CESAER

The strong and united voice of universities of science and technology in Europe

Keeping science open?

Current challenges in the day-to-day reality of universities

White paper

18 October 2023

Authors and contributors

The white paper was prepared by the following authors:

- Irna van der Molen, University of Twente, Netherlands;
- Dana Gheorghe, University Politehnica of Bucharest, Romania;
- Christina Daouti, University of Surrey (now at University College London);
- Vincent Eechaudt, University of Ghent, Belgium

Support from the CESAER Secretariat was provided by Mattias Björnmalm (Secretary General) and Justine Moynat (IT & Communication Officer).

The CESAER Task Force Openness of Science & Technology 2022-2023 was instrumental in providing feedback for this paper. The authors thank all members of the task force for their valuable input.

The authors extend a special thank you to the valuable feedback received from:

- Sabine van Gastel, TNO, the Netherlands
- Fredrik Karlsson, KTH Royal Institute of Technology, Sweden
- Klaas Kroes, Delft University of Technology
- Karel Luyben, President of EOSC Association, President 2014-2017 of CESAER and Rector Magnificus Emeritus of TU Delft
- Edward Ricketts, CESAER Secretariat (currently European Commission)
- Gülsün Sağlamer, President of European Women Rectors Association and former Rector of Istanbul Technical University
- Ernst Schmachtenberg, Vice President 2014-2017 of CESAER and former Rector of RWTH Aachen University
- Vilhelm Verendel, Chalmers University of Technology, Sweden
- Peter Weijland, Delft University of Technology

Contact

For any questions or enquiries, please contact the Secretariat via the details provided on https://www.cesaer.org/contact/

Please reference this document using http://doi.org/10.5281/zenodo.8355324

Rooted in advanced engineering education and research, CESAER is an international association of leading specialised and comprehensive universities with a strong science and technology profile that advocate, learn from each other and inspire debates. Our Members champion excellence in higher education, training, research and innovation, contribute to knowledge societies for a sustainable future and deliver significant scientific, economic, social and societal impact.

Contents

Glossary

Selected key concepts used in this white paper are briefly defined below in alphabetical order. Given the scope of this white paper, the authors have chosen to stay close to the definitions used by the EU institutions, or those provided by relevant European networks.

Academic freedom is defined at the individual level, as "the freedom of academic staff and students to engage in research, teaching, learning and communication in and with society without interference nor fear of reprisal." (European Commission, 2022, p. 7)[1]

Dual-use items are "items, including software and technology, which can be used for both civil and military purposes, and includes items which can be used for the design, development, production or use of nuclear, chemical or biological weapons or their means of delivery, including all items which can be used for both non-explosive uses and assisting in any way in the manufacture of nuclear weapons or other nuclear explosive devices." (EU Regulation 2021/821, art. 2(1))

Economic security encompasses "certain economic flows and activities [that] can present a risk to our security" (European Commission, JOIN(2023) 20 final, p.1). This includes, in particular, "risks related to: (1) resilience of supply chains; (2) physical and cybersecurity of critical infrastructure; (3) technology security and technology leakage; and (4) weaponization of economic dependencies or economic coercion" (European Commission, JOIN(2023) 20 final, p.4). For the purpose of this paper, it is important to note that the European Commission states that "these risks can occur along the entire value chain, from knowledge creation and basic research to commercialisation and manufacturing at scale" (European Commission, JOIN(2023) 20 final, p.4).

Export control is one of the ways to control the trans-boundary transfer of technology, and prevent the misuse of research. "Export control regimes [are] multilateral arrangements seeking to prevent the proliferation of nuclear, biological and chemical weapons and their means of delivery, as well as to prevent the destabilising accumulation of conventional arms and dual-use items, e.g. by establishing lists of items which should be under control." (Commission Recommendation (EU) 2021/1700 of 15 September 2021, glossary).

FAIR data refers to a set of principles that aim to make research data Findable, Accessible, Interoperable and Reusable. A key reference for the FAIR principles is Go-FAIR. The FAIR data principles are supported by EU policy (Horizon Europe Annotated Model Grant Agreement dated 1 April 2023) and practical recommendations.

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)." (European Commission, 2022, Tackling foreign R&I interference. Staff Working document, p. 7).

[1] Annex I of the Rome Communiqué of the Ministers responsible for higher education (2020) contains a 2-page "Statement on Academic Freedom".

Freedom of scientific research[2] is connected to the broader concept of *academic freedom* which in turn is defined in the Lima Declaration (1988, page 2) and the *Magna Charta Universitatum* (1988 and 2020, first principle) which refers to research and teaching being "intellectually and morally independent of all political influence and economic interests".

Complementing the Lima Declaration, *Institutional or university autonomy* can be further elaborated as "the right of the university to determine its organisation and administrative structures, to decide on priorities, manage its budget, hire personnel and admit students, decide on the content and form of its teaching and research" (Matei and Iwinska, in: Curaj, Deca and Pricopie, 2018, p. 349)[3].

International sanctions are "restrictive measures that target states, or entities and individuals" in order to maintain or restore international security. These are seen as "an essential tool through which the EU can intervene where necessary to prevent conflict or respond to emerging or current crises" (European Commission, 2023).

Knowledge security is not a concept clearly defined by the European Commission who refer, instead, to 'foreign interference' (see above) and the 'potential misuse of research' (see below). Given the absence of a clear definition by the Commission, we will use the following definition in this paper: "knowledge security is first and foremost about preventing the unwanted transfer of (sensitive) knowledge and technology, which could negatively impact the national security of a country and damage the capacity for innovation. It also concerns the covert influence of state actors on higher education and science, which can lead, among other things, to forms of (self-) censorship that are detrimental to academic freedom. Finally, knowledge security involves ethical issues that may be related to collaboration with individuals and institutions from countries where fundamental rights are not respected." (National Knowledge Security Guidelines, 2022, p.4).

Open access (OA) "refers to the practice of providing online access to scientific information that is free of charge to the user and is reusable". (European Commission, DG Research and Innovation, accessed on 6 September 2023).

Open science is the umbrella concept for all subcategories mentioned later on in this report. Open science has been defined by the European Commission in 2016 as "a process based on cooperation and the diffusion of knowledge by using digital technologies and new collaborative tools" (European Commission, 2016, p. 33). Three years later, in a factsheet on open science, the Commission defined open science not anymore as a 'process', but as "a system change allowing for better science through open and collaborative ways of producing and sharing knowledge and data, as early as possible in the research process, and for

[2] The Ministerial Conference on the European Research Area on 20 October 2020 in Bonn states: "The freedom of scientific research is a universal right and public good. It is a core principle of the European Union and as such anchored in the Charter of Fundamental Rights of the EU" (Bonn Declaration on Freedom of Scientific Research, 2020, p.2).

[3] Curaj, A., Deca, L. and Pricopie, R. (eds.). 2018. European Higher Education Area: The Impact of Past and Future Policies. Springer Open.

communicating and sharing results" (European Commission, 2019, p.1).[4] In this paper, we use the second definition, which encompasses a range of practices (e.g., research data sharing, open source software etc) mentioned later in this report.

Openness-of-science refers, in this paper, to the open culture and accessibility of science and technology to other sectors, stakeholders, or nationalities. It includes all '*open-for-science'* practices, seeking to minimise barriers to (inter)national academic and scientific cooperation, it includes open innovation, with 'users in the spotlight' and 'creating a well-functioning ecosystem' (EU, 2016, p. 13), stakeholder participation, citizen science, as well as the welcoming of students and staff from other countries and nationalities.

Securitisation (Ch. 4.3) refers, in this paper, to "the reframing of regular policy issues, such as climate change, migration, and emerging technologies, into matters of 'security'"(OECD, 2023).[5]

The '*potential misuse of research*' refers, in this paper, to research involving materials, technologies and information that have "the potential to harm humans, animals or the environment and may have substantial negative impacts on the security of individuals, groups or states" (European Commission, 2021, p. 1).

[4] UNESCO is more elaborate about the ways of doing this, when it refers to making "multilingual scientific knowledge openly available, accessible and reusable for everyone, to increase scientific collaborations and sharing of information for the benefits of science and society, and to open the processes of scientific knowledge creation, evaluation and communication to societal actors beyond the traditional scientific community" (Unesco, 2021, p. 7).

[5] According to the securitisation theory in international relations, once an issue is presented in the political domain as an existential threat (when it is 'securitised'), then "actions are justified outside the normal bounds of the political domain" (Security: A New Framework for Analysis, Buzan, Ole Waever, De Wilde, 1998, p.23-24).

Preface

'Open innovation, open science and open to the world' were three main policy goals for research and innovation of the European Union (EU) introduced in 2015. The collaborative, international and open nature of science and innovation was presented as instrumental for the development of new ideas and as sustainable investments in the future of Europe (European Commission, 2015). Since then, this notion of 'triple-openness' has come under increasing pressure, including from considerations introduced by the COVID-19 pandemic, the Russian invasion of Ukraine, increasing geopolitical tensions notably between China and the US, also in relation to Taiwan. In response to these global challenges, the EU has moved from triple-openness towards instead embracing 'balanced openness' through the approach 'as open as possible, as closed as necessary'. In recent years this has evolved in 'as open as possible, as restricted as necessary' or 'open if possible, restricted if necessary' and variations thereof. We use this terminology[6] to avoid unnecessary dichotomy.

What this 'openness' exactly means is still not always defined nor clear, notably in relation to who should or has the authority to decide on the balance or co-existence of 'open' and 'restricted'. In the day-to-day reality of universities, 'open' and 'restricted' often go together. Therefore, research and innovation actors, including universities, are often confronted with the interpretation, operationalisation and implementation of this balance into their day-to-day operations. This is particularly challenging for universities as they have unique societal roles and responsibilities, and depend of deep societal and international engagement to be able to fulfil their roles and responsibilities.

Universities of science & technology (S&T) are at the tip of the spear in this area as they engage at the forefront of the scientific and technological developments (e.g. for key enabling technologies or emerging technologies such as AI and quantum) which are often the focus of (geopolitical) tensions. Universities of S&T are therefore navigating an evolving landscape attempting to, at the same time, judiciously fulfil considerations related to open science, academic freedom, principles of non-discrimination, research integrity and knowledge security. Some principles go together and reinforce each other in day-to-day practice, while others are in real or perceived conflict and generate discussion.

The objective of this paper is threefold:

1. provide more background to the discourse 'as open as possible and as restricted as necessary';
2. explore what it means for day-to-day operations at universities of S&T to be 'as open as possible and as restricted as necessary'; and
3. provide recommendations to keep science open in this rapidly evolving context.

[6] However, when another paper, document or presentation to which we refer uses the phrase: 'as open as possible, as closed as necessary', this will not be changed.

In line with these objectives, this paper specifically addresses the following questions:

1. How should the discourse on ‘as open as possible and as restricted as necessary’ be understood in the context of current geopolitical developments?
2. What does it mean for day-to-day operations at universities to be as open as possible and as restricted as necessary?
3. What measures are necessary to keep science open in the current geopolitical context?

This paper is an exploratory paper intended to enrich the discourse, and reveal some of the related day-to-day practices at universities particularly related to open science and knowledge security measures.

Chapter 1 highlights the urgency of the topic. Chapter 2 outlines some geopolitical developments that have resulted in a stronger call for protective measures in science and technology. Chapter 3 elaborates the connections to open science, and shows how the two go together in different shades and manifestations of openness and closedness, rather than being two extremes on either side of a continuum. Chapter 4 explores what the measures for knowledge security mean in the day-to-day reality of universities of S&T, and chapter 5 provides conclusions and recommendations.

This paper is, first and foremost, written to inform and provide guidance to executive and leadership levels at universities of S&T, such as members of executive boards, rectors, deans, vice-deans for research, members of faculty boards, scientific directors, business directors, and directors in charge of internationalisation policy at universities. Furthermore, and equally important, the paper intends to inform policy advisors at relevant authorities, ministries and institutions, from regional through national to the European level.

