POLICY PAPER

From Awareness to Action: Research Security in Czech and European Academia

Dominika Remžová, Ivana Karásková

AMO.CZ

POLICY PAPER

From Awareness to Action: Research Security in Czech and European Academia

Dominika Remžová, Ivana Karásková

FROM AWARENESS TO ACTION: RESEARCH SECURITY IN CZECH AND EUROPEAN ACADEMIA

Policy paper
March 2025

Editor – Ivana Karásková
Authors – Dominika Remžová, Ivana Karásková
Citation – Dominika Remžová and Ivana Karásková, *From Awareness to Action: Research Security in Czech and European Academia* (Prague: Association for International Affairs, 2025).

The publication of this paper was supported by the Foreign, Commonwealth & Development Office (FCDO).

UK Science
& Technology
Network

Acknowledgment – The authors of this publication would like to thank the interviewees for their kind sharing of information and feedback.

Proofreading – Theo Singleton
Typesetting – Zdeňka Plocrová
Print – ON tisk, s.r.o.

ASSOCIATION FOR INTERNATIONAL AFFAIRS (AMO)

Žitná 27/608
CZ 110 00 Praha 1
Tel.: +420 224 813 460
info@amo.cz
www.amo.cz

ISBN 978-80-88470-57-1 (pdf)
ISBN 978-80-88470-56-4 (print)

Table of contents

Executive summary

- As global research collaboration expands, research security has emerged as a crucial aspect of protecting intellectual property, technological advancements, and academic integrity. The European Union has increasingly recognised research security as part of its broader economic and national security strategies. The EU's approach emphasises risk-based assessments, due diligence procedures, and sector-specific policies rather than blanket restrictions.

- Some European countries, notably Germany, the Netherlands, and the United Kingdom, have led efforts to implement research security frameworks, balancing academic freedom with national security considerations. The Czech Republic has also made significant strides in acknowledging and addressing the risks associated with foreign influence in academia. However, the current measures remain largely reactive rather than proactive, with a notable gap between policy adoption and institutional implementation.

- This policy paper examines the evolving research security landscape in the Czech Republic, drawing comparisons with established best practices in other European countries.

- The United Kingdom has developed one of the most advanced research security ecosystems, implementing trusted research guidance and due diligence tools to help universities assess international collaborations. The UK government has actively worked with universities to embed risk management processes while maintaining openness to global partnerships. Several problems, however, persist, especially when it comes to funding research (but also teaching and other functions) at universities, which are extensively reliant on external funding sources, including from China.

- The Netherlands has adopted a knowledge security approach, creating a centralised advisory body (the National Contact Point for Knowledge Security) that provides universities and research institutes with risk assessment advice and strategic guidance. This system allows Dutch academia to mitigate foreign interference risks without overly restricting international collaborations. However, while the Dutch have made significant progress in implementation of knowledge security measures, the recurrence of research security breaches within individual institutions underscores the continued need for awareness raising.

- Germany has taken a sector-specific approach, with leading non-university research institutes such as the Max Planck Society, Fraunhofer Society, Helmholtz, and Leibniz Associations developing their own internal research security frameworks. The German system highlights the importance of industry collaboration and tailored security protocols within high-risk fields such as artificial intelligence, quantum computing, and biotechnology. Yet the lack of a federal approach leads to significant discrepancies between individual institutions (especially universities) and researchers.

- While Czech academic institutions have introduced regulatory frameworks and hired security personnel, the implementation of these measures at the individual researcher level remains inconsistent. In general, this is a problem all countries covered in this paper continue to face.

- Many academics perceive research security policies as a bureaucratic imposition, with concerns that they might stifle international collaboration. Furthermore, institutions tend to view research security as a compliance exercise rather than a comprehensive risk management strategy.

- This policy paper advocates for a whole-system approach to research security, integrating clear guidelines, institutional support, and financial incentives to enhance compliance.

- It also proposes tailored risk assessments, addressing both subject- and issue-specific risks, rather than blanket restrictions on academic collaboration. Drawing from successful models abroad, the recommendations provided aim to ensure that Czech academia remains secure yet globally engaged.

Recommendations

- ➜ While Czech institutions have embraced the discourse of countering foreign influence, research security remains largely declaratory. Academic leadership must embed security measures into daily operations, ensuring that policies are understood and applied at all levels.

- ➜ Institutions must not only comply with research security policies but also internalize their rationale. This requires building trust within the academic community.

- ➜ Given resource constraints, the Czech government should consider establishing a national advisory body, similar to the Dutch Contact Point for Knowledge Security, to provide expert guidance and coordination.

- ➜ The Czech Republic has limited research engagement with China, raising the question of whether a comprehensive risk assessment system is necessary. A case-by-case approach should be adopted to balance security concerns with the benefits of international collaboration.

- ➜ Current research security measures focus on technological risks but often neglect softer forms of interference, such as ideological pressure or self-censorship among scholars; issues that can occur not just within science, technology, engineering, mathematics (STEM) but also humanities and social sciences. Thus, Czech universities must expand their research security strategies to include cultural, political, and financial dimensions of foreign influence, drawing inspiration from German approach.

- ➜ Security assessments should go beyond categorical risk classifications (e.g., banning all China-affiliated researchers) and instead adopt context-specific evaluations.

- ➜ Institutions need specialized training to equip researchers and administrators with the knowledge to differentiate between legitimate collaboration and potential security threats. This should be adapted to the needs of different disciplines, drawing potential inspiration from the approaches of various institutions in the Netherlands, particularly those that have faced research security challenges and learned from them.

- ➜ A successful research security framework relies on bottom-up input from academics. Their experiences and concerns should be systematically incorporated into policy refinements.

- ➜ Universities should establish robust feedback channels to ensure that security policies evolve in response to real-world challenges.

- ➜ By implementing these recommendations, the Czech Republic can shift from a reactive, compliance-based approach to a proactive, integrated system that safeguards its research ecosystem while maintaining openness to global scientific collaboration.

Introduction

As the international system becomes increasingly shaped by geopolitical and mercantilist tendencies, research security has emerged as an integral part of a broader agenda that prioritises national security, technological sovereignty, and economic competitiveness. Indeed, the European Commission's proposal for enhancing research security situates it within the framework of its economic security strategy,[1] reinforcing the ongoing 'security pivot' in policymaking and highlighting the need for states and institutions to strike a balance between openness to international collaborations and safeguarding sensitive research.

Competitiveness, in particular, has become a defining priority for the European Union, especially as it seeks to close the gap with the United States and China in key technological fields. In 2023, the EU has published a list of ten critical technologies to safeguard as part of its economic security strategy, highlighting artificial intelligence (AI), advanced semiconductors, quantum and biotechnologies as the greatest areas of risk.[2] Moreover, European Commission President Ursula von der Leyen has repeatedly emphasised the need for Europe to strengthen its technological and industrial base to maintain its position as a global economic powerhouse. In her 2025 speech on European competitiveness, she stressed that while the EU remains an economic leader, it faces an urgent need to catch up in key technological domains, particularly in AI, quantum computing, and biotechnology.[3] Thus, the EU's competitiveness is not only about economic growth but also about ensuring strategic autonomy, reducing reliance on foreign technologies, and safeguarding innovation from external risks.

Europe has often been a frontrunner in establishing regulatory frameworks but lags in scaling innovation. Compared to the United States and China, where rapid investment and private or state sectors' involvement drive progress, Europe has struggled with fragmented research funding, slow adoption of new technologies, and complex regulatory hurdles. As the world enters a new era of economic competition, the EU recognises that it must accelerate investment in research and innovation while reinforcing its security policies to protect cutting-edge knowledge from being leveraged by geopolitical competitors. Strengthening technological leadership requires not only research funding but also collaborative strategies to ensure that European innovation ecosystems remain resilient in the face of growing international challenges.

Among the EU's strategic technologies, AI stands out as a key driver of innovation and economic growth, particularly due to its role in electric vehicles and autonomous driving – the future of the EU's major industry. Recognising its transformative potential, the EU has developed a comprehensive AI strategy to enhance industrial competitiveness, modernise public services, and safeguard technological sovereignty.[4] A central goal is to reduce reliance on external AI models and hardware, fostering cross-border collaboration among European research institutions.

While AI presents immense opportunities, it also introduces security challenges, including cybersecurity risks, dual-use applications, and intellectual property (IP)

concerns. Given China's substantial investment in AI research – particularly in state surveillance, predictive analytics, and military applications – the EU has emphasised robust governance and risk mitigation to prevent misuse.

The Czech Republic is well positioned within Europe's AI research landscape, with strengths in machine learning, computational linguistics, and cybersecurity. The Ministry of Industry and Trade has prioritised AI as a pillar of digital transformation, supporting research initiatives and public-private partnerships.[5] Czech researchers have played leading roles in European AI projects, reinforcing the country's growing reputation in the field. A notable example is Charles University's coordination of a major European project on open large language models, which underscores Czech academia's role in advancing AI innovation.[6]

As Czech involvement in researching key technologies grows, so does the need for strong research security frameworks. Safeguarding sensitive innovations from foreign exploitation is essential to ensuring that academic openness does not come at the expense of national, economic and technological security.

China has demonstrated a strong interest in AI and other critical technologies, often pursuing partnerships with foreign institutions to access cutting-edge research. It has actively sought to engage with European universities and research centres, sometimes through funding mechanisms that lack transparency or clear end-use agreements.[7] These collaborations, while beneficial in many respects, raise questions about IP protection, data security, and potential technology transfer to the Chinese military-industrial complex.

The broader debate on research collaboration with China remains unresolved within the EU. Some European policymakers advocate for greater restrictions on partnerships in fields where China leads, such as AI or quantum computing, fearing that these collaborations could compromise European security. Others argue for a balanced approach, maintaining research exchanges while implementing stricter security guidelines. Regardless of the direction Europe ultimately takes, the Czech Republic faces the challenge of developing a clear and proactive research security strategy that allows for open scientific collaboration while minimising risks.

And while the technological aspect of research security – as highlighted by the discussion above – remains of utmost importance, research security risks go beyond STEM disciplines. This is evident in the recurrent cases of foreign interference such as censorship and other types of research security breaches in humanities and social sciences, undermining academic integrity and freedoms within western higher education institutions (HEIs). In this way, the risks include potential costs to not just the EU's competitiveness and security, but also its long-held values and norms.

Research design and methods

Definitions of research security vary across countries, institutions and contexts, leading to significant divergencies across European research security frameworks. The United Kingdom uses the term 'trusted research',[8] the Netherlands refers to 'knowledge security', and Germany employs 'safeguarding research'. This policy paper follows both the EU and the Organisation for Economic Co-operation and Development (OECD) in using the term 'research security', ensuring convergence with broader European and international policy discussions.

The paper builds upon the findings of the 2022 AMO report titled *How to do trusted research: China-specific guidelines for European stakeholders*,[9] which provided an important impetus to national-level discussions on (not only China-specific) research security approach in Czech academia. Unlike the previous report, however, this policy paper places a strong emphasis on the perspectives of practitioners, who play a critical role in implementing and utilising research security measures within HEIs. Practitioners are defined as both academic and professional services staff – i.e., researchers, administrators, and management representatives – all of whom contribute to institutional (and some also to sectoral) approaches to research security.

In a similar manner, HEIs are defined as including a diverse array of institutions, including universities, university-affiliated or non-university research institutes, funding bodies and other sectoral bodies that bring together different HEI practitioners. In the case of Germany, for example, where non-university research institutes play a particularly significant role in research output and funding, the report includes an assessment of institutions such as the Max Planck Society, Fraunhofer Society, Helmholtz Association, and Leibniz Association.

The selection of country cases also differs from the 2022 report, with this paper focusing on the Czech Republic, Germany, the Netherlands, and the UK. The countries were selected based on their representativeness of broader European regions, which enhances the theoretical transferability of the report's findings, making them relevant not only to the Czech Republic but also to other European countries seeking to strengthen their research security policies – though the focus on the Czech Republic remains.

The past three years have seen a growing recognition of research security concerns among Czech policymakers, universities, and funding bodies alike. Further refinement is, thus, needed to ensure that research security measures do not unnecessarily hinder international collaboration, particularly in fields where Czech research can benefit from global engagement.

Moreover, since 2019, when the authors began actively engaging with the topic of research security,[10] the overall preference for actor-agnostic and risk-based approaches has remained prevalent. However, China has been the implicit reference for many of the newly introduced measures, even if it is rarely mentioned explicitly in official policy documents. And while the authors broadly support existing approaches, sev-

eral key challenges to their successful implementation have emerged. These include, inter alia, the absence of China-specific language in research security policies, leading to ambiguities in risk assessment, a lack of China expertise among practitioners, resulting in limited awareness of country-specific risks and a variability in risk perception across disciplines, with differences between humanities, social sciences and STEM often overlooked.

