/fileadmin/redaktion/Ueber_uns/Kooperationen/Information_The_Handling_of_Security-Relevant_Research_in_Germany_-_An_Overview_web.pdf

²⁸³ HRK - German Rectors Conference. (2020). *Guidelines and Standards in International University Cooperation*. https://www.hrk.de/fileadmin/redaktion/hrk/02-Dokumente/02-01-Beschluesse/Beschluss_Leitlinien_und_Standards_HRK_Praesidium_6.4.2020_EN.pdf; HRK - German Rectors Conference. (2020). *Guiding Questions on University Cooperation with the People's Republic of China*. https://www.chinazentrum.uni-kiel.de/de/aktuelles/datei-aktuelles/2023/info-china-kooperation/01_handreichungen-leitfaeden/03_HRK_Guiding-question-on-university-cooperation-with-the-PR-China_2020.pdf/

²⁸⁴ I. D'Hooghe., J. Lammertink. (2022). 'How National Governments and Research Institutions Safeguard Knowledge Development in Science and Technology'. *Leiden Asia Centre & AWTI*. <https://leidenasiacentre.nl/wp-content/uploads/2022/11/How-National-Governments-and-Research-Institutions-Safeguard-Knowledge-Development-in-Science-and-Technology.pdf>. P.29.

²⁸⁵ T. Gabel. (2024). 'Germany mulls new research security organisation'. *Science Business*. <https://sciencebusiness.net/news/germany-mulls-new-research-security-organisation>

²⁸⁶ DFG (2023). *Recommendations on dealing with risks in international research cooperation*. <https://www.dfg.de/resource/blob/289704/585cb3b48bb8e9f5b6e57e0e0a0d700e/risiken-int-kooperationen-en-data.pdf>

²⁸⁷ Humboldt Foundation. (n.d.). *Security-relevant research in international relations, collaborations. Context and stance of the Humboldt Foundation*. <https://www.humboldt-foundation.de/en/explore/about-the-humboldt-foundation/security-relevant-research>

²⁸⁸ Max Planck Gesellschaft. (2024). *International Collaboration – Background and Guidelines for the Development of International Collaborations of the Max-Planck-Gesellschaft*. <https://www.mpg.de/16767044/mpg-leitlinien-int-kooperationen-2024.pdf>

-
- ²⁸⁹ Fraunhofer-Gesellschaft (2019), *Fraunhofer Principles of Cooperation*, <https://archives.greenairnews.com/www.fraunhofer.de/en/about-fraunhofer/corporate-responsibility/governance/declaration-project-cooperation.html>
- ²⁹⁰ Fraunhofer-Gesellschaft, *Fraunhofer Ethics Committee for Security-Relevant Research (REC)*, <https://archives.greenairnews.com/www.fraunhofer.de/en/about-fraunhofer/corporate-responsibility/research-and-development/ethics-committee-for-security-relevant-research.html>
- ²⁹¹ Humboldt Foundation. (n.d.). *Security-relevant research in international relations, collaborations. Context and stance of the Humboldt Foundation*. <https://www.humboldt-foundation.de/en/explore/about-the-humboldt-foundation/security-relevant-research>
- ²⁹² BAFA. (2023). *Manual Export Control and Academia*. https://www.bafa.de/SharedDocs/Downloads/EN/Foreign_Trade/ec_manual_export_control_and_academia.html?nn=1444524
- ²⁹³ BAFA. (2019). *Export Control in Science and Research*. https://www.bafa.de/SharedDocs/Downloads/EN/Foreign_Trade/ec_awareness_academia.htm
- ²⁹⁴ See: BMWK (2021), *Investment Screening*, <https://www.bmwk.de/Redaktion/EN/Artikel/Foreign-Trade/investment-screening.html> and M. J. Werner and S. Holinde (2024), 'Germany: Global rules on foreign direct investment', *Norton Rose Fulbright*, <https://www.nortonrosefulbright.com/en/knowledge/publications/f5b8d5d0/germany>
- ²⁹⁵ T. Gabel. (2024). 'Germany mulls new research security organisation'. *Science Business*. <https://sciencebusiness.net/news/germany-mulls-new-research-security-organisation>
- ²⁹⁶ Ministry of University and Research. (2024, 6/12/2024). Press Release: Research: MUR, we are working on an Italian model for security
- ²⁹⁷ Decode39 (2024). *How Italy plans to tackle foreign interference in research*. <https://decode39.com/9677/how-italy-plans-to-tackle-foreign-interference-in-research/>
- ²⁹⁸ Ministry of University and Research. (2025). *Universities*, <https://dati-ustat.mur.gov.it/dataset/bed0c71e-9f86-4a0f-a266-963b6f7bbbd2/resource/820aefe6-0662-4656-84ec-d8859a2a3b7e/download/atenei.csv>
- ²⁹⁹ STATISTA. (2025). *Academic and Research Staff in Italy*. <https://www.statista.com/statistics/1088533/number-of-university-teachers-by-rank-and-gender-in-italy/>
- ³⁰⁰ CNR. (2025). *CNR in Figures*. <https://www.cnr.it/en/cnr-in-figures>
- ³⁰¹ Council of the European Union. (2024). *Council Recommendation on Enhancing Research Security, 2024/0012(NLE)*, https://research-and-innovation.ec.europa.eu/document/download/e82a2fd9-ac12-488a-a948-87639eef10d4_en
- ³⁰² Italian Institute of Technology. (2024). *Strategic Plan - 2024-2029*. <https://multimedia.iit.it/asset-bank/assetfile/22393.pdf>
- ³⁰³ QS (2020), 'Italian Universities and Internationalisation', <https://www.qschina.cn/en/where-to-study/europe/italy/italian-universities-internationalization>
- ³⁰⁴ OECD (2024), *Education at a Glance 2024: OECD Indicators*, OECD Publishing, Paris, <https://doi.org/10.1787/c00cad36-en>.
- ³⁰⁵ European Tertiary Education Register, 2019, *Internationalisation of Academic Staff in European Higher Education*, https://eter-project.com/uploads/analytical-reports/ETER_AnalyticalReport_01_final.pdf
- ³⁰⁶ Kwiek M. (2021), 'What large-scale publication and citation data tell us about international research collaboration in Europe: changing national patterns in global contexts', *Studies in Higher Education*. 46(12): 2629-2649. <https://doi.org/10.1080/03075079.2020.1749254>
- ³⁰⁷ National Science Board (2023), *Science and Engineering Indicators: Publications Output: U.S. Trends and International Comparisons. Supplementary Table SPBS-33* <https://nces.nsf.gov/pubs/nsb202333/table/SPBS-33>
- ³⁰⁸ European Research Area (n.d). *ERA Performance Indicators*, https://european-research-area.ec.europa.eu/scoreboard-reports?countries%5B0%5D=42&countries%5B1%5D=46&countries%5B2%5D=25&countries%5B3%5D=50&countries%5B4%5D=55&countries%5B5%5D=60&countries%5B6%5D=61&edit-countries-42=on&edit-countries-46=on&edit-countries-25=on&edit-countries-50=on&edit-countries-55=on&edit-countries-60=on&edit-countries-61=on&field_related_sb_indicator_target_id=123
-