With this paper, we encourage and provide guidance to the ongoing debate on (protective) measures that are needed to safeguard and advance knowledge societies and the values that underpin them, by keeping science open.

Executive Summary

Through scientific research, universities have been catalysts for social, technological and economic progress. This would not have been possible if universities did not engage in international collaboration, and promoting research with top level research organisations worldwide. Nevertheless, the strong international embedding and openness to the world have also left universities more vulnerable to unwanted foreign interference, unwanted knowledge transfer of technology that falls under export controls, or the misuse of research results for internal repression and human rights violations.

The openness can also come with risks that might be harmful to Europe's economic security, for instance risks to the resilience of supply chains, or risks to the cybersecurity of critical infrastructure. As these threats have become more visible, the narrative has shifted from open science and 'open-for-science' to 'as open as possible, as closed as necessary' and to 'as open as possible, as restricted as necessary'. While the narrative is clear, the practical impact of this policy change remains unsure.

This paper presents the results from an early survey conducted on universities' policy on foreign interference, knowledge security and the impact of government and university restrictions on international collaborations. The survey shows differences between countries and universities. While there is a common EU narrative (EU's global approach to cooperation in Research & Innovation), authorities and universities are at various stages of implementation. Sanctions, dual-use controls in academia and other measures taken by governments and universities seem to have impacted some practices more than others:

- Open access publications, open data and FAIR data are, at present, only in a minor way affected by export control and other knowledge security measures. Other aspects - such as IP and trade secrets, research integrity, data sovereignty, benefit sharing, or administrative burden - play a more prominent role for open and FAIR data.
- Knowledge security measures have differentially impacted universities, in terms of human resources, choice of partnerships, external funding and on some of the operational processes in the universities.
- The admittance of PhDs and staff is gradually affected through screening, visa-vetting procedures and debates about PhDs coming in with state-scholarships. Universities in certain countries have introduced stricter criteria for incoming PhD students and researchers. An EU approach is required to avoid inequalities amongst member states.
- Dual-use controls do not yet lead to a major impact on the number of publications on dual-use technologies or teaching by academic staff. Publications and presentations rarely meet the control thresholds in their entirety but it reflects a significant future barrier for (open) scientific processes.

While universities of science and technology (S&T) increasingly have policies in place for knowledge security and export control, universities can only do this based on the information available to them and within the boundaries of the legal frameworks in place. Therefore,

authorities have a clear role to play by creating the pre-conditions for effective implementation, providing the frameworks, regulations and ensuring necessary resources.

The EU can play a role through further discussion with representatives from universities and scientific networks on all areas of concern: the changing geopolitical landscape, the effects of the global approach, the freedom of scientific research, the applicability of their export regime on scientific publications and presentations.

Openness, transparency, security, academic freedom and research integrity are crucial elements for responsible internationalisation of universities. Universities are most familiar with their research, partnerships, student admittance, and HR processes, and are best placed to assess the sensitivity and risk of misuse of the research, of partnerships or to address vulnerabilities in their HR policy. Apart from additional measures for knowledge security, universities can also embed knowledge security through existing policies, instruments and tools in order to keep science open, transparent and secure.

Last, but not least, in the light of increasing securitisation, all stakeholders (EU, national authorities and universities) should take mitigating measures to make sure that scientists are not and will not be at risk.

Chapter 1. Urgency and objective

Universities and research organisations have long been encouraged to intensify their institutional cooperation with international partners globally, and to develop policies for open science with the guiding principle of 'as open as possible and as closed as necessary'[7] (e.g., H2020 Programme Guidelines on FAIR Data Management in Horizon 2020). Recently the discourse has changed from an emphasis on the first half of the sentence, towards increasing attention on the latter half. This white paper gives more background to this discourse, reveals what it means for the day-to-day operations at universities, and provides recommendations to keep science as open as possible in the changing geopolitical context.

International research cooperation, characterised by the free exchange of ideas, is a catalyst for high quality research and helps to resolve pressing global issues on sustainability, public health, energy transition, climate change, and migration, amongst many others. Moreover, many research topics are by definition cross-border and therefore depend on cooperation across disciplines and national borders. As such, the strong international embedding of researchers in international consortia and the inter-relations between universities, industry and broader society across continents and cultures has been key for progress in research and innovation (see also 'In pursuit of knowledge', Van de Walle, 2023). Moreover, many scientists find that international cooperation enriches their (professional) life by creating cultural awareness and providing a source of inspiration for future scientific projects.

In addition to the benefits of international scientific cooperation at individual and institutional level, such cooperation may also serve geopolitical, societal, economic objectives (Clingendael, 2021). International scientific cooperation is a common feature of large-scale scientific infrastructures[8] at the European or global level. Science and technology also play an important role in connecting through science diplomacy in various ways: (a) science and technology can support diplomatic efforts and can then be seen as a form of soft diplomacy; (b) diplomacy can facilitate international scientific cooperation such as in support of negotiations on large scale research infrastructures, and/or (c) science can inform and support decision-making processes, and can sometimes contribute to the process of negotiations in conflict resolution[9].

Notwithstanding the multitude of benefits, international scientific cooperation also brings risks of foreign interference. This ranges from legitimate cooperation to acquire knowledge and develop materials and technology (as identified within a country's long-term geopolitical and economic agenda), to less legitimate and illegitimate forms such as monitoring the student diaspora, espionage, cyberattacks on academic IT infrastructure or the misuse of collaborative research results. A recent report from the UK Higher Education Policy Institute (Brown, 2022, HEPI report 147) shows various examples of foreign interference from the

[7] When the original paper, document or presentation uses the phrase: 'as open as possible, as closed as necessary', such as in this case, then 'closed' is not changed to 'restricted'. See preface.

[8] e.g., European Strategy Forum for Research Infrastructures, Global Reporting Initiative, or the European Open Science Cloud

[9] For more information on science diplomacy in the European context, see science diplomacy.

UK, Australia, and the US, ranging from stealth attacks, collecting intelligence on COVID-19 vaccine development, IP theft, infiltration in management of specific institutes at universities, to recruitment programs on campuses run by the Chinese government. Investigative journalists in various European countries[10] published a series of articles under the heading 'China Science Investigation', mapping ties between European universities with Chinese universities known for their close ties with the Chinese military. These examples show how complicated it is to extend the limits of open science throughout the world taking into account of the high risk of international interference.

In its 'Tackling R&I foreign interference' document[11] the European Commission identified different tactics of foreign interference: political pressure, financial support, exploiting people, digital intrusions, and information manipulation (EC, 2022, p. 16-17). The document includes several recommendations for universities to counter the risk of foreign interference. Another guiding document (not legally binding) for universities is Recommendation (EU) 2021/1700[12], related to unwanted transfer of technology through export control. This recommendation, intended to support universities and research organisations to establish internal compliance programs, provides common research scenarios that may trigger export controls, including teaching, consulting, collaborating, organising (virtual) conferences/meetings/seminars, publication, and exporting tangible dual-use items (EU, 2021/1700, appendix 2).

The combination of these measures (to counter foreign interference, international sanctions, export controls), inevitably entail restrictions on international collaboration, student and staff mobility, open science and openness of science and technology. Some R&D hubs, innovation hubs and Research & Technology Organisations (RTOs)[13] have reviewed and tightened their cooperation procedures and partnership strategies. Universities of S&T are following at a rapid pace, doing their own risk assessments, and learning from each other in their own contexts (D'hooghe and Lammertink, 2022, AWTI, 2022).

A mix of regulation and self-regulation has been initiated, leading to a variety of legally binding measures, policy measures, and self-regulation. As indicated by the Advisory Council for Science, Technology and Innovation (AWTI) in the Netherlands, "there is considerable variety in the level of enforcement of measures between and within national approaches".

Universities play an important role in the implementation of knowledge security. As part of their role to ensure legal compliance and pursue self-regulation, universities have recently (particularly from 2020 onwards) started to adjust their operational processes. Some

[10] Netherlands, Germany, Belgium, Spain, Italy, Switzerland, and Denmark.

[11] A staff working document which, while not legally binding, provides guidance.

[12] The full name is: Commission Recommendation (EU) 2021/1700 of 15 September 2021 on internal compliance programmes for controls of research involving dual-use items under Regulation (EU) 2021/821 of the European Parliament and of the Council setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items.

[13] That do research on sensitive technologies, such as quantum technology, artificial intelligence, photonics, semiconductors robotics, opto-electronics, nanotechnology or radar technology.

universities hence adjusted their decision-making process for particular topics, made adjustments to the services offered to staff and students, and created awareness at operational, tactical and strategic level. Some are reviewing their authorisation procedures for accessing accounts, systems, and buildings, their legal advisory process, their pre-employment screening, adjusting their HR information system, contract management processes, adjusting their archival and documentation system, training international agreement coordinators in knowledge security, reviewing their internationalisation policy, or broadening the mandate of their ethics committees. Universities realise that adjustments of existing and the design of new measures can only be effective if properly implemented and if processes for continuous improvement processes are in place.

While these measures reflect the commitment and engagement of universities of S&T, during many of these processes, universities are also struggling with questions about interpretation and implementation, in particular when they are confronted with potential conflicting principles and values. A sometimes-heard concern amongst policymakers, scientists and higher management in universities of S&T are that the combination of measures affect: (a) some core values, in particular inclusiveness, openness, academic freedom; (b) core operational processes, in particular recruitment, financial systems, contracting; (c) excellence, in particular in attracting excellent students and scientists, also when they originate from high-risk countries; and (d) innovation capacity. Key questions that come up in this context include:

- How do current export control, sanction policies, and measures to counter foreign interference impact international collaboration, and student and staff mobility?
- Is 'open science' and the 'openness of science' restricted? If so, in what way(s) and by whom? What is the role of non-disclosure agreements and trade secrets?
- Can data and research results for 'sensitive' technologies[14] still be shared freely amongst academics?
- Are international researchers still welcome to work on research projects with dual-use technologies, key-enabling technologies and emerging technologies?
- Are we moving towards a situation where export permits are necessary for tertiary education and for scientific publications?
- Do country-specific sanctions on dual use and other technology require universities to block students with these nationalities to participate in particular educational activities?

In other words, how does the change in the geopolitical context affect the way-of-working for universities? How can the EU and national authorities support universities? These and other questions all result from efforts to 'keep science open where possible and restricted there where needed' in a changing geopolitical landscape. For this reason, in the next chapter, we will review the changing (geopolitical) context that makes such discussions necessary.

[14] What is sensitive and not is not clearly defined and different interpretations are used by various countries and for different purposes. Some of the technologies are mentioned in Shaping and Securing EU's open strategic autonomy by 2040 and beyond, or NATO's Science and Technology trends for 2020 - 2040 that are outlined by NATO (2020). It is often a combination of dual-use technology, key enabling technology and/or emerging technology.

Method

This white paper is an exploratory paper based on experiences and expert input and discussions across the CESAER membership, it is not the result of scientific research. At the start of the process, an inventory has been conducted across CESAER Members through a survey on current practices in relation to knowledge security and export control. The tables in the annexes are supporting material to the text of this paper. The tables illustrate current (restrictions to) open-science practices and to openness of science. Extensive input has particularly been provided by the members of the CESAER Task Force Openness of Science and Technology and reviewed by peers at CESAER Member universities. The format for the first table is based on open-science practices in various phases of the research lifecycle while the format for the second table is based on the management of selected operational processes at universities.

The tables are intended to provide illustrative examples and are not intended to be exhaustive nor representative for all universities, partners, funding agencies or authorities. For example, the variety amongst so-called 'partners' is quite large. The term 'partners' covers everything from partner universities, SMEs, NGOs, hospitals, governmental organisations to high-tech industry. Some of these have strong compliance needs related to well-developed legislative frameworks (e.g. patient privacy considerations in the healthcare setting), others do not. Some restrictions are present in particular EU member states, but not in others. Given the large variety of types of data, different scenarios, different types of collaboration and the technology domains it is almost impossible to be complete.