Practitioners' resistance to the perceived 'securitisation' of research and the politicisation of HEIs further complicates the enforcement of research security measures. As a result, the authors have identified the recurrence of bad practice and even malpractice – defined as different types of research security issues or breaches such as self-censorship or data theft – partly due to the above factors.

To further understand these challenges, the authors conducted 15 semi-structured one-on-one or group interviews – both in person and online – with Czech, British, Dutch, and German policymakers and practitioners (see Annex I). To encourage open and candid discussion on this sensitive topic, interviewees were granted anonymity. The interviews were structured around several key themes: the importance, drivers, and limitations of existing research security measures, challenges persisting despite current policies, barriers to the effective implementation of research security, and the risks and costs of failing to strengthen these mechanisms. Throughout the analysis, several common concerns emerged, including the increasing politicisation of HEIs, the securitisation of research, and the bureaucratisation of scientific collaboration. In addition, the study revealed a discrepancy between general awareness of research security risks and a more detailed, subject-specific understanding of these risks. While many practitioners recognised the necessity of research security, there was often a lack of specific knowledge about risks associated with different countries, disciplines, and research topics.

Costs were widely perceived as being difficult to measure, with the discussions evolving around hypothetical risks (rather than concrete costs), which is consistent with most of the existing measures. What became evident throughout the interviews was also the apparent cautiousness of several practitioners, who focused on broad overviews over specific details, as well as the uncertainty as to whether their respective national, sectoral, institutional, or individual approaches were representative of good practice, wondering as to whether others have better answers than them.

The first part of the report examines developments in the Czech Republic, critically assessing the measures taken to enhance research security at the national, institutional, and sectoral levels. The second part draws inspiration from international best practices, focusing on the United Kingdom, the Netherlands, and Germany, where governments and academic institutions have proactively developed research security frameworks while maintaining openness to scientific collaboration. By analysing progress, stagnation, and setbacks in the adoption, implementation, and utilisation of research security measures in these countries, the policy paper seeks to identify effective research security strategies that could inform Czech policymakers and institutions.

The third part of the report provides concrete recommendations for Czech stakeholders, drawing on the best and worst practices identified across the four case studies. The policy paper advocates for guidelines that incorporate country-specific,

subject-specific, and issue-specific sections, checklists or toolkits. This is believed to complement existing measures by providing clearer discussions on the nature and levels of risk associated with different countries, subject areas, and research topics. Instead of a one-size-fits-all model, the report suggests tailored risk assessments that reflect the distinctive security considerations of various academic disciplines.

Equally important is striking a balance between bottom-up practitioners' perspectives and top-down policy mandates. While it is crucial to incorporate the insights of researchers, administrators, and institutional leaders, certain level of centralisation and structural enforcement must be ensured to strengthen research security effectively. A hybrid approach that combines bottom-up engagement with top-down regulation, supplemented by concrete examples of both good and bad practice, is the most viable way forward.

From crisis to strategy: research security in the Czech Republic

In the Czech Republic, the process of adopting research security measures originated from a specific negative experience. The Ministry of the Interior of the Czech Republic published the first research security-specific guidelines in 2021 as a direct response to a case of Chinese interference at Charles University, the oldest and most prestigious public university in the country. Scandals related to Chinese influence at the university (see Case 1) played a pivotal role in initiating a national debate on foreign interference. Charles University took the lead by approaching the Ministry of the Interior for guidance, which subsequently led to the adoption of the first university-level research security framework, formalised through a rector's decree.[11]

The decree establishes a formal framework for safeguarding scientific integrity, academic freedom, and intellectual property, while ensuring compliance with national security policies. It applies across all faculties, institutes, and research units within the university, reflecting a growing awareness of research security risks and the need for structured institutional oversight. At the core of the decree is a risk-based approach to international collaboration, focusing on the protection of scientific knowledge, data, and innovation from potential misuse. Recognising the heightened risks associated with certain research areas, the decree introduces a system of mandatory reporting which applies to cases where a student, prospective employee, or partner involved in a research or education project may breach – or is suspected of breaching – the international sanctions regime.

To further mitigate risks, the decree mandates due diligence procedures for international partnerships, requiring academic staff to screen potential collaborators, particularly when there is a risk of harm to the university's reputation or that of its employees or students, the exertion of foreign influence, a breach of restrictions under international control and sanctions regimes, or the theft of intellectual property. This process includes assessing institutional affiliations, funding sources, and legal ties to foreign governments, aiming to prevent unintentional knowledge transfer to entities that could exploit European research for strategic, military, or political purposes.

The decree establishes the position of a university security manager, responsible for overseeing institutional resilience at the university. This role involves developing and continuously refining the institutional resilience framework, conducting regular risk assessments, and identifying high-risk areas within academic programs, research disciplines, equipment and facilities. The security manager is also tasked with designing and implementing a structured training program for employees and students to enhance institutional resilience, as well as providing consultations and advisory services on related issues.

In addition to internal responsibilities, the security manager collaborates with other universities, government authorities, security agencies, diplomatic missions,

CASE 1: FUNDING OF PERSONNEL, EVENTS, AND OTHER ACTIVITIES OF A UNIVERSITY RESEARCH CENTRE BY CCP-LINKED INSTITUTIONS (HUMANITIES AND SOCIAL SCIENCES)

Institution	Charles University
Incident(s)	In 2016, Charles University, the oldest and most prestigious university in the Czech Republic, established the Czech-Chinese Centre as an expert, university-wide institute by a rector's decree.[12] The Centre was intended to serve as a hub for "research and education focused on political, economic, legal, social, territorial, media, cultural and security studies within the framework of cooperation between the Czech Republic and China."[13] However, the Centre's annual conferences were almost exclusively funded by the Embassy of the People's Republic of China in Prague and, as a result, leaned to pro-Beijing narratives. The collaboration with the Chinese embassy was also implied by the embassy's logo on the conference programmes.[14] The conferences were organised by the secretary of the Czech-Chinese Centre, who invoiced events to the Chinese embassy. He also invoiced the Chinese embassy for a course taught at the Charles University titled "The New Silk Road – China's Global Project."[15] Students attending the course, who submitted the best essays, were subsequently invited by the Chinese embassy on an all-expenses-paid trip to China as part of the Bridge for the Future programme.[16] This case represents a specific convergence of several problematic aspects: direct Chinese influence on the activities of a research centre at a prestigious academic institution; the implicit influence of the Chinese embassy on a course taught at one of its faculties and breach of students' personal data which were shared with the Chinese embassy.
Impact(s)	The extensive and detailed media coverage of the Czech-Chinese Centre case remains exceptional within the Central and Eastern European context. The case also attracted international attention, with major outlets such as the Financial Times reporting on the issue.[17] In an effort to mitigate reputational damage to Charles University, the Centre was dissolved, researchers implicated in the financial scheme were dismissed, and the university formally approached the Czech Ministry of the Interior to request practical guidelines – intended for both staff and students – to safeguard against illegitimate influence.[18]
Lesson(s)	The case underscores the inherent risks and institutional vulnerabilities associated with dependence on a single source of funding, particularly when such funding originates from a Chinese partner. Reliance on a sole external contributor – especially one with potential geopolitical or strategic motivations – can compromise the autonomy of academic institutions. This highlights the importance of diversified funding structures and the need for robust due diligence mechanisms when engaging with international partners. Charles University has introduced a system of due diligence procedures for international partnerships, requiring academic staff to assess potential collaborators – particularly in cases where there is a risk to the university's reputation or that of its employees or students; exposure to foreign influence; violations of international control and sanctions regimes; or the potential theft of intellectual property. This process entails evaluating institutional affiliations, sources of funding, and legal connections to foreign governments. In addition, the university has established the position of a security manager, tasked with overseeing and strengthening the institution's overall resilience.[19]

Source: Auhors' compliation

international organizations, and other relevant stakeholders to ensure a coordinated approach to research security.

At the faculty level, representatives of institutional resilience are appointed from among the staff. These representatives act as liaisons between the university security manager and faculty leadership, facilitating the exchange of information. They receive and process reports and concerns related to institutional resilience from faculty staff and students, offering consultations and guidance where necessary. Additionally, they regularly assess and identify high-risk study programs, academic disciplines, research teams, and projects, forwarding this information to the university security manager for further evaluation and action.

As one of the first formalised research security policies within Czech academia, this decree sets an important precedent for other universities in the country, encouraging them to adopt similar structured frameworks to mitigate risks while maintaining openness to international collaboration. Indeed, Palacký University in Olomouc has followed suit, creating the position of a security manager, while the Czech Academy of Sciences has also implemented internal guidelines, although these remain unavailable to the broader public.

Beyond individual universities and research centres, research security measures have been adopted primarily at the national level. The Ministry of the Interior introduced research security guidelines in cooperation with Charles University in 2021,[20] followed by the inclusion of research security in the Security Strategy of the Czech Republic in 2023.[21] At the same time, the Ministry of Education, Youth and Sports (MŠMT) has taken on a coordinating role, ensuring that responses to malign foreign influence are coherent rather than fragmented. In spring 2023, the MŠMT established the Inter-Ministerial Working Group for Combating Illegitimate Influence in the Higher Education and Research Environment,[22] facilitating coordination across government and academic stakeholders. The ministry has also authored three key documents: one focusing on institutional resilience, and two methodological guidelines establishing minimum due diligence standards.[23]

Czech respondents were explicit that the adoption of these research security measures has been largely reactive, with two main catalysts: growing international awareness of foreign interference (particularly lessons drawn from the UK and US) and a widely publicised security breach at Charles University's Czech-Chinese Centre, linked to Chinese funding.[24]

Interviews with government representatives highlighted Charles University, Palacký University Olomouc, and the Czech Academy of Sciences as the institutions that have made the most progress in implementing and utilising research security measures. Notably, these are the same institutions that have faced major challenges in their collaborations with China, further illustrating the reactive nature of Czech policy responses (see Table 1).

As in cases of Germany, the Netherlands and the UK, discussions surrounding research security in the Czech Republic are shaped by securitisation concerns. While the debate remains primarily centred at the national level, MŠMT has introduced the topic to the Czech Rectors' Conference (CRC) and continues to hold working dialogues with individual universities. These efforts raise the possibility of future sectoral and institutional measures.

One such measure already implemented is the reporting requirement for HEIs, which mandates annual submissions. The HEIs must submit two reports to the ministry annually – one covering the institution's overall activities and the other its financial management. From 2025 onwards, the annual report on institutional activities will include a dedicated section on strengthening resilience against 'illegitimate influence,' a term favoured by the Czech regulators as well as used by the HEIs.[25]

Beyond regulatory measures, government representatives also pointed to financial support mechanisms available to HEIs. Funding is available through programmes such as the Johannes Amos Comenius Programme (OP JAK), which is co-funded by the EU. This programme allows universities to allocate funds for dedicated staff, tools, or activities related to research security, depending on their specific institutional needs.

Learning from the best: identifying patterns in early adoptions of research security measures

As previously discussed, approaches to research security and perceptions of risk vary significantly across national contexts. The Czech case illustrates a notable (yet outlying) pattern in reaction to research security breaches, with initial concerns emerging primarily in the humanities and social sciences, before later extending to STEM disciplines.

To evaluate the extent to which this can indeed be categorised as an outlier, the authors aggregated data from primary and secondary literature and corroborated findings through interviews with stakeholders. This comparative analysis examines whether the initial drivers prompting a country to adopt research security measures differ significantly among the Czech Republic, Germany, the Netherlands, and the United Kingdom. By synthesising insights from multiple sources, this section aims to identify common challenges, best practices, and key divergences in research security policies across national, sectoral, and institutional levels.

The sub-sections are structured as follows: the first sub-section is based on the authors' macro-level analysis, providing information about the types of breaches that occurred within the selected HEIs; the second sub-section is based on the authors' micro-level analysis of transcripts from conducted interviews, which, corroborated against publicly available information, provide insights into practitioners' perceptions of different research security measures within the selected countries, as well as the different institutions involved in the adoption and implementation of these measures; and the third sub-section provides information about the selected research security measures at national and sectoral levels, focusing on their China-, subject- and issue-specific aspects.

STEM, HUMANITIES, OR SOCIAL SCIENCES: WHERE DOES THE ISSUE LIE?

