How National Governments and Research Institutions Safeguard Knowledge Development in Science and Technology

LEIDEN ASIA CENTRE
Partners in Research and Knowledge

Awti Adviesraad voor wetenschap, technologie en innovatie

Ingrid d'Hooghe
Jonas Lammertink

November, 2022

The LeidenAsiaCentre is an independent research centre affiliated with Leiden University and made possible by a grant from the Vaes Elias Fund. The centre focuses on academic research with direct application to society. All research projects are conducted in close cooperation with a wide variety of partners from Dutch society.

More information can be found on our website:

www.leidenasiacentre.nl

For contact or orders: info@leidenasiacentre.nl

M. de Vrieshof 3, 2311 BZ Leiden, The Netherlands

LEIDEN ASIA CENTRE
Partners in Research and Knowledge

Awti Adviesraad voor wetenschap, technologie en innovatie

SUMMARY

EXECUTIVE SUMMARY

This study provides an overview and comparative analysis of nine national approaches to strengthening knowledge security and the forces that drive them. The national approaches are those of Australia, Czech Republic, Finland, France, Germany, Japan, Taiwan, the United Kingdom and the United States. They all have developed different approaches, depending on the national political context, geographical location, experiences with foreign interference and the level of internationalization of the higher education and research sector. The approaches vary in comprehensiveness, practicality, and the roles played by government actors and representatives of the higher education and research sector.

The study finds that coherence and practicality of measures, good coordination between the stakeholders involved, and government support for bottom-up activities by universities, are among the major factors that impact the effectiveness of an approach. The report concludes with best practices that the case studies offer; they include the promotion of international collaboration and coordination with regard to developing standards for research security, an approach that avoids securitization of international research collaboration, and the establishment of organizations that facilitate direct communication and coordination between the government and the higher education sector.

1 3 5 7 9
CONTENTS

CONTENTS

INTRODUCTION

An open academic environment and unrestricted international collaboration are regarded as essential to the advancement of science. At the same time, geopolitical developments and an unprecedented acceleration in the speed and scale of technological advances pose new and increased risks and challenges to the practice of science, technology and innovation (STI). These developments are sometimes at odds with national security, in particular where international collaboration in STI is concerned. Many countries feel the need to defend their science and technology from foreign interference and concrete risks of unwanted transfer of knowledge and technology, breaches of academic freedom, and unethical use of research, for example for certain military or political monitoring purposes. As a result, they are developing approaches to deal with these issues.

This study aims to provide a systematic overview and comparative analysis of nine national approaches to knowledge security and the forces that drive them. It is commissioned by the Dutch Advisory Council for Science, Technology and Innovation (AWTI) and serves as input for a broader AWTI study that will provide policy advice to the Dutch government. The main research question this study addresses is: How do national governments and research institutions safeguard knowledge development in science and technology in the light of the new or increased risks due to geopolitical and international developments?

The aim is to deepen understanding on approaches to knowledge security, foreign interference and safeguarding academic freedom and on the explicit or implicit rationales for the identified measures. In addition, we aim to identify best practices that may provide inspiration to policy makers and the research sector across the globe, including for the Netherlands. The selected cases concern: Australia, Czech Republic, Finland, France, Germany, Japan, Taiwan, United Kingdom and the United States. They have been selected after a quick scan of 13 countries. The selection of the nine cases was based on the criteria of existence of a national approach, accessibility to materials and resource persons, and the aim to provide geographical variety as well as a variety of approaches to safeguarding knowledge development in STI.

FRAMEWORK METHODOLOGY

FRAMEWORK AND METHODOLOGY

Conceptualization

The central concept upon which the framework for this study is built is 'knowledge security' as it is understood in the National Knowledge Security Guidelines of the Dutch government. In the Netherlands, knowledge security is generally defined as a broad concept that is "first and foremost about the undesirable transfer of sensitive knowledge and technology" but also entails "the covert influencing of education and research by state actors", which may place academic freedom and social safety in jeopardy, and "ethical issues that can be at play in collaboration with countries that do not respect fundamental rights". Ethical Practices in international collaboration concern two areas: application of ethical research methods and prevention of "ethics dumping" in foreign countries with less strict governance of research ethics; and the ethical use of knowledge, e.g. avoiding the use of research results to violate human rights (National Knowledge Security Guidelines 2022).

Our understanding of *academic freedom* is based on a conceptualization by the European Commission (Tackling R&I Foreign Interference 2022): the freedom of academic staff and students to engage in research, teaching, learning and communication in and with society without interference nor fear of reprisal. Freedom of academic research encompasses:

- right to freely define research questions, choose and develop theories, gather empirical material and employ academic research methods, to question accepted wisdom and bring forward new ideas.
- right to share, disseminate and publish the results thereof, including through training and teaching.
- the freedom of researchers to express their opinion without being disadvantaged by the institution or system in which they work or by governmental or institutional censorship.
- pursue curiosity, creativity and critical spirit in all these areas, in order to build a comprehensive knowledge base and provide students with broad training.

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

Framework for analysis and comparison

The approaches studied for this report vary greatly in both form and content. For example, the measures that governments take range from roundtable working groups, to guidelines, to legally binding regulations. Some of these measures are developed by (associations of) knowledge institutions, others by government or semi-government agencies. In order to analyze and compare the variety of approaches to knowledge security that are developed in the countries that serve as case studies for this report, the approaches need to be unpacked in a structured way. This will be done in two steps.

Step one consists of mapping the concrete actions and processes aimed at strengthening knowledge security that are developed in each of the case countries. After identifying the actions and processes of the approaches, we proceed to step two: ana-

lyzing how these findings affect issues such as the nature and effectiveness of an approach.

Preceding these two steps is a brief section on the national context of each case study. The approaches to safeguarding knowledge security are not developed in a vacuum; they take shape within a specific political environment and governance structure (e.g. Germany where the federal government has no competency with regard to education). Furthermore, they are impacted by a country's or region's (geo-) political outlook and foreign relations, experiences of foreign interference, public debates, and by its research environment. This background information is important to understand the rationale, content, and effectiveness of an approach.

Step one: Mapping

The most important measures, special bodies and other initiatives that the case countries are developing in word and/or deed are displayed in tables. For initiatives that are particularly relevant or noteworthy, we discuss the following aspects in more detail:

a. Format(s): refers to the format of measures and actions that are taken as part of the national approach. These measures can come in the form of formal guidelines, special government agencies, working groups, websites, laws, etc.
b. Actors: refers to the actors involved in a particular initiative at all points of the process: the initiation, development, and implementation phases. The actors involved may affect the form and content of an approach, the level of acceptance among stakeholders, and the way measures are implemented.
c. Practical topics covered: refers to the topics at micro level that need to be addressed when developing knowledge security approaches such as dual use, student exchanges, cyber security, research partnerships, governance structures within research institutes, and the issue of responsibility etc.

Step two: Analysis

The framework for analysis consists of those elements and aspects of the approaches that go beyond a description of what is happening on the ground: they call for interpretation of, and making cross connections between, the information mapped in step one. The aspects are:

d. Character and comprehensiveness of approaches. The comprehensiveness of an approach is assessed on the basis of attention for A. the four steps for safeguarding knowledge security, which we define as: (1) Raising awareness (2) Identifying risks (3) Mitigating risks (4) Identifying opportunities (based on previous LeidenAsiaCentre research); and B. the three macro elements of knowledge security as defined above: preventing undesirable knowledge transfer, protecting academic freedom, and ensuring ethical practices.
e. Level of practicality and elaboration. This aspect concerns the extent to which an approach moves beyond abstract discussions and offers detailed and concrete tools that facilitate implementation in daily practice. It deals with questions such as: are definitions and responsibilities clearly formulated? Are measures supported by government agencies? Are guiding materials and/or best practices provided?
f. Coherence of measures. An approach will be assessed as being coherent when measures and regulations are linking to, and supporting each other. It also points

to coordination between actors involved in implementing and developing measures.

g. Implementation and enforcement. The mapping process identifies the formats, the actors involved, and the level of enforcement of the most relevant measures within a national approach. Based on the relations between these aspects and - if available - evaluations, the extent to which implementation is promoted, facilitated and realized will be assessed. Enforcement level refers to the extent to which a measure/initiative is enforced by legal or other means. The level of enforcement can affect the acceptance, effectiveness and practicality of an approach.
h. Effectiveness. The extent to which an approach contributes to the strengthening of knowledge security, such as developing risks analyses and addressing cyber security issues. This will be based on factual data and on the assessment of those involved in the respective approaches. For example, on evaluations organized by responsible authorities.

Many of these factors are interconnected, e.g. the national context will likely impact the character of an approach, and there will be a connection between the coherence and practicality of an approach and its effectiveness. Where significant and relevant, these interconnections will be analyzed and discussed.

Methodology

The research for this study consists of a combination of desk research of primary and secondary sources, and interviews. The focus is on desk research; a limited number of online interviews, conversations or written exchanges have provided complimentary information and insight. They involve 14 researchers, 15 policy makers in the area of knowledge security, and 5 Dutch officials stationed abroad. Furthermore, two international seminars on knowledge security provided information. Primary sources include policy documents, regulations, letters to parliaments, speeches and statements. Secondary sources include academic literature, research reports, and media reports.

Limitations

The report is limited in scope. It is based on desk research with limited time for interviews. In some cases, access to information and resource persons willing to share insights proved challenging (e.g. France and the Czech Republic), in other cases language issues complicated desk research (e.g. Finland, Japan, and the Czech Republic). Furthermore, the study focuses on measures and regulations aimed specifically at universities and public research institutions. This means that this study does not deal with measures aimed at corporate R&D, or policies regarding export controls, sanctions, and cyber security, since these target multiple sectors. As a result of these limitations, the researchers can only draw cautious and general conclusions.

1. AUSTRALIA

1. National context

Australia's approach to knowledge security is shaped by various factors. An important factor is the concern regarding Chinese influence and interference in Australia's society and the higher education sector, where tuition paying Chinese students provide considerable income for universities (Financial Review 2020). Reports of CCP-linked financial donations to pro-Beijing politicians and researchers in Australia resulted in widely publicized controversies (CSIS 2020). Incidents of Chinese students fiercely defending Beijing's policies at Australian campuses drew further attention to Chinese influence in the higher education sector (ABC 2019). Concerns were amplified by a Human Rights Watch report on Chinese surveillance and intimidation of students at Australian universities (HRW 2021) and reports on the undisclosed cooperation of China's military and security agencies with Western and Chinese universities, raising questions about unwanted sensitive knowledge transfers to China. (ASPI 2018; 2019; 2020).

A second factor are the military and security concerns regarding China, which have grown since Australia's opposition to Chinese claims in the South China Sea and China's success in strengthening military ties in the South Pacific. Economic and technological security considerations have resulted in stronger scrutiny of foreign takeovers and the removal of Chinese companies from 5G infrastructure. Cyber-attacks on Australian universities drew further attention to such security issues.

These factors contributed to deteriorating Sino-Australian relations, a highly politicized debate surrounding the topic of knowledge security and the development of an extensive national approach to counter the risks. A Parliamentary Inquiry, published in March 2022, investigated the awareness of the HE sector regarding national security risks and the effectiveness of government policies. The report contains 27 recommendations for the HE sector and government agencies to strengthen their knowledge security (Parliamentary Joint Committee on Intelligence and Security 2022). Many other important initiatives are discussed below under "mapping".

Under the current Australian government, efforts are taken to normalize the bilateral relationship. Nonetheless, the efforts to counter foreign interference continue. More recently, there are calls to counterbalance the attention for security risks with efforts to build resilience and seek investment in research. The latter is a challenge due to the fact that investments in research in Australia are below the OECD average, making universities more dependent on foreign resources (Interview AU1 and OECD 2022).

In the Australian approach, "foreign interference" is generally understood as the common denominator of all knowledge security risks, whether they relate to undesired knowledge transfers or academic freedom.

2. Mapping

Major knowledge security initiatives and measures in Australia

Format(s)	Initiative	Actors
Guidelines and recommendations	Guidelines to counter foreign interference in the Australian university sector with Online Guidance Material	UFIT; Department of Education, Skills and Employment; Universities Australia; Group of Eight Australia
	International collaboration advice	Department of Industry, Science and Resources
	Inquiry into national security risks affecting the Australian higher education and research sector	Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia
	Model Code for the Protection of Freedom of Speech and Academic Freedom in Australian Higher Education Providers	Department of Education
Laws and regulations	Foreign Influence Transparency Scheme	Attorney-General's Department
	Foreign Arrangements Scheme	Department of Foreign Affairs and Trade
	National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018	Department of Home Affairs

Major actors in knowledge security in Australia

Actors	Actions
University Foreign Interference Taskforce (UFIT) Steering Group and Working Groups	Developing and updating Guidelines and Guidance Materials; Awareness raising
National Counter Foreign Interference Coordinator, Department of Home Affairs	Briefing university senior executives on threats and national security policy; Engage with universities to increase understanding of the foreign interference threat, and ways to respond to those risks
Australian Security Intelligence Organisation (ASIO)	Briefing university senior executives on threats and national security policy; Engage with universities to increase understanding of the foreign interference threat, and ways to respond to those risks
Critical Technologies Policy Coordination Office (CTPCO)	Providing: advice on technology developments, risks and opportunities, updates to the sector on critical technologies of national interest to Australia, and recommends actions to promote and protect critical technologies

The Guidelines to Counter Foreign Interference in the Australian University Sector

These comprehensive country neutral Guidelines are developed by the University Foreign Interference Taskforce (UFIT) (see below) and are supported by a website with guidance materials. They were first launched in 2019 and revised and updated in 2021. The first version was relatively general and intended to raise awareness and get the whole sector on board. The current updated version provides clearer instructions on implementation and devotes more attention to on-campus freedom of expression and safety of students (Interview AU1; Interview AU2). The Guidelines make recommendations regarding (1) governance and risk frameworks, (2) communication, education and knowledge sharing, (3) due diligence, risk assessments and management, and (4) cyber security. The online guidance offers supporting material, such as case studies and templates. The Guidelines were designed in part to convince the government that the sector can create the necessary tools themselves, instead of depending solely on an approach of legislation imposed from above (Interview AU2).

Foreign Influence Transparency Scheme

This scheme came into effect in 2018 and is based on the Foreign Influence Transparency Scheme Act 2018, which was modeled after a similar act in the United States (Draffen and NG 2020). Its purpose is to provide "the public and government decision-makers with visibility of the nature, level and extent of foreign influence on Australia's government and political process" (Foreign Influence Transparency Scheme). Under the scheme, actors that undertake certain activities (e.g. political lobbying) on behalf of, or enter into an arrangement with, a foreign principal (e.g. a foreign government official) can face registration obligations in a public register. This also applies to the academic sector. Failing to comply with obligations under the scheme is a criminal offense. The Attorney-General's Department's website offers online supporting material and instructions to assist those who might have registration obligations. This includes factsheets, a compliance strategy and contact details.

Foreign Arrangements Scheme

This scheme commenced in 2020 with the purpose of ensuring that arrangements of local governments and their organizations (including public universities) with foreign entities do not undermine Australia's foreign policies. Under the scheme, universities need to notify or seek approval from the Minister of Foreign Affairs and Trade when they want to enter an arrangement with a foreign entity without institutional autonomy (Department of Foreign Affairs and Trade 2021). It is then up to the Minister to decide whether or not the arrangement would harm Australia's foreign relations, or be inconsistent with its foreign policy (Department of Foreign Affairs and Trade). The arrangement and the decision of the Minister are recorded in a public register. The Department of Foreign Affairs and Trade offers support materials on a special website about the scheme.

