European Commission

TACKLING R&I FOREIGN INTERFERENCE

Staff Working Document

Research and Innovation

Tackling R&I foreign interference. Staff Working Document

European Commission
Directorate-General for Research and Innovation
Directorate A — ERA & Innovation
Unit A.3 — R&I Actors and Research Careers

Email RTD-ACTORS-AND-CAREERS@ec.europa.eu
RTD-PUBLICATIONS@ec.europa.eu
European Commission
B-1049 Brussels

Manuscript completed in January 2022.
First edition.

PDF ISBN 978-92-76-46520-1 doi:10.2777/513746 KI-09-22-004-EN-N

Luxembourg: Publications Office of the European Union, 2022

EUROPEAN COMMISSION

Tackling R&I foreign interference

Staff Working Document

2022 Directorate-General for Research and Innovation

SUMMARY

Foreign interference (FI) occurs when activities are carried out by, or on behalf of, a foreign state-level actor, which are coercive, covert, deceptive, or corrupting and are contrary to the sovereignty, values, and interests of the European Union (EU). EU **Higher Education Institutions (HEIs)** and **Research Performing Organisations (RPOs)** can benefit from a comprehensive strategy for tackling foreign interference that covers key areas of attention grouped into the following four categories: values, governance, partnerships and cybersecurity. A non-exhaustive list of possible mitigation measures that can help HEIs and RPOs to develop a comprehensive strategy, tailored to their needs, is outlined below.

VALUES

1 Identify countries and partner institutions where academic freedom is at risk.

- Consult the global **Academic Freedom Index (AFi)** as a first point of orientation.
- Then conduct a more detailed **assessment** of the **research, educational and institutional environment** in the country and at the specific partner institution.
- Subsequently, **analyse** the external actors' **motives** for undermining academic freedom and monitor the external actors' **capacities** for restricting and/or instrumentalising European researchers and institutions.

2 Conduct a vulnerability assessment to understand external pressures on academic freedom and integrity in your institution.

- Undertake institution and/or project-specific **vulnerability** assessments.
- Review if existing cooperation with external actors has created any **dependencies.**
- Verify that all **partnership** agreements adequately protect academic freedom.
- Monitor **external appointments** as well as honorary degrees awarded to researchers.
- Provide **training** to everyone who interacts with institutions where academic freedom and universal values are at risk.
- Set-up a **reporting** mechanism to map threats to academic freedom in the institution.

3 Strengthen commitment to academic freedom and integrity at institutional and individual levels

- Address **specific vulnerabilities** once they are **identified.**
- Provide **training** to everyone who interacts with institutions where academic freedom and universal values are at risk.
- Integrate academic freedom and integrity into the **core curriculum** of any academic education programme.

- **Affirm frequently** and **publicly** the importance of academic freedom and integrity.
- **Raise awareness** among students, academic and administrative staff for the importance and protection of fundamental academic values
- **Support** scholars who work on research topics that external actors seek to supress.
- Launch a **dedicated support programme** for visiting scholars and incoming students from countries where academic freedom is threatened.
- Help **protect persecuted scholars** or students by providing (temporary) sanctuary.
- Consider signing a **democracy pledge.**

4 Continue to cooperate with partners in repressive settings.

- **Avoid stigmatising** or **alienating** students, academic colleagues and institutions in non-liberal institutional environments.
- **Create awareness** and **understanding** of how repressive settings can affect academic freedom.
- **Review standard ethics procedure**s to ensure that risky research in repressive settings will not automatically be rejected (and thereby repressed) by the relevant committee.
- Provide guidance and tailored technical support on **data** and **digital security** to help manage surveillance risks in repressive settings
- Set up an **emergency procedure** to deal with cases of harassment, detention or disappearance.
- Commit to **transparency** and **screening mechanisms** tailored to address collaboration with repressive settings.

GOVERNANCE

1 Publish a Code of Conduct for Foreign Interference.

- **Ensures protection of:**
  - **academic** freedom;
  - **data security** and intellectual property;
  - **excellence** and **openness** in **research, teaching** and **support** for learning;
  - **ethics, integrity** and **trust**.

- **Includes procedures for:**
  - **identification** of foreign interference (including data breaches and ethically unsound research);
  - **whistleblower protection**;
  - dealing with **internal conflicts of interest.**

2 Establish a Foreign Interference Committee

- **Integrated with existing institutional structure and responsible for:**
  - **awareness raising** through education & training;
  - **monitoring** of potential risks;
  - **management of research data and intellectual assets** in international cooperations and providing advice and support to research groups involved;
  - **risk management** and **risk mitigation;**
  - **investigation** of foreign Interference.

PARTNERSHIPS

1 Develop general prerequisites for the implementation of a risk management system

- A Foreign Interference Investigation Committee should ensure that knowledge security and academic integrity is safeguarded in all partnerships by **reviewing procedures** and **expanding** and **strengthening** them where needed.
- **Raise broad awareness** of potential risks involved in engaging in a partnership and of the ways the institution seeks to **mitigate** them.
- Raise support for a **risk management strategy.**
- Create awareness and knowledge of **export control legislation** and **Foreign Direct Investment (FDI) screening.**
- Identify and protect the institution's **'crown jewels**' and understand the potential technological, security and economic interest from third countries'
- Define criteria for the reporting of plans for a partnership to the FI Committee and determine who is **accountable** for following up on the reporting.
- Define the **minimum levels of due diligence** for different types of partnerships.
- The Foreign Interference Committee could establish a **risk management subcommittee or working group.**

2 Establish a sound procedure for developing robust partnership agreements

- **Develop a positive agenda**: identify safe or low-risk areas for international collaboration.
- **Prepare for partnership:** ensure it is based on a strategic vision as part of internationalisation.
- Develop a sound knowledge of the partner organisation, of its place in the national research system of its country.
- **Perform due diligence**: gather information enabling staff to assess potential risks with regard to security, values and reputation.

- **Carefully negotiate partnership agreement:** ensure transparent delineation of responsibilities including financial commitments, IPR, data management and Open Science.
- **Monitor the implementation of the agreement:** focus on issues related to potential foreign interference.
- Assess the outcomes of the collaboration and draw lessons for future engagement

CYBERSECURITY

1 Raise awareness of cybersecurity risks

- Develop training and organise seminars on all available and implemented **data protection technologies** including **confidential computing.**
- **Educate** and **train** researchers, students, and administrative and support staff in **cyber hygiene** and to identify the risks and know how to avoid or deal with cyberattacks.
- Develop and communicate **easy-to-follow escalation processes** in case of suspected cyberattacks and advertise a **single point of contact for triaging** the reported incidents.
- Maintain and communicate a **Top 10 cybersecurity risk list.**
- Publish regular newsletters with **best practices** describing cybersecurity incidents.

2 Detect and prevent cybersecurity attacks from foreign interference actors

- Set up and perform **Open Source Intelligence (OSINT) investigations** on a regular basis and create **alert capabilities** to flag outlier behaviour.
- Develop **screening procedures** for researchers and administrative and support staff.
- **Procure cybersecurity-certified equipment** and invest in developing **confidentiality protection solutions** for datasets including confidential computing.
- Implement **physical access controls** appropriate to the level required.
- Develop for the office/corporate activity cluster a **centralised management approach** for operating systems and installed applications and disable and remove local administration rights (LAR).
- Enable **two-factor authentication** (2FA) to access critical services and repositories and maintain and enforce **block-lists** to prohibit access to known malicious or infringing websites.

3 Respond to and recover from cybersecurity attacks from foreign interference:

- Develop **situational awareness capabilities** by sharing lessons learnt and updating shared blacklists, reputation systems and databases.
- Develop a **plan for incident handling** which includes clear processes involving both affected parties and those required to handle the response. Adopt practices and elements from incident handling models such as the **SIM3 Security Incident Management Maturity Model.**

- Implement **forensic readiness capabilities** to reduce the time to respond.
- Follow **disciplinary action** for offending staff and in doing so include evidence from the **digital investigation.**
- Involve relevant **law enforcement agencies, national intelligence and security agencies, Intellectual Property offices,** and **data protection authorities** for incidents.

GLOSSARY

Key concepts used for the purposes of this staff working document are set out below:

ACADEMIC FREEDOM:

is defined as freedom of academic staff and students to engage in research, teaching, learning and communication in and with society without interference nor fear of reprisal. Freedom of academic research encompasses the right to freely define research questions, choose and develop theories, gather empirical material and employ academic research methods, to question accepted wisdom and bring forward new ideas. It entails the right to share, disseminate and publish the results thereof, including through training and teaching. It is the freedom of researchers to express their opinion without being disadvantaged by the institution or system in which they work or by governmental or institutional censorship.

COERCION:

the action of making somebody do something that they do not want to do, using force or threatening to use force.

DISINFORMATION:

false or misleading content that is spread with an intention to deceive or secure economic or political gain and which may cause public harm.

FOREIGN INTERFERENCE:

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

HIGHER EDUCATION INSTITUTION:

an institution which, in accordance with national law or practice, offers recognised degrees or other recognised tertiary level qualifications, regardless of what such an establishment is called, or a comparable institution at tertiary level which is considered by the national authorities as eligible to participate in the Programme in their respective territories;

HYBRID THREATS:

variety of coercive and subversive activities (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to destabilize states and societies, cause direct damage, or gain leverage, while remaining below the threshold of formally declared warfare.

MISINFORMATION:

false or misleading content shared without harmful intent though the effects can still be harmful, e.g. when people share false information with friends and family in good faith.

OPEN SCIENCE:

an approach to the scientific process based on open cooperative work, tolls and diffusing knowledge, in

particular in accordance with the following elements: (a) open access to scientific publications resulting from research funded under the Programme, and (b) open access to research data, including those underlying scientific publications, in accordance with the principle 'as open as possible, as closed as necessary'.

RESEARCH INFRASTRUCTURE:

facilities that provide resources and services for the research communities to conduct research and foster innovation in their fields, including the associated human resources, major equipment or sets of instruments; knowledge-related facilities such as collections, archives or scientific data infrastructures; computing systems, communication networks and any other infrastructure of a unique nature and open to external users, essential to achieve excellence in R&I; they may, where relevant, be used beyond research, for example for education or public services and they may be 'single sited', 'virtual' or 'distributed';

RESEARCH PERFORMING ORGANISATION:

organisation that carries out research or technological development as one of its main objectives.

THIRD COUNTRY:

a country that is not a member of the European Union as well as a country or territory whose citizens do not enjoy the European Union right to free movement, as defined in Art. 2(5) of the Regulation (EU) 2016/399 (Schengen Borders Code).

THREAT ACTOR:

a foreign actor that is typically state-owned or state-sponsored and that engages in foreign interference.

FOREWORD

In the recent decades, research and innovation have increasingly expanded beyond national borders to become fully internationalised. The creation, accumulation of knowledge and innovative outputs are nurtured by international networks of academic and technological cooperation. At the same time, the expansion of activities to countries outside the European Union involves a number of risks and challenges that need to be managed.

Europe's Higher Education Institutions (HEI) and Research Performing Organisations (RPO) have a strong record of internationalisation. They have facilitated the development of international curricula, fostered international research and innovation projects, and supported the circulation of students, staff and knowledge.

As set out in the Communication 'The Global Approach to R&I'[1], which describes the new strategy for international cooperation to face the transformed global environment, the EU's approach is based on a positive agenda of partnership coupled with the constructive management of differences. Reciprocity, a level playing field and fair competition across all areas of cooperation must be guaranteed. The EU will seek to maximise its internal cohesion and effectiveness in its dealings with foreign actors that demonstrate coercive, covert, deceptive or corrupting behaviour and are contrary to the EU's sovereignty, values and interests.

This Staff Working Document is designed to provide information on practices to mitigate foreign interference risks to HEIs and RPOs in support of their endeavour to safeguard their fundamental values, including academic freedom, integrity and institutional autonomy and to protect their staff, students, research findings and assets. Accordingly, it does not intend to limit international collaboration but rather to promote international collaboration that is as open as possible and as closed as necessary. Moreover, it is not designed to burden HEIs and RPOs with additional administration but to encourage integration of possible measures as much as possible in existing structures.

While this document aims to be as concrete as possible, there is no one-size-fits-all approach; and each organisations needs to tailor their own set of measures. It is intended as a toolkit of measures to help develop a comprehensive strategy, covering key areas of attention grouped into four categories: values, governance, partnerships and cybersecurity.

This Staff Working Document has been co-created with Member States and stakeholders[2] and is meant as an inventory of best practices and collection of evidence, which is neither exhaustive nor binding. This means that although it provides detailed information on a number of issues, there might be elements that are not included in this document. Moreover, it should be used as a source of inspiration. Member States and organisations might consider adopting other measures on the same subject. Building resistance and responding to foreign interference incidents should be done in consultation with and with support of local and national authorities, where appropriate.

This document is for information purposes only. It does not constitute the official position of the Commission, nor does it prejudge any such position.

---

[1] European Commission (2021) Communication on the Global Approach to Research and Innovation COM(2021) 252 final available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2021:252:FIN

[2] Research and innovation institutions including higher education institutions, Research and Technology Organisations, research infrastructures, research funding organisations, industry and related associations.

TABLE OF CONTENT

1. INTRODUCTION

1.1. FOREIGN INTERFERENCE

While all governments try to influence discussions and decisions on issues of strategic importance to them, **foreign interference** occurs when activities are carried out by, or on behalf of, a foreign state-level actor, which are coercive, covert, deceptive, or corrupting and are contrary to the sovereignty, values, and interests of the European Union (EU). The **objectives of foreign interference** serve to further the political, socio-cultural, economic, and technological interests of the foreign actor:

- to **unlawfully retrieve information** of interest to the foreign actor
- to **influence decisions** in favour of the foreign actor
- to **undermine values** perceived as contrary to the foreign actor

Foreign actors may target national authorities and strategically important organisations and individuals in foreign interference. Targeted organisations can be active in all sectors of society including the public, private, and third sectors. Similarly, targeted individuals can be active at all levels within their organisations or be individually of strategic importance. Foreign actors can deploy a number of **tactics of foreign interference** to realise their objectives, for instance:

- **political pressure** by influential representatives on strategic decision makers
- **financial support** in the form of investments, donations, funding, and loans
- **exploiting people** in strategic positions who are coerced, recruited, or placed
- **digital intrusions** breaching cybersecurity remotely or physically on location
- **spreading disinformation** against local interests or promoting foreign interests

Foreign interference thus forms a hybrid threat that involves state-level foreign actors and their proxies who deploy a wide range of conventional and unconventional tactics to achieve their objectives. Any risk mitigation or response needs to take into account the hybrid nature of this threat. One known target of foreign interference is Higher Education Institutions (HEIs) and Research Performing Organisations (RPOs). Some fictive **examples of foreign interference in HEIs and RPOs** include:

- **A research leader at an RPO which is collaborating with a foreign actor is pressured into restricting or cancelling lectures, workshops, conferences, or projects on specific topics.**
- **A foreign actor finances and supports the establishment and staffing of a language and cultural centre at a HEI which enables the spreading of propaganda, spread of disinformation and information manipulation and facilitates espionage.**
- **A technology transfer officer at an RPO is recruited by a foreign actor and is subsequently coerced or blackmailed into gaining access to and sharing confidential research and IP.**

- **A foreign state-sponsored hacker group runs a phishing campaign on students and staff of a HEI to harvest their accounts and gain unauthorised access to publications, data, and code.**
- **A foreign actor runs a disinformation campaign on social media targeting a research group or researchers at an RPO and discrediting their research on specific topics.**

This Staff Working Document **aims to inform HEIs and RPOs** about the risks of foreign interference and help safeguard their fundamental rights and values of academic freedom, integrity, and autonomy as well as protect their students, staff, research, and intellectual property. Addressing foreign interference in HEIs and RPOs requires awareness and vigilance by all members of the academic community, who are collectively responsible for identifying, reporting, and responding to cases of foreign interference.