Based on the macro-level analysis of the publicly available data, it became clear that there is a wide variety of issues that continue to occur when collaborating with Chinese partners, and which carry significant (albeit different) risks for the western institutions involved. These range from reputational, financial, legal and security costs to risks to academic freedom, independence of research and institutional autonomy. The issues mapped by this policy paper – several of which had occurred after the adoption of major research security measures – could be categorised into the following main issue areas (or types of breaches): sharing, transfer and theft of sensitive data (with heightened risks when it comes to personal and big data); R&D collaboration,

transfer and theft of dual-use technology (with heightened risks when it comes to emerging and disruptive technologies, EDTs, i.e., AI, quantum, biotech, integrated circuits, and new materials); IP infringement; censorship (including self-censorship), propaganda and other forms of interference; and funding of personnel and projects.

While most of the issues are intertwined and fall under several issue areas, a clear distinction can be made between issues associated with STEM subjects, and those associated with social sciences and humanities. STEM disciplines are dominated by concerns about data, technology, and IP theft, and are thus linked to more tangible risks, while humanities and social sciences are dominated by concerns about interference that are more abstract, which could partly explain the greater attention paid to STEM in research security. Yet, while the risks may indeed be more substantial when it comes to STEM, the abstract risks posed by censorship and propaganda efforts can lead to concrete costs for the very same academic freedoms most of the respondents interviewed for this policy paper were concerned about. This is important, as most of the existing measures (see Table 2) do not provide a comprehensive framework and discussion about risks based on the subject area or the types of issues they are most likely to be linked with.

The existing measures are also focused predominantly on research-related risks. However, as research does not occur within a vacuum, greater attention needs to be paid to teaching, funding, recruitment, and other functions of HEIs. This could further highlight the risks (and indeed costs) associated with humanities and social sciences, as exemplified by the long-standing concerns about the role of Confucius Institutes (CIs), China Scholarship Council (CSC) scholarships and joint educational institutes, to name a few.[26]

Moreover, while this paper concerns issues within individual countries, it is important to highlight the ongoing recurrence of issues at the EU level, as exemplified by the continued collaboration with the Seven Sons of National Defence (国防七子) – i.e., Chinese universities with deep ties to China's military and defence establishments that are directly controlled by the Ministry of Industry and Information Technology (MIIT) – within Horizon Europe projects.[27]

GOVERNMENTS OR ACADEMIC INSTITUTIONS: WHO DRIVES THE AGENDA?

While most interviewees (except the Czechs) had not much to say about the drivers of different research security measures – i.e., whether the impetus came from inside or outside their respective institutions or countries and whether the process was proactive or reactive – the government involvement and the importance of external impetus was implied by recurring references to increased politicisation of HEIs, securitisation of (scientific) research and bureaucratisation of (scientific research) processes by policymakers responsible for the adoption of national guidelines. These were themes repeated across most of our interviews.

In a similar fashion, the interviewees had not much to say about specific issues that had occurred within their own or other institutions (even after being prompted or asked directly), although the continued recurrence of different types of research

TABLE 1: SELECTED CASES OF CHINESE INTERFERENCE IN EUROPEAN ACADEMIA

Country	Institution	Subject area(s)	Issue area(s)
Czech Republic	Charles University[28]	humanities and social sciences	funding of events organised by the university's Czech-Chinese Centre by the Embassy of the People's Republic of China in Prague
Czech Republic	Palacký University Olomouc[29]	humanities and social sciences	Chinese propaganda disseminated by a Confucius Institute embedded within the university
Czech Republic	University of Pardubice[30]	STEM	collaboration with Chinese military-linked institutions, including on R&D of technology with military applications
Czech Republic	Czech Academy of Sciences[31]	STEM	some research funded exclusively by Chinese sources
Germany	Fraunhofer Society[32]	STEM	collaboration on R&D of dual-use technology (including EDTs) with Chinese military-linked institutions (e.g., at the Fraunhofer Institute for Electronic Nano Systems)
Germany	Max Planck Society[33]	STEM	collaboration on research of dual-use technology (including EDTs) with Chinese military-linked institutions
Germany	RWTH Aachen University[34]	STEM	collaboration on R&D of dual-use technology (including EDTs) with Chinese military-linked institutions
Germany	University of Duisburg-Essen[35]	humanities and social sciences	interference into the university's events and other activities by a Confucius Institute within the university and a Chinese consulate in Düsseldorf
Netherlands	Free University Amsterdam[36] (VU Amsterdam)	humanities and social sciences	funding of personnel, events, and other activities at a human rights research centre by CCP-linked institutions
Netherlands	Delft University of Technology[37] (TU Delft)	STEM	collaboration on R&D of dual-use technology (including EDTs) with Chinese military-linked institutions
Netherlands	University of Amsterdam[38]	STEM	collaboration on R&D of dual-use technology (including EDTs) with Chinese military-linked institutions
Netherlands	Leiden University[39]	STEM	collaboration on R&D of dual-use technology (including EDTs) with Chinese military-linked institutions
United Kingdom	Imperial College London[40]	STEM	data sharing, funding, and collaboration on R&D of dual-use technology (including EDTs) with Chinese military-linked institutions
United Kingdom	University of Manchester[41]	STEM	funding and collaboration on R&D of dual-use technology (including EDTs) with Chinese military-linked institutions
United Kingdom	University of Cambridge[42]	STEM	tech transfer and collaboration on R&D of dual-use technology (including EDTs) with Chinese military-linked institutions
United Kingdom	King's College London[43]	humanities and social sciences	funding of personnel and other activities at the university's China institute by CCP-linked individuals
United Kingdom	University of Nottingham[44]	humanities and social sciences	interference into events and activities of the university's Chinese studies school by a Confucius Institute and Chinese embassy

Source: Authors' compilation

security breaches was confirmed, with hypothetical issues discussed in terms of risks. Reputational risks were mentioned by all (but especially the British) respondents, with German respondents also emphasising risks posed to what they termed as the 'normal' functioning of science. In addition, all respondents agreed that risks vary between different subject areas and countries, though most of them were unable to provide concrete examples, and several (especially the UK researchers) respondents downplayed the level of risks associated with social sciences and humanities.

In the UK, research security measures were adopted across all levels, though they seem to be driven mainly by the national and sectoral levels, with the institutional level responding to these. HEIs play an active role in the implementation of research security measures within their structures, and many participate in sectoral groups that work collaboratively with the government. For example, the Academic Technology Approval Scheme (ATAS) – administered by the Foreign, Commonwealth & Development Office (FCDO) – requires researchers (including visiting academics) and postgraduate students (except those from certain exempted countries) to obtain clearance if their work involves knowledge applicable to military technology or weapons of mass destruction. Apart from the FCDO, the Department for Science, Innovation and Technology (DSIT) plays another key role in adopting and enforcing policies at the national level.

The Research Collaboration Advice Team (RCAT), which was requested by HEIs themselves, acts as the first point of contact for official advice about risks linked to international research collaboration. RCAT has advisors in offices around the UK and works closely with other organisations at both national and sectoral levels that play a major role in the development of research security measures, including the National Protective Security Authority (NPSA), UK Research and Innovation (UKRI) and Universities UK (UUK), all of which have published their own guidelines.

Government agencies with a broader focus, such as the National Cyber Security Centre (NCSC), are involved as well, with some interviewees specifically mentioning interactions with NCSC regarding collaborative research with China. Similarly to the existence of different reports and guidelines at the EU and OECD levels,[45] the G7 has published two papers that include information about the different definitions of research security (including the difference between research security and research integrity) and best practices,[46] while facilitating the sharing of resources through its Virtual Academy.[47]

At a sectoral level, most initiatives concern export controls (and thus STEM disciplines), with the Higher Education Export Control Association (HEECA) working closely with the Universities UK Export Control Group (UUK ECG), UKRI, NPSA and the government's Export Control Joint Unit (ECJU) that sits at the Department of Business and Trade. Besides HEECA, another major body representing the practitioners (namely the professional services) is the Association of Research Managers and Administrators (ARMA) that hosts the Higher Education Security Forum (HESF).

At an institutional level, the discussions took off in 2018-2019, with the University of Manchester and Imperial College London being among those leading the way, and while not stated explicitly, the interviewees implied that in both cases the impetus came not only from the government level but also from the major security breaches that occurred within the respective institutions (see Case 2).

CASE 2: FUNDING AND COLLABORATION ON R&D OF DUAL-USE TECHNOLOGY (STEM)

Institution	Imperial College London
Incident(s)	Imperial College London and the University of Manchester were among the first UK universities to adopt research security measures at an institutional level – both in response to incidents that had occurred within the institutions and in response to the government incentive. There were several widely publicised incidents that had occurred within Imperial; most of them concerning collaboration with Chinese companies and research institutes that have both direct and indirect links to the People's Liberation Army (PLA). Among the most controversial were the joint labs with Chinese defence companies, namely the Aviation Industry Corporation of China (AVIC), the Aero Engine Corporation of China (AECC), and the AECC's subsidiary – the Beijing Institute for Aeronautical Materials (BIAM).[48] AVIC, AECC and BIAM are all major suppliers of military aircraft and engines to the PLA. Between 2012 and 2022, Imperial hosted both the AVIC Centre for Structural Design and Manufacture and the BIAM-Imperial (previously AVIC) Centre for Materials, Characterisation, Processing and Modelling, which were closed after the UK government's Export Control Joint Unit (ECJU) rejected their export licence applications.[49] Another major incident in this issue area concerned the Future Digital Ocean Innovation Centre, which was established through partnership between the Imperial's Data Science Institute (DSI) and the Jiangsu Automation Research Institute (JARI), the latter of which is a major supplier of combat drones to the Chinese navy. The DSI-JARI agreement was signed in 2019 and terminated in 2021 thanks to the UK's export controls legislation. According to investigation by the UK-China Transparency network, the DSI's former head and manager responsible for Chinese partnerships both had explicit links to the CCP's United Front Work Department (UFWD).[50]
Impact(s)	The repercussions of these collaborations and their subsequent cancellations were major, ranging from financial losses (e.g., the expected funding amount for the DSI-JARI project was £3 million, with the Imperial returning all upfront funding following the cancellation of the project) to reputational costs (with several major media outlets, including the Guardian and the Financial Times, having reported on these links). Most importantly, however, these collaborations highlighted the risks of data and technology transfers that would directly benefit the military-industrial complex in China. The Imperial complied with the legislation on export controls and terminated these high-risk partnerships. It has also strengthened its own due diligence procedures to align them more closely with the national-level research security measures and policies, including the National Security and Investment Act (NSI Act) and the trusted research guidance by the National Protective Security Authority (NPSA).
Lesson(s)	The university's Research Office has developed several institutional-level policies, including the Relationships Policy from 2024,[51] and created checklists and toolkits that provide advice on different aspects of research security – from identifying potential partners, through managing risks, to safeguarding existing research projects. There are also internal trainings available to the members of staff, with the university planning to launch a trusted research e-learning module soon. At the same time, debates about how to define 'dual-use' while balancing open scientific research with national security concerns continue, with many researchers resisting the 'securitisation' of science and academia. Indeed, the continued collaborations on basic scientific research between Imperial researchers and Chinese scientists from PLA-linked institutions, including the Seven Sons of National Defence (国防七子) such as the Harbin Institute of Technology and the Northwestern Polytechnical University,[52] further highlight the complexity of these issues, especially as basic research, unlike applied research, often falls outside the scope of the existing measures.

Source: Auhors' compliation

While most interviewees acknowledged the progress made at the institutional level, especially when it comes to the variety of administrative positions created to provide guidance and ensure compliance with both national- and institutional-level research security measures, several problems persist. Chief among these is the perception of the measures as recommendations, with the compliance left on the willingness of individual academics, many of whom are less than enthusiastic, as they see these measures as bureaucratic burdens inhibiting their research. Indeed, as mentioned before, researchers are often more concerned about preserving the values and norms associated with open academic research, than what many described as a shift in government policy that went from encouraging research with China to constraining it. These were concerns echoed predominantly by academics from STEM disciplines, who acknowledged China's leadership in their respective research areas, expressing concerns about the potential negative effects of limited collaboration on their own research projects.

It is also important to note that the national-level measures are not implemented consistently across all universities, with most universities seen as laggards in this area. The same can be said about institutional-level measures, where most universities lag far behind the early adopters.

Similarly to the UK, research security measures in the Netherlands were adopted across all levels, and the national guidelines, alongside the National Contact Point for Knowledge Security,[53] were referenced by most respondents from the other three countries as examples of good practice. Indeed, several interviewees emphasized the importance of a centralised, national-level body akin to the Dutch contact point that can not only enforce but also facilitate the implementation of national policies by providing the relevant support and resources, especially for universities that often lack both financial and human capital. To some extent, the point was compared to the RCAT offices in the UK, though these were seen as less proactive and efficient.