Some stakeholders find it hard to understand why this scheme also applies to the HE sector. They regard the scheme as the outcome of a political conflict between different levels of government, after an incident with a local government that signed an agreement with China without the support of the central authorities. These stakeholders call it a bureaucratic nightmare and find it a disappointing measure (Interview AU2).

University Foreign Interference Taskforce (UFIT)

The University Foreign Interference Taskforce (UFIT), founded in 2019 with the aim of developing the Guidelines, consists of representatives of the HE sector and government agencies, with both sides equally represented. UFIT's purpose is to "enhance safeguards against the risk of foreign interference" (UFIT 2021). As with its Guidelines, UFIT was designed to promote self-regulation of the sector as an alternative to imposed legislation from above. According to one interlocutor, without the existence of UFIT, there might have been more foreign interference legislation targeting universities (Interview AU1). UFIT's aim is to facilitate information sharing and creating understanding between government agencies and universities. It was also founded specifically so that security services have an appropriate platform to share confidential information about potential risks with higher education institutions (HEIs). The founding of UFIT was more driven by the security departments than the educational departments (Interview AU2).

UFIT is headed by a Steering Group of fourteen members, seven of which are drawn from the following government agencies: Attorney-General's Department, Australian Secret Intelligence Organisation (ASIO), Australian Cyber Security Centre, Department of Defence, Department of Education, Department of Foreign Affairs and Trade, Department of Home Affairs. The other seven are representatives of the HE sector from the highest (university president) level. The Steering Group is supported by several working groups that are formed around specific topics. These working groups consist of experts with knowledge on the subject and provide input to the Steering Group. The working groups are not permanent and are founded whenever more expertise is required about a certain topic (Interview AU2).

3. Analysis

The Australian approach is relatively comprehensive and addresses three of the four steps for safeguarding knowledge security that we have identified in our framework. The approach includes many efforts to raise awareness and to identify and mitigate risks. The Guidelines, for example, strongly emphasize that universities should offer programs to raise awareness and mechanisms for staff and students to report concerns of foreign interference. Similarly, the Guidelines and the many regulations and transparency schemes offer tools to identify and mitigate risks. However, the Australian approach offers relatively little when it comes to identifying opportunities for safe cooperation.

The Australian approach focuses on preventing undesirable knowledge transfers and protecting academic freedom. This is understandable, considering the high-profile incidents of foreign interference in Australian politics and academia, and the concerns over technology falling in the hands of foreign armies. While most initiatives focus on one of the two elements, the UFIT Guidelines bring both together and address them as one. With regard to undesirable knowledge transfers, the focus has shifted from analyzing dual-use risks (which is very difficult to determine) to risks stemming from relationships (e.g. between an institute and a foreign army) (Interview AU1). Relatively little attention is devoted ensuring ethical research practices.

On paper, there appears to be a high level of coherence between the different initiatives, as many policies and measures consistently refer to one another. Especially the Guidelines and its guidance material are noteworthy in that regard, offering links to many different government agencies, policy documents and regulatory frameworks. In practice, the coordination and communication between government departments and agencies is sometimes insufficient, as interlocutors and the parliamentary in-

quiry indicate, resulting in a lack of coherence between measures (Interview AU2). One group of universities even stated: "We need a stop to the endless production of piecemeal laws with little or no reference to each other or to the powers needed to achieve the outcomes required" (Parliamentary Joint Committee on Intelligence and Security 2022). One interlocutor also indicated that universities have to analyze potential partners based on available open source information, and would like to see more coordination and information sharing with the government in this regard (Interview AU1).

The Australian approach is a mix of legally binding regulations and non-mandatory guidance. For example, the Guidelines state they intend to offer "support" and "advice", while universities "are encouraged to consider the Guidelines". This, combined with the emphasis on institutional autonomy and proportionality, suggests a relatively flexible and moderate level of enforcement. The Guidelines do mention that the government may "seek assurance from universities that their approach to counter foreign interference aligns with these Guidelines", but so far this has been a voluntary mechanism where universities assure the government that they implement the Guidelines (Interview AU1). The online guidance material is even less stringent in tone, being "advisory only" (Department of Education 2022). Nonetheless, although the guidelines themselves are not enforced as such, the official university accreditor does currently also audit institutions on their foreign interference and cyber security policies (Interview AU1).

The Guidelines are relatively elaborate, concrete and practical. They contain clear definitions, while every recommendation is unpacked and made concrete. The online guidance material offers explanatory case studies and guiding questions, as well as links to government agencies and regulations. Furthermore, the Guidelines make suggestions for assigning responsibilities within an institution. This practical character stimulates the implementation of measures. However, practitioners also indicate that the Guidelines are insufficiently attuned to the specific needs of individual universities, who are sometimes uncertain whether they are applying the Guidelines too strictly or too leniently. Therefore, some would like to receive clearer instructions on implementation (Interview AU1). Coordination on the implementation of the Guidelines between universities is relatively informal, possibly because Australian universities use security as a competitive advantage and are therefore unwilling to share details on their security policies with their peers. There are only incidental and anecdotal discussions between universities (Interview AU1).

The parliamentary inquiry finds that UFIT and its Guidelines have been effective in improving awareness and implementing measures to counter knowledge security risks at many universities, although the level of awareness varies within the sector. Universities have also been very positive about UFIT, praising it as Australia's most successful initiative in countering foreign interference while respecting institutional autonomy. Sector representatives recommended that UFIT should "be the primary mechanism to improve the sector's defenses against national security risks". The enthusiasm stems from the successful cooperation between government and universities, by expanding information networks of and bringing in government security and intelligence professionals. The sector called for an even deeper engagement with the government within the UFIT framework (Parliamentary Joint Committee on Intelligence and Security 2022).

2. CZECH REPUBLIC

1. National context

The Czech Republic's national approach to knowledge security is shaped by interactions with Russian and Chinese actors. Relations with both countries are complicated because of the diverging views within Czech's government on how the Czech Republic should position itself. There is less political consensus on this issue compared to other countries in this study. Any position taken by the government is contested both internally and externally (Interview CZ2). President Zeman is especially outspoken in this regard, maintaining very friendly relations with Beijing and, until recently, Putin, much to the dismay of others in power.

Concerns about Russian interference in the Czech Republic have increased since the annexation of Crimea in 2014, resulting in various countermeasures, which also impact the area of knowledge security. Cyber-attacks that have been linked to Russia have prompted the drafting of a national cyber security strategy. The latest version (2021) points out that foreign state actors are increasingly interested in targeting entities with unique knowledge, including academic and research institutions, and that there is an increased risk of industrial espionage in academia and research (NUKIB 2021). However, the strategy does not further address the issue of knowledge security of HEIs specifically.

Another way in which Russia has shaped the Czech approach to knowledge security is through its hybrid warfare activities. In January 2017, the Centre Against Hybrid Threats (until July 2022 the Centre Against Terrorism and Hybrid Threats) was set up by the Ministry of the Interior to prevent Russian disinformation campaigns to interfere in the general elections later that year (Guardian 2016). The Centre disseminates information, raises awareness and proposes substantive and legislative solutions to counter hybrid threats. It drafted the Counter Foreign Interference Manual for the Czech Academic Sector in 2021 (discussed under Mapping). What's more, hybrid threats from Russia also resulted in the drafting of a National Strategy for Countering Hybrid Interference in 2021 (Ministry of Defence 2021). This document does, however, not address the issue of scientific knowledge security specifically.

While interactions with Russia resulted in strategies on cyber security and hybrid threats, interactions with China specifically resulted in strategies to counter interference in the HE sector. Relations with China have been highly politicized for a number of years, also affecting the sphere of knowledge cooperation. Various universities experienced incidents of Chinese interference, such as the censoring of topics in educational programs. In 2019, the Czech-Chinese Centre at Prague's Charles University was closed after it was found that the university received secret payments from the Chinese embassy (LeidenAsiaCentre 2020). The centre was founded around 2014/2015, at a time when the government still very much promoted cooperation with China (Interview CZ1). In response to this incident, Charles University requested assistance from the Centre Against Hybrid Threats to increase its resilience against foreign interference, which resulted in the Counter Foreign Interference Manual for the Czech Academic Sector in 2022.

2. Mapping

Major knowledge security initiatives and measures in the Czech Republic

Format(s)	Initiative	Actors
Guidelines and recommendations	Counter Foreign Interference Manual for the Czech Academic Sector	Centre Against Hybrid Threats
	Handbook Technical Assistance and Intangible Transfer of Technology	Financial Analytical Office
Policies	National Cyber Security Strategy of the Czech Republic for the period from 2021 to 2025	National Security Authority
	National Strategy for countering Hybrid Interference	Ministry of Defence & Armed Forces

Major actors in knowledge security in the Czech Republic

Actors	Actions
Centre Against Hybrid Threats	Combating hybrid threats as part of Czech's internal security
Financial Analytical Office	Source of information on sanctioned entities and application of sanctions
Coordinator of the Agenda of Countering Hybrid Interference within the National Security Council	The coordination of information exchange and the planning policies for countering hybrid threats

Counter Foreign Interference Manual for the Czech Academic Sector

This manual was published by the Centre Against Hybrid Threats (see below) at the request of Prague's Charles University, which had asked the Centre for "methodical help with resilience-building measures against foreign interference at the institutional level" (MVCR 2022). In response, the Centre published this country-neutral "general methodical document". The Manual is based on similar documents published on this topic by the EU and the governments of the US, UK, Germany and Australia, as well as a number of non-Czech universities. The "findings and recommendations of these documents were adapted to the Czech environment" (MVCR 2022). The Manual was originally published in 2021 in Czech. In March 2022, an English version was published (Interview CZ1).

The Manual covers many practical topics. It provides governance recommendations on risk management, due diligence, communication and training, and cyber security. What is noteworthy is that about half of the document is devoted to explaining the different methods which foreign actors might use to target individuals in order to interfere in Czech academia and society. This is to help individual actors to prepare for situations in which they "may become of interest to a foreign power" and to assist them in responding adequately in such a situation (MVCR 2022). According to one stakeholder, these recommendations are quite directly adapted from instructions for intelligence or military officials, which are not suitable for academics (Interview CZ1). What also stands out is the emphasis on preserving documentation on risk assess-

ment for individual cases and of the decision making process on measures taken. This would provide a "fundamental retrospective view" (MVCR 2022). Preserving documentation for the sake of transparency is a very concrete piece of advice that is not often found in the recommendations published in other countries.

3. Analysis

The Czech national approach to knowledge security is quite comprehensive and addresses three of the four steps for safeguarding knowledge security. The first two steps of raising awareness and identifying risks are covered, for example, in the Manual's introduction that provides recommendations on how HEIs could train their staff and an extensive explanation of various interference techniques. Recommendations for mitigating risks are also provided, such as on the adoption of due diligence processes and cyber security strategies. The final step of identifying opportunities for safe cooperation receives less attention.

The Manual covers all three types of risks (preventing undesirable knowledge transfer, protecting academic freedom and ensuring ethical practices). Although there is a brief sub-paragraph on "Research and Intellectual Property Protection", the focus of the manual appears to be on preventing foreign actors from having unwanted political influence in Czech academia and undermining academic freedom. Although the discussion of interference techniques addresses undesired knowledge transfers, issues such "theft", "dual-use" and "intellectual property" are much less prominently discussed in the Manual than issues relating to "freedom" or "influence" (MVCR 2022). This is understandable given the national context in which the Czech approach to knowledge security developed and also because another document (the Handbook Technical Assistance and Intangible Transfer of Technology) already explains in detail how HEIs should deal with restrictions (e.g. sanctions, export controls) on, for example, the sharing of dual-use knowledge.

It is clear that a certain level of coherence within the Czech approach is pursued. This is apparent, for example, in the National Strategy for Countering Hybrid Interference, which states that it is "in conformity with other national security policies", including the National Cyber Security Strategy. It does not mention the Manual, however, nor the Centre Against Hybrid Threats (Ministry of Defence 2021). What's more, the National Cyber Security Strategy and the Manual never mention one another nor the National Strategy for Countering Hybrid Interference, or the Centre Against Hybrid Threats, despite the clear overlaps in content. The same appears to be true for the website of the National Office of Cyber and Information Security.

The Manual does provide links to other relevant resources, such as topic-specific recommendations by the National Cyber Security Centre. Strangely enough, the Manual also does not link to or mention the Handbook Technical Assistance and Intangible Transfer of Technology, but does provide links to relevant websites regarding international sanctions, including the Financial Analytical Office which drafted the Handbook. The Manual does call upon HEIs to "share their knowledge and experience relating to the ever-evolving risk of interference" in working groups or online platforms within institutions and across the sector. This would promote coherence in policy and practice, but it is unclear whether such initiatives have started so far. A clear overview of relevant government agencies, other policy documents, or legislation is lacking, though there are some references to relevant laws.

This shortage of coherence could stem from the lack of coordination between Czech government agencies and departments, which operate very independently of one another and in a siloed manner, according to one interlocutor (Interview CZ1). The

Manual, for example, was developed by a specific government department, and not officially endorsed by the minister or mandated by the wider government. The counter intelligence services appear to have played a relatively large role in this case, which explains the extensive focus and detailed instructions on the ways in which individuals might be targeted by foreign intelligence services (Interview CZ1). The shortage of coherence is further fueled by the lack of political consensus within the government and between (semi-)government institutions. Some officials who are appointed to lead relevant government agencies are outspoken pro-EU and take a tough stance towards Russia and China, while others are favoring a less confrontational approach towards the latter two countries (Interview CZ2).

Regarding the enforcement level of the recommendations, the Manual makes it very clear that "In no way is the aim to impose new legal or administrative obligations on universities; on the contrary – the implementation of counter interference measures resides on the principles of voluntariness and personal and institutional responsibility". The document furthermore underlines the importance of measures taken by universities themselves and calls itself a "collection of advice and recommendations"(MVCR 2022). Interlocutors have pointed out that Czech universities very much emphasize their autonomy and that adherence to any guidance fully depends on the leadership of an individual university (Interview CZ1; Interview CZ2).

The Manual offers quite practical tools that facilitate implementation. For example, a list of definitions of important terms is included, as well as questionnaires. This makes the recommendations, which are often already quite detailed and specific, even more concrete. Especially the discussion of interference techniques contains very detailed recommendations, such as on the risks of accepting a USB as a gift from a foreign partner. The Manual furthermore calls for practices that facilitate implementation. However, one interlocutor would have liked clearer instructions from the government on which cooperation is safe and unsafe, in part because it was the government who promoted academic collaboration with China in the past (Interview CZ1).

Finally, it is noteworthy that the Manual states that the media and the public will increasingly demand risk assessments of foreign partners, and that institutions face reputational risks for not having proper risk strategies (MCVR 2022). This emphasizes the benefits of putting in practice the recommendations to researchers and institutions, thereby promoting its implementation. Considering the Czech Republic's highly politicized relationship with China, which also affects academics, this is a sensible point to make.

3. FINLAND

1. National context

Finland's approach to knowledge security is developing in a context in which relations with Russia and China are both particularly important. However, it is first and foremost the changing relationship with China that shapes the recent Finnish initiatives to safeguard knowledge security. This is because Finland's society has long been adapting to Russian espionage, political interference and cyber threats, whereas the challenges that China poses are relatively new. Finland's higher education sector has decades-long experience with addressing knowledge security risks related to Russia, and universities and scholars therefore have built up "tacit knowledge" of these risks, and how to address them. The need for new and specific knowledge security measures in response to Russian activities is thus not deemed necessary (Interview FI2).