This Staff Working Document is not intended to burden HEIs and RPOs with additional regulations but instead to inform them of the multi-dimensional aspects of foreign interference and assist them in their **strategic planning to address foreign interference.** A comprehensive approach is needed which comprises four key phases: awareness; prevention; response; recovery. These phases to a large extent represent the concept of resilience. Fostering resilience in against such threats will allow HEI and RPOs to be more prepared, give them the tools to identify such threats early enough and take the necessary action. Individuals at all levels in HEIs and RPOs first need to be made aware of the risks of foreign interference. Guidance is secondly required on how to prevent suspected cases of foreign interference. Concrete and timely actions are thirdly required when cases of foreign interference have been confirmed. Plans for recovery finally need to deal with the negative consequences of cases of foreign interference.

1.2. GUIDING PRINCIPLES

Guiding principles to address foreign interference could be grounded in the legal provisions of primary European law giving an objective and authoritative framework of norms and values. This includes the Treaty on the European Union (TEU), Treaty on the Functioning of the European Union (TFEU), European Union Charter of Fundamental Rights (EUCFR), as well as the European Convention on Human Rights (ECHR). In particular, Article 2 of the TFEU states the founding values of the EU as respect for human dignity, freedom, democracy, equality, rule of law, and human rights as well as referring to pluralism, non-discrimination, tolerance, justice, solidarity, and (gender) equality.

Addressing **foreign interference in the context of education and research** should be grounded in principles ensuring academic freedom, institutional autonomy, research integrity and ethics, and excellence and openness in education and research. These are incorporated in the following documents: the European Code of Conduct for Research Integrity[3], European Charter for Researchers[4], Code of Conduct for the Recruitment of Researchers, the Rome Ministerial Communiqué Annex 1 on Academic Freedom[5], Bonn Declaration on Freedom of Scientific Research, Lima Declaration on Academic Freedom and Autonomy

[3] ALLEA. (2017). The European Code of Conduct for Research Integrity: Revised Edition. Berlin

[4] Commission Recommendation, 2005/251/EC of 11.03.2005 on the European Charter for Researchers and on a Code of Conduct for the Recruitment of Researchers

[5] https://ehea.info/Upload/Rome_Ministerial_Communique_Annex_I.pdf

of Institutions of Higher Education[6], Utrecht Declaration on Academic Freedom[7], and Magna Charta Universitatum[8]. In particular, Article 179 of the TFEU sets the overall objective of encouraging and strengthening scientific and technological cooperation and development through a European Research Area (ERA). Article 165 of the TFEU sets mobility of students and teachers as one of the aims of the Union action in the field of education. Ensuring this freedom to be mobile and fostering higher education autonomy through quality are key elements of the development of a European Education Area (EEA)[9].

Four objectives of the ERA[10] are at potential risk from foreign interference: support free circulation of researchers, knowledge, and technology; encourage high-quality research and technological development; promote competitiveness in research and innovation; support co-operation and interdisciplinarity between all sectors in their research and technology development activities. Free circulation may enable interference and reduce the level-playing field and degree of reciprocity between Europe and the world. High-quality research and technologies arising from support and competitiveness are valuable assets and make Europe a primary target for interference. Collaboration with countries from outside of Europe may lead to a conflict with value systems which are not in agreement with European values. Strategies for tackling foreign interference need to mitigate against such risks while at the same time upholding and safeguarding these four cornerstones of the ERA. The measures to reduce the risk of foreign interference should be proportionate so as not to endanger the scientific process which crucially relies on collaboration and knowledge sharing.

The planned **European Education Area (EEA)** and the strategic cooperation framework to achieve it by 2030 are founded on the role of education as promoting democratic values. The EEA will also be outward-looking and a catalyst for international cooperation that extends beyond Europe's borders. This international dimension recognises that "cooperation in education and training has gradually become an important instrument for the implementation of EU external policies, based on European values, trust and autonomy"[11]. These are the values that need to be upheld in practice and policy, at national and international level.

Foreign interference is naturally not confined to Europe but is inherently a global challenge which has **consequences for international relations and collaboration.** Indeed, international academic collaboration is an essential asset and strategic pillar for European HEIs and RPOs. It is therefore crucial to maintain and further enhance international research and innovation co-operation, whilst ensuring a robust and trusted system in which the risks of foreign interference are managed and the benefits of collaboration are realised. Principles for engaging international partners should be further grounded in international agreements including the Charter of the United Nations[12], Universal Declaration of Human

[6] 68th General Assembly of World University Service. (1998). The Declaration on Academic Freedom and Autonomy of Institutions of Higher Education. Available at: http://ace.ucv.ro/pdf/lima.pdf

[7] AHRI. (2016). Utrecht Declaration on Academic Freedom. Utrecht. Available at: http://new.ahri-network.org/wp-content/uploads/2018/09/AHRI-Utrecht-Declaration-2016-3.pdf

[8] University of Bologna.(1986). Magna Charta Universitatum. Available at: http://www.magna-charta.org/resources/files/the-magna-charta/english

[9] COM(2020) 625 final of 30.09.2020; Council Resolution on "a strategic framework for European cooperation in education and training towards the European Education Area and beyond (2021-2030)"

[10] COM(2020) 628 final of 30.09.2020

[11] Council Resolution on a strategic framework for European cooperation in education and training towards the European Education Area and beyond (2021-2030), 19 February 2021

[12] United Nations. (1945). Charter of the United Nations. [online] Available at: https://www.un.org/en/charter- united-nations

Rights[13], and the United Nations Sustainable Development Goals (SDGs)[14]. Europe should stay 'open to the world'[15] yet be vigilant and ready to respond to foreign interference.

1.3. HEIs AND RPOs AS TARGETS

Scientific research is a collaborative process by nature in which researchers and organisations typically build upon existing research and collaborate to further scientific development. This open and collaborative spirit enables the success of HEIs and RPOs but also may open them up more easily to foreign interference. HEIs and RPOs are of particular interest to foreign actors due to their prominent role in society, their co-operation with the public, private, and third sectors, and their creation of knowledge and innovative new technologies that are crucial for tackling societal challenges and ensuring prosperity and are often relevant for dual civil and military usages.

HEIs and RPOs are a key pillar of society and reflect in a way the values of their countries. They educate students who become key members of society. They conduct research and create knowledge that serves to increase our understanding of the world and guide society with reason and evidence. Their researchers are experts in their fields and act as knowledge gatekeepers providing critical and reasoned viewpoints on important societal topics that feed into public perceptions and influence policy making. This is especially important for tackling fake news and building resilience to information manipulation and disinformation, facilitated by the rising dominance of social media and alternative popular news outlets that are increasingly vulnerable to instrumentalisation by foreign actors. HEIs and RPOs are furthermore bastions of free speech, promoters of critical and independent thinking and protect the freedom of academic inquiry. Foreign interference aims to disrupt and undermine these roles, and by extension, forms a threat for society as a whole.

The research that HEIs and RPOs conduct is crucial for a developing society and market economy. They probe the nature of all the scientific domains of natural sciences, engineering and technology, medical and health sciences, agricultural sciences, social sciences, and the humanities. Their outputs produce value across all sectors of society and form the backbone of the knowledge economy. New discoveries fuel technological innovation leading to a higher quality of life for citizens. New products and services lead to a thriving market place and economic prosperity for a country. Collaborative and interdisciplinary research, in particular, is vital for addressing the societal challenges of our times and realising the SDGs. Foreign interference aims to not only scientifically and economically profit from targeted assets, but to disrupt the scientific, economic, and social development of targeted countries.

Foreign actors further target HEIs and RPOs because they are especially **vulnerable to interference attacks.** They are typically large organisations serving many students and/or employing many temporary and permanent staff across various departments. This allows for multiple entry points and individuals to target for attacks. They typically manage large-scale information and communications technology

[13] United Nations. (1948) Universal Declaration of Human Rights. [online] Available at: https://www.un.org/en/about-us/un-charter/full-text

[14] United Nations. (n.d.). About the Sustainable Development Goals. Available at: https://www.un.org/sustainabledevelopment/sustainable-development-goals

[15] European Commission. (2016). Open Innovation, Open Science, Open to the World. Available at: https://op.europa.eu/en/publication-detail/-/publication/3213b335-1cbc-11e6-ba9a-01aa75ed71a1

infrastructures, whereby cyberattacks can disrupt the activities of students and researchers and give access to entire networks and databases. Values of openness and collaboration, which are crucial for science to progress, condition students and researchers to be open and trusting of colleagues and collaborators. Often tactics of interference include calling on the patriotic duty of foreign nationals with whom scientific collaborations are established. The objectives and tactics of foreign interference aim to exploit these vulnerabilities at HEIs and RPOs.

1.4. IMPLICATIONS FOR HEIs AND RPOs

The hybrid nature of **foreign interference poses a multi-dimensional threat** which has implications across levels and individuals at HEIs and RPOs. The main objectives and intended outcomes of foreign interference complement each other and serve to disadvantage HEIs and RPOs to the benefit of state-level foreign actors as in Table 1.1. These foreign actors deploy a combination of tactics, techniques and procedures against HEIs and RPOs as in Table 1.2. The actual targets of foreign interference are strategic individuals in positions at all levels in HEIs and RPOs as in Table 1.3.

Table 1.1: Possible Objectives and Intended Outcomes of Foreign Interference

OBJECTIVES	INTENDED OUTCOMES
Retrieve information	Access confidential information, network infrastructure, (high-performance) computing infrastructure, physical asset management, core services management, research equipment, research methodologies, research data, research software, research publications, IPR, and personal data
Influence decisions	Influence decisions enabling the retrieval of information and the undermining of values as well as giving a strategic and competitive advantage, favouring involvement in collaborations and projects, and influencing the selection of students and staff
Undermine values	Discredit and breach human rights, democracy, freedom of speech, and the rule of law as well as values linked to research and education including academic freedom, openness, transparency, accountability, ethics, integrity, trust, privacy, IPR, and mutually beneficial collaboration

Table 1.2: Possible Tactics and Techniques of Foreign Interference

TACTICS	TECHNIQUES
Political pressure	Improper attempts by high-level representatives of national authorities or politically linked organisations to pressure strategic decision makers with favours or repercussions
Financial support	Creating financial dependencies through investments in large-scale projects and joint ventures in the local or foreign country, donations to an endowment fund or for specific programmes, funding for research projects or specific initiatives, and loans with or without favourable conditions for specific projects and ventures.

Exploiting people	Coercing in the short-term or recruitment in the long-term of individuals in strategic positions via social engineering, bribes, blackmail, or intimidation as well as the selection and placement of allied individuals in strategic positions
Digital intrusions	Remote unauthorised access via phishing, hacking, or malware and local unauthorised access via computer terminals or wifi into digital networks and databases as well as any authorised access for unauthorised usages
Information manipulation	Dissemination of false and/or misleading information that discredits local viewpoints or promotes foreign viewpoints via the internet, social media, and online or physical lectures and events. Manipulation of discourse through the use of inauthentic accounts, fake websites, fake personas and information suppression.

Table 1.3: Targeted Positions and Individuals of Foreign Interference

TARGETED POSITIONS	TARGETED INDIVIDUALS
Students	Bachelor and master level students
Researchers	Early-career and senior researchers
Administrative staff	HR, ICT, legal, financial, policy, and project management staff
Research support staff	Library, IPR, technology transfer, and research management staff

1.5. IMPLICATIONS FOR OPEN SCIENCE

The pursuit of scientific knowledge and discoveries is a **collaborative and competitive endeavour.** Researchers build upon the work of past and present colleagues and collaborate within and across disciplines to address complex scientific and societal challenges. Yet researchers also compete with each other for research positions, funding, and awards as well as to bring innovative products and services arising from their discoveries to the market. And HEIs and RPOs themselves compete with each other for prestige, resources, and rankings as well as the ability to attract the best students, researchers, and collaborators. There is thus an ever-present tension between the need to collaborate for the good of science and the need to compete for the self-interest of researchers and organisations.

This tension between collaboration and competition in academia has resulted in a **traditionally closed collaborative system,** where researchers are not incentivised to work openly but rather to restrict their methodologies and outputs. An exacerbating factor is the primary focus in academia on publishing research results in prestigious journals and bringing innovative outputs to the market. The rise of digitisation and the internet has resulted in increasingly ideal supporting conditions for researchers to collaborate and share research outputs. Indeed, the main objective of Open Science is to take advantage of digital technologies and enable researchers to collaborate and share their research more openly and effectively. The realisation of Open Science is a policy priority of the European Commission and the European Open Science Cloud (EOSC), in particular, will be a key enabler of Open Science.

Open Science consists of a range of practices to provide transparency to research work in order to safeguard scientific integrity and facilitate collaboration and sharing. The most prominent **practices in Open Science** focus on reproducibility and open access of publications, data, and software. Reproducibility means that results obtained from a research study should be achieved again, with a high degree of agreement, when the research study is replicated by other researchers using the same methodology. In practice, this means that research studies should be published and described in enough detail so as other competent researchers are able to replicate the study. Open Methodology aims to open up the methodological aims and steps behind a research project as well as giving access to notes, protocols, workflows, and developments during the project. Open Access for publications aims to replace the subscription-based system of closed academic journals and open up the access to publication without embargoes and fees for readers. Open Access to data aims to open up research data to be freely used by others, and to make research data Findable, Accessible, Interoperable, and Reusable (FAIR). Lastly, Open Source aims to open up the software code and algorithms behind programs and applications that crucially support research.

It is important to note that Open Science is not necessarily binary in the sense of open versus closed, but is rather a spectrum of openness, where different types and aspects of research outputs can be opened or not depending on the nature of the research. This is reflected in the motto 'as open as possible and closed as necessary'. Research outputs may justifiably not be opened for privacy, security, political, military, and commercial reasons. The broad application of Open Science principles challenges the concept of interference by foreign actors since, by definition, information is in the open and available to all. The drive towards openness, nonetheless, needs to be carefully examined in the context of balanced benefits of openness versus closeness. While the goal of Open Science is that ultimately all scientists around the world open up their research as much as possible, such an open approach may be disadvantageous to researchers, organisations, and countries when foreign actors are not reciprocating but instead exploiting openly available materials solely for their own advantage.

Opening up research methodologies shows no immediate disadvantages to foreign interference. Project descriptions and detailed plans for projects solely explain a project and could be shared unless the project is of a sensitive or confidential nature. Sharing project notes, such as laboratory notes, during the implementation of the project should similarly not be problematic as the researchers themselves choose what they want to share and make an assessment. There is a risk, however, that methodological notes which upon the time of release seem innocuous could later have implications for foreign dual use applications as the project progresses or new discoveries are made. An element of foresight is thus needed in opening up potential dual use research. Also, foreign actors could collect information from different sources and collate them in order to reconstruct the big picture. Therefore, it is important to raise awareness and develop tips-and-hints to identify potentially sensitive information.

Opening up research publications similarly shows no immediate disadvantages to foreign interference. Research is typically only published when the researchers are ready to share their results and after undergoing an extensive peer review process by specialists in the field. Potentially sensitive findings for dual civil and military use are thus typically not chosen to be published by the author or could be flagged during project monitoring or in the peer review process. There should also be no issues with IP as this should have been clarified, and patent applications filed, before submission and publication of the research. An assessment may need to be made, however, of possible strategic and competitive disadvantages to

the mass accumulation of open research publications and future deployment of machine learning and artificial intelligence on collections of publications for new and unforeseen discoveries. This also applies to subscription publications which can be accessed by foreign actors.