The government-level facilitation and the collaborative nature are seen as the two major aspects of the Dutch approach. The National Knowledge Security Guidelines were published in 2022 as a response to rising government concerns about technological competitiveness, geopolitical tensions and several research security incidents that had occurred across Europe, including in the Netherlands (see Case 3). The guidelines were themselves drawn in collaboration with universities and other research institutions, including sectoral bodies like the Royal Netherlands Academy of Arts and Sciences (KNAW) and the Dutch Research Council (NWO), which is a major funding body under the Dutch government. The guidelines are always evolving, with initial focus on export controls later complemented by a focus on influence operations and ethical considerations that can impact broader academic freedom as well as personal safety of both researchers and students within Dutch universities.

While the Ministry of Education, Culture and Science is responsible for overseeing the institutional-level compliance, the responsibility for implementation lies with the individual institutions, which attempt to balance maintaining values of open science (emphasised as important for scientific growth) with protecting sensitive knowledge areas – all while being under various financial and institutional constraints. At the institutional level, the initial activities focused on awareness raising, with the posi-

tions for university-level policy advisers and faculty-level contact points accompanied by presentations and training programmes based on specific examples and tailored to specific subject areas. And while the current focus – especially at the national level – is on creating more nuanced, context-specific risk assessment methodologies across different subject areas, with planned initiatives including a screening mechanism for sensitive technologies, the need for continued awareness raising efforts was emphasised by all interviewees.

The Netherlands was also one of the countries perceived as most active at the EU level, especially when it comes to setting up minimum research security standards that would apply to all actors seeking funding under FP10, and cooperating within Horizon Europe.

Finally, Germany has adopted several guidelines at the sectoral level, while lacking guidelines at the national level. The only major national-level measure is the export control manual published and administered by the Federal Office for Economic Affairs and Export Control (BAFA), though unlike the UK's ECJU, BAFA can act only if approached by the practitioners (namely researchers) themselves.

Discussions on research security gained traction in 2018-2019, driven mainly by funding bodies, especially project management agencies. These agencies could be seen as intermediaries between the relevant ministries, namely the Federal Ministry of Education and Research (BMBF), and individual HEIs; and among them, the DLR Projektträger – i.e., the project management agency of the German Aerospace Center (DLR) – drives the discussion, especially when it comes to research security measures related to China. Indeed, the DLR has developed into a de facto advisory body for the BMBF.

While the agencies drive the development of research security measures, the initial impetus came from structural shifts in both national and international environments, with one interviewee referencing a visit to the Netherlands as eye-opening, and another relating the gradual shift toward securitisation of research to a broader shift in Germany's China policy while noting that the discussions are both need- and fear-driven. And while the interviewees all praised the Dutch whole-of-government approach for its coherence and transparency, they also emphasised the unique features of the DLR approach – namely, its (re)conceptualisation of international collaboration as an inherent part of science that, similarly to science, needs to be safeguarded; and the understanding that concrete measures need to be developed in a bottom-up manner by researchers themselves.

The respondents further emphasised the unique (and sometimes inhibiting) features of the German higher education system, namely its decentralised nature and emphasis on institutional autonomy, which were deemed as a major challenge to the adoption of federal-level guidelines, while also linked to structural barriers preventing effective implementation and utilisation of the existing sectoral and institutional measures. These include resource constraints (especially at universities that tend to lack both financial and human resources); format (with the guidelines perceived as recommendations rather than mandates); practitioners' lack of knowledge concerning the Chinese partners, contracts and higher education system and, most importantly, resistance on the part of academics (especially the more senior ones) to accepting any level of regulation – whether it comes from the state or their own institution – that

CASE 3: FUNDING OF PERSONNEL, EVENTS, AND OTHER ACTIVITIES OF A UNIVERSITY RESEARCH CENTRE BY CCP-LINKED INSTITUTIONS (HUMANITIES AND SOCIAL SCIENCES)

Institution	Vrije Universiteit Amsterdam (VU Amsterdam)
Incident(s)	The Dutch public broadcaster NOS reported that the Cross Cultural Human Rights Centre (CCHRC) at VU Amsterdam was exclusively funded by a Chinese partner.[54] Specifically, in the years 2018, 2019, and 2020, the Centre received annual subsidies ranging from €250,000 to €300,000 from the Southwest University of Political Science and Law in Chongqing.[55] The CCHRC engaged in a range of academic activities, including the publication of a scholarly journal and the organisation of conferences. According to the financing agreement between the two institutions, the Centre's mission was to promote a "global view of human rights," with particular attention to how non-Western countries – China, in particular – conceptualise human rights. Controversy arose when several affiliated researchers publicly downplayed the human rights situation of Uyghurs in China. For instance, the Centre's website stated: "The situation we encountered in the four cities in [the] trip [to China] did not reflect the grim situation as depicted in the Western reports. There is definitely no discrimination of Uyghurs or other minorities in the region." The Centre's director later asserted that any apparent alignment between the CCHRC's publicly expressed positions and those of the Chinese Communist Party was purely coincidental and not the result of direct influence or external direction.[56]
Impact(s)	The incident had significant reputational repercussions, as extensive media coverage provoked public outcry and prompted strong condemnations from the Dutch Minister of Education and other officials. The controversy also resulted in financial consequences: in an effort to mitigate the scandal, the university opted to return the subsidy it had already received from the Chinese partner for that financial year. Based on previous contributions, this amount is estimated to have ranged between €250,000 and €300,000.
Lesson(s)	In response to the situation, the university immediately suspended the activities of the Centre, including the cancellation of all scheduled lectures for students. A committee was subsequently established to conduct an internal investigation into the Centre's operations. The university later announced that the committee found no evidence that individual researchers had had their views 'bought' or that self-censorship had occurred under pressure from Chinese partners. The committee also concluded that there had been insufficient openness and transparency regarding the way in which the Centre was financed.[57] As a result, the CCHRC was later disbanded. The case underscores the risks associated with a limited understanding of China's political objectives, as well as the tactics, techniques, and procedures employed to exert influence over academic institutions in liberal democracies. It reveals serious shortcomings in due diligence and risk assessment, particularly in the context of partnerships with foreign actors operating within a different normative framework. Moreover, the situation illustrates the institutional vulnerability that arises from an overreliance on a single external funder, especially one with authoritarian state affiliations.

Source: Auhors' compliation

would infringe on their academic freedoms and what they deem as the 'normal' way of doing open scientific research.

This resistance is further strengthened by the perceived politicisation and securitisation of scientific research, new layers of bureaucracy imposed on the researchers as well as their lack of awareness of the risks associated with Chinese collaborators. One interviewee emphasised the need for generational change and educational

initiatives to instil awareness of different research security issues and risks among young scholars. This interviewee also emphasised the lack of empirical evidence when it comes to concrete measures and examples of costs emanating from risks of collaborating with Chinese partners as another aspect contributing to the resistance on the part of researchers.

While emphasising that all the main research-intensive institutes (i.e., Max Planck, Fraunhofer, Leibniz and Helmholtz) have robust research security measures, especially the applied science institutes like Helmholtz and Fraunhofer that focus on cutting-edge technologies, many of these are internal documents, which further contributes to the perception of the German approach as scattered and lagging behind. The Max Planck Society, which does basic research and is thus more theoretically oriented, has several publicly available guidelines, but this seems to be an exception rather than a rule, with one interviewee pointing at the role of Chinese partners in concerns associated with making these documents public. It was also mentioned that the BMBF is in the process of setting up a research security and investment screening unit based on ongoing consultations with other stakeholders and branches of the federal government.

Moreover, the interviewees emphasised the trade-offs between rigid research security measures that could stifle innovation (i.e., over-regulation), on one hand, and insufficient safeguards that could leave German institutions vulnerable to a variety of risks (i.e., under-regulation), on the other. One interviewee noted that an unintended consequence of over-regulation and decreased engagement with China could be a decreased understanding of China (based on narratives rather than facts) as well as a decreased flow of knowledge that could diminish Germany's own ability to maintain its competitive edge in the fields of science where China continues to have major breakthroughs. Another interviewee mentioned the notion of 'unintended decoupling' as a descriptor for the situation in Germany, where the different stakeholders do not pursue decoupling per se but initiate fewer and fewer new collaborations instead.

In terms of the types of risks, the German interviewees mentioned reputational, contractual, and financial risks, with the latter seen as the most difficult to measure. One interviewee also mentioned their own change of mind when it comes to reputational risks, which they now see as short-lasting and thus less important. This is unlike the situation in the UK, where reputational risks were mentioned as important by all interviewees (especially researchers and academics from the major Russell Group universities), though several academics also questioned this over-emphasis on institutional reputation. There was also an agreement that the risks faced by STEM subjects are different to those faced by humanities and social sciences, albeit STEM disciplines, especially those with potential military and dual-use applications, were seen as attracting greater attention and necessitating more stringent research security measures (see Case 4). Humanities and social sciences often lack the same level of attention, though one interviewee noted that most of the issues that had occurred in Germany and led to actual costs relate to these neglected subject areas. This again differred from the UK, where all respondents associated the actual costs with STEM subjects.

Indeed, this interviewee saw the differentiation between humanities, social sciences and STEM subjects in terms of actual costs in the case of the former and potential risks in the case of the latter, thus highlighting the importance of paying attention to

CASE 4: FUNDING AND COLLABORATION ON R&D OF DUAL-USE TECHNOLOGY (STEM)

Institution	RWTH Aachen University
Incident(s)	Several German media outlets (most extensively the investigative outlet Correctiv)[58] reported on the extensive links between researchers at the RWTH Aachen and the Chinese scientists. There is a continued collaboration between RWTH Aachen and the Seven Sons of National Defence (国防七子), including the Harbin Institute of Technology and the Northwestern Polytechnical University.[59] The university also has a strategic partnership with Tsinghua University, which, while not being a Seven Sons institution, is supervised by the State Administration of Science, Technology, and Industry for National Defence (SASTIND).[60] An example of a risky collaboration in the area of dual-use technology is the Artificial Assisted Heart Overseas Research and Development Institution, a joint project between the RWTH Aachen University in Germany, the Northwestern University of Applied Sciences in Switzerland and the China Academy of Launch Vehicle Technology (CALT). CALT is a subsidiary of China Aerospace Science and Technology Corporation (CASC), a major supplier of missiles, rockets, and satellites to the PLA.[61] The Australian Strategic Policy Institute (ASPI) notes that the technology in artificial hearts is similar to that in missile control systems, which seems to align with CALT's practice of funding civilian technologies with dual-use applications.
Impact(s)	The incident likely resulted in tangible costs related to the transfer of data and technology to China, which could be utilised by the Chinese military. It also carried reputational repercussions, following Correctiv's publication, which prompted several public statements by political figures, including former Green Party Bundestag member Kai Gehring.[62]
Lesson(s)	RWTH Aachen has published a statement in response to the Correctiv article, which notes that the university cooperates with federal agencies, namely the Federal Office for Economic Affairs and Export Control (BAFA) and has its own internal procedures to manage and safeguard collaborations with its partners.[63] Most importantly, however, the university notes that the reported collaborations fell under the category of basic research, which highlights the continued neglect of risks in basic research by practitioners.

Source: Auhors' compliation

all subject areas. The difficulty in measuring, assessing and prioritising risks due to the lack of a unified and sound methodology, alongside a lack of concrete examples of actual costs, were mentioned as further complicating the attempts at persuading the researchers to take the topic of research security seriously, thus highlighting the intertwined nature of research security challenges.

BEST AND WORST PRACTICES: TOWARDS BALANCED, INCLUSIVE AND SPECIFIC GUIDELINES

Due to the significant differences in higher education governance structures between the four countries, there are limits to the transfer of best practices from one country to another. For example, the reason for the higher number of measures adopted at sectoral (rather than national) levels in Germany lies in its decentralised governance structure, which is not the case in the other three countries. This, however,

does not prevent the creation of country-specific, issue-specific, and subject-specific checklists and toolkits within the existing measures that could be amended to fit the governance structures of individual countries.

The existing measures range from broad guidelines and instruments (including export controls, investment screening mechanisms and visa regulations) adopted by policymakers at the national level (i.e., top-down approaches) to specific policies and tools (including teams or individual members of staff responsible for providing advice and overseeing the implementation of the respective measures) adopted by practitioners at the institutional level (i.e., bottom-up approaches). Sectoral measures adopted by specific committees, groups, and organisations representative of the higher education sector lie somewhere in between.

Most of the existing measures at national and sectoral levels (see Table 2) do not include China-specific sections, be it in the forms of checklist or other toolkits. The same can be said about any sections on issue-specific risks, with most of the selected measures including only sporadic references, without any extensive, comprehensive discussions of these. Subject-specific sections are similarly lacking in detail, and are in most cases limited to STEM disciplines and the list of critical technologies that require greater scrutiny of international collaborations. Moreover, the inclusion of these sections need to be complemented by broader cultural and structural changes at the levels of individual institutions, as without these, the measures will be limited to another checklist exercise that does not lead to any substantive improvements to research security.

