OECD publishing

INTEGRITY AND SECURITY IN THE GLOBAL RESEARCH ECOSYSTEM

OECD SCIENCE, TECHNOLOGY AND INDUSTRY
POLICY PAPERS
June 2022 **No. 130**

OECD
BETTER POLICIES FOR BETTER LIVES

This paper was approved and declassified by written procedure by the Committee on Scientific and Technological Policy on 15/05/2022 and prepared for publication by the OECD Secretariat.

Note to Delegations:

This document is also available on O.N.E under the reference code: DSTI/STP/GSF(2021)11/FINAL

Integrity and security in the global research ecosystem

Responsibilities for research integrity and security are distributed across multiple actors in the international research ecosystem. These include, national governments, research funding agencies, research institutions, universities, academic associations, and intergovernmental organisations. This report describes policy initiatives and actions from these different actors to safeguard national and economic security whilst protecting freedom of enquiry, promoting international research cooperation, and ensuring openness and non-discrimination. It includes examples of actions that are being taking to prevent foreign interference, manage risks, and help ensure trust in science in the future, and offers recommendations to help countries develop effective policies to strengthen research security as part of a broader framework of research integrity.

Foreword

Scientific discovery occurs in an interconnected, international ecosystem that collectively leverages intellect, know-how, talent, financial resources, and infrastructure from around the world. Freedom of scientific research and international collaboration are cornerstones of scientific progress. Open and transparent communication and dissemination of scientific information and data and sharing of research materials are essential for the global science ecosystem to operate effectively. Global challenges like the COVID-19 pandemic, climate change and other complex socio-economic issues cannot be tackled without international research collaboration.

However, new challenges and threats are emerging as some governments and non-state actors exhibit increasingly forceful efforts to unfairly exploit and distort the open research environment for their own interests. Many countries now consider unauthorised information transfer and foreign interference in public research as a serious national and economic security risk and a threat to freedom of scientific research.

The COVID-19 pandemic was declared early in 2020 and it quickly became apparent that international research collaboration and sharing of data and information would be critical for managing this global crisis. However, as the true scale of the pandemic became apparent, issues around access to scientific knowledge and technologies were increasingly influenced by geopolitical considerations. Research security became a live issue for the research and policy community as countries strived to protect their interests and control over access to vaccines and other therapeutic developments. The integrity of the global research ecosystem was threatened, while trust in science decreased for important sectors of the population in many countries.

As the pandemic progressed, with science in the spotlight, the OECD Global Science Forum launched a project in October 2020 on “Integrity and Security in the Global Research Ecosystem” (see Annex B for Terms of Reference). As indicated by the title, there was recognition from the outset that the integrity and security of research are intertwined and need to be considered together. Likewise, the inherently international nature of public research is embedded across the project. Hence, the aim of the project was to identify good practices to safeguard national and economic security whilst protecting freedom of enquiry, promoting international research cooperation, and ensuring openness and non-discrimination.

As this project reached completion, in the first months of 2022, Ukraine was subjected to large-scale military aggression by Russia. Universities and public research institutions across the OECD have been obliged to re-visit their ties with both of these countries. Many have chosen to cease collaborations with Russian institutions and/or taken measures to accommodate refugee scientists from Ukraine. Hopefully these actions will only need to be temporary but they clearly illustrate again the influence of geopolitical considerations on research and the highly dynamic nature of security concerns. Today’s allies or friends can quickly be perceived as tomorrow’s threats. In the midst of this complex and rapidly changing world, maintaining the integrity and security of the global research ecosystem is perhaps more pertinent now than it has been before. It is not always an easy topic to discuss, and there are strongly held and often polarised views, but it is an issue that cannot be ignored.

This report identifies and analyses good practices to safeguard national and economic security whilst protecting freedom of enquiry, promoting international research cooperation, and ensuring openness and non-discrimination. Responsibilities for research integrity and security are distributed across multiple actors in the international research ecosystem. These include national governments, research funding agencies, research institutions, universities, academic associations, and intergovernmental organisations. The report provides practical information and guidance for each of these actors. The good practice examples in the report are also being made available in an online monitoring tool of governments' STI policy initiatives relating to research security (https://stip.oecd.org/stip/).

Acknowledgements

An international Expert Group (EG, see Annex C) was established, through nominations from GSF delegates, to oversee and implement this project. This final policy report is the product of that Group's work. It was drafted by the OECD-GSF Secretariat, Yoshiaki Tamura and Carthage Smith, with input from all EG members. In addition, a number of other individuals made important contributions. This includes more than 30 experts, who participated as presenters or panellists in two dedicated project workshops that focused on identifying challenges and good practices. These events were attended by around 150 representatives from national governments, research funding agencies, research institutions, universities, academic associations, and international organisations from more than 30 countries.

Table of contents

Tables

Figures

Boxes

1 Executive summary

Scientific discovery occurs in an interconnected, interdisciplinary, and international ecosystem that collectively leverages intellect, know-how, talent, financial resources, and infrastructure from around the world. Freedom of scientific research and international collaboration are cornerstones of scientific progress. Open and transparent communication, dissemination of scientific information and data, and sharing of research materials are essential for the global science ecosystem to operate effectively.

However, new challenges and threats are emerging as some governments and non-state actors exhibit increasingly forceful efforts to unfairly exploit and distort the open research environment for their own interests. Several OECD countries now consider unauthorised information transfer and foreign interference in research as a serious national and economic security risk and a threat to the freedom of scientific research. This has important implications for several core aspects of research, including international collaboration, research training, recruitment, and peer review of grant proposals. If not carefully managed, security risks can seriously damage the health and effectiveness of the international research ecosystem and undermine trust in research findings.

This report is based on an analysis of publicly available documents and additional information collected from a group of 13 OECD countries represented on an expert group, which oversaw the work (see Annex C). It also includes the outcomes of two dedicated international workshops. The report identifies and analyses good practices to safeguard national and economic security whilst protecting freedom of enquiry, promoting international research cooperation, and ensuring openness and non-discrimination.

Responsibilities for research integrity and security are distributed across multiple actors, operating at different scales, in the international research ecosystem. These include national governments, research funding agencies, research institutions, universities, academic associations, and intergovernmental organisations. Many of these actors are already taking measures that provide a sound basis for future policy development, although there is considerable potential for mutual learning across sectors and countries.

At the national government level, regulations exist already in several countries to control sensitive information. In order to comply with these, research institutions, universities, and researchers may be legally required to disclose conflicts of interest (COI) and conflicts of commitment (COC). Governments have developed guidelines and checklists to increase awareness of risks to research security and integrity, and these are frequently accompanied by policies and measures for mitigating the risks. In some countries, intelligence agencies, law enforcement agencies, research institutions, and universities have increased cooperation and information exchange to help researchers identify and manage risks and strengthen security in international collaboration.

At the funding agency level, guidelines can help define and manage COI and COC for funding applicants, peer reviewers, and research agency staff. Several funding agencies have integrated risk assessment and management into their funding application and review processes. Applicants are asked to complete risk assessment questionnaires and to work with agencies and host institutions to develop risk mitigation plans if they identify national and economic security risks.

Public research institutions (PRIs) are developing tools to systematically assess the risks of foreign interference and inform decisions on new research opportunities. Researchers and contractors at some

PRIs have been prohibited from working in specific foreign government-sponsored or affiliated activities, including some talent recruitment programmes, where these have been assessed to be of high risk.

In universities, rules and guidelines are being developed to mitigate risks to research security and protect the integrity and freedom of scientific research. Some universities have established dedicated committees or structures to manage research security risks and provide research security training to raise awareness among researchers and administrative staff. University associations have carried out surveys to identify and raise awareness of the various practices that universities are implementing to ensure research security.

Academic associations are developing consensus guidelines for their members and the broader research community. Some academic associations organise workshops to raise awareness among researchers and share experiences. Others have established local committees to advise research institutions and universities. In some instances, they also advise national governments on appropriate policy actions that balance research security and scientific freedom considerations.

At the intergovernmental level, the G7 countries have established a working group on the security and integrity of the research ecosystem and are planning to develop a common set of principles to help to protect the research and innovation ecosystem from risks to open and reciprocal research collaboration. The European Commission published a toolkit in early 2022 on how to mitigate foreign interference in research and innovation.

Building on what is ongoing, this report lays out seven over-arching recommendations, each of which requires actions from a variety of actors:

1. Underscore the importance of freedom of scientific research and international collaboration as a key element of the global research ecosystem
2. Integrate research security considerations into national and institutional frameworks for research integrity
3. Promote a proportionate and systematic approach to risk management in research
4. Promote openness and transparency in relation to conflicts of interest or commitment
5. Develop clear guidelines, streamline procedures, and limit unnecessary bureaucracy
6. Work across sectors and institutions to develop more integrated and effective policy
7. Enhance international information exchange on research integrity and security

These recommendations, including suggestions for specific actions, are laid out more fully in the next section of this report.

2 Policy recommendations and options for action

The following recommendations emerged from the survey of countries and discussions at two international workshops that were conducted in this project. Although research integrity and security are common concerns across OECD countries, the context varies considerably. Hence, the priority attached to each policy recommendation and the related options for action is likely also to vary across countries. More specific information and examples of what different countries are already doing to address these recommendations are included in Section 6 of this report.

2.1. Underscore the importance of freedom of scientific research and international collaboration as a key element of the global research ecosystem

Freedom of enquiry and international collaboration constitute an essential part of scientific research and are enshrined in a number of formal and informal recommendations and declarations from international organisations. Geopolitical tensions and the behaviour of governments can undermine scientific freedom and international collaboration and create real or perceived xenophobia or prejudice.

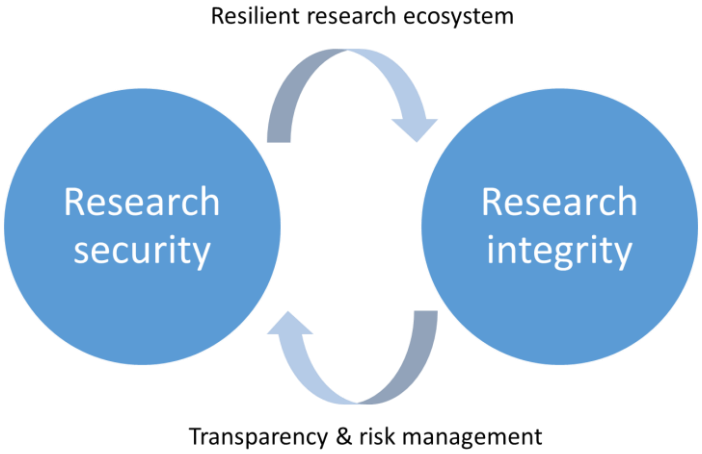
- Governments should promote international collaboration, whilst taking a proportionate risk management approach to security issues. In this context, international mobility and the recruitment of foreign researchers should be recognised as an essential part of international collaboration.
- Research institutions and universities should maintain welcoming and inclusive environments, in which freedom of scientific research and science communication is respected and all people are treated equally, regardless of race or national origin.

2.2. Integrate research security considerations into national and institutional frameworks for research integrity

As international collaboration becomes more widespread and the geographic distribution of scientific production changes, mitigating unauthorised information transfer and foreign interference needs to be included in considerations of research integrity and scientific responsibility (see Figure 2.1 and Annex A).

- Security and risk management should be integrated into institutional culture and processes as an essential aspect of research integrity. To help achieve this, governments, funding agencies, research institutions, universities, and academic associations can, for example, organise dedicated workshops or develop education and training programmes (see examples in 6.1.2, 6.5.3, and 6.7).
- Countries can expand the remit of national research integrity offices, where these already exist, or may wish to establish a dedicated national contact point or centre of expertise for research security within government to work with counterparts across the research ecosystem (see examples in 6.1.2).

Figure 2.1. Research integrity and research security



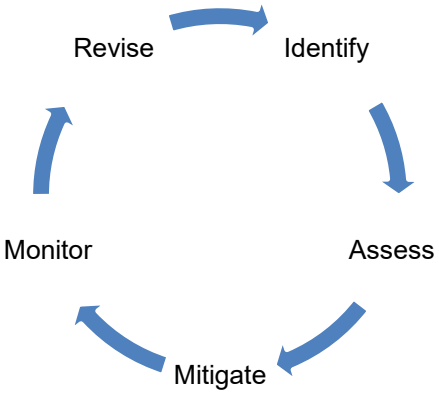
Strengthening research integrity by increasing transparency, disclosing potential Conflicts of Interest (COI) and Conflicts of Commitment (COC) and managing risks, will protect research security. Research security - preventing foreign state or non-state interference with research - will in turn strengthen research integrity.

2.3. Promote a proportionate and systematic approach to risk management in research

Risk management needs to acknowledge freedom of scientific research on the one hand, and security considerations, on the other hand. Policies and actions to address research integrity and security should be based on sound risk identification and assessments and be regularly revisited and revised as necessary. Not every research institution or research project will face the same level or type of risk. Maintaining institutional autonomy in risk management and decision making is key not only to effectively identifying risk but also to gaining crucial buy-in across the research sector.

- Science and security agencies need to develop trusted processes that ensure regular exchanges of information and promote mutual understanding of the benefits and risks of international collaboration (see examples in 6.1.3).
- Governments should encourage responsible self-management (self-policing) by universities and professional associations and support capacity building to better understand, identify, and mitigate potential risks (see examples in 6.1.2).
- Governments, funding agencies, research institutions, and universities need to regularly assess the maturity of their security strategies and adjust policy initiatives or actions to ensure effectiveness (see Figure 2.2). It is important to monitor for unintended consequences, including discrimination against specific population groups and ethnic profiling or reductions in research collaborations.

Figure 2.2. Risk management cycle



Risk management includes risk identification, assessment, and mitigation. Risk mitigation measures should be proportionate to the likelihood and potential impact of risks. After implementing risk mitigation measures, positive and negative effects need to be monitored and mitigation measures may need to be revised accordingly.

2.4. Promote openness and transparency in relation to conflicts of interest or commitment

It is not always easy to recognise and avoid potential COI and COC while collaborating internationally. It is important to clarify requirements for disclosure of potential COI and COC and establish processes that support transparency and help manage risks.

- Governments should work collaboratively with research providers, including universities, to raise awareness of research security issues and clearly communicate what information research providers and researchers are required or expected to provide (see examples in 6.1.2, 6.1.3, 6.2.2, and 6.5.3).
- Funding agencies, research institutions, and universities need to establish clear and transparent systems to ensure that researchers declare information about COI and COC and potential research security risks. Checklists or toolkits can be helpful resources to guide the risk identification and mitigation process (see examples in 6.2).
- Universities, research institutions and individual researchers should implement transparent processes to ensure due diligence when establishing research partnerships. In addition to assessing the risks for new projects, ongoing projects must be monitored (see examples in 6.3, 6.5.1, and 6.5.2).

2.5. Develop clear guidelines, streamline procedures, and limit unnecessary bureaucracy

Governments, funding agencies, research institutions, and universities need to develop simple, clear, and unambiguous guidelines that are targeted at specific risks to avoid unnecessarily burdening researchers.

National governments and funding agencies should limit additional administrative burden related to security measures and, where possible, leverage existing processes. Confusing, complicated, and burdensome rules are unlikely to be effective and can have a negative impact on the development of research.

- New procedures for ensuring research security may be required but, in so far as it is possible, the procedures should be harmonised with existing procedures and/or structures (see examples in 6.1.1, 6.2.3, 6.3, and 6.5.2).
- Universities and research institutions should establish transparent processes to help researchers navigate the policy landscape and minimise the burden of new regulations and guidance. Engaging researchers in the development of policies can help improve their effectiveness (see examples in 6.3 and 6.5.2).

2.6. Work across sectors and institutions to develop more integrated and effective policy

Different stakeholder actions need to be coordinated effectively for mutual benefit. Research integrity and security is relevant across many government policy areas (see Box 2.1). At the same time, research integrity and security engage multiple stakeholders outside of ministries, including funding agencies, research institutions, universities, and individual scientists. This complexity can make it challenging to agree on responsibilities and actions to protect research integrity and security.

- Governments can establish coordination structures that bring together different ministries or departments with an interest in research security. Such structures can play an important consultation and communication role and advise on and monitor relevant policy initiatives (see examples in 6.1.1 and 6.1.3).
- Ministries or agencies responsible for education, science and innovation need to facilitate collaboration and exchange of information among the different actors in the research ecosystem (funding agencies, research institutions, universities, and the academic research community) while at the same time liaising closely with other governmental bodies (see examples in 6.1.3).
- Research institutions and universities should share information on research security issues and the cases that they are confronted with, both within their own institution and with other research institutions and stakeholders in the research ecosystem (see examples in 6.4 and 6.7).

Box 2.1. Policy areas related to research integrity and security

Civil security

Cybersecurity

Defence and intelligence

Education

Foreign investment

Immigration

Innovation and intellectual property rights (IPR)

Law enforcement

Privacy and data governance

Science

Trade and export control

2.7. Enhance international information exchange on research integrity and security

Scientific progress depends on international collaboration and open sharing of data and information. It is in all countries' best interests to work together to build mutual understanding and strengthen collective approaches to research integrity and security.

- Governments, funding agencies, research institutions, and universities need to organise international dialogues to exchange information on challenges and good practices relating to research integrity and security (see examples in 6.8).
- Research integrity and security issues should be explicitly considered in developing scientific cooperation agreements between national governments, funding agencies, research institutions, and universities.
- OECD and other international organisations with a remit for science, technology, and innovation (STI) policy, should work with countries to promote exchange of information and policy development on research integrity, research security, and international collaboration (see examples in 6.8).

3 Introduction

Scientific discovery occurs in an interconnected, interdisciplinary, and international ecosystem that collectively leverages intellect, know-how, talent, financial resources, and infrastructure from around the world. Freedom of scientific research and international collaboration are cornerstones of scientific progress. Open and transparent communication and dissemination of scientific information and data and sharing of research materials are essential for the global science ecosystem to operate effectively.

However, new challenges and threats are emerging as some governments and non-state actors exhibit increasingly forceful efforts to unfairly exploit and distort the open research environment for their own interests. A number of OECD countries now consider unauthorised information transfers and foreign interference in research as a serious national and economic security risk (JASON, 2019[1]; D'Hooghe and Lammertink, 2020[2]; Australian Security Intelligence Organisation, 2020[3]) as well as a threat to freedom of scientific research. This has important implications for a range of activities that are critical for the research enterprise, including international collaboration, research training, recruitment, and peer review of grant proposals. Security risks, if not carefully managed, can damage the health and effectiveness of the international research ecosystem and undermine trust in research findings.

It is in response to these concerns that the OECD Global Science Forum (GSF) agreed in 2020 to initiate a project on "Integrity and security in the global research ecosystem." This project aimed to identify good practices to safeguard national and economic security whilst protecting freedom of enquiry, promoting international research cooperation, and ensuring openness and non-discrimination (see Annex B for the full terms of reference). It was overseen by an international Expert Group, who assisted with the collection of information and case examples. This country specific information was supplemented by a desk-top analysis of publically available documents and two dedicated international workshops that focused on good practices that national governments, funding agencies, research institutions, universities, international research projects and infrastructures, and academic associations are implementing.

Research integrity is synonymous with good research practice and the behaviour of individual scientists and, as such, can encompass a range of issues including ethics and the prevention of individual misconduct (e.g. fabrication, falsification, and plagiarism). However, this project focuses on strengthening the integrity of the research ecosystem, with a particular focus on mitigating national and economic security threats and foreign interference with freedom of scientific research. It concentrates on the roles and responsibilities of Governments – including research agencies – and public research providers – including research institutions and universities- in making the global research ecosystem more resilient to risks to its integrity and security. In so doing, the project aims to be country-agnostic and recognises that different perceptions of national security risks are influenced by geopolitical considerations that change over time.