Opening up research data sets requires caution to safeguard against foreign interference. The core of the research enterprise is the collection and curation of data. This data can be opened and updated during the course of a project or after the project has ended. The findability of the data depends on its descriptive metadata and the usefulness of the data depends on its format. As the researcher makes the judgement on what data is to be published and how, taking institutional and funding policies into account, no sensitive or confidential data should in principle be released. The review of published data sets is, however, not common and should be further developed and supported in future. Similar to open publications, an assessment may need to be made on the mass accumulation of open data sets and the deployment of machine learning and artificial intelligence on such data sets. It should be noted that there are no common standards for opening data and therefore much open data does not have metadata or is not usefully structured to be meaningfully exploited. International initiatives promoting open research data standards and platforms should be encouraged when they aim to provide a level-playing field in terms of research data sharing in a particular domain (e.g. COVID-19).

FAIR data sets are less vulnerable than open data sets as they are not by necessity open. That is, FAIR data does not need to but can be open just as open data does not need to but can be FAIR. These data sets are provided with metadata that follows the FAIR principles so that machines can find the data and then help researchers to exploit the data. As opposed to open data, FAIR data can be accessed under privacy conditions so that there is an agreement as to how to access and further share or restrict the data. FAIR data can also be accessed via data visiting, whereby the data is stored at the host organisation and can only be accessed by a smart algorithm that can perform queries on the data. In such cases, the level of access to the data is determined by the researcher, organisation, or national data laws. FAIR data that is not open therefore poses no immediate disadvantages to foreign interference. FAIR data that is also open, however, should be treated as machine-readable open data.

Opening up research software, lastly, shows no immediate disadvantages to foreign interference. Research software can serve to run experimental equipment or perform analyses on research data. The importance of the software is directly linked to the role of the equipment and the nature of the research data. Once again, the researcher makes a judgement on opening up the software so that nothing is shared that may pose potential risks. Even then, having the software may not be useful without access to the related equipment or data. An assessment will need to be made on the mass harvesting and combining of software via machine learning and artificial intelligence in the future.

A common issue with these open practices is that we do not yet know how **machine learning and artificial intelligence** will be able to exploit large collections of open methodologies, publications, data and software. This is especially relevant given the development of EOSC which aims to provide access to research in Europe and enable machine learning and artificial intelligence to combine research data and identify new correlations and discoveries. In any case, the researchers themselves, taking institutional and funding policies into account, are responsible for determining what should be opened in Open Science. Any risks to opening research can thus be mitigated by informing researchers about foreign interference and to

forward think about potential implications of their research for future civil and military exploitation before sharing. What seems at first glance to be 'safe' research could prove though interoperability to have dual use applications by foreign actors in the future.

1.6. MULTI-DIMENSIONAL APPROACH

The hybrid nature of foreign interference requires **awareness and vigilance by HEIs and RPOs. Needless to say, the threat of foreign interference is not limited to HEIs and RPOs.** Indeed, public institutions, SMEs, large companies, and NGOs as well as the collaborations between them and with HEIs and RPOs are also at risk. For HEIs and RPOs, the risks extend across all research activities, scientific domains, research outputs, and individuals at the organisations. A multi-dimensional approach to identifying and addressing foreign interference at HEIs and RPOs is therefore needed that takes all of these dimensions into account. Ensuring a safe research and education environment is a responsibility of HEIs and RPOs. Being aware of and protecting against foreign interference, however, requires a shared responsibility of both the organisations and their students and/or staff.

Foreign interference can constitute an element of Hybrid activity. As mentioned in the "The landscape of Hybrid Threats: A conceptual model"[16], financing of cultural groups and think tanks as well as influencing of curricula and academia are listed as possible tools of hybrid activity. An actor can affect the target state's education either by changing the views of key individuals, such as teachers, guardians, rectors, civil servants or policy-makers, or by changing the educational curricula.

A **balance is needed** between maintaining vigilance and reducing risks versus ensuring effective and timely response and recovery capabilities. It is important to stress that HEIs and RPOs should not create a culture of fear towards collaboration with foreign researchers or organisations but rather a culture of awareness and collective responsibility to combat foreign interference. Responses should be proportionate to the risks, scope, and character of the collaboration as well as be informed through due diligence and information from multiple sources. The possible measures presented in this Staff Working Document serve as an initial introduction to developing strategic policies against foreign interference at HEIs and RPOs. It is expected that HEIs and RPOs will build upon these possible actions and tailor their own internal actions according to their specific needs and environments. Additional tools may need to be developed (including context-specific risk assessments, checklists, screening mechanisms, and best practices) to support HEIs and RPOs in identifying and addressing gaps.

The Staff Working Document is structured around **four overarching areas for HEIs and RPOs** to organise their strategic planning on foreign interference. Chapter 2 addresses the values of HEIs and RPOs that are often attacked by foreign interference. Chapter 3 deals with governance structures at HEIs and RPOs to counter foreign interference. Chapter 4 focuses on the risks to partnerships between HEIs and RPOs and foreign actors. Chapter 5 details the cybersecurity risks to HEIs and RPOs posed by foreign interference. Each chapter concludes with a concrete set of potential measures on how to address the identified risks of foreign interference.

[16] https://op.europa.eu/en/publication-detail/-/publication/b534e5b3-7268-11eb-9ac9-01aa75ed71a1/language-en

2. VALUES

2.1. INTRODUCTION

In an era of academic and research internationalisation on the one hand, and a 'third wave' of autocratisation on the other,[17] European HEIs and RPOs are facing new challenges to their free and rights-based operation. These challenges arise from interaction with institutions and individuals that often enrich research and teaching but, at the same time, work in an environment where academia is systematically controlled. Sometimes, the very openness of free universities towards scholars, researchers and students from other countries, the research carried out globally by their academics, and numerous other forms of international exchange and collaboration that are key to universities' success put the unhindered operation of academics and researchers at risk.

Principles of human rights, rule of law, and democracy come under pressure, be it because autocratic and illiberal governments exercise direct control over international academic and research cooperation, or because HEIs and RPOs that are beholden to repressive governments mediate that control. Repression of free academia beyond borders endangers scholars and/ or students and induces self-censorship. It can also compromise academic administration. Risks encountered in this context crystallise as threats to the principles of academic freedom and integrity.

The "freedom indispensable for scientific research" is a universal right, recognized by the International Covenant on Economic Social and Cultural Rights, which has been ratified by more than 170 states to date.[18] It is also recognised as foundational in the EU treaty system. EU Member States reconfirmed their commitment to this freedom in October 2020 by issuing the Bonn Declaration on Freedom of Scientific Research.

Ensuring fundamental academic values is one of the key commitments of the Bologna Process. In the Rome ministerial Communiqué of November 2020, Ministers stated that they commit to upholding institutional autonomy, academic freedom and integrity, participation of students and staff, and public responsibility for and of higher education. They adopted the definition of academic freedom as freedom of academic staff and students to engage in research, teaching, learning and communication in and with society without interference nor fear of reprisal.

The realisation of academic freedom depends on respect for other values, rights and principles, including freedom of speech – a fundamental right of everyone, including but not limited to academics and researchers. The specific requirements flowing from such principles must be responsive to the evolving (and in different EU Member States, somewhat differently institutionalised) university environment.

Sections 2.2 and 2.3 of this chapter prepares the ground for a rights-based assessment and discussion of

[17] Anna Lührmann, Staffan I. Lindberg, "A third wave of autocratization is here: what is new about it?," in Democratization 2019, Vol. 26, No. 7, 1095-1113, https://doi.org/10.1080/13510347.2019.1582029.

[18] https://treaties.un.org/pages/ViewDetails.aspx?src=IND&mtdsg_no=IV-3&chapter=4&clang=_en, and General Comment Number 25 of the UN Committee on Economic, Social and Cultural Rights, https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC/C/GC/25&Lang=en

current threats to academic freedom and integrity in the specific context of academic internationalisation (section 2.4). The chapter concludes with potential measures on how to manage risks and respond to actions that compromise academic freedom.

2.2. ACADEMIC FREEDOM AS A UNIVERSAL RIGHT AND PUBLIC GOOD

Although academic freedom is often referenced in discussions about academic exchange, little attention has so far been given to how the concept of academic freedom should inform our understanding of the threats that are the focus of this Staff Working Document. Accordingly, this section briefly outlines major conceptual features and debates relevant to the discussion.

At its most basic, the concept of academic freedom reflects the insight that it is important for academics and researchers to be able to work and students to study free from undue constraints or interference, and it is often described as a precondition for academic excellence. But even though it may be tempting to make an argument for freedom simply by pointing to its social usefulness, the concept calls for an account that recognises its interdependence with a wider body of values and principles. The Parliamentary Assembly of the Council of Europe, in its report on 'Threats to academic freedom and autonomy of higher education institutions in Europe,' has characterised academic freedom as 'fundamental, on the one hand, to furthering research, the pursuit of truth, research collaboration and the quality of higher education' as well as 'essential to democratic societies.'[19]

Academic freedom as a universal idea. Historically, the idea of academic freedom has been articulated and defended in the wake of events that threaten these freedoms, and there has not been a linear progression towards better protection. In the 1960s, United Nations member states negotiated a binding obligation by including a guarantee of the freedom indispensable for scientific research in the International Covenant on Economic, Social and Cultural Rights (article 15).[20] Later important documents include the 1988 Lima Declaration on Academic Freedom and Autonomy of Institutions of Higher Education[21], the 1990 Kampala Declaration on Intellectual Freedom and Social Responsibility[22], and also the 2013 Hefei Statement on the ten characteristics of contemporary research universities[23], to name but a few declarations from around the world. The member states of the United Nations Education, Science and Cultural Organization (UNESCO) have also committed to academic freedom by issuing several recommendations, notably the UNESCO Recommendation on Science and Scientific Researchers, adopted in 2017, and the earlier UNESCO Recommendation concerning the Status of Higher-Education Teaching Personnel, adopted in 1997[24]. The Bologna Process recognises the importance of education and educational cooperation in the development

[19] Mr Koloman Brenner, Committee on Culture, Science, Education and Media of the Council of Europe Parliamentary Committee, Summary Rapporteur Report, 16 October 2020. https://pace.coe.int/en/files/28749

[20] International Covenant on Economic, Social and Cultural Rights (adopted 16 December 1966, entered into force 3 January 1976) 993 UNTS 3 (ICESCR).

[21] Available online here: https://www.wusgermany.de/sites/wusgermany.de/files/userfiles/WUS-Internationales/wus-lima-englisch.pdf

[22] http://hrlibrary.umn.edu/africa/KAMDOK.htm

[23] https://www.leru.org/publications/hefei-statement. Note that the formulation "responsible exercise of academic freedom" paves the way for a restrictive interpretation of academic freedom.

[24] http://portal.unesco.org/en/ev.php-URL_ID=49455&URL_DO=DO_TOPIC&URL_SECTION=201.html and http://portal.unesco.org/en/ev.php-URL_ID=13144&URL_DO=DO_TOPIC&URL_SECTION=201.html.

and strengthening democratic societies since the 1999 Bologna Declaration[25] and emphasises that in international academic cooperation and exchanges, academic values should prevail, as stated in the Berlin Communiqué.[26] The Bologna Process recognises the importance of education and educational cooperation in the development and strengthening democratic societies since the 1999 Bologna Declaration and emphasises that in international academic cooperation and exchanges, academic values should prevail, as stated in the Berlin Communiqué.

The European Union and its Member States have articulated, debated, codified, and institutionalised the principles of academic freedom and academic integrity, principles which the European Union itself understands as fundamental. The EU Charter of Fundamental Rights, for instance, describes the Union as 'founded on the indivisible, universal values of human dignity, freedom, equality and solidarity' and 'based on the principles of democracy and the rule of law' in the Preamble.[27] And the Bonn Declaration unequivocally recognizes universality in the very first sentence: "The freedom of scientific research is a universal right and public good."

2.3. ACADEMIC FREEDOM AS A FUNDAMENTAL RIGHT IN THE EU

Academic freedom:

> **Is defined as freedom of academic staff and students to engage in research, teaching, learning and communication in and with society without interference nor fear of reprisal[28]. Scientific and academic freedom are set as one of the three key areas in which the European Higher Education Area cooperates with the European Research Area. Freedom of scientific research encompasses the right to freely define research questions, choose and develop theories, gather empirical material and employ academic research methods, to question accepted wisdom and bring forward new ideas. It entails the right to share, disseminate and publish the results thereof, including through training and teaching. It is the freedom of researchers to express their opinion without being disadvantaged by the institution or system in which they work or by governmental or institutional censorship. It is also the freedom to associate in professional or representative academic bodies. Freedom of scientific research requires physical and virtual mobility in pursuit of one's research work, requires a culture of gender equality, the freedom to interact with students and colleagues. Freedom of scientific research is informed by the standards of academic disciplines. At the same time, it enables researchers to challenge these standards when and if new research results begin to question their current validity.[29]**

Within the EU treaty framework, an explicit legal guarantee for academic freedom can be found in Article 13 of the Charter of Fundamental Rights, '*The arts and scientific research shall be free of constraint. Academic*

[25] https://ehea.info/Upload/document/ministerial_declarations/1999_Bologna_Declaration_English_553028.pdf
[26] https://ehea.info/Upload/document/ministerial_declarations/2003_Berlin_Communique_English_577284.pdf
[27] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT
[28] https://ehea.info/Upload/Rome_Ministerial_Communique.pdf
[29] Ibid.

freedom shall be respected.'[30] Similar to other rights which require states not only to prevent these rights to be violated by public authorities, but also to actively promote the right and to protect against threats from third parties. Article 13 of the Charter imposes positive obligations to promote the right and to protect against coercions including also from third parties. The EU member states have committed to a normatively ambitious and comprehensive interpretation of this freedom, which reflects the principles of rule of law and democracy so central to the EU project, both in terms of the EU's internal values, and in terms of its interaction with other systems. Thus, for example, Article 2 of the Treaty on European Union states that *'The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. These values are common to the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail.'* [31] Article 179 TFEU acknowledges the need for researchers to cooperate freely across borders within the 'European Research Area' and Article 165 defines mobility of students and teachers as one of the main aims of the Union action in the field of education. Against this background, it is not surprising that EU institutions, notably the European Parliament, and EU Member States have responded to perceived pressures on academic freedom through external exchanges by adopting several resolutions and declarations relevant to our discussion.[32]

Academic freedom and integrity as interdependent and structurally complex ideas. Academic freedom is part of a wider web of interdependent human rights, such as non-discrimination rights, freedom of speech, association and movement as well as liberty of person. This is important to understanding the complexity of threats to academic freedom since academic freedom may only be fully guaranteed through respect for all human rights, understood as indivisible from each other and from the values of a democratic society.[33]

As stated by a recent decision of the Court of Justice of the European Union[34], the concept of academic freedom includes not only substantively autonomous research and teaching that is free from state interference, but also its institutional and organisational framework. Affiliation with a state or private university is, in practice, an essential condition for academic research. The university serves as a platform for academic discourse and a network and infrastructure for teaching staff, students and donors. Consequently, the concept of academic freedom cannot be isolated from other fundamental academic values like institutional autonomy, or the participation of staff and students in higher education governance.