TABLE 2: SELECTED NATIONAL- AND SECTORAL-LEVEL GUIDELINES IN THE CZECH REPUBLIC, GERMANY, NETHERLANDS, AND THE UNITED KINGDOM

Country	Year	Author	Level	Name	China-specific	Subject-specific	Issue-specific
Czech Republic	2021	Ministry of the Interior	National	Counter Foreign Interference Manual for the Czech Academic Sector[64]	NO	NO	PARTLY
Czech Republic	2021	Financial Analytical Office	National	Technical Assistance and Intangible Transfer of Technology[65]	NO	YES (STEM)	PARTLY
Czech Republic	2024	Ministry of Education, Youth and Sports (MŠMT)	National	Recommendations on research security-related due diligence, risk management and anti-interference measures[66]	NO	YES (STEM)	YES
Germany	2020	German Academic Exchange Service (DAAD)	Sectoral	No Red Lines: Academic Cooperation Within Complex Legal and Regulatory Environments[67]	NO	YES	PARTLY
Germany	2020	German Rectors' Conference (HRK)	Sectoral	Guiding Questions on University Cooperation with the People's Republic of China[68]	YES	NO	PARTLY

Germany	2020	Commission of Experts for Research and Innovation (EFI)	Sectoral	Report on Research, Innovation and Technological Performance in Germany[69]	YES	YES (STEM)	PARTLY
Germany	2023	Federal Office for Economic Affairs and Export Control (BAFA)	National	Export Control and Academia Manual (2nd Edition)[70]	NO	YES (STEM)	PARTLY
Germany	2024	DLR Projekträger	Sectoral	Due Diligence in Science: Manual for an Assessment Process: Safeguarding Science and Scientific Cooperation[71]	NO	YES (STEM)	YES
Netherlands	2022	Joint initiative of the Dutch government and the knowledge sector	National	National Knowledge Security Guidelines: Secure International Collaboration[72]	NO	YES (STEM)	YES
Netherlands	2024	Universities of the Netherlands (UNL)	Sectoral	Capability Maturity Model: Knowledge Security[73]	NO	NO	YES
United Kingdom	2013	Foreign, Commonwealth and Development Office (FCDO)	National	Academic Technology Approval Scheme (ATAS) [74]	NO	YES (STEM)	NO
United Kingdom	2020	Universities UK (UUK)	Sectoral	Managing Risks in Internationalisation: Security Related Issues[75]	NO	YES (STEM)	YES
United Kingdom	2021	Export Control Joint Unit (ECJU)	National	Export Controls Applying to Academic Research[76]	NO	YES (STEM)	PARTLY
United Kingdom	2021	Cabinet Office	National	National Security and Investment Act: Guidance for the Higher Education and Research-Intensive Sectors (NSI Act)[77]	NO	YES (STEM)	PARTLY
United Kingdom	2021	UK Research and Innovation (UKRI)	Sectoral	Trusted Research and Innovation Principles[78]	NO	NO	PARTLY
United Kingdom	2024	National Protective Security Authority (NPSA)	National	Trusted Research Guidance for Academics[79]	NO	YES (STEM)	YES

Source: Authors' compilation

Explainer: The 'China-specific' column refers to any language concerning China-specific risks within the selected documents. The 'subject-specific' column refers to any language concerning subject-specific risks, and if limited to just one subject area, specifying which (STEM, humanities, and social sciences). The 'issue-specific' column refers to any language concerning issue-specific risks, with the designation 'partly' meaning that the document refers to at least one issue area (e.g., sharing, transfer and theft of sensitive data; R&D collaboration, transfer and theft of dual-use technology; IP infringement; censorship, propaganda and other forms of interference; funding of personnel and projects), but lacks a more detailed, comprehensive discussion.

Conclusion

While Czech academic institutions have formally adopted the discourse of countering malign foreign influence, there is a significant risk that these efforts remain largely declaratory. Many universities and research institutions have endorsed research security measures at the policy level, yet the extent to which these institutions (and the individual practitioners) have internalised the logic of the agenda and its underlying objectives remains uncertain. Without deeper institutionalisation, there is a possibility that compliance with research security measures will be superficial, reducing them to symbolic commitments rather than effective safeguards.

The research security measures introduced thus far – including policy recommendations, internal regulations, and the recruitment of administrative staff tasked with managing the agenda – have not yet been fully integrated into the daily functioning of academic institutions. A notable gap exists between institutional leadership and academic staff in terms of awareness, understanding, and practical application of research security principles.

While university leadership may adopt security-oriented policies, it is the academics and researchers themselves who initiate and implement international collaborations, including those with partners from countries where research security concerns are particularly pronounced, such as China. This disconnect raises concerns about the effectiveness of current measures, as policies alone do not automatically translate into institutional behavioural change.

A key challenge in embedding research security within Czech academia lies in the misalignment between formal institutional hierarchies and the actual functioning of academic environments. While universities and research institutions may appear hierarchical on paper, in practice, they operate within highly decentralised and relatively autonomous academic cultures. The traditional collegial and independent nature of academic work means that institutional leadership does not necessarily exert strong control over the international partnerships and collaborations pursued by individual researchers and research teams. Consequently, policy decisions taken at the top do not always trickle down effectively, leading to inconsistent implementation of security measures across departments and research groups.

Further complicating the integration of research security measures is the academic community's general resistance to security-driven policymaking. The counter-interference agenda introduces a security-oriented perspective that is often at odds with traditional academic values such as openness, freedom of inquiry, and international collaboration. Many researchers view security concerns as an external imposition rather than an intrinsic part of their professional responsibilities. The academic culture, particularly within the social sciences and humanities, tends to be wary of securitisation, perceiving it as a potential constraint on academic freedom rather than a necessary safeguard. In contrast, STEM disciplines, where concerns about

intellectual property theft and dual-use research are more tangible, tend to be more receptive to discussions on research security.

These factors highlight the complexity of institutionalising research security within Czech academia. While significant progress has been made at the policy level, ensuring that these measures are understood, accepted, and effectively implemented across academic institutions remains a major challenge. Without a strategic approach that bridges the gap between leadership and academic staff, and without targeted engagement efforts that address the specific concerns of researchers across different disciplines, research security in the Czech Republic risks remaining an administrative formality rather than a fully functional protective framework.

Our analysis has demonstrated that while the Czech Republic has made important strides in research security, significant gaps remain in the actual implementation and internalisation of these measures within academic institutions. Policies have been adopted, guidelines introduced, and administrative structures expanded, yet a disconnect persists between formal commitments and the practical realities of academic collaboration. The challenge is no longer merely raising awareness or introducing regulations, but rather ensuring that research security becomes an integral part of institutional culture and decision-making processes.

The following recommendations outline concrete steps to address these shortcomings. They emphasise the need for a whole-system approach, where research security is not merely a top-down directive but a shared institutional responsibility. Key areas for improvement include enhancing academic ownership of the agenda, refining due diligence processes, broadening the understanding of foreign interference risks, and ensuring long-term sustainability through institutional support and government-backed initiatives. Taken together, these recommendations aim to transform research security in the Czech Republic from a reactive policy response to a fully functional and integrated system that balances openness to international collaboration with the protection of national and academic interests.

Recommendations for stakeholders

Build a working system that goes beyond 'just' awareness: The Czech academic sector has made notable progress in addressing malign foreign influence, moving from initial awareness towards institutionalising research security. Universities and research centres have adopted formal norms and recommendations, established internal regulations, and created new administrative positions dedicated to managing this agenda. These steps demonstrate a clear commitment to enhancing research security.

However, there is a risk of complacency – institutions may declare the problem "solved" simply by adopting policies and hiring dedicated personnel, without ensuring that these measures translate into a fully functional system. In the academic environment, the bulk of international collaboration, including collaboration with scholars from countries of concern such as China, is initiated at the level of individual researchers or research teams. For research security measures to be effective, they must be understood and applied at this operational level. This requires ongoing engagement, clear communication, and a nuanced evaluation of the risks associated with international partnerships.

A whole-system approach – adapted to the specific structure of academia – is needed. Research security must be embedded across all levels of the academic ecosystem, including institutional leadership, administrative teams, and individual researchers. While universities have formal hierarchical structures, their actual functioning is much more decentralised. Effective implementation of research security policies must acknowledge this reality. Merely issuing regulations and hiring security officers is insufficient; there must be ongoing internal communication, tailored guidance, and regular engagement with researchers to ensure that security concerns are understood and internalised without compromising the academic culture of openness.

Encourage academic ownership... or outsource it: For research security to be effective, universities must not only comply with external recommendations but internalise the rationale behind them, making security awareness an integral part of everyday academic practice.

Achieving this is challenging for two reasons. First, securitising international cooperation runs counter to traditional academic values of openness, collegiality, and the free exchange of ideas. With the exception of research institutions working on cutting-edge technologies or classified projects, many academics view security-driven restrictions as a barrier rather than a necessity. Reputation also plays a role: while security policymakers often highlight the reputational risks of collaborating with actors from problematic countries, academics may be equally concerned about the stigma of being perceived as aligned with state security services. Managing this tension requires careful calibration, as well as trust-building efforts that respect academic norms.

Second, foreign influence is just one of many new demands placed on academic institutions in recent years. Research security measures require additional time, finan-

cial resources, and personnel – all of which are often already stretched thin. Unless the Czech government provides dedicated and substantial funding to support this agenda, there is a risk that institutions will engage in purely symbolic compliance, implementing research security measures for appearances rather than effectiveness.

Given these challenges, the Czech government may need to go well beyond the Inter-Ministerial Working Group, centralising expertise by establishing a national advisory body, similar to the Dutch National Contact Point for Knowledge Security. A specialised unit could provide consistent guidance, expertise, and training to universities, reducing the burden on individual institutions while ensuring a coordinated national approach.

Move beyond binary approach: In developing policies to mitigate China's malign influence, Czech institutions often look to the UK, US, Australia, and other countries with extensive experience in countering foreign interference. However, this approach risks overlooking a fundamental difference: the scale of collaboration with China in the Czech Republic is relatively limited. Unlike major Western research hubs, Czech universities do not host large numbers of Chinese scholars or students, nor do they have extensive institutional partnerships with Chinese universities. This raises an important question: should Czech academia even invest in building a complex risk assessment system for China-related collaborations, or would a simple ban – similar to the post-2022 embargo on Russian academic partnerships – suffice?

The authors advise against such a shortcut approach for two key reasons. First, despite its authoritarian political system, China remains a leading centre of scientific innovation, particularly in fields such as AI, quantum computing, and biotechnology. Engaging with Chinese researchers can bring valuable insights and collaborations, whether in terms of academic knowledge, access to new research data, or intercultural exchange. Recent breakthroughs, such as China's DeepSeek large language model, demonstrate that excluding Chinese scholars entirely would mean ignoring key developments in global research.

Second, the future of global academic collaboration is unlikely to be defined by rigid ideological divides. While democratic countries may seek to limit technological transfers to authoritarian states, a binary approach – e.g. "India, yes; China, no" – is unlikely to be sustainable in the long run. As the international order becomes more multipolar, European countries, including the Czech Republic, will need to develop a flexible and nuanced research security system – one that can assess risks and benefits on a case-by-case basis rather than defaulting to blanket bans.

Deal with real issues: Existing research security guidelines often begin with broad definitions of malign foreign influence, yet in practice, they tend to focus on technological and security-driven risks, such as the protection of sensitive research and critical technologies. While this focus is understandable, it can lead to a narrow and incomplete approach to research security.

A significant proportion of foreign interference occurs not in classified research settings but in everyday academic interactions, such as classroom discussions, student exchanges, and joint publications. For example, Chinese students enrolled in Czech universities may feel pressured to monitor class discussions or report polit-

ically sensitive content to their state apparatus. However, current research security frameworks lack specific guidance on how to manage such situations despite these being perhaps more prevalent than the cases of hosting incoming Chinese scholars.

To build a comprehensive research security system, Czech academic institutions must ensure that their guidelines address a full spectrum of risks, including not only technical threats but also academic integrity concerns, ideological pressures, and soft influence operations. Achieving this will require greater engagement with frontline researchers, feedback loops to capture real-world experiences, and training on how to navigate politically sensitive issues in an academic setting.

Improve due diligence: Some counter-interference measures, such as restricting access to sensitive research for scholars from high-risk countries, are relatively straightforward. However, other cases require nuanced judgment. For example, should a Chinese professor be invited to lecture on political philosophy at a Czech university if their published work critiques liberal democracy? Does such a course provide valuable academic insight, or does it represent an attempt at ideological influence?