The paper includes a multitude of references (through the use of both hyperlinks to online sources and to a list of references including to offline sources), which can be used to complement and enrich the information provided in the paper. Throughout the paper, the authors refer to several EU documents and papers in various stages of 'formality' and with different levels of legal authority. This ranges from legally binding regulations adopted by the EU institutions, to decisions adopted by the European Commission to more informal staff working documents and guidance documents that are not legally binding. In some cases, such as the Marseille Declaration, it is a political declaration intended to guide political developments. Any reader interested in the legal implications for their own context of any document reference in this paper is advised to solicit independent legal advice competent in their own region.

Table 1 in Annex 1 outlines various stages of the research cycle and provides examples of measures that are currently restricting or enabling open science. The 'restrictions' are mostly based on protection, security and compliance needs. For table 1, we used the four phases identified by Gownaris et al (2022): (a) study design and tracking; (b) data collection; (c) publication; (d) outreach[15].

[15] The scheme from the Center for Open Science includes even more phases (creative design, resourcing, planning, conducting, interpreting, reporting, publishing, discussing), but we have chosen the version by Gownaris (2022) to keep it more compact.

Table 2 in Annex 1 provides examples of key practices that affect the open culture and accessibility of science and technology to other sectors, stakeholders, or nationalities. It includes various 'o*pen-for-science'* practices, seeking to minimise barriers to (inter)national academic and scientific cooperation.

Chapter 2. Context

2.1 Changing geopolitical relations

'Open innovation, open science and open to the world' were the three main policy goals for EU research and innovation in 2015. The collaborative, international and open nature of science and innovation was presented as instrumental for the development of new ideas and as sustainable investments in the future of Europe (European Commission, 2015). Universities were encouraged for years to start new international collaborations and to explore the potential for student and staff exchange, innovative research projects, joint research centres or labs, or valorisation.

Since then, the world has drastically changed with, amongst others, the COVID-19 pandemic, the Russian invasion of Ukraine, increasing tensions between China and the US including around Taiwan[16]. These and other international developments had an impact also on the day-to-day realities of universities. Universities have become, more than in the past, targets of unwanted knowledge transfer in particular in relation to sensitive technologies. 'Unwanted' refers here to knowledge transfer that falls outside the legitimate context of research cooperation. While international cooperation is still encouraged, and the value of openness is emphasised and reiterated, the European Union, national authorities and universities have become more aware of risks related to such cooperation and the responsibilities that this implies. Given the changed circumstances, they are in search of a new balance, as exemplified by 'Europe's China doctrine' launched in 2023 by the European Commission in the form of a European Economic Security Strategy where research and technology feature prominently.

Deterioration of relations

The relations of the European Union with the Russian Federation quickly deteriorated after a series of critical events and acts of aggression towards Ukraine. The changing geopolitical landscape, together with economic, environmental, technological and societal trends[17], has resulted in a broader understanding and deeper awareness of risks that come with Europe's dependency for its industry, talents, research and innovation, resources and (raw) materials on other countries, including the Russian Federation, China, South-Korea, the Democratic Republic of the Congo, and the United States (HCSS, 2022)[18].

[16] Of relevance in this context is that Taiwan is home to the Taiwan Semiconductor Manufacturing Company (TSMC), one of the main designers and manufacturers in the global high-end chips industry (Clingendael, 2021; HCSS, 2022).

[17] As summarized in: Störmer, E., Muench, S., Vesnic-Alujevic, L., Vesnic-Alujevic, L., Scapolo, F., Cagnin, C. (2021). Shaping and securing the EU's open strategic autonomy by 2040 and beyond (European Commission Joint Research Centre Science for Policy Report). Publications Office of the European Union. https://data.europa.eu/doi/10.2760/877497

[18] "EU companies are becoming increasingly reliant on US and Chinese companies like Meta, Google, Microsoft and Baidu, to access general purpose AI systems that underpin other AI tools, a dependency that could stop Brussels setting global standards for the technology" (David Matthews in Science Business, 3 Nov. 2022).

Due to heightened concerns over (inter)national security in the last couple of years, the US[19], the EU the UK, the Russian Federation and China have all adjusted their laws and regulations on export control, divestment orders, data protection, foreign interference, adjusted their denied persons list, entity lists and 'unverified lists', and have increasingly taken other (protective) measures in strategic sectors[20] based on technological foresight studies and geopolitical analyses. The awareness of this changing landscape resulted in a gradual shift of the 'open innovation, open science and open to the world' promoted earlier. This was further specified in the last few years through:

1. the Global Approach to Research and Innovation (non-binding communication by the European Commission);
2. the Marseille Declaration (non-binding political declaration by the French Presidency of the Council of the EU);
3. the European Economic Security Strategy (non-binding communication by the European Commission)
4. the EU-US Trade and Technology Council (coordination forum established at the EU-US Summit on 15 June 2021 in Brussels)

These four developments are briefly discussed in the sections below.

2.1.1. Global approach to Research and Innovation

In May 2021, the Commission published its Global approach to Research and Innovation which was designed to provide strategic orientations on an open approach, a level-playing field and reciprocity in international cooperation to "better safeguard [EU] interests, values and expertise" within the new geopolitical context.

Reducing dependencies, protecting EU interests and values, and widening the scope of economic opportunities have become the main considerations. Openness and protectionism are complementary in the Global Approach Communication in order "to avoid a takeover of the EU's critical assets, whilst harvesting the benefits of collaboration and competition of economies". (Cagnin, a.o., 2021, p. 80).

The Guidelines on Tackling R&I foreign interference, aimed partly at universities and research centres, reflect these concerns as well: "The defence of European values like academic freedom, research ethics and integrity, gender equality and diversity, and open science and data, is essential in a multipolar world where the system of rules-based multilateralism is undermined by foreign actors that interfere in academia, unduly appropriate

[19] For more specific information, see the Bateman, J. (2022). Specific measures for the Semi-conductor industry and Chips are announced in the US Chips Act and the EU Chips Act. A comparison between the US Chips Act and the EU Chips Act can be found here. See also the more recent announcement (October 2022) by the US Bureau of Industry and Security on the 'Implementation of Additional Export Controls.'

[20] See for example the Carnegie Endowment for International Peace (2022); the recent changes in the EU export regulations (2021); China's White paper on export controls (2021), and the Made in China 2025 initiative (2018).

intellectual property, and evade a level playing field based on reciprocity." (European External Action Service, 2022).

The earlier mentioned developments at the international geopolitical level contributed to a gradual change. While multilateralism and 'openness' is still considered to be the default for scientific cooperation, with its Global Approach the EU is making a distinction between 'like-minded countries' and those who are not adhering to the same principles and values. The EU will apply openness in particular to its members, the associated countries, and like-minded countries, such as the US, Canada, Norway, the UK, Japan, and others when reciprocity is seen as guaranteed. This applies not only to industrialised countries, but also to partners based in Africa (e.g. the 'Africa Initiative').

The Global Approach also highlights the role of Science Diplomacy: science, technology and innovation are seen as instrumental for political leverage and soft power[21]. This is perceived as having various advantages:

- "A stronger focus on science, technology and innovation in foreign and security policies enables the EU to respond to such challenges, while simultaneously enhancing its resilience and strategic autonomy" (EEAS, 2022)
- "The inclusion of science, technology and innovation in the EU's diplomatic toolbox and messaging does not only enhance the quality of our policy, but also helps the EU to project soft power and pursue its values and interests more effectively" (EEAS, 2022).

Box 1: Horizon Europe

Horizon Europe is the EU's framework programme for research and innovation with over € 95 billion allocated for the period of 2021-2027. While Horizon Europe includes several open science related initiatives, it also foresees provisions to safeguard EU's strategic interests as identified in the new R&I internationalisation policy.

Article 22(5) of the Horizon Europe Regulation 2021/695 provides that the work programmes (which provides details for what and how funding will be allocated) may limit participation in actions supported by the programme when there is a justified need to safeguard the EU's strategic assets, interests, autonomy or security. In these exceptional and justified circumstances, the EU could limit participation in the programme to legal entities established only in EU member states or in specified associated or other non-EU countries. The work programme may therefore exclude the participation of legal entities established in the EU, or in associated countries directly or indirectly controlled by non-associated third countries[22]. This has been effectuated with the Decision (EU) 2022/2506 of December 2022 to cut off 30

[21] The instrumentalisation of Research and Innovation for political leverage or as foreign policy instrument received a response from the European Association of Universities (EUA) and was recently criticised in a recent editorial of Nature (December 2022).

[22] See also answer to the European Parliament given by EC Commissioner Vestager on 18.08.2023 on the question of Huawei's participation in Horizon Europe projects and receipt of funding

higher education and cultural institutions in Hungary, including 21 universities, from Horizon Europe and Erasmus funding over ongoing concerns about rule of law breaches.

In parallel, as preventive measures, the Commission proposed to make use of provisions under the Horizon Europe Regulation to further mitigate risks it identified to EU interests, such as those on exploitation of results in non-associated non-EU countries (Art. 39(6)), on the transfer of ownership of results (Art. 40(4)) or on security agreements with non-EU countries (Art. 20(1)).

2.1.2. The Marseille Declaration

As a follow-up to the Global Approach's commitment to developing principles for international cooperation in R&I, the French Presidency of the Council of the EU organised a meeting in Marseille in March 2022 for EU science ministers. The meeting took place a couple of weeks after the Russian invasion of Ukraine. It aimed to discuss the values and principles for international research cooperation and to restore balance to international partnerships.

The resulting Marseille Declaration on international cooperation in R&I underlines that "International cooperation in R&I, as well as in higher education, is of geopolitical and strategic importance for the European Union" (Présidence française du Conseil de l'union Européenne, 2022, p.2, par. 2).

The Declaration sets out nine key principles and values for international cooperation[23] and underlines the importance of the 'openness' of science[24], and of the concept of 'open science'. The latter is further elaborated as the "opening or sharing of research data and software and source codes produced by research, access to networks, support to open science infrastructures, open participation of societal actors in the scientific process, communication with the general public and open innovation" (Marseille Declaration, 2022, p. 5, item 7e). In June 2022, the G7 meeting in Frankfurt reiterated the importance of research security, academic freedom and open science. Research integrity[25] and transparency are mentioned as key elements to achieve this. Openness can, in this context, therefore be seen as both serving and competing with geopolitical and economic and interests.

[23] freedom of scientific research, ethics and integrity, research excellence, gender equality and open science, intellectual property, personal data, value creation and societal and economic impact, societal and environmental responsibility and solidarity and risk management/security.

[24] "It is important to welcome the willingness of researchers, innovators, academics and students to collaborate internationally and to ensure that they can work and collaborate freely in an environment based on principles and values shared by all actors, thus ensuring a balanced cooperation. It is crucial to maintain openness in order to strengthen partnerships with their counterparts in other countries" (Marseille Declaration, March 2022, item 5).

[25] The European Code of Conduct for Research Integrity can be found here.

2.1.3. Towards strategic autonomy for a stronger Europe

During the COVID-19 pandemic, there was a rush (particularly among political and economic leaders) towards acknowledging the vulnerability and technological dependency of the EU towards the rest of the world, with concepts such as 'technological sovereignty' and 'strategic autonomy' quickly gaining momentum (European Commission, 2021, p.3). The underlying logic was that Europe should be more resilient, become a more powerful player, and interdependencies should be mutual. The OECD (2023) summarised some of these interdependencies between the US, EU, China and the UK showing several trends[26].