It also means that the individual person's enjoyment of academic freedom is central, and that the institutions hosting and nurturing teaching and research can be both victims and perpetrators of violations of the principle. Academic freedom therefore must not only be protected against interference by state actors, but also – within limits – external non-state actors such as private businesses.[35] It also operates internally, that

[30] Available online here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

[31] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012M%2FTXT

[32] In addition to the Bonn Declaration, see European Parliament, Resolution on the state of EU-China relations, 12 September 2018; European Parliament, Defence of academic freedom in the EU's external action, 29 November 2018.Disucssed in detail in section II.

[33] The relationship between human rights and democracy is subject to debate but the EU affirms both as indispensable. The EU Human Rights and Democracy Action Plan for 2020-2024 requires the European Union to: "Support action to protect academic freedom, the autonomy of education institutions, as well as their capacity to provide online and distance learning. Promote the implementation of human rights education on the basis of the World Programme for Human Rights Education".

[34] Judgment of the Court of 6 October 2020 in Case C 66/18 European Commission v Hungary. Available at:https://curia.europa.eu/juris/document/document.jsf;jsessionid=63B56AF69A1DB47C51863DB95E22FD64?text=&docid=232082&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=7178288

[35] See e.g. John Gerard Ruggie (draft, June 2017), 'The social construction of the UN Business and Human Rights Principles,' Corporate Responsibility Initiative Working Paper No. 67. Cambridge, MA: John F. Kennedy School of Government, Harvard University.

is, within academic institutions, especially insofar as these institutions control the work of their academic staff and activities of students. Thus **academic freedom has individual and institutional** aspects.

2.4. UNDERSTANDING THE RISKS POSED BY INTERNATIONAL EXCHANGE AND COLLABORATION WITH REGARD TO ACADEMIC FREEDOM

Exchange and collaboration in academia encompasses activities and programmes ranging from students opting to study abroad to collaborative transnational research projects, foreign campuses, and international travel by scholars. The European Union has recognised that internationalisation is central to many of the most meaningful and valuable academic endeavours. Through many of its programmes and mechanisms, the EU has evolved into an active and major global supporter of academic internationalisation. For example, 4.700 participants from 124 non-EU countries participated in the research programme Horizon 2020, which 'demonstrates a very broad international outreach attracting talent from around the world in particular from higher education organisations.'[36]

However, the dissemination of principles and institutional or political practices is never unilateral. The challenges to liberal democracy mentioned at the beginning of this chapter have also significantly affected the ability of academic communities to operate freely and with integrity. International academic exchange and collaboration with countries undergoing autocratization, as well as with established autocracies, where academia is subject to invasive or repressive controls, can effectively 'export' these problems beyond such countries' borders. This is done, for example, by controlling citizens working abroad, by obligating them to regularly report to embassies, by incentivizing scholars and students to report on each other, by surveying and even censoring digital communication – including but not limited to virtual classrooms – by harassing or detaining critical scholars when they return home, or by harassing family members that remain at home or even taking them as hostages. The export of repressive controls also includes pressure on academic publishing houses in liberal democracies to censor content, the denial of visas for critical scholars who seek to visit repressive countries for their academic work, and the insertion of legal clauses in cooperation agreements of the academic institutions in the European Union that effectively turn them into enablers of academic freedom violations.

Last but not least, authoritarian practices include attempts to co-opt scholars and institutions. While all states engage in public diplomacy – and there is nothing wrong with that – covert efforts to incentivize academics through funding, honorary titles, paid positions and other privileges, constitute a threat to academic freedom and integrity and can therefore be perceived as foreign interference. This is the case when scholars are nudged or threatened into normalizing intrusive political control over academic institutions. In addition to attempts at influencing individual scholars' behaviour, the normalization of repression can also take the form of highly visible agreements and declarations with prominent academic institutions in Europe, thereby bolstering the reputation and legitimacy of research institutions in repressive contexts. Researchers in Europe and abroad who understand the propaganda efforts that underlie such statements

[36] 'From Horizon 2020 to Horizon Europe,' February 2019, available online at https://ec.europa.eu/info/sites/info/files/research_and_innovation/knowledge_publications_tools_and_data/documents/h2020_monitoring_flash_022019.pdf

perceive European institutions' approval as wilful ignorance or, even worse, as complicity. In combination, authoritarian practices and their accommodation risk fostering a climate of fear and hindering scholars from searching for truth. At the core of this risk are conflicts of interest,[37] principles and values.

Activities detrimental to academic freedom and integrity may be carried out not only by actors originating from autocratic countries or institutions ('autocratic actors'). Such activities can also originate with actors in democratic settings, such as for-profit research funders that prioritize their own interests over sound and reliable research, or universities concluding agreements resulting in self-censorship, or academic publishers deciding to accept and implement censorship instructions from a foreign government or other actors.

In light of these realities, the new Horizon Europe programme (which builds on Horizon 2020 and runs from 2021 to 2027) highlights the importance of academic freedom. It expressly refers to article 13 of the Charter of Fundamental Rights and commits to promoting the respect of academic freedom in all countries that benefit from the programme's funds. Similarly, according to Regulation 2021/817 establishing Erasmus+, it should be ensured that academic freedom is respected by the countries receiving funds under the Programme.[38] Fundamental academic values will be the backbone of the higher education transformation agenda.

2.5. POSSIBLE MEASURES TO REDUCE AND MANAGE RISKS TO ACADEMIC FREEDOM AND INTEGRITY IN EUROPE

In light of the diversity of universities and research institutions across the European Union, there is no 'one size fits all' solution. A risk management and response strategy tailored to the specific institutional environment of each system is indispensable, because specific institutions' vulnerabilities as well as students and individual scholars' exposure to threats that undermine academic freedom and integrity vary greatly from system to system. Having said this, it is suggested that it is possible to articulate some rules and principles that apply across a variety of different institutional settings:

a) Identify countries and partner institutions where academic freedom is at risk

For countries where academic freedom is generally well respected, there is no need for a detailed assessment of values at risk. However, academic cooperation with institutions or individuals from countries where academic freedom is under pressure always requires risk analysis and the development of a mitigation strategy. This means that it is important, in a first step, to identify countries of concern for the purposes of the present discussion.

The global Academic Freedom Index (AFi) provides a first point of orientation. This index makes country-level data available on (1) the freedom to research and teach; (2) freedom of academic exchange and dissemination; (3) institutional autonomy; (4) campus integrity; and (5) freedom of academic and cultural expression. The aggregate AFi combines all five indicators into a score between 0 and 1, with 0 being the bottom of the scale.[39]

---

[37] "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), Recommended Principles to Guide Academy-Industry Relationships, The AAUP Foundation, https://www.aaup.org/file/Academy-Industry%20Relationships_0.pdf

[38] See Recital 65 of Reg. 2021/817 which reads : "In line with Article 13 of the Charter, it should also be ensured that academic freedom is respected by the countries receiving funds under the Programme.".

[39] The Academic Freedom Index was developed collaboratively by experts at the Global Public Policy Institute, the Friedrich-Alexander-Universität Erlangen-Nürnberg, the Scholars at Risk Network, and the V-Dem Institute. For an introduction to the Academic Freedom Index and guidance on how to use it in day-to-day operations, see Katrin Kinzelbach, Ilyas Saliba, Janika Spannagel, Robert Quinn, 'Free Universities: Putting the Academic Freedom Index Into Action,' GPPi, March 2020, https://www.gppi.net/2020/03/26/free-universities.

When dealing with counterparts in countries where academic freedom is not well protected (AFi status group C or lower, i.e. AFi scores < 0.6), research institutions could:

- **Conduct a more detailed assessment of the research, education and institutional environment in the country and at the specific partner institution (note that there may be sub-national differences which are not captured by the AFi score).**
- **Analyse the external actors' motives for undermining academic freedom, and how these motives may relate to specific educational and research endeavours conducted by European researchers and institutions.**
- **Monitor the external actors' capacities for restricting and/ or instrumentalising European researchers and institutions.**
- **Consider the security implications that may occur during cooperation with academic institutions operating in third countries with restricted academic freedom.**

b) Conduct a vulnerability assessment to understand external pressures on academic freedom and integrity in the institution

In addition to understanding external actors' motives and capacities for undermining academic freedom, it is crucially important to analyse the structures and mechanisms that can lead academic actors in Europe to become complicit with such attacks. Often, the precondition for the success of external attacks on academic freedom in Europe is active cooperation or (in the case of coercion) at least passivity by European states, institutions and academics. Introspection is the first step for developing a tailored response. Accordingly, research institutions could:

- **Undertake institution and/or project-specific vulnerability assessments to trace how external pressures may impact research, teaching, publication and outreach activities.**
- **Review if existing cooperation with external actors has created any dependencies (financial or other) that may motivate academic actors to self-censor in line with external requests or threats.**
- **Verify that all partnership agreements adequately protect academic freedom and do not include clauses that place undue limitations on research, teaching and public speaking (see also Chapter 5).**
- **Monitor external appointments as well as honorary degrees awarded to researchers, and ensure regular reporting of such engagements to minimize risks of co-optation and instrumentalisation.**
- **Ensure that everyone who interacts with institutions and individuals in – or from – countries where academic freedom and universal values are at risk have received adequate training to address human rights-related challenges in such settings.**
- **Set-up a reporting mechanism to map threats to academic freedom in the institution.**

c) Strengthen commitment to academic freedom and integrity at institutional and individual levels

In light of persistent threats to academic freedom, it is insufficient to focus on addressing specific vulnerabilities once they are identified. Instead, European universities and research institutions are well advised to adopt a preventive approach by fostering an environment where the commitment to academic freedom and integrity is cherished and practiced as a matter of course. A consistent promotion of these values will strengthen institutional and individual resilience against any attempts to undermine them. This requires academic institutions to:

- **Integrate academic freedom and integrity into the core curriculum of any academic education program, thereby building up sound foundational knowledge on these values – and related rights – across the academic profession.**
- **Examine and, if necessary, amend internal quality assurance processes to ensure that they address the protection and promotion of academic freedom. Cooperate, when needed, to update national external quality assurance agency guidelines, as well as the Standards and Guidelines for Quality Assurance in the European Higher Education Area, to cover fundamental academic values.**
- **Affirm frequently and publicly the importance of academic freedom and integrity, including in academic internationalisation contexts.**
- **Raise awareness among students, academic and administrative staff for the importance and protection of fundamental academic values.**
- **Explicitly incorporate academic freedom in the context of transnational collaborative activity or interaction, notably through written clauses in cooperation agreements, and institutionalise these requirements through relevant administrative procedures.**
- **Ensure that everyone who interacts with institutions and individuals in – or from – countries where academic freedom and universal values are at risk have received adequate training to address human rights-related challenges in such settings.**
- **Support scholars who work on research topics or engage in education activities that external actors seek to supress, for example through visa bans, or boycott of courses by: offering regular conversations on how the institution's management can best support the respective scholar; considering the obstacles in performance appraisal and contract extension decisions so that external attempts to undermine research do not negatively affect the individual scholar's career; and by providing legal assistance in the case of smear campaigns and defamation lawsuits.**
- **Launch a dedicated support programme for visiting scholars and students from repressive countries – as well as for students from these countries.**

- **Help protect persecuted scholars or students by providing (temporary) sanctuary,[40] including from countries in which the institution may have important ongoing cooperation projects (if applicable), thereby demonstrating that the institution's commitment to academic freedom is a matter of principle and not subject to negotiation.**
- **Consider signing a democracy pledge – rejecting funding from authoritarian countries or actors beholden to such countries.[41]**

d) Continue to cooperate with partners in repressive settings

Academics and institutions deciding about cooperative projects with scholars and institutions in repressive settings often face seemingly irresolvable dilemmas. For example, a decision to self-censor in a piece of academic writing may be motivated by elements of fear and even complicity, but it can also be motivated by the legitimate goal of protecting colleagues abroad or by the wish to uphold a cooperation project/ agreement or to gain access to important data. In such situations, scholars may feel that they must weigh the imperative of doing no harm, or the value of continued research, against the imperative of speaking the truth.

Rather than fighting the phenomenon of self-censorship or other accommodative behaviour, European academia must recognize that vulnerability to authoritarian and illiberal interference is an undeniable reality in the contemporary context of globalized knowledge production, and that this vulnerability results in a political responsibility to strengthen academics institutions' ability to deal with these challenges. The task, then, is to build capacity for better analysing, detecting and responding to such threats without putting an end to international research cooperation.

It is important to avoid stigmatising or alienating academic colleagues and institutions in settings where illiberal or authoritarian constraints make it difficult to engage in academic endeavours and uphold scholars' responsibility to the truth. Academic freedom cannot be protected by othering and alienating, instead this is a sure way to place the principle and value itself at risk.

Consequently, European universities and research institutions should:

- **Ensure continued openness to exchange and collaboration with scholars and students in non-liberal institutional environments.**
- **Create awareness and understanding of how repressive settings can affect academic freedom and integrity among proposed collaboration partners by offering general trainings as well as guidance for project-specific risk assessments.**
- **Review standard ethics procedures to ensure that risky research in repressive settings will not automatically be rejected (and thereby repressed) by the relevant committee but, rather, adjusted as necessary to minimize the identified risks.**
- **Provide guidance and tailored technical support on data and digital security to help manage**

[40] See: Scholars At Risk, 'Protection,' https://www.scholarsatrisk.org/protection/ and the European initiative Inspireeurope, coordinated by Maynooth University: https://www.maynoothuniversity.ie/sar-europe/inspireurope.

[41] See: Thorsten Benner, 'It's time for think tanks and universities to take the democracy pledge,' Washington Post,16 January 2019, https://www.washingtonpost.com/opinions/2019/01/16/its-time-think-tanks-universities-take-democracy-pledge/.

surveillance risks in repressive settings – thereby helping to ensure that the researcher and his or her counterparts remain safe while conducting research (see also Chapter 5).

- Set up an emergency procedure to deal with cases of harassment, detention or disappearance.
- Facilitate best practice exchanges and mutual learning on how academics and students can cope with incentives and pressure to self-censor.
- Commit to transparency and screening mechanisms tailored to address collaboration with repressive settings.

3. GOVERNANCE

3.1. INTRODUCTION

A robust system of governance is necessary for HEIs and RPOs to operate effectively and ensure the protection of their values, security and competiveness from foreign interference. Given the nature of the threats of foreign interference that can occur at institutional and individual level, governance should be a combination of top down and bottom up measures. While the overall responsibility is institutional, each person in an institution should be aware of the issues and how to identify potential threats. There must be clear leadership from the top combined with individual responsibility supported by education and training. It is critical to have a governance structure in place that can ensure that these two can be effectively managed. Some examples of possible measures on how to address foreign interference governance in Germany, Sweden and the UK are given below.

Examples of Governance

Sweden

The Swedish Foundation for International Cooperation in Research and Higher Education has published *Responsible internationalisation: Guidelines for reflection on international academic collaboration*[42]. This document outlines the types of foreign interference that can arise in the context of international collaboration. The role of staff and students at all levels and the institutions are highlighted. The approach taken is to provide a list of questions for each area that should be asked before engaging in a collaborative venture. This should result in an assessment of the contents and consequences of international collaboration before, during and after a project.

Germany

The German Rectors Conference (HRK) *Guidelines and standards in international university cooperation*[43] emphasises robust governance and professional management. This is in the context of increasing complexity of international cooperation which needs to be accompanied by increased professionalisation of the structures and processes provided at universities in support of internationalisation. They stress that a successful collaboration is based on clarity and transparency in the allocation of tasks and responsibilities. In addition, there should be joint transparent decision-making structures that also include procedures applying in the event of a disagreement and clearly outlined exit strategies in the interests of risk management.