Research security officers responsible for due diligence assessments often lack the academic expertise to make such determinations. As a result, institutions risk falling back on rigid categorical assessments, such as prohibiting collaboration with Chinese universities based solely on their links to China's civil-military fusion strategy. While this approach may appear risk-averse, it can also lead to unnecessary restrictions that hinder legitimate academic engagement.

To ensure effective and fair due diligence, Czech institutions must move beyond regulatory checklists and develop a system where research security is embedded into institutional decision-making at all levels. This requires enhanced communication between security personnel and academic leadership, ensuring that assessments are both rigorous and context aware.

ANNEX 1: ANONYMISED LIST OF INTERVIEWEES

Date	Country	Institution	Format
15/10/2024	United Kingdom	University of Nottingham	One-on-one interview
16/10/2024	United Kingdom	King's College London	One-on-one interview
17/10/2024	United Kingdom	University of Manchester, Higher Education Security Forum (HESF), and Higher Education Export Control Association (HEECA)	One-on-one interview
22/10/2024	United Kingdom	Imperial College London	One-on-one interview
23/10/2024	United Kingdom	Department for Science, Innovation and Technology (DSIT), including Research Collaboration Advice Team (RCAT)	Closed-door discussion (roundtable)
23/10/2024	United Kingdom	Imperial College London	Closed-door discussion (roundtable)
24/10/2024	United Kingdom	University of Cambridge	One-on-one interview
24/10/2024	Czech Republic	Charles University	One-on-one interview
24/10/2024	Czech Republic	Ministry of Education, Youth and Sports (MŠMT)	One-on-one interview
19/11/2024	Germany	German Aerospace Centre (DLR)	One-on-one interview
25/11/2024	Germany	Max Planck Society	One-on-one interview
16/12/2024	Netherlands	VU Amsterdam	One-on-one interview
17/12/2024	Netherlands	Clingendael Institute, Leiden Asia Centre	One-on-one interview
19/12/2024	Netherlands	TU Delft	One-on-one interview
5/2/2025	Czech Republic	Charles University	One-on-one interview

Source: Authors' compilation

About Authors

Ivana Karásková, is the China Team Lead at the Association for International Affairs (AMO). She founded and coordinates two international projects on China: MapInfluenCE, analysing Chinese and Russian influence in Central Europe, and China Observers in Central and Eastern Europe (CHOICE), a network of over 130 China researchers from 30 countries. From April 2023 to March 2024, she served as Special Advisor to European Commission Vice-President Věra Jourová, consulting on the Defence of Democracy package.

Since 2020, Ivana has been an Associate Fellow at the Mercator Institute for China Studies (MERICS) and is part of the China expert pool at the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) in Helsinki. She has also been working as a researcher at the Faculty of Social Sciences, Charles University, where she focuses on resilience of supply chains against foreign information manipulation and interference. Her research spans China's influence, propaganda, disinformation, EU-China relations, and state resilience.

Ivana holds a Ph.D. in International Relations and degrees in Journalism, European Studies, and Mass Communication. She has completed research stays in China, Taiwan, and the US (as a Fulbright scholar at Columbia University). She has testified at the US Congress, European Parliament, Belgian Parliament, Bundestag, and Canada's House of Commons, briefed NATO and senior politicians and institutions across Europe. Her expertise has been cited in The New York Times, BBC, Politico, Financial Times, Al Jazeera, Le Monde, and more.

✉ *ivana.karaskova@amo.cz* 𝕏 *@ivana_karaskova*

Dominika Remžová is a China Analyst at AMO, specializing in Chinese foreign and economic policies, with a particular focus on industrial policy, supply chains, critical raw materials, and electric vehicles.

Dominika has a wealth of research experience, including her most recent work at the International Institute for Strategic Studies (IISS) in Berlin, where she collaborated on projects focusing on the effectiveness and sustainability of EU CSDP missions and defence cooperation in the Eastern Mediterranean, and the Central European Institute of Asian Studies (CEIAS) in Bratislava, where she focused on Taiwan's domestic politics and external relations. She has also

worked at the University of Nottingham's Rights Lab, where she researched human rights abuses in Xinjiang.

Dominika is pursuing her PhD in Political Science and International Relations at the University of Nottingham, where she has been focusing on positions of different Central and Eastern European countries in global value chains and their respective foreign policies toward China and Taiwan. Currently, she is also an editor at the University's Taiwan Research Hub and a frequent contributor to the Hub's magazine – Taiwan Insight. She has earned her Master's degree in Taiwan Studies from the School of Oriental and African Studies (SOAS) in London and her Bachelor's degree in Chinese Studies from the University of Manchester.

✉ *dominika.remzova@amo.cz* 𝕏 *@DominikaRemzova*

About AMO

Association for International Affairs (AMO) is a non-governmental non-profit organization founded in 1997. It is not bound to any political party or ideology. The mission of AMO has been to contribute to a deeper understanding of international affairs through a broad range of educational and research activities. We offer space for the expression and realisation of ideas, thoughts and projects for the development of education, understanding and tolerance among people.

AMO is a unique transparent platform that brokers dialogue between the general public, academia, civil society, politics and business. It has a tradition of promoting the interest of Czech citizens in international affairs and provides information necessary for forming independent opinion on current events both at home and abroad.

With its activities, it supports an active approach to foreign policy, provides an independent analysis of current political issues and encourages expert and public debate on related topics. Among our goals is a systematic observation, analysis and commentary on international affairs with a special focus on Czech foreign policy.

IN ORDER TO ACHIEVE ITS GOALS AMO:

- → formulates and publishes briefing, research and policy papers;
- → arranges international conferences, expert seminars, roundtables, public debates;
- → organizes educational projects;
- → presents critical assessments and comments on current events for local and international press;
- → creates vital conditions for growth of a new expert generation;
- → promotes interest in international relations in the wider public domain;
- → cooperates with like-minded local and international institutions.

FOLLOW US!

amo.cz
facebook.com/AMO.cz
x.com/AMO_cz
youtube.com/AMOcz
linkedin.com/company/AMOcz
instagram.com/AMO.cz

Footnotes

1 "EU Member States adopt recommendations to enhance research security," European Commission, 23 May 2024, https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/eu-member-states-adopt-recommendations-enhance-research-security-2024-05-23_en.

2 "Annex to the Commission Recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States," European Commission, 3 October 2023, https://defence-industry-space.ec.europa.eu/system/files/2023-10/C_2023_6689_1_EN_annexe_acte_autonome_part1_v9.pdf; "Commission recommends carrying out risk assessments on four technology areas: advanced semiconductors, artificial intelligence, quantum, biotechnologies," European Commission, 3 October 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4735.

3 European Commission, "An EU Compass to regain competitiveness and secure sustainable prosperity," 29 January 2025, https://ec.europa.eu/commission/presscorner/detail/en/ip_25_339.

4 "Artificial Intelligence for Europe," European Commission, COM (2018) 237 final, 25 April 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018DC0237.

5 "Artificial Intelligence," Ministry of Industry and Trade of the Czech Republic, https://mpo.gov.cz/en/business/digital-economy/artificial-intelligence/.

6 "Univerzita Karlova koordinuje projekt otevřených AI jazykových modelů v Evropě," VědaVýzkum.cz, 7 February 2025, https://vedavyzkum.cz/granty-a-dotace/univerzita-karlova-hlavnim-koordinatorem-rozsahleho-projektu-otevrene-velke-jazykove-modely-pro-umelou-inteligenci-v-evrope.

7 Ivana Karásková, Filip Šebok, and Veronika Blablová, *How to Do Trusted Research: China-Specific Guidelines for European Stakeholders* (Association for International Affairs (AMO), 2022), https://www.amo.cz/wp-content/uploads/2022/09/HTDTR_report_how-to-do-trusted-research_A4_18_web.pdf.

8 The United Kingdom uses the G7's definition of 'research security' when referring to the range of issues and risks associated with international research collaboration. The term 'trusted research' refers to the UK Government's suite of publicly available advice and guidance.

9 Ivana Karásková, Filip Šebok, and Veronika Blablová, *How to Do Trusted Research: China-Specific Guidelines for European Stakeholders* (Association for International Affairs (AMO), 2022), https://www.amo.cz/wp-content/uploads/2022/09/HTDTR_report_how-to-do-trusted-research_A4_18_web.pdf.

10 E.g.: Ivana Karásková, *Vliv Číny v českém akademickém prostředí a jak se mu bránit* (Association for International Affairs (AMO), 2019), https://mapinfluence.eu/wp-content/uploads/2019/12/Vliv-Ciny-v-ceskem-akademickem-prostredi-a-jak-se-mu-branit.pdf; Ivana Karásková, "Countering China's Influence Campaigns at European Universities," *The Diplomat*, 22 February 2020, https://thediplomat.com/2020/02/countering-chinas-influence-campaigns-at-european-universities/.

11 "Opatření rektora č. 43/2021," Charles University, 15 November 2021, https://cuni.cz/UK-11424.html.

12 "Opatření rektora č. 6/2016," Charles University, 15 March 2016, https://cuni.cz/uk-7383.html.

13 Ibid.

14 Lukáš Valášek and Jan Horák, „Konference, které pořádá rektor UK Zima, platila skrytě statisíci čínská ambasáda," *Aktuálně,* 25 October 2019, https://zpravy.aktualne.cz/domaci/konferenci-uk-platila-cina- stredisko-bezpecnostni-politiky/r~79c2b80ef4b311e9858fac1f6b220ee8/.

15 Lukáš Valášek and Eliška Halaštová, „Čínská ambasáda tajně financovala i předmět na univerzitě o výhodách Hedvábné stezky," *Aktuálně*, 29 October 2019, https://zpravy.aktualne.cz/domaci/cinska-ambasada-tajne-poslala-penize-i-na-predmet-uk-o- vyhod/r~7fa1adb8f71311e9b1410cc47ab5f122/.

16 The programme Bridge for the Future remains relatively underreported, and the process by which participants are selected is not entirely transparent. The initiative is organised by the All-China Youth Federation (ACYF), an organisation operating under the Central Committee of the Chinese Communist Party (CCP). It pursues objectives aligned with those of the United Front Work Department (UFWD), a CCP body tasked with co-opting and neutralising both domestic and international sources of potential opposition to the Party.

17 Kathrin Hille and James Shotter: „Czech university mired in Chinese influence scandal," *Financial Times*, 11 November 2019, https://www.ft.com/content/ba8645ca-016c-11ea-b7bc-f3fa4e77dd47.

18 *Protivlivový manuál pro sektor vysokých škol* (Ministry of the Interior of the Czech Republic, Department of Security Policy, and Centre Against Hybrid Threats (CTHH), 2021), https://mv.gov.cz/chh/clanek/terorismus-web-aktuality-aktuality-protivlivovy-manual-pro-sektor-vysokych-skol.aspx.

19 "Opatření rektora č. 43/2021," Charles University, 15 November 2021, https://cuni.cz/UK-11424.html.

20 *Protivlivový manuál pro sektor vysokých škol* (Ministry of the Interior of the Czech Republic, Department of Security Policy, and Centre Against Hybrid Threats (CTHH), 2021), https://mv.gov.cz/chh/clanek/terorismus-web-aktuality-aktuality-protivlivovy-manual-pro-sektor-vysokych-skol.aspx.

21 An Article 108 of the strategy clearly states that "[the state] must also prevent the efforts of some state or non-state actors to acquire economic or technological advantage through illegitimate means or to directly harm private companies, academic and other scientific research institutions or directly, the interests of the Czech Republic. A key role in dealing with these threats is the proper institutional setting and staffing mechanisms to safeguard an open business and investment environment." See *Bezpečnostní strategie ČR* (Office of the Government of the Czech Republic, 2023), https://mocr.mo.gov.cz/images/id_40001_50000/46088/Bezpecnostni_strategie_Ceske_republiky_2023.pdf.

22 The group consists of representatives of the Ministry of Education, Youth and Sports; the Ministry of Interior; the Ministry of Industry and Trade; the National Cyber and Information Security Authority; the Financial Analysis Authority; the Council for Research, Development and Innovation and the Office of the Minister for Science, Research and Innovation. Representatives of the Academy of Sciences of the Czech Republic and universities participate in the meetings of the group as permanent guests.