This report is structured with the policy recommendations at the front (section 2) immediately after the Executive Summary. Following a brief introduction and glossary, the rest of the report then provides the context and rationale for these recommendations. Section 4 explores how international collaboration is increasing and contributing to science and society and summarises existing frameworks for international research collaboration. Section 5 explores the relationship between research integrity, research security and international collaboration, which are the three key interacting themes of this report, and the security and foreign interference challenges that countries are concerned about. Section 6 describes policy initiatives and actions that countries are implementing to address research integrity and security concerns.

Box 3.1. Glossary

One of the challenges in discussing research integrity, research security and associated concepts, is that definitions differ across countries and communities. To build a common understanding and avoid misinterpretation, it is important to have shared definitions of key terminology. The 'working definitions' that are used throughout this document are briefly summarised below. A longer discussion of the nuances and different perspectives regarding some of these key terms is presented in Annex A.

Conflicts of interest (COI) & conflicts of commitment (COC)

A conflict of interest is a set of circumstances that create a risk that professional judgment or actions regarding a primary interest will be unduly influenced by a secondary interest (American Association of University Professors, 2014[4]; UK Research and Innovation, n.d.[5]). A conflict of commitment is a situation in which an individual accepts excessive workloads or conflicting duties from multiple employers (Office of Science and Technology Policy, 2020[6]).

Detrimental research practices

Detrimental research practices are actions that violate traditional values of the research enterprise and that may be detrimental to the research process (Committee on Responsible Science et al., 2017[7]). Detrimental research practices include misrepresentation, breach of duty of care, and improperly dealing with allegations of misconduct (Purdue University, n.d.[8]). Theft, deception, and coercion are detrimental research practices that are more directly of concern in relation to research security (see Section 5).

Dual-use research of concern

Dual-use research of concern can (based on current understanding) be reasonably anticipated to generate knowledge or technology that has the potential to be exploited to purposely cause harm and threaten public health or national security, although the research itself is conducted for beneficial purposes (Public Safety Canada, 2020[9]; BBSRC, MRC and Wellcome Trust, 2015[10]).

Due diligence

Due diligence is analysis of an organization done in preparation for a transaction with that organisation (Merriam-Webster, n.d.[11]). In international research collaboration, due diligence includes enquiry into a partner's past activities, the sector that it operates in, commercial and ethical standing of its governing body, and the legal and regulatory environment of the partner (Universities UK, 2020[12]).

Freedom of scientific research

Freedom of scientific research encompasses the right to freely define research questions, choose and develop theories, gather empirical material, devise and employ sound academic research methods, to question accepted wisdom and bring forward new ideas. It entails the right to share, disseminate, and publish research results openly, including through training and teaching. It is the freedom of researchers to express their opinion without being disadvantaged by the system in which they work or by governmental or institutional censorship and discrimination. It is also the freedom to associate in professional or representative academic bodies and associated scientific meetings (Ministerial Conference on the European Research Area, 2020[13]).

Foreign interference vs foreign influence

Foreign interference is carried out by, or on behalf of a foreign actor and is contrary to national sovereignty, values, and interests. It is coercive, covert, deceptive, or corrupting. This is in contrast to foreign influence, which is part of normal diplomatic relations and is normally conducted in an open and transparent manner (University Foreign Interference Taskforce, 2021[14]). Whilst it can be useful in some circumstances to make the distinction between interference and influence, the line between these two is not always clear.

Knowledge security

Knowledge security means preventing the unauthorised transfer of knowledge and technology. It also includes preventing covert influence by state actors on higher education and research, which can impair the freedom of scientific research either directly or via self-censorship.

Open Science

Open Science can be defined as efforts by researchers, governments, research funding agencies or the scientific community to make the primary outputs of publicly funded research results – publications and the research data – publicly accessible in a digital format with no or minimal restriction as a means for accelerating research (OECD, 2015[15]). Broader definitions emphasise a closer relationship between science and society as part of Open Science.

Reciprocity

Reciprocity is the practice of exchanging research materials, outputs, and knowledge in a manner that benefits all collaborating partners. It is necessary for effective cooperation because it helps to ensure that cooperation is mutually beneficial even if there may be asymmetries in the capacity of research partners to reciprocate cooperation or exploit its benefits.

Research ecosystem

Research systems involve different actors, including research funders, different types of research institutions and universities and individual researchers. These actors are interdependent, operating together in a dynamic ecosystem. Policy frameworks and formal or informal rules, norms and standards are all critical aspects of the governance of research ecosystems, which operate at different scales from local to global. The global research ecosystem is characterised by interactions between actors in different countries that have different national interests.

Research integrity

Research integrity is an overarching term that refers to the ethos of research (Sutrop, Parder and Juurik, 2020[16]). Integrity may be attributed to individual researchers, but also to institutions or the entire research ecosystem. In this project, “research integrity” refers specifically to certain values, norms, and principles that constitute good scientific practice (freedom of scientific research, openness, honesty, accountability, etc.) and regulate international research collaboration (reciprocity, equity, non-discrimination, etc.). These apply to individual researchers, research institutions and science as a social system, and to every stage of the research process (see Figure 2.1).

Research misconduct

Research misconduct can be narrowly defined as fabrication, falsification, or plagiarism (FFP) in proposing, performing, or reviewing research, or in reporting research results. Fabrication is making up data or results and recording or reporting them. Falsification is manipulating research materials,

equipment, or processes, or changing or omitting data or results such that the research is not accurately represented in the research record. Plagiarism is the appropriation of another person's ideas, processes, results, or words without giving appropriate credit (Office of Science and Technology Policy, 2000[17]).

Research security

In a globalised research ecosystem, ensuring research security means preventing undesirable foreign state or non-state interference with research. The main goal of research security is to protect the research ecosystem and thus protect legitimate national and economic interests (see Figure 2.1).

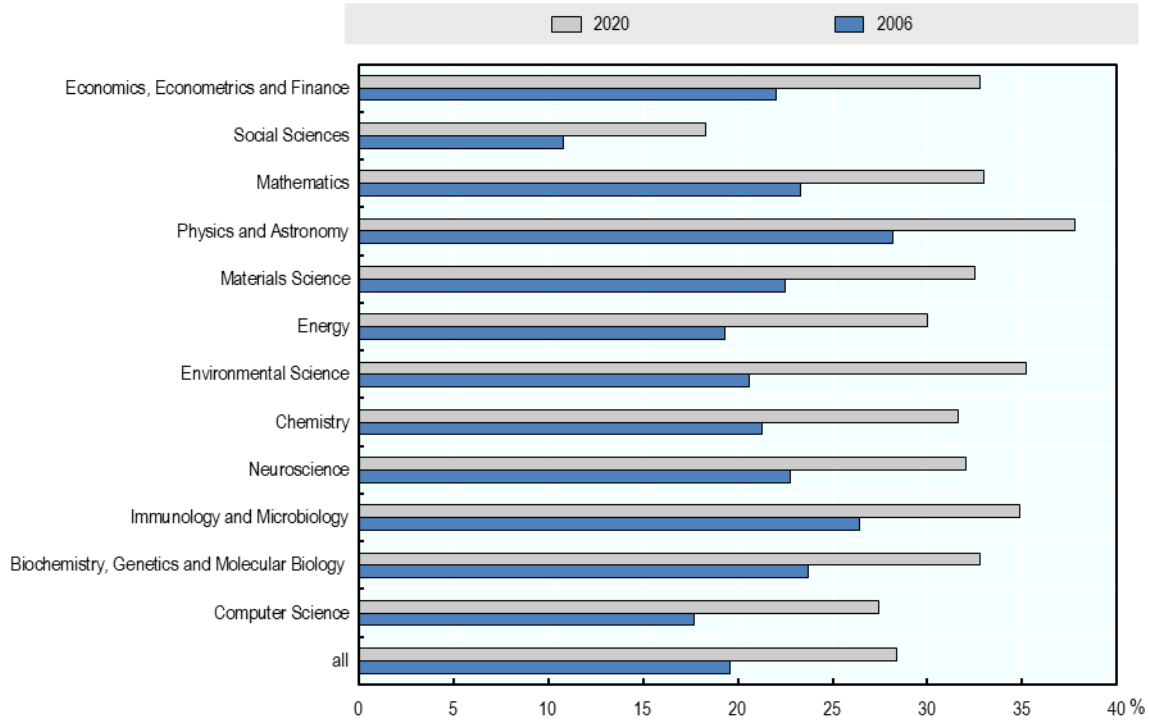
Science Diplomacy

Science diplomacy is broadly understood as a series of practices that stand at the intersection of science and diplomacy. Science diplomacy has been divided into three phenomena: science for diplomacy – the use of science to advance diplomatic objectives; diplomacy for science – the use of diplomatic action to further scientific and technological progress; and science in diplomacy – the direct involvement of science or scientific actors in diplomatic processes (European Union Science Diplomacy Alliance, n.d.[18]).

4 International collaboration – a key element of the global research ecosystem

International collaboration is an essential part of the way science operates. In OECD countries, the percentage of scientific publications involving international collaboration has increased from 20% in 2006 to 28% in 2020 and this progression is similar across all scientific fields (see Figure 4.1) (OECD, 2021[19]; n.d.[20]).

Figure 4.1. Percentage of scientific publications involving international co-authorships, OECD, 2006 and 2020



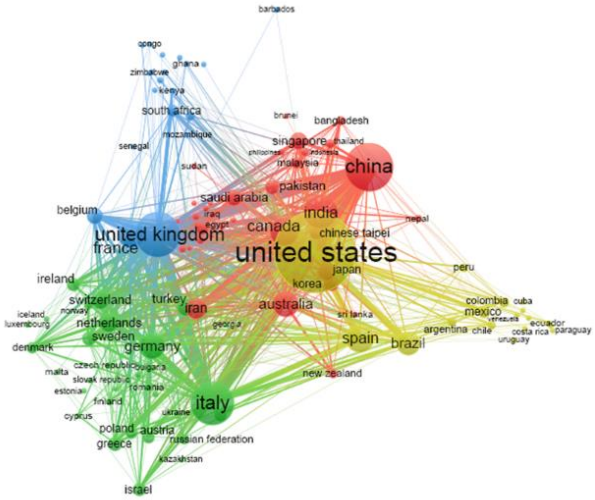
Note: The figure shows the percentage of scientific publications co-authored among institutions in different countries.
Source: OECD calculations based on Scopus Custom Data, Elsevier, Version 5.2021, September 2021 (OECD, 2021[19]; n.d.[20]).

StatLink https://stat.link/7o0p25k/

Global problems like the COVID-19 pandemic, climate change or other socio-economic challenges cannot be tackled without international research collaboration. The global response to the COVID-19 pandemic

exemplifies the importance of international collaboration. This is illustrated in Figure 4.2 and Figure 4.3 (OECD, 2021[21]). These figures also illustrate the generally apolitical nature of scientific collaboration, with researchers from different countries working together regardless of the geopolitical and ideological positions of governments. Open science and the sharing of research data and information across borders have been essential for the scientific response to the pandemic (OECD, 2020[22]).

Figure 4.2. International scientific collaboration on COVID-19 biomedical research from January to 30 November 2020



Note: Lines between items represent collaborative links between economies. The distance between two economies indicates the relatedness of the economies in terms of co-authorship links. In general, the closer two economies are located to each other, the stronger their relatedness. Please refer to https://doi.org/10.1787/888934223099 for more methodological information. The United States and the People's Republic of China (hereafter China) are among the two major contributors to COVID-19 publications on PubMed. They are also each other's main collaborating partners. Other economies with high engagement in international research collaborations on COVID-19 include the United Kingdom, Germany, France, Italy, Australia, Canada, and India.

Note by Republic of Türkiye:

The information in this document with reference to "Cyprus" relates to the southern part of the Island. There is no single authority representing both Turkish and Greek Cypriot people on the Island. Türkiye recognises the Turkish Republic of Northern Cyprus (TRNC). Until a lasting and equitable solution is found within the context of the United Nations, Türkiye shall preserve its position concerning the "Cyprus issue."

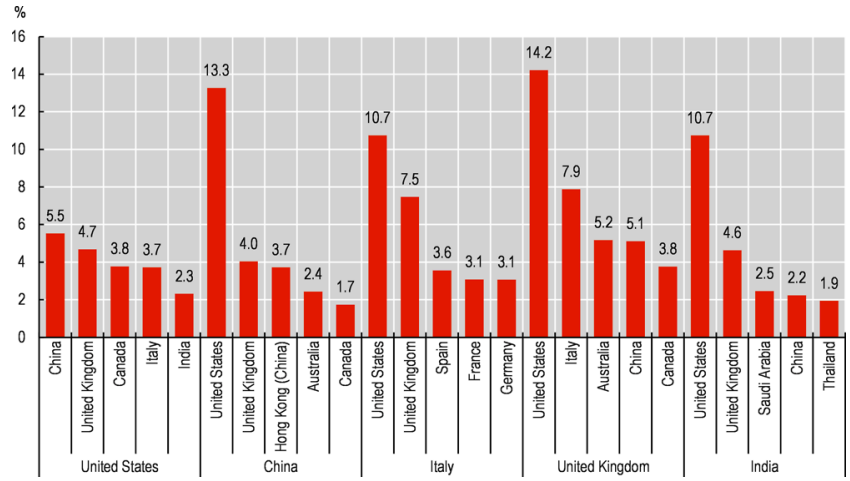
Note by all the European Union Member States of the OECD and the European Union:

The Republic of Cyprus is recognised by all members of the United Nations with the exception of Türkiye. The information in this document relates to the area under the effective control of the Government of the Republic of Cyprus.

Source: OECD Science, Technology and Innovation Outlook 2021, based on U.S. National Institutes of Health PubMed data, https://pubmed.ncbi.nlm.nih.gov/ (accessed 30 November 2020) (OECD, 2021[21])

StatLink https://doi.org/10.1787/888934223099

Figure 4.3. Selected economies, in terms of the total number of medical research publications (fractional counts), and their top five partner economies, from 1 January to 30 November 2020



Note: The period covers 1 January to 30 November 2020 and includes 74 115 documents. The United States co-authored 16 964 documents. 84% of those were domestic co-authorships, while the remainder involved international collaboration. The top collaboration partner of the United States is the People's Republic of China (hereafter China), and US-China collaboration represents 5.5% of all United States publications on COVID-19-related medical research.
Source: OECD Science, Technology and Innovation Outlook 2021 based on U.S. National Institutes of Health (NIH) PubMed data, https://pubmed.ncbi.nlm.nih.gov/ (accessed 30 November 2020) (OECD, 2021[21])

StatLink https://doi.org/10.1787/888934223479

4.1. The multilateral framework for international scientific exchange and collaboration

International collaboration constitutes an essential part of scientific research and is enshrined in a number of formal and informal recommendations and declarations from international organisations, which establish the basis of how and why such collaboration should be promoted (see Table 4.1). These international principles and norms have been approved by a large majority of countries either globally (UN, UNESCO, OECD) or regionally (EU).

Table 4.1. Multilateral framework for international scientific exchange and collaboration

Recommendation/Declaration	Main emphasis
International Covenant on Economic, Social and Cultural Rights (United Nations Human Rights Office of the High Commissioner, 1966[23])	State Parties must take action to "ensure the conservation, the development, and the diffusion of science and culture." They also agree to respect "the freedom indispensable for scientific research and creative activity" and recognise "the benefits to be derived from the encouragement and development of international contacts and cooperation in the scientific and cultural fields."
Recommendation on Science and Scientific Researchers (UNESCO, 2017[24])	Countries are recommended to "establish and facilitate mechanisms for collaborative open science and facilitate sharing of scientific knowledge while ensuring other rights are respected.
UNESCO Recommendation on Open Science (UNESCO, 2021[25])	Countries are encouraged to develop effective institutional and national open science policies and legal frameworks that are consistent with existing international and regional law.
Recommendation of the Council on International Co-operation in Science and Technology (OECD, 2021[26])	This recommendation states that Member countries should emphasise the importance of mutually beneficial scientific and technological transfers and of removing barriers that slow economic and social progress. Its signatories agree to promote co-operative projects, encourage exchanges of students and scientists between Member countries, facilitate access to basic research facilities to international scientists and engineers, and promote the dissemination of basic research results. In this Recommendation, countries are called upon "to establish a harmonised understanding of

	scientific values and norms (such as research integrity and freedom of scientific inquiry and expression) when engaging in international co-operation in science and technology". It also emphasises "taking appropriate measures to mitigate and to counter the possible risks associated with international co-operation in science and technology in order to facilitate the effectiveness and efficiency of co-operation for mutual benefit."
Recommendation of the Council for Facilitating International Technology Co-operation with and among Businesses (OECD, 2022[27])	It recommends minimising barriers for effective and efficient technology co-operation while taking appropriate measures to prevent and mitigate risks in international technology co-operation such as data leakage or theft, forced technology transfer, exploitative extraction of research resources, misuse of dual-use technologies. Countries are encouraged to support collaboration between businesses, universities, public research, and civil society in the development of international governance frameworks for the use and application of new and emerging technologies, taking into account effective risk management and appropriate regulatory environments.
Recommendation of the Council concerning Access to Research Data from Public Funding (OECD, 2021[28])	It advocates for wide sharing of data and other research-relevant digital objects (metadata, algorithms, workflows, models, and software, including code).
Recommendation of the Council in Responsible Innovation in Neurotechnology (OECD, 2019[29])	It calls on countries to foster scientific collaboration and support an international culture of open science by creating joint infrastructures and environments for sharing data relating to neurotechnology.
Recommendation of the Council on Artificial Intelligence (OECD, 2019[30])	It makes reference to desirability of sharing AI knowledge and encouraging international initiatives.
Statutes and Rules of Procedure (International Science Council (ISC), 2018[31])	The International Science Council commits to promoting "equitable opportunities for access to science and its benefits, and opposes discrimination based on such factors as ethnic origin, religion, citizenship, language, political or other opinion, sex, gender identity, sexual orientation, disability, or age". All the members of ISC, which includes national academies from 180 countries and scientific unions, representing all fields of research, are committed to withholding the universality of science, which has been used, for example, to defend the mobility of scientists between countries in the face of political embargoes.
Bonn Declaration on Freedom of Scientific Research (Ministerial Conference on the European Research Area, 2020[13])	Research Ministers of the European Union and the European Commissioner for Innovation, Research, Culture, Education and Youth adopted the *Bonn Declaration on Freedom of Scientific Research* (Ministerial Conference on the European Research Area, 2020[13]), which commits signatories to protect freedom of scientific research, including freedom of expression, freedom of association, freedom of movement and the right to education.
Marseille Declaration on International Cooperation in Research and Innovation (R&I) (French Presidency of the Council of the European Union, 2022[32])	EU ministers for higher education, research, and innovation agree to promote and protect freedom of scientific research and academic freedom in international research, innovation, and higher education collaboration while taking measures to counter and manage security risks inherent to international cooperation.
Singapore Statement on Research Integrity (World Conference on Research Integrity, 2010[33])	This statement provides a normative basis for the consideration of research integrity in different national and cultural contexts and the development of detailed guidelines and practices. It defines the main principles of research integrity, and the associated responsibilities of researchers. The four principles are honesty, accountability, professional courtesy and fairness, and good stewardship (see Annex A for more details). These principles, or variations of them are taken up in a number of other international or national declaration, codes and guidelines concerning research integrity (e.g. The All European Academies (2017[34]), Science Europe (2016[35]), the InterAcademy Partnership (IAP) (2016[36]), etc.).

It is notable that the recently revised *Recommendation of the Council on International Cooperation in Science and Technology* (OECD, 2021[26]) and the *Marseille Declaration* (French Presidency of the Council of the European Union, 2022[32]) specifically mention the need to take measures to counter the risks inherent in international cooperation. Overall, however, the emphasis of all these recommendations is on the value of open and inclusive international collaboration in research and the role of governments in supporting such collaboration, whilst respecting the autonomy and freedom of scientific research. The values and norms and actions that are described in these various international agreements are mirrored in a plethora of guidelines and codes at national and institutional level and largely govern the operations of the global research ecosystem.