This is a different story when it comes to China. Finland enjoyed a relatively pragmatic relationship and strong economic connections with China, compared to some of its Nordic neighbors. However, in recent years Finnish security services started warning against potential Chinese threats and foreign investment screening tightened. As in many European countries, Finland's relations with China began to deteriorate. In 2021, Finland's Ministry of Foreign Affairs published its Governmental Action Plan on China, in which it adopted the EU's label of China as a "systemic rival" (The Diplomat 2022).

The changing political climate also reached the higher education sector. In the past, China was simply seen as a partner that offered indispensable opportunities and resources for academic collaboration. On the institutional level, China was the most important collaboration partner of Finland's natural science universities (Interview FI1). Precisely because China was such an important partner, an informal China roundtable was established where information and experiences regarding the cooperation could be shared among Finnish stakeholders. At that time, everyone was still very open, positive and proud of their collaboration with China, and there was competition between the institutions in that regard. This mindset changed when security officials and intelligence services informed university rectors of the geopolitical implications and risks of this cooperation (Interview FI1; Interview FI2). In 2022, Finland's only Confucius Institute was closed over concerns that it was used for propaganda purposes by the Chinese government (Myklebust 2022).

The HE sector realized that its awareness of risks of collaborating with China was very limited. Knowledge institutions indicated that they wanted assurances about the conditions under which they could safely cooperate with China. They also wanted to be able to show their Chinese partners the conditions that institution in Finland have to respect when cooperating.

This motivated stakeholders to draft the Recommendations for academic cooperation with China. Institutions in Finland had already welcomed guidelines from other countries and the EU, which inspired the initiators to do the same (Interview FI1; interview FI2).

Universities have come together to discuss their response to Russia's invasion of Ukraine, resulting in a new emphasis on taking measures that are not China-specific. Roundtables on academic cooperation with other countries which address knowledge security, including Russia, do already exist. Nonetheless, the importance of

academic collaboration with China and the lack of risk awareness is still the main factor shaping Finland's national approach, and is also the reason why the recommendations for academic cooperation with China have not been made state-agnostic (Interview FI1; interview FI2). Finland does not make use of one specific term to refer to knowledge security, but the approach emphasizes collaboration based on the principles and interests of Finnish institutions.

2. Mapping

Major knowledge security initiatives and measures in Finland

Format(s)	Initiative	Actors
Guidelines and recommendations	Recommendations for academic cooperation with China	Ministry of Education and Culture; HE institutions; research institutes; other stakeholders
	Governmental Action Plan on China 2021	Ministry of Foreign Affairs
Special bodies	China Roundtable with six working groups	Representatives of the international and legal offices of Finnish universities, China scholars, other university staff involved in cooperation with China, Ministry of Education and Culture, Ministry of Foreign Affairs
	Roundtables for rectors on knowledge security	Rectors of knowledge institutions

Major actors in knowledge security in Finland

Actors	Actions
Finnish National Board on Research Integrity TENK	Promoting the responsible conduct of research, prevenings research misconduct, promoting discussion and spreading information on research integrity in Finland
Team Finland Knowledge network	Creating a more internationally oriented position in higher education and research for Finland by attracting talented people to Finland and building contacts for sharing Finnish knowledge, expertise and educational innovation

Recommendations for academic cooperation with China

The 17-page recommendations are available in Finnish, Swedish and English, and were published in March 2022 by the Ministry of Education and Culture. There was continuous input from the China roundtable (see below) during the drafting process, which was overseen by the same ministry. Basically all actors that participated in the roundtable were involved in the drafting process, as well as the Ministry of Economic Affairs and Employment and the Academy of Finland. It was the Finnish Science Councilor for China who together with the Ministry of Education and Culture formulated the final version.

Clearly, the document is not state agnostic. However, the recommendations themselves do not actually mention China anywhere, and could be directly applied to other countries. It is solely the accompanying background text that addresses China specifically. The recommendations address issues of: (1) Safe cooperation (good governance, due diligence, risk management, intervention and communication strategies for problems and crises); (2) Ethical cooperation (academic integrity, freedom, autonomy, ethical application of knowledge, accounting for cultural and political content and connotations); and (3) Awareness of risks (political and economic limitations, such as sanctions, and security risks, such as data breaches and political interference). All three risk areas of academic freedom, knowledge transfer and ethical standards are thereby covered. The document is quite brief and the recommendations are very general, without detailed instructions, sharp definitions, clear assignments of responsibilities or materials that support implementation.

China roundtable with six working groups

The China roundtable is a very informal, bottom-up meeting between representatives of the international offices of Finnish universities and China scholars, with the Ministry of Education and Culture and Ministry of Foreign Affairs also involved, the former officially running the roundtable. The Finnish Science Councilor for China has been the driving force of the initiative. Under the China roundtable, there are six working groups each focusing on a specific theme. These are:

- Traffic lights and risk matrix
- Evaluating partnerships
- Information security
- ICT cooperation
- Legal issues
- Concrete support for staff and students

These working groups were founded when the recommendations were being completed. Since these recommendations are relatively general, the working groups were formed to facilitate discussion on how to implement them in practice. Stakeholders were free to join any group they wanted. The working groups are open to a broader range of participants than the roundtable. Representatives from research institutes, academics who cooperate with China themselves and representatives from the legal offices of universities are also part of these groups.

The discussions about who should be responsible for the implementation of the recommendations (the universities or an overarching authority) are still going on. The working groups therefore have not put out concrete initiatives yet. However, the working group *Concrete support for staff and students* is, for example, contemplating guidelines on how to brief new foreign students and staff at Finnish universities about principles such as academic freedom, privacy and data protection (Interview FI2).

3. Analysis

The Finnish national approach is still quite small scale because of its recent inception and, according to one interlocutor, because Finland's approach to foreign policy in general is relatively non-confrontational (Interview FI2). As a result, only a small number of measures have been taken. The approach is also still in the process of covering all four steps of a comprehensive approach to safeguarding knowledge

security. The first step of raising awareness has been taken, and the measures are currently directed at risk identification and mitigation. The fourth step of identifying opportunities for safe cooperation is currently left for HEIs to take. While the focus of the Finnish approach was initially on knowledge transfers and the ethical use of technology, the issue of academic freedom is increasingly becoming an important element of the discussion (Interview FI1).

One of the benefits of the bottom-up and informal nature of the Finnish approach is that it creates a high level of coherence. Many stakeholders are able to join the roundtable and working groups, making communication relatively direct. For example, the Ministry of Foreign Affairs was present in every roundtable meeting, and the recommendations are attuned to their Governmental Action Plan on China 2021. Furthermore, universities of applied sciences are also incorporated in the process, while the government is trying to be as open as possible, and sharing all information with the stakeholders (Interview FI1).

While HEIs do take the recommendations document seriously, institutions or researchers are not being evaluated based on that specific document and the recommendations are thus not directly enforced. However, all recommendations are based on general principles, such as practicing research ethics and upholding academic freedom, which Finnish universities need to uphold and on which they are assessed. Furthermore, there are informal discussions on how the recommendations are being applied at institutions. In severe cases, the Finnish security agencies, who are very well connected with the sector, would step in (Interview FI1; Interview FI2). There are no indications that actors are required to join the roundtables or working groups, and as such, there is not a sense of enforcement in that regard.

So far, stakeholders have reacted positively towards the roundtable and its working groups. The recommendations are also welcomed as timely and useful. The bottom-up and informal approach is appreciated in particular, as it engages a lot of people from different departments and institutions, while giving universities a sense of responsibility for implementing policies, according to our interlocutors (Interview FI1; Interview FI2).

However, some problems have also been identified with the approach. First of all, one interlocutor indicates that institutions face a lack of resources and capacity to further the development of the approach and would welcome a representative assigned by the government to keep schedules and provide structure. Furthermore, more attention should be devoted on how to apply the recommendations in different disciplines. According to our interlocutors, the issues and solutions vary widely between the natural and social disciplines, which challenges any singular approach. It has also proven to be a challenge to ensure that the recommendations actually reach the practitioners on the work floor who directly cooperate with China, according to our interlocutors (Interview FI1; Interview FI2).

4. FRANCE

1. National context

In France, measures around knowledge security should be understood in the context of the country's highly centralized education system, highly-developed national strategic culture, and the aim for strategic autonomy of France. These features are illustrated, for example, by the importance that policy documents attach to the protection of "patrimoine scientifique" or "scientific heritage". France is home to more than 3500 public and private institutes of higher education, including 72 universities, 271 doctoral schools and 227 engineering schools. Universities are public institutions, financed by the state (Campus France). In 2020 France spent 2.3% of its GDP on R&D (OECD 2022).

Both the government and the media in France have reported on foreign interference and knowledge security breaches, including theft of strategic or sensitive information from French research laboratories. A comprehensive Senate report, titled "Better protect our scientific heritage and our academic freedoms", that deals with foreign influence in education and research collaboration has contributed to government and public discussions on the need for a broad approach to knowledge security (exchange F2).

Knowledge security, however, is not a familiar term in France. The French government uses the concept Protection of the Scientific and Technical Potential of the Nation (PPST) to discuss issues of research security. The PPST system aims to protect access to research institutes and their strategic knowledge and know-how as well as sensitive technologies (SGDSN PPST).

2. Mapping

Major knowledge security initiatives and measures in France

Format(s)	Initiative	Actors
Guidelines and recommendations	No national guidelines found	
Research reports	Influences étatiques extra-européennes dans le monde universitaire et académique français et leur incidences (2021)	André Gattolin, Senator
	Chinese Influence Operations	Institute for Strategic research of the Ecole Militaire (IRSEM)
Laws and regulations	Ministerial Decision	Prime Minister
	Interministerial Circular	Prime Minister
	Education Law & Research Law	

Major actors in knowledge security in France

Actors	Actions
The General Secretariat for Defence and National Security (SGDSN)	Monitoring security; advising and supporting policymaking
Ministry of Higher Education and Research	Screening of international MoU's of research institutes Strong involvement in SGDSN
Ministry of Defense Ministry of Economy and Finance Ministry of Agriculture Ministry of Sustainable Development Ministry of Health	The ministries listed here participate actively in the PPST system, including the delimitation of the Restricted Regime Zones
Senior Defense and Security Official (HFDS)	Provides advice and coordination for various ministries for all questions relating to defense and security, including PPST. It has a dedicated service involved in screening international science collaboration contracts

The French approach has two main elements: (1) the "Protection of the Scientific and Technical Potential of the Nation (PPST)" framework and (2) screening of contracts of international collaboration.

The PPST Network

Most knowledge security measures in France are developed and executed within the national framework "Protection of the Scientific and Technical Potential of the Nation (PPST)". The PPST system targets public and private establishments with the aim to protect strategic scientific knowledge and know-how as well as sensitive technologies, the capture of which could contain risks (e.g. economic risks, terrorism, or the proliferation of conventional weapons or arms of mass destruction) that harm national interests (SGDSN PPST). The official body responsible for PPST, including the inter-ministerial coordination of the system, is the General Secretariat for Defence and National Security (SGDSN), an inter-ministerial body placed under the authority of the French Prime Minister. It assists the head of government in designing and implementing security and defense policies. Implementation of the PPST is based on the Interministerial Circular for Implementation of the PPST Mechanism (2012) and Ministerial Decision (2012), which regulates details of the PPST-system.

The PPST system offers:

- Protection of all material and immaterial goods specific to fundamental or applied scientific activity and to the technological development of the nation.
- Legal and administrative protection based on access control, both physical and virtual, to sensitive information held within protected areas.
- Establishment of protected areas: the "restricted regime zones" (ZRR). The ZRR are defined spaces within which strategic research or production activities are to be protected because of the interest they present for the competitiveness of the institution or the nation. The delimitation of a ZRR is based on the identification - with the help of checklists - of knowledge that organizations want to protect.

The process is overseen by SGDN. Examples are laboratories hosting strategic or sensitive research or production activities.

SDGN explicitly mentions the aim to balance between protection and promoting science collaboration, but it is not clear if and how the promotion of science collaboration is worked on within the PPST-system.

Protection measures include regulation of access to the ZRR, implementation of a policy for the protection of information systems, and ongoing consultation with State services to accompany the implementation and to adapt the protection if necessary (SGDSN Plaquette). Digital and cyber security are also covered by the PPST system; a guiding document provides many details on the French Restricted Information System Regime (SIRR).

PPST is developed on the basis of consultation between public authorities and the institutions. The consultation leads to an agreement between the research institution and the sectoral ministry; the agreement is implemented based on support of the institution; the rules are not pro-actively enforced but there are penal consequences for offenders of the ZRR rules. These rules may differ between ZRRs: each entity decides, according to its means and needs, whether or not to deploy technical tools such as badge readers, surveillance cameras, etc. (PPST Q&A).

Ministries involved in the PPST-system are the Ministry of Higher Education and Research (MESR), the Ministry of Defense, the Ministry of Economy, Finance and the Recovery, the Ministry of Agriculture and Food, the Ministry of Ecology, Sustainable Development and Energy, and the Ministry of Health and Prevention. They play major roles in the development and implementation of the PPST-system in the research areas they are responsible for, including the delimitation of the Restricted Regime Zones (ZRR).

Screening of contracts

The second pillar of the French approach concerns the screening of all international academic collaboration contracts. The screening finds a legal base in the Education Law, which lays down the principle of freedom for universities and institutes to sign contracts with foreign universities and research institutes. However, this freedom is supervised by the Ministry of Higher Education and Research and the Ministry of Foreign Affairs. The Ministries review the collaboration contracts and have one month to express their opposition. After this period, the agreement is deemed approved. According to the Sentate report of September 2021, 912 files had been submitted for revision since 1 January 2019, with a negative review rate of 6.5%. The screening is the responsibility of the Senior Defense and Security Official (Haut Fonctionnaire de Défense et de Sécurité (HFDS)) at the Ministry of Higher Education and Research (HFDS-MESRI). At the university level, an officer of the Ministry of Defense is responsible for delivering the contracts for screening to the HFDS (exchange F4).

Raising awareness

The comprehensive Senate Report Better Protect our Scientific Heritage and our Academic Freedoms (Senator André Gattolin, 2021) plays an important role in stimulating the public debate about knowledge security. It deals with foreign interference and the theft of sensitive scientific data in order to obtain a strategic, economic or military advantage. The report also notes the issue of "self-censorship that some academics may be practicing when they handle certain questions related to complex geopolitical situations". It identifies three factors that make French HEIs vulnerable: insufficient budgetary resources; administrative weakness in management at auto-

nomous institutions and contradictory demands of welcoming foreign students and more rigorous control; and a culture of openness of a research sector that is by nature reluctant to view its activity in a context of conflict and national interest. It ends with 26 recommendations to protect academic freedom and the scientific heritage of France.

3. Analysis

The two policies that constitute the French approach towards knowledge security, the PPST system and the screening of agreements and contracts, focus on the identification and mitigation of risks. No public evidence of activities aimed at raising awareness was found, other than the report by Senator André Gattolin.