23 *Posilování odolnosti vůči nelegitimnímu ovlivňování ve vysokoškolském a výzkumném prostředí* (Ministry of Education, Youth and Sports (MŠMT), 2024), https://msmt.gov.cz/uploads/O31/O311/Bezpecnost_vyzkumu_posilovani_odolnosti_vuci_nelegitimnimu_ovlivnovani/Posilovani_odolnosti_vuci_nelegitimnimu_ovlivnovani_ve_vysokoskolskem_a_vyzkumnem_prostredi.pdf; *Metodické doporučení k řízení rizik v oblasti bezpečnosti výzkumu na institucionální úrovni* (Ministry of Education, Youth and Sports (MŠMT), 2024), https://msmt.gov.cz/uploads/O31/O311/Bezpecnost_vyzkumu_posilovani_odolnosti_vuci_nelegitimnimu_ovlivnovani/Metodicke_doporuceni_k_rizeni_rizik_bezpecnosti_vyzkumu_na_institucionalni_urovni.pdf; *Metodické doporučení, kterým se efinuje minimální rozsah due dilligence a řízení rizik spolupráce s třetími stranami v rámci posilování odolnosti vysokoškolského a výzkumného prostředí vůči nelegitimnímu ovlivňování* (Ministry of Education, Youth and Sports (MŠMT), 2024), https://msmt.gov.cz/uploads/O31/O311/Bezpecnost_vyzkumu_posilovani_odolnosti_vuci_nelegitimnimu_ovlivnovani/Metodicke_doporuceni_due_diligence_a_rizeni_rizik_spoluprace.pdf.

24 Alžběta Bajerová, "The Czech-Chinese Centre of Influence: How Chinese Embassy in Prague Secretly Funded Activities at the Top Czech University," *China Observers in Central and Eastern Europe (CHOICE)*, 7 November 2019, https://chinaobservers.eu/the-czech-chinese-centre-of-influence-how-chinese-embassy-in-prague-secretly-funded-activities-at-the-top-czech-university/.

25 See Ministry of Education, Youth and Sports (MŠMT) website dedicated to research security: https://msmt.gov.cz/vyzkum-a-vyvoj-2/narodni-podpora-1.

26 Sam Dunning and Anson Kwong, *An Investigation of China's Confucius Institutes in the UK* (Henry Jackson Society, 2022), https://henryjacksonsociety.org/wp-content/uploads/2022/10/Confucius-Institutes-in-UK.pdf; Robert Clark, *The Strategic Dependence of UK Universities on China – and Where Should They Turn Next?* (Civitas, 2023), https://www.civitas.org.uk/content/files/The-Strategic-Dependence-of-UK-Universities-on-China-.pdf; Tau Yang, *The Hidden Role of the Chinese Communist Party in UK-China Joint Educational Institutes* (China Strategic Risks Institute, 2024), https://static1.squarespace.com/static/61d5a7bdbb804663a82e154a/t/66edb21174241201973b9778/1726853654513/CCP_Governance_in_JEI.pdf; Ingrid d'Hooghe and Xiaoxue Martin, *Dutch collaboration with PhD students sponsored by the China Scholarship Council* (Clingendael Institute, 2024), https://www.clingendael.org/sites/default/files/2024-03/Report%20Dutch_Collaboration_with_CSC_PhD_students.pdf.

27 "China's military is tapping into EU-funded research," *Politico*, 27 June 2024, https://www.politico.eu/article/eu-funds-research-that-involves-chinese-military-linked-universities/.

28 Matej Šimalčík and Adam Kalivoda, *China-Europe Academic Engagement Tracker* (Central European Institute of Asian Studies (CEIAS), 2022), https://academytracker.ceias.eu/map/eu/Czech%20Republic/Charles%20University%20(UK); Kahrin Hille and James Shotter, "Czech university mired in Chinese influence scandal," *Financial Times*, 11 November 2019, https://www.ft.com/content/ba8645ca-016c-11ea-b7bc-f3fa4e77dd47; Lukáš Valášek, "Akademici si "odkláněli" miliony, univerzita náhle couvá z vymáhání," *Seznam Zprávy*, 5 November 2023, https://www.seznamzpravy.cz/clanek/domaci-kauzy-karlova-univerzita-vycouvala-z-vymahani-milionu-po-akademicich-placenych-cinou-238657.

29 Matej Šimalčík and Adam Kalivoda, *China-Europe Academic Engagement Tracker* (Central European Institute of Asian Studies (CEIAS), 2022), https://academytracker.ceias.eu/map/eu/Czech%20Republic/Palacky%20University%20in%20Olomouc%20(UP); "Konfucius v Praze: Zdaž to není koneckonců radostné?," *Sinopsis*, 25 November 2019, https://sinopsis.cz/konfucius-v-praze-zdaz-to-neni-koneckoncu-radostne-2/.

30 Matej Šimalčík and Adam Kalivoda, *China-Europe Academic Engagement Tracker* (Central European Institute of Asian Studies (CEIAS), 2022), https://academytracker.ceias.eu/map/eu/Czech%20Republic/University%20of%20Pardubice%20(UPa); Artur Janoušek, "Český expert na výbušniny spolupracuje s čínskými specialisty na zbraně. Před 'verbováním' Pekingu varuje BIS," *iROZHLAS*, 16 March 2022, https://www.irozhlas.cz/zpravy-domov/profesor-svatopluk-zeman-vybusniny-spoluprace-cina-zbrane-univerzita-pardubice_2203160600_sam.

31 Ivana Karásková, Filip Šebok, and Veronika Blablová, *Čína jako riziko pro bezpečnost výzkumu: doporučení pro akademické a výzkumné instituce* (Asociace pro mezinárodní otázky (AMO), 2022), https://www.amo.cz/wp-content/uploads/2022/11/HTDTR_cina-jako-riziko-pro-bezpecnost-vyzkumu.pdf; "China-Europe Academic Engagement Tracker," Central European Institute of Asian Studies (CEIAS), https://academytracker.ceias.eu/map/eu/Czech%20Republic.

32 Ryan Fedasiuk, *The China Scholarship Council: An Overview* (Centre for Security and Emerging Technology (CSET), 2020), https://cset.georgetown.edu/publication/the-china-scholarship-council-an-overview/; Matej Šimalčík and Adam Kalivoda, *China-Europe Academic Engagement Tracker* (Central European Institute of Asian Studies (CEIAS), 2022), https://academytracker.ceias.eu/map/eu/Germany/Fraunhofer%20Society; Esther Felden, Sandra Petersmann, and Naomi Conrad, "Are European academics helping China's military?," *Deutsche Welle (DW)*, 19 May 2022, https://www.dw.com/en/are-european-academics-helping-chinas-military/a-61834716.

33 Matej Šimalčík and Adam Kalivoda, *China-Europe Academic Engagement Tracker* (Central European Institute of Asian Studies (CEIAS), 2022), https://academytracker.ceias.eu/map/eu/Germany/Max%20Planck%20Society; "Statement of the Max Planck Society regarding the China Science Investigation published in the Süddeutsche Zeitung on May 19, 2022," Max Planck Society, https://www.mpg.de/18707939/Statement-China-Science-Investigation-MPG.pdf.

34 Alex Joske, *The China Defence Universities Tracker* (Australian Strategic Policy Institute (ASPI), 2019), https://www.aspi.org.au/report/china-defence-universities-tracker; Matej Šimalčík and Adam Kalivoda, *China-Europe Academic Engagement Tracker* (Central European Institute of Asian Studies (CEIAS), 2022), https://academytracker.ceias.eu/map/eu/Germany/RWTH%20Aachen%20University; Till Eckert, Olaya Argüeso, Sophia Stahl, Benjamin Schubert and Mohamed Anwar, "Deutsche Hochschulen als Ziel der Chinesischen Militärmacht," *Correctiv*, 19 October 2022, https://correctiv.org/aktuelles/wirtschaft/2022/05/18/deutschland-hochschulen-kooperation-mit-china-militaer/; Till Eckert, "Die Bling-Bling-Professoren aus Aachen," *Correctiv*, 18 June 2024, https://correctiv.org/aktuelles/china-science-investigation/2024/06/18/die-bling-bling-professoren-aus-aachen/.

35 Matej Šimalčík and Adam Kalivoda, *China-Europe Academic Engagement Tracker* (Central European Institute of Asian Studies (CEIAS), 2022); Guy Chazan, "China blamed for cancellation of events for German book on Xi Jinping," *Financial Times*, 26 October 2021, https://www.ft.com/content/8e4af031-6d07-4b3b-816b-1fc9194b6e4a; Nadine Wojcik, "How does Germany deal with Chinese censorship?", *Deutsche Welle (DW)*, 29 October 2021, https://www.dw.com/en/germany-how-does-it-deal-with-chinese-censorship/a-59653971.

36 "Dutch University Hit by Chinese Government Funding Scandal," *Human Rights Watch*, 20 January 2022, https://www.hrw.org/news/2022/01/20/dutch-university-hit-chinese-government-funding-scandal; Lukas Kotkamp, "Dutch university scandal taps into fears of Chinese influence peddling," *Politico*, 24 January 2022, https://www.politico.eu/article/dutch-university-amsterdam-scandal-taps-china-influence/; Jon Henley, "Dutch university gives up Chinese funding due to impartiality concerns," *The Guardian*, 25 January 2022, https://www.theguardian.com/world/2022/jan/25/dutch-university-gives-up-chinese-funding-due-to-impartiality-concerns.

37 Ryan Fedasiuk, T*he China Scholarship Council: An Overview* (Center for Security and Emerging Technology (CSET), 2020), https://cset.georgetown.edu/publication/the-china-scholarship-council-an-overview/; Annebelle De Bruijn, Dorine Booij, Heleen Emanuel, Mira Sys and Siem Eikelenboom, "China Stuurt Gericht Tientallen Militaire Onderzoekers Naar Nederland Om Gevoelige Kennis Te Vergaren," *Follow the Money - Platform Voor Onderzoeksjournalistiek*, 7 June 2024, https://www.ftm.nl/artikelen/china-stuurt-militaire-onderzoekers-naar-nederlandse-universiteiten?share=YiGBygBDLDFUQgj7eK9By1n19X5Qr70922ySm%2Fy6JpzgckDnPqg2Fi3k1XwSUZc%3D; Annebelle De Bruijn, "How TU Delft unintentionally helps the Chinese army," Delta, 26 March 2021, https://delta.tudelft.nl/en/article/how-tu-delft-unintentionally-helps-chinese-army; "Chinese scientists at TU Delft use knowledge for national army," *Ad Valvas*, 30 March 2021, https://advalvas.vu.nl/en/science-education/chinese-scientists-tu-delft-use-knowledge-national-army/.

38 Annebelle De Bruijn, Dorine Booij, Heleen Emanuel, Mira Sys and Siem Eikelenboom, "China Stuurt Gericht Tientallen Militaire Onderzoekers Naar Nederland Om Gevoelige Kennis Te Vergaren," *Follow the Money - Platform Voor Onderzoeksjournalistiek*, 7 June 2024, https://www.ftm.nl/artikelen/china-stuurt-militaire-onderzoekers-naar-nederlandse-universiteiten?share=YiGBygBDLDFUQgj7eK9By1n19X5Qr70922ySm%2Fy6JpzgckDnPqg2Fi3k1XwSUZc%3D.

39 Annebelle De Bruijn, Dorine Booij, Heleen Emanuel, Mira Sys and Siem Eikelenboom, "China Stuurt Gericht Tientallen Militaire Onderzoekers Naar Nederland Om Gevoelige Kennis Te Vergaren," *Follow the Money - Platform Voor Onderzoeksjournalistiek*, 7 June 2024, https://www.ftm.nl/artikelen/china-stuurt-militaire-onderzoekers-naar-nederlandse-universiteiten?share=YiGBygBDLDFUQgj7eK9By1n19X5Qr70922ySm%2Fy6JpzgckDnPqg2Fi3k1XwSUZc%3D; "Current MOU and student/staff exchange agreements, Leiden University," Leiden University, https://www.staff.universiteitleiden.nl/binaries/content/assets/ul2staff/onderwijs/agreement-overview-14.4.17.pdf.

40 Alex Joske, *The China Defence Universities Tracker* (Australian Strategic Policy Institute (ASPI), 2019), https://www.aspi.org.au/report/china-defence-universities-tracker; "Imperial College London & the Chinese Military," UK-China Transparency, 16 June 2024, https://ukctransparency.org/wp-content/uploads/2024/06/Imperial-College-London-the-Chinese-military.pdf; Hannah Devlin, "Imperial College to shut joint research ventures with Chinese defence firms," *The Guardian*, 11 September 2022, https://www.theguardian.com/world/2022/sep/11/imperial-college-to-shut-joint-research-ventures-with-chinese-defence-firms; Lucy Fisher and Jamie John, "Imperial College London academics worked with Chinese military-linked institutions," *Financial Times*, 5 March 2024, https://www.ft.com/content/73e5ef6f-0e67-449f-a520-1f2df20276be; Hannah Devlin, "Chinese firm sought to use UK university links to access AI for possible military use," *The Guardian*, 16 June 2024, https://www.theguardian.com/education/article/2024/jun/16/chinese-firm-sought-to-use-uk-university-links-to-access-ai-for-possible-military-use.