United Kingdom

Universities UK (UUK) has published guidelines on *Managing Risks in Internationalisation:*

[42] https://www.stint.se/wp-content/uploads/2020/01/STINT_rapport_Responsible_internationalisation.pdf

[43] https://www.hrk.de/fileadmin/redaktion/hrk/02-Dokumente/02-01-Beschluesse/Beschluss_Leitlinien_und_Standards_HRK_Praesidium_6.4.2020_EN.pdf

security related issues[44]**. This emphasises the importance of good governance and effective risk management processes to help to protect individuals, institutions and the sector from the legal, financial and reputational consequences of security-related risks. They also stress the need to develop a positive, risk-informed culture, underpinned by robust governance, reporting and risk-management structures.**

While foreign interference is not a new issue it is receiving greater attention especially in the context of Open Science policies. It will be up to each institution to decide how to deal with this issue as for the moment it is voluntary. However, as with research ethics and research integrity, funding agencies may introduce mandatory requirements to have procedures in place to address foreign interference.

Above, guidelines are provided that can be adapted to national and regional contexts given the wide diversity of institutional legal structures across Europe. The specific cases of governance for Values, Partnerships and Cybersecurity are addressed in Chapters 2, 4 and 5.

Governance in this context is complex given that foreign interference can occur at institutional and individual level. For example, the need for institutions to attract external funding can lead to compromises by leadership on fundamental values that opens the door to foreign interference. Financial donations or co-funding of institutes may be accompanied with pressure to limit discourse and hence academic freedom on issues that are not consistent with the views of the donor. Pressures to publish and attract research grants can lead to researchers simply following the money without being aware of or regard for foreign interference. However, it is important to understand that the behaviour of researchers may also be driven by institutional pressures to increase overall publication performance in order to boost university rankings. These examples emphasise the need for a form of institutional oversight that could be organised internally or externally. In any case there will be need for a process for individuals to have recourse to address what may be institutional failures.

3.2. FOREIGN INTERFERENCE COMMITTEE

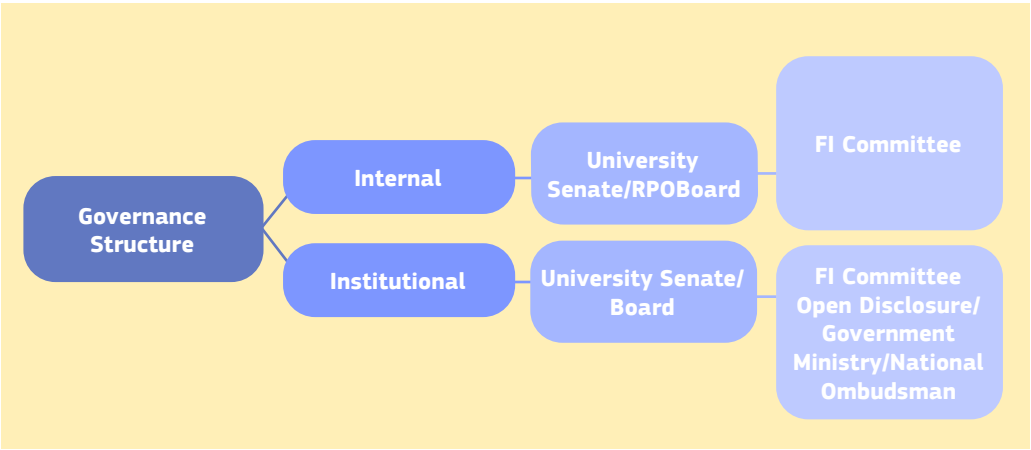
Issues relating to foreign interference can be dealt with by appointing an institution wide **Foreign Interference Committee** (FI Committee) that would be similar to that for research ethics, ethics in security relevant research or research integrity, for example. In fact, it would be expedient to integrate the governance role to one of the relevant existing committees to reduce bureaucracy. For universities, this high-level committee would be appointed by the university senate or board depending on the institutional regulations. It would be expected that such a committee would include senior staff, for example, the Vice President for Research, Vice President for Academic Affairs and the Chair of the Ethics Committee. A senior member of management would be appointed who will act as a point of contact for disclosure. It will be essential that the approach for managing potential instances of foreign interference is not seen as yet another administrative burden placed on staff. On the contrary, avoiding foreign interference should be viewed from the perspective developing individual and institutional resilience to external threats. Furthermore, FI Committees from different institutions could establish good connections in order to facilitate exchange of information and best practices.

[44] https://www.universitiesuk.ac.uk/policy-and-analysis/reports/Pages/managing-risks-in-internationalisation.aspx

In the case of issues relating to foreign interference at institutional level, there may need to be additional external oversight. This could be provided by the government body that funds universities or a national ombudsman could be appointed in this role. However, one must be conscious of striking a balance between institutional autonomy and accountability. The possible guiding principle here for institutions should be to ensure an effective self-governance that respects academic freedom and human rights[45]. Having an open system that combines open disclosure and internal criticism within the institution could provide a robust means for addressing foreign interference at institutional level. This could be achieved by inviting external experts to work with the FI Committee on issues that relate to foreign interference at institutional level.

In each case the governance of foreign interference should ultimately be the responsibility of the university senate or board depending on institutional management and oversight, see Figure 3.1.

Figure 3.1: Governance structures for foreign interference.



As stated above, in order to have an efficient structure that does not increase bureaucracy, the management of foreign interference should be integrated to the work of an existing committee. Given the nature of the issues involved this could be one of the committees that manage ethics, research integrity or dual use. The role of the **FI Committee** would be to have oversight of (see Figure 3.2),

- Awareness raising through Education & Training;
- Monitoring of potential risks;
- Management of research data and intellectual assets in international cooperations and providing advice and support to research groups involved;
- Risk Management and Mitigation; and
- Investigation of Foreign Interference.

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

The Committee will manage the identification of risks and mitigation measures. These will include those risks that concern core values, international partnerships and security (both infrastructure and cybersecurity). However, these risk studies should only be carried out when the countries involved do pose a potential hazard (see also Chapter 2 and 4 for details). The details of foreign interference for these are detailed in the relevant sections of this document. The Committee will oversee measures to raise awareness of potential threats from foreign interference among staff and students. This will be achieved through education and training as the proactive participation of staff and students will be a core component of identifying risks. This importance of awareness raising and training has already been stressed in the previous chapter on Values. The Committee will provide guidance and oversee measures to ensure smart management of intellectual assets and compliance with intellectual property rules in international cooperations. The FI Committee will also be responsible for investigating cases of potential foreign interference. This may require external expert input especially when dealing with cases of institutional foreign interference. In instances it may be necessary to impose disciplinary procedures, but the focus will be identifying and avoiding potential foreign interference. When assessing risk, it is important that FI Committee safeguards academic freedom.

Figure 3.2: Governance processes

3.3. POSSIBLE PREVENTIVE MEASURES

Ideally, the potential for foreign interference should be recognised before it becomes an actual threat. The combination of awareness raising through education and training along with risk monitoring and analysis will be effective mechanisms to identify and avoid foreign interference. The governance structure described above will be necessary to ensure that values and competitivity are protected ensuring both internal and external oversight.

It will be important to have a structure in place that can be adapted to different national and different research systems. There are lessons to be learned from the approach to the governance of research integrity in universities and RPOs across Europe. There are varying national approaches, but all share the same principles of the need for institutional and personal responsibility. In the case of research integrity funding agencies play a major role as it is often their funds that have been used in research where scientific misconduct has occurred. Similarly, funding agencies could play a role in the governance

of foreign interference. For example, research partnerships that involve Third Countries are often funded by national and European agencies. Public universities are partially funded by government and therefore the state could play a role where institutions could facilitate foreign interference. At this level it could be important to introduce a screening mechanism of financial donations in case they come from countries or institutions flagged as potential risk of foreign interference. This however will require delicate balancing between institutional autonomy and government oversight. In order to maintain independence, universities and RPO's will need a robust procedure that will convince national authorities.

The Example of Research Integrity

There are similarities between the governance against foreign interference and the governance for research integrity. Therefore, one can learn from and draw on that experience of governance for research integrity and apply it to foreign interference. One thing that has emerged is that promoting research integrity policies, improving mentoring and training, and encouraging transparent communication amongst researchers helps reduce scientific misconduct[46]. In a similar vein for protecting values and competitiveness, it will be important to promote policies to ensure

- academic freedom;
- excellence, openness and freedom in research, teaching and support for learning;
- data security and protecting Intellectual Property
- ethics, integrity and trust.

There are many national examples of good practice in dealing with Research Integrity that can be drawn upon when dealing with foreign interference. A common theme is the approach of supportive governance to create an incentivised rather than a punitive environment. The governance of research integrity is usually a combination of internal and external oversight.

Ireland

The Irish National Research Integrity Forum[47] is collaboration between universities, RPO's and funding agencies to oversee and ensure good practice in research. A core element is supporting the development and roll-out of research integrity training programmes for staff and students. The principles to support good pratice are captured in the *National Policy Statement on Ensuring Research Integrity in Ireland*[48]. The autonomy of institutions is respected in that investigations are carried out internally but will the option of external review if deemed necessary.

Luxembourg

The Luxembourg Agency for Research Integrity (LARI)[49] was established in 2016 as a joint venture between the university, RPO and national research funding organisations. The approach

[46] See for example, https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0127556
[47] https://www.iua.ie/for-researchers/research-integrity/
[48] https://www.iua.ie/wp-content/uploads/2019/08/IUA_Research_Integrity_in_Ireland_Report_2019.pdf
[49] https://lari.lu

is to promote the responsible conduct of research and ensure an independent process to investigate potential instances of scientific misconduct. LARI provides training on good practice along with peer learning and coaching. The investigative procedure ensures that whistleblowers can retain a level of anonymity. This is very important in cases where a PhD candidate reports misconduct by their supervisor, for example.

An effective way of encapsulating all of issues that relate to foreign interference would be the development of an institutional **Code of Conduct for Protecting Institutions from Foreign Interference** that ensures the protection of,

- academic freedom;
- data security, privacy and Intellectual Property[50];
- excellence and openness in research, teaching and support for learning;
- ethics, integrity and trust.

The Code should include procedures for,

- Identification of foreign interference (including data breaches and ethically unsound research)
- Disclosure procedure that protects the identity of individuals
- Whistleblower protection
- Dealing with internal conflicts of interest

When dealing with potential risk, the code would be applied to assess risk and initiate the appropriate internal procedures if necessary. A key part of this process will be the individual responsibility of researchers to assess the risk of situations that could lead to foreign interference. These could range from data requests, or invitations to visit third countries for collaboration.

At individual level it is important of course to have **corrective measures** in place through disciplinary procedures especially for those who knowingly engage in supporting Foreign Interference. This could be reinforced by including clauses on foreign interference in staff contract as is the case for ethics. However, it is important to stress that the majority of individuals do not support foreign interference, but it may be actions on their part that inadvertently give rise to such threats. Therefore, and it is important to educate and **incentivise** them to recognise and disclose foreign interference based on clear evidence. Part of this must be the protection of those who do disclose such behaviour especially for students and early stage and early career researchers (R1-R2). These are particularly vulnerable groups especially if they are disclosing behaviour facilitating Foreign Interference by supervisors or mentors. For these reasons there should be a robust system to protect **whistleblowers**[51] as part of the governance.

[50] The Commission Communication 'A New ERA for Research and Innovation' (COM(2020)628 final) announces to update and develop guiding principles for knowledge valorisation and a code of practice for the smart use of intellectual property, by the end of 2022, which could become a further reference for developing the IP chapter of an institutional Code of Conduct for Protecting Institutions from Foreign Interference

[51] https://www.consilium.europa.eu/en/press/press-releases/2019/10/07/better-protection-of-whistle-blowers-new-eu-wide-rules-to-kick-in-in-2021/

3.4. SUPPORTIVE TOOLS

Good governance can only be effective with the full participation of staff and students at all levels from Bachelor and Master level students to executive and research leaders. This must incentivise staff to engage fully but also have investigative and disciplinary procedures.

Raising Awareness

The key to avoiding foreign interference is to ensure that all staff and students are made aware and shown how to carry out their own analysis of potential risks in their daily activities. Of paramount importance, it is necessary to have training in place to understand the nature and types of foreign interference that can occur. This type of training should be for all staff and students and recognised as part of continuous professional development. In particular, this training should be included as part of standard generic/ transferable skills training for students and researchers (at all levels R1-R4) in a manner similar to research integrity and research ethics. For PhD candidates it could be integrated into graduate programmes and structured doctoral training. Other involved staff such as business developers, IP managers and exports control experts should not be excluded from receiving appropriate training.

Training can be delivered through formal courses and workshops. There can be mentoring of students and researchers by senior staff. The training should be tailored for different levels of student and staff categories as the associated threats are different. For example, at the level of PhD candidate, foreign interference may be simply requests for data from third country institutions. At senior researcher level (R4), it may be proposals to carry out ethically unsound research in a third country as part of an internationally collaborative project. The trainings should be inclusive as not only research staff but other staff as well can be targeted. Training will typically include the following:

- Institutional Code of Conduct for Foreign Interference;
- Identification of Foreign Interference (including data breaches and ethically unsound research);
- IP management and protection;
- export control and dual use legislation;
- Disclosure procedure;
- Whistleblower protection; and
- Dealing with internal conflicts of interest.

Investigative Procedures

The FI Committee may instigate an investigation into potential foreign interference following disclosure. This could be an instance where a proposed or existing international partnership could lead to data security issues. If the issue cannot be resolved to the satisfaction of the FI Committee, the planned or existing collaboration will be cancelled.

Corrective Measures

If following an investigation it becomes clear that a member of staff or a student have been actively involved in foreign interference then the normal institutional disciplinary procedures can be applied.

From an institutional perspective there should be legal protections to ensure that staff are fully informed and contractually obliged to avoid foreign interference. This can be included in contracts in a similar manner to ethics and dual use.

Possible measures on Governance

In order to put in place a strong governance to address issues of foreign interference at institutional and individual level, universities and RPO's should

Publish a Code of Conduct for Foreign Interference.

- Ensures protection of
  - academic freedom;
  - data security and intellectual property;
  - excellence and openness in research, teaching and support for learning;
  - ethics, integrity and trust
- includes procedures for
  - identification of foreign interference (including data breaches and ethically unsound research);
  - whistleblower protection;
  - dealing with internal conflicts of interest

Establish a Foreign Interference (FI) Committee

- FI Committee integrated with existing institutional structure (e.g. ethics, research integrity)
- FI Committee connected with FI Committees of other institutions and local, regional and national authorities.
- FI Committee responsible for,
  - awareness raising through education & training;
  - monitoring of potential risks;
  - monitoring of potential risks;
  - management of research data and intellectual assets in international cooperations and providing advice and support to research groups involved;
  - risk management and risk mitigation;
  - investigation of Foreign Interference.

4. PARTNERSHIPS

4.1. INTRODUCTION

Research and education at HEIs and RPOs is highly internationalized: institutions, academics and researchers often collaborate with their counterparts from multiple countries on teaching and research. Therefore, engaging in international partnerships in research and education is important for European HEIs and RPOs. Research partnerships are major drivers in the advancement of research and innovation, and as a result, of economic growth. Educational partnerships contribute to diversity in the classroom and to the quality of education. A partnership is a relationship based on mutually beneficial collaboration and the idea that results are better achieved together than alone. There are informal partnerships, such as dialogues and small-scale cooperation between individual scholars, and formal partnerships, which refer to collaboration based on a formal agreement. In both types of partnership all parties involved should be equally committed to the relationship and act responsibly and ethically. In practice this is not always the case.