The European Parliament Research Services (EPRS) described the trend towards strategic autonomy and technological sovereignty as a steady 'retreat inwards' from globalisation and international economic integration. This global shift to a more inward-oriented stance has led the EU to contemplate on how to "become more autonomous, sovereign and resilient" (EPRS, 2020, p. 6). The Joint Research Centre (JRC) 'Science for Policy' report 'Shaping and securing EU's open strategic autonomy by 2040 and beyond' (2021) provides various scenarios and ingredients to achieve strategic autonomy, in relation to geopolitics, technology, economy, the environment and society.

In line with this trend, on 20 June 2023, the European Commission launched its 'European Economic Security Strategy' and a few days later, the European Council stated in its conclusions, particularly in relation to China, that it will "reduce critical dependencies and vulnerabilities, including in its supply chains, and will de-risk and diversify where necessary and appropriate" (30 June 2023, p. 9, par. 32).

Frontier Economics and the European Centre for International Political Economy (ECIPE, 2022) have set out a broad taxonomy of strategic autonomy policies and identified policies, regulations and initiatives that are:

1. meant to achieve long term industrial and trade policy objectives;
2. developed to correct market failures related to products and activities in the EU;
3. developed to correct market failures related to production and processing methods with extra-territorial reach, or;
4. developed in response to trade measures or behaviours by non-EU jurisdictions.

A similar typology of strategic autonomy policies and initiatives is based on characterising initiatives in terms of protection, promotion, projection, or combinations thereof (OECD, 2023)[27]. These are in line with the three approaches within the European Economic Security Strategy (European Commission, 20 June 2023) of: promoting the EU's competitiveness,

[26] With reference to (and figures of): bilateral collaboration intensity trends in scientific publications; changes in international collaboration US - China per technology domain; foreign-born human resources for S&T, foreign-born origin students, and net flows of scientific authors for top-publishing countries (OECD, 2023, Ch. 2).

[27] The first policy intervention (protection) aims to restrict technology flows and reduce dependency vulnerabilities, the second policy intervention (promotion) intends to enhance industrial performance through STI investments and the third intervention (projection) is meant to extend and deepen international STI linkages. The OECD (2023) refers to a number of relevant policy initiatives from China, the US and the EU that fall within this typology of protection/promotion/projection.

protecting the EU's economic security and partnering with the broadest possible range of partners to strengthen economic security. Research and innovation play a key role in all three strands. One of the actions announced in this communication is that “the Commission and the High Representative, within their respective competences, will […] propose measures to improve research security ensuring a systematic and rigorous enforcement of the existing tools and identifying any remaining gaps. It will do so while preserving the openness of our system, which is the bedrock for our innovative economies” (European Commission, 2023, p.8).

2.1.4. Strengthening the relation between the EU and the US

Between the EU and the US, the EU-US Trade and Technology Council (EU-US TTC) was established in 2021 to coordinate approaches to key global trade, economic, and technology issues, in particular on export controls, foreign direct investment screening, secure supply chains, technology standards and global trade challenges.

These topics reflect and affect current framing on strategic autonomy and technological sovereignty by the EU, and can be expected to result in joint or similar measures between the EU and the US.

In other areas the EU and US are more divergent, such as on AI and data governance (Science Business, Strategic Autonomy. A guide for the perplexed, 2023). Even more so, the EU’s ‘blocking statute’ (Council Regulation (EC) No 2271/96 of 22 November 1996) prohibits compliance with laws passed by another country that have extraterritorial impacts. It was first enacted to counter US sanctions on businesses engaged in activities in countries such as Cuba or Iran[28].

2.2 From foresight studies to the identification of critical technologies

A number of strategic documents were published in 2021/2022, including the joint statement by CESAER and the UK Royal Academy of Engineering on key technologies. Building on the JRC’s ‘Science for Policy’ report, the EU published its EU strategic foresight report 2021 referring to global trends that will affect the EU in the coming decades.

The ten following areas were identified as strategic trends:

1. Ensuring sustainable and resilient health and food systems;
2. Securing decarbonised and affordable energy;
3. Strengthening capacity in data management, AI and cutting edge technologies;
4. Securing and diversifying supply of critical raw materials;

[28] Some cases are known where universities of science and technology in Europe and research organisations for applied research identified and complied with US sanctions due to the extra-territorial scope of these sanctions on the re-export of US-originating software and technology. In those cases, it has put restrictions on participation of students/staff from particular nationalities to join in certain research projects.

5. Ensuring first-mover global position in standard-setting;[29]
6. Building resilient and future-proof economies and financial systems;
7. Developing and retaining skills and talent matching EU ambitions;
8. Strengthening security and defence capacities and access to space;
9. Working with global partners to promote peace, security and prosperity for all;
10. Strengthening the resilience of institutions.

The EU Strategic Foresight Report 2022 explored the 'twinning' of the green and digital transitions in the new geopolitical context, and identified various critical technologies that are essential for achieving these transitions (European Union, 2022). While the Foresight report of 2022 looked at the role of critical technologies in achieving transitions, the EU Roadmap on critical technologies for security and defence took it one step further: it "outlines a path for boosting research, technology development and innovation (RTD&I) and reducing the EU's strategic dependencies in critical technologies and value chains for security and defence" (COM(2022) 61 final, p.1). This is an example of a clear 'promotion' strategy, one of the three policy interventions as described earlier. Similar to the EU Strategic Foresight Report of 2022, the EU roadmap refers to the establishment of an EU Observatory of Critical Technologies to identify, monitor and assess critical technologies for space, defence and related civil sectors, their potential application and related value and supply chains.

Identification of critical and sensitive technologies[30] also takes place at the national level, for example in the Netherlands, France, UK, and the US. These complement the lists of military technology[31] and dual-use technology already in use. The lists of critical and sensitive technologies are developed for various purposes, such as:

a. direct foreign investment screening;
b. visa vetting;[32]
c. collecting intelligence and performing security analyses;
d. monitoring supply-chains (and associated risks) of critical technologies (e.g. by the EU Observatory);
e. risk analyses by universities.

[29] Standardisation, especially in the area of rare earth materials, will be a key-element for the global technological landscape of the future. (HCSS, 2020 and HCSS, 2020). See also Bjerkem, J., Harbour, M. 2020. *Europe as a global standard-setter: The strategic importance of European standardisation*. Discussion Paper. European Policy Center, 15 October, 2020. As well as Teleanu, S. 2021. The geopolitics of digital standards: China's role in standard-setting organisations. Published by DiploFoundation/Geneva Internet Platform and Multilateral Dialogue Konrad Adenauer Foundation Geneva.

[30] France has made a useful distinction between essential, critical, and strategic technology

[31] Council. 2023. Common military list of the European Union. adopted by the Council on 20 February 2023 (equipment covered by Council Common Position 2008/944/CFSP defining common rules governing the control of exports of military technology and equipment) (updating and replacing the Common Military List of the European Union adopted by the Council on 21 February 2022 (1)) (CFSP) (2023/C 72/02).

[32] Additional screening of students, PhD students, researchers and foreign employees that need a visa and want to work on critical or sensitive technology

2.3 From critical and sensitive technologies to day-to-day realities

In practice, universities and researchers are struggling to keep up with the rapidly evolving geopolitical reality and with new administrative hurdles appearing in their day-to-day operations. Researchers who were encouraged, for many years, to cooperate with globally leading universities and companies in emerging and key-enabling technologies are suddenly faced with new questions and new procedures to assess potential and real risks of their research cooperation and joint educational programmes, extending beyond the research and educational domains and into political and economic considerations.

How does this affect their research progress, publication process, presentations at seminars and conferences, open science activities, teaching activities, and cooperation with other universities and research organisations, the intellectual property rights (IPR) policies and recruitment of foreign nationals?

It is against this background that this paper will explore what it means for day-to-day operations at universities to be 'as open as possible and as restricted as necessary' in the context of knowledge security[33]; and to provide recommendations to keep science as open as possible in the changing geopolitical context. To enrich the understanding around 'as open as possible', the following chapter will summarise recent developments on open science and review open science practices, before moving to the day-to-day operations of universities.

[33] The phrase 'As open as possible, as closed as necessary' has earlier often been used in relation to IP and in relation to commercialisation of research outputs.

Chapter 3. Open science

3.1 Evolution of open science practices: key aspects

The last two decades have witnessed an evolution of the concept of open science, from a focus on open access to publications to a call for openness and transparency in the creation and sharing of a broader range of outputs and in research practices and partnerships. This is reflected in the European Commission definition introduced earlier in this report.

In the context of this paper, we briefly review these practices and assess how they may be affected, in both policy terms and in everyday practice, by the changing geopolitical context and measures taken to address them.

Open science encompasses a range of practices applied throughout the research cycle, seeking to make the creation, sharing and evaluation of knowledge accessible, reusable, transparent, collaborative and inclusive. It is helpful here to define and distinguish 'open science' practices (sharing of research outcomes and resources; transparent research practices) and 'openness-of-science' practices, seeking to minimise barriers to scientific cooperation (enabling the movement of researchers and students, the informal communication of results, and the co-creation of research between different groups, including with the public). Of the two, it is the latter which is most likely to be affected by security measures and around which policy and processes need to be shaped. This being said, the export control regimes may also have a major effect on scientific publications when publications that potentially meet the dual-use threshold, will all become subject to scrutiny for export control (EU recommendations 2021/1700, 2021, p. L338/10). While the recommendation recognises the push for open science, it also states that this does not exempt researchers and research organisations from screening proposed publications and data sets in relation to export controls on dual-use technology.

It is important to remember that export control considerations rarely play into considerations related to open access to scientific publications (i.e., scientific publications that are free-to-read for everyone) versus paid-access to scientific publications (i.e., the conventional way of publishing where readers pay a subscription to a scientific journal to be able to read a scientific publication). Access in this sense is for the latter option only restricted by the ability to pay, which is not typically the type of access restriction that would be needed if there are export control considerations.

Open science practices include:

- Open access to peer-reviewed scientific publications (such as journal articles), including rights retention and the application of open licences; repositories supporting open standards, and business models supporting open access publishing.
- *FAIR data*, which is essential for the verification and reproducibility of published results, the sharing of null or negative results, and for innovation. For data to be

discoverable and reusable, several actions and decisions are necessary over the course of a research project: including deciding what constitutes 'data', preparing and documenting data sets, storage and preservation, licensing and sharing. It is the A of Accessibility that can determine who has access to what and under which conditions. This can thus be restricted use: restricted in time, restricted in place, restricted for certain groups etc.

- Software and code may constitute 'research data' if they underpin the results of a study. This includes open-source software, hardware and code released under open licences that meet the Open Definition.
- Preregistration of research designs, registered reports, early sharing of articles (preprints), and open peer review models, adopted early on in the project, to reduce cognitive biases, support research integrity and reproducibility and enable rapid and efficient disclosure of research findings, as well as to spur collaboration and further research.

Openness-of-science practices include, but are not limited to:

- Recruitment of researchers (including students) from different countries, disciplines and backgrounds to write bids for funding and work on collaborative projects;
- Informal discussions and dissemination of research ideas, problems, findings and knowledge, including through meetings and correspondence;
- Collaboration with industrial partners, practitioners and policymakers.

All the practices outlined above share some key characteristics: they are increasingly recognised as essential for scientific integrity and to enable innovation and collaboration; they are increasingly embedded in government, funder and institutional policies, and their uptake is monitored and rewarded.

To various degrees, they are likely to be affected by legal, ethical and security factors and therefore, policies mandating or encouraging them increasingly need to be flexible and harmonised with other policies, legal frameworks and social, economic and geopolitical realities. This chapter continues with EU policies and guidance on open science and then provides examples of country-specific approaches.

3.2 EU policies and guidance on open science

The drive towards open science at the EU level gained momentum with the preparations for and start of Horizon 2020 around 2013/2014. To boost the openness and global internationalisation of science, the European Commission implemented policies and initiatives to promote open science and make research more accessible. For reference, currently the European Commission has eight ambitions for its open science policy: open data, European Open Science Cloud, new generation metrics, mutual learning on open

science, future of scholarly communication, rewards, research integrity & reproducibility of scientific research, education & skills, and citizen science.