5 Foreign interference in research processes

A growing number of countries are concerned about threats to national and economic security in international scientific collaboration and exchange. These threats can go beyond unauthorised information and technology transfers and theft of intellectual property. There are particular concerns about the intimidation of researchers on university campuses, which can result in vulnerable individuals being coerced to undertake theft and espionage. Researchers in social sciences and humanities (SSH) in particular can be coerced by state entities to avoid activities or censor their communications on certain research topics. Self-censorship can also be caused by the fear of state interference, particularly in a climate where researchers feel vulnerable or unsupported. Such interference has implications for the conduct and management of research, but equally, there is concern that both the threats and an over-zealous response to them, may undermine the integrity and the basic principles and norms for research.

In general, countries have well-regulated export control systems that are applied, for example, to armaments and nuclear technology to protect national security or uphold non-proliferation obligations. Conventional export control systems are primarily focused on sensitive technologies, and, in this regard, national governments have routinely defined research on chemical, biological, radiological, nuclear, and explosive technologies as dual-use. The development of armaments, including related dual-use technologies, is the subject of a number of international legal conventions (United Nations, 2013[37]; 1968[38]; 1972[39]).

It is less easy to control the intangible transfer of data, information and know-how and scientific research carried out without a specific practical aim; basic research has traditionally been exempt from export controls (Government of the United Kingdom, 2021[40]). At the same time, it is recognised that knowledge from many areas of fundamental research could be considered as potentially dual-use. For instance, artificial intelligence (AI) or quantum computing have the potential for both civilian and military use, as well as being the focus of intense economic competition between companies, countries, and regions. Traditional laws protect intellectual property rights. However, protecting data, information and know-how are not easy in the internet era and restrictions on access may conflict with research integrity principles and open science.

It is a major challenge for countries to maintain the balance between open and trust-based scientific collaboration and protective but potentially restrictive regulations. Over-regulation or excessive intervention can affect the freedom of scientific enquiry and exchange whereas the lack of shared and respected international regulations and norms can lead not only to misappropriation of research but also to certain types of research being selectively conducted in countries that do not impose legal or ethical restraints. Policies are required to facilitate common global approaches that promote trusted international collaboration and the open exchange of ideas, without interference by governments.

5.1. The link between research integrity, research security and international research collaboration

Research integrity is built upon the values, norms, and principles that constitute good scientific practice (academic freedom, openness, honesty, accountability, etc.) and regulate international research collaboration (reciprocity, equity, non-discrimination, etc.). Research security aims to protect the research ecosystem and national security and economic interests from external interference, including foreign state or non-state interference. Both research integrity and research security are essential for protecting the research ecosystem (see earlier Figure 2.1). The identification and management of COI and COC are important for research security and will also improve research integrity.

Balancing open international collaboration, research integrity and research security is a challenge for all stakeholders in the research ecosystem, including governments, funding agencies, research institutions, universities, academic associations, and individual researchers.

5.2. Detrimental research practices

Whilst individual research misconduct is commonly associated with falsification, fabrication, and plagiarism (FFP) and a variety of 'questionable' research practices, there are a number of other 'detrimental practices' that are more directly of concern in relation to research security (Australian Security Intelligence Organisation, 2020[3]). These often manifest at the level of individual or organizational behaviour but they are typically motivated and/or supported by the interests of foreign states or non-state actors. They may also directly involve international collaborations and partnerships between research institutions and universities.

Detrimental practices of concern in a number of OECD countries are described below.

5.2.1. Theft or misuse of data, samples, or know-how

Countries are concerned about theft in international collaboration and exchange. Theft is the acquisition of data, samples, or know-how without the permission of the principal investigator or host institution. Theft can be carried out using different physical or cyber techniques and may be associated also with conflicts of interest and conflicts of commitment.

Joint research can be misused by organisations and institutions in foreign countries. Foreign partners can exploit participation in a research partnership or collaborative activity to access knowledge, products or technologies that are exploited to gain unfair economic advantage, misapplied for malevolent application or misused to cause harm (BBSRC, MRC and Wellcome Trust, 2015[10]). Misappropriation by a foreign partner can result in reputational harm as well as institutional/national economic loss.

Box 5.1. Case studies – research theft

Several countries have developed case studies to illustrate the research integrity and security risks that can arise in routine research practice. These cases are either anonymised or fictional and are designed to reflect familiar scenarios that can be used in training and awareness-raising.

Research theft

A researcher worked in a number of medical research labs, stole trade secrets, and transferred them to a foreign country after receiving payments from a foreign government. The researcher also started a company to produce and sell medical kits based on the stolen trade secrets. She was prosecuted and received a 30-month prison sentence and had to pay 3 million euros in restitution and forfeit additional assets because of her conviction (Department of Justice, 2021[41]).

Internal threats

A university researcher is mandated to sponsor three PhD students at her university. In order to facilitate the work schedule of the students, she grants them 24/7 access to the research building and the lab. She returned to work late one evening and noticed a student in the lab looking through research data and notes not relevant to the work with which the student was involved. The information had been left unsecured by another team member. If the information was sensitive or confidential, then she and her research team might run the risk of forfeiting potential personal, professional, or economic and commercial gains that could be achieved from their research. This could also have a negative impact on her team's reputation and careers (Government of Canada, 2021[42]).

Potential misuse by criminal hackers

A proposed research project aims to systematically identify vulnerabilities in computer programmes, particularly in the operating systems of wireless routers, smartphones, and laptops using AI methods and to develop automated defensive measures. The results of this research project would come in useful everywhere where these computer programmes need to be monitored and updated regularly. At the same time, the results would allow the identification and exploitation of these vulnerabilities in numerous devices that are not regularly monitored and updated (German National Academy of Sciences Leopoldina, n.d.[43]). *How can the risks inherent in this project be effectively managed?*

Source: *Hospital Researcher Sentenced to Prison for Conspiring to Steal Trade Secrets and Sell to China* (Department of Justice, 2021[41]); *Scenario 3 - Insider threats and research theft* (Government of Canada, 2021[42]); *Information on Selected Security-Relevant Research Topics and Case Studies* (German National Academy of Sciences Leopoldina, n.d.[43])

5.2.2. Deceptive practices

Deceptive practices include intentional hiding or omission of information. Concealing foreign or commercial compensation or alliances is recognised as a deceptive practice that is often associated with conflicts of interest or conflicts of commitment. For instance, a foreign scholar seeking employment might be tempted not report an affiliation with an institution in a home country or may not report information that a visa official may consider pertinent (JASON, 2019[1]).

Running a satellite laboratory or group in another institution and/or foreign country without declaring it to a researcher's principal employer can also be considered as a deceptive practice. Providing materials from a home institution to a satellite lab, in contravention to the rules or guidance of the home institution, is theft (JASON, 2019[1]), although it may not always be immediately recognised as such by the parties concerned.

Double dipping is a particular form of deceptive practice. A researcher can 'double-dip' by applying for funding for a host institution to carry out research already completed or funded by another entity, in some cases another country (Office of Science and Technology Policy, 2020[6]). Again, the borderline between double dipping and normal research funding processes, which can involve multiple donors supporting closely related work, is not always easy to define.

A foreign student can enrol in a university while concealing conflicts of commitment, including associations with foreign security forces or companies. Universities may then train such personnel without realising that they are potentially undermining national or economic security (Parliamentary Joint Committee on Intelligence and Security, 2021[44]). Similarly, research institutions and universities may recruit overseas personnel with undeclared conflicts of interest or commitment. In this regard, it is important to note that many countries have specific programmes to encourage mobility or recruit overseas talent and some of these may include conditions that make them susceptible to coercive practices (see next section).

Failure to acknowledge or provide due credit for scientific ideas and work is also a deceptive practice. This has traditionally been recognised as an important aspect of research integrity, particularly in relation to the authorship of scientific publications. However, in the context of research security, it takes on a broader dimension that can sometimes equate to theft.

Box 5.2. Case studies – deceptive practices

Several countries developed case studies to illustrate the research integrity and security risks that can arise in routine research practice. These cases are either anonymised or fictional and are designed to reflect familiar scenarios that can be used in training and awareness-raising.

Failure to disclose foreign funding and affiliations

A researcher funded by a national funding agency did not declare any information about foreign funding and affiliations in his funding proposal while required to do so under the proposal and award policies of the national funding agency. The funding agency issued a subpoena, the researcher produced some documents, including a partial application to a foreign talent programme, but the information was insufficient. The funding agency suspended the researcher's awards to his university and imposed a government-wide debarment on the researcher (including a bar on serving as a reviewer, advisor, or consultant) for a fixed term in view of the researcher's failure to respond to the subpoena (National Science Foundation, n.d.[45]).

Employment with a foreign military university

A professor in engineering and information technology worked in his home institution on publicly-funded projects on swarm systems for agricultural applications. It was revealed in the media that he was affiliated as a professor at a foreign military university. He had not declared his role with the foreign university to his home institution (Department of Education, Skills and Employment, 2021[46]).

Source: *Research Security* (National Science Foundation, n.d.[45]); *Scenario 2 - Participation in foreign talent and recruitment programs* (Government of Canada, 2021[47]); *Case Studies – Due diligence, risk assessments and management* (Department of Education, Skills and Employment, 2021[46])

5.2.3. Coercive practices

For a scholar carrying out research overseas, coercion may take the form of withholding scholarship or fellowship funds, or threats to the scholar's family in their home country, if the scholar does not report on research activities and collect information for their home country. A foreign researcher can be coerced also

by a host country or institution by the threat of loss of resources, prestige, or privileges. Regulations requiring researchers to cooperate with intelligence and security services from one country whilst operating in another country are a form of coercion that comes with the threat of legal action (JASON, 2019[1]). Such regulations are applicable in some talent programmes. Coercive practices generate conflicts of interest and conflicts of commitment and can make it very difficult for individuals to declare these conflicts.

Coercive practices can inhibit the freedom of scientific research. A country may discourage a foreign researcher from conducting research that is sensitive to that country by threatening to limit or cancel existing partnerships (Bekkers, Oosterveld and Verhagen, 2019[48]). The country may also restrict access to local information, including information on human rights situations, which can be a particular challenge for some areas of study in social sciences and humanities (SSH) (Tardell, 2021[49]; Human Rights Watch, 2021[50]; Gattolin, 2021[51]). Some international researchers feel pressure from their governments to self-censor, cooperate with certain companies, or engage in talent programmes. At the same time, some foreign researchers feel excluded or discriminated against in their host countries even though they do not cooperate with their national government or foreign organisations.

In addition to individuals, 'independent' research organisations and institutions can also be subject to strong state control/influence and may be compelled/encouraged to share information either because of laws or requirements or to assure state support for their activities domestically and abroad. There are examples of universities in OECD countries that have established partnerships with overseas institutions for training and research, whilst ignoring that these institutions are subject to strong political and/or military influence. Similarly, such institutional partnerships, which often need to accommodate important cultural differences, may not always give due attention to good ethical practices and freedom of scientific research. Such partnerships can generate problematic conflicts of interest or conflicts of commitment for institutions and their staff and students.

Box 5.3. Case studies – coercive practices

Several countries developed case studies to illustrate the research integrity and security risks that can arise in routine research practice. These cases are either anonymised or fictional and are designed to reflect familiar scenarios that can be used in training and awareness-raising.

Foreign interference with publication

A professor published a paper on a foreign country's response to COVID-19, predicting a dire situation. The foreign country's Consulate approached her university to request the paper be retracted and a public apology be issued because the paper criticised and embarrassed the foreign government. The university declined the request from the Consulate to retract the paper and apologise. The university has a strong commitment to freedom of speech and academic freedom and considered the research and paper had undergone comprehensive peer review (Department of Education, Skills and Employment, 2021[52]).

Participation in foreign talent and recruitment programmes

A professor was approached by a foreign university to become an adjunct professor in his field of expertise. The foreign university offered to cover all travel costs and pay him to deliver lectures and participate in research projects for three months out of the year during a summer semester. If the professor had accepted the position, he might have been obligated or under pressure to disclose confidential or commercial information as a condition of the agreement or during the work term at the foreign institution. The national government of his home country recommends that any appointments to foreign institutions should be disclosed to home institutions (Government of Canada, 2021[47]).

Source: *Case Studies – Governance and risk frameworks* (Department of Education, Skills and Employment, 2021[52])

5.3. Challenges for research evaluation

5.3.1. Breaches of confidentiality

Peer reviewers have access to confidential information prior to publication or grant award and can transfer the information to other entities, including foreign countries (JASON, 2019[1]). Diversion of proprietary information and data can undermine trust between different actors who are part of the research enterprise, as well as public trust in science (Office of Science and Technology Policy, 2020[6]).

5.3.2. Distorted decisions

Peer reviewers, including foreign reviewers, often have privileged access to confidential, unpublished information. This can be used for personal gain, which is considered as misconduct in breach of established research integrity principles. From a research security perspective, a reviewer who has conflicts of interest or conflicts of commitment can distort decisions in peer-review processes in order to benefit outside entities, including foreign countries.

Box 5.4. Case studies – challenges for research evaluation

Several countries developed case studies to illustrate the research integrity and security risks that can arise in routine research practice. These cases are either anonymised or fictional and are designed to reflect familiar scenarios that can be used in training and awareness-raising.

Breaches of confidentiality

A well-published senior researcher at a national institution had four awards, with funding totalling more than $1 million, terminated for breaches of confidentiality, linked to COI and COC. During a thorough investigation by a national funding agency, it was found that the researcher had multiple undisclosed foreign affiliations in violation of the funding agency's policy. The investigation found that the researcher violated the peer review process by repeatedly sharing the reviewers' names and reviewer scores with foreign research institutions. The researcher was part of a foreign talent plan which in itself was allowable. However, the talent plan affiliation was not disclosed to the funding agency and there were terms in the talent plan contract that could be linked to both the nondisclosure and the concerning behaviours (National Science Foundation, n.d.[45]).

5.4. Cybersecurity

Cybersecurity is a growing concern for research in many countries. In the increasingly digitalised world, many public and private institutions are concerned about cybersecurity and many of the issues related to cybersecurity are not specific to research (OECD, 2015[53]). In this regard, research institutions and universities need to deploy accepted best practices for public infrastructure, including adoption of rigorous risk management processes, to ensure that their IT infrastructure, data assets and related activities are secure (National Cyber Security Centre, 2019[54]). In addition, there are specific areas of concern that relate to research, which is inherently international and open but often generates and uses sensitive and high-value data and information.

Cyberattacks can damage data or IT systems at universities or research institutions, resulting in a loss of research data or suspension of research activities (Canadian Centre for Cyber Security, 2020[55]). Cyber threat actors can also use the information systems of universities or research institutions to attack other organisations. Virtual meetings, which have increased enormously during the COVID-19 pandemic, are particularly vulnerable to such attacks.

Individual researchers, who often use the internet to exchange in an open and informal way and to communicate internationally without paying due attention to security, are particularly vulnerable. Phishing attacks are one of the most common ways to steal personal and other data or insert ransomware into computing systems. Phishing emails induce a researcher to submit sensitive information, access malicious websites, or download infected attachments (Centre for the Protection of National Infrastructure (CPNI), n.d.[56]).

Physical theft of research data/knowledge can occur while a researcher is at their home institution, but risks are potentially higher when travelling abroad; this is of particular concern given international mobility is an important aspect of research. While travelling, data or documents can be stolen at hotels, conference spaces or in transport (U15 Group of Canadian Research Universities and Universities Canada, 2019[57]). Files can be transferred using a USB drive memory card at a conference, or a researcher's computer can be infected with computer viruses via a memory card (Centre for the Protection of National Infrastructure (CPNI), n.d.[56]). In this way, physical theft or interference with IT equipment can be a precursor to subsequent cyber-attacks.

Box 5.5. Case studies – cybersecurity

Several countries developed case studies to illustrate the research integrity and security risks that can arise in routine research practice. These cases are either anonymised or fictional and are designed to reflect familiar scenarios that can be used in training and awareness-raising.

Remote access information

A PhD student from an academic laboratory was invited to attend an overseas conference in their area of specialisation. The student was asked to present on research they are conducting on new agri-business drone capabilities. During the event, the information for remote access was captured by a foreign actor and a permanent access link to the university's system and to the student's research was established. Within a month of returning, the student's research had been copied and prototypes were developed, appearing on the open market. The drone technology was also adapted by the foreign country for use in military operations (Department of Education, Skills and Employment, 2021[58]).

Physical theft of data during travel

A researcher travelled to an international conference abroad, where his research was presented and discussed. The researcher brought his computer with him and a USB key containing information related to his work. During the conference, he contacted several international partners, with whom he exchanged information and data by connecting his USB key to colleagues' devices. If his data or findings had been misappropriated, recognition for the research work could easily have been misattributed (Government of Canada, 2021[59]).

Source: *Case Studies – Cybersecurity* (Department of Education, Skills and Employment, 2021[58]); *Scenario 5 - Security and travel* (Government of Canada, 2021[59])

6 Policy initiatives and actions

Responsibilities for research integrity and security are distributed across a number of actors in the international research ecosystem. These include national governments; research funding agencies; research institutions and universities; and academic and university associations. Some of the actions that are already being taken by these different actors to protect research integrity and security are described below.

The majority of these examples are taken from the United States, Australia, the United Kingdom, and Canada, and it is fair to say that these are the countries that have been most active in monitoring research security and publicly expressing their concerns. More recently, however, several other countries have also become more engaged as discussions around technological sovereignty in relation to the COVID-19 pandemic have spilled over into broader concerns about who appropriates and benefits from nationally funded public research.

6.1. National governments

6.1.1. Policies and regulations

In response to growing concerns about national and economic security risks and the need to protect research integrity and freedom of scientific research, some governments have being taking action for several years. For instance, in 2018, the U. S. Department of Justice announced the creation of a new initiative focused on specific threats to national security, including in the academic sector. There have been several cases of prosecutions (not always successful) against individual scientists or scholars working in the United States (Department of Justice, n.d.[60]; 2020[61]; 2018[62]; 2021[63]). The U.S. Congress has passed legislation authorising and requiring the disclosure of funding sources in applications for federal research and development awards (116th Congress, 2021[64]). In addition, the U.S. Government issued a presidential memorandum to strengthen cooperation between law enforcement agencies and funding agencies and direct these agencies to strengthen the protection of U.S. government-supported research (The White House, 2021[65]). This is accompanied by implementation guidance, which addresses: disclosure policy (ensuring that federally-funded researchers provide their funding agencies and research organizations with appropriate information concerning external involvements that may bear on potential conflicts of interest and commitment); oversight and enforcement (ensuring that federal agencies have clear and appropriate policies concerning consequences for violations of disclosure requirements and interagency sharing of information about such violations); standardised disclosure requirements across agencies and digital reporting tools that facilitate easy compliance; and, ensuring that research organizations that receive substantial federal R&D funding maintain appropriate research security programmes (The White House, 2021[66]; National Science and Technology Council, 2022[67]). The most recent guidance has a focus on ensuring that policies and processes across government are clear and uniform and do not fuel xenophobia or prejudice.

In the United Kingdom, the National Security and Investment (NSI) Act allows the national government to intervene in certain acquisitions that could harm the UK's national security (Department for Business, Energy & Industrial Strategy, 2021[68]). When UK assets, including those held by universities or public

research institutions, in 17 sensitive areas of the economy are to be put on the market, the seller is legally obliged to notify the government. Most of these sensitive areas (see Table 6.1) are research-intensive and characterised by a variety of public-private research partnerships. The United Kingdom also has an Academic Technology Approval Scheme (ATAS), which applies to international students who are intending to study at the postgraduate level in certain sensitive subjects (Foreign & Commonwealth Office and Foreign, Commonwealth & Development Office, 2013[69]). Students from certain countries must apply for an ATAS certificate before they can study in these fields in the United Kingdom.