Parties involved jointly shape a partnership based on their own interests, academic traditions and their national academic systems. These traditions and systems may differ considerably and parties may want to rely on their own procedures, may have different views on how to shape the collaboration, or on what to include in the agreement. Academic partners may need to adhere to local laws and regulations that are not in line with European (national) laws or norms. Institutions and/or the entities overseeing and/or funding them, may seek to exploit or compromise collaboration or to influence a partnership deal through providing negative incentives (e.g. threats) or positive incentives (e.g. financial arrangements) targeted at an institution or individuals, leading to a breach of knowledge security or academic integrity, including research integrity. In recent years, a growing number of cases of interference in international partnerships of European HEIs and RPOs have been reported and concerns about potential risks of partnerships have become more pronounced.

EXAMPLES

- **Lack of reciprocity in data sharing. In partnerships between European and third country research institutes it regularly happens that the partners in the third country do not receive permission to share raw data gathered within the context of the joint research project. While the European side provides all the data, the third country will classify data as being strategic or sensitive, and therefore not eligible to sharing with foreign partners.**
- **Accepting a third country requirement to abide by their national law. In 2020, it emerged that an EU Member State had signed a contract binding it to abide by third country law instead of its national law. This would give the third country government strong leverage to censor teaching programs.**
- **Third country partner side not respecting financial commitments. There have been numerous cases where a third country partner fails to live up to its financial commitments in co-funded projects. For example, under the EU research and innovation programme Horizon 2020, only 60% of joint projects have received the negotiated third country co-funding.**

In order to mitigate the risks involved, a formal partnership with a foreign entity should be built on the basis of reciprocity and transparency and needs to be established with much care and attention to details. HEIs and RPOs should make it their priority to develop risk management strategies and apply them when designing, negotiating and implementing partnerships. These tasks may not be part of the DNA of scientists and staff working at HEIs and RPOs. Many institutions and researchers highly value the open character of academic collaboration and want to focus on the opportunities and benefits rather than on the risks. However, effective risk management is in institutions' own interest. It helps them to protect their long-term competitive positions in research, safeguard the security and academic freedom of their staff and students, and to keep their good reputations.

4.2. THE RISKS

The decision to confirm collaboration in an agreement is a step towards establishing new collaboration or expanding or intensifying existing collaboration. Establishing a formal partnership always carries the risks of one side not living up to the agreement. In particular in transnational collaboration, partners working in different academic traditions and systems may have different assumptions from the start. Often parties involved decide to keep the agreement simple and brief, assuming they share the same values, norms, and expectations and agreeing in good faith to work out the details at a later stage. However, when the details of an agreement are not explicitly discussed and/or negotiated upon early on, differences may arise and grow into problems once the joint project is under way.

There are several types of risks, including financial, security, ethical and reputational risks. Concrete risks include:

- Lack of reciprocity
    - in commitment to the partnership
    - in access to information, research facilities, research results
- Unequal investments and/or unequal benefits.
- Conflicts about the use of research data in publications or about sharing/exporting research data.
- Loss or compromise of Intellectual Property: IP issues may affect the conduct, publication, and commercial exploitation of results during and after a project. In particular when research results are of (potential) commercial interest to partners, there is a risk of misappropriation or even theft of copy rights or patents, or unauthorised transfer of research findings to local non-EU industries.
- Conflicts about (first) authorship of publications in scientific journals. Authorship is a major basis for a scientist's individual reputation, credit, financial revenues, and career opportunities.
- Breaches of academic freedom.
- Unexpected limitations for conducting research following from local laws;
- Dual use of research results: use for military purposes or for applications that are used to violate human right.

- Making available funds and economic resources which benefit, directly or indirectly, sanctioned persons, entities and bodies in certain third countries under EU Restrictive measures (EU sanctions)[52].

4.3. MINIMIZING THE RISKS AND DEVELOPING SUSTAINABLE PARTNERSHIPS

In order to minimize and manage the above risks when entering into an international partnership, institutions need to develop or strengthen risk management strategies and procedures. Such a strategy consists of a number of steps:

1. **the development of general prerequisites for the implementation of a risk management system. Various policy lines, procedures and regulations need to be in place before the risks of collaboration projects can be successfully assessed and mitigated;**
2. **due diligence: the potential partnership needs to be assessed in terms of potential risks;**
3. **subsequently, the partnership agreement or contract should be carefully negotiated;**
4. **finally, the implementation of the contract needs to be monitored.**

These four steps are elaborated upon in the following sections.

4.3.1. Prerequisites for risk management: what needs to be in place?

In order to ensure that knowledge security and academic integrity is safeguarded in all partnerships, HEIs and RPOs are should review their procedures and expand and strengthen them where needed. This should be overseen by the institution's **FI Committee** as part of the governance of partnerships. Some issues need to be considered and decided upon before the potential risks of partnerships can be assessed. In concrete and practical terms institutions should:

- **Raise** broad **awareness** of potential risks involved in engaging in a partnership and of the ways their institution seeks to mitigate them. This can be achieved through training on foreign interference and dissemination of information at all levels, including research group levels. The information can be published at the institution's website and in newsletters and should be brought to academics and researchers' attention through round tables, workshops and training sessions fine-tuned to the needs of each specific group according to work environment (legal, ICT, internationalisation) or fields of research. The information should explain:
  - the potential risks involved in partnerships;
  - how and where scientists and officers can find information or get support at institutional level (through the FI Committee);
  - when and to whom to report plans for a partnership; and
  - the due diligence procedures to be followed.

[52] Overview of the restrictive measures adopted by the EU can be found on https://sanctionsmap.eu/#/main

It is recommended that each department and research group appoint a person responsible for raising awareness and that risk management with regard to partnerships is regular put at the agenda of senior staff meetings.

- **Raise support for a risk management strategy** by explaining why implementation of such a framework is in the individual, HEI/RPO's or national interest, it will help to:
    - protect researchers, their rights, and their reputations;
    - safeguard the institution's overall interests, including their knowledge position and reputation.

Following the relevant procedures will provide researchers engaging in complex partnerships clarity and confidence, in particular when a partnership is developed in a politicized environment and concerns are raised by the media, fellow scholars, political parties, or society.

- **Create awareness** and knowledge of **export control legislation**; make clear that it is the responsibility of researchers to consider and monitor all potential end-uses and misuses of their research.
- I**dentify** the institution's **'crown jewels'**: areas of high-level research and expertise in which the HEI/RPO stands out and/or which are of strategic importance to the HEI/RPO and potentially of special commercial or technological interest to other parties. All collaborations in these areas should be monitored and careful management of intellectual assets, including protection measures, should be applied.
- Define criteria for the **reporting of plans** for a partnership to the FI Committee and determine who is accountable for following up on the reporting, e.g., starting up the due diligence procedure. The criteria for reporting a potential project may include its scope or character, e.g. teaching or research collaboration; specific fields of research, or the category of foreign partner (e.g. in a country with a different academic or political system).
- Define **the minimum levels** of **due diligence** for different types of partnerships - including donations by partners - and determine who is responsible for performing or outsourcing due diligence. The criteria for the level of due diligence may include the scope of the project, specific fields of research, specific partners in specific countries.
- **Define red lines for collaboration**
    - Identify when the institution's knowledge security, academic freedom, and reputation would be at risk and when a partnership/collaboration is crossing a red line.
    - Identify acceptable and unacceptable risks for collaboration, e.g. overseas education may be subject to restrictions that may not safeguard the institution's norms and values.
    - In addition to general criteria, a specific project may call for additional criteria or a specific weighing of benefits and risks. Who should be involved in this procedure?
- The FI Committee should establish a risk management subcommittee or working group responsible for:
    - Developing and overseeing risk mitigation procedures

- Assessing the risks
- Safeguarding the institution's values and crown jewels
- Keeping an overview of sensitive partnerships (because of the partner, research area or research topic)
- Reporting to senior executives
- Providing information and support to researchers with plans for a partnership: e.g. assess if (further) due diligence is called for and/or a potential project complies with legislation and/or ethical standards.

The working group ideally consist of scientists from multiple fields of study and officers from multiple departments, incl. security, international relations, legal and ICT departments

- **Gather and communicate information** about existing and potential partners (overseen by the **FI Committee**), best practices in mitigating risk, instances of breaches of knowledge security and academic integrity.
- Develop transparent principles and **procedures for an exit strategy.** If a partnership needs to be terminated before it expires, rules-based arrangements need to be in place, addressing issues such as security and interests of students and staff, IPR, and assets.
- **Ensure the availability of expertise:** hire or ensure access to expertise on risks, specific countries or partners, legal issues and on intercultural communication.
- Develop web pages **providing information** on knowledge security risks and how to mitigate them, including links to support offices and organisations and toolboxes.
- **Create a culture of trust** within the institutions in which staff feel free to raise concerns about a partnership or to discuss conflicting interests.
- **Promote the FI Committee** to whom problems can be reported by all involved in the partnership, including the partner institution's students and staff members working in the institution.
- **Be transparent** about procedures and requirements and communicate them to existing and potential partners, ensure they are aware of the institution's commitment to academic freedom and knowledge security.

4.3.2. Preparing for an agreement

The next step is to consider the potential collaboration project / partnership at a more detailed level. Staff and researchers involved in leading the potential project should:

- Ensure the partnership is based on a **strategic vision**
  - Identify, in advance, the main aim of the partnership, including its specific goals and the benefits for the institution its added value and that for the potential partner's institution.

- Consider short-term interests and benefits (e.g. financial means, talents) versus long-term risks (e.g. dependency, loss of knowledge position) and determine how the collaboration fits into the institution's long-term research and internationalisation strategies.

- Perform **due diligence**
  - Gather information enabling staff to assess potential risks with regard to security, values and reputation. Consider the ideological, political, and/or moral implications linked to the specific partnership. Depending on the partnership the information to be gathered may include:
  - Relevant laws and regulations in the partner's country, including rules on overall security, data sharing, research ethics, intellectual property protection, etc. Is the project subject to specific local legislation? If so, how does this affect the collaboration?
    - The potential partner's overall agenda and specific activities and interests, including (potential) commercial activities and interest.
    - Affiliations and relationships of the partner institution and of the researchers involved in the project, e.g. affiliations with military institutions, companies, involvement in dubious activities. Also use information in the language of the partner, because this often differs from the published English translations and involve language experts.
    - The relationship of the potential partner with government authorities; the degree of independence from the local government.
    - The potential partner's decision making structures and procedures.
    - The potential partner's track record on transnational collaboration and adherence to European norms and values. This should include research into past incidents of foreign interference involving the respective partner in other countries around the globe.
    - Its level of transparency; commitment to academic integrity, including procedures to ensure adherence to research ethics and academic freedom.
  - In addition the researchers involved should consider:
    - the potential use of research results for dual-use technology or for purposes that are not in line with EU or national policies aimed at strengthening economic, security, or social benefits.
    - Check if the project complies with the European dual-use Regulation 821/2021[53] and the annual amendments to the EU dual-use control list[54], the corresponding national export control legislation, Commission recommendations for compliance[55], Foreign Direct Investment screening Regulation[56] and other relevant regulations[57].
    - Check if the plan for the project needs to be reported or presented to the central level or

[53] Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast) (OJ L 206, 11.6.2021, p. 1).

[54] Delegated Acts containing the annually amended EU dual-use control list (latest 2020/1749);

[55] Commission Recommendation 2019/1318 on internal compliance programmes for dual-use trade controls under regulation 428/2009

[56] Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union

[57] EU Restrictive measures targeting certain third countries; need to check against the lists of sanctioned natural and legal persons, entities and bodies in certain third countries, see https://sanctionsmap.eu/#/main

specific committees(s) at the HEI/RPO's.
  - In case of collaboration in education: does the curriculum meet the requirements of the institution in terms of quality and academic integrity.

- Raise awareness of and gather knowledge about possible cultural differences that may hamper the negotiation of an agreement and or the collaboration, e.g. a preference to leave (potential) conflicts or difficulties undiscussed, and or to have a brief agreement, leaving details to be worked out at a later stage. This approach is to be avoided as undiscussed different assumptions and expectations may lead to serious problems. The involvement of experts in cross-cultural communication or negotiation should be considered.

4.3.3. Negotiating an agreement/contract

When an institution aims to establish a formal partnership, it is important to be transparent about, and communicate to the potential partner, about its commitment to all elements of academic integrity, including academic freedom. Agreements should be open to consultation across the HEI/RPO and to public scrutiny. The institution's standard clauses may provide a good basis but do not necessarily cover all necessary details with regard to specific projects. An agreement should address the essential elements below:

- Definitions of the parties involved.
- Overall goals and concrete results of the collaboration.
- Financial responsibilities and financial reporting:
  - Who will pay what costs?
  - In case of a grant both sides need to agree to the grant stipulations.
- Timeline of delivery of results; consider appointing of a liaison person on both sides.
- Reciprocity with regard to:
  - Transparency concerning project progress: agree on regular reporting and establish communication lines.
  - Access to and use of data gathered and produced within the project.
  - Access to and use of facilities, machines, instruments and infrastructure.
- Clauses about the protection and management of intellectual property (IP).
  - Defining background intellectual assets, whether or not they are protected by IP rights such as copyright, patents, trademarks, designs, database rights and geographical indications.
  - Defining intellectual property that will result from the partnership, whether or not it will be protected by IP rights.
  - Managing the background assets and results, including as regards their ownership and their use:
    - Criteria for (first) authorship of publications; these criteria differ across fields of study and academic traditions.

  - Confidentiality obligations;
  - Access and dissemination rights between the members of the partnership;
  - Licensing of results (and of background, where necessary) to third parties;

- Potential transfers of ownership of results (especially outside the EU).
- Data management. The EU has several legal instruments with regard to copy rights, but each country has its own copyright law and policy.
- Policy on Open Science, Open Access to scientific publications, data and research results including Open FAIR Data.
- Rights pertaining to the involvement of third parties.
- Respect of values and ethical standards; most countries or universities have their own Code of Conduct Code for Research Integrity, including academic freedom; in some cases – e.g. use of human subjects - specific research protocols need to be followed and/or special ethics committees need to be consulted.
- General provisions such as applicability of laws, liability and dispute settlement.
- Exit strategy: include a clause on the conditions – including breaches of academic integrity and procedures for early termination or withdrawal from the agreement.

4.3.4. Implementing the collaboration

After the conclusion of an agreement the implementation calls for continued attention. HEIs and RPOs should structurally monitor and review the collaboration project. They should ensure that:

- Partners comply with the agreement, including the financial commitments and regularly provide progress reports
- All parties involved report (potential) difficulties at an early stage and work together towards solving them
- The partnership will be dissolved when problems cannot be solved and pose a serious risk to the institution's security, values, and reputation.

4.4. FACILITATING THE DEVELOPMENT AND IMPLEMENTATION OF SUSTAINABLE PARTNERSHIPS: NATIONAL COLLABORATION, BEST PRACTICES AND TOOLBOXES

As discussed in this chapter mitigating the risks with regards to partnerships requires a multifaceted and information-based approach, commensurate to the perceived risks and benefits of the collaboration. It also requires the cooperation of multiple individuals at various levels, including leaders, policy officers, country specialists, communication officers, security officers, and multiple departments, including the legal department and ICT department, and most of all, the researchers and principal investigators involved in the (potential) project. Raising awareness about potential risks, communicating regulations and procedures

pertaining to partnerships, openly debating dilemma's and proportionality of regulations, and offering support to individual researchers of research groups will facilitate implementation of risk management strategies. It will be the role of the **FI Committee** to coordinate this work.

In recent years, an increasing group of European HEIs, RPOs, and governments have come to realize the need to step up the mitigation of risks involved in partnerships. Some have developed guidelines (see 4.4.1 below) or strengthened their existing risk management strategies. Others lack the knowledge and capacity to take up this comprehensive and challenging task or are concerned about the possible financial burden of implementing measures. Pooling resources may be part of the solution.