41 Alex Joske, *The China Defence Universities Tracker* (Australian Strategic Policy Institute (ASPI), 2019), https://www.aspi.org.au/report/china-defence-universities-tracker; Hannah Devlin and Ian Sample, "UK academia's links to Chinese defence firms 'harmful for national security'," *The Guardian*, 25 November 2019, https://www.theguardian.com/education/2019/nov/25/uk-academias-links-to-chinese-defence-firms-harmful-for-national-security; "UK blocks University of Manchester sensor deal With Chinese company," *BBC News,* 23 July 2022, https://www.bbc.co.uk/news/technology-62243424.

42 "Cambridge University's collaboration with the Chinese military," UK-China Transparency, https://ukctransparency.org/wp-content/uploads/2023/09/REPORT-Cambridge-Universitys-collaboration-with-the-Chinese-military.pdf; Emma Yeomans, "Cambridge University to end partnership with Chinese missiles company," *The Times*, 4 September 2023, https://www.thetimes.com/business-money/technology/article/cambridge-university-to-end-partnership-with-chinese-missiles-company-fwshmm6mc.

43 "Research report on the Lau China Institute," UK-China Transparency, 29 July 2024, https://ukctransparency.org/wp-content/uploads/2024/07/Lau-China-Institute-REPORT-1.pdf; Fiona Hamilton, "King's College London donor linked to Communist Party of China," *The Times*, 29 July 2024, https://www.thetimes.com/uk/education/article/kings-college-london-donor-linked-to-communist-party-of-china-n7j2fsjvz; Lyndon Lee, "Critics question Beijing-friendly donor's ties to UK-China institute," *Voice of America*, 1 August 2024, https://www.voanews.com/a/critics-question-beijing-friendly-donor-s-ties-to-uk-china-institute/7725999.html.

44 Alex Joske, *The China Defence Universities Tracker* (Australian Strategic Policy Institute (ASPI), 2019), https://www.aspi.org.au/report/china-defence-universities-tracker; Patrik Sawer, "Former head of Chinese studies at Nottingham University 'censored by Chinese Communist Party'," *The Telegraph*, 28 November 2023, https://www.telegraph.co.uk/news/2023/11/28/academics-british-universities-censored-communist-party/; Amy Hawkins, "China influencing leading British universities, documentary claims," *The Guardian*, 28 November 2023, https://www.theguardian.com/education/2023/nov/28/china-influencing-leading-british-universities-documentary-claims.

45 "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Global Approach to Research and Innovation, Europe's strategy for international cooperation in a changing world," European Commission, COM (2021) 252 final, 18 May 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021DC0252; OECD, "Integrity and Security in the global research ecosystem," OECD Science, Technology and Industry Policy Papers, June 2022, https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/06/integrity-and-security-in-the-global-research-ecosystem_2bd8511d/1c416f43-en.pdf.

46 "G7 Common Values and Principles on Research Security and Research Integrity," Government of Canada, June 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; "G7 Best Practices for Secure and Open Research," Government of Canada, 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.

47 See G7 Virtual Academy: Research Security & Integrity website: https://europa.eu/sinapse/sinapse/community/0505f60a-287b-11ed-b6d0-0050568bf5be/login.

48 Alex Joske, *The China Defence Universities Tracker* (Australian Strategic Policy Institute (ASPI), 2019), https://www.aspi.org.au/report/china-defence-universities-tracker.

49 Hannah Devlin, "Imperial College to shut joint research ventures with Chinese defence firms," *The Guardian*, 11 September 2022, https://www.theguardian.com/world/2022/sep/11/imperial-college-to-shut-joint-research-ventures-with-chinese-defence-firms.

50 "Imperial College London & the Chinese Military," UK-China Transparency, 16 June 2024, https://ukctransparency.org/wp-content/uploads/2024/06/Imperial-College-London-the-Chinese-military.pdf.

51 "Relationships Policy," Imperial College London, 12 July 2024, https://www.imperial.ac.uk/media/imperial-college/administration-and-support-services/secretariat/public/about-the-secretariat/what-we-do/ethics/Relationships-Policy-2024.pdf.

52 https://www.ft.com/content/73e5ef6f-0e67-449f-a520-1f2df20276be Lucy Fisher and Jamie John, "Imperial College London academics worked with Chinese military-linked institutions," *Financial Times*, 5 March 2024, https://www.ft.com/content/73e5ef6f-0e67-449f-a520-1f2df20276be

53 See Government of the Netherlands Contact Point for Knowledge Security website: https://english.loketkennisveiligheid.nl.

54 Laura Steenbeeke and Robert Chesal, „China financiert onderzoek naar mensenrechten aan VU," *NOS*, 19 January 2022, https://nos.nl/artikel/2413702-china-financiert-onderzoek-naar-mensenrechten-aan-vu.

55 Yojana Sharma, „University funding row raises Chinese influence fears," University World News, 26 January 2022, https://www.universityworldnews.com/post.php?story=20220126093628860.

56 Ibid.

57 The Cross Cultural Human Rights Centre (CCHRC), the centre of VU Amsterdam that conducted research on human rights, will be disbanded," VU Amsterdam, 11 July 2022, https://vu.nl/en/news/2022/vu-closes-human-rights-centre-after-external-investigation.

58 Till Eckert, "Die Bling-Bling-Professoren aus Aachen," *Correctiv*, 18 June 2024, https://correctiv.org/aktuelles/china-science-investigation/2024/06/18/die-bling-bling-professoren-aus-aachen/.

59 Matej Šimalčík and Adam Kalivoda, *China-Europe Academic Engagement Tracker* (Central European Institute of Asian Studies (CEIAS), 2022), https://academytracker.ceias.eu/map/eu/Germany/RWTH%20Aachen%20University/Northwestern%20Polytechnical%20University.

60 See RWTH Aachen website dedicated to strategic partnerships: https://www.rwth-aachen.de/go/id/dwrq/lidx/1.

61 Alex Joske, *The China Defence Universities Tracker* (Australian Strategic Policy Institute (ASPI), 2019), https://www.aspi.org.au/report/china-defence-universities-tracker.

62 Kai Gehring, "Pressestatement von Kai Gehring zur Correctiv Recherche zur RWTH Aachen," 24 June 2024, https://www.kai-gehring.de/pressestatement-von-kai-gehring-zur-correctiv-recherche-zur-rwth-aachen/.

63 "Position der RWTH Aachen zur aktuellen Berichterstattung," RWTH Aachen Univerisity, 19 June 2024, https://www.rwth-aachen.de/cms/root/Die-RWTH/Aktuell/Pressemitteilungen/Juni-2024/~bieuwx/Position-der-RWTH-zur-CORRECTIV-Berichte/.

64 *Protivlivový manuál pro sektor vysokých škol* (Ministry of the Interior of the Czech Republic, Department of Security Policy, and Centre Against Hybrid Threats (CTHH), 2021), https://cuni.cz/UK-11805-version1-protivlivovy_manual_pro_sektor_vysokych_skol___20210622.pdf.

65 *Handbook: Technical Assistance and Intangible Transfer of Technology: What? Where? Why? For universities, scientific institutes, research institutes and the general public* (Financial Analytical Office, 2021), https://fau.gov.cz/files/prirucka-technicke-pomoci-a-nehmotneho-prenosu-technologii-en.pdf.

66 *Metodické doporučení, kterým se definuje minimální rozsah due diligence a řízení rizik spolupráce s třetími stranami v rámci posilování odolnosti vysokoškolského a výzkumného prostředí vůči nelegitimnímu ovlivňování (Metodické doporučení ke spolupráci s třetími stranami)* (Ministry of Education, Youth and Sports (MŠMT), 2024), https://msmt.gov.cz/uploads/O31/O311/Bezpecnost_vyzkumu_posilovani_odolnosti_vuci_nelegitimnimu_ovlivnovani/Metodicke_doporuceni_due_diligence_a_rizeni_rizik_spoluprace.pdf; *Metodické doporučení k řízení rizik v oblasti bezpečnosti výzkumu na institucionální úrovni* (Ministry of Education, Youth and Sports (MŠMT), 2024), https://msmt.gov.cz/uploads/O31/O311/Bezpecnost_vyzkumu_posilovani_odolnosti_vuci_nelegitimnimu_ovlivnovani/Metodicke_doporuceni_k_rizeni_rizik_bezpecnosti_vyzkumu_na_institucionalni_urovni.pdf; *Posilování odolnosti vůči nelegitimnímu ovlivňování ve vysokoškolském a výzkumném prostředí* (Ministry of Education, Youth and Sports (MŠMT), 2024), https://msmt.gov.cz/uploads/O31/O311/Bezpecnost_vyzkumu_posilovani_odolnosti_vuci_nelegitimnimu_ovlivnovani/Posilovani_odolnosti_vuci_nelegitimnimu_ovlivnovani_ve_vysokoskolskem_a_vyzkumnem_prostredi.pdf.

67 *Keine roten Linien: Wissenschaftskooperationen unter komplexen Rahmenbedingungen* (German Academic Exchange Service (DAAD), 2020), https://static.daad.de/media/daad_de/pdfs_nicht_barrierefrei/infos-services-fuer-hochschulen/kompetenzzentrum/dokumente/daad_kiwi_kompass_keinerotenlinien_2020.pdf.

68 *Resolution of the 690th Executive Board of the HRK on 9 September 2020: Guiding questions on university cooperation with the People's Republic of China* (German Rectors' Conference (HRK), 2020), https://www.hrk.de/fileadmin/redaktion/hrk/02-Dokumente/02-01-Beschluesse/HRK_Resolution_Guiding_question_on_university_cooperation_with_the_PR_China_9.9.2020.pdf.

69 *Report on Research, Innovation and Technological Performance in Germany* (Commission of Experts for Research and Innovation (EFI), 2020), https://www.e-fi.de/fileadmin/Assets/Gutachten/EFI_Report_2020.pdf.

70 *Manual: Export Control and Academia* (Federal Office for Economic Affairs and Export Control (BAFA), 2023), https://www.bafa.de/SharedDocs/Downloads/EN/Foreign_Trade/ec_manual_export_control_and_academia.html?nn=1444524.

71 *Due Diligence in Science: Handreichung für einen Prüfprozess zum Wissenschafts- und Kooperationsschutz in der internationalen Zusammenarbeit von Hochschulen und Forschungseinrichtungen* (German Aerospace Centre (DLR) – DLR Projektträger, 2024), https://www.safeguarding-science.eu/wp-content/uploads/Due-Diligence-in-Science_German-Handreichung2024.pdf.

72 *National knowledge security guidelines: Secure international collaboration* (National Contact Point for Knowledge Security, 2022), https://english.loketkennisveiligheid.nl/documents/2022/04/07/national-knowledge-security-guidelines.

73 *Capability Maturity Model: Knowledge Security* (Universities of the Netherlands (UNL), 2024), https://www.universiteitenvannederland.nl/files/publications/UNL%20Capability%20Maturity%20Model%20Knowledge%20Security%20ENG-DEF.pdf.

74 *Academic Technology Approval Scheme* (ATAS) (Foreign, Commonwealth & Development Office (FCDO), 2013, updated 2025), https://www.gov.uk/guidance/academic-technology-approval-scheme

75 *Managing Risks in Internationalisation: Security Related Issues* (Universities UK (UUK), 2020), https://www.universitiesuk.ac.uk/sites/default/files/uploads/Reports/managing-risks-in-internationalisation.pdf.

76 *Guidance: Export controls applying to academic research* (Export Control Joint Unit (ECJU), Department for International Trade, and Department for Business and Trade, 2021, updated 2024), https://www.gov.uk/guidance/export-controls-applying-to-academic-research.

77 *National Security and Investment Act: guidance for the higher education and research-intensive sectors (NSI Act)* (Cabinet Office, 2021, updated 2024), https://www.gov.uk/government/publications/national-security-and-investment-act-guidance-for-the-higher-education-and-research-intensive-sectors/national-security-and-investment-act-guidance-for-the-higher-education-and-research-intensive-sectors.

78 *Trusted Research and Innovation Principles* (UK Research and Innovation (UKRI), 2021), https://www.ukri.org/wp-content/uploads/2021/08/UKRI-170821-TrustedResearchandInnovationPrinciples.pdf.

79 *Trusted Research Guidance for Academics* (National Protective Security Authority (NPSA), 2024), https://www.npsa.gov.uk/system/files/trusted-research-guidance-for-academia-digital-july24.pdf.