The sensitive areas identified in the UK NSI Act have considerable overlap with security sensitive areas that have been identified by other national and regional bodies. In Canada, individual researchers are requested to assess the potential national security risks of international collaborative projects and the *National Security Guidelines for Research Partnerships* (Government of Canada, 2021[70]) identify research areas that may be considered sensitive or dual-use and require particular attention (see Table 6.1). Complementing this sensitive technology list, the Guidelines also ask researchers to assess whether their work contains sensitive data covered by more traditional controlled goods regulations.

In Japan, technology transfers to domestic residents have not been deemed as exports, but the national government has begun to control sensitive technology transfers to domestic residents who might be influenced by foreign governments or companies. Residents who receive significant financial benefits or have contracts (such as employment contracts) from foreign governments or companies will be considered to be potentially influenced by foreign governments or companies.

Some national policies identify specific 'sensitive' countries that they consider liable to foreign interference, but many take country-agnostic approaches. Country-specific approaches have the advantage of focusing the main risk management efforts of public research institutions and universities on a small number of countries. But inherent in this, is the risk of prejudice, cultural bias, and discrimination against certain populations. The country agnostic approach acknowledges that a list of countries that are considered sensitive at one point in time may change in the future and that risks may be associated with partnerships and collaborations between countries that might normally be considered as political allies.

Table 6.1. Sensitive technology and information areas

	Sensitive areas or technologies
National Security and Investment Act, United Kingdom	Advanced materials Advanced robotics Artificial intelligence Civil nuclear Communications Computing hardware Critical suppliers to government Cryptographic authentication Data infrastructure Defence Energy Military and dual-use Quantum technologies Satellite and space technologies Suppliers to the emergency services Synthetic biology Transport
National Security Guidelines for Research Partnerships, Canada	Advanced materials and manufacturing Advanced ocean technologies Advanced sensing and surveillance Advanced weapons Aerospace

	Artificial intelligence Biotechnology Energy generation, storage and transmission Medical technology Neurotechnology and human-machine integration Next generation computing and digital infrastructure Position, navigation and timing Quantum science Robotics and autonomous systems Space technology
Classification of Information in Horizon Europe Projects, the European Commission	Subject-matters of the research: – Explosives – Chemical, biological, radiological, and nuclear – Critical infrastructure and utilities – Border security – Intelligent surveillance – Terrorism – Organised crime – Digital security – Space Types of the research/results: – Threat assessments – Vulnerability assessments – Specifications – Capability assessments – Incidents/scenarios

Source: *National Security and Investment Act* (Department for Business, Energy & Industrial Strategy, 2021[68]); *National Security Guidelines for Research Partnerships* (Government of Canada, 2021[70]); *Classification of Information in Horizon Europe Projects* (European Commission, 2021[71])

6.1.2. Guidance

Governments and governmental agencies have developed guidelines for the research sector, to enhance integrity and security. These often provide guidance for universities or funding agencies, but in some case can be applied also at an individual researcher scale.

The U.S. Government has published *Recommended Practices for Strengthening the Security and Integrity of America's Science and Technology Research Enterprise* (National Science & Technology Council, 2021[72]) that include recommendations for research organisations to better protect security and integrity. These recommendations include establishing organisational policies regarding COI and COC, standardising requirements for disclosure of information, providing training to researchers on responsible conduct of research, and ensuring appropriate and effective consequences for violation of disclosure requirements.

The UK's Centre for the Protection of National Infrastructure (CPNI) (n.d.[56]) has published *Trusted Research Guidance for Academia*, which aims to promote integrity in international research collaboration. It is particularly designed for researchers in areas seen as critical for UK's research and innovation sector: STEM subjects, emerging and potentially dual-use technologies, and commercially sensitive research areas. This guidance has been produced in consultation with the research and university community. The CPNI gives an overview of the risks associated with international collaborations, and of the way UK researchers could be exposed to them. Guidelines include advice at the university level and for individuals. Researchers can access the guidelines on the CPNI's web page and the CPNI also provides a checklist for researchers to evaluate their research proposals by answering key questions (see Box 6.1) (Centre for the Protection of National Infrastructure (CPNI), 2020[73]; n.d.[74]). In addition to the *Trusted Research*

Guidance for Academia, the UK Export Control Joint Unit (2021[40]) has published guidance that focuses on export controls applying to academic research.

The Government of the United Kingdom (2021[75]) has established a new Research Collaboration Advice Team (RCAT) that offers researchers advice on how to protect their work from hostile activity, ensuring international collaboration is done safely and securely. The advice covers export controls, cyber security, and protection of intellectual property. The RCAT acts as a single point of contact in government and responds to requests from British universities who have identified potential risks within current projects or proposals. Advisers also proactively approach research institutions and universities and support them to implement advice and guidance.

Box 6.1. UK CPNI's checklist for evaluating research proposals

The UK CPNI developed a checklist that includes following questions to evaluate collaborative research proposals.

About new partners

Why does a partner want to work with you?

What are they expecting in return for their financial support or involvement?

Is the organisation associated with a country which may be viewed as hostile to the UK or one which has different democratic and ethical values from our own?

Has due diligence into the partner identified any involvement in research on behalf of the military or police with links to a hostile state?

Set within the context of any information gained from due diligence, could your research be misused or have unintended applications which would be negative?

Are there any legal, regulatory or university policy constraints on undertaking your research with this partner?

Having considered the answers to the above questions, are there potential reputational or ethical risks to you or the university?

Does the decision about this research need to be escalated within your department?

About research relationships

Are the terms of any proposed Memorandum of Understanding (MoU) in keeping with the expectations of your department and university?

Are you providing existing intellectual property (IP), research data, confidential or personally identifiable data to the project? If so, how is this going to be protected?

Who will own any IP that is generated?

Do you have plans in place for protecting the resulting IP?

What contractual requirements are you able to put in place to protect the interests of your academic institutions?

What access will the research partner have to your IT network? If they do have access, what broader visibility might this provide?

Is there any physical separation or protection required between research in similar fields?

About existing partners

Would proceeding with the research raise potential conflicts of interest with existing research partners?

Have you spoken with your existing partners about any potential conflict of interest?

Have you considered the terms of any non-disclosure agreements? Does this include an expectation that you will need to provide visibility to existing partners?

Will this research breach any existing contractual agreements that you, your department or university already have?

Source: *Checklist: evaluating research proposals* (Centre for the Protection of National Infrastructure (CPNI), n.d.[74])

The New Zealand government has developed *Trusted Research Guidance* for research institutions, universities, and researchers (2021[76]). This guidance includes analysis of already existing legislation on education, research, science and technology, customs, privacy, immigration, intelligence and security and overseas investment that are applicable to research security issues.

In 2019, the Australian Minister for Education established the University Foreign Interference Taskforce (UFIT), which created *guidelines to counter foreign interference in the Australian university sector* (2021[14]). The taskforce brings together universities and government agencies to collaborate on countering foreign interference. The UFIT guidelines cover governance frameworks, due diligence, communication, and education on risk and cyber security. The guidelines are complemented by guidance material that includes case studies, tool kits, and best-practice guides. The guidelines were refreshed in 2021 to better address how foreign interference threats have evolved since the initial guidelines were released and to assist universities to better identify and respond to risks of foreign interference. The refreshed Guidelines are more specific and measurable, adaptable to new and emerging foreign interference risks, and can be implemented by universities in a way that is proportionate to their own risks.

In 2020, The Canadian government published a *Policy Statement on Research Security and COVID-19* (Government of Canada, 2020[77]). In this statement, it encourages members of the research ecosystem to be aware of the potential risks to their work and asks them to take appropriate measures to protect their knowledge creation and innovations, while maintaining a strong commitment to Open Science and support for a global research response to the COVID-19 pandemic.

The Canadian government has more recently published *National Security Guidelines for Research Partnerships* to prevent foreign interference, espionage, and unwanted knowledge transfer that can contribute to advancements in the military, security, and intelligence capabilities of states or groups that pose a threat to Canada or that may enable the disruption of the Canadian economy, society, and critical infrastructure (Government of Canada, 2021[70]). The guidelines identify sensitive research areas that have the potential for dual-use or are targeted by foreign governments, militaries, or other actors (see Table 6.1). The guidelines apply to federal research partnership funding, but all researchers are encouraged to protect their work by using the guidelines to assess and mitigate risks associated with potential research partnerships. Researchers must complete a risk assessment form when submitting applications to the federal research partnership funding programme (Government of Canada, 2021[78]).

The Canadian government has also been working closely with partners from the academic and national security communities to develop two self-paced online courses focused on training researchers and other university staff. Titled “Introduction to research security” and “Cyber security for researchers” respectively, these 40min courses provide high-level overviews of key information and engage users with a variety of pedagogical techniques. These courses are voluntary and free, can be accessed via the Safeguarding Your Research portal (Government of Canada, 2021[79]), and a certificate of completion is provided to users. Canada is exploring further avenues for course creation and training-the-trainer style courses.

In Japan, the national government has formulated a set of policy directions to ensure research integrity in response to new risks associated with the internationalization and openness of research (see Annex A) (Integrated Innovation Strategy Promotion Council, 2021[80]). This requires researchers to report information on foreign financial support and affiliations to both the research institutions to which they belong and to funding agencies. The national government revised its guidelines on public research funding in 2021 and made it possible for researchers to store the information that they need to report in the Cross-ministerial R&D Management System (e-Rad) to reduce the administrative burden on researchers. Consequences in the event of failure to report the information include bans on future research funding applications for five years. The national government has been conducting seminars on the new policy

directions for research institutions and universities and providing template checklists for research institutions, universities, and researchers.

The Netherlands is also developing guidelines, checklists and self-evaluation tools for research institutions and universities to make clear what factors need to be taken into account in international collaboration in order to protect knowledge security (Ministry of Education, Culture and Science, 2020[81]; 2021[82]). Knowledge security, in this context, is defined as preventing the unauthorised transfer of knowledge and technology and covert influence on higher education and research by state actors, which can lead to self-censorship and impair academic freedom. The national government is planning to establish a knowledge security centre that will be a central point for responding to questions from research institutions and universities and will assist their decision-making.

6.1.3. Sharing of information between research institutions, universities, intelligence and law enforcement agencies

More effective cooperation and exchange of information between intelligence agencies, law enforcement agencies, research institutions, and universities are considered necessary by both governments and research institutions in a number of OECD countries. Respect from governments for the freedom and autonomy of scientific research is an essential pre-condition for such cooperation to be effective.

The Presidential Memorandum on United States Government-Supported Research and Development National Security Policy (The White House, 2021[65]) requires the Director of the Office of Science and Technology Policy (OSTP), in coordination with the Director of National Intelligence (DNI) and heads of other agencies as appropriate, to engage with the U.S. R&D enterprise to enhance awareness of risks to research security and integrity and policies and measures for mitigating the risks. In the United States, scientists have been prosecuted for failing to properly disclose COI and COC to funding agencies (Cho, Kingdollar and Soshi, 2021[63]) and these prosecutions have led to considerable unease and protests in the academic community. This has led to the recommendation by the U.S. Government that institutions establish ties with local Federal Bureau of Investigation (FBI) offices, allowing for better communication and understanding of concerns by both entities.

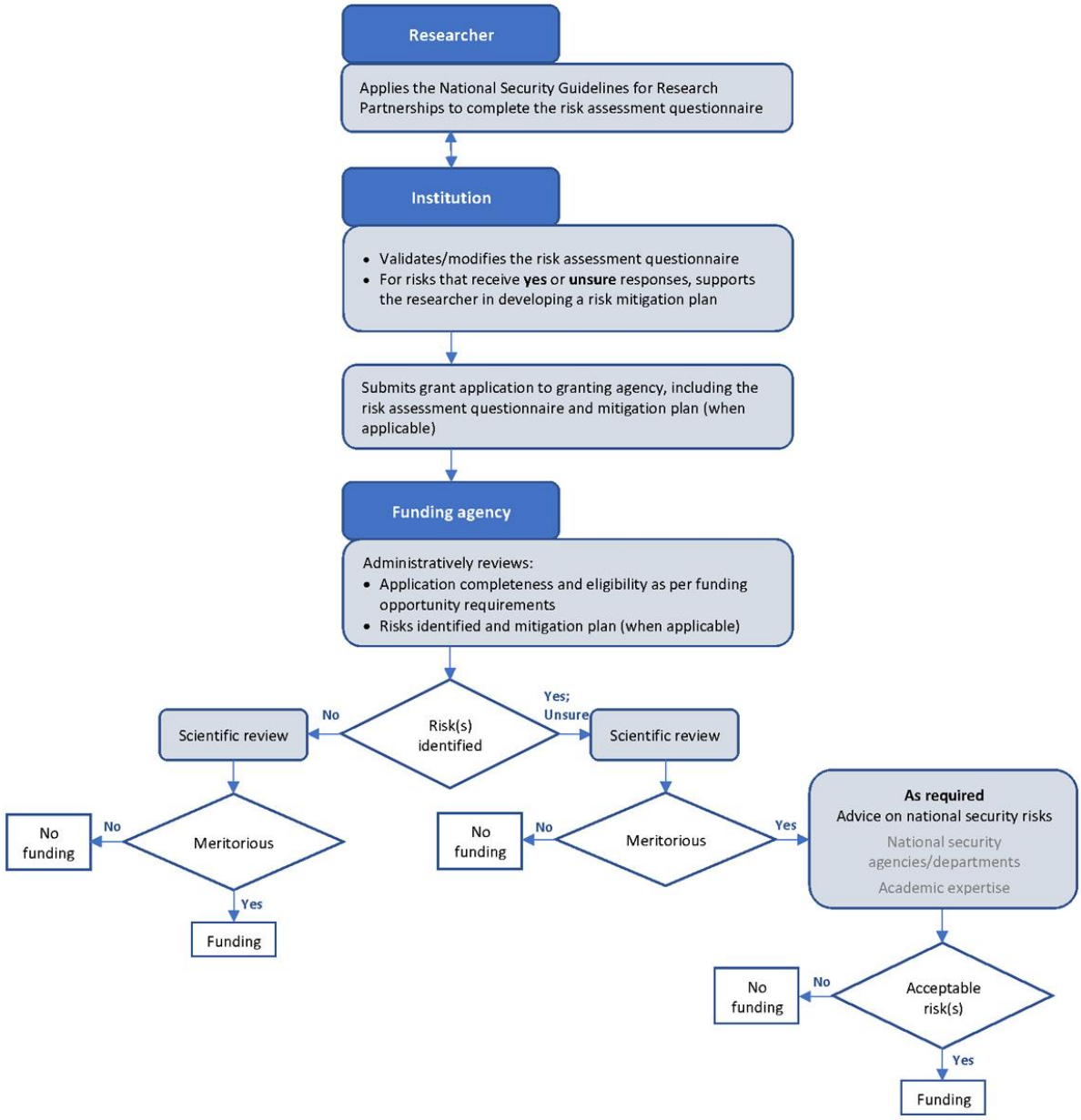
Similarly, other countries are promoting increased cooperation between research institutions, universities, and government agencies. The University Foreign Interference Taskforce is a joint initiative of the Australian Department of Education, Skills, and Employment and the Department of Home Affairs. The Taskforce's *Guidelines to Counter Foreign Interference in the Australian University Sector* (2021[14]), were developed jointly through a steering group and four working groups (Research and Intellectual Property, Foreign Collaboration, Cyber Security, Communication and Culture) with approximately 40 members from universities and government agencies, including intelligence agencies.

In the United Kingdom, the Centre for the Protection of National Infrastructure (CPNI) participates in workshops run collaboratively with partners in the academic sector to help universities manage national security risks to research. The workshops aim to help scholars to identify and manage risks and security in international research collaborations. The CPNI STEM Universities Forum was also established in 2021 to share, in confidence, mutually beneficial information on secure research collaboration. The CPNI STEM Universities Forum members are UK STEM research intensive universities and organisations, the CPNI, and the National Cyber Security Centre. Where appropriate the forum invites representatives from government and arms-length bodies.

Canada has created the Government of Canada-Universities Working Group (Government of Canada, n.d.[83]). It gathers together universities, government departments, federal granting councils, and national security agencies. The founding documents state that it "was established to advance open and collaborative research in a way that also safeguards research and maximises benefits to Canadians." At the operational level, the Natural Science and Engineering Research Council's (NSERC) Alliance Grants

Programme has implemented a risk assessment process whereby grant applications are referred to national security agencies or relevant government departments when a risk is identified (see Figure 6.1) (Government of Canada, 2021[78]).

Figure 6.1. A grant proposal risk assessment process



In the NSERC's Alliance Grants Programme (Canada), risk questionnaires (see Box 6.2) and risk mitigation plans are required and reviewed. Specific applications are referred to national security agencies or relevant government departments as necessary.
Source: *Risk Assessment Form, National Security Guidelines for Research Partnerships* (Government of Canada, 2021[78])

6.2. Funding agencies

6.2.1. Guidelines and regulations

In addition to a variety of measures to promote integrity and openness, some funding agencies are taking specific measures to address unwanted foreign interference in research. These include actions targeted at applicants and recipients of research funding, those involved in the review of research proposals and agency staff.

UK Research and Innovation (UKRI) sets clear expectations about the environment and the ways in which the research it supports should be conducted through a set of funding policies and terms and conditions, backed up by guidance and an active funding assurance or audit programme. UKRI (2021[84]) also published principles that set out its expectations for organisations that it funds in relation to due diligence for international collaboration. However, being mindful of the autonomy of research organisations, UKRI does not actively monitor compliance with its guidelines.

The U.S. National Science Foundation (NSF) forbids its staff to participate in foreign government talent recruitment programs. It has created a position of chief of research security strategy and policy, who is responsible for developing and implementing strategies to improve research security and the agency's coordination with other federal agencies (National Science Foundation, 2020[85]).

In Norway, projects funded by the National Research Council are governed by a contract. The contract requires that the project manager must comply with applicable laws and regulations, ethical guidelines as well as recognised quality standards and norms for good research practice. In Portugal, an administrative law imposes a COI declaration on all of those that have any role in the grant review process.

6.2.2. Managing conflicts of interest or commitment

Regulations or guidelines relating to declarations of COI and/or COC can be targeted at funding applicants, researchers working on projects supported by a funding agency, peer reviewers, and research agency staff. While funding agencies in different countries have more or less the same rules, they have adapted their disclosure requirements to particular contexts (see Table 6.2).