4.4.1. Pooling resources: exchange with peer institutions and government organisations

Pooling resources and knowledge with other HEIs and RPOs and government organizations through the **FI Committee** will be beneficial to all involved. This can be organized by national organizations of HEIs and/or may be encouraged and facilitated by government stakeholders. Institutions that lack the necessary capacity and knowledge can be supported and encouraged by peer institutions and government organizations. Collaboration and coordination with peers will not only give institutions access to knowledge, experiences, and best practices but may also contribute to overall support of staff and students for regulations. Sharing information about problematic partnerships and cases of breaches of academic integrity and knowledge security can be helpful in raising awareness and in fine-tuning risk management strategies. Furthermore, a shared commitment among institutions to design and respect regulations pertaining to partnerships will help create mutual trust and solidarity, which in its turn will facilitate implementation and compliance.

Institutions can request government organisations such as the Ministry of Education and Science, Ministry of Foreign Affairs to provide support and facilitate HEIs and RPOs in the development and implementation of risk management strategies. Government organisations may support institutions' efforts in raising awareness and managing risks by:

- Raising awareness at the national level of potential risks of educational and research partnerships.
- Establishing a central point to gather information and unlock knowledge and best practices as well as cases of breaches of knowledge security and academic integrity.
- Encouraging HEIs and RPOs to work together and pool their sources.
- Offer consultation sessions to discuss potentially sensitive collaboration.
- Offer support with regard to internal compliance with export control[58] and access to sensitive research regulations.

National approaches may also be supported by joint European monitoring of risks and the sharing of information and best practices.

In the context of international initiatives devoted to the wide and open sharing of data and other research

[58] Commission Recommendation 2019/1318 on internal compliance programmes for dual-use trade controls under regulation 428/2009

objects (e.g. EOSC and others), the issue of foreign interference gains relevance due to the wide international stakeholder community targeted. Candidate members should be screened prior to being admitted as full members in each of these bodies, and it should be ensured (and upheld) that only members nominated as mandated organisations by the Member State or Associated Countries act on behalf of the countries responsible for their mandate, and that mechanisms exist to take pertinent action when this is not the case.

4.4.2. Developing a positive agenda

Risks are inherent in partnerships, but it should be emphasized that most partnerships do not encounter serious problems, and, in many cases, potential risks can be mitigated. Stakeholders are therefore advised to also develop a positive agenda for the expansion of sustainable collaboration. The development of partnerships can be encouraged by identifying safe or low-risk areas for international collaboration and therefore do not need to be subject to intense scrutiny.

5. CYBERSECURITY

5.1. INTRODUCTION

The **aim of this chapter** is to take a risk-based approach to cybersecurity at HEIs and RPOs and offer possible measures to mitigate against the main vulnerabilities and threats for the three asset groups at HEIs and RPOs. §5.2 looks at the people including the students and staff at HEIs and RPOs. §5.3 addresses the physical and digital infrastructure at HEIs and RPOs. §5.4 deals with the IP stemming from research activities at HEIs and RPOs. It should be noted that the distinction between assets and threats is not always clear cut as some assets can become threats in which case an external threat can then turn into an insider threat. §5.5 offers possible measures to mitigate against the identified risks.

Cyberattacks are one of the most publicly recognisable examples of foreign interference and typically involve attempts by organisations, which may be state-owned or state-sponsored to gain access to and control of the digital infrastructure of the target organisation. Ransomware attacks form the majority of reported cyberattacks in HEIs and RPOs and are noticeable due to their particular modus operandi of advertising themselves in order to coerce the target to pay the requested ransom. This is different in the case of sabotage or espionage on HEIs and RPOs where the threat actor actively attempts to evade detection in order to achieve their objectives. Cyberattacks on HEIs and RPOs aim to exploit the vulnerabilities of the three most important **asset groups** at HEIs and RPOs:

- People visiting, studying, and working at the organisations
- Technical and support infrastructure at the organisations
- Intellectual Property (IP) from research at the organisations

Coordinated cyberattacks on HEIs and RPOs are often carried out by known **Advanced Persistent Threat (APT)** groups which are state-owned or state-sponsored. They are advanced in deploying a range of tactics and techniques to gain access to targeted digital infrastructure. They are persistent in conducting operations which may be stealthy or remain undetected for extended periods to achieve their objectives. They are a threat in having the capability and intent to exploit the vulnerabilities of their target. Some examples of APT groups known to have targeted HEIs and RPOs are in Table 5.1.

Table 5.1: Known APT Groups Targeting HEIs and RPOs

APT GROUP	ALSO KNOWN AS	FIRST SEEN	NOTES
APT10	MenuPass	2006	In 2016 and 2018, APT10 was found to target Japanese universities. From September through November 2016, APT10 targeted Japanese academics working in several areas of science, along with a Japanese pharmaceutical organisation and a US-based subsidiary of a Japanese manufacturing organisation.

APT28	Fancy Bear, Pawn Storm, Sofacy, Sednit, Tsar Team, Strontium	2004	This is one of the most well-staffed and skilled APT groups which is attributed to have delivered high profile campaigns (including the theft of sensitive information from the DNC and interfering with US elections). APT28's modus operandi has been observed to have attacked a wide range of industries and organisations (including universities but also private schools and a kindergarten in Germany)
SILENT LIBRARIAN	TA407, Cobalt Dickens, Mabna Institute	2018	Deploys phishing campaigns against universities to harvest university accounts. The group has a similar modus operandi and similar objectives as Sci-Hub. Members were indicted in the US accused of the following damages: around $3.4 billion worth of intellectual property loss due to unauthorised access; 31.5 terabytes of academic data and IP theft from compromised universities; 7998 university accounts compromised; 3768 US-based professor accounts compromised

5.2. PEOPLE

5.2.1. Researchers

Researchers play a **core role in education and research** that defines HEIs and RPOs, having a full understanding of both the research project lifecycle and their organisations, and as such fall into the core definition of an insider who can significantly undermine the security of their organisations. The on-boarding and off-boarding of contract researchers also poses a risk if the hiring organisation does not perform sufficient background checks or there is a lack of process for returning IP and equipment at the end of a contract. Researchers are further evaluated and assessed on the number of published articles and citations in scientific journals (the so-called 'publish or perish' mentality), their research income from competitive research grants, and invited lectures and conferences. This places enormous pressure on researchers who may as a result exhibit risky behaviour open to foreign interference.

Researchers are typically involved in attracting new research funding and contributing to core activities of their organisations as well as activities of awarded projects. **Attracting and retaining competent and talented researchers** takes time and effort. As such, a potential 'brain-drain' would be detrimental to an organisation's research capabilities. In a strict sense, scientific publications leak details of an organisation's personnel, their expertise, projects which they have been engaged with, and their collaboration network. Moreover, the average salary of a researcher in a HEI or RPO can be considerably lower than in the private sector, especially for specialisations in computer science.

The **pressure to publish and attract funding** as part of the requirements in the tenure track system may force (underperforming) researchers to behave in ways that can compromise the integrity of their research including: seeking collaborations with individuals or organisations without undertaking due diligence; submitting research to questionable or predatory publication venues; conducting partial or biased research; applying poor judgement in releasing and publishing data; underestimating risks related to foreign travel. In these cases, an academic is transformed from an asset to an insider threat. A lack of transparency (bolstered by poor organisational processes) in declaring conflicts of interest, for instance by researchers working on behalf of external bodies, also forms a breach of integrity.

A **lack of awareness and training on secure and safe operations** is another key vulnerability. Failure to perform security hardening of networked research equipment through negligence or ignorance increases an organisation's potential attack surface. Using web services or downloading software to bypass paywalls and gain access to scientific papers and other research content are risky actions as these can introduce malware to an organisation's infrastructure. This also applies to researchers who go abroad, to attend conferences or collaborate on research, where mobile phones and laptops can be scanned on entering the country and Wi-Fi networks can lack adequate security.

Researchers with ties to foreign actors may be subject to blackmail or other coercive actions or even willingly collaborate with foreign actors, elevating them to insider threats. A compromised researcher may, for example, exploit the absence of physical access controls and visit the lab outside of office hours to photograph spaces, layouts, and devices (including make and model, serial numbers, and other device ID details) resulting in a breach to a confidential lab configuration. An example of a researcher with ties to a foreign actor who gained access to sensitive data is a research assistant at the Medical College of Wisconsin who stole vials of a patented compound used in cancer research in 2013. The researcher copied 384 files to his personal laptop, enabling him to publish the cancer data and independently claim IP ownership as well as use the stolen files to apply for research funding.

There are lastly potential threats stemming from **loose off-boarding practices at HEIs and RPOs.** Researchers who go on a sabbatical or unpaid leave to a foreign organisation may keep their employee status and user credentials at their home organisation and have access to their home infrastructure and resources which can then be exploited by foreign actors. This similarly applies to researchers who leave an organisation but temporarily retain their credentials and access. Academics with a low profile and primarily a managerial track career, who thus may have a higher level of clearance, may be especially targeted for recruitment by foreign actors and coerced to perform in their new position by exfiltrating confidential information and research IP at their previous employer.

5.2.2. Students

Students **engage with researchers in the education and research process** and often collaborate in the creation of research IP. From a security perspective, students are in large numbers and have access to computing equipment and network, with many talented students being placed in the right environment to showcase their intellectual capabilities. Students involved in research initiatives and projects may gain higher access privileges to devices, networks, equipment, and resources than peers focusing on education, and in so doing pose an insider threat. Upon graduation, some students become more engaged in research via postgraduate studies (masters or PhD degrees) or seek careers as researchers in RPOs. A supply of good quality undergraduate students is critical to HEIs and RPOs.

5.2.3. Research support and administrative staff

Research support and administrative staff (such as project and technology transfer officers) may not necessarily participate in research output creation, but nevertheless have an **instrumental role in the support of research activities.** They typically participate in the grant preparation, assurance, compliance,

and (cost) management aspects of a research project. As such, they are situated in a department that accumulates a vast amount of research IP and have unrestricted access to systems and databases that are not normally accessible to the researchers. This includes access to research proposals, financial and legal information, researcher contracts, and other personal information (including salary details and historical data on travels for project meetings and conferences). Research support officers are thus a prime target for exfiltrating such information by foreign interference.

While research support and administrative staff generally perform tasks of a well-defined scope and follow mature processes for the administration of a research project, they may not have received a **sufficient level of awareness and training in cybersecurity.** Given that they potentially handle or have access to the whole portfolio of the organisation's research grants (both successful and unsuccessful), they are potentially a 'soft spot' and entry point to the organisation, offering a threat actor high returns during the early phases of an attack. The off-boarding of experienced and long-serving staff upon ending their employment with the organisation is also considerably challenging. User account deletions and removals do not guarantee that a departing employee does not have unauthorised copies of all research material they handled throughout the period of their employment.

5.2.4. Collaborations

Research thrives when people and organisations work together. HEIs and RPOs generally engage in **collaboration networks** with other academic organisations as well as organisations from the public and private sectors. These networks can collectively leverage different skills and expertise, which in turn fuels interdisciplinary research, giving an opportunity to produce an outcome that is greater than the sum of the parts. At the same time, the collaboration extends the boundaries of the underlying virtual organisation, effectively increasing the potential risks of cyberattacks on all asset groups.

Collaborators in a research project may be introduced at any stage in the project lifecycle, with an increased probability to join being during the proposal stages where the formation of the project consortium takes place. During this stage not all partners may have due diligence mechanisms in place to perform adequate background checks on potential partners. A threat actor may, for example, obtain intelligence on prospective partners (from a partner search tool[59]) to identify the most willing or likely targets (and possibly match them with organisations under their influence) before approaching them. The result is a breach in the confidentiality and trusted sharing environments of the consortium. The probability of success of a threat actor entering such a collaboration network increases if there is also pressure to develop and submit a quality proposal in a short period of time. The risks of foreign interference for HEIs and RPOs in partnerships involving foreign actors is further described in §4.

5.2.5. Disinformation and information manipulation

The intentional and coordinated manipulation of the information environment by foreign actors is especially challenging in the domain of HEIs and RPOs, who rely on factual information for their research. The tangible

[59] For example https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/how-to-participate/partner-search

impact foreign disinformation and information manipulation can have, especially in the field of science, has been highlighted during the COVID-19 pandemic when foreign actors attempted to manipulate public discourse and discredit scientific evidence pertaining to vaccines for their own benefit.

Additionally, authoritarian regimes aim to distort public discourse and suppress independent and critical voices who present information/research that contradicts their narratives and is critical of their repressive systems. Foreign disinformation and information manipulation therefore pose two challenges to HEIs and RPOs: i) manipulated information may be introduced into the research of students and researchers to strengthen a foreign actor's narrative, and ii) institutions, students and researchers may become the target of disinformation and information manipulation if they research/publish issues that are unfavourable for or critical of repressive and authoritarian regimes.

Social media in particular – due to the ease and speed with which information can reach large audiences – can be used by foreign actors to reach out, co-opt or harass researchers, influence organisations' decisions and directions and affect the performance and impact of research outputs. The consequences can be of varying magnitude, ranging from starting online petitions to the destruction of physical property. Social media can also be used by foreign actors to promote their own values which can run counter to HEIs and RPOs.

5.3. INFRASTRUCTURE

5.3.1. Libraries

Most HEIs and RPOs spend a **considerable budget on subscriptions** for online access to scientific journals and databases of conference proceedings. Subscriptions are implemented through two main options: location-based or user-based. With the location-based approach, the user has access to the publication repository as long as they access the paper from within the university campus network. User-based access requires the user to log in to the repository, normally through a federated sign-on solution. This form of access became popular during the COVID-19 lockdown where most campuses were not accessible and users were asked to work from home. Harvesting the credentials of university users gives a threat actor free access to non-open access papers but more significantly to personal and confidentially stored information. As such, libraries are a pivotal asset for targeted cyberattacks.

Libraries on limited **budgets for journal subscriptions** and not having processes to check the authenticity of subscription providers may introduce rogue agents who offer special or discounted deals on 'institutional' subscriptions. These agents then circulate the same usernames and passwords across multiple institutions for accessing the subscriptions. Moreover, limited subscriptions and access to research articles may incentivise research staff to seek illegal downloadable copies of articles. Sites advertising bypass of paywalls and free access to papers can mount watering hole attacks[60] against HEIs and RPOs. On the other side of the spectrum, libraries with an abundance of journal subscriptions make their users attractive targets as their log-on credentials are used to access these subscriptions through single sign-on or federated sign-on portals. In addition, as journal subscriptions can also be checked via the IP address (allowing seamless access for users working on campus without the need to authenticate), on-campus IT assets are key targets for cyberattacks.

[60] A watering hole attack is a security exploit in which an attacker guesses or observes which websites an organisation frequently uses and infects one or more of them with malware.

Paywall bypassing technologies providing free access to scientific articles that normally require individual purchasing or subscription rely on the continuous feed of valid access credentials or licensed IP addresses. Although the main goal of these services is to provide access to research papers, the modus operandi of the attack exposes the victim organisation as a whole, as the value of a compromised account exceeds that offered by a library subscription. A representative example is poor cybersecurity practices (such as a lack of URL scanning in email messages) allowing a threat actor to send phishing emails advertising free access to scientific papers in a reputable journal to users. Victims are then redirected to a fake user authentication panel (such as a fake Shibboleth single sign-on window) where their credentials are captured, resulting in complete access to research folders, personal data, personal communication, emails, shared folders, and journal subscriptions.