-
- ³⁰⁹ Decode39. (2024). 'How Italy plans to tackle foreign interference in research', <https://decode39.com/9677/how-italy-plans-to-tackle-foreign-interference-in-research/>
- ³¹⁰ Decode39. (2024). 'How Italy plans to tackle foreign interference in research', <https://decode39.com/9677/how-italy-plans-to-tackle-foreign-interference-in-research/>
- ³¹¹ Casarini, N. (2021). 'Silk Road Academic Connections: China–Italy Cooperation in Higher Education and Its Implications for the West', *The Istituto Affari Internazionali (IAI)*. <https://www.iai.it/sites/default/files/iaip2144.pdf>
- ³¹² European Think-tank Network on China (ETNC). (2024) 'National Perspectives on Europe's De-risking from China', *Clingendael*, https://www.clingendael.org/sites/default/files/2024-7/ETNC2024_National_Perspectives_on_Europes_De-risking_from_China.pdf
- ³¹³ Interview IT UL-1.
- ³¹⁴ F. Turone. (2024). 'Italian research sector recognises security concerns.' *Research Professional News*. <https://www.researchprofessionalnews.com/rr-news-europe-italy-2024-11-italian-research-sector-recognises-security-concerns/>
- ³¹⁵ Interview IT RSO-1.
- ³¹⁶ Interview IT UL-1.
- ³¹⁷ Editorial Staff. (2025). Research Safety Guidelines Coming Soon. *Il Sole 24 Ore*.
- ³¹⁸ Ministry of University and Research. (2024, 6/12/2024). Press Release: Research: MUR, we are working on an Italian model for security
- ³¹⁹ European Research Managers Association. (2025). *Promoting European cooperation in developing responses to research security challenges: Online Event [in 2024]*. <https://earma.org/news/promoting-european-cooperation-developing-responses-research-security-challenges-online-event/>
- ³²⁰ Interview IT UL-1.
- ³²¹ Interview IT UA-1.
- ³²² European Commission. (2023). C(2023) 6689, *Commission Recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States*. https://defence-industry-space.ec.europa.eu/document/download/31c246f2-f0ab-4cdf-a338-b00dc16abd36_en?filename=C_2023_6689_1_EN_ACT_part1_v8.pdf
- ³²³ Interview IT UA-1.
- ³²⁴ Interview IT UA-1.
- ³²⁵ Interview IT UL-1.
- ³²⁶ Interview IT UL-1.
- ³²⁷ Interview IT UA-1.
- ³²⁸ Interview IT UL-1.
- ³²⁹ Interview IT UL-1.
- ³³⁰ University of Bologna (2025). 'Visiting scholars for research and other researchers from abroad', <https://www.unibo.it/en/university/international-outreach/international-staff-professors-and-researchers/visiting-scholars-for-research-and-other-researchers-from-abroad>
- ³³¹ Italian Visa (2025). 'Research Visa', <https://www.italianvisa.it/research-visa/>.
- ³³² Interview IT UL-1.
- ³³³ There are a range of other universities of applied science where research is much less intensive and aligned primarily towards supporting their teaching specialisms
- ³³⁴ NWO (n.d.), *Knowledge Coalition*, <https://www.nwo.nl/en/knowledge-coalition>
- ³³⁵ Rathenau Instituut (2024), 'The share of foreign scientific personnel', <https://www.rathenau.nl/en/science-figures/personnel/international-researchers/share-foreign-scientific-personnel>
- ³³⁶ Rathenau Instituut (2024), 'The share of foreign scientific personnel', <https://www.rathenau.nl/en/science-figures/personnel/international-researchers/share-foreign-scientific-personnel>
- ³³⁷ NUFFIC, (2023), *Fact Sheet on International Students*, <https://www.nuffic.nl/sites/default/files/2023-08/2023%20NUF%20factsheet%20international%20students%20EN%20mei%202023.pdf>
- ³³⁸ Rathenau Instituut (2025), 'From PhD student to PhD Student', <https://www.rathenau.nl/nl/wetenschap-cijfers/wetenschappers/van-promovendus-tot-promotie>
-