These include mechanisms, infrastructures, and programmes to remove obstacles and barriers to open science, addressing the link between open science and intellectual property rights, between open science and funding mechanisms, between open science and metrics, between open science and the reform of research assessment, and between open science and rewarding policy for researchers. Many initiatives have been and are being generated through the following policies and mechanisms: the Open Science Policy Platform, the European Open Science Cloud, the Horizon Program, the European Research Council and the European Open Data Portal. This area remains high priority for the European Commission, including as exemplified with action #1 of the ERA Policy Agenda 2022-2024.

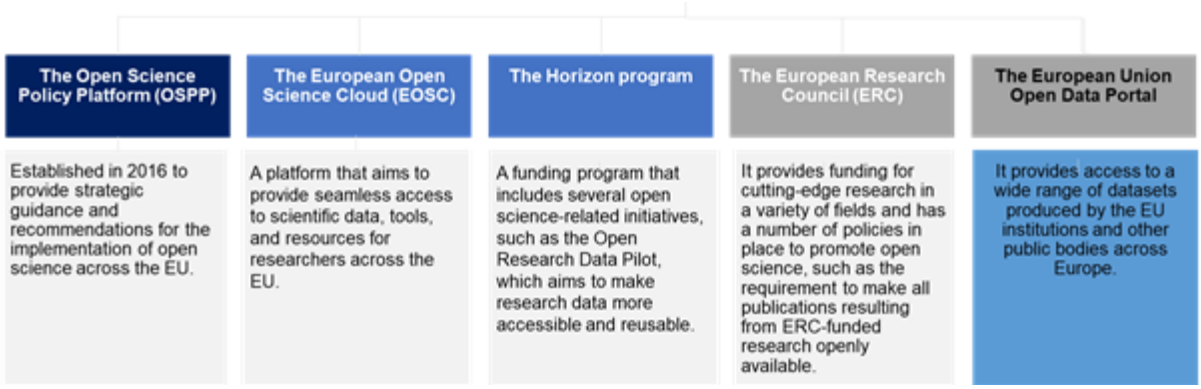


Figure 1. Selection of policies and implementation of Open Science at the European level.

The various initiatives mentioned above include one or more of the following requirements or recommendations.

- European Research Council Open access guidelines on the implementation of open access to scientific publications and research data, in particular in relation to peer-reviewed scientific publications;
- A Horizon Europe General Model Grant Agreement that enables authors to retain intellectual property rights to their publications, enabling them to share them under Creative Commons licences;
- Requirements to make research data FAIR and as open as possible;
- Establishment of the platform Open Research Europe and the European Open Science Cloud to support EU-funded researchers in meeting these requirements;
- Support, encouragement and reward of reproducible research practices and early dissemination of findings (preprints, lab notebooks);
- Support, encouragement and reward of citizen science projects;

- Provision of open science education and skills training to researchers;
- The development of next-generation metrics and altmetrics that reward open science;
- Establishment of the Open Science monitor to gauge progress.

One key initiative is the European Open Science Cloud (EOSC), which aims to provide a common infrastructure for scientists and researchers to store, share, and analyse data across borders and disciplines. EOSC was built from several initiatives, such as the FAIR Data Action Plan (Grootveld et al., 2018) aimed to ensure that data produced by EU-funded research is Findable, Accessible, Interoperable, and Reusable (FAIR). The plan includes guidelines for data management and sharing, as well as tools and services to support researchers in making their data FAIR.

The importance attached to Open Science at the European level becomes even more evident when it is integrated in the reform of the research assessment system. On November 2021, the EU Council adopted Conclusions on the 'Future governance of the European Research Area (ERA)' and a 'Pact for research and innovation in Europe', setting out priorities and a streamlined governance framework for the ERA, including an ERA policy agenda for 2022-2024 (containing 20 key actions). Two of the ERA priority actions are:

- "Enable the open sharing of knowledge and the re-use of research outputs, including through the development of the European Open Science Cloud" and
- "Advance towards the reform of the Assessment System for research, researchers and institutions to improve their quality, performance and impact".

The adoption of the Pact for Research and Innovation in Europe and the Council Conclusions on the ERA governance advanced the reform of the ERA, which started in 2020. During 2021 the Commission held consultations with European and international stakeholders, including CESAER, on the reform of the research assessment summarising the outcomes in a scoping report "Towards a reform of the research assessment system".

At the end of that year, the Commission launched the process towards an agreement on reforming research assessment calling for organisations to express their interest in being part of a coalition for reform. In January 2022, CESAER was invited to join a core group to prepare the reform, and 2022 ended with the publication of the Agreement for the Reform of Research Assessment and the creation of the Coalition for Advancing Research Assessment (CoARA). The principles for reform are explicitly promoting the recognition and reward of open science practices. Open science, one can argue, has become more than a set of practices, it has become a standard in itself.

3.3 Country-level uptake of open science

The uptake of open science and open access is not happening by itself. Research funders and research performers play an important role in this development working together with

universities and their communities. A consortium of national research funding organisations, supported by the European Commission and the European Research Council, joined forces in cOAlition S to further enhance open access. Together they launched Plan S, an initiative for open access publishing that was launched in September 2018. Plan S required that, from 2021, scientific publications that result from research funded by public grants must be published in compliant open access journals or platforms. More and more national and international funders now support the principles of cOAlition S on immediate open access to research publications, rights retention by authors and research organisations, and sharing creative work under copyright law by various forms of licensing (referred to as CC-BY licensing). Plan S and the advancement towards open access publishing received broad support from the academic community, including from CESAER as elaborated in its positions in 2020 and in 2023.

Current data suggest that two-thirds of research funders worldwide mandate deposit in open access repositories and an additional one-fifth encourage the practice. Some 37% of research funders mandate open access publishing, while an additional 32% encourage it (Juliet Statistics[34], accessed 9 August 2023). Plan S principles have been pivotal in shaping the way open access infrastructure and scholarly communication business models are evolving, and has had a substantial impact on institutional strategies for open access at universities of S&T (CESAER white paper, 2022).

In the United Kingdom, for example, UK Research and Innovation (UKRI) and the Wellcome Trust support both open access publishing and repository deposits. Funding for open access publishing in the UK is only supported if a publisher demonstrates a commitment to transition into full and sustainable open access; and rights retention to enable immediate deposit with a CC-BY licence is also mandated. This has implications for the ways open access is implemented at both institutional and researcher level.

Broader open science policy and activity across EU member states and relevant countries from the European Research Area is monitored and updated by several organisations, including: OpenAIRE's National Open Access Desks (NOADs), SPARC Europe/the Digital Curation Centre, and the EOSC Portal. Uptake and implementation of open science policy is regularly monitored and updated in the report 'Analysis of open access policies in Europe'.

3.4 Balancing open science with other needs

Scientific collaboration lies at the heart of open science, with the ultimate goal being to produce research for the benefit of society. For this to be possible, it is necessary to lift as many barriers as possible in the ways that information, tools and resources are shared among scientists and with the public throughout the research process. While there is broad consensus around the many benefits open science bring to research, other needs or goals related to science and technology can bring in different considerations.

[34] monitoring Open Science for the European Commission, Research and Innovation.

The European Commission's 2022 report on 'Open Science and Intellectual Property Rights' recognises the importance of balancing the sharing and reusing of scholarly knowledge for the benefit of society with the protection of the interests of different stakeholders, including private and commercial research organisations[35]. It highlights the need to address the challenge faced by businesses and industry in adopting open science practices while fulfilling the requirements of Intellectual Property Rights (IPR). The report suggests aligning the balance between openness on the one hand and IPR protection on the other hand, with the principle of "as open as possible, as restricted as necessary" for research data.

Finding a balance is, however, not always a two-dimensional dilemma at the level of universities and research organisations. Other aspects - such as research integrity, knowledge security, export control, data sovereignty, benefit sharing, transaction costs, administrative burden - may play a role as well, and sometimes in combination or at other levels (national/international). A simple trade-off between 'closed' and 'open' is therefore too simplistic. The Academic Cooperation Association's President in a May 2023 article discussed "how to strike a balance between openness and realism", which will for some likely be a controversial way to frame the discussion, but highlights the complexity of the issue.

A good example of this is the international and rather technical debate on various policy options for global access to Digital Sequencing Information (DSI). While not relating to IPR, knowledge security or export control, it is included here, as it shows how different interests play a role in regulating or restricting open access of data. More information and access to the database can be found on the DSI website.

Box 2: Access to the Digital Sequencing Information on Genetic Resources

The importance of open access to specific data emerged in the international debate around the digital sequencing of genome information, and in the context of the Convention on Biological Diversity. Digital sequencing refers to the ability to decode and digitally archive DNA. As described by Scholtz et al, sequence data were not only essential for technological innovation in life sciences and biodiversity, but the "free and open access to SARS-CoV-2 sequences also enabled the rapid development of diagnostic kits and vaccines." (Scholtz et al, 2022, p. 1).

While parties to the United Nations Convention on Biological Diversity (CBD) acknowledged countries' sovereign rights to their own genetic resources (GR), the practices of working through bilateral arrangements, prior informed consent and mutually agreed terms were not very efficient and rules were not clear. Some biodiverse lower and middle-income countries (LMICs) argued that they missed out on potential commercial benefits created from the use of DSI. They preferred to keep control over their own data as long as there were no arrangements for an equal share of the benefits. This created tension under the CBD, as other countries feared an administrative burden and regulatory complexity, when their access to the

[35] See the CESAER report on Openness and commercialisation: How the two can go together (2020)

DSI was to be negotiated on a country-by-country basis.

To solve this, various policy options were discussed and finally negotiated at the Conference of Parties at the CBD. The figure below gives a typology of these policy options. It shows the complexity of the discussion in relation to access and benefit sharing (ABS), prior-informed consent (PIC), mutually agreed terms (MAT), the Nagoya Protocol (NP), the Convention on Biological Diversity (CBD), the nature of the mechanism, and funding mechanisms.

In December 2022, the 15th Conference of Parties to the CBD decided to "develop a multilateral mechanism for benefit-sharing from the use of DSI that is consistent with open access to data, avoiding the challenges that would be created by a bilateral approach – such as increased regulatory complexity and administrative burdens which could disproportionately affect research institutes in developing countries where financial, technical and legal resources are particularly scarce" (DSI Scientific Network, 2022). The development of the mechanism still needs further work.

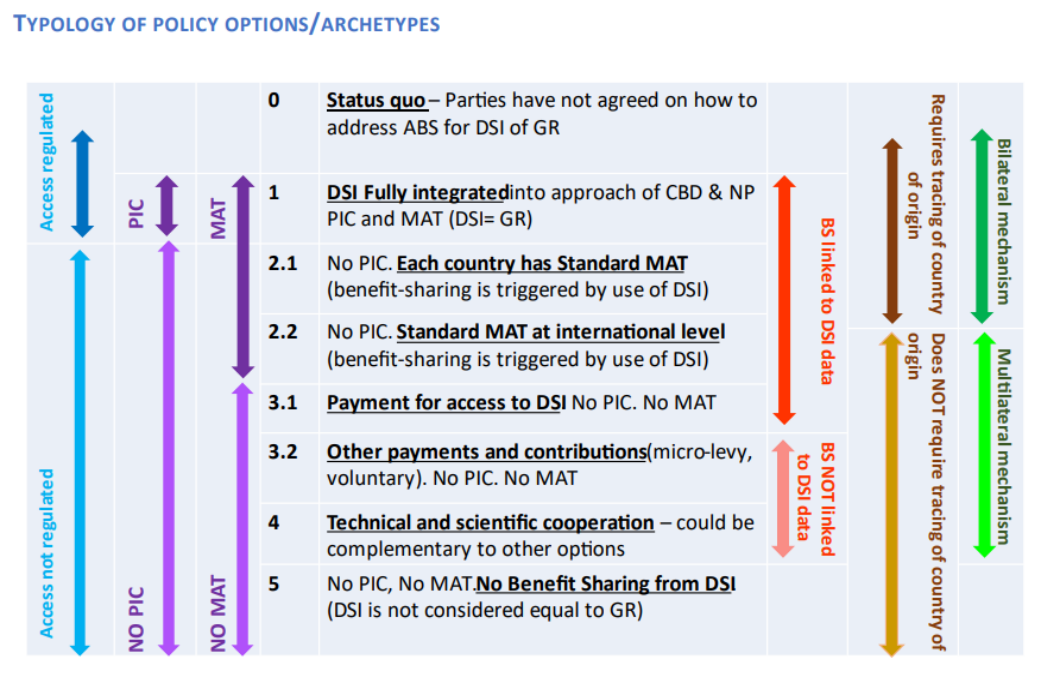


Figure 2: Typology of policy options / archetypes. Source: CBD, 2021, webinar 3.