The PPST-system is based on the French tradition of protectionism with regard to the country's "scientific heritage" ("Patrimoine Scientifique") and the country's aim for strategic autonomy (Interview F1). At the institutional and practical level, e.g. the delimitation of Restricted Regime Zones (ZRR), measures are developed in consultation with research institutions, with supervision by SGDSN. Interestingly, this system is not focused on who comes into the country (visa) but through limiting (physically and online) access to labs or parts of research institutes. This approach has the advantage of not having to screen individual people but does not address risks of interference beyond the area of high-tech research. That being said, the limited scope of PPST, its clear instructions, and the involvement of the research institutes and many ministries, each with its own expertise, should enable an effective implementation. It is not clear whether this is indeed the case, due to a lack of access to information.

The screening of all international contracts by the French Ministry of Higher Education and Research is unique within the group of countries examined for this report. Although there are little details available about the implementation of this measure, the Senate report finding that at least 912 contracts were reviewed in the period 2019-mid 2021, with a negative review rate of 6.5%, suggests a certain level of effectiveness.

Actively protecting academic freedom and identifying opportunities are not discussed as elements of the French approach to knowledge security, although the Senate report calls for putting interference firmly on the policy agenda and supporting universities to "protect their values of academic freedom and scientific integrity while respecting their autonomy".

5. GERMANY

1. National context

Germany's approach to knowledge security is shaped by its federal political system. In Germany, the federal ministries have no competency in the field of education, it is the 16 federal states that are responsible for education, including the basic funding and organization of higher education and research institutes. Each state has its own laws governing higher education and there may be differences in structure and organization of HEIs between the states. However, the states have agreed on certain basic principles laid down in the framework of the Standing Conference of the Ministers of Education and Cultural Affairs (HRK HEI-system).

Germany is a major player in scientific research. In 2020 it spent 3% of its GDP on R&D (OECD-Germany) and it is the fourth largest spender (6% in 2019) of global research and development (US National Science Foundation 2022). The country has 115 universities and big non-university research institutions, such as – the Max Planck Society, the Helmholtz Association, the Leibniz Association and the Fraunhofer Society. Academic exchange and international collaboration are important elements of Germany's educational policy: Germany is the most popular non-English-speaking host country for international students and comes fourth worldwide (after the USA, the UK and Australia) in terms of numbers of enrolled foreign students. This can partially be explained by the fact that there are no tuition fees in Germany. However, Germany is also an attractive destination for academic personnel: at the four research institutions mentioned above, some 18,000 (25% of total academic personnel) researchers come from abroad (Networking academia).

In Germany, discussions and actions on knowledge security were initially focused on China, driven by the national intelligence agency's warnings about potential sensitive technology transfers to China, international reports on Chinese interference in academia, such as the ASPI report on Chinese military's collaboration with foreign universities, and questions raised in the German Bundestag about Chinese influence on Confucius Institutes in Germany (Deutscher Bundestag 2019). However the debate soon evolved to state agnostic discussions and actions (Interview G4).

Stakeholders in Germany do not use a specific term or wording for discussing the issues that are part of the definition of knowledge security used in this report. Every document uses different wording and often the word "security" is avoided.

2. Mapping

Major knowledge security initiatives and measures in Germany

Format(s)	Initiative	Actors
Guidelines and recommendations	Guidelines and standards in international university cooperation (2020)	The German Rectors' Conference (HRK): association of German state and state-recognized universities
	Guiding Questions on University Cooperation with the People's Republic of China (2020)	The German Rectors' Conference (HRK)

	Risks for the German research location - Guidelines for dealing with scientific espionage and spying on competitors in the scientific context	WISKOS: Industrial espionage and spying on competitors in Germany and Europe; project funded by the German Federal Ministry of Education and Research (BMBF)
	No red lines - science cooperation under complex framework conditions (2020)	German Academic Exchange Service (DAAD)
	Risky Business: Rethinking Research Cooperation with Non-Democracies. Strategies for Foundations, Universities, Civil Society Organizations, and Think Tanks (2020)	Global Public Policy Institute (GPPi)
Activities	Monthly webinars	BMBF, together with HRK, DLR, and the Alliance of Science Organisations
	Support meetings for legal questions regarding safe contracts	BMBF together with DLR, and a legal company
Opportunity management	Pathways to Research with China: Knowledge, Approaches, Recommendations (2020)	AG China-Forschung: Working Group China Research, Lower Saxony's Ministry for Science and Culture

Major actors in knowledge security in Germany

Actors	Actions
Federal Ministry of Education and Research (BMBF)	Funding and promotion of safe international collaboration Webinars aimed at raising awareness (together with HRK, DLR, and the Alliance of Science Organisations)
Ministry of Foreign Affairs	Inter-ministerial coordination; contributing foreign policy information relevant to knowledge security
Ministry of Economic Affairs	Dual use, tech transfer, and export control regulations
The German Rectors' Conference (HRK)	Country neutral & China specific guidelines Awareness raising
Alliance of Science Organisations	"Freedom is our system. Together for Science" campaign: events seminars, publications
National Academy of Sciences Leopoldina	Awareness raising and (ethical) standard setting

In 2020 various guidelines were published in Germany, all with a different focus:

General guidelines

In April 2020, the German Rectors' Conference (HRK), an association of 269 public and government-recognized universities in Germany, published the Guidelines and standards in international university cooperation (2020). The document provides German universities and research institutions with comprehensive guidance for setting up and maintaining international cooperation projects and international part-

nerships. It deals with all elements of knowledge security, including academic integrity and freedom as well as cultural differences. In September of the same year, it was complemented by the Guiding Questions on University Cooperation with the People's Republic of China (2020). This China-specific document presents 59 guiding questions that address concerns that may arise in the cooperation with Chinese partners. It aims to find a balance between risk management and opportunity management by both emphasizing the importance and mutual benefits of research collaboration with China and pointing out that there are growing concerns about the influence of the Chinese Communist Party (CCP) on research institutions and about the limitations of academic freedom in China. It provides many practical recommendations, including for continued dialogue with Chinese partners.

The German Academic Exchange Service (DAAD), in collaboration with universities, published its own guidelines, No red lines - science cooperation under complex framework conditions (2020, 57p). They support higher education institutions in making a risk and benefit analysis of their international collaboration based on six criteria: (1) Security situation, (2) General political imperative, (3) Rule of law and socio-political framework, (4) Opportunities and risks of the respective science system, (5) Performance and accuracy of the scientific partner institution(s), and (6) Embedding in one's own institutional strategy. It also considers academic freedom.

Guidelines focusing on espionage

The Risks for the German research location - Guidelines for dealing with scientific espionage and spying on competitors in the scientific context (28p) focus on scientific espionage. These guidelines are developed by WISKOS, a project addressing industrial espionage and spying on competitors in Germany and Europe; it is funded by the German Federal Ministry of Education (BMBF). The guidelines provide German universities and research institutions with information on espionage activities. Furthermore, they offer recommendations and additional resources. They address common themes, such as risk analysis and governance structures within universities, but also make specific suggestions such as to track researchers' career paths after they leave the institution.

Guidelines from research institutes

In 2021, the big research institutes, such as the Max Planck Society and Leibnitz Association became very active in publishing guidelines and reports, e.g. on identification of research areas that are vulnerable to foreign interference. Because of their comprehensiveness, two documents of the Max Planck Society are included here.

1. The comprehensive and detailed Guidelines For Responsible Conduct (2021, 72p), which are supported by examples and cases, aimed at helping researchers to act in accordance with the values of the Max Planck Society (integrity, transparency, respect) and to raise awareness of pitfalls. The document encompasses all areas of knowledge security, including tech transfer, IT risks, ethical research practices and ethical use of research, export control, conflict of interest, and academic freedom.
2. The more specific Guidelines for International Collaborations (2021, 28p) directed at scientists at the Max Planck Society who start an international collaboration and "seek to balance freedom of research, compliance with regulations and individual responsibility". The document aims to raise awareness of potential risks and to acquaint researchers with the applicable legal rules and requirements, and the options for obtaining advice.

The National Academy of Sciences Leopoldina is also active in the field of knowledge security. It plays an important role in setting ethical standards (interview G-5), which also pertains to academic freedom in its broadest sense. Furthermore it published the Information Brochure: The Handling of Security-Relevant Research in Germany – An Overview (2022), which defines the concept of Security-Relevant Research and addresses the risks involved by providing information on selected security-relevant research topics and case studies.

Webinars series and the development of tools

The German Federal Ministry of Education and Research (BMBF) organizes monthly seminars for the academic community on topics related to knowledge security, together with the German Rectors' Conference (HRK), the Alliance of Science Organisations, and DLR Project Management Agency. The seminars are well attended, thanks to the close collaboration with the HRK and the Alliance (interviews G3, G4). The BMBF also invests in building knowledge on relevant themes, e.g. through the program to build China Competence. The Federal Ministry of Foreign Affairs is responsible for inter-ministerial coordination on issues related to international collaboration and knowledge security, and contributes relevant (country) information, e.g. to the above seminars. The German Ministry of Economic Affairs and Export Control (BAFA), promotes implementation of dual use, tech transfer and export control regulations. It has an Export Control and Academia webportal.

The associations and actors like DLR are active in organizing conferences (G4, G5) and developing tools aimed at facilitating risk assessment by researchers and identification of critical and sensitive areas of research.

Freedom of science and academic freedom

In 2019, the Alliance of Science Organisations, an association of the ten most important science and research organizations in Germany, ran the "Freedom is our system. Together for science" campaign. This initiative comprised a series of events, speeches, debates and opinion pieces in which the science system was critically scrutinized and attention was drawn to instances in which academic freedom comes under global threat. The campaign conveyed "a message in support of freedom in research and teaching against the restrictions and exertion of influence that are gaining ground in many places" (Alliance campaign and Campaign Portal).

Focus on opportunities

The white paper Pathways to Research with China: Knowledge, Approaches, Recommendations (2020), was written by the Working Group China Research (AG China-Forschung) that was appointed by Lower Saxony's Ministry for Science and Culture. It identifies opportunities in collaboration with China. It provides information about the academic system in China, examples of successful cooperation with China and best practices in developing collaboration, such as having an on-site presence in China and having balanced funding.

3. Analysis

The German approach is very comprehensive and is characterized by a strong involvement of the academic community through the German Rectors' Conference, the Alliance of Science Organisations, the National Academy of Sciences Leopoldina and the big non-university research institutes (Interview G1). The approach therefore is largely bottom-up. The Federal ministries are active in promoting and supporting the development and dissemination of relevant knowledge and in raising awareness.

Since the Federal Ministry of Education and Research is not competent in the area of education, it also supports the ministries of the federal states (Länder) in developing relevant measures and activities.

Measures and activities are not only aimed at the prevention of undesirable knowledge transfer and the promotion of ethical practices, but also actively consider the protection of academic freedom, as evidenced, for example, by the "Freedom is our system. Together for science" campaign, but also by references to academic freedom in other guidelines. Academic freedom is understood as a part of the broader concept of "freedom of scientific research", as laid down in the Bonn Declaration. The Bonn Declaration, adopted by the Ministerial Conference on the European Research Area, aims to protect critical discourse and condemns violations of freedom of scientific research, including freedom of expression, freedom of association, the freedom of movement and the right to education.

The comprehensiveness is also evidenced by the fact that the German approach deals with awareness raising, identification and mitigation of risks *and* the identification of opportunities. Attention for opportunities is not only the central theme in white paper of the Lower Saxony's Working Group China Research but is included in most guidelines. They provide practical suggestions for the continuation or expansion of research collaboration with countries of concern.

What also stands out in the German approach is that many guidelines and activities avoid words and terms like "knowledge/research security" or "foreign interference". The research institutes and science organizations find the solutions to the risks of international collaboration, that have recently come to the fore, already in the long existing guidelines and code of conducts for international collaboration, ethical research, and the regimes for research related to dual use technology and products. The overriding approach, as one interlocutor put it, is: "all rules for safe, sound, and ethical collaboration have been in place for a long time. The good practices are already there, we only must refresh them and draw more attention to the need for compliance" (Interview G5).

These factors result in a very balanced bottom-up approach without enforcement, that pays attention to the opportunity side and that avoids the securitization of international collaboration that many researchers around the globe, including many of our interlocutors, complain about. Weaknesses of the German approach are related to the federal structure and the lack of mandate of the German Ministry of Education and Research in the area of education. This sometimes leads to longer lines of communication and/or complicates horizontal and vertical coordination (Interviews G3, G4). Furthermore, it results in the lack of one point of coordination for all actions and measures (Interview G5).

Because the various elements of knowledge security are dealt with not as a separate issue but are rather integrated in broader efforts to strengthen ethical research and protect freedom of scientific research, there is no official evaluation of the effectiveness of measures and activities. As far as the participation in conferences and monthly webinars, and efforts to develop tools to analyze and mitigate risk analysis can be considered indicators, the approach seems to have positive results with regard to drawing attention and raising awareness. Some interlocutors are more skeptical about the effectiveness in terms of strengthening compliance among individual researchers (Interviews G1, G2).

Germany is also active in promoting international collaboration and coordination regarding research security, among others in the context of G7, of which Germany holds the Presidency in 2022. The G7 framework includes a Working Group on the

Security and Integrity of the Global Research Ecosystem (SIGRE), which works on the review of existing principles of research security and research integrity, the identification of voluntary standards of conduct and best practice, and on the strengthening of exchange of best practices across the research community (SIGRE paper 2022).

6. JAPAN

1. National context

Japan is a major academic player in the world: it is the third-largest investor in research & development, behind the United States and China, ranks third as patent filer in the world, and ranks second in number of Nobel Prize winners in physics. However, because of decreasing research funding at universities, Japan's global position in scientific research is weakening and the country also lags behind in terms of international collaboration in science and innovation among OECD countries. For example, only 1% of its patents involve co-innovation, and 24.4% of scientific publications involve international co-authorship (European Commission, RTD, 2018). According to experts, this is a result of both Japanese restrictions on international collaboration and a focus on research for the domestic market (Asahi Shimbum, 23 august 2021).

In recent years concerns about inappropriate influence from foreign countries and undesirable technology transfer have become more prominent in Japan. This is partially because of incidents and reports of risks of international collaboration with China, but also as a result of the international attention for the risks of international STI collaboration, in particular in the US, which is Japan's prominent academic and political partner (Kakuchi, Dec. 2020; Tokyo Review Dec 2019). As discussed below, Japan's approach to knowledge security is formulated in country neutral terms, but media reports and the national debate in Japan often refer to China, as does the US in joint meetings with Japan (see e.g. Carnegie Endowment 2021). This is not surprising in view of both the long-time political tensions between Japan and China and the fact that over the past decade, China has become an important S&T partner for Japan. Chinese graduate students comprise around 50% of foreign research students in top universities in Japan (Kakuchi, 23 July 2020) and Chinese scholars are the largest group of foreign academics at Japanese universities at 22% (2017), overtaking scholars from the US at 19% (Futao Huang).

The concept that Japan uses to discuss knowledge security is "research integrity". It is defined as: "the soundness and fairness of research, which must be newly secured against the new risks that accompany the internationalization and openness of research. These new risks undermine the fundamental values of the research environment, such as openness and transparency, and may cause researchers to have conflicts of interest and responsibilities" (MEXT portal). Furthermore, research security measures are regarded as "an autonomous code of conduct to be adhered to by the research community including researchers and research organizations" (CAO report 2021).