-
- ³³⁹ Kwiek M. (2021), 'What large-scale publication and citation data tell us about international research collaboration in Europe: changing national patterns in global contexts', *Studies in Higher Education*. 46(12) :2629-2649. <https://doi.org/10.1080/03075079.2020.1749254>
- ³⁴⁰ National Science Board (2023), *Science and Engineering Indicators: Publications Output: U.S. Trends and International Comparisons. Supplementary Table SPBS-33* <https://nces.nsf.gov/pubs/nsb202333/table/SPBS-33>
- ³⁴¹ Rathenau Instituut (2024). 'China: A scientific superpower in the making' <https://www.rathenau.nl/en/science-figures/process/collaboration/china-scientific-superpower-making>
- ³⁴² Universiteiten van Nederland (2022), *National Knowledge Security Guidelines: Secure International Relations*, <https://open.overheid.nl/documenten/ronl-5379d1b4f8b9784bf518251032507a965be9c92d/pdf>
- ³⁴³ Feedback: Boosting Research Security in the EU. (2024). https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14056-Boosting-research-security-in-the-EU-guidance_en
- ³⁴⁴ KNAW. (2023). *Knowledge Security: Academy Position Paper*. <https://storage.knaw.nl/2023-10/Knowledge-security-Academy-Position-Paper-October-2023.pdf>
- ³⁴⁵ The only specific mention of threat actors is in reference to official sanctions placed on countries such as North Korea and Iran
- ³⁴⁶ D'Hooghe, I., Lammertink, J. (2020) 'Towards Sustainable Europe-China Collaboration in Higher Education and Research', *Leiden Asia Centre*. <https://leidenasiacentre.nl/wp-content/uploads/2020/10/Towards-Sustainable-Europe-China-Collaboration-in-Higher-Education-and-Research.pdf> ; Bekkers, F., Oosterveld, W., Verhagen, P. (2019). 'Checklist for collaboration with Chinese universities and other research institutions'. *Hague Centre for Strategic Studies*. <https://hcss.nl/wp-content/uploads/2021/01/BZ127566-HCSS-Checklist-for-collaboration-with-Chinese-Universities.pdf>
- ³⁴⁷ I. D'Hooghe., X. Martin. (2024). 'Dutch collaboration with PhD students sponsored by the China Scholarship Council', *Clingendael and CKN*. https://www.clingendael.org/sites/default/files/2024-03/Report_Dutch_Collaboration_with_CSC_PhD_students_final.pdf
- ³⁴⁸ K. Soeteman. (2023) 'Minister delays introduction of 'knowledge safety test'', *Research Professional News*. <https://www.researchprofessionalnews.com/rr-news-europe-netherlands-2023-1-minister-delays-introduction-of-knowledge-safety-test/>
- ³⁴⁹ K. Soeteman. (2023). 'Dutch universities ramp up response to espionage threats', *Research Professional News*. <https://www.researchprofessionalnews.com/rr-news-europe-netherlands-2023-10-dutch-universities-ramp-up-response-to-espionage-threats/>
- ³⁵⁰ D'Hooghe, I., Lammertink, J. (2020) 'Towards Sustainable Europe-China Collaboration in Higher Education and Research', *Leiden Asia Centre*. <https://leidenasiacentre.nl/wp-content/uploads/2020/10/Towards-Sustainable-Europe-China-Collaboration-in-Higher-Education-and-Research.pdf>
- ³⁵¹ Ministry of Foreign Affairs (2019), 'The Netherlands and China: A New Balance', <https://www.government.nl/documents/policy-notes/2019/05/15/china-strategy-the-netherlands--china-a-new-balance>
- ³⁵² G. Diercks, J. Deuten, P. Diederens, . (2019) Kennis in het vizier (Knowledge in the Sights) <https://www.rathenau.nl/nl/werking-van-het-wetenschapssysteem/kennis-het-vizier> (Dutch language version)
- ³⁵³ F. Bekkers, W. Oosterveld, P. Verhagen, P. (2019). 'Checklist for collaboration with Chinese universities and other research institutions'. *Hague Centre for Strategic Studies*. <https://hcss.nl/wp-content/uploads/2021/01/BZ127566-HCSS-Checklist-for-collaboration-with-Chinese-Universities.pdf>
- ³⁵⁴ I. van Engelshoven, F. Grapperhaus, M. Keijzer (2020), 'Knowledge Security in Higher Education and Research', [Letter to Parliament] <https://www.government.nl/documents/letters/2020/11/27/knowledge-security-in-higher-education-and-research>
- ³⁵⁵ Universiteiten van Nederland (2022), *National Knowledge Security Guidelines: Secure International Relations*, <https://open.overheid.nl/documenten/ronl-5379d1b4f8b9784bf518251032507a965be9c92d/pdf>
- ³⁵⁶ Government of the Netherlands, Contact Point for Knowledge Security, <https://english.loketkennisveiligheid.nl/>