Table 6.2. Type of activity to be disclosed to funding agencies

	targets	Interests to be declared
Australian Research Council (ARC)	Funding applicants, peer reviewers and agency staff	– Professional positions – Membership of committees of other organisations – Consultancies – Foreign financial support (cash or in-kind) for research-related activities – Current or past associations or affiliations with a foreign-sponsored talent programme (for the last 10 years) – Current associations or affiliations with a foreign government, foreign political party, foreign state-owned enterprise, foreign military and/or foreign police organisations – Boards of directors – Advisory groups – Professional relationships – Family and personal relationships – Financial interests, including receiving recompense in the form of cash, services or equipment from other parties to support research activities
Canada Foundation for Innovation (CFI), Canadian	Funding applicants and peer reviewers	– Professional or personal benefit resulting from the funding opportunity or application being reviewed – A professional or personal relationship with an Applicant or the Applicant's institution

Institutes of Health Research (CIHR), Natural Sciences and Engineering Research Council of Canada (NSERC), and Social Sciences and Humanities Research Council of Canada (SSHRC)		– A direct or indirect financial interest in a funding opportunity or application being reviewed
German Research Foundation (DFG)	Peer reviewers	As a rule, the following circumstances result in exclusion: 1. First-degree relationship, marriage, life partnership, domestic partnership 2. Personal financial interest in the proposal's success or financial interest by persons listed under no. 1 3. Current or planned close scientific cooperation 4. For proposals from universities: Spokespersons from research associations are excluded from participating in the peer review panel for proposals that are decided upon in the same meeting as their own proposal. 5. Dependent employment relationship or supervisory relationship (e.g. teacher-student relationship up to and including the postdoctoral phase) extending six years beyond the conclusion of the relationship 6. a) For proposals from legal persons: The affiliation or pending transfer to this or to a participating institution. b) For proposals from natural persons: The affiliation or pending transfer to the same department or to the same non-university research institute. 7. For proposals from universities: Researchers who are active in a university council or similar supervisory board of the applying university are excluded from participating in the review and decision-making process for proposals from this university. As a rule, the following circumstances must be handled on an individual case basis: 8. Relationships that do not fall under no. 1, other personal ties or conflicts. 9. Financial interests of persons listed under no. 8. 10. For proposals from natural persons: The affiliation with or pending transfer to the same university or to the same non-university research institution. 11. Participation in university bodies other than those listed under no. 7, e.g. in scientific advisory committees in the greater research environment. 12. Research cooperation within the last three years, e.g. joint publications. 13. Preparation of a proposal or implementation of a project with a closely related research topic (competition). 14. Participation in an ongoing appointment process or one that has been completed within the past 12 months as an applicant or internal member of the appointment committee. 15. Participation in mutual review processes within the past 12 months.
UK Research and Innovation (UKRI)	Funding applicants	– Personal remuneration from organisations or project partners involved in the proposed research (other than the named employing organisation) – Significant shareholdings or other financial interests in organisations that are involved in or might benefit from the research – Research support (financial or in-kind) from commercial organisations involved in the grant or might benefit from the outcome of the research that is not mentioned in the application – Un-remunerated involvement with any organisation named on the application or which might benefit from the research or its outcomes – Political/pressure group associations – Relevant known interests of family members and persons living in the same household
U.S. Federal Research Agencies	Funding applicants	– Professional preparation (e.g. educational degrees) – Organizational Affiliations – Academic, professional or institutional appointments – Current and pending support of all R&D projects regardless of whether the support is direct monetary contribution or in-kind contribution

		– Current or pending participation in, or applications to, programmes sponsored by foreign governments, instrumentalities, or entities, including foreign government-sponsored talent recruitment programmes – Visiting scholars funded by an external entity – Students and postdoctoral researchers funded by an external entity – Paid consulting that falls outside of an individual's appointment; separate from institution's agreement – Travel supported/paid by an external entity to perform research activities with an associated time commitment – Certification by the individual that the information disclosed is accurate, current, and complete

Source: *ARC Conflict of Interest and Confidentiality Policy* (Australian Research Council, 2020[86]); *Conflict of Interest and Confidentiality* (Government of Canada, 2016[87]); *Guidelines for Avoiding Conflicts of Interest* (German Research Foundation (DFG), n.d.[88]);*Declaration of Interests: Applicants* (UK Research and Innovation (UKRI), n.d.[89]); *Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development* (National Science and Technology Council, 2022[67])

In addition to regulations and guidelines, the U.S. Government Accountability Office (GAO) (2020[90]) recommends that funding agencies have written procedures to address cases of failure to disclose required information, such as foreign affiliations. The written procedures outline investigation processes including roles and responsibilities and include administrative or enforcement actions that may be taken if allegations are substantiated. The administrative or enforcement actions available to a funding agency include asking the researcher's university to open an investigation, suspending grants, or referring cases for prosecution.

6.2.3. Risk assessment and management

Several funding agencies have integrated risk assessment into their funding application and review processes.

In Canada, applicants to the Natural Science and Engineering Research Council's (NSERC) Alliance Grants Program, a federal research funding partnership, need to fill in risk assessment questionnaires (see Box 6.2). If applicants identify risks, they need to develop risk mitigation plans. The funding agency reviews risk assessment questionnaires and risk mitigation plans before making funding decisions (see Figure 6.1).

The U.S. Department of Energy (DOE) has developed a Science and Technology Risk Matrix to identify areas of critical emerging research that do not have regulatory control mechanisms but may warrant additional protective measures due to their national or economic security implications (United States Department of Energy, 2021[91]). DOE uses this Risk Matrix to guide and manage Departmental decisions related to international engagements.

Box 6.2. Risk assessment questionnaire

In Canada, the National Security Guidelines for Research Partnerships require researchers to fill a questionnaire that includes the following yes-no questions.

Know your research

The research knowledge or intellectual property (IP) generated by this research could be of interest to foreign governments, militaries, or their proxies.

The field of research has potential military, policing, or intelligence applications, even if that is not your intended use for it.

The research falls under areas identified as sensitive.

You are working with areas covered by the Guide to Canada's Export Control List and the Nuclear Non-proliferation Import and Export Control Regulations.

You are working in research areas related to goods/technology identified in Section 35 of the Defence Production Act and known as the Controlled Goods List.

You are working in areas covered by the Export Control List, the Import Control List, and the Area Control List, as amended from time to time.

You are working in research areas related to critical minerals and critical mineral supply chains.

You are working with sensitive personal data or large amounts of data that could be sensitive in the aggregate.

You are working in research areas focused on critical infrastructure.

The research facilities or infrastructure used to support the proposed project house sensitive data and/or provide access to infrastructure unrelated to this specific partnership.

Know your partner

Your partner organization, their parent organization, and/or their subsidiaries/affiliates have affiliations or partnerships that could lead to the transfer of research to third party governments, militaries, or organizations that could negatively impact Canada’s national security.

Your partner organization, their parent organization, and/or their subsidiaries/affiliates could be subject to foreign government influence or control (e.g. there are policies and/or laws that compel knowledge transfer to that state).

There is an offer of funding where the ultimate source of the money and/or value to the funder is unclear.

There is an offer of funding which is conditional upon the researcher transferring to or replicating their work in a foreign country (e.g. setting up a mirror lab).

Your partner organization has been charged, admitted guilt, or has been convicted of fraud, bribery, espionage, corruption, or other criminal acts that could speak to a lack of transparency or ethical behaviour.

There is information to suggest that conflicts of interest or affiliations exist for any research team members that could lead to transfer of research to third party governments, militaries, or other organizations.

Your partner organization will have access to Canadian facilities, networks, or assets for conducting the research unrelated to this specific partnership.

Your partner organization is in a country listed on the Area Control List.

Source: *Risk Assessment Form* (Government of Canada, 2021[78])

Several UK research councils and the Wellcome Trust (2021[92]) include a question on grant application forms requiring applicants to consider short and medium-term risks of misuse associated with their proposal. They also provide guidance on risks of misuse to external experts who peer-review grant applications. If a situation arises where concerns about a serious risk of misuse have been raised and the concerns cannot be solved - via management strategies agreed with host institutions - an application will not be funded. Researchers are expected to notify funders and host institutions of any newly emerging risks in relation to dual-use research of concern that emerge during a project and may not have been identified at the grant application stage.

The German Research Foundation (DFG) and the National Academy of Sciences Leopoldina have developed guidelines to minimise risks of misuse and assist self-regulation by individual researchers, research institutions and universities (German Research Foundation (DFG) and German National Academy of Sciences Leopoldina, 2014[93]). The guidelines recommend individual researchers implement risk analysis, risk minimisation, responsible publication of sensitive results and abstain from research that has a high risk of misuse. Research institutions and universities are recommended to develop ethical rules for handling security-relevant research in addition to complying with legal regulations. In addition to the guidelines, the DFG includes the handling of security-related aspects of research projects in its application guidelines. Applicants are required to assess whether their proposed projects involve immediate risks of dual-use. If such risks exist, they need to present a risk-benefit analyses and describe measures to minimise the risks. If the applicants' research institutions or universities have research ethics committees, the committees need to be consulted in advance and statements from the committees need to be attached to the research proposals (German Research Foundation (DFG), n.d.[94]).

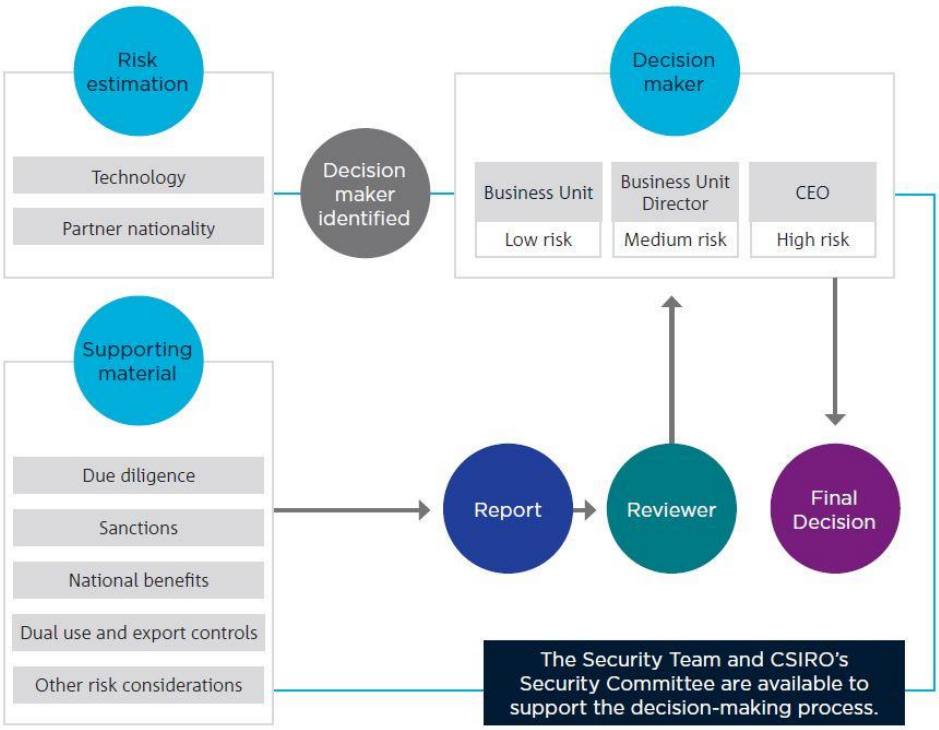
6.3. Public research institutions

Some public research institutions (PRIs) are parts of government ministries or agencies and have a mission to promote research and innovation in specific sectors of their national economies. In this situation, researchers are employed as public servants at these PRIs and are subject to relevant regulations and guidance that apply to public servants more broadly. In other contexts, PRIs may be independent from governments and able to set their own employment conditions in a way that is a similar to the operation of universities in many countries – noting also that university staff can have public servant status in some countries.

The U.S. Department of Energy (DOE) prohibits its employees and contractors from working in the DOE complex while concurrently participating in certain foreign government sponsored talent recruitment programmes or certain foreign government sponsored or affiliated activities.

In 2020-2021, the Commonwealth Scientific and Industrial Research Organisation (CSIRO) in Australia developed the Research Engagements Sensitivities Tool (REST) to assess foreign interference risks and systematically make decisions on new research opportunities. The rank of the final decision maker for project approval corresponds to the assessed risk level of a project. When reviewers identify high risks, the CEO must approve any collaboration with new partners (see Figure 6.2). The CSIRO has begun sharing its tools and know-how for risk assessment with Australian Universities.

Figure 6.2. Research Engagements Sensitivities Tool (REST)



The CSIRO in Australia developed the Research Engagements Sensitivities Tool (REST) to assess foreign interference risks and systematically make decisions on new research opportunities.

In Germany, the Max Planck Society has recently developed new guidelines for its researchers (Max Planck Society, 2021[95]). The guidelines recommend researchers to identify and minimise risks relating to human rights, academic freedom, and scientific espionage before they start international collaboration. In addition, administrative headquarters need to approve third-party funds before researchers can accept such funds (Max Planck Society, 2021[96]). When researchers have questions about rules, an ombudsperson can provide them with confidential advice (Max Planck Society, n.d.[97]). In a similar line to the Max Planck Society, the Leibniz Association requires its institutions and researchers to assess political situations in partner countries and the associated motivation of research partners (Leibniz Association, 2021[98]).

6.4. University associations

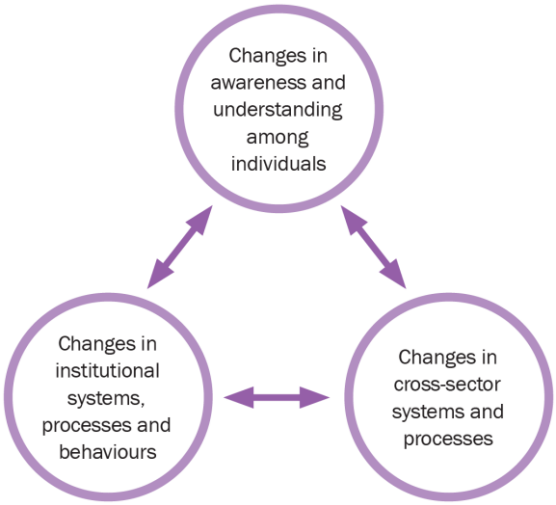
University associations can play an important role in providing guidance to universities. The U15 Group of Canadian Research Universities, a collective of some of Canada's most research-intensive universities, has published a guide, *Mitigating Economic and/or Geopolitical Risks in Sensitive Research Projects* (2019[99]). It aims to provide researchers and research service offices with practical advice and best practices to undertake an economic and geopolitical risk assessment and mitigate key risks. The guide contains practical checklists and a matrix to assess economic and geopolitical risks. The checklist cover topics such as building a strong project team; assessing non-academic partners; cybersecurity and data management; reviewing the use of research findings; and international travel.

In the United States, the Association of Public Land-grant Universities (APLU) and the Association of American Universities (AAU) (2020[100]), published the University Actions to Address Concerns about Security Threats and Undue Foreign Government Influence on Campus. They surveyed practices that universities are employing to ensure the security of research, protect against intellectual property theft and academic espionage, and prevent actions or activities by foreign governments and/or other entities that seek to exert undue foreign government influence or infringe on core academic values. The AAU and the APLU (2021[101]) identified fundamental principles and values that should be maintained in response to security concerns. The values include academic freedom, free expression, inclusion, diversity, transparency, and collaboration as well as the declaration of possible conflicts of interest and respect for intellectual property. They also call on the government to minimise administrative barriers to the establishment of both informal collaborations and formal agreements with international researchers.

The German Rectors' Conference formulated guidelines and standards for international partnerships for German universities (2020[102]). Regarding joint research, the guidelines are based on the principles of freedom of research, added value of joint research, observance of scientific, ethical, and legal standards, equal partnership, and promoting researcher mobility. Ethical and legal standards include laws for the protection of intellectual property as well as regulations on handling security-related research. The German Academic Exchange Service has also published guidelines and provides a contact point for advice to help universities assess international partnerships.

Universities UK (UUK) (2020[12]), the representative organisation for the UK's universities, has published guidelines to support universities, enabling them to protect themselves, their staff, and students, and also manage risks associated with internationalisation. The guidelines include key actions and case studies for governing bodies and executive leaders of universities. The UUK argues that changes in awareness and understanding among individuals, changes in institutional systems, processes, and behaviours and changes in cross-sector systems and processes are essential to mitigate international security threats while maintaining sustainable and secure international partnerships (see Figure 6.3). The UUK affirms that senior university leaders can improve institutional resilience to security-related issues by developing a risk-aware culture.

Figure 6.3. Intermediate outcomes for Universities UK's approach to security-related issues



Universities UK (UUK) set three long-term goals on security-related issues: 1) UK universities can demonstrate that they have coherent, proactive, strategic, and operational approaches to managing and mitigating international security threats; 2) UK universities are confident and able to pursue sustainable, secure international partnerships; 3) The UK higher education sector and the government have a clear, collaborative and constructive approach towards protecting and promoting growth in research and innovation (R&I), institutional autonomy and academic freedom in the context of security challenges. To achieve long-term goals, the UUK has identified three intermediate outcomes: a) increased awareness and understanding among individuals, both staff and students, of security-related issues, b) stronger institutional systems, processes and behaviours, and c) wider changes to the ecosystem including the interface between universities and government, and in the resilience of the system. These intermediate outcomes overlap with each other and are mutually reinforcing.
Source: *Managing Risks in Internationalisation: Security Related Issues* (Universities UK, 2020[12])

The Universities UK (UUK) recommends that universities consider reputational, ethical and security risks in addition to financial risks (Universities UK, 2020[12]). UUK identifies actions that universities should take, including knowing your partner, making risk-informed decisions, striking and maintaining robust agreements, and establishing a clear set of roles and responsibilities for staff. These are seen as part of overall due diligence processes that assess the security-related risks and mitigate potential damage to universities (see Box 6.3). Due diligence is also seen as critical to protecting staff and students travelling and working abroad.

Box 6.3. Implementation of due diligence processes

The Universities UK (UUK) action list to ensure due diligence

Know your partner

- Support staff to make informed decisions, including requiring staff to disclose partnerships and collaborations wherever possible

Make risk-informed decisions

- Ask partner organisations to complete a questionnaire or submit documentation or evidence
- Make use of the academic experts employed at their institution, web searches, subscription services and professional firms

Strike and maintain robust agreements

- Use best-practice contracting mechanisms and policies to manage security-related risks
- Include clauses that protect the integrity of academic activity in terms and conditions of agreements or memoranda of understanding
- Review regularly international partnerships and projects as well as sources of income, such as investments, donations, philanthropy, commercialisation, capital investment, tuition fee income and staff honorary and consultancy appointments
- Have an appropriate exit strategy to withdraw from agreements without incurring any liabilities if the ongoing due diligence exercise reveals that the overseas organisation or researcher is no longer an appropriate partner

Establish clear roles and responsibilities for staff

- Support staff to identify security-related risks and to act on them

Source: *Managing Risks in Internationalisation: security related issues* (Universities UK, 2020[12])

The Swedish Foundation for International Cooperation in Research and Higher Education (STINT) has developed *Responsible Internationalisation: Guidelines for Reflection on International Academic*

Collaboration (Shih, Gaunt and Östlund, 2020[103]) that include key questions to be addressed at different stages of a collaboration. Some of these questions assess risks that may restrict academic freedom (see Box 6.4). These guidelines provide a basis for dialogue between and within Swedish universities.

Box 6.4. Protecting academic freedom

Responsible Internationalisation: Guidelines for Reflection on International Academic Collaboration lists the following questions to assess risks that may restrict academic freedom or infringe Swedish laws or international treaties:

Academic freedom

- Does the way the project is funded entail risks regarding independence, integrity, ethics, or academic freedom?
- Do researchers and HEIs have overall and relevant knowledge of the political, social, and cultural conditions in the partner country?
- What type of support is offered to researchers at institutional level to help them understand and navigate the context of the partner country?
- Could a collaboration affect the independence of one's own HEI in relation to other parties?
- What should be done when academic freedom is restricted? Where should the line be drawn? How does this research affect the project partner?

Legal context

- Are there direct risks for dual use of research results?
- Are there research results that may be regarded as strategic products?
- Could the scientific content of the project be restricted by international sanctions?

Source: *Responsible Internationalisation: Guidelines for reflection on international academic collaboration* (Shih, Gaunt and Östlund, 2020[103])

6.5. Universities

6.5.1. Policies and guidelines

A number of individual universities in different countries have begun to set their own rules and guidelines to mitigate risks to research security and to promote and secure research integrity and freedom of scientific research. These policies have often been developed after individual cases of concern have come to light or after discussions with national security agencies. Some illustrative examples of what universities are doing are given in this section, although an exhaustive review of all relevant activities was beyond the scope of this report.

The University of Texas at Austin (n.d.[104]) aims "to provide a transparent system of disclosure, approval, and documentation of employees' activities outside of the university that might otherwise raise concerns about conflicts of interest or conflicts of commitment." The university policy requires researchers to complete a Financial Interest Disclosure and complete mandatory training. The University of Michigan (USA), Rochester University (USA), the University of Toronto (Canada) and McGill University (Canada) have developed similar policies that aim to not only ensure compliance with domestic laws, but also to protect freedom of scientific research from illegal foreign interference.