Sci-Hub is an **example of a paywall bypassing technology** that offers free access to over 70 million scientific papers. Sci-Hub manages to access the papers by obtaining account user credentials that have legitimate access through university subscriptions. An array of techniques is used to obtain the usernames and passwords, such as phishing, dictionary attacks, and system compromises. Although a large number of papers can be downloaded from a single user account, the staggering volume of the papers downloaded illegally suggests that the website maintains lists of compromised accounts. This inevitably leads to additional risks such as the leaking of personal data and confidential information[61].

5.3.2. IT Infrastructure

Technical infrastructure at HEIs and RPOs typically comprises **complex computing and networking systems** which are needed to support education, research, and business activities. In terms of network access, there is both wired and wireless access, and in some cases there may be unauthenticated guest access to the network for visitors. Access to core services (such as payroll, personnel, and IT management infrastructure) is typically the most restricted. However, some services may be outsourced, such as storage (using third party cloud services), web hosting for some sites and subdomains, and email (by delegating this to third party email providers). It is worth noting that the information concerning which services are outsourced is publicly available and can be discovered via Open Source Intelligence (OSINT). For instance, outsourced email capabilities are captured in the publicly available Domain Name System (DNS) records (primarily as TXT Sender Policy Framework (SPF) information). This increases the scope and blurs the boundaries of the infrastructure.

HEIs and RPOs are also expected to host a wide variety of **specialised computing and networking equipment** on different maturity levels ranging from early prototypes to commercial products. Therefore, cybersecurity certification of these products cannot be expected or enforced as this would impair the research itself. Moreover, the networking technologies and protocols themselves can also follow different maturity levels. For instance, the so-called 5G pioneer bands or the IoT narrow band were at experimental stages for a considerable amount of time. Any laboratories or devices offering such access could not offer adequate access control via these channels. All laboratories, if attached to the rest of the organisational infrastructure, in principle increase the overall risk and exposure.

IT systems required for performing core business functions of the organisation are secondary assets which indirectly support education and research activities. These systems include: personnel and

[61] https://www.bbc.co.uk/news/amp/education-56462390

finance systems and databases; student registry and user account management; directory services; general purpose and teaching labs; e-learning services; network management and access; physical asset management (including timetabling); collaboration software and environments; distributed and shared storage spaces; call centre infrastructure. A further complication is the explosion in the number of personal devices as well as the use of additional software due to increased teleworking as a result of the COVID-19 pandemic.

The aggregation of systems and accounts through shared third-party platforms and single sign-on mechanisms, in conjunction with the increased teleworking due to the pandemic, has resulted in a **blurring or even crossing of the boundaries between personal and private activities.** A good example is Microsoft SharePoint and Teams which has been adopted by many primary and secondary schools in the sudden shift to e-learning platforms. If members of the same household share the same device to access these applications, there is naturally an increased risk of leaks and attacks. Moreover, the inability for HEIs and RPOs to manage and update the software of the home computer of students and staff exacerbates the situation. With regards to Teams, it was possible for an attacker to perform an account takeover simply by sending a malicious GIF image through the application[62].

HEI and RPO network and computing infrastructures have a **tendency to inflate and expand** to keep ahead of the game and meet the ever-increasing needs of the users. The users themselves, in fact, may also have personal state-of-the-art devices which they use to access the network. With new nodes being introduced regularly, it is obvious that a campus computing and network infrastructure experiences a related increasing amount of entropy. For example, the lack of processes for updating all devices, withdrawing and sanitising outdated devices, and securely introducing and managing new devices increases the attack surface at scale and therefore the risks to foreign interference.

Ransomware is one of the most frequent types of attacks on HEIs and RPOs. The motives of a threat actor leveraging a ransomware attack are typically financial and can manifest in two main forms having a different impact in each case: attacks on availability and integrity where the ransomware encrypts all files making the research inaccessible to legitimate owners and users; attacks on confidentiality where the attackers exfiltrate the data and threaten to publish the data online or sell to other bidders. Moreover, in the case of a targeted ransomware attack (rather than a generic 'scatter gun' type of attack with a fixed ransom price), the value of the encrypted or stolen research as well as the value of the HEI or RPO may also be factored in). This can result in staggering ransom amounts such as the attack against the University of California which paid $1.14 million dollars to hackers[63].

5.3.3. Research laboratories

Research laboratories are primary assets and essential enablers to conduct applied research. A laboratory's value is not only expressed by the hardware it contains (which in fact is a depreciative asset) but also the knowledge of setting up the laboratory and configuring the equipment (including the layout of a room in some cases and the exact make and model of the devices). Such knowledge can have a substantial value as it could be a product of a long-term and systematic research activity. Research laboratories may also include dedicated and specially trained technical personnel.

[62] https://www.cyberark.com/resources/threat-research-blog/beware-of-the-gif-account-takeover-vulnerability-in-microsoft-teams
[63] https://www.bbc.co.uk/news/technology-53214783

State-of-the-art **research equipment** in a laboratory may not have incorporated security-by-design or security-by-default principles. This is evidenced by many publicly available reports on IoT vulnerabilities and security incidents concerning IoT devices and specialised equipment. Research equipment may also not have been through extensive quality testing or may not meet acceptable criteria to produce reliable data in a discipline. This can be particularly applicable to low-cost equipment such as the low-cost measurement devices used for capturing environmental data.

The **operators of the research equipment** may need increased privileges to use the devices and this extends to computer systems within the laboratory's network. Having administrative rights in these laboratories increases the risks considerably, especially if the operator's expertise is not in computer science. Absence of physical controls such as key card access and proactively prohibiting foreign devices (such as portable disks and USB drives) increases the risk of a leak of research IP (including laboratory configuration and profile) and enabling a foreign actor to develop a shadow laboratory.

5.4. INTELLECTUAL PROPERTY (IP)

5.4.1. Research data, methods, algorithms and IP

IP creation is a continuous process that happens across the entire research project lifecycle and often involves inter-institutional, intersectoral, and international collaboration. Research IP covers all information and knowledge that is produced either as research output or from preparatory and supporting activities. Research IP typically encompasses data (such as data sets produced by or fed into research activities), methods (which are techniques and approaches invented to achieve an outcome), and algorithms (which are particular cases of a method implemented using a computer system). Methods differ from algorithms in that disclosure of a particular method may not necessarily provide an advantage, especially if this requires a substantial and specialised infrastructure (such as developing nanotechnology solutions). In the case of software, such barriers are unlikely to exist and algorithms may be instantly actionable and exploitable (as some cases with Artificial Intelligence show). Guaranteeing **confidentiality of research IP** may not always be feasible or may even be in conflict with the purpose and goals of particular policies or national legislation. For example, environmental data sets need to include location information as a minimum requirement for the data to be of use and added value.

Unsurprisingly, the **different research disciplines** have their own practices and requirements as well as barriers to undertake research in a particular area. Individuals may voluntarily share data, designs, software, and firmware[64] or may be required to do so by the relevant law (for example the exceptions and limitations in the Union's copyright acquis which are permitted under international IP agreements and Horizon Europe Regulation on open access). Some may even allow remote access to testbeds and sensors which produce data in real time. The different disciplines also carry varying levels of systematic risk. Sabotaging medical research, for example, may have direct and severe consequences to human life. Despite the subtle or obvious differences of the various disciplines, a common denominator for all of the sciences is that the overwhelming volume of research is captured and processed in a digital form. As such, cybersecurity is a concern across all disciplines when it comes to protecting research IP.

[64] https://www.frontiersin.org/articles/10.3389/feart.2019.00221/full

A researcher producing IP may not realise or appreciate the **value and implications of research IP** and as such may make an ill-advised or ill thought out decision on publishing (or not publishing) their IP. This may be due to a lack of foresight or that, for instance, the data may contain considerably more information than what initially envisaged. In fact, information-rich data sets are expected to have unmined information hidden and the purpose of publishing is to exploit these data sets to their fullest extent. Creating good quality data sets is a challenging process by itself, so research communities strive to support and contribute in such efforts which can run counter to principles of good data governance.

The **risk of a vendor lock-in** is high for HEIs and RPOs as the research and innovation process typically involves adopting unproven and experimental technologies that are low on the technology readiness scale. The introduction of specialised technology by a foreign vendor into the supply chain can make it extremely challenging or expensive for HEIs and RPOs to continue with or break free from the lock-in. A representative example of such a lock-in is the insertion of backdoors into critical infrastructure as raised in the risk assessment of 5G networks by the NIS Cooperation Group[65].

5.4.2. Reputation

Reputation is an intangible asset of utmost importance for HEIs and RPOs and is dependent on the **overall brand of the organisation.** Academic institutions are particularly proud to promote high-quality tuition and leading cutting-edge research as well as their international ranking. Integrity in research entails credibility and correctness of the intellectual output as well as attribution of the individual or team that has produced the underlying IP. Reputation can be affected by any practices undermining ethical and integrity standards. Errors in the research data produced by a genuine error, intentional falsification, or through external interference are representative actions that have varying impacts on reputation. Other incidents involve collaboration and engagement with parties who do not subscribe to research and academic integrity standards. A measure of integrity compliance is the retraction of published papers. RetractionWatch[66] is an initiative that collates information of retracted papers with reasons for retraction in a searchable database[67]. For example, a noteworthy spike in the number of retractions was observed between 2009 and 2011 in the context of IEEE conferences[68].

Reputation is collectively affected by vulnerabilities of the individual assets that, as a collection, make up the organisation. Two main risks for the reputation of HEIs and RPOs are the **falsification of data and artificial inflation of citation metrics** by researchers. Falsification of data attacks the integrity of data and by extension the research, researchers, and reputation of the organisation as whole. For metrics, Google Scholar maintains the number of citations, h-index, and i10-index metrics, which are calculated from publication databases and website sources. As Google Scholar allows a user to manually update and intervene with records, it is easy for an author to create false records by adding papers that they have not authored or cause citations of a paper to be counted multiple times by uploading the same paper to many databases. The citation metrics in Scopus are more reliable as they only index papers from a select number of sources and authors cannot easily modify the records.

[65] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132
[66] https://retractionwatch.com
[67] http://retractiondatabase.org/RetractionSearch.aspx
[68] https://www.sciencemag.org/news/2018/10/what-massive-database-retracted-papers-reveals-about-science-publishing-s-death-penalty

5.5. POSSIBLE MEASURES

Raise awareness of cybersecurity risks from foreign interference:

- Develop training and organise seminars on all available and implemented data protection technologies including confidential computing[69].
- Educate and train researchers, students, and administrative and support staff in cyber hygiene and to identify the risks and know how to avoid or deal with cyberattacks.
- Develop and communicate easy-to-follow escalation processes in case of suspected cyberattacks and advertise a single point of contact for triaging the reported incidents.
- Maintain and communicate a Top 10 cybersecurity risk list for the organisation ensuring that all users understand the different types of ransomware and cybersecurity defence practices.
- Publish regular newsletters with best practices describing real cybersecurity incidents affecting the community including narratives with suggestions of behaviour and actions.

Detect and prevent cybersecurity attacks from foreign interference actors:

- Set up and perform OSINT investigations on a regular basis to detect leaks of user credentials for accessing networks and systems, confidential data, and research IP of the organisation.
- Create alert capabilities to flag outlier behaviour by monitoring activities, budgets, and assets including frequent travel abroad, unexpected high funding from non-competitive bids, personnel count not proportional to expected efforts, and co-author lists in publications.
- Develop screening procedures for researchers and administrative and support staff as part of the on-boarding process and for newly introduced individuals and organisations in collaborations as well as adopt security clearance processes for medium to high-risk projects.
- Conduct a risk assessment for researchers on sabbaticals or career breaks by considering their positions, visiting organisations, and need to maintain access at their home organisations.
- Procure cybersecurity-certified equipment and invest in developing confidentiality protection solutions for datasets including confidential computing.
- Implement physical access controls appropriate to the level required by research conducted in a laboratory and where required prohibit the use of unauthorised electronic devices.
- Clearly cluster end-user laptops and desktops on the basis of their purpose (office/corporate activities and research activities).
- Develop for the office/corporate activity cluster a centralised management approach for operating systems and installed applications and disable and remove local administration rights (LAR).
- Develop a separate IT environment to host laptops and desktops falling in the “research activity

[69] https://confidentialcomputing.io

cluster", to separate them from the normal corporate environment, and adopts, where possible a centralised management approach for operating systems. Any deviation from the centralised management approach is assessed in order to define compensatory measure to mitigate additional risks induced by this deviation (e.g. segregated network and dedicated IT infrastructure).

- Enable two-factor authentication (2FA) to access critical services and repositories and maintain and enforce blocklists to prohibit access to known malicious or infringing websites.

Respond to and recover from cybersecurity attacks from foreign interferers:

- Develop situational awareness capabilities of HEI and RPO communities by sharing lessons learnt and updating shared blacklists, reputation systems, and databases including external stakeholders such as publishing companies in the case of a plagiarised scientific article.
- Develop a plan for incident handling which includes clear processes involving both affected parties and those required to handle the response and adopt practices and elements from incident handling models such as the SIM3 Security Incident Management Maturity Model[70].
- Develop a plan for information sharing with external parties during the handling of an incident taking into account for HEIs and RPOs which are maintaining a CSIRT/CERT that there may be Memoranda of Understanding or information sharing agreements in place.
- Implement forensic readiness capabilities to reduce the time to respond when a breach is detected by allowing the incident handler to effectively navigate through the incident data, correlate the events, and make an informed judgement on the severity of the incident.
- Follow disciplinary action for offending staff and in doing so include evidence from the digital investigation in a form that is understandable and accessible by all parties involved in the disciplinary procedure possibly using a template to help structure and present the findings.
- Consider involving relevant law enforcement agencies, Intellectual Property offices, and data protection authorities for incidents that are likely to involve litigation.

[70] https://opencsirt.org/wp-content/uploads/2019/12/SIM3-mkXVIIIc.pdf

Getting in touch with the EU

IN PERSON

All over the European Union there are hundreds of Europe Direct information centres.
You can find the address of the centre nearest you at:
https://europa.eu/european-union/contact_en

ON THE PHONE OR BY EMAIL

Europe Direct is a service that answers your questions about the European Union.
You can contact this service:

– by freephone: **00 800 6 7 8 9 10 11** (certain operators may charge for these calls),

– at the following standard number: **+32 22999696**, or

– by email via: **https://europa.eu/european-union/contact_en**

Finding information about the EU

ONLINE

Information about the European Union in all the official languages of the EU is available on the Europa website at: **https://europa.eu/european-union/index_en**

EU PUBLICATIONS

You can download or order free and priced EU publications from:
https://op.europa.eu/en/publications. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see **https://europa.eu/european-union/contact_en**).

EU LAW AND RELATED DOCUMENTS

For access to legal information from the EU, including all EU law since 1952 in all the official language versions, go to EUR-Lex at: **http://eur-lex.europa.eu**

OPEN DATA FROM THE EU

The EU Open Data Portal (**http://data.europa.eu/euodp/en**) provides access to datasets from the EU. Data can be downloaded and reused for free, for both commercial and non-commercial purposes.

This publication presents the Staff Working Document on tackling R&I foreign interference. Foreign interference occurs when activities are carried out by, or on behalf of, a foreign state-level actor, which are coercive, covert, deceptive, or corrupting and are contrary to the sovereignty, values, and interests of the European Union (EU). EU Higher Education Institutions (HEIs) and Research Performing Organisations (RPOs) can benefit from a comprehensive strategy for tackling foreign interference that covers key areas of attention grouped into the following four categories: values, governance, partnerships and cybersecurity. The document contains a non-exhaustive list of possible mitigation measures that can help HEIs and RPOs to develop a comprehensive strategy, tailored to their needs.

Publications Office
of the European Union