3.5 Balancing open science with knowledge security

While previous sections show how various interests may need to be balanced in different contexts (across universities and research organisations, between universities and industry, across and between countries), in the remainder of this paper, we focus primarily on the balance between open science and knowledge security. The next chapter will start by providing examples for how knowledge security and export control affect the day-to-day realities of universities of science & technology.

Chapter 4. Knowledge security: measures and effects

4.1 Knowledge security measures

Knowledge security was defined, at the start of this white paper as: “preventing the unwanted transfer of (sensitive) knowledge and technology, which could negatively impact the national security of a country and damage the capacity for innovation. It also concerns the covert influence of state actors on higher education and science, which can lead, among other things, to forms of (self-) censorship that are detrimental to academic freedom. Finally, knowledge security involves ethical issues that may be related to collaboration with individuals and institutions from countries where fundamental rights are not respected” (Knowledge Security Guidelines, 2022, p.4)). It thus has three elements: (a) unwanted transfer of sensitive technology, (b) covert influence of state actors, and (c) ethical issues.

Concerns regarding the unwanted transfer of sensitive technology include, amongst others, the potential misuse of research data and output for human rights violations, cybersurveillance, or terrorism or the possibility that research data, methods, output or technical assistance (training and education) will be made available [to individuals, entities and regimes] to further develop, produce or distribute weapons of mass destruction. The covert influence of state actors includes efforts to retrieve information, to influence decisions or to undermine values, through political pressure, financial support, exploiting people, digital intrusions or the manipulation of information. Ethical issues may relate to the desirability of working with particular partners on particular research questions or with sensitive data.

As various aspects are covered by different organisational units and legal frameworks (both at national and European level), this sometimes makes it difficult for universities to develop their measures in a way that these address all three perspectives, while also upholding key principles such as those underpinning open science, non-discrimination and equal treatment, and academic freedom.

4.2 Measures in place by universities of science and technology

The measures taken by universities and research organisations include a variety of measures, such as data protection measures, export control and checks on international sanctions, measures to prevent and address R&I foreign interference, screening of staff, due diligence of partners, or measures in relation to ethics and research integrity. The more advanced universities of S&T in this area have started to identify information that can help them in decision-making, such as bibliometric analyses, dashboards, or an assessment of vulnerable research infrastructure. Universities of S&T in Europe have become more aware of the importance of proper risk assessments of their partnerships, their activities, sensitive technologies and knowledge security risks.[36]

[36] Another report includes a broader geographic scope, including the US, Japan, Australia, Taiwan, UK, and Finland. d’Hooghe, I. and J. Lammertink. November 2022. How National Governments and Research Institutions Safeguard Knowledge Development in Science and Technology. Leiden Asia Centre and the AWTI.

An internal survey from March 2022 (conducted within the CESAER network) showed that 12 out of 15 responding universities of S&T had one or more contact points, an advisor or a team on knowledge security; 11 out of 15 were familiar with the national policies and regulations on export control (and 3 others to some extent); 10 out of 15 had national policies or guidelines on export control. Approximately half of the respondents indicated that their university had a policy and/or an internal compliance program on knowledge security and export control in place.

The others indicate that an internal policy document or a compliance program is in the making. The figure below shows the uptake of measures mentioned by the Commission Recommendation (EU) 2021/1700 of 15 September 2021 on internal compliance programmes for controls of research involving dual-use items under Regulation (EU) 2021/821. Recommendation (EU) 2021/1700 is a non-binding document to guide universities in the interpretation and implementation of the (legally binding) dual-use regulation, Regulation (EU) 2021/821[37] . Although there is little comparison material from earlier years, it confirms that universities have become quite aware of the need for measures in knowledge security and export control.

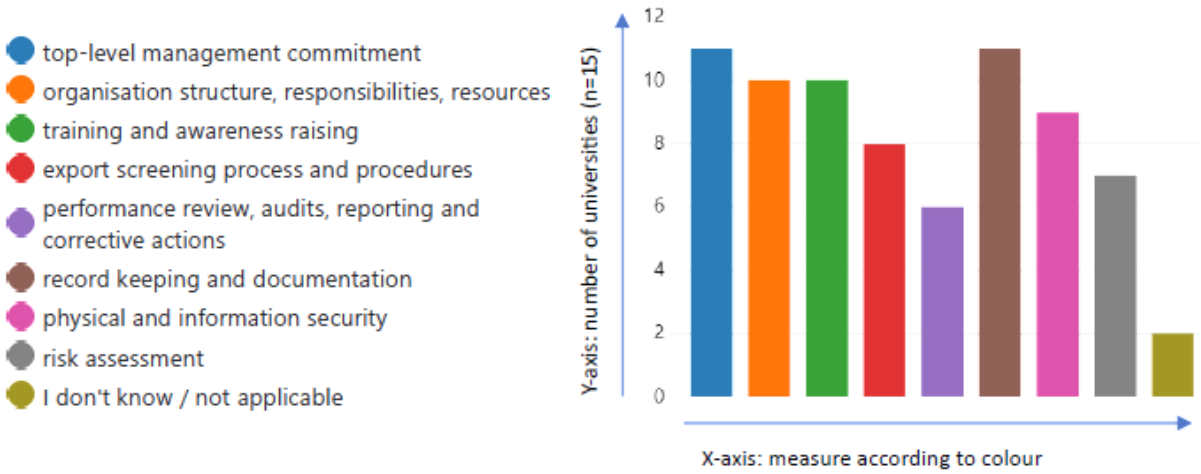


Fig 3: Uptake of measures from Recommendation (EU) 2021/1700 on internal compliance programmes (source: an internal CESAER survey with 15 CESAER Member universities, May 2022).

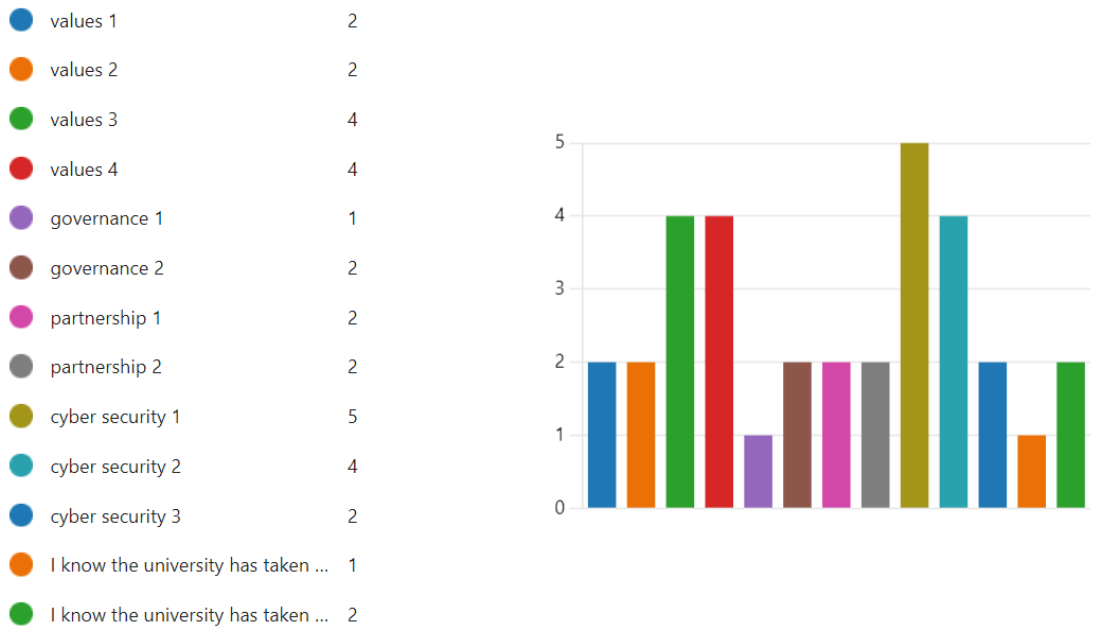
R&I Foreign Interference

As indicated at the start of this chapter, knowledge security has three components: unwanted knowledge transfer of sensitive technology (including dual-use technology), foreign interference, and ethical issues. As such, the EU Recommendation 2021/1700 was drafted to support universities with an internal compliance program for export control of dual-

[37] 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). Annex 1 is replaced by: Council. 2023. Regulations. Commission Delegated Regulation (EU) 2023/996 of 23 February 2023 amending Regulation (EU) 2021/821 of the European Parliament and the Council as regards the list of dual-use items.

use technology. The Tackling R&I Foreign interference publication (European Commission, 2022) was, for its part, drafted to provide tools and instruments to universities and research organisations to support them in relation to foreign interference.

Quite interesting is to see the uptake of the potential mitigation measures from this guideline. The topics are taken from the summary of the staff working document on p. 2-6 (see table below). The figure indicates that, [with the exception of cybersecurity] values as openness, academic freedom, non-discrimination, and integrity still have higher priority in comparison to risks and vulnerability. This outcome is not surprising, given the recent nature of the (inter) national re-focussing on risks of cooperation. Over the last decades, universities were encouraged to explore opportunities for cooperation with partners all over the world, to find opportunities for student and staff mobility, for external funding. Combined with declining budget allocated to universities by their government across large parts of Europe, universities were pushed to search for alternatives (including globally) also to diversity income streams.



X-axis: measure uptake according to colour; Y-axis: number of universities (n=15). See the legend below for details.

Fig 4: potential mitigation measures. Source: internal CESAER survey, 2022.

Legend:

Value:

1. Identify countries and partner institutions where academic freedom is at risk;
2. Conduct a vulnerability assessment to understand external pressures on academic freedom and integrity;
3. Strengthen commitment to academic freedom and integrity at institutional and individual levels;
4. Continue to cooperate with partners in repressive settings

Governance:

1. Publish a Code of Conduct for Foreign Interference;
2. Establish a Foreign Interference Committee

Partnerships:

1. Develop general prerequisites for the implementation of a risk management system;
2. Establish a sound procedure for developing robust partnership agreements;

Cybersecurity:

1. Raise awareness of cybersecurity risks;
2. Detect and prevent cybersecurity attacks from foreign interference actors;
3. Respond to and recover from cybersecurity attacks from foreign interference

Other:

'I know the university has taken measures but I am not able to share this'

'I know the university has taken measures but I am not sure which ones'.

[Source for listing of mitigating measures: European Commission. 2022. p. 2 - 6.]