Rochester University's interim guidelines (Committee on Science and Security, 2019[105]) cover every aspect of research collaboration, whether on campus or abroad. Disclosure of any kind of international collaboration and support is required (talent programme, grants, gifts, etc.) and this is now the case in many U.S. universities. Rochester University also closely oversees visitors, including students, faculty and researchers, or short-term visitors (lab and facility visits, guest lecturers, speakers), to make sure its policies are respected.

The University of Toronto has developed a *Research Partnership Security Checklist for International Partnerships* (University of Toronto, 2021[106]). The checklist assists principal investigators to assess the suitability and potential risks of engaging with an international partner before proceeding with a specific project. Principal investigators need to complete the checklist within two weeks of submitting research proposals or before initiating international research partnerships.

6.5.2. Management and oversight

Some Universities give responsibility to dedicated committees or structures to manage research security risks.

For instance, the University of Michigan has a Research COI Committee (University of Michigan, n.d.[107]). The committee reviews the disclosures of outside activities from researchers whose research proposals will be sponsored to determine whether an external activity could directly and significantly affect the design, conduct, or reporting of research. A review by the Research COI Committee aims to ensure that the personal interests of an individual do not unduly influence his/her primary obligations to the science, the research sponsors, the university, colleagues, or students. When COIs are identified, strategies can usually be developed to enable them to be properly managed.

In the Netherlands, a Knowledge Security Advisory Team exists in every university (Association of Universities in the Netherlands (VSNU), 2021[82]). This a virtual team made up of relevant experts on safety risk management, information security and international collaboration and it can co-opt additional experts on specific research topics, countries and human resource issues, etc. This team supports the executive board of a university to make decisions on knowledge security issues. When a small university does not have all expertise needed to assess knowledge security risks, the university can 'borrow' expertise from a Knowledge Security Advisory Team at another university.

Whilst most universities in most countries do not have dedicated committees to manage research security and conflicts of interest, many of them do have structures that might be considered as having responsibility for these issues. Institutional review boards, ethics committees, and research integrity committees may all play a role in different contexts, provided that they are appropriately constituted and resourced.

6.5.3. Research security training

Some universities are taking action to raise staff awareness about research security issues through training programmes.

The University of Michigan offers training options related to research ethics and compliance. The Programme for Education and Evaluation in Responsible Research and Scholarship provides online training modules for faculty, staff, and students (University of Michigan, n.d.[108]). Topics cover include research integrity, conflicts of interest, export controls, and research information security. Initially the training this was a requirement only for people working on federally funded projects but now all faculty, staff, and students involved in scholarship and research are expected to complete the training.

In Sweden, Lund University requires all PhD students to take a research ethics course. The course aims to provide a foundation of research integrity and knowledge of research ethics, including ethical challenges in the development and implementation of new technologies (Lund University, 2020[109]). In Norway, the

Act on ethics and integrity in research requires all research institutions and universities to provide education in research ethics, including misuse of new technologies, to all employees and researchers (Langtvedt, 2020[110]). As these initiatives already explicitly address issues related to research integrity and misuse of new technologies, it is easy to imagine that they can be extended, as necessary, to address broader issues relating to research security. Likewise, there are undoubtedly many other education and training activities in Universities across the world that could be readily adapted to incorporate research security.

6.6. International research projects and infrastructures

The research that is carried out in some international research projects or research infrastructures is related to recognised dual-use technologies, for example research in some areas of nuclear physics or biodefence. In these cases, the research is conducted within the established frameworks of national and international regulations and conventions that relate to those technologies. However, most international research projects and infrastructures address topics that are not covered by international conventions and not considered as sensitive topics in many countries. Large scale international projects and infrastructures often have their own governance structures and, in a few cases, have autonomous international legal status. Funding and ownership may be shared across many countries and, in this context, national and economic security concerns and views on foreign interference take on a different perspective.

An illustrative example is the Human Brain Project (HBP) funded by the European Union. This major international project has developed a dedicated Responsible Research and Innovation framework to ensure that it all its activities are carried out in accordance with established ethical principles and the legal regulations that are applicable in different jurisdictions. This includes specific attention to human rights and data protection. The project monitors political, security, intelligence, and military uses/misuse of scientific and technological findings as well as responding to ethical and societal concerns emerging as the research progresses (Human Brain Project, n.d.[111]).

6.7. Academic associations

Academic associations play an important role in providing guidelines to their members and the broader research community. The National Academies of Sciences, Engineering and Medicine in the United States has launched a National Science, Technology and Security Roundtable (National Academies of Sciences, Engineering and Medicine, 2020[112]). The roundtable brings together individuals from research agencies, national intelligence, law enforcement, academic research, and business communities. It identifies and considers security risks involving federally funded research and development, identifies effective approaches for communicating risks to the academic and scientific community, and shares best practices for mitigating the risks.

The UK Royal Society (2021[113]) provided comments on the Foreign Influence Registration Scheme (FIRS) when it was under consideration by the Government of the United Kingdom. In a letter to the Home Office, the Society acknowledged that there are threats from hostile activities, including theft, misuse, or exploitation of research and loss of personal information. If these threats are not addressed they can result in damage to individuals or institutional reputation and, in some instances, present a wider threat to society. At the same time, the Society emphasised the risk that over-zealous regulations could have a chilling effect on the academic research community and act as a deterrent to international research collaboration. This public feedback has helped establish the key parameters that need to be considered and balanced in developing appropriate policy action.

The German Academy of Sciences Leopoldina regularly organises conferences and workshops on the handling of security-relevant research and invites experts from various disciplines (German National

Academy of Sciences Leopoldina, n.d.[114]). The events aim to raise awareness among researchers of security-relevant aspects of their research and to share experiences. Participants discuss specific security-relevant research projects and whether self-regulated restrictions for researchers are sufficient to prevent dystopian scenarios of malicious use. The German Academy of Sciences Leopoldina helps German research institutions and universities establish local committees responsible for ethics in security-relevant research. 130 local committees or contact persons are now actively helping the research community in ethical assessments of security-relevant research projects (German National Academy of Sciences Leopoldina and German Research Foundation (DFG), 2020[115]; German National Academy of Science Leopoldina, n.d.[116]).

JASON, an independent advisory group of scientists from the United States, has proposed a series of instructive questions that principal investigators need to consider before engaging with foreign research entities, and the questions have been utilised as a toolkit/checklist by American researchers (JASON, 2019[1]).

6.8. Multilateral activities

The G7 countries established a working group on the Security and Integrity of the Research Ecosystem (SIGRE) in mid-2021 that aims to develop a common set of principles that will help to protect the research and innovation ecosystem across the G7 from risks to open and reciprocal research collaboration (G7, 2021[117]). The working group plans to develop proposals for a virtual academy and toolkit, bringing together the skills and experience of researchers, innovators, business leaders, and policy makers to develop a shared understanding of research integrity and security. This will extend on an established dialogue among the Five Eyes countries, including Australia, Canada, New Zealand, the United Kingdom, and the United States, on promoting and protecting the integrity of the international research and development enterprise.

The European Commission recently published a toolkit on how to mitigate foreign interference in research and innovation (European Commission, 2022[118]). The toolkit outlines best practices to support research institutions and universities in safeguarding their fundamental values, including academic freedom, integrity and institutional autonomy, as well as to protect their staff, students, research findings and assets. In addition to the toolkit, the classification of information in Horizon Europe projects identifies research subjects and types of information that are potentially sensitive and are subject to specific risk assessment and management procedures(see Table 6.1) (European Commission, 2021[71]).

The Asia-Pacific Economic Cooperation (APEC) forum has developed *APEC Guiding Principles for Research Integrity* to clarify responsibilities in conducting and administrating research (APEC Human Resources Development Working Group, 2022[119]). To increase transparency, the principles recommend that researchers disclose financial, familial, scholarly, professional, and other interests that may be a perceived, potential, or actual conflict of interest. At the same time, it is recommended that research institutions provide frameworks to support researchers to disclose and manage their interests.

At the funding agency level, Science Europe and the Global Research Council (GRC), which are networks of research-funding organisations, initiated a discussion in 2021 on research ethics, integrity, and culture that was stimulated by experiences in the scientific response to COVID-19. . At its plenary meeting in May 2022, the GRC approved a *Statement of Principles and Practices for Research Ethics, Integrity, and Culture in the Context of Rapid-Results Research* (Global Research Council, 2022[120]). This includes consideration of issues related to research security.

7 Concluding remarks

In an unpredictable and rapidly changing world, science provides new knowledge that is critical for informing the policy decisions and development of technologies that are necessary to address global societal challenges. International collaboration and scientific freedom are essential for scientific progress. However, there are increasing concerns in many countries about the misappropriation and censure of science and foreign interference in research. These are serious threats to the integrity of the global research ecosystem and policy action is required to ensure that they are recognised and managed in a way that strengthens both the security and integrity of research and promotes public trust.

This report describes policy initiatives and actions to safeguard national and economic security whilst protecting freedom of enquiry, promoting international research cooperation, and ensuring openness and non-discrimination. Responsibilities for research integrity and security are distributed across several actors in the international research ecosystem. These include national governments; research funding agencies; research institutions and universities; and academic and university associations. These actors need to work together, both nationally and internationally to develop and implement effective policies that will help ensure trust in science in the future.

The seven over-arching recommendations summarised at the outset of this report (see Section 2) should help countries to address research security as part of a broader framework of research integrity. For each recommendation, a number of policy options are proposed, based on the examples of good practices that are described in section 6.

Although research integrity and security is a common concern across OECD countries, the context varies considerably. As a consequence, the priority attached to each policy recommendation and the related options for action are also likely to vary across countries. Governments, funding agencies, research institutions, and universities need to regularly assess the maturity of their security strategies and adjust policy initiatives or actions to ensure effectiveness while monitoring unintended consequences.

References

116th Congress (2021), *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021*, https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf. [64]

All European Academies (2017), *The European Code of Conduct for Research Integrity*, https://www.allea.org/wp-content/uploads/2017/05/ALLEA-European-Code-of-Conduct-for-Research-Integrity-2017.pdf. [34]

American Association of University Professors (2014), *Recommended Principles to Guide Academy-Industry Relationships*, The AAUP Foundation, https://www.aaup.org/file/Academy-Industry%20Relationships_0.pdf. [4]

APEC Human Resources Development Working Group (2022), *APEC Guiding Principles for Research Integrity*, https://www.apec.org/apecapi/publication/getfile?publicationId=1a7ab7d8-6d0c-4d94-be4b-2342cd08cdfa. [119]

Association of American Universities (AAU) and Association of Public Land-grand Universities (APLU) (2021), *Principles and Values to Guide Actions Relevant to Foreign Government Interference in University Research*, https://www.aau.edu/key-issues/principles-and-values-guide-actions-relevant-foreign-government-interference-university. [101]

Association of Universities in the Netherlands (VSNU) (2021), *Framework Knowledge Security Dutch Universities*, https://www.universiteitenvannederland.nl/files/documenten/Domeinen/Integrale%20veiligheid/VSNU%20Framework%20Knowledge%20Security%20Dutch%20Universities.pdf. [82]

Association Public Land-grant Universities (APLU); Association of American Universities (AAU); (2020), *University Actions to Address Concerns about Security Threats and Undue Foreign Government Influence on Campus*, https://www.aplu.org/members/councils/governmental-affairs/CGA-library/effective-science-and-security-practices---what-campuses-are-doing/file. [100]

Australian Research Council (2020), *ARC Conflict of Interest and Confidentiality Policy*, https://www.arc.gov.au/policies-strategies/policy/arc-conflict-interest-and-confidentiality-policy/arc-conflict-interest-and-confidentiality-policy. [86]

Australian Security Intelligence Organisation (2020), *ASIO Submission to the Parliamentary Joint Committee on Intelligence and Security*, https://www.aph.gov.au/DocumentStore.ashx?id=9f0851be-082b-4b56-ac25-873163fb73c4&subId=699731. [3]

BBSRC, MRC and Wellcome Trust (2015), *BBSRC, MRC and Wellcome Trust Position Statement on Dual Use Research of Concern and Research Misuse*, https://cms.wellcome.org/sites/default/files/wtp059491.pdf. [10]

Bekkers, F., W. Oosterveld and P. Verhagen (2019), *Checklist for Collaboration with Chinese Universities and Other Research Institutions*, https://hcss.nl/report/checklist-for-collaboration-with-chinese-universities-and-other-research-institutions/. [48]

Bladwin, D. (1997), "The concept of security", *Review of International Studies*, Vol. 23/1, pp. 5-26, https://doi.org/10.1017/s0260210597000053. [129]

Canadian Centre for Cyber Security (2020), *Cyber Threat Bulletin: Impact of COVID-19 on Cyber Threats to the Health Sector*, https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-impact-covid-19-cyber-threats-health-sector. [55]

Centre for the Protection of National Infrastructure (CPNI) (2020), *Trusted Research Guidance for Academia*, https://www.cpni.gov.uk/trusted-research-guidance-academia. [73]

Centre for the Protection of National Infrastructure (CPNI) (n.d.), *Checklist: Evaluating research proposals*, https://www.cpni.gov.uk/system/files/Trusted%20Research%20Checklist%20for%20Academia.pdf. [74]

Centre for the Protection of National Infrastructure (CPNI) (n.d.), *Trusted Research Guidance for Academics*, https://www.cpni.gov.uk/system/files/Trusted%20Research%20Guidance%20for%20Academia.pdf. [56]

Cho, I., B. Kingdollar and M. Soshi (2021), *Harvard professor Charles Lieber found guilty of lying about China ties*, The Harvard Crimson, https://www.thecrimson.com/article/2021/12/22/lieber-verdict-day6/?utm_source=Nature+Briefing&utm_campaign=f22b5a5686-briefing-dy-20220104&utm_medium=email&utm_term=0_c9dfd39373-f22b5a5686-45800330#.YeJY0h5Mxws.link (accessed on 15 January 2022). [63]

Committee on Economic, Social and Cultural Rights (2020), *General Comment No. 25 (2020) on Science and Economic, Social and Cultural Rights (Article 15 (1) (b), (2), (3) and (4) of the International Covenant on Economic, Social and Cultural Rights)*, https://undocs.org/E/C.12/GC/25. [136]

Committee on Responsible Science et al. (2017), *Fostering Integrity in Research*, National Academies Press, Washington, D.C., https://doi.org/10.17226/21896. [7]

Committee on Science and Security (2019), *International Research & Global Collaboration*, http://www.rochester.edu/research/pdfs/international-research-guidelines.pdf. [105]

Department for Business, Energy & Industrial Strategy (2021), *National security and investment act: guidance for the higher education and research-intensive sectors*, https://www.gov.uk/government/publications/national-security-and-investment-act-guidance-for-the-higher-education-and-research-intensive-sectors/national-security-and-investment-act-guidance-for-the-higher-education-and-research-intensive-sectors (accessed on 5 August 2021). [68]

Department of Education, Skills and Employment (2021), *Case studies – cybersecurity*, https://www.dese.gov.au/guidelines-counter-foreign-interference-australian-university-sector/case-studies/case-studies-cybersecurity (accessed on 13 January 2022). [58]

Department of Education, Skills and Employment (2021), *Case studies – due diligence, risk assessments and management*, https://www.dese.gov.au/guidelines-counter-foreign-interference-australian-university-sector/case-studies/case-studies-due-diligence#toc-case-study-1-safeguarding-national-security (accessed on 13 January 2022). [46]

Department of Education, Skills and Employment (2021), *Case studies – governance and risk frameworks*, https://www.dese.gov.au/guidelines-counter-foreign-interference-australian-university-sector/case-studies/case-studies-governance-and-risk-frameworks#toc-case-study-3-protecting-academic-freedom (accessed on 13 January 2022). [52]

Department of Justice (2021), *Hospital researcher sentenced to prison for conspiring to steal trade secrets and sell to China*, https://www.justice.gov/opa/pr/hospital-researcher-sentenced-prison-conspiring-steal-trade-secrets-and-sell-china (accessed on 24 March 2022). [41]

Department of Justice (2020), *The China Initiative: year-in-review (2019-20)*, https://www.justice.gov/opa/pr/china-initiative-year-review-2019-20 (accessed on 13 May 2022). [61]

Department of Justice (2018), *Attorney general Jeff Session's China Initiative fact sheet*, https://www.justice.gov/opa/speech/file/1107256/download (accessed on 18 June 2020). [62]

Department of Justice (n.d.), *Information about the Department of Justice's China Initiative and a compilation of China-related prosecutions since 2018*, https://www.justice.gov/nsd/information-about-department-justice-s-china-initiative-and-compilation-china-related (accessed on 8 May 2021). [60]

D'Hooghe, I. and J. Lammertink (2020), *Towards Sustainable Europe-China Collaboration in Higher Education in Research*, https://leidenasiacentre.nl/wp-content/uploads/2020/10/Towards-Sustainable-Europe-China-Collaboration-in-Higher-Education-and-Research.pdf. [2]

European Commission (2022), *Tackling R&I Foreign Interference*, https://doi.org/10.2777/513746. [118]

European Commission (2021), *Classification of Information in Horizon Europe Projects*, https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/classification-of-information-in-he-projects_he_en.pdf. [71]

European Commission (2020), *Concept Note on Tackling Foreign Interference in Higher Education Institutions and Research Organisations*, https://s3.eu-central-1.amazonaws.com/euobs-media/3ef6dc3d60ee27a2df16f62d47e93fdc.pdf. [132]

European Union Science Diplomacy Alliance (n.d.), *www.science-diplomacy.eu*, https://www.science-diplomacy.eu/ (accessed on 22 January 2022). [18]

Fedasiuk, R. and E. Weinstein (2020), *Universities and the Chinese Defense Technology Workforce*, Center for Security and Emerging Technology, https://doi.org/10.51593/20200043. [131]

Flagg, M. and Z. Arnold (2021), *New Research Security Institutions Short Policy Brief*, Center for Security and Emerging Technology, https://doi.org/10.51593/20200051. [130]

Foreign & Commonwealth Office and Foreign, Commonwealth & Development Office (2013), *Academic Technology Approval Scheme (ATAS)*, https://www.gov.uk/guidance/academic-technology-approval-scheme (accessed on 5 August 2021). [69]

French Presidency of the Council of the European Union (2022), *Marseille Declaration on International Cooperation in Research and Innovation (R&I)*, https://presidence-francaise.consilium.europa.eu/media/xi1khxzg/marseille-declaration.pdf. [32]

G7 (2021), *G7 Research Compact*, https://www.g7uk.org/wp-content/uploads/2021/06/G7-2021-Research-Compact-PDF-356KB-2-pages-1.pdf. [117]

Gattolin, A. (2021), *Rapport D'information*, http://www.senat.fr/rap/r20-873/r20-8731.pdf. [51]

German National Academy of Science Leopoldina (n.d.), *Contact persons and commissions in Germany responsible for ethics of security-relevant research*, https://www.leopoldina.org/ueber-uns/kooperationen/gemeinsamer-ausschuss-dual-use/kommissionsliste/?tx_leoinstitutions_institutionslist%5Baction%5D=list&tx_leoinstitutions_institutionslist%5Bcontroller%5D=List&cHash=8e12faffd7dcfa05a6ef95703d72a04a (accessed on 23 February 2022). [116]

German National Academy of Sciences Leopoldina (n.d.), *Conferences and workshops of the Joint Committee on the Handling of Security-Relevant Research*, https://www.leopoldina.org/en/about-us/cooperations/joint-committee-on-dual-use/dual-use-conferences-and-workshops/. [114]

German National Academy of Sciences Leopoldina (n.d.), *Information on selected security-relevant research topics and case studies*, https://www.leopoldina.org/en/about-us/cooperations/joint-committee-on-dual-use/research-topics-and-case-studies/#c8500 (accessed on 16 January 2022). [43]

German National Academy of Sciences Leopoldina and German Research Foundation (DFG) (2020), *Joint Committee of the DFG and Leopoldina on the Handling of Security-Relevant Research - Third Progress Report*, https://www.leopoldina.org/uploads/tx_leopublication/2020_Progress_Report_Joint_Committee_Dual_Use.pdf. [115]