-
- ³⁵⁷ B. Upton. (2023). 'Dutch research security hotline sees 'big increase' in queries', *Times Higher Education*. <https://www.timeshighereducation.com/news/dutch-research-security-hotline-sees-big-increase-queries>
- ³⁵⁸ Interviews NL UA-1, UA-2, UA-3
- ³⁵⁹ Interviews NL UA-1, UA-2, UA-3
- ³⁶⁰ CESAER (2023). *Workshop on Research Security: Multilateral Dialogue on Principles and Values in International Research and Innovation Cooperation*. <https://www.cesaer.org/content/3-task-forces/2022-2023/task-force-openness-science-technology/20231207-research-security-event.pdf>, p.11.
- ³⁶¹ K. Soeteman. (2023) 'Minister delays introduction of 'knowledge safety test'', *Research Professional News*. <https://www.researchprofessionalnews.com/rr-news-europe-netherlands-2023-1-minister-delays-introduction-of-knowledge-safety-test/>
- ³⁶² NWO (n.d.) Knowledge Coalition, <https://www.nwo.nl/en/knowledge-coalition>
- ³⁶³ Rathenau Institute Website: <https://www.rathenau.nl/en>
- ³⁶⁴ Rathenau Instituut (2024), 'China: A scientific superpower in the making', <https://www.rathenau.nl/en/science-figures/process/collaboration/china-scientific-superpower-making>
- ³⁶⁵ Universiteiten van Nederland (2022), *National Knowledge Security Guidelines: Secure International Relations*, <https://open.overheid.nl/documenten/ronl-5379d1b4f8b9784bf518251032507a965be9c92d/pdf>
- ³⁶⁶ CESAER (2023). *Workshop on Research Security: Multilateral Dialogue on Principles and Values in International Research and Innovation Cooperation*. <https://www.cesaer.org/content/3-task-forces/2022-2023/task-force-openness-science-technology/20231207-research-security-event.pdf>
- ³⁶⁷ K. Soeteman. (2023). 'Dutch universities ramp up response to espionage threats', *Research Professional News*. <https://www.researchprofessionalnews.com/rr-news-europe-netherlands-2023-10-dutch-universities-ramp-up-response-to-espionage-threats/>
- ³⁶⁸ Government of the Netherlands, Contact Point for Knowledge Security. <https://english.loketkennisveiligheid.nl/>
- ³⁶⁹ NL PM-1, PM-2
- ³⁷⁰ Oberon-Dialogic (2023), *Sector view on knowledge security universities 2023*, <https://www.rijksoverheid.nl/documenten/rapporten/2023/09/11/bijlage-1-oberon-dialogic-sectorbeeld-kennisveiligheid-universiteiten-2023> (Dutch language version)
- ³⁷¹ R. Puylaert, (n.d). 'Knowledge Security', *Universities of the Netherlands* <https://www.universiteitenvannederland.nl/onderwerpen/onderzoek/kennisveiligheid> (Dutch language version)
- ³⁷² AWTI (2022), 'Knowledge in Conflict - Safety and Freedom in Balance', <https://www.awti.nl/documenten/adviezen/2022/11/29/index> (Dutch language version)
- ³⁷³ Universities of the Netherlands (2024), *Capability Maturity Model: Knowledge Security*, <https://www.universiteitenvannederland.nl/files/publications/UNL%20Capability%20Maturity%20Model%20Knowledge%20Security%20ENG-DEF.pdf>
- ³⁷⁴ AWTI (2022), 'Knowledge in Conflict - Safety and Freedom in Balance', <https://www.awti.nl/documenten/adviezen/2022/11/29/index> (Dutch language version)
- ³⁷⁵ KNAW (2023). 'Royal Netherlands Academy of Arts and Sciences (KNAW) warns against proposed Knowledge Security Act', *KNAW [Website]*. <https://www.know.nl/en/news/royal-netherlands-academy-arts-and-sciences-know-warns-against-proposed-knowledge-security-act>
- ³⁷⁶ Interviews NL UA-1, UA-2, UA-3
- ³⁷⁷ H. Onderwijs Persbureau, (2024), 'Screening of foreign students and researchers still years away', *Erasmus Magazine*, <https://www.erasmusmagazine.nl/en/2024/10/31/screening-of-foreign-students-and-researchers-still-years-away/>
- ³⁷⁸ *Progress on the approach to knowledge security in higher education and science* (2024) https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2024D40959&did=2024D40959
- ³⁷⁹ Government of the Netherlands (n.d.) *Legislation, treaties and international agreements on the export of strategic goods*, <https://www.government.nl/topics/export-controls-of-strategic-goods/laws-and-rules-on-the-export-of-strategic-goods>
-