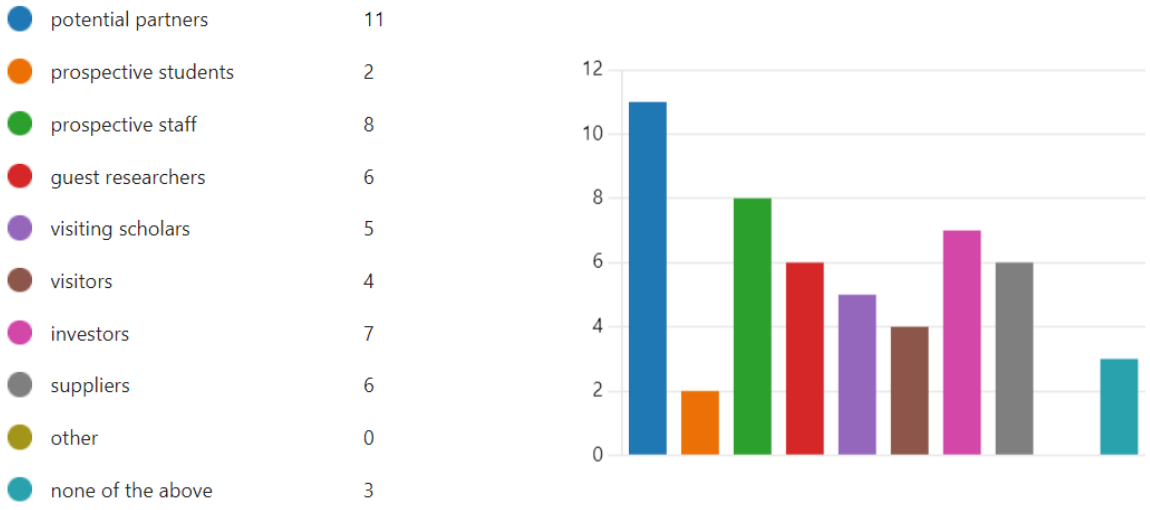
When asking whether and how the toolkit on tackling R&I Foreign Interference could be improved, some of the answers were to:

1. reflect on the efficient use of scarce resources, as no university will have the capacity and resources to take up all suggested measures;
2. encourage a selection of measures that fits with the context and specific nature of each university and the context they are working in;
3. reflect on the impact of all measures for the universities themselves in terms of (academic) freedom, open science, and institutional autonomy of universities;
4. pay attention to these risks not only far away but also 'at home'.

Screening and due diligence

Screening for sanctions is an important measure in knowledge security policies. Universities are obliged to comply with EU law, including sanctions at EU level. From the answers to the question who are screened against the applicable sanctions lists, it becomes clear that the

awareness is there: potential partners, prospective staff, investors and suppliers are screened on the sanctions lists for more than half of the participating universities.



X-axis: measure uptake according to colour; Y-axis: number of universities (n=15).

Fig 5: screening against international sanctions. Source: internal CESAER survey.

The answer of 11 out of 15 universities indicates that they have a screening in place for prospective partners, it does not yet, however, indicate how the screening is performed, what are the criteria, at what level the screening is performed and in what way is it decisive for partnership selection. Therefore, another question is asked about 'due diligence', tools that provide more background information about the organisation.

Due diligence, however, is done by only 5 out of the 15 universities that took part in the survey. A major reason for this seems related to the lack of information with regard to existing tools for due diligence that provides relevant information from the perspective of knowledge security. Suppliers and investors are another interesting category, and screened by half of the participating universities.

As the survey was designed to be anonymous, it is too early to tell whether this might be related to the foreign investment screening mechanisms that some countries are preparing or have adopted. Some foreign (state-owned) companies were known to invest in spin-offs at or within universities (to enlarge their geographic scope), while other cases show that major investment companies invested in entire high-tech campuses, in order to be at the forefront of innovation, and at the same time to gain more influence within universities.

Learning and training

Several universities are learning from each other through their national university organisation[38] or through European networks of universities[39]. This is, however, more so in some countries than in others. In some EU member states, universities are aligning with their national authorities, in others they are more independent. The national approach ranges from: (a) a top-down and regulated approach, (b) a decentralised approach with self-regulation by the sector, or (c) a mix of the two previous approaches. In some EU member states, authorities have taken up a role in organising seminars, workshops or in the development of a learning community: d'Hooghe and Lammertink (2022) discuss these differences per country and position the roles and approach in the national context.

The European Open Science Cloud (EOSC) ecosystem also plays an important role in the learning and training, as its aims to federate and coordinate key European infrastructures for open science, and together with OpenAire, guidelines for researchers to deal with Intellectual Property Rights, data protection laws and regulations on non-personal data in the context of open science and open data policy (EOSC, 2022).

[38] The Universities of the Netherlands (UNL), for example, are offering universities a set of partnering tools that can be used on a voluntary basis by the universities and adjusted to the requirements of the own organisation

[39] Some of the most active in this area are: CESAER, LERU, EECARO and EOSC.

Box 3: Learning from measures in the commercial sector

A recent report by the European Innovation Council and SMEs Executive Agency (EISMEA), analysed "to what extent the EU legal framework on trade secret protection applies to data which was shared across firms and organisations". It also looked at the application of trade secrets by European firms in practice (EISMEA, 2022).

While the report is primarily meant to help in creating a 'safe environment for business-to-business (B2B) data sharing' (EISMEA, 2022, p. 1) it is interesting to look at the range of data sharing and data protection mechanisms, the motivations, practices and experiences as documented amongst participating businesses in various sectors. Universities make use of similar categories of measures as companies:

1. legal protection measures, such as non-disclosure agreements (NDAs), data sharing agreements, collaboration agreements, trade secret clauses, material transfers, specific licensing agreements; patents, copyrights, database rights;
2. technical protection measures related to IT, cybersecurity, or other technical measures such as seals, safes, corporate security;
3. employment related measures, such as training, guidelines and policies for employees; specific clearing processes during staff recruitment or actions targeted at leaving staff to ensure post-employment confidentiality; or
4. engaging professionals within the organisation or through the use of external consultants.

The desired combination of such measures is, amongst businesses, defined by the nature of the sector (be it energy, health, R&D, automotive or something else). The report specifies in detail various forms and manifestations of sharing and protecting data, the different types of data[40], and scenarios for data sharing and protection.

4.3 Effects of measures on open science and 'openness-of-science'

A frequently asked question is how to apply the processes keeping an open and cooperative spirit and avoiding administrative burden. As risk management is often mentioned in seminars and debates, one of the respondents indicated that while "risk management can play an important role to keep science open rather than restricting scientists and universities in their choice of topics, their publications, recruitment and partnerships". Framing is increasingly important in this respect. Academic freedom or open science are not necessarily at odds with knowledge security, while it is regularly framed as such. Similarly, raising concerns over academic freedom or discrimination is not necessarily 'naïve'

[40] More in particular: raw data, processed data, aggregated data, structured data, unstructured data, business-data, data incorporating know-how, data created because of regulatory requirements, other content, predominantly machine-generated data, predominantly human-generated data, personal data, non-personal data (EISMEA, 2022)

(although sometimes portrayed as such), also not in the current geopolitical context in which science and technology are increasingly 'securitised'.

As measures may impact open science and 'open-for-science', particular attention is given to their proportionality, implementability, and effectiveness. The next section will address some of the challenges in the day-to-day realities of universities, in relation to (a) research output, (b) recruitment/HR, (c) PhD population and (d) student population. By doing so, it will also explore answers to some of the key questions that came up in Chapter 1.

4.3.1 Do export control, sanctions, and other measures affect international collaboration?

Sanctions and export control are not invoked with the intention to prohibit international scientific cooperation, but may still have some effect in particular situations. Export control regimes typically serve a number of other purposes: wartime controls, delineating trade with an adversary, Weapons of Mass Destruction (WMD) proliferation controls, UN Security Council resolution 1540-based controls to prevent proliferation from and through non-state actors, human security export controls, and strategic competition controls (Stewart, 2023, p. 40-42). International academic cooperation that relates to so-called 'dual-use' technology listed under Regulation 2021/821 is subject to export control, but fundamental research, and knowledge transfer of knowledge that is already in the public domain are generally exempted from such controls.

One can observe quite some variation amongst universities and countries in the uptake of measures: while some take almost no measures, other universities have established, from 2021/2022 onwards, an internal compliance program, developed processes, frameworks, tools, and flowcharts, have awareness campaigns in place and provide support to researchers, support staff and higher management to be compliant with the export control regimes, have established knowledge security advisory teams and regular contact with their chief information security officer (CISO).

The variety amongst universities is not only related to the awareness of (legal and policy advisors within) universities on this topic, but also related to differences amongst universities. While general universities without a strong profile in science & technology typically have fewer departments and activities in relation to (listed) technology, universities of science and technology are typically deeply involved in international cooperation on technology that is listed under Regulation 2021/821. The urgency and incentive for universities of science and technology to have an internal compliance program in place for export control, is therefore much stronger.

One of the challenges is that scientific collaborative projects are not always clearly demarcated at the start and may change during the course of a project. The requested end-uses or end users are also not always clear. Moreover, researchers are not always able to specify the technology under the project as listed or not-listed under Regulation 2021/821, or they can argue that some of the listed technology is used, but not developed. When specific information is required by the authorities, but lacking, the process gets delayed. The response time from the national competent authorities may vary from days to several

months. In several cases with a long processing time, these delays had a chilling effect on international scientific cooperation. Some researchers and legal advisors indicated that the processing times sometimes were so lengthy, that the potential partner or the researchers themselves backed out of their intended research cooperation.

Support from the national and competent authorities can encourage universities with their internal compliance: easy communication channels, clear instructions and a support desk might help, on the one hand, universities to submit the required information without delays, and on the other hand, authorities to process requests faster.

International sanctions are - in general - more easy to apply than export checks thanks to easily accessible tools such as the EU sanctions map and targeted communication[41]. In addition to sanctions and the dual-use regulations as legal principles, the dual-use categories of Regulation 2021/821 are sometimes copied (with adjustments) as 'risk indicators' for other policy measures, such as foreign investment screening, or knowledge security screening, as in the Netherlands. Although some impact on international scientific collaboration, on student and staff mobility, or the recruitment of PHD candidates is inevitable, it is too early to have scientific and quantified evidence on the impact of sanctions and export regimes in the European context[42]. In specific technological domains, some measures are likely to result in additional shortages in terms of attracting students and scientists from non-EU countries (FEPS, 2022, p.3).

4.3.2 Is open science and openness of science restricted? If so, in what way and by whom?

While open science has become the standard within the EU and for research organisations and universities across Europe, we also see that export control regulations are adding to the complexity of implementation. For example, according to Commission Recommendation 2021/1700, the act of publishing research is subject to export control when the content is considered controlled military and dual-use technology. In other words, when parts of the preprint or intended publication are listed in the dual-use Regulation (EU 2021/821), the Commission Recommendations state that the author(s) have to check with the authorities whether an export permit is required, also when it is to be released for (open access) publication.

Export control and knowledge security are not the only barriers to open science: privacy concerns, IP and commercial interests may already limit the realisation of open science. collaboration/co-authorship agreements may be opposed with the terms of reuse of publications. For example, rights retention requirements Plan S and the expectation to share the articles under a Creative Commons licence (CC BY) may be at odds with IP policies at

[41] An exception are the country-specific sanctions on dual-use (and a range of other) technologies that apply to Iran, Syria, the Russian Federation, Belarus, Myanmar and the Democratic People's Republic of Korea (DPRK). These sanctions combine two legislative frameworks, with historically different purposes.

[42] A few publications do show effects of measures in the context of the US and China (Aghion, et al. 2023 and Xie et al. 2023); OECD 2023.

country or university level. This makes it essential that rights and licensing are addressed in collaboration agreements, and/or that IP policies are harmonised across funders and institutions.

Data management plans (DMPs), research integrity tools, or security instructions, may assist researchers to navigate between open science and restrictions on sharing data. For example, projects funded under Horizon Europe 2021-2027 provide researchers with guidance to address security issues through a security scrutiny process.