German Rectors' Conference (2020), *Guidelines and Standards in International University Cooperation*, https://www.hrk.de/resolutions-publications/resolutions/beschluss/detail/guidelines-and-standards-in-international-university-cooperation/. [102]

German Research Foundation (DFG) (n.d.), *Guidelines for Avoiding Conflicts of Interest*, https://www.dfg.de/formulare/10_201/10_201_en.pdf. [88]

German Research Foundation (DFG) (n.d.), *Proposal Preparation Instructions*, https://www.dfg.de/formulare/54_01/54_01_en.pdf. [94]

German Research Foundation (DFG) and German National Academy of Sciences Leopoldina (2014), *Scientific Freedom and Scientific Responsibility*, https://www.dfg.de/download/pdf/dfg_im_profil/geschaeftsstelle/publikationen/stellungnahmen_papiere/2014/dfg-leopoldina_forschungsrisiken_de_en.pdf. [93]

Global Research Council (2022), *Statement of Principles and Practices for Research Ethics, Integrity, and Culture in the Context of Rapid-Results Research*, https://globalresearchcouncil.org/fileadmin/documents/GRC_Publications/SoP_Research_Ethics_May_2022.pdf. [120]

Global Research Council (n.d.), *Statement of Principles for Research Integrity*, https://www.globalresearchcouncil.org/fileadmin/documents/GRC_Publications/grc_statement_principles_research_integrity_FINAL.pdf. [121]

Government Accountability Office (2020), *Agencies Need to Enhance Policies to Address Foreign Influence*, https://www.gao.gov/assets/gao-21-130.pdf. [90]

Government of Canada (2021), *Executive summary of national security guidelines for research partnerships*, https://www.ic.gc.ca/eic/site/063.nsf/eng/h_98256.html (accessed on 5 August 2021). [70]

Government of Canada (2021), *Risk assessment form*, https://www.ic.gc.ca/eic/site/063.nsf/eng/h_98257.html (accessed on 5 August 2021). [78]

Government of Canada (2021), *Safeguarding your research*, https://www.ic.gc.ca/eic/site/063.nsf/eng/h_97955.html (accessed on 13 May 2022). [79]

Government of Canada (2021), *Scenario 2 - participation in foreign talent and recruitment programs*, https://www.ic.gc.ca/eic/site/063.nsf/eng/h_98278.html (accessed on 13 January 2022). [47]

Government of Canada (2021), *Scenario 3 - insider threats and research theft*, https://www.ic.gc.ca/eic/site/063.nsf/eng/h_98279.html (accessed on 13 January 2022). [42]

Government of Canada (2021), *Scenario 5 - security and travel*, https://www.ic.gc.ca/eic/site/063.nsf/eng/h_98281.html (accessed on 13 January 2021). [59]

Government of Canada (2020), *Policy statement on research security and covid-19*, https://www.canada.ca/en/innovation-science-economic-development/news/2020/09/policy-statement-on-research-security-and-covid-19.html (accessed on 8 May 2021). [77]

Government of Canada (2016), *Conflict of interest and confidentiality*, http://www.science.gc.ca/eic/site/063.nsf/eng/h_90108244.html?OpenDocument (accessed on 9 May 2021). [87]

Government of Canada (n.d.), *About us*, https://www.ic.gc.ca/eic/site/063.nsf/eng/h_98090.html (accessed on 8 May 2021). [83]

Government of the United Kingdom (2021), *Dedicated government team to protect researchers' work from hostile activity*, https://www.gov.uk/government/news/dedicated-government-team-to-protect-researchers-work-from-hostile-activity (accessed on 4 October 2021). [75]

Government of the United Kingdom (2021), *Export controls applying to academic research*, https://www.gov.uk/guidance/export-controls-applying-to-academic-research (accessed on 23 September 2021). [40]

Human Brain Project (n.d.), *Responsible research and innovation*, https://www.humanbrainproject.eu/en/about/project-structure/work-packages/work-package-9/ (accessed on 22 January 2022). [111]

Human Rights Watch (2021), *They Don't Understand the Fear We Have*, https://www.hrw.org/report/2021/06/30/they-dont-understand-fear-we-have/how-chinas-long-reach-repression-undermines. [50]

Integrated Innovation Strategy Promotion Council (2021), *Regarding the Response Policy for Securing Research Integrity Against New Risks Associated with the Internationalization and Openness of Research Activities*, https://www8.cao.go.jp/cstp/tougosenryaku/9kai/siryo1-2.pdf. [80]

InterAcademy Partnership (IAP) (2016), *Doing Global Science: A Guide to Responsible Conduct in the Global Research Enterprise*, https://www.interacademies.org/publication/doing-global-science-guide-responsible-conduct-global-research-enterprise. [36]

International Science Council (ISC) (2018), *Statutes and Rules of Procedure*, https://council.science/wp-content/uploads/2018/06/ISC-Statutes-approved-May-2018.pdf. [31]

JASON (2019), *Fundamental Research Security*, https://nsf.gov/news/special_reports/jasonsecurity/JSR-19-2IFundamentalResearchSecurity_12062019FINAL.pdf. [1]

Kivimaa, P. (2022), "Transforming innovation policy in the context of global security", *Environmental Innovation and Societal Transitions*, Vol. 43, pp. 55-61, https://doi.org/10.1016/j.eist.2022.03.005. [128]

Langtvedt, N. (2020), *The act on ethics and integrity in research*, https://www.forskningsetikk.no/en/resources/the-research-ethics-library/legal-statutes-and-guidelines/the-act-on-ethics-and-integrity-in-research/ (accessed on 22 February 2022). [110]

Leibniz Association (2021), *Risk Management in International Scientific Cooperation – points to consider*, https://www.leibniz-gemeinschaft.de/fileadmin/user_upload/Bilder_und_Downloads/%C3%9Cber_uns/Internationales/Risk_management_in_international_scientific_cooperation.pdf. [98]

Lund University (2020), *Research Ethics*, https://www.student.lth.se/fileadmin/lth/genombrottet/Course_Plan__Research_Ethics_2021__GEM090F__ENG_.pdf. [109]

Max Planck Society (2021), *Guidelines for Responsible Conduct*, https://www.mpg.de/18156413/leitplancken.pdf. [96]

Max Planck Society (2021), *Guidelines for the Development of International Collaborations of the Max-Planck-Gesellschaft*, https://www.mpg.de/16784189/mpg-guidelines-for-international-cooperations-2021.pdf. [95]

Max Planck Society (n.d.), *Ombudspersons*, https://www.mpg.de/about-us/organisation/ombudspersons (accessed on 22 February 2022). [97]

McGill University (n.d.), *Foreign interference*, https://www.mcgill.ca/research/about/foreign-interference (accessed on 7 May 2021). [133]

Medical Research Council (MRC), Biotechnology and Biological Sciences Research Council (BBSRC), and Wellcome Trust (2021), *Managing Risks of Research Misuse: joint policy statement*, https://www.ukri.org/publications/managing-risks-of-research-misuse-joint-policy-statement/. [92]

Merriam-Webster (n.d.), *Due diligence*, https://www.merriam-webster.com/dictionary/due%20diligence (accessed on 28 September 2021). [11]

Merton, R. (1973), *The Normative Structure of Science*, University of Chicago Press, https://press.uchicago.edu/ucp/books/book/chicago/S/bo28451565.html. [141]

Ministerial Conference on the European Research Area (2020), *Bonn Declaration on Freedom of Scientific Research*, https://www.bmbf.de/files/10_2_2_Bonn_Declaration_en_final.pdf. [13]

Ministry of Education, Culture and Science (2020), *Knowledge Security in Higher Education and Research*, https://www.government.nl/documents/letters/2020/11/27/knowledge-security-in-higher-education-and-research. [81]

National Academies of Sciences, Engineering and Medicine (2020), *Co-chairs appointed to lead new national science, technology, and security roundtable*, https://www.nationalacademies.org/news/2020/10/co-chairs-appointed-to-lead-new-national-science-technology-and-security-roundtable#:~:text=Roundtable%20%7C%20National%20Academies-,Co%2DChairs%20Appointed%20to%20Lead%20New,Science%2C%20Technology%2C%20and% (accessed on 31 August 2021). [112]

National Cyber Security Centre (2019), *The Cyber Threat to Universities*, https://www.ncsc.gov.uk/report/the-cyber-threat-to-universities. [54]

National Institutes of Health (n.d.), *What is research integrity*, https://grants.nih.gov/policy/research_integrity/what-is.htm. [124]

National Science & Technology Council (2021), *Recommended Practices for Strengthening the Security and Integrity of America's Science and Technology Research Enterprise*, https://trumpwhitehouse.archives.gov/wp-content/uploads/2021/01/NSTC-Research-Security-Best-Practices-Jan2021.pdf. [72]

National Science and Technology Council (2022), *Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-supported Research and Development*, https://www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf. [67]

National Science Foundation (2020), *NSF creates new research security chief position*, https://www.nsf.gov/news/news_summ.jsp?cntn_id=300086 (accessed on 8 May 2021). [85]

National Science Foundation (n.d.), *Research security*, https://beta.nsf.gov/research-security (accessed on 24 February 2022). [45]

New Zealand Government (2021), *Trusted Research*, https://protectivesecurity.govt.nz//assets/Campaigns/PSR-ResearchGuidancespreads-17Mar21.pdf. [76]

OECD (2022), *Recommendation of the Council for Facilitating International Technology Co-operation with and among Businesses*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0282. [27]

OECD (2021), *OECD Calculations Based on Scopus Custom Data, Elsevier, Version 5.2021, September 2021*, https://stip.oecd.org/stats/SB-StatTrends.html?i=INTL_20_X&v=3&t=2006,2020&s=OECD (accessed on 2 September 2021). [19]

OECD (2021), *OECD Science, Technology and Innovation Outlook 2021: Times of Crisis and Opportunity*, OECD Publishing, Paris, https://dx.doi.org/10.1787/75f79015-en. [21]

OECD (2021), *Recommendation of the Council Concerning Access to Research Data from Public Funding*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0347. [28]

OECD (2021), *Recommendation of the Council on International Co-operation in Science and Technology*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0237. [26]

OECD (2020), *Why Open Science Is Critical to Combatting COVID-19*, https://read.oecd-ilibrary.org/view/?ref=129_129916-31pgjnl6cb&title=Why-open-science-is-critical-to-combatting-COVID-19. [22]

OECD (2019), *Recommendation of the Council on Artificial Intelligence*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449. [30]

OECD (2019), *Recommendation of the Council on Responsible Innovation in Neurotechnology*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0457#mainTex. [29]

OECD (2015), *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264245471-en. [53]

OECD (2015), "Making Open Science a Reality", *OECD Science, Technology and Industry Policy Papers*, No. 25, OECD Publishing, Paris, https://dx.doi.org/10.1787/5jrs2f963zs1-en. [15]

OECD (2009), *Co-ordinating Committee for Facilitating International Research Misconduct Investigations*, http://www.oecd.org/sti/inno/42713295.pdf. [127]

OECD (2009), *Investigating Research Misconduct Allegations in International Collaborative Research Projects*, http://www.oecd.org/sti/inno/42770261.pdf. [140]

OECD (2007), *Report from the Workshop on Best Practices for Ensuring Scientific Integrity and Preventing Misconduct*, http://www.oecd.org/science/inno/40188303.pdf. [139]

OECD (n.d.), *Scientometrics*, https://www.oecd.org/sti/inno/scientometrics.htm (accessed on 25 February 2022). [20]

Office of Science and Technology Policy (2020), *Enhancing the Security and Integrity of America's Research Enterprise*, https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/07/Enhancing-the-Security-and-Integrity-of-Americas-Research-Enterprise.pdf. [6]

Office of Science and Technology Policy (2000), "Federal policy on research misconduct", *Federal Register*, Vol. 65/235, pp. 76260-76264, https://www.govinfo.gov/content/pkg/FR-2000-12-06/html/00-30852.htm. [17]

Parliamentary Joint Committee on Intelligence and Security (2021), *Official Committee Hansard: National security risks affecting the Australian higher education and research*, https://parlinfo.aph.gov.au/parlInfo/download/committees/commjnt/3ca6fe4f-b221-48f6-812e-ccfd3cd59d55/toc_pdf/Parliamentary%20Joint%20Committee%20on%20Intelligence%20and%20Security_2021_03_19_8604_Official.pdf;fileType=application%2Fpdf#search=%22committe. [44]

PricewaterhouseCoopers Aarata LLC (2021), *Research Integrity Investigation and Analysis Report*, https://www8.cao.go.jp/cstp/english/doc/report_en.pdf. [125]

Public Safety Canada (2020), *Building Security Awareness in the Academic Community*, https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/cntr-prlfrtn/sfgrdng-scnc/_fls/sfgrdng-scnc-cdmc-cmmnty-en.pdf. [9]

Purdue University (n.d.), *Detrimental research practices (DRPs)*, https://www.purdue.edu/gradschool/academics/detrimental-research-practices.html (accessed on 26 September 2021). [8]

Royal Society (2021), *Royal Society Submission to Home Office Consultation on Legislation to Counter State Threats*, https://royalsociety.org/topics-policy/publications/2021/royal-society-submission-to-home-office-consultation-on-legislation-to-counter-state-threats/. [113]

Science Europe (2016), *Research Integrity Practices in Science Europe Member Organisations*, https://doi.org/10.5281/zenodo.5060196. [35]

Shih, T., A. Gaunt and S. Östlund (2020), *Responsible Internationalisation: Guidelines for Reflection on International Academic Collaboration*, https://www.stint.se/wp-content/uploads/2020/02/STINT__Responsible_Internationalisation.pdf. [103]

Sutrop, M., M. Parder and M. Juurik (2020), "Research ethics codes and guidelines", in *Handbook of Research Ethics and Scientific Integrity*, Springer International Publishing, Cham, https://doi.org/10.1007/978-3-030-16759-2_2. [16]

Tardell, M. (2021), *Swedish Experiences of Research Collaboration with China: Challenges and the Way Forward*, https://www.ui.se/globalassets/ui.se-eng/publications/other-publications/swedish-experiences-of-research-collaboration-with-china.pdf. [49]

The Norwegian National Research Ethics Committees (2016), *Guidelines for Research Ethics in Science and Technology*, https://www.forskningsetikk.no/globalassets/dokumenter/4-publikasjoner-som-pdf/60126_fek_guidelines_nent_digital.pdf. [122]

The University of Texas at Austin (n.d.), *Conflict of interest, conflict of commitment, & outside activities*, https://provost.utexas.edu/policies-and-compliance/conflict-of-interest (accessed on 9 July 2020). [104]

The White House (2021), *Clear rules for research security and researcher responsibility*, https://www.whitehouse.gov/ostp/news-updates/2021/08/10/clear-rules-for-research-security-and-researcher-responsibility/ (accessed on 14 January 2022). [66]

The White House (2021), *Presidential Memorandum on United States Government-Supported Research and Development National Security Policy*, https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/?utm_source=link. [65]

U15 Group of Canadian Research Universities (2019), *Mitigating Economic and/or Geopolitical Risks in Sensitive Research Projects*, https://telfer.uottawa.ca/assets/research/documents/docs/Mitigating-economic-and-or-geopolitical-risks-in-sensitive-research-projects-dec-2019.pdf. [99]

U15 Group of Canadian Research Universities and Universities Canada (2019), *Travel Security Guide for University Researchers and Staff*, https://www.univcan.ca/tools-for-navigating-changing-geopolitical-realities/. [57]

UK Research and Innovation (2021), *UK Research and Innovation Trusted Research and Innovation Principles*, https://www.ukri.org/wp-content/uploads/2021/08/UKRI-170821-TrustedResearchandInnovationPrinciples.pdf. [84]

UK Research and Innovation (n.d.), *UK Research and Innovation Conflicts of Interest Policy*, https://www.ukri.org/wp-content/uploads/2020/11/UKRI-171120-ConflictsOfInterestPolicy-Dec19.pdf.pdf. [5]

UK Research and Innovation (UKRI) (n.d.), *Declaration of Interests: Applicants*, https://www.ukri.org/wp-content/uploads/2020/11/UKRI-261120-Declaration-of-Interests-for-applicants-v2.pdf. [89]

UNESCO (2021), *UNESCO Recommendation on Open Science*, https://unesdoc.unesco.org/ark:/48223/pf0000379949.locale=en. [25]

UNESCO (2017), *Recommendation on Science and Scientific Researchers*, The United Nations Educational, Scientific and Cultural Organization, https://unesdoc.unesco.org/ark:/48223/pf0000263618. [24]

UNESCO (2005), *Universal Declaration on Bioethics and Human Rights*, http://portal.unesco.org/en/ev.php-URL_ID=31058&URL_DO=DO_TOPIC&URL_SECTION=201.html. [137]

UNESCO (1997), *Recommendation Concerning the Status of Higher-Education Teaching Personnel*, http://portal.unesco.org/en/ev.php-URL_ID=13144&URL_DO=DO_TOPIC&URL_SECTION=201.html. [138]

United Nations (2013), *The Arms Trade Treaty*, https://thearmstradetreaty.org/hyper-images/file/ATT_English/ATT_English.pdf?templateId=137253. [37]

United Nations (1972), *Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction*, https://treaties.unoda.org/t/bwc (accessed on 13 May 2022). [39]

United Nations (1968), *Treaty on the Non-proliferation of Nuclear Weapons (NPT)*, https://www.un.org/disarmament/wmd/nuclear/npt/text (accessed on 13 May 2022). [38]

United Nations Human Rights Office of the High Commissioner (1966), *International Covenant on Economic, Social and Cultural Rights*, https://www.ohchr.org/en/professionalinterest/pages/cescr.aspx. [23]

United States Department of Energy (2021), *Unclassified Foreign National Access Program*, https://www.directives.doe.gov/directives-documents/100-series/0142.3-BOrder-b-chg1-ltdchg. [91]

Universities UK (2020), *Managing Risks in Internationalisation: Security Related Issues*, https://www.universitiesuk.ac.uk/policy-and-analysis/reports/Documents/2020/managing-risks-in-internationalisation.pdf. [12]

Universities UK (2019), *The Concordat to Support Research Integrity*, https://www.universitiesuk.ac.uk/sites/default/files/field/downloads/2021-08/Updated%20FINAL-the-concordat-to-support-research-integrity.pdf. [123]

University Foreign Interference Taskforce (2021), *Guidelines to Counter Foreign Interference in the Australian University Sector*, https://www.dese.gov.au/guidelines-counter-foreign-interference-australian-university-sector/resources/guidelines-counter-foreign-interference-australian-university-sector. [14]

University of Michigan (n.d.), *Conflict of Interest (COI)*, https://research-compliance.umich.edu/conflict-interest-coi (accessed on 9 May 2021). [107]

University of Michigan (n.d.), *Welcome to PEERRS*, http://my.research.umich.edu/peerrs/ (accessed on 9 May 2021). [108]

University of Toronto (2021), *Research Partnership Security Checklist for International Partnerships*, https://www.utsc.utoronto.ca/research/sites/utsc.utoronto.ca.research/files/docs/Research-Partnership-Security-Checklist-for-International-Partnerships.pdf. [106]

World Conference on Research Integrity (2013), *Montreal Statement on Research Integrity in Cross-Boundary Research Collaborations*, https://wcrif.org/montreal-statement/file. [126]

World Conference on Research Integrity (2010), *Singapore Statement on Research Integrity*, https://wcrif.org/documents/327-singapore-statement-a4size/file. [33]

World Intellectual Property Organization (1996), *WIPO Copyright Treaty (WCT)*, https://wipolex.wipo.int/en/text/295157. [135]

World Intellectual Property Organization (1979), *Paris Convention for the Protection of Industrial Property*, https://wipolex.wipo.int/en/text/287556. [134]

Annex A. Key concepts and different perspectives

Whilst the short working definitions of key terms used in this document are given in the glossary (Box 3.1), several of these terms are used or perceived differently in different countries and communities. It is important to understand these distinctions, when trying to build common understanding in a global ecosystem. Hence this annex revisits some of these key terms in more depth, using illustrative examples from a small number of international bodies or countries.