-
- ³⁸⁰ Government of the Netherlands (n.d.), *Dutch government policy on international sanctions*, [HYPERLINK "https://www.government.nl/topics/international-sanctions/policy-international-sanctions"](https://www.government.nl/topics/international-sanctions/policy-international-sanctions)<https://www.government.nl/topics/international-sanctions/policy-international-sanctions>
- ³⁸¹ Government of the Netherlands (n.d.), *For which technical studies do I need an exemption from the knowledge embargo and how do I apply for one?* <https://www.rijksoverheid.nl/onderwerpen/hoger-onderwijs/vraag-en-antwoord/waarom-heb-ik-een-ontheffing-nodig-voor-bepaalde-technische-nucleaire-studies>
- ³⁸² Interviews NL UA-1, UA-2, UA-3
- ³⁸³ K. Soeteman. (2023). 'Dutch universities ramp up response to espionage threats', *Research Professional News*. <https://www.researchprofessionalnews.com/rr-news-europe-netherlands-2023-10-dutch-universities-ramp-up-response-to-espionage-threats/>
- ³⁸⁴ Tweede Kamer (2024), *Progress on the approach to knowledge security in higher education and science*, https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2024D40959&did=2024D40959
- ³⁸⁵ It's worth noting that in its response to the European Commission's consultation on research security, the ministry (OCW) supported the creation of a European monitoring facility to help Member States assess knowledge security risks.
- ³⁸⁶ STATISTA. (2025). *Universities in Spain in 2022/2023, by region*. <https://www.statista.com/statistics/445160/number-of-universities-in-spain-by-region/>
- ³⁸⁷ CSIC. (2025). *Institutes, centres & units*. <https://www.csic.es/en/csic/organisation/institutes-centres-units>
- ³⁸⁸ Council of the European Union. (2024). Council Recommendation on Enhancing Research Security, 2024/0012(NLE), https://research-and-innovation.ec.europa.eu/document/download/e82a2fd9-ac12-488a-a948-87639eef10d4_en
- ³⁸⁹ SOMM Excellence Alliance. (2024). *Centres and Units*. <https://somma.es/about/centres-and-units/>
- ³⁹⁰ <https://www.wissenschaft-welt offen.de/en/in-focus-selected-findings-of-the-publication/international-academics-and-researchers-at-public-universities-and-research-institutes-in-major-host-countries/>
- ³⁹¹ <https://www.universityworldnews.com/post.php?story=20231218084718960>
- ³⁹² <https://www.universityworldnews.com/post.php?story=20231218084718960>
- ³⁹³ <https://www.universityworldnews.com/post.php?story=20231218084718960>
- ³⁹⁴ <https://www.studying-in-spain.com/spain-international-student-statistics/>
- ³⁹⁵ Kwiek M. (2021), 'What large-scale publication and citation data tell us about international research collaboration in Europe: changing national patterns in global contexts', *Studies in Higher Education*. 46(12) :2629-2649. <https://doi.org/10.1080/03075079.2020.1749254>
- ³⁹⁶ Aksnes, D. W., & Sivertsen, G. (2023). Global trends in international research collaboration, 1980-2021. *Journal of Data and Information Science*, 8(2), 26-42. <https://doi.org/10.2478/jdis-2023-0015>
- ³⁹⁷ National Science Board (2023), *Science and Engineering Indicators: Publications Output: U.S. Trends and International Comparisons. Supplementary Table SPBS-33*, <https://nces.nsf.gov/pubs/nsb202333/table/SPBS-33>
- ³⁹⁸ European Research Area Platform, (n.d.), 'ERA Performance Indicators', https://european-research-area.ec.europa.eu/scoreboard-reports?countries%5B0%5D=42&countries%5B1%5D=46&countries%5B2%5D=25&countries%5B3%5D=50&countries%5B4%5D=55&countries%5B5%5D=60&countries%5B6%5D=61&edit-countries-42=on&edit-countries-46=on&edit-countries-25=on&edit-countries-50=on&edit-countries-55=on&edit-countries-60=on&edit-countries-61=on&field_related_sb_indicator_target_id=123
- ³⁹⁹ Kwiek M. (2021), 'What large-scale publication and citation data tell us about international research collaboration in Europe: changing national patterns in global contexts', *Studies in Higher Education*. 46(12) :2629-2649. <https://doi.org/10.1080/03075079.2020.1749254>
- ⁴⁰⁰ Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast), (2021).

-
- ⁴⁰¹ Council of the European Union. (2024). *Council Recommendation on Enhancing Research Security*, https://www.safeguarding-science.eu/wp-content/uploads/Council-Recommendations_research-security.pdf
- ⁴⁰² Interview ES RPO-1, ES-PM1 and PM-3.
- ⁴⁰³ ENS. (n.d.) *What is the National Security Framework (ENS)?* <https://ens.ccn.cni.es/en/what-is-the-ens>
- ⁴⁰⁴ Norton Rose Fulbright (2025). 'Spain: Global Rules on Foreign Direct Investment.' <https://www.nortonrosefulbright.com/en/knowledge/publications/65c365bc/spain> .
- ⁴⁰⁵ Interview ES UL-2.
- ⁴⁰⁶ Navajas-Adán, J., Badia-Gelabert, E., Jiménez-Saurina, L., Marijuán-Martín, M. J., & Mayo-García, R. (2024). Perceptions and dilemmas around cyber-security in a Spanish research center after a cyber-attack. *International Journal of Information Security*, 23(3), 2315-2331. <https://doi.org/10.1007/s10207-024-00847-7>
- ⁴⁰⁷ Government of Spain. (2025). *National Security Council*. <https://www.dsn.gob.es/es>
- ⁴⁰⁸ KonBriefing Research (2025). 'Cyber-attacks on universities University ransomware attacks & data breaches worldwide', <https://konbriefing.com/en-topics/cyber-attacks-universities.html>
- ⁴⁰⁹ Interview ES RPO-1.
- ⁴¹⁰ Interview ES UL-1.
- ⁴¹¹ Interview ES UL-2.
- ⁴¹² Interview ES RPO-1.
- ⁴¹³ Interview ES UL-2.
- ⁴¹⁴ Interview ES RPO-1, PM-1, PM-2, PM-3.
- ⁴¹⁵ Interview ES RPO-1, RPO-2, PM-1, PM-2, PM-3.
- ⁴¹⁶ Interview ES UL-2 but the existence of this view was also noted by ES RPO-2.
- ⁴¹⁷ Also noted by ES PM-3.
- ⁴¹⁸ Interview ES RPO-2, ES PM-2, PM-3.
- ⁴¹⁹ Faber, S. (2022). 'Blocking Access to the Recent Past: Threats to Academic Freedom in Post-dictatorial Spain', *Copyright American Association of University Professors*, 13. https://www.aaup.org/sites/default/files/Faber_JAF13.pdf
- ⁴²⁰ The government assignment (also referred to as "the government mandate") was issued to the three organisations in June 2023. They produced two reports that are being considered by the the Ministry of Education and Research.
- ⁴²¹ UHR (2024) *Responsible Internationalization. Partial Report of a Government Assignment* (Ansvarsfull internationalisering. Delrapportering av ett regeringsuppdrag, UHR:s rapportserie 2024:1) https://www.uhr.se/globalassets/_uhr.se/publikationer/2024/ansvarsfull-internationalisering_uhr-2024_1.pdf and UHR (2025) *National Support Structure for Responsible Internationalisation*, https://www.uhr.se/globalassets/_uhr.se/english/about-the-council/national-support-function-for-responsible-internationalisation---final-report-2025.pdf
- ⁴²² STINT (Stiftelsen för internationalisering av högre utbildning och forskning or The Swedish Foundation for International Cooperation in Research and Higher Education) was set up by the Swedish Government in 1994 to enhance the international competitiveness of Swedish higher education institutions by being a national knowledge resource on internationalisation. <https://www.stint.se/en/>
- ⁴²³ It should also be noted that, in May 2023, Sweden introduced the first ministerial discussion on responsible internationalisation during its EU Presidency.
- ⁴²⁴ Data from the OECD Data Explorer: enrolment of mobile students in tertiary education and total enrolments in tertiary education in 2022.
- ⁴²⁵ Wissenschaft Weltoffen, (n.d.) 'International academics and researchers at public universities and research institutes in major host countries', <https://www.wissenschaft-weltoffen.de/en/in-focus-selected-findings-of-the-publication/international-academics-and-researchers-at-public-universities-and-research-institutes-in-major-host-countries/>
- ⁴²⁶ Data from the OECD Data Explorer: R&D personnel by sector of performance and function, 2021.
- ⁴²⁷ Kwiek M. (2021), 'What large-scale publication and citation data tell us about international research collaboration in Europe: changing national patterns in global contexts', *Studies in Higher Education*. 46(12) :2629-2649. <https://doi.org/10.1080/03075079.2020.1749254>
-