In Japan, research security is an element of the broader concept of 'economic security' (Interview J3). Economic security encompasses four areas: securing supply chains of critical materials, such as semiconductors; ensuring security of basic infrastructure; identifying leading areas of innovation and technology development to ensure competitiveness; and selecting and classifying Japanese patents to protect critical technologies (CFR 2022). Economic security has become a priority area for the Japanese government, which appointed a Minister for Economic Security in 2021 and passed an Economic Security Promotion Act in 2022 (see also below).

2. Mapping

Major knowledge security initiatives and measures in Japan

Format(s)	Initiative	Actors
Measures, regulations, and guidelines	Policy for ensuring Research Integrity against new risks accompanying the internationalization and openness of research activities (2021, 4 p.)	Science, Technology and Innovation Promotion Secretariat of the Cabinet Office
	Policy Measures for Ensuring Research Integrity (revised 2022, 7 p.)	Science, Technology and Innovation Promotion Secretariat of the Cabinet Office
	Guidelines for Appropriate Execution of Competitive Research Funds (2021)	Revised by the Liaison Committee of Related Ministries on Competitive Research Funds
Guidelines and checklists	A checklist (template) for Universities and Research Institutes (2021)	Cabinet Office
Recommendation	A checklist (template) for Researchers (2021)	Cabinet Office
Relevant research reports	Research Integrity Investigation and Analysis Report (2021)	Commissioned by the Cabinet Office
Laws and regulations	Economic Security Promotion Law (2022)	Implemented by multiple relevant ministries

Major actors in knowledge security in Japan

Actors	Actions
Cabinet Office and Council for Science technology and Innovation	Coordination and development of research integrity policies and measures; commissioning research
Ministry of Education, Culture, Sports, Science and Technology (MEXT)	Implementation; Checklists Outreach: briefing sessions and materials, including a video
Ministry of Economy, Trade and Industry (METI)	Implementation of economic security measures Export control
Ministry of Foreign Affairs	International dimension of / international collaboration on economic security and research integrity Screening

In 2019, the government put economic security on the agenda; the development of policies with regard to research integrity took off a year later, in 2020. In previous years, Japan had already invested in strengthening the implementation of export control regulations (Exchange J1, J2; Kakuchi and Sharma, 2021), but now it was ready to broaden its focus. Japan's Cabinet Office took the lead: it held review meet-

ings, commissioned research, and began to develop policies and regulations. Major documents and activities include:

Integrated Innovation Strategy 2020

The 2020 version of the yearly strategy includes: steps to monitor ongoing international research collaboration; support to raise awareness among Japanese companies, universities and research organizations about information leakage and technology theft; and initiatives to step up coordination between ministries and agencies to strengthen security measures (Kakuchi 23 July 2020). It also stated that international students and foreign researchers would become subject to strict visa screening in the future. In 2021, the Ministry of Foreign Affairs requested a budget of US$2.1 million to "strengthen scrutiny of visa applications with a view to preventing technology theft" (Kakuchi, Dec. 2020; Kakuchi and Sharma 2021). In a briefing on economic security in the framework of EU-Japan collaboration, METI confirmed this policy (METI-EU 2022) and the plan was indeed realized in 2022 (Reuters 2022).

Integrity in open and international research (2020)

This report by the Center for Research and Development Strategy (CRDS), an affiliated institution of the Japan Science and Technology Agency, offers reference material and input for actively addressing research integrity. It discusses the risks associated with openness and internationalization and trends in research integrity

Research Integrity Investigation and Analysis Report March 2021

This is a report by Pricewaterhouse Coopers Aarata LLC, commissioned by the Cabinet Office. The report contains proposals from a "Research Integrity Investigation Committee", consisting of government officials and research sector representatives, for a code of conduct for researchers and research organizations aimed at promoting research integrity.

Policy for ensuring research integrity against new risks accompanying the internationalization and openness of research activities (Cabinet Office, April 2021)

This set of measures addresses efforts for disclosure of information about international collaboration, raising awareness at universities and research institutes, revising rules for funding of research, and promoting interdepartmental collaboration, including with the Japanese Ministry of Economy, Trade and Industry, and the Ministry of Health, Labor and Welfare. The policy was revised and expanded in 2022 (see below). They were complemented by the **Guidelines for Appropriate Execution of Competitive Research Funds (2021)** which focus on disclosure.

Policy for ensuring research Integrity (Outline) (Cabinet Office, 2022)

This more practically oriented update focuses on responsibilities for individual researchers (information disclosure), universities and research institutes (strengthening research security management), and funding agencies (disclosure and assessment of information). It furthermore places the development of research integrity in Japan explicitly in the context of developments regarding knowledge security elsewhere in the world, in particular the US and the UK. It also aims to develop international coherence in approaches to promoting safe international research collaboration through the framework of the G7, making use of Japan holding the G7 Presidency in 2023.

In December 2021 the Cabinet Office published two checklists, which are promoted and disseminated by MEXT:

1. Checklist template for researchers (2p) This checklist focuses on due diligence, reporting to/seeking advice from university policy makers, disclosure of information, including on MoU's, joint projects, and international traveling.
2. Checklist template for universities and research institutes (2p) This checklist focuses on governance with regard to research integrity at universities and raises questions such as: is there a consultation desk for researchers? are staff members trained on ensuring research integrity? how do you ensure transparency and ensure reporting from researchers?

In addition, Japan has recently (May 2022) asked universities to screen foreign students and staff and flag people with ties to foreign governments or foreign military institutions. Adherence to this new guideline is voluntary (Reuters 2022).

As a result of the new measures The Japanese Ministry of Education, Culture, Sports, Science and Technology (MEXT) engaged in outreach to universities and research institutes, requesting them to proceed with implementing the measures. MEXT held briefing sessions, developed briefing material, made a video briefing, available at YouTube, and developed a Web portal on Research Security.

Actors

Cabinet Office and its Council for Science, Technology and Innovation (CSTI)

The Cabinet Office coordinates and develops policies that transcend the responsibilities and work fields of one ministry, and as such it is a driving force for the development of policies with regard to research integrity and the broader issue of economic security. In particular its Council for Science, Technology and Innovation (CSTI), plays a major role in developing relevant measures and actions. CSTI, which structures funding in STI, is chaired by the Prime Minister and consists of Ministers of eight STI-related ministries, incl. MEXT and METI, public and private STI stakeholders and the President of the Japan Science Council

The **Ministry of Education, Culture, Sports, Science and Technology** oversees the national universities and most research institutes and distributes most government funding for S&T research. It plays a prominent role in the dissemination and implementation of measures for research integrity, through organizing outreach activities such as briefings and a promotion video; encouraging and evaluating progress in the implementation of measures and tools, such as the checklists mentioned above; and providing support, e.g. through a research integrity web portal.

3. Analysis

Japan is a relative latecomer in developing measures to address knowledge security - other than export control – but is has used this fact to its benefit by carefully studying and learning from other countries' approaches. The Cabinet Office early on commissioned research on the issue of "research integrity", which provided further input for the development of policies. Currently Japan is catching up quickly.

The measures that have been introduced in the past two years are comprehensive: they deal with all the risks, except for risks to academic freedom, and they cover the steps of raising awareness, and identifying and mitigating risks. Generally, there is a focus on the disclosure of information. The outreach materials, including the checklists, are practical and provide concrete suggestions. Japanese documents and

research reports also emphasize the importance of identifying opportunities for collaboration, but this general aim is not elaborated upon in the measures. Research promotion is a separate policy track. Measures and guidelines are not particularly detailed.

With the Cabinet Office as the driver and coordinator of policies, Japan's approach has a top-down character. There are no bottom-up activities or guidelines developed by research communities or university associations. University officials and prominent researchers do participate in committees that provide input for or feedback on policy measures (Interview J4). Guidelines are not enforced, adherence is voluntary. However, MEXT inquiries into the implementation of measures at universities. Thanks to the coordination of the Cabinet Office, the Japanese approach is coherent. Policymakers may also have benefited from the lessons learned in other countries that they extensively studied.

It is too early to evaluate the effectiveness of the approach as the Japanese government has only started its outreach to universities in 2021, but public and interview responses suggest that there are many challenges (Exchange J5). One major challenge concerns awareness of the policy measures among researchers, which is still low; interlocutors suggest this may be due to the strong top-down approach (Exchanges J1, J5). A second challenge concerns the lack of insight among researchers and university staff into risks of collaboration with specific institutions in specific countries, notably China (Kakuchi and Sharma 2021). Furthermore, many researchers prefer to focus on the benefits of international collaboration with countries such as China (Kakuchi and Sharma 2021), and on Japan's need for, if not dependence on students and staff from China (Reuters 2022). A report by the Carnegie Endowment argues that Japan requires "a more holistic approach that considers high-priority security issues in the development of a legal framework, with sufficient penalties", and points out that the country should develop a "more robust security culture in key institutions" (Carnegie Endowment 2021).

What stands out in the Japanese approach is the country's explicit aim to engage in international collaboration and coordination regarding research security. Japan is engaged in collaboration with various 'like-minded' countries and plans to put security measures to promote safe international research collaboration, and the creation of principles of integrity, on the agenda of the 'G7 Security and Integrity of the Global Research Ecosystem Working Group' (see e.g. BMBF 2022), when it will hold the G7 Presidency in 2023 (Policy for ensuring research Integrity, Kakuchi and Sharma).

7. TAIWAN

1. National context

Taiwan's position on knowledge security is shaped by its complicated relation with the People's Republic of China and the fact that most countries in the world do not recognize Taiwan as a sovereign country. China considers Taiwan part of its sovereign territory and is pursuing reunification with the island. In efforts to convince the island to give up its resistance against reunification, China is putting growing economic, digital and military pressure on Taiwan, including all types of interference, also in academia. For example, in August 2022, a Chinese group hacked the computers of the National Taiwan University, causing the home pages of two university offices to display the message "There is only one China in the world." (Taiwan News 2022).

Due to the lack of diplomatic relations, Taiwan depends on economic engagement with the world. As a result, ensuring knowledge security and economic security are of existential importance for Taiwan and measures to protect science and technology and mitigate risks of Chinese interference are self-evident elements of Taiwanese policies, laws and societal initiatives. This self-evidence may explain the lack of discussion of the concept of "knowledge security" (Exchange T1).

The importance of research and development to Taiwan is reflected in the figures: in 2019, Taiwan ranked 4th in the world on innovation capability and 6th on science infrastructure (MOEA 2022). In 2020 Taiwan invested 3.6% of its GDP in R&D (OECD R&D) and the island is one of the world's leading producers of information and communication technology products.

Despite tense cross-strait relations, student exchanges between China and Taiwan flourished between 2011 and 2019. They peaked in 2015 and 2016 with more than 41,000 Chinese students being enrolled in short term and degree study programs in Taiwan. From 2017 onwards the number declined, allegedly due to tightening control on visas on the Chinese side (MPIWG 2020 and MAC 2022). In April 2020, the Chinese government suspended all applications from Chinese students to Taiwanese universities (PRCMoE 2019). The measures were taken in the context of the Covid-19 pandemic, but some observers expect them to be more permanent (MPIWG 2020). In 2022, the Taiwanese Ministry of Education launched a policy that encourages Taiwanese public and private universities to enroll more foreign students who are not fluent in Mandarin (Study International 2022).

2. Mapping

Major knowledge security initiatives and measures in Taiwan

Format(s)	Initiative	Actors
Guidelines and recommendations	Government-funded National Core Science and Technology Research Program Safety Control Operation Manual	National Security Council Science and Technology Team
Laws and regulations	National Security Act	
	Act Governing Relations Between the People of the Taiwan Area and the Mainland Area	

	Measures for Permitting People from the Mainland Area to Enter the Taiwan Area	
	Eight Must-Knows for Studying in Mainland China	ROC Mainland Affairs Council

Major actors in knowledge security in Taiwan

Actors	Actions
National Security Council Science and Technology Team	Operates the Safety Control Operation Manual
Ministry of Education	Implementation of laws and measures
Ministry of the Interior	Measures for Permitting People from the Mainland Area to Enter the Taiwan Area
ROC Mainland Affairs Council	Development and implementation of Cross-Straits relations policy

As discussed above, the concept of "knowledge security" is not well-known in Taiwan. The only official guidance document regarding knowledge security is the Government-funded National Core Science and Technology Research Program Safety Control Operation Manual (National Security Council, 2019; updated 2022). This comprehensive and detailed manual stipulates procedures to be followed for government-funded national core science and technology research projects. It is operated by the Science and Technology Team of the National Security Council and provides "administrative guidance", meaning it is not legally enforced.

The Manual lists six fields as national core science and technology research areas: (1) Agricultural science and technology (responsibility of Agriculture Committee); (2) Manufacturing Key Technologies (responsibility of the Ministry of Economic Affairs); (3) Aerospace and Satellite Technology (responsibility of National Science Council); (4) Ocean Science and Technology (responsibility of Ocean Commission); (5) Advanced Integrated Circuit Design and Process Technology (responsibility of National Science Council); and (6) Key technologies for Network Security (responsibility of the Executive Yuan). The manual describes the government's safety management measures and provides an overview of regulations and review mechanisms, as well as model disclosure forms and questionnaires.

Laws and regulations

Knowledge security issues are governed by several laws. The National Security Act (last amended 2022), protects national core critical technology from "acquisition, use, disclosure, reproduction and concealment of any national core critical technology" by "Offshore Entities" ("foreign countries, Mainland China, Hong Kong, Macao, or hostile foreign forces"). The "national core critical technologies" are defined as technologies that meet specific requirements and the outflow of which to the Foreign Entities will significantly damage Taiwan's national security, competitiveness in industries or economic development. They are reviewed on a regular basis.

The Act Governing Relations between the People of the Taiwan Area and the Mainland Area (The Cross-Strait Act, last amended 2022) protects Taiwan's high-tech industry and prevents the outflow of key technologies by regulating dealings between the peoples of the Taiwan Area and the Mainland Area, including the engagement

of Mainland Chinese with Taiwanese universities and research institutions. Mainland Chinese citizens may serve as faculty members, researchers of any academic or research institution if they have a household registration in Taiwan. However, they are not allowed to perform any work involving national security or confidential science-tech research unless having held a household registration in Taiwan for more than twenty years (Art. 21).

The Measures for Permitting People from the Mainland Area to Enter the Taiwan Area deal with issues such as cross-strait cooperation and forbids, for example, cooperation between Taiwanese universities and China's political parties, government or military agencies (Art. 33). The Ministry of Education is keen on ensuring compliance as a recent case illustrates. In 2021, the Cross-Strait Tsinghua Research Institute, which had established an office at the Taiwanese National Tsing Hua University's (NTHU) main campus without securing approval from the government was closed and its personnel was sent back to China. The Ministry followed up with sending "a notice to all colleges and universities in Taiwan, informing them that any cooperation with China's political parties, government or military agencies is unlawful'" (Taipei Times 2021).

In the past years, scrutiny regarding adherence to these laws has increased. Recently two Taiwanese professors who taught critical technologies - anti-ship missile and semiconductor technology - in China under the Chinese Changjiang Scholar Talent Recruitment program were investigated for leaking state secrets (Taipei Times 28 July 2022; Taipei Times 29 July 2022).

Raising awareness

With the aim of raising awareness about limitations to democratic and academic freedoms in China, Taiwan's Mainland Affairs Council (MAC) published the Eight Must-Knows for Studying in Mainland China (2022) on its "Taiwanese Students Area" portal. The "must-knows" include issues such as the "increasing difficulty of pursuing further studies in Europe or the US with Mainland diplomas", and information about Chinese state surveillance and censorship, and Taiwanese "consultation hotlines". The portal collects information and references to protect Taiwanese young people planning on studying or developing in mainland China.