Research integrity

The *Singapore Statement on Research Integrity* (World Conference on Research Integrity, 2010[33]) describes the broadly recognised principles of research integrity, and the related responsibilities of researchers. This provides a normative basis for the consideration of research integrity in different national and cultural contexts and the development of detailed guidelines and practices. It defined the main principles of research integrity, and the associated responsibilities of researchers. The four principles are honesty, accountability, professional courtesy and fairness, and good stewardship. Research integrity is adherence to these principles in proposing, performing, evaluating, and reporting research and development activities. The four principles can be extrapolated to 14 responsibilities, encompassing issues of research misconduct ("FFP," Falsification, Fabrication, Plagiarism,) authorship, peer review, conflict of interest disclosure, or research ethics. [Note the focus of the Singapore statement is focused on individual researchers]

The Global Research Council *Statement of Principles for Research Integrity* (n.d.[121]) focuses on the responsibilities of research funding agencies in creating an international environment rooted in research integrity. It defines those principles for funding agencies as: leadership, promotion, education, transparent processes, response to allegations of misconduct, conditions for research support, and international cooperation.

The All European Academies (2017[34]), which comprises more than 50 academies from over 40 countries in Europe, defines fundamental principles of research integrity as being reliability, honesty, respect and accountability.

In Norway, scientific integrity is considered as being embedded in fundamental research ethics. Scientific integrity is about maintaining and complying with good scientific practice associated with the collective commitment to the pursuit for truth. Misconduct is serious breach of good scientific practice Norms of scientific integrity apply to all types of research and in every stage of the research process (The Norwegian National Research Ethics Committees, 2016[122]).

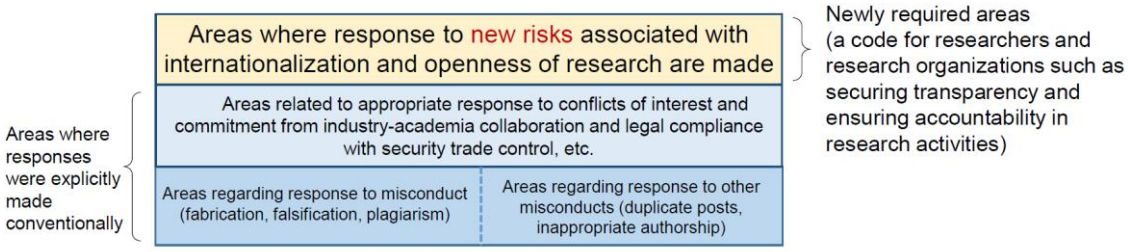
In the United Kingdom, honesty, rigor, transparency and open communication, care and respect for all, and accountability are the key elements of UK's Concordat to Support Research Integrity (Universities UK, 2019[123]).

The National Institutes of Health (NIH, United States) states that research integrity includes the use of honest and verifiable methods in proposing, performing, and evaluating research; reporting research

results with particular attention to adherence to rules, regulations, guidelines; and following commonly accepted professional codes or norms (National Institutes of Health, n.d.[124]).

The Government of Japan considers that research integrity is to "be adhered to by Japanese researchers and research organizations to assure accountability and transparency in research activities for maintaining sharing research results and reciprocity." It further considers that research integrity includes "a response to new risks that individual researchers will have to face following the trend of increasing internationalization and openness of research" (see Figure A A.1) (PricewaterhouseCoopers Aarata LLC, 2021[125])

Figure A A.1. Different aspects of research integrity



Source: *Research Investigation and Analysis Report, Cabinet Office* (PricewaterhouseCoopers Aarata LLC, 2021[125])

Despite differences in their interpretation of research integrity, most countries have recognised the need for a set of principles and guidelines for individual researchers to ensure good research conduct. Some attention has also been given to ensuring research integrity, i.e., good research conduct, in international collaborations (see Montreal statement (World Conference on Research Integrity, 2013[126])) and OECD-GSF produced a report and practical guide on *Facilitating International Research Misconduct Investigations* in 2009 (OECD, 2009[127]). However, none of this national or international guidance takes into consideration the broader issues relating to research security that impact on the behaviour of individual researchers and affect the integrity of the international research ecosystem.

Research security

In general, security refers to the absence of threats or low risks regarding societal values, or sufficient protection against threats. It does not only mean the protection of nation states, but also of individuals, societal structures, technical systems, and humanity as a whole (Kivimaa, 2022[128]; Bladwin, 1997[129]).

Research integrity refers to the veracity and quality of research whereas research security tends to refer to the actions taken to protect against, identify, and/or mitigate the risks to the inputs, processes, and outputs of science and research from unauthorised access, theft, or espionage.

Research security is often considered separately from research integrity, as it is normally associated with technology and/or military issues that have their own dedicated regulations and practices. For example, in South Korea, research integrity is a familiar concept in the academic sector, whereas research security is associated with the industrial sector.

The Centre for Security and Emerging Technologies (CSET) (Flagg and Arnold, 2021[130]) in the United States defines research security as "preventing foreign actors from acquiring scientific research through means that are illegal or contrary to prevailing norms, such as rewards, deception, coercion, and theft."

Thus, in a globalised research ecosystem, securing research means preventing the following: undue political influence over research, undesirable dual-use applications of research findings, conflicts of interest

and conflicts of commitment, and cyber-attacks. The main goals of research security is to protect the integrity and health of the national and international research system, but also national economic interests – by securing intellectual property, intellectual knowledge and know-how and preventing the unfair exploitation of these assets by unwelcome state and non-state parties.

Conflicts of interest & conflicts of commitment

Researchers and their institutions often receive funding from multiple sources and have multiple affiliations and roles in international collaborations and public-private partnerships. This in itself is not necessarily problematic. However, conflicts of interest and conflicts of commitment can distort behaviours and undermine public confidence in science. While conflict of interest and conflict of commitment overlap and are sometimes used interchangeably, these terms can be distinguished as follows:

Conflict of interest: A conflict of interest is a set of circumstances that create a risk that professional judgment or actions regarding a primary interest will be unduly influenced by a secondary interest (American Association of University Professors, 2014[4]; UK Research and Innovation, n.d.[5]). Conflicts of interest, which may be at the level of individuals or institutions, are often associated with financial transactions.

Conflict of commitment: A conflict of commitment can arise in a situation in which an individual accepts excessive workloads or conflicting duties from multiple employers (Office of Science and Technology Policy, 2020[6]). This can be extrapolated from individuals to laboratories or institutions, which have multiple commitments and a finite capacity to deliver.

Reciprocity

Most results from publicly funded research are shared between researchers and with society in an increasingly open process. At the same time, the benefits, drawbacks, and burden associated with research activities are also shared (The Norwegian National Research Ethics Committees, 2016[122]). Reciprocity is the practice of exchanging materials, knowledge, data, access to facilities and natural sites, and training and personnel exchanges in a manner that benefits all collaborating partners and spreads the burden. It is necessary for effective cooperation because it ensures that cooperation is mutually beneficial even if there may be asymmetries in the capacity of research partners to reciprocate cooperation. Thus, reciprocity in cooperation means transparency, equal access to research and facilities, data sharing, and compliance with contracts (D'Hooghe and Lammertink, 2020[2]).

For reciprocity to be universally accepted it must be considered alongside equity. Equitable access to the benefits of science is embedded in the overarching normative frameworks that govern international science (see Section 4). The recent emphasis on Open Science has increased the focus on ensuring equitable access. If reciprocity means that you only get out what you put in, or that everyone needs to contribute equally, then it may prejudice against those countries, institutions, or individuals with less resources or capacity and serve to reinforce existing power differentials. This is not what reciprocity is supposed to do. Hence, it is important to consider reciprocity and equity in tandem.

Dual-use research and technology

Dual-use research or technology has the potential to be exploited to purposely cause harm, or threaten public health or national security, although conducted for other beneficial purposes (Public Safety Canada, 2020[9]; D'Hooghe and Lammertink, 2020[2]) (see Box 3.1).

Dual-use technologies and other sensitive technologies are managed through export control regulations, but there is often no clear demarcation between civilian and dual-use technologies. JASON (2019[1]) concluded that controlling areas of fundamental research, which have obvious potential for dual-use, such as artificial intelligence, robotics and battery technologies is neither feasible nor desirable.

Reports from the Georgetown Walsh School of Foreign Service Centre for Security and Emerging Technologies (2020[131]) highlight the risks associated with direct or indirect collaborations with foreign institutions linked with the military sector (military universities, defence companies, etc.). Such collaborations could increase the risks of civilian technologies and knowledge being applied for foreign military purposes.

Foreign interference vs Foreign influence

Several countries make a distinction between foreign interference and foreign influence. These two terms overlap and are sometimes used synonymously. However, where the distinction is made, foreign interference applies to deliberately concealed and unwelcome activities, whereas foreign influence refers to transparent and normal diplomatic relations.

Foreign interference: interference carried out by, or on behalf of a foreign actor, which is coercive, covert, deceptive or corrupting and is contrary to national sovereignty, values and interests (University Foreign Interference Taskforce, 2021[14]; European Commission, 2020[132]). Some of the practices that would fall into this scope include researchers hiding military affiliations; undisclosed affiliation with a foreign government or company; and cyber-attacks. (McGill University, n.d.[133]) .

Foreign influence: Foreign influence is conducted in an open and transparent manner (University Foreign Interference Taskforce, 2021[14]). Every country influences other countries through a variety of methods. For instance, promoting cultural exchange is a common activity - governments in many countries support cultural events or language education abroad.

Annex B. Terms of reference, research integrity within the global science[1] ecosystem

These ToR have been prepared by a Scoping Group following the decision at the 42nd meeting of the OECD Global Science Forum (GSF) to initiate a project on Research Norms, Standards and Integrity.

The Project

Challenge

Increasingly, basic scientific discovery occurs in an interconnected, interdisciplinary, and international ecosystem that collectively leverages intellect, know-how, talent, and infrastructure from around the world. Freedom of inquiry and international collaboration are cornerstones of scientific progress. Open and transparent communication and dissemination of scientific information and data and sharing of materials are considered essential for the global science ecosystem to operate effectively and this openness is commonly associated with values such as non-discrimination, equity, and accountability. Cooperation in research also takes into account the notions of reciprocity– the exchange of materials and knowledge in a manner that benefits all collaborating partners-- and meritocracy, which ensures a level playing field where the best ideas and innovations can advance. It is generally accepted within the science community that these practices and norms[2] need to be respected for the ecosystem to function effectively.

Whilst basic scientific knowledge can be considered as a global public good, the utilisation of this knowledge by individual countries and/or actors depends on the effectiveness of national innovation systems and partially falls under international regulatory regimes for intellectual property (World Intellectual Property Organization, 1979[134]; 1996[135]). However, research and innovation are a continuum and the boundary between pre-competitive research (global good) and competitive research (liable to IPR protection) is often not clear- cut. This creates a tension between the global functioning of science and various expectations of economic return. Governments and other actors can undermine the integrity of the global scientific ecosystem by engaging in activities that suit their own agendas but are inconsistent with established norms and principles of research cooperation.

At the same time, as society faces more complex challenges that do not recognise national borders, such as global warming, biodiversity loss, natural disasters, economic migration and health pandemics, a wide

[1] This project incorporates all scientific disciplines including STEM and social sciences and humanities (SSH).

[2] Including Merton's CUDOS norms (1973[141]) - universalism, communism, disinterestedness and organised scepticism.

Universalism: scientific validity is independent of the socio-political status/personal attributes of its participants.

Communism: all scientists should have common ownership of scientific goods to promote collective collaboration.

Disinterestedness: scientific institutions act for the benefit of a common scientific enterprise rather than for the personal gain of individuals within them.

Organised scepticism: scientific claims should be exposed to critical scrutiny before being accepted.

range of stakeholders, including not only the public sector but also private sector actors, need to work together to address these challenges. This is both a global good and an economic development imperative for all countries. The COVID-19 pandemic starkly highlights both the critical importance of international and cross-sector collaboration in science in crises and the challenges that this presents. Sharing of scientific data, materials and results across countries and sectors have enabled the scientific community to support the development and implementation of policies to respond to the immediate crisis, and it is clear that international cooperation and openness will continue to be vital for the development of new diagnostic and therapeutic interventions. Who wins the race for the first vaccine and how the public good versus potential economic benefits associated with this are divided are much less clear but it would be naive to suggest that geo-politics and financial interests will not be major determinants. Upholding ethical standards and ensuring the rigour and integrity of research under intense pressure and public scrutiny is a major challenge for the international science ecosystem as it responds to COVID-19 pandemic.

Despite the tensions, the international science ecosystem has tended to function reasonably well up to this point. Internationally recognised normative agreements and legal regulations have created framework conditions that have been widely respected with democratic processes providing the necessary checks and balances (International Science Council (ISC), 2018[31]; World Intellectual Property Organization, 1979[134]; 1996[135]; United Nations Human Rights Office of the High Commissioner, 1966[23]; 2020[136]) (UNESCO, 2017[24]; 2005[137]; 1997[138]). There have been occasional aberrations, but over time the universality of science has been largely upheld. However new challenges and threats are emerging as some governments and non-state actors exhibit increasingly sophisticated efforts to over-ride established norms and practices and exploit the open research environment for their own interests. Unauthorised information transfers are now considered a serious national and economic security risk by a number of OECD countries. This has important implications for the integrity of a range of research activities, such as peer review of grant proposals, research training, recruitment and collaboration. If these issues are not addressed, and the integrity of the global science ecosystem assured, then international collaborations and trust in science are seriously at risk.

A systematic approach to strengthen research integrity and the research ecosystem

The two objectives of this activity are to identify and collate case studies, policies, applicable laws, regulations and procedures from Member States that focus on integrity of the research ecosystem, and to identify best practices that countries could employ to ensure research integrity as well as freedom of inquiry.

The project aims to provide countries with practical information and recommendations to deal with conflicts of interest and conflicts of commitment[3] and promote research integrity. The intention is to facilitate mutual learning and discussion among stakeholders across different countries by holding international workshops.

The final output will be a report, including policy recommendations/options. Key questions to be addressed include:

1. What principles and norms do governments/responsible science authorities rely on to support research and international collaboration? What regulations, policies and practices

[3] A conflict of interest is a set of circumstances that create a risk that professional judgment or actions regarding a primary interest will be unduly influenced by a secondary interest (American Association of University Professors, 2014[4]; UK Research and Innovation, n.d.[5]). A conflict of commitment can arise in a situation in which an individual accepts excessive workloads or conflicting duties from multiple employers (Ministerial Conference on the European Research Area, 2020[13]). Conflict of interest and conflict of commitment overlap and are sometimes used interchangeably. A compilation of definitions as they apply to research integrity can be found elsewhere (JASON, 2019[1]).

operationalise these principles and, in turn, reinforce the integrity of national and global research ecosystems?

2. How do governments/responsible science authorities encourage disclosure of, seek to prevent, and/or mitigate, and/or manage conflicts of interest and conflicts of commitment within the research ecosystem?
3. How do responsible authorities balance national and economic security with promoting scientific cooperation, protecting academic freedom, openness and non-discrimination?
4. How can governments increase awareness of risks to the integrity of the research enterprise – including from repressive influences, hostile actors, or foreign interference – among universities, research institutions and researchers? How can research-performing organisations, such as universities, and research funders reduce the risks of, or respond to, actions that threaten the integrity of the research system?
5. How are research institutions implementing existing norms and standards – or considering new measures – to uphold the integrity of the research ecosystem? How are they dealing with new or emerging challenges and conflicts, including from actors that subvert existing rules, abrogate accepted academic norms, or disregard academic freedom or democratic and human rights norms?
6. When selecting students, team members and research partners, or accepting funding how do researchers and research institutions make informed and balanced decisions that take into account risks to research integrity while up-holding the principles of non-discrimination and freedom of inquiry?
7. What types of benefit-risk analyses are performed to assess potential international research partnerships? How do they ensure mutual benefit sharing in collaborations, especially with international partners?
8. How can funding agencies ensure that the assessment of research, including the peer-review process, is secure and fair and does not lead to misappropriation of ideas and intellectual capital? How can they best detect, monitor and manage potential conflicts of interest and conflicts of commitment?
9. How can governments and funding agencies provide guidance and incentives to research institutions to strengthen research integrity?

Previous GSF work on Research Norms, Standards and Integrity

The project is related to the earlier OECD-GSF works on Report from the Workshop on Best Practices for Ensuring Scientific Integrity and Preventing Misconduct (OECD, 2007[139]) and Investigating Research Misconduct Allegations in International Collaborative Research Projects (OECD, 2009[140]) that focused on individual misconduct such as fabrication, falsification and plagiarism.

The GSF Project

This project will:

1. Collect information about the challenges as perceived in different countries and the extent to which these are addressed in relevant international frameworks, national policies, regulations, measures/programs and institutional practices.
2. Implement horizontal analysis of the collected information at each political initiative level. As necessary, implement a vertical analysis of the information for each country.

3. Hold international workshops that bring together international experts and representatives of relevant stakeholder communities to collect additional information and case studies, and facilitate mutual learning among the participants.
4. On the basis of findings acquired through these activities, make a final report that provides good practice examples and policy recommendations/options for stakeholders.

It is recognised that this is an ambitious project and the intention is to get a broad overview of challenges, concerns and actions being taken across different countries and institutions. This should lead to the identification of good practices, which could provide the basis for subsequent in-depth follow-up projects, e.g. to develop toolkits or guidelines addressing specific threats to the integrity of research.

Proposed Participants

The project is to be carried out under the aegis of GSF. An Expert Group (EG) to oversee the project activities and outputs, will be established with nominations from GSF delegates.

Annex C. GSF expert group membership

Country	Name	Affiliation	Organisation
Australia	Rachael Mitchell / Michelle Traynor-Brack / Freya Kaine	Director, National Security Engagement	Department of Education, Skills and Employment
Canada	Sinead Tuite	Senior Director, Digital Research Infrastructure	Innovation, Science and Economic Development Canada / Government of Canada
Canada	Martha Crago	Vice-Principal (Research and Innovation)	McGill University
France	Fabien Laurençon		Ministry of Economy and Finance, the Department of Economic Security
Germany	Andra-Maria Popa	Scientific Researcher	DLR project management agency
Germany	Claudia Hefftler[1]	Scientific Researcher	DLR project management agency
Japan	Kimikazu Iwase	Principal Fellow	Centre for Research and Development Strategy (CRDS), Japan Science and Technology Agency (JST)
Japan	Eriko Yamazaki	Deputy Director for International Affairs	Secretariat of Science, Technology and Innovation Policy, Cabinet Office, Government of Japan
Korea	Inkyoung Sun	Head of Office of Development Cooperation Research	Science and Technology Policy Institute (STEPI)
Korea	Sun Kun Oh	Emeritus Professor of Physics	Konkuk University
Netherlands	Peter-Paul Verbeek[2]	Professor of Philosophy of Technology	University of Twente
Norway	Helene Ingierd	General Director	The Norwegian National Research Ethics Committees
Portugal	Bruno Béu		Foundation for Science and Technology
South Africa	Liapeng Matsau	Deputy Director	Research, South African Qualifications Authority
South Africa	Pradish Rampersadh	Chief Executive Officer	South African Council for Natural Scientific Professions (SACNASP)
Switzerland	Edwin Charles Constable	Professor	University of Basel
United Kingdom	Ben Sharman	Senior Global Policy Manager	UK Research and Innovation
United Kingdom	Sion Griffiths		International Research and Innovation Team BEIS
United States	Michael Imperiale	Associate Vice President for Research - Policy and Compliance	University of Michigan
United States	Bridget M. Turaga	Programme Director	Office of International Science and Engineering, National Science Foundation

[1] Until November 2021

[2] Attended only the first EG meeting on 27th January 2021.