-
- ⁴²⁸ National Science Board (2023), *Science and Engineering Indicators: Publications Output: U.S. Trends and International Comparisons. Supplementary Table SPBS-33*
<https://nces.nsf.gov/pubs/nsb202333/table/SPBS-33>
- ⁴²⁹ T. Shih., M. Garvi., S. Östlund (2022). 'Recommendations to higher education institutions on how to work with responsible internationalisation.' *The Swedish Foundation for International Cooperation in Research and Higher Education* (STINT). https://www.stint.se/wp-content/uploads/2022/09/STINT_Ansvarsfull-internation_web.pdf p.4
- ⁴³⁰ UHR (2024), *National Support Structure for Responsible Internationalisation*,
https://www.uhr.se/globalassets/_uhr.se/english/about-the-council/national-support-function-for-responsible-internationalisation---final-report-2025.pdf
- ⁴³¹ STINT (2020). *Responsible Internationalisation: Guidelines for reflection on international academic collaboration*. https://www.stint.se/wp-content/uploads/2020/02/STINT_Responsible_Internationalisation.pdf and T. Shih., M. Garvi., S. Östlund. (2022). 'Recommendations to higher education institutions on how to work with responsible internationalisation.' *The Swedish Foundation for International Cooperation in Research and Higher Education* (STINT). https://www.stint.se/wp-content/uploads/2022/09/STINT_Ansvarsfull-internation_web.pdf
- ⁴³² Interviews: SWE UA4 and others
- ⁴³³ Interviews: SWE FA2; SWE FA4
- ⁴³⁴ Interviews: SWE UA1; SWE UA3-7; SW UO1; SWE FA4
- ⁴³⁵ Maria Nilsson, State Secretary for the Ministry of Education, speaking at the Nordic Council of Ministers Conference on Nordic Approaches to Responsible Internationalisation, Stockholm, December 2024.
- ⁴³⁶ Nordic Council of Ministers Conference on Nordic Approaches to Responsible Internationalisation, Stockholm, December 2024.
- ⁴³⁷ Säkerhetspolisens årsbok 2023-2024 (sakerhetspolisen.se) (Security Service Yearbook 2023-2024) <https://sakerhetspolisen.se/download/18.5cb30b118d1e95affec37/1708502268494/L%C3%A4gesbild%202023-2024.pdf>; Interviews: SWE FA2; SWE FA4
- ⁴³⁸ Interviews: SWE PM1-3; SWE UA1; SWE UA3-7
- ⁴³⁹ SWE UA8-9; SWE UA1: there was also scandal during 2023. The media examined KTH and several other universities and highlighted their cooperations with China, including through the China Scholarship Council.
- ⁴⁴⁰ Interviews: SWE UA1; SWE FA2; Säkerhetspolisens årsbok 2023-2024 (sakerhetspolisen.se) (Security Service Yearbook 2023-2024) <https://sakerhetspolisen.se/download/18.5cb30b118d1e95affec37/1708502268494/L%C3%A4gesbild%202023-2024.pdf>
- ⁴⁴¹ Interview: SWE FA3
- ⁴⁴² Interview: SWE UA1
- ⁴⁴³ J. Petter Myklebust, (2022), 'Research security rules: Is university autonomy at risk?'. *University World News*, <https://www.universityworldnews.com/post.php?story=20220531144822860>
- ⁴⁴⁴ Security Service Yearbook Säkerhetspolisens årsbok 2023-2024 (sakerhetspolisen.se)
- ⁴⁴⁵ Nordic Council of Ministers conference on responsible internationalisation
- ⁴⁴⁶ Security Service Yearbook Säkerhetspolisens årsbok 2023-2024 (sakerhetspolisen.se)
- ⁴⁴⁷ STINT (2020). *Responsible Internationalisation: Guidelines for reflection on international academic collaboration*. https://www.stint.se/wp-content/uploads/2020/02/STINT_Responsible_Internationalisation.pdf T. Shih., M. Garvi., S. Östlund. (2022). 'Recommendations to higher education institutions on how to work with responsible internationalisation.' *The Swedish Foundation for International Cooperation in Research and Higher Education* (STINT). https://www.stint.se/wp-content/uploads/2022/09/STINT_Ansvarsfull-internation_web.pdf
- ⁴⁴⁸ Interview: SWE FA4; SWE PM1
- ⁴⁴⁹ Interviews: SWE UO1; SWE FA4; SWE IE1

⁴⁵⁰ J. Petter Myklebust, (2022), 'Research security rules: Is university autonomy at risk?'. *University World News*, <https://www.universityworldnews.com/post.php?story=20220531144822860> and interview: EU UO6