To protect Taiwanese citizens from disinformation activities which also target higher education in Taiwan, the Taiwanese government and civil society have developed various tools. Examples are the Doublethink Lab, which provides research and tools that aim to strengthen democratic resilience against influence operations by non-democratic regimes; and the Taiwan FactCheck Center which fact-checks and verifies false information, either coming from media coverage or online rumors covering multiple themes, including educational debates, business activities, and government policies. The government itself is also active in this domain, as it established a "Disinformation Coordination Team" which encourages the development of training materials and lessons on media literacy, and tech tools to identify and address disinformation (NBR 2021).

Taiwanese universities generally provide online information and guidance on matters concerning overseas students and staff and on projects involving tech transfer, see for example Taiwan National University's webpages on TNU Chinese students and TNU tech transfer.

3. Analysis

Knowledge security is of existential importance to Taiwan. Therefore, the Taiwanese government has developed legislation and guidance materials that address the risks of undesirable technology transfer and foreign interference. However, the concept of knowledge security as such is not very familiar to Taiwanese policy makers or academics and there is no broad and integrated Taiwanese approach to knowledge security (Exchange T2). Instead, measures are part of broader policies aimed at addressing economic security and tackling foreign interference, and in particular disinformation. As Taiwan suffers from strong and broadly targeted foreign interference from China, most legislation and measures focus on the mitigation of risks posed by China.

Policies related to technology transfers are developed and implemented in a largely top-down manner, through a strengthening of laws aimed at preventing the leakage of knowledge and IP to China and talent poaching by China. There is also increased scrutiny regarding adherence to laws. However, measures that tackle foreign interference through Chinese disinformation activities, are often developed by societal organizations, and have a bottom-up character. They are broadly oriented and do not specifically target academia. An initiative that does target students is the "Eight Must-Knowns" document, which warns students who want to study in China for limitations to democratic and academic freedom; it is developed by the Mainland Affairs Council.

Taiwanese measures focus on the identification and mitigation of risks. Efforts to raise awareness are diffuse: with regard to the risks of undesirable tech transfers, awareness raising takes place in the broader context of economic security, disinformation and cyber threats; with regard to academic freedom, they are part of programs that develop resilience against foreign interference in all domains. Many Universities provide information about rules regarding tech transfer and cross-strait relations on their website.

In terms of the practicality of measures, the Safety Control Operation Manual contains detailed rules and provides model forms and questionnaires. Regarding topics such as restrictions on student exchanges with China, practical information is provided on both government and university websites. Cyber security is a vital area in protecting overall national security in Taiwan, but policies in this realm are not specifically addressing the academic research sector. There is no information available on the effectiveness of regulations in Taiwan. However, incidents of infringements of regulations illustrate that Taiwan has strengthened its scrutiny of compliance with laws pertaining to core technologies.

8. UNITED KINGDOM

1. National Context

Within Europe, the UK has a relatively unique HE sector, because of its world renowned universities, which attract large numbers of foreign students and scholars. Furthermore, many research institutes around the globe seek collaboration with UK universities and institutes. Tuition-paying foreign students have become a significant source of income for universities in the UK. Furthermore, domestic R&D investments are relatively limited (1.7% of GDP in 2019, well below the OECD average of 2,5%), which makes attracting foreign research funding more important (OECD). In 2017-2018, 17% of research income came from international sources, while currently 42% of postgraduates and 31% of university staff are from outside the UK (CPNI). The international character of the HE sector means that it is especially vulnerable to knowledge security issues (Interview UK2).

In 2019, a House of Commons committee published an inquiry which found evidence of foreign influence in UK universities, including censorship activities and the harassment and monitoring of students. The committee argued that the sector and government failed to acknowledge this problem (Foreign Affairs Committee 2019). The accusation that universities overly rely on tuition fees from Chinese students makes this issue more acute (The Guardian 2020). Furthermore, intelligence agencies expressed concerns regarding the state-directed theft of intellectual and research property from universities involving Chinese students (The Times 2019).

Several initiatives unfolded in response. Guidelines and recommendations have been developed by several organizations, which are discussed below. The government also adopted a legislative approach. Under the Academic Technology Approval Scheme (ATAS), students and researchers from certain countries who want to study sensitive subjects will have to apply for a certificate. In January 2022, the National Security and Investment Act came into force, which grants the government "the right to scrutinize and intervene in acquisitions made by anyone, including universities, that could harm the UK's national security" (UUK 2022).

The Higher Education (Freedom of Speech) Bill, currently under discussion in parliament, includes an obligation for universities to declare foreign funding over £75,000 from certain countries (Mitchell 2022). Finally, an amendment to the National Security Bill, currently discussed in parliament as well, will introduce a Foreign Influence Registration Scheme. The Scheme's aim is to make clandestine political activity illegal by compelling "those acting for a foreign power or entity to declare political influencing activity – and criminalize those who do not" (Home Office 2022). Although the Scheme does not focus on universities per se, it was in fact initiated in response to the Novichok poisonings in Salisbury in 2018, it could introduce obligations to universities and scholars (Allen & Overy 2022). There is not one overarching term in the UK that is commonly used to refer to knowledge security.

2. Mapping

Major knowledge security initiatives and measures in the United Kingdom

Format(s)	Initiative	Actors
Guidelines and recommendations	Trusted Research Guidance for Academia with additional guidance	Centre for the Protection of National Infrastructure (CPNI)
	Model Code of Conduct for the Protection of Academic Freedom and the Academic Community in the Context of the Internationalisation of the UK Higher Education Sector	Academic Freedom and Internationalisation Working Group (AFIWG)
	Managing risks in Internationalisation: Security related issues	Universities UK (UUK)
	Trusted Research and Innovation Principles	UK Research and Innovation (UKRI)
Laws and regulations	Higher Education Freedom of Speech Bill	Parliament of the United Kingdom
	Foreign Influence Registration Scheme	Home Office
	Academic Technology Approval Scheme (ATAS)	Foreign, Commonwealth & Development Office

Major actors in knowledge security in the United Kingdom

Actors	Actions
Centre for the Protection of National Infrastructure (CPNI)	Advises organizations that are part of the national infrastructure on security issues
Academic Freedom and Internationalisation Working Group (AFIWG)	Work on the protection of academic freedom and engage in advocacy for members of the academic community at risk across the world
Universities UK (UUK)	Advocacy association for universities in the UK
UK Research and Innovation (UKRI)	Government research funding organization
Technology Transfer Office	Supports the knowledge assets of the public sector to deliver value to the UK economy and society.
Research Collaboration Advice Team (RCAT)	Providing research institutions with a first point of contact for official advice about national security risks linked to international research

Trusted Research Guidance for Academia (2022)

These guidelines specifically address international research collaboration. They were first published in 2019, this updated version is from March 2022. The guidelines are developed by the Centre for the Protection of National Infrastructure (CPNI), a government authority which advises organizations that are part of the national infrastructure on security issues. According to one interlocutor, this guidance is the single

most important, universally understood and generally accepted guidance in the UK (Interview UK1).

Considering the tasks of the CPNI, it is not surprising that the Trusted Guidance focuses on preventing undesirable knowledge transfers, more so that on protecting academic freedom. The Guidance itself indicates that it is particularly relevant to "researchers in STEM subjects, dual-use technologies, emerging technologies and commercially sensitive research areas" and is designed to help protect "intellectual property, sensitive research and personal information" (CPNI). The guidance therefore offers mostly advice on issues such as cyber security, export controls and the protection of intellectual property. The main body of the Trusted Guidance is accompanied by a series of supporting documents to promote implementation.

Model Code of Conduct for the Protection of Academic Freedom and the Academic Community in the Context of the Internationalisation of the UK Higher Education Sector

This model code is developed by the Academic Freedom and Internationalisation Working Group (AFIWG), which is part of the Human Rights Consortium of London University, in cooperation with the Council for At-Risk Academics, Scholars at Risk and the University and College Union. AFIWG has used funding from the Economic and Social Research Council to develop the code. Its focus is on protecting academic freedom, which it sees challenged by repressive government, marketisation and "an opportunistic approach to building global ties within the higher education sector". The document states explicitly that these challenges "extend beyond questions of intellectual property and national security", thereby setting it apart from the CPNI guidance. The document lists the general responsibilities of HE institutions and provides recommendations. The Code is also designed to promote the implementation of the UUK guidelines (see below).

Managing risks in Internationalisation: Security related issues (2021)

This guidance was published in 2020 (current version was updated in 2021) by Universities UK (UUK), the main advocacy association for universities in the country. UUK is funded mainly through its 140 member institutions. The association developed the document at the request of the UK Minister of State for Universities and in coordination and cooperation with the government (LAC 2020, p. 44). The guidelines specifically target the governing bodies and executive heads of universities and make it very clear that it is their responsibility to protect their institution, to establish a clear governance structure and identify staff members who will be responsible for managing the risks set out in these guidelines. In order to promote adherence, UUK calls for the governing bodies of HEIs to receive an annual report identifying the risks the institution faces and how these are mitigated.

The guidance acknowledges that there are broadly two aspects of knowledge security, which it defines as (1) "attempts by overseas/hostile/external actors or those acting on their behalf to illegitimately acquire academic research and expertise" and (2) "interfere with academic discourse". While the CPNI and AFIWG each focus on one of these two aspects respectively, the UUK guidance aims to address both. It contains recommendations on protecting the reputation and values, staff and students, campuses, and international partnerships of universities. To clarify each set of recommendations, the guidelines include case studies and links to additional resources. A glossary with definitions of important terms is also included as well as further guidance material, such as guiding questions and a checklist.

Trusted Research and Innovation Principles (2021)

This document was published in 2021 by UK Research and Innovation (UKRI), a government research funding organization. UKRI makes clear that any organization that receives its funding should adopt these principles and be able to provide evidence that suitable measures have been put in place. The principles set out requirements regarding due diligence and the management of information security, sensitive data and intellectual assets. They mostly focus on preventing undesirable knowledge transfers but also address research integrity and ethical standards.

Actors

Research Collaboration Advice Team (RCAT)

The Research Collaboration Advice Team (RCAT) is part of the Department for Business, Energy & Industrial Strategy of the UK government. It is "a collaboration between the government and academia which provides research institutions with a first point of contact for official advice about national security risks linked to international research". An interlocutor pointed out that RCAT provides advice in the early stages of potential research projects. For example, if a university is planning a project with a foreign partner, and this partner turns out to be on an internal government red list, RCAT can advise the university early on to stop the collaboration (Interview UK1). This is in line with what the organization states itself: "RCAT works across government to make national security advice accessible and digestible for the academic community." Its partners include CPNI, UKRI and UUK (RCAT).

RCAT focuses on preventing undesirable knowledge transfer and less on the protection of academic freedom. It supports academics and university leaders to understand risks and to introduce safeguards by promoting awareness of official security policies, laws and regulations and offering risk-management guidance. At the same time, RCAT aims to improve the understanding within the government of how academics encounter and tackle risks, and how the government and academics can work together to improve practices (RCAT). One interlocutor was very positive about this role of RCAT (Interview UK1).

3. Analysis

The national approach to knowledge security in the UK stands out because of its variety of measures and actors. Risks related to undesirable knowledge transfers and academic freedom are both covered, though most guidance (e.g. by CPNI, UKRI, RCAT) predominantly focuses on the first element. Interlocutors have also noted this two-pronged approach. One respondent argued that these elements should indeed be addressed separately and stated that a focus on the first element could lead to the "securitization" of knowledge, which would in turn negatively impact academic freedom (Interview UK2). Another interlocutor looks at both elements as two sides of the same coin, that do not have to be in tension with one another (Interview UK1).

The UK's approach is relatively comprehensive. As in most other countries, the first three steps for safeguarding knowledge security (raising awareness, identifying risks, and mitigating risks) are covered, but little attention is devoted to identifying opportunities. What especially stands out is the many types of actors that are involved in the approach. The government, university managements (via UUK), scholars, unions and civil society organizations have all been involved in drafting guiding material. The approach also contains both top-down (e.g. CPNI) and bottom up (e.g. AFIWG) initiatives.

The level of enforcement among the initiatives is diverse. Guidelines are not strictly enforced from above. However, there are public self-enforcement systems within HEIs that are assessed by the Quality Assurance Agency for Higher Education (QAA). Each university clarifies how it ensures that due diligence practices are in place and other universities call them out if they do not. Such self-regulating control mechanisms within the sector are often organized through organizations such as UUK (Interview UK1). In the case of the AFIWG Code, the aim is not to force universities to adopt the recommendations, but to convince them to engage with the problem (Interview UK2).

Obviously, HEIs and scholars are forced by law to abide by ATAS, and, once they have passed through parliament, also by the Higher Education Freedom of Speech Bill and Foreign Influence Registration Scheme. Furthermore, the UKRI and other funding agencies require HEIs to adopt their principles as a condition for receiving funding (Interview UK1). The move towards more legislation and funding conditions is indicative of a recent shift. In the past, the UK government trusted universities to address knowledge security themselves, while they were assessed from time to time by the QAA. Currently, the government is more directly involving itself through legislation, while funding bodies such as UKRI are more proactive with their guidance (Interview UK1). According to an interlocutor, one reason why the state feels the need to step in, is that individual universities are unwilling to be the first one, for example, to decline funding from a particular party, because they fear this would benefit competitors who do not have to abide by stricter policies yet (Interview UK2).

There appears to be a high level of coherence within the approach. For example, many of the guidelines consistently refer to relevant organizations, regulations, other resources, and one another. This is especially true for the CPNI, UKRI and UUK guidelines. They call upon institutions to make use of the available government support (UUK). UKRI indicates that it works closely with the sector to align policies and coordinate approaches (UKRI). This organization even made a summary in which the key points of the guidelines of UUK, CPNI and UKRI are combined. Another illustration of the coherence is that one university who was developing a training video about export controls received funding from UUK to make it available to all institutions (Interview UK1).

There is also coherence in the engagement between the HE sector and the government. RCAT is especially noteworthy because it creates direct contacts between the two. UUK is also regarded as a strong interface between universities and the government. Such coordination, at least on the topic of security, has improved over the years. According to one interlocutor, the government has learned from other countries how important this is (Interview UK1). On the topic of protecting academic freedom, the level of coordination and coherence is less clear.

Many of the guidelines are relatively practical in nature. They do not only provide many links to supporting materials and organizations, but they also include clear definitions, scenarios, lessons learned, case studies and checklists that make the recommendations more concrete. This facilitates implementation. Furthermore, the UUK guidelines clearly assign responsibility to the governing bodies and executive heads of universities. Implementation is also encouraged by pointing to the reputational and financial damage institutions could suffer when they are not properly addressing security risks (CPNI and UUK guidelines).

Based on the input from interlocutors, risk awareness, risk identification and risk mitigation mechanisms are relatively well developed among universities. Scholars and staff are increasingly understanding the need for such mechanisms. According to

one interlocutor, organizations such as RCAT are important in this process: when more parties make the same case, it becomes more convincing (Interview UK1). In that sense, the approach is effective.

However, less positive aspects have also been reported. For example, one interlocutor expects that because of the Foreign Influence Registration Scheme, some projects will not materialize, simply because it would be too costly to complete all the bureaucratic work (Interview UK1). Furthermore, interlocutors believe that some of the initiatives are driven by (conservative) political agendas instead of real risks (Interviews UK1; Interview UK2). One respondent is also afraid that the securitization narrative could result in interference in academic freedom and McCarthyism, which would make academia overly cautious (Interview UK2). Ultimately, part of the problem is also the fact that the UK's HE sector receives a lot of foreign funding. In order to really address vulnerabilities, funding structures in the sector would have to change, according to one interlocutor (Interview UK2).