⁴⁵¹ SUHF (2024) Guidelines regarding higher education institutions' responsibility for ethics in research abroad. <https://suhf.se/app/uploads/2024/10/REC-2024-2-Guidelines-regarding-higher-education-institutions-responsibility-for-ethics-in-research-abroad.-Adopted-by-SUHF-board-on-27-August-2024.pdf>

⁴⁵² Interview: SWE IE1

⁴⁵³ E. Mo Welin. (2024). 'Research security as part of the EU's economic security strategy'. *Swedish National China Centre*. <https://kinacentrum.se/en/publications/research-security-as-part-of-the-eus-economic-security-strategy/>

⁴⁵⁴ UHR (2024) *Responsible Internationalization. Partial Report of a Government Assignment* (Ansvarsfull internationalisering. Delrapportering av ett regeringsuppdrag, UHR:s rapportserie 2024:1) https://www.uhr.se/globalassets/_uhr.se/publikationer/2024/ansvarsfull-internationalisering_uhr-2024_1.pdf

⁴⁵⁵ UHR (2025), *National Support Structure for Responsible Internationalisation*, https://www.uhr.se/globalassets/_uhr.se/english/about-the-council/national-support-function-for-responsible-internationalisation---final-report-2025.pdf

⁴⁵⁶ Interviews: SWE PM1; SWE UO1; SWE FA1; SWE FA3; SWE FA4; SWE IE1; SWE IE2

⁴⁵⁷ L. Hellerstedt. (2023). 'Espionage against Swedish Higher Education institutions continues to increase'. *Universitets Lararen* [Online]. <https://universitetslararen.se/2023/03/30/espionage-against-swedish-higher-education-institutions-continues-to-increase/>

⁴⁵⁸ Interview: SWE PM1; SWE OU1

⁴⁵⁹ Interview: SWE PM1; SWE UA1; SWE FA4

⁴⁶⁰ UHR (2025), *National Support Structure for Responsible Internationalisation*, https://www.uhr.se/globalassets/_uhr.se/english/about-the-council/national-support-function-for-responsible-internationalisation---final-report-2025.pdf

⁴⁶¹ European Commission, 'Open Science', European Research Executive Agency: https://rea.ec.europa.eu/open-science_en

⁴⁶² UHR (2025), *National Support Structure for Responsible Internationalisation*, https://www.uhr.se/globalassets/_uhr.se/english/about-the-council/national-support-function-for-responsible-internationalisation---final-report-2025.pdf

⁴⁶³ Interviews: SWE UO1; SWE FA3; SWE FA4

⁴⁶⁴ Interviews: SWE FA2; SWE UA3-7; SWE UA8

⁴⁶⁵ Interviews: SWE UA1; SWE FA2; comments by delegates at the Nordic Council conference, Stockholm, December 2024

⁴⁶⁶ Interviews: SWE UA3-7; SWE UA8-9;

⁴⁶⁷ SWE PM1; SWE IE1; SWE UO1; SWE UA3-7; SWE UA8

⁴⁶⁸ Interviews: SWE OU1; SWE FA2; SWE FA4; SWE UA3-7; SWE UA9

⁴⁶⁹ SWE UO1; SWE IE2; SWE UA1

⁴⁷⁰ Interview: SWE FA4

⁴⁷¹ Interview: SWE UA1

⁴⁷² Interviews: SWE UO1; SWE UA8-9; SWE IE1

⁴⁷³ UHR (2025), *National Support Structure for Responsible Internationalisation*, https://www.uhr.se/globalassets/_uhr.se/english/about-the-council/national-support-function-for-responsible-internationalisation---final-report-2025.pdf

⁴⁷⁴ Interviews: SWE UA1; SWE UA8-9; SWE IE2; SWE FA2

⁴⁷⁵ Interviews: SWE UA3-7

⁴⁷⁶ Interviews: SWE UA1; SWE UA8-9; SWE IE1

⁴⁷⁷ T. Shih., M. Garvi., S. Östlund. (2022). 'Recommendations to higher education institutions on how to work with responsible internationalisation.' *The Swedish Foundation for International Cooperation in Research and Higher Education (STINT)*. https://www.stint.se/wp-content/uploads/2022/09/STINT_Ansvarsfull-international_web.pdf