9. UNITED STATES OF AMERICA

1. National Context

In recent years the United States (US) Congress and other federal organizations and departments have become increasingly concerned about inappropriate foreign influence at research institutions and universities in the US. This concern has led to a plethora of policies and measures aimed at mitigating security risks posed to the open US academic environment. While the policies are country neutral in name, many are developed with a specific country in mind: China. A long list of reported incidents involving Chinese actors have heightened this concern (GAO 2020; Hoover Institution 2020; US senate 2019; NIH; Wilson Center 2020; FBI 2020).

These developments are largely shaped by the US-China geopolitical rivalry and in particular the US-China rivalry in technology. This battle for leadership in STI, and in particular in core technologies like 5G, semiconductors and artificial intelligence, started during the Obama administration, was intensified during the Trump administration, and has been continued under the current Biden administration, which recently identified China as the "most consequential geopolitical challenge facing America in a post-Cold War era" (National Security Strategy 2022).

The US approach to knowledge security is also shaped by the country's federal structure. Like in Germany, the individual states are responsible for higher education in the US (USDoE). This means that the federal government can only influence higher education and research through funding and national legislation and security regulations.

The US is still the number one performer and collaborator in science, technology and innovation (STI) activities in the world, but this position is increasingly challenged by China. In 2019, the US was the largest spender (27% of the world total) of global research and development (R&D) (US National Science Foundation 2022) and the country is home to many of the world's top universities. However, China, which in 2019 was the second largest spender (22% of the world total) of global R&D, has already overtaken the US in scientific research output and number of researchers (Rathenau Institute 2022).

It is in this context that the US launched, in 2018, the "China Initiative", a programme that aimed to protect the US science and technology enterprise from espionage by China. The programme, run by the US department of Justice, was highly criticized for its unfair treatment of Chinese Americans and residents of Chinese origin, and for its lack of effectiveness. It ended in February 2022 and is to be replaced by a broader programme that will also cover other countries of concern.

Most stakeholders refer to knowledge security in terms of "foreign interference" and "undue" or "inappropriate foreign influences on research integrity". The Office of Science and Technology Policy (OSTP) uses the term "research security" and defines it as: "safeguarding the U.S. research enterprise against the misappropriation of research and development to the detriment of national or economic security, related violations of research integrity, and foreign government interference" (OSTP August 2022).

2. Mapping

Major knowledge security initiatives and measures in the United States

Format(s)	Initiative	Actors
Regulations, guidelines and recommendations	National Security Presidential Memorandum 33 on National Security Policy for United States & Guidance for Implementing National Security Presidential Memorandum 33 (2022, 34 p.)	National Science and Technology Committee (NSTC), Joint Committee on the Research Environment (JCORE) of the White House Office of Science and Technology Policy (OSTP)
	Recommended Practices for Strengthening the Security and Integrity of America's Science and Technology Enterprise (2021, 22 p.)	National Science and Technology Committee (NSTC), JCORE of the White House OSTP
	University Actions to Address Concerns about Security Threats and Undue Foreign Government Influence on Campus (Updated May 2020, 7 p.)	Association of American Universities (AAU) & Association of Public and Land-grant Universities (APLU)
	Framework for Review of Individual Global Engagements in Academic Research (2020)	Council on Governmental Relations
Laws and regulations	Chips and Science Act (2022)	
	National Defense Authorization Act (yearly)	
	Confucius Act (2021)	
	Disclosure requirements NIH Similar for funding agencies, such as DARPA and NASA	National Institute of Health (NIH)
Web portals (examples)	Research Security	National Science Foundation
	Foreign Interference webpages	National Institute of Health
	Science and Security	Association of American Universities (AAU)
	Chinese Talent Program Tracker	Center for Security and Emerging Technology (CSET)

Major actors in knowledge security in the United States

Actors	Actions
Government	
White House Office of Science and Technology Policy (OSTP)	Policies, broad measures and coordination
National Science and Technology Committee (NSTC)	Policies, broad measures and coordination
Department of Education	Reporting Obligations: Foreign Gifts and Contracts Disclosures
Department of Energy	Disclosure requirements for research funding; Directive regarding Foreign Government Sponsored or Affiliated Activities (2020)
Department of Defense	Disclosure requirements for research funding
Department of Commerce	Funding; Unverified List
Federal Funding Agencies	
National Science Foundation (NSF)	Proposal and Award Policies and Procedures Guides (2020); NSF Dear Colleague Research Protection Letter (2019); Jason Report on Fundamental Research Security (2019); Webportal
National Institute of Health (NIH), ACD Working Group on Foreign Influences on Research Integrity	Foreign Interference policies Foreign Interference Report with Recommendations
Defense Advanced Research Projects Agency (DARPA)	Countering Foreign Influence Program (2021)
National Aeronautics and Space Administration (NASA)	Proposers Guidebook (updated 2021)
University Associations	
AAU & American (APLU)	Guidelines; input on government guidelines and regulations
Council on Governmental Relations	Framework for Review of Individual Global Engagements in Academic Research
American Council on Education	Collaboration with international counterparts on safe, secure and sustainable internationalization
Other	
Association of University Export Control Officers (AUECO)	Implementation and training
Academic & Security Counter Exploitation Program (ASCE)	Helps address foreign threats to US academic institutions; works with federal agencies like the FBI

As the tables show, the White House and many federal government departments and federal funding agencies have commissioned or executed research, and issued regulations, guidelines, guiding materials, laws, regulations and/or other communi-

cations on the topic of knowledge security. In addition, associations of universities and higher education organizations have published briefings, guidelines, and guidance materials. Some of the actions discussed below apply specifically to research institutions and others apply more broadly to all recipients of federal funding. Although many government policies and measures are developed in consultation with the academic and research community, they are issued, promoted and executed by the US government, and therefore relatively top-down in character.

In 2021, the US government's National Science and Technology Council (NSTC) published two documents. Firstly, the National Security Presidential Memorandum 33 on "U.S. Government Supported Research and Development National Security Policy" (NSPM-33, 14 January 2021), which is directed at federal research agencies and provides actions that emphasize standardized policies and practices with regard to disclosing information to assess conflicts of interest and of commitment among researchers and research organizations applying for federal research funding.

Secondly, the complementary Recommended Practices for Strengthening the Security and Integrity of America's Science and Technology Enterprise, (January 15, 2021, 22p.) offers 21 recommendations to research organizations covering topics such as: Organizational Leadership and Oversight: Openness and Transparency; Training, Support, and Information; Compliance with regulations; and Potential Risks Associated with Collaborations, including foreign visitors to campus'; and protecting data. It states that the US open research environment benefits the development of science but also emphasizes that research institutions and universities must strengthen research security and academic integrity.

A year later, the NSTC published the Guidance for Implementing National Security Presidential Memorandum 33 on National Security Policy for United States Government-Supported Research and Development (January 2022, 34 pp.). This document provides guidance to Federal departments and agencies regarding their implementation of the above NSPM-33. The Guidance covers five key topics:

1. Suggestions for standardized disclosure requirements for federal funding. The Federal science funding agencies have meanwhile agreed to move towards adopting standardized formats. In August 2022, An Update on Research Security: Streamlining Disclosure Standards to Enhance Clarity, Transparency, and Equity was published, making draft standardized disclosure materials available for public comment and review until October 31st 2022. At this moment, many national organizations that fund research, such as the National Institute of Health (NIH), Defense Advanced Research Projects Agency Disclosure (DARPA) and the National Aeronautics and Space Administration (NASA), each have their own regulations and disclosure requirements: NIH disclosure requirements, NASA Guidelines for Promoting Scientific and Research Integrity, DARPA Disclosures Checklist. Therefore, standardization will be welcomed.
2. Digital Persistent Identifiers (DPI): researchers who receive federal funding must be registered with a DPI service. DPI's should include regularly updated disclosure information and be accessible by research institutions.
3. Consequences for violation of disclosure requirements, varying from administrative and civil, to criminal consequences
4. Information sharing. This concerns information sharing by funding agencies with e.g. law enforcement agencies and the Department of Homeland Security.

5. Security programs. Research organizations receiving federal research funding of US$50 million or more should have a certified research security program in place, the development of which is supported by the government.

The "Guidance" also explicitly states that it seeks to "to ensure that policies do not fuel xenophobia or prejudice" (p. 6). This can be understood as a retraction from the China Initiative policy (see "national context").

Legislation

Many US laws are relevant to the implementation of knowledge security measures; only some of the most relevant recent laws will be highlighted here. The yearly National Defense Authorization Acts (NDAA) bills authorize funding levels and set forth policies for the Department of Defense (DOD), including its research programs. For example, the FY 2020 NDAA called for a National Science, Technology, and Security Roundtable, which brought together individuals from the research agencies, national intelligence, law enforcement, academic research, and business communities and discussed possibilities to find a good balance between the protection of national and economic security and ensuring the open exchange of ideas and the attraction of international talent required to advance US S&T.

The FY21 NDAA addresses disclosure of funding sources in applications for federal research and development awards. It also gives colleges until October 2023 to discontinue Confucius Institute programming or lose eligibility for defense funding. This law complements the Confucius act (2021) or in full the "Concerns Over Nations Funding University Campus Institutes in the United States Act", which denies Department of Education funding to universities that host Confucius Institutes, and that don't comply with new oversight rules and regulations. In June 2022, 104 of the 118 Confucius Institutes that once existed in the US, have closed or are in the process of doing so (NAS 2022). This seems to indicate the above Acts were highly effective, but a recent report by the National Association of Scholars, After Confucius Institutes suggests that further scrutiny is called for as in a considerable number of cases, the institutes have been replaced with similar programs.

The recent Chips and Science Act (2022), seeks to advance US global leadership in new technologies by providing funding to the US science and technology enterprise, but also to protect it by restricting research collaboration with "foreign countries of concern", such as China, Iran, North Korea, and Russia.

Bottom-up initiatives

In 2020, two major bottom-up initiatives were taken by associations of universities. In January, the Council of Government Relations, published the Framework for Review of Individual Global Engagements in Academic Research (2020, 21p). This document does not present a prescriptive approach but provides a structure that aids institutions in analyzing global engagements, assessing potential risks, and developing strategies for mitigation. In May 2020 the Association of American Universities (AAU) and the Association of Public and Land-grant Universities (APLU) jointly published the "University Actions to Address Concerns about Security Threats and Undue Foreign Government Influence on Campus" (Updated May 2020, 7 p.) It presents "effective practices" that universities have developed to tackle foreign interference in areas such as awareness and communications; training of faculty and staff; coordination of activities within universities; risk assessment; cyber security, and data protection; academic freedom; travel safeguards; international visitors at the campus; and export control compliance.

Also worth mentioning is A New Institutional Approach to Research Security in the United States (2021) by the Center for Security and Emerging Technology (CSET). It argues that to effectively protect US research and development, the government should not dominate U.S. research security efforts, but needs to empower frontline researchers as partners and rely less on mandates and punitive tactics. It proposes a new, public-private research security clearinghouse, with leadership from academia, business, philanthropy, and government and a presence in the most active R&D hubs across the United States. CSET also provides a Chinese Talent Program Tracker: a catalog of Chinese State-sponsored initiatives that aim to recruit foreign experts and students to work in positions in government, academia, industry and defense in support of China's strategic civilian and military goals.

3. Analysis

The US national approach is very comprehensive. Taken together, the guidelines and regulations by federal government organizations, funding agencies and associations of universities cover the areas of awareness raising, risk identification, and risk mitigation. They focus on issues such as academic espionage, including theft of intellectual property and diversion of intellectual capital. At a practical level, a particular focus lies on information disclosure by institutions and researchers, recruitment of US scientists into foreign government-sponsored talent programs that focus on critical emerging technologies, and prevention of breaches of integrity in the peer review process. The US also has a security clearance system that restricts who can work on sensitive research. Furthermore, government funding can be cut off for universities and research organizations that fail to report funds received from foreign sources. Most government actions focus on federal funding of research, only some apply to research institution themselves. Though China is seen as posing the biggest risk to knowledge security, most documents are largely country neutral. Some, however, identify countries of concern, including Russia and Iran, or specifically mention China.

The guidelines and guidance materials seek to balance between maintaining an open academic environment and addressing risks. However, the main focal point is on funding US research rather than on identifying opportunities in international collaboration. Many policies are based on and supported by research into foreign interference. Although the approach has a strong top-down character, the academic community is extensively engaged in developing policies and practical tools (Interview US1). A good example is the opportunity provided to the research community to comment upon the draft standardized disclosure forms, to be used by all federal funding agencies.

The enforcement level of policies and regulations, other than export controls, is limited. Most policies provide "guidance", existing of regular engagement and information sharing with the research community; standardization of disclosure information to assess potential conflicts of interest and conflicts of commitment; coordination of the development of researcher digital persistent identifiers; and the development of standards for research security programs. Funding agencies can cut off funding in case of non-compliance.

Taken together, the guidelines and regulations are elaborate, and many measures are of a practical character, providing frameworks for risk assessment, model forms, web portals with online tools and links to government offices as well as associations of universities that provide practical support. Most universities and research institutions take the risks seriously and ensure that obligations to funding agencies and the government are met (Interview US2). They develop policies, stimulate awareness and

organize training activities and support for researchers, enabling them to conduct research without risk of penalties (see e.g. Stanford University's Global Engagement Review Program or Northwestern University's Protecting against Improper Foreign Interference in Research Guidance webpages).

The many actions on knowledge security have resulted in a noodle bowl of regulations and requirements to be navigated by universities and research institutions (Interview US1). As measures are not always coherent and may change quickly, implementation can be challenging for universities and research institutes (Exchange US1). On top of this, intra-agency struggles among federal agencies complicate matters. Nevertheless, in recent years many universities have developed research security programs (University Actions 2020). To what extent these programs are effective in reaching academic staff members is not known. With regard to the implementation of regulations by funding agencies, the GAO report (2020) "Federal Research: Agencies Need to Enhance Policies to Address Foreign Influence" found that "two of the five agencies reviewed do not have agency-wide financial conflict of interest policies, and none of the 5 have non-financial policies (e.g., for researchers with multiple professional appointments)".

Implementation is also hampered by the fact that many scientists in the US are concerned about or disagree with the measures. Concerns focus on a number of weaknesses in US guidelines, such as (MITRE 2020):

- lack of a clear line between proper and improper collaboration;
- lack of knowledge data to make an informed decision;
- lack of process monitoring: many risks arise at later points in the grant-and-research lifecycle;
- lack of coherence
- a focus on specific countries rather than on improper actions, which creates a hostile environment for foreign talent.

Other weaknesses of the US approach include the lack of an authority to regulate research that the government does not perform or fund, or to advise researchers on security issues that do not implicate federal laws or funds. This is relevant as 75% of research in the US is privately funded. Other factors hampering the effectiveness of regulations are a lack of expertise among policy makers of the research environment and its practices; and wariness of restrictions on scientific openness and collaboration (CSET Report 2021). The report recommends empowering researchers as true partners, and proposes a new, public-private research security clearinghouse, with leadership from academia, business, philanthropy, and government, and a presence in the most active R&D hubs across the United States.