-
- ⁴⁷⁸ UHR (2024) *Responsible Internationalization. Partial Report of a Government Assignment* (Ansvarsfull internationalisering. Delrapportering av ett regeringsuppdrag, UHR:s rapportserie 2024:1) https://www.uhr.se/globalassets/_uhr.se/publikationer/2024/ansvarsfull-internationalisering_uhr-2024_1.pdf
- ⁴⁷⁹ UHR (2024) *Responsible Internationalization. Partial Report of a Government Assignment* (Ansvarsfull internationalisering. Delrapportering av ett regeringsuppdrag, UHR:s rapportserie 2024:1) https://www.uhr.se/globalassets/_uhr.se/publikationer/2024/ansvarsfull-internationalisering_uhr-2024_1.pdf
- ⁴⁸⁰ Interview: SWE IE1; SWE IE2
- ⁴⁸¹ J. Petter Myklebust, (2024), 'Universities oppose guidelines on internationalisation', *University World News*, <https://www.universityworldnews.com/post.php?story=20240930174150195>
- ⁴⁸² Interview: SWE PM1-3
- ⁴⁸³ Nordic Council conference on responsible internationalisation
- ⁴⁸⁴ Interview: SWE UA1; SWE UA8-9
- ⁴⁸⁵ UHR (2025), *National Support Structure for Responsible Internationalisation*, https://www.uhr.se/globalassets/_uhr.se/english/about-the-council/national-support-function-for-responsible-internationalisation---final-report-2025.pdf
- ⁴⁸⁶ SWE IE2
- ⁴⁸⁷ Others counter that this view misunderstands the proposals that have been sent to government.
- ⁴⁸⁸ SWE FA4
- ⁴⁸⁹ Interview: SWE UA9
- ⁴⁹⁰ SWE UA3-7
- ⁴⁹¹ Interview SWE FA2
- ⁴⁹² Interview: SWE UA1
- ⁴⁹³ Interview: SWE UA1
- ⁴⁹⁴ Interview: SWE UA3-7
- ⁴⁹⁵ Interview: SWE UA3-7
- ⁴⁹⁶ Interview: SWE UA8-9
- ⁴⁹⁷ Gothenburg University, Karolinska Institutet, Luleå University of Technology, Malmö University and Jönköping University of Stiftelsen.
- ⁴⁹⁸ UHR (2025), *National Support Structure for Responsible Internationalisation*, https://www.uhr.se/globalassets/_uhr.se/english/about-the-council/national-support-function-for-responsible-internationalisation---final-report-2025.pdf
- ⁴⁹⁹ Interview: SWE UA6
- ⁵⁰⁰ For further information see KTH's guidance pages: <https://intra.kth.se/en/campus/sakerhet/sakerhetsskydd/sakerhetsskydd-1.1329363>
- ⁵⁰¹ Interview: SWE PM1-3
- ⁵⁰² Interview: SWE UA8
- ⁵⁰³ Personal correspondence with SWE UA1.
- ⁵⁰⁴ M. Lisaerde. (2023). 'Sweden looks at universities' awareness of security risks'. *Research Professional News. Clarivate*. <https://www.researchprofessionalnews.com/rr-news-europe-nordics-2023-9-sweden-looks-at-universities-awareness-of-security-risks/> ; J. P. Myklebust. (2024). 'Universities oppose guidelines on internationalisation'. *University World News*. <https://www.universityworldnews.com/post.php?story=20240930174150195>
- ⁵⁰⁵ J. Petter Myklebust, (2023), 'Security vs openness: Towards responsible internationalisation' *University World News*, <https://www.universityworldnews.com/post.php?story=20230922130059893>
- ⁵⁰⁶ Discussion at the Nordic Council of Ministers Conference on Nordic Approaches to Responsible Internationalisation, Stockholm, December 2024.
- ⁵⁰⁷ European Council (2024). European Council Recommendation for Enhancing Research Security. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C_202403510
- ⁵⁰⁸ Interviews: EU UO1; EU UO6
- ⁵⁰⁹ Interviews: EU UO1; EU UO3-4

-
- ⁵¹⁰ European Commission. (2020). *Concept Note on Tackling Foreign Interference in Higher Education Institutions and Research Organisations*. <https://s3.eu-central-1.amazonaws.com/euobs-media/3ef6dc3d60ee27a2df16f62d47e93fdc.pdf>
- ⁵¹¹ European Commission. (2021). *Global Approach to Research and Innovation*. COM(2021) 252 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2021%3A252%3AFIN>
- ⁵¹² European Commission. (2021). *Commission Recommendation (EU) 2021/1700 of 15 September 2021 on internal compliance programmes for controls of research involving dual-use items*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021H1700>
- ⁵¹³ European Commission. (2022). *Tackling R&I Foreign Interference: Staff Working Document*. <https://op.europa.eu/en/publication-detail/-/publication/3faf52e8-79a2-11ec-9136-01aa75ed71a1/language-en>
- ⁵¹⁴ EU. (2023). *European Economic Security Strategy*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023JC0020&qid=1687525961309>
- ⁵¹⁵ European Council (2024). *European Council Recommendation for Enhancing Research Security*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C_202403510
- ⁵¹⁶ European Commission. (2024). *Proposal for a Council Recommendation on Enhancing Research Security*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52024DC0026> p.12.
- ⁵¹⁷ Universiteiten van Nederland (2022), *National Knowledge Security Guidelines: Secure International Relations*, <https://open.overheid.nl/documenten/ronl-5379d1b4f8b9784bf518251032507a965be9c92d/pdf> p.9.
- ⁵¹⁸ A. Brinza., U. A. Bêrzina- čerenkova., P. Le Corre., J. Seaman., R. Turcsányu., S. Vladisavljev. (2024). *EU-China relations: De-risking or de-coupling – the future of the EU strategy towards China*. *European Parliament*. [https://www.europarl.europa.eu/RegData/etudes/STUD/2024/754446/EXPO_STU\(2024\)754446_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2024/754446/EXPO_STU(2024)754446_EN.pdf) viii.
- ⁵¹⁹ <https://op.europa.eu/en/publication-detail/-/publication/3faf52e8-79a2-11ec-9136-01aa75ed71a1/language-en>
- ⁵²⁰ <https://eur-lex.europa.eu/eli/reco/2023/2113/oj/eng>
- ⁵²¹ The other technology areas listed included advanced connectivity, navigation and digital technologies, advanced sensing technologies, space and propulsion technologies, energy, robotics and autonomous systems, advanced materials, manufacturing, and recycling technologies.
- ⁵²² Interviews: EU UO6
- ⁵²³ LERU. (2024). 'Improving Research Security in European Universities'. *LERU* [Online]. <https://www.leru.org/news/leru-welcomes-proposals-for-more-secure-research-in-the-future>
- ⁵²⁴ Feedback: Boosting Research Security in the EU. (2024). <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14056-Boosting-research-security-in-the-EU-guidance- en>
- ⁵²⁵ Interviews EU UO3; EU UO4; EU UO6
- ⁵²⁶ Interview: EU UO3

**Manchester Institute of
Innovation Research**



The University of Manchester

ISBN 978-0-946007-40-0



9 780946 007400