ANALYSIS AND CONCLUSIONS

This chapter compares the nine national approaches to knowledge security that were examined. The comparison addresses the elements of (1) Conceptualization and debates on knowledge security; (2) National contexts; (3) Comprehensiveness, focus, and coherence; (4) The roles of government and sector actors and enforcement; and (5) Practicality, implementation, and effectiveness. Finally, the chapter identifies several "best practices" from the case studies.

1. Conceptualization and debates on knowledge security

This study takes the Dutch definition of the term "knowledge security" as the central concept for analyzing the conceptualization and comprehensiveness of approaches in other countries. The broad definition, as used in the Netherlands, refers first and foremost to preventing undesirable transfer of sensitive knowledge and technology but also refers to countering covert activities aimed at influence and interference activities on the part of state actors within the context of higher education and science, and to ensuring ethical research and practices relating to collaboration with individuals and institutions from countries in which fundamental rights are not respected (National knowledge security guidelines). Across the nine countries studied, knowledge security is conceptualized in different ways. Although there is often much light between words and actions, we found that in many cases the wording used to discuss knowledge security reflects the focus and character of the approach, and/or the motivation behind developing an approach.

Australia, and to a lesser extent the Czech Republic, predominantly use the term "foreign interference". In both countries this is reflective of the fact that high-profile incidents of Chinese interference in politics and on campuses were a major motivation to develop policies and regulations. However, although the term in the Czech Republic is mostly understood as interference in academic freedom, in Australia, "foreign interference" is understood as not only covering issues related to academic freedom, but also undesired transfer of knowledge.

Finland and Germany avoid terminology that strongly emphasizes the securitization of international research collaboration. In both countries, various terms are used, and documents often refer to principles and codes that have already been developed by their (associations of) research institutions. In Germany, knowledge security issues are often discussed in the framework of broader concepts such as "freedom of science", which also includes elements such as openness, exchange, internationalism, diversity, equality, responsibility and reflexivity (Bonn Declaration). The Japanese term "research integrity" sounds neutral, but this wording does not reflect the Japanese approach, which is also discussed as an element of economic security.

In the UK and US too, single overarching concepts are lacking. In both countries, the variety of terms reflects a separation between the aims of protecting academic freedom and preventing undesired knowledge transfers. Whereas guidance published by government agencies largely focus on the prevention of undesired knowledge transfers, guidelines developed by the sector also cover the protection of academic freedom. In the US, legislation on the Confucius Institutes is an exception as it explicitly mentions the protection of academic freedom. In the UK scholars and civil society organizations have joined forces to create guidance that specifically addresses the

issue of the protection of academic freedom in the internationalization of the higher education sector.

In France, the dominant term, "Protection of the Scientific and Technical Potential of the Nation (PPST)", mirrors the focus on tackling undesirable technology transfers. Finally, Taiwan is a special case as measures are developed without being discussed in terms of knowledge security, and because societal efforts to protect the Taiwanese population against foreign interference from "undemocratic countries" (read: China) are entirely separated from policies addressing the risks of undesirable tech transfers.

Various interlocutors spoke about the importance of avoiding wording that may strengthen the trend to securitize international collaboration in higher education and research, as this may alienate researchers, negatively affect academic freedom and hamper the development of such collaboration. Others point to the need to provide clarity and call things by their name as prerequisites for the development of focused policies to raise awareness and address the risks.

2. National contexts

In most countries, geopolitical developments, such as the increasing US-China tech rivalry, and the growing foreign interference in higher education and research at home and abroad by autocratic regimes, are the major factors shaping the national approaches to knowledge security. This is specifically true for concerns about Chinese and Russian political interference in the higher education and research sector as well as in society at large. Particularly in Japan, Taiwan, and Australia, the proximity to China figures strongly in the approaches to national and economic security. As one interlocutor said: "In Taiwan a focus on security is of existential importance to survival" (T1). For Finland and the Czech Republic, the same applies with regard to Russia. Therefore, it is not surprising that most national approaches, though state agnostic in name, have been developed with specific countries in mind: China, and to a lesser extent, Russia. It is noteworthy that Finland is the only country with a very recent explicitly China-specific approach to knowledge security, in other countries the most recent documents are state-agnostic. The fact that China is an important driver of knowledge security policies is not just a consequence of geopolitics and US policies aimed at containing China, but also of the prominence of China as a primary academic partner in high-level research in many countries.

In most countries, there is consensus across the political spectrum about the need to address risks of international research collaboration, leading to fairly consistent approaches. When there is a lack of national consensus, this may result in a less coherent approach, as is the case in the Czech Republic, where government actions are not always well coordinated. Domestic political tensions also play a role in the UK and Australia, where interlocutors have pointed out that some initiatives are not only driven by real risks, but also by domestic political agendas.

A second important factor is the level of internationalization of the higher education and research sector. Countries that attract large numbers of foreign students and staff, such as the US, UK, Australia, and Germany have a relatively high sense of urgency and an extensive approach. In countries with globally recognized strong technical universities and research institutes, the issue of undesired knowledge transfers is a prominent issue. In countries with high-profile cases of foreign interference, such as Czech-Republic, Australia, and the US, and/or much consideration in parliament and society for foreign interference, such as the UK and the US, there is relatively

much attention for the need to address violations of academic freedom (see also paragraph 3 below) .

3. Comprehensiveness, focus, and coherence

According to our framework, a comprehensive approach to knowledge security consists of four steps: (1) Raising awareness; (2) Identifying risks; (3) Mitigating risks; and (4) Identifying opportunities. In most countries, the first three steps are largely covered by policies and measures. However, in Finland, where the issue has only recently been put on the agenda, only step one (raising awareness) has been fully completed. In France, the focus is on identifying and mitigating risks, this study found little evidence of broad awareness campaigns in the country. However, it is important to note that in many countries, regulations cover publicly funded research only. This is problematic as much research is privately funded. The French PPST system is an exception as it covers both publicly and privately funded research establishments.

Except for the cases of Germany, Finland and Japan, there is little evidence that countries explicitly seek a balance between risk management and opportunity management within the framework of knowledge security. Policies aimed at expanding and strengthening international collaboration are often developed in an entirely separate track, without referring to risks. The researchers consider this lack of attention for opportunities within the framework of knowledge security a missed opportunity. A lack of coordination between the two tracks may result in different and potentially confusing messages to the research community. Furthermore, the integration of risk and opportunity management may make policies more attractive to the research community. The need for coordination of the two tracks will become more prominent when governments or institutes develop and publish lists of safe and/or unsafe areas for international collaboration, which so far has not yet happened at a national level.

A comprehensive approach to knowledge security includes the element of academic freedom. Although the need to address breaches of academic freedom in research collaboration is often mentioned in policy documents and public debates, this has not resulted in the development of many concrete actions aimed at strengthening academic freedom. One exception is Australia, where the national guidelines explicitly urge universities to provide training on the topic of academic freedom and freedom of speech, as well as to create reporting mechanisms for foreign interference that can result in self-censorship, such as intimidation and harassment. Another exception are policies and measures that scrutinize the functioning of Confucius Institutes, such as in the US. It can be concluded that in general it is challenging to develop integral measures that raise awareness and understanding of academic freedom and to deal with dilemmas that arise from addressing breaches of academic freedom.

The coherence of a national approach is often related to the level of coordination between government offices themselves and between the government and the research sector. In turn, coherence has an impact on implementation and effectiveness. The better stakeholders communicate and coordinate, the more coherent the policies and guidelines produced by different types of actors. A great example is the UK, where guidelines developed by a government security organization, an association of universities, and a research funding agency are aligned with, and provide cross-references to, one another. The Australian approach is coherent on paper as guidance material, policies, legislation, and agencies are developed through UFIT (see case) and often refer to one another. However, some interlocutors said that coordination between government offices and between government and the sector still needed to be strengthened.

The approaches of the Czech Republic and US lack coherence and/or continuity. The Czech guiding documents hardly refer to one another, and successive governments have different views on the urgency of addressing knowledge security. In the US, the lack of coherence is a result of the great number of measures and sometimes rapid introduction and withdrawal of measures, and less of domestic politics as there is a bipartisan agreement on the need to address knowledge security.

4. The roles of government and sector actors and enforcement

There is a wide variety among the national approaches in terms of the structure in which initiatives and measures are developed and put forward. On one side of the spectrum are Japan, and to a lesser extent France and the Czech Republic, which can be characterized as having a primarily top-down structure as their approaches primarily consist of government instructions and guidelines. On the other side of the spectrum is Finland with an approach that is based on informal roundtables. In Germany too, the sector itself plays a dominant role in developing guidelines and tools, something that is largely explained by the fact that the federal government has no mandate in the area of higher education and state level ministries do not always have the capacity to extensively deal with issues of knowledge security. In the middle of the spectrum are the national approaches of Australia, the UK, Taiwan, and the US, which consist of both top-down measures, including specific legislation, and bottom-up initiatives by the sector, or in the case of Taiwan by societal actors.

The character of the overall structure of an approach is not always telling of the level of coordination between the government and the sector. In France, the US, and to a lesser extent in Japan, measures that are put forward and implemented in a top-down manner often have been developed in collaboration with sector representatives. In some countries, such as Australia, Finland and the UK, special organizations facilitate direct communication and coordination between the two sectors, something that is often highly appreciated by all stakeholders. Some interlocutors indicate they would welcome even more coordination with or receive clearer instructions from the government through such intermediating organizations. In the case of the Czech Republic and Taiwan, we have not found sufficient information about the extent to which the government and sector coordinate their efforts.

There is considerable variety in the level of enforcement of measures between and within national approaches. Especially in France, the UK, the US, and Australia, the government has opted for a largely or partially legislative approach, for example by introducing registration obligations for certain types of international collaboration (Australia), disclosure or reporting obligations for researchers and research institutes that apply for public funding for research projects (US and UK), screening obligations for contracts (France) or governance regulations for Confucius Institutes (US). While guidelines are technically not legally enforced, universities can be strongly urged to adopt guidelines because of peer monitoring and peer pressure. Furthermore, in the UK and Australia, official quality assurance agencies or accreditors do an audit of the implementation of knowledge security policies at higher education and research institutions.

5. Practicality, implementation, and effectiveness

The countries examined have not yet conducted official and comprehensive evaluations of their knowledge security initiatives. This may be due to the fairly recent introduction of policies and measures. In Australia and France, measures have been reviewed through a parliamentary inquiry and a senate report respectively. This lack of overall evaluations makes it difficult to draw conclusions about the effectiveness

CONCLUSION

of approaches. Instead, based on circumstantial evidence such as assessments by interlocutors, attendance of activities aimed at raising awareness, university webpages, we present some cautious and general observations.

In view of the broad engagement of the sector in developing policies and the many events organized for the education and research community, the approaches of Australia, Finland, Germany, the UK, and the US seem to have contributed to raised levels of awareness of risks of international collaboration. Regarding the implementation of risk identification and mitigation mechanisms, the French international contract screening mechanism has led to concrete results in terms of number of contracts screened. The caveat here is that there is no information available about how extensive the screening is carried out. In countries with organizations that facilitate direct communication between the government and the sector, such as UFIT (Australia), the China Roundtable (Finland) and RCAT (UK), stakeholders are positive about the achievements and roles of these organizations in facilitating coordination and promoting coherence.

There is often a link between the coherence and practicality of an approach and its effectiveness. Legislation and guidelines are more easily implemented and adhered to if they: provide clear and detailed instructions; are accompanied by easily accessible guidance material and concrete practical support by government or funding agencies; and are aligned and supportive of each other. In some countries, such as Australia and the UK, coherence is relatively strong. Their guidelines and measures are also detailed and concrete, and come with extensive supporting material, such as best practices, case studies, and checklists. In France and Taiwan, the combination of narrowly focused measures that provide clear instructions similarly promotes implementation. Various interlocutors indicate that enforcement and/or strong guidance regarding compliance contribute to the actual implementation of guidelines at universities and research institutes.

SUGGESTIONS AND BEST PRACTICES

Reports as well as exchanges with interlocutors have pointed towards ways in which the implementation of knowledge security measures can be improved. First, competition between universities for foreign funding or students may hinder effectiveness. Interlocutors have indicated that universities are not always willing to share details about their approach with peers at other research institutes or are reluctant to be the first one to embrace stricter measures, because of the competition for international funding and students. Secondly, they mention that government support for building capacity for dealing with knowledge security, both in terms of human resources and expertise, would help universities to implement risk assessment frameworks. Thirdly, since the type of risks vary greatly between individual universities and between disciplines (e.g. STEM and humanities), some respondents have pointed to the ineffectiveness of developing a singular approach that lumps protection of academic freedom and prevention of undesirable knowledge transfers together. They find it hard to implement measures at their individual institutions based on general recommendations and argue that separate guidance and measures could be beneficial. However, other interlocutors emphasize the need of an integral approach that encompasses tech transfer, ethical research as well as academic freedom, because values underpin all academic activity, no matter the field of science. In an additional suggestion, an interlocutor mentioned that pointing to the reputational damage that universities risk if they do not consider risks of international collaboration could help convince them to implement guidelines and measures.

Best practices

This study concludes with a brief overview of best practices that may provide inspiration for other countries, including the Netherlands.

- The establishment of organizations that facilitate direct communication and coordination between the government and the higher education sector (such as those in Australia, Finland and the UK). This measure has been very positively reviewed in reports and by interlocutors. In some cases, such bodies specifically bring security and intelligence agencies together with universities. Furthermore, such collaboration provides the sector with the opportunity to demonstrate their capabilities to self-regulate.
- Another best practice, related to the one above, is the creation of opportunities for the higher education sector to develop bottom-up activities and measures, as has been the case in, for example Germany, Finland and the UK. An explicit invitation or financial support for involvement of the sector in developing measures can contribute to greater acceptance of other initiatives within the national approach to knowledge security that have a more top-down character.
- German efforts to integrate measures regarding knowledge security into existing frameworks are inspiring for three reasons: their effort-saving procedures, the aim to avoid a strong securitization of international research collaboration; and a potentially greater acceptance by the research sector. The approach is based on the idea that everything that needs to be done to address knowledge security risks is already laid down in longstanding codes of conduct for ethical or responsible research, and that there is no need for new and specifically developed measures and regulations; revision and expansion of existing texts may be sufficient. In a similar vein, the issue of protecting academic freedom is viewed as an element

of the broader concept of "freedom of scientific research", as laid down in the Bonn Declaration. A caveat here is that this approach may lack clear messaging towards the community about new risks in collaboration, arising from geopolitical developments.

- Pro-active investment in global collaboration and coordination with regard to developing principles of research security and measures that address infringement of scientific research security, through e.g. the G7 Working Group on the Security and Integrity of the Global Research Ecosystem (SIGRE) (Germany and Japan). This can be considered a best practice because ultimately, science has no borders, and common principles, standards and procedures may facilitate international application of measures. Furthermore, a strengthening of exchange of best practices across the international research community increases mutual learning and provides inspiration. This study has also found that various like-minded countries are already learning from each other's national approaches.
- The French approach of restricting (physical) access to certain research facilities instead of restricting visa for certain students and researchers can be considered a best practice for its avoidance of profiling students and researchers from specific countries.
- The French approach to government screening of all international research collaboration contracts relieves universities of the burden to conduct an in-depth investigation of potential partners and weigh different and contradictory interests (e.g. university interests versus national interests). Furthermore, in case of a negative evaluation, the fact that it was the government that advised negatively may help preserve the relationship with the potential partner concerned.