In everyday practice researchers may receive a more generic 'as closed as necessary' instruction, asking them to be mindful of both IP considerations and security issues. Lack of harmonisation between policies and guidance across different countries but also between related policies within a country needs to be addressed. Specifically, when the complexity of IP hampers open science, harmonisation of IP policies across borders can help, as well as model IP agreements with 'open science' in mind. When commercial interests are of concern, then non-disclosure agreements and other agreements may be honoured with a view to open up science as soon as it is possible. The call for open dissemination of other research outputs (notably, research data as well as infrastructure) from the start and throughout the research cycle is in such scenarios at odds with the drive to commercialise research. As shown by the EISMEA, the two major barriers for sharing data by commercial firms are the risk of losing competitive edge when sharing, and the risk of losing control over one's data (EISMEA, 2022, p. 58).

Data is, however, not the only relevant category. Likewise, open source software and code, measures and instruments, research designs and protocols, lab notebooks and analysis tools may conflict, on one hand, with trade secrets and the exploitation of commercially sensitive results. Sharing software and codes, measures and instruments, international travel with educational material, or foreign access to cloud data, may also conflict with the dual-use regulations.

4.3.3 Is research output affected by export control?

At this moment, dual-use regulations seem to not yet have an effect on research output or publications. Mutually conflicting principles make it difficult to apply the dual-use regulations to the publication process.

In addition to the question whether publications are controlled or de-controlled, it is necessary to know whether any of the exemptions apply: whether it is fundamental research, whether it is already in the public domain, or whether it contains the minimum necessary information for patents. The Commission Recommendation (EU) 2021/1700 on Internal Compliance Programs[43] states: "Presentations or publications will rarely in entirety meet the controlled technology threshold. Some subsections or small excerpts may meet the threshold. Only these parts are licence required if the researcher or research organisation is in need of guidance, they can contact their national competent authority" (European

[43] The Recommendation (EU) 2021/1700 is a legally non-binding document, a tool to assist Universities in setting-up an Internal Compliance Program. Its recommendations apply to the interpretation and implementation of the Dual-use regulation 2021/821 which is legally binding.

Commission, 2021, L338, p. 17). The advice is that, in such a case, the researcher could amend or omit the specific part, or contact the competent authority with an individual licence application for that part of the publication. The recommendation remains, however, unclear about the specific information that is required to meet the threshold. Only that piece of specific technical information is subject to a license at publication if that information is used to develop, produce or use the controlled item. While 'technology' required for the 'production', 'development' and 'use' of classified goods are all defined, 'specific information' is not. One of the key take-aways as formulated by the Commission is that it is very rare that the described technology meets the threshold, or contains information that is specific enough to achieve the "controlled performance levels, characteristics or functions from the dual-use control list" (European Commission, 2021, L338, p. 17).

An additional complicating factor is that most publications are about incremental dual-use research already in the public domain. This creates complexity with regards to efforts to differentiate within a research paper on a dual-use topic what is controlled technology. This then questions the proportionality of applying export control to presentations and publications.

At the same time, the Recommendation' reads that: "The intended act of releasing the (object code for) software or technology in the public domain is not sufficient for becoming de-controlled. That means that a to-be research output (open-source software, publication, conference material) can only benefit from this de-control if the listed dual-use software or technology that it contains is already in the public domain. Hence, the act of releasing without an authorization could be a violation of export controls" (Recommendation (EU) 2021/1700, p. 19). This assumes a check by the author(s) for each preprint to be compliant with the dual-use regulation. With this statement, a challenge presents itself between the authorities, the authors and the publishers with mutually conflicting conditions inherent in the procedures and process for publication (a so-called 'catch 22').

Since the release of the Commission Recommendation (EU) 2021/1700 on Internal Compliance Programs, no further clarification or practical guidance has been issued by the European Commission on publications and presentations. There also has been no European case law that provides tipping points on the challenges as described. The existing and enduring pressure by governments to subject publications to export control has created much internal debate between universities' compliance officers and scientists, delaying the much desired progress on internal compliance.

If no further clarification or easy classification tools[44] are provided to researchers, the national competent authorities (such as the customs office) should have skilled reviewers in place to assess whether pre-prints with dual-use potential contain controlled technology[45]. Scientists are under a high pressure to publish and, with a few exceptions, are not aware of

[44] The TIM dual-use web platform from the EU is an important step in this direction, although researchers are not familiar with this platform. Furthermore, it does not help in defining whether or not the content of the publication meets the dual-use threshold.

[45] Estimates are that around 5.000 - 15.000 publications per university of S&T per year might need a classification. Estimates based on a quick bibliometric analysis by a few universities of science and technology based on their annual publication output. Only a very small percentage is likely to meet the thresholds.

the need to request a classification *before* confirmation by the publisher that it is eligible to be published.

The publisher, on the other hand, is not eager to accept a delay of several months *after* having confirmed a preprint is acceptable for publication. Nor are they eager to leave out sections that make the article most interesting. In general, publishers want to publish scientific output that is as innovative as possible. The most innovative elements on dual-use technology are likely to be the most sensitive, for precisely that reason: it has not yet been published. When the competent authorities suggest removal or adjustment of the most innovative elements, the publisher is more likely to reject the article. Moreover, without a transparent lead in the article on removal or adjustment of research output by the authors (to fulfil the requirements from customs authorities), the research output is not reproducible anymore and lacks scientific rigour.

The recommendations here are in line with the European Export Control Association for Research Organisations (EECARO)[46], that is "to follow the US Export Administration Regulations (EAR) approach in exempting published information and information intended to be published from export controls and to allow for an unrestricted publishing in publicly available scientific journals – print or online - including sharing information with co-authors and reviewers abroad, to enable a smooth and timely peer review process" (EECARO, 25 May 2023, p.2)[47].

If not, then it would be worthwhile to develop a standard and systematic risk assessment together with the EU research community and national or European Policy makers (the EU Coordination Group for Dual-Use Goods), which could be accepted as a new toolkit for publications and presentations as part of a revision of the Commission Recommendation (EU) 2021/1700 on Internal Compliance Programs.

4.3.4 Is recruitment and HR policy affected by screening and visa-vetting measures?

One of the countries that has a security screening in place for students and/or researchers that will study or work on sensitive technologies is the UK, with its Academic Technology Approval Scheme (ATAS scheme). The Netherlands, which already has a measure of supervision in place in relation to North Korea and Iran, is in the process of preparing measures/regulations similar as the ATAS scheme. In both cases a screening is required for students/staff/researchers who want to work on sensitive technology and conditional for granting a visa or residence permit.

The ATAS scheme has recently been evaluated by the Russell Group consisting of 24 UK universities. The Russell Group reports that "severe delays in a pre-visa checking scheme

[46] in their comments to the EU-US Trade and Technology Council' s Export Controls Working Group (WG 7).

[47] One of the frequently asked questions on deemed export addresses this question: "I plan to publish in a foreign journal a scientific paper describing the results of my research, which is in an area listed in the EAR as requiring a license to all countries except Canada. Do I need a license to send a copy to my publisher abroad?" (Bureau of Industry and Security, US Department of Commerce, accessed 1 september 2023)

are endangering research in vital areas such as medicine, engineering and computer science and undermining the UK's science superpower ambitions" (Russell Group, 8 March 2023, more details can be found here).

The potential loss of access to (and thereby the recruitment of) top-scientists in particular technology areas is also a generally felt concern amongst universities in the Netherlands, amongst the universities that have experience with the screening procedures in relation to the knowledge embargo[48] for Iran and North Korea. This procedure was evaluated in 2021 and resulted in a range of recommendations (ABDTOPConsult 2021, p.3).

Some scientists argue that these measures resulted *de facto* in a selective screening process and nationality profiling by vacancy holders. Indeed, researchers from high-risk countries are less likely to receive an invitation from the university than scientists from 'safer countries'. Others scientists deny such an effect. Having insight in criteria for a positive or negative advice will therefore help universities to keep their open character ('open to the world'), to attract top-scientists, and to avoid *de facto* discrimination.

In some technology areas the scientists are predominantly originating from non-EU countries, for instance in the area of semiconductor technology. This would pose another challenge, to find top scientists within Europe or like-minded countries. Another concern that was raised amongst some universities in the UK and in the Netherlands, is the 'waterbed effect'. Without similar measures in other countries of the EU, scientists with non-EU citizenship might move to those countries in the EU, where screening is not required.

France has chosen a different pathway, it chose a set of measures that are referred to as the "Protection of the Scientific and Technical Potential of the Nation (PPST)". Rather than restricting access of researchers and students from other countries to sensitive research domains, it limits the online and physical access to buildings and lab facilities (protected sectors and restrictive access zones) (see also d'Hooghe and Lammertink, 2022). While the procedure is a different one, the procedures for access approval to protected sectors and restrictive access zones also caused delays and loss of PhD candidates in France, as already indicated by Jean-Pierre Damiano (2017) in a publication from the HAL open science on the Protection of the scientific potential and technology of the Nation (Damiano, 2017). In addition, the French government performs a government screening of all international research collaboration contracts.

4.3.5 Is the PhD population affected by visa-vetting procedures or scholarship restrictions?

Ongoing discussions are taking place on restricting the admittance of PhD candidates receiving state-sponsored scholarships when the conditions for these scholarships restrict the personal and/or academic freedoms of these PhD candidates. One example directly affecting Swedish universities was reported in the Swedish mass media in January 2023. While all scholarships and subsidies are subject to particular conditions, some conditions are

[48] This knowledge embargo refers to the screening of all scientific staff and students (in their graduation phase) of a select set of research groups that are considered to have knowledge in-house that can be used for the development and production of missile technology.

believed to affect principles of academic freedom. This is not restricted to one particular country only. Therefore, some universities of S&T have stopped admitting PhD candidates with such scholarships all together, while other universities are looking at a broader spectrum to decide over the acceptance of individual PhDs with such a scholarship, such as the civilian or military nature of their home university, the sensitivity of the technology, the income level compared to legal subsistence minimum, or reports of pressure to abide by the conditions. While in the past 'capacity development' was a motivation in favour of academic cooperation and joint PhD programs, knowledge security is now a motivation against academic cooperation and joint PhD programs with partners in some of these countries.

Scientific and support staff reported a mental effect of security screenings on some of the PhD candidates and scientists, in particular from countries with repressive regimes[49]. At the same time, some students or staff members from repressive regimes are also afraid to talk openly with fellow nationals, especially those who grew up in a culture of distrust and intimidation.

Universities are struggling with these, sometimes conflicting, concerns. They feel pressure to put security over an open academic culture and some feel pressure to avoid the recruitment of excellent scientists from high-risk countries. The culture of trust that has been there at universities is partially eroding and more for some than for others.

The European Commission staff working document 'Tackling R&I foreign interference' recognises this risk, and provides recommendations to address these concerns. It states: "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" (European Commission, 2022, p. 29). It is therefore important for universities of S&T, as for other universities, to recognise their contribution, and to consider the wellbeing of these PhD candidates and colleagues.

4.3.6 How do sanctions and export control affect teaching, instruction and training?

Teaching, instruction and training have become subject of the concept 'technical assistance' in the current dual-use regulation 2100/821. This regulation defines 'technical assistance' as "any technical support related to repairs, development, manufacture, assembly, testing, maintenance, or any other technical service, and may take forms such as instruction, advice, training, transmission of working knowledge or skills or consulting services, including by electronic means as well as by telephone or any other verbal forms of assistance" (art. 2, sub 9). Country-specific international sanctions[50] are applied to dual-use technologies or

[49] Such effects were also reported by some media.

[50] Sanctions may also apply to individuals or to students and staff from sanctioned universities and research organisations. These are not discussed here.

other technologies in specific sectors[51], for citizens from Iran, Russia and Belarus, Syria, North-Korea, and Myanmar under different legal resolutions/regulations and annexes.

It is up to the national competent authorities (NCAs) to determine how to implement this: "The Commission takes the view that the provision of higher education and the undertaking of applied research could fall under the notion of 'technical assistance' as provided by the sanctions regulations. It is for the NCA to determine in each individual case whether the preconditions of the relevant regulations in order for such activities to constitute technical assistance are met, and, if they are, to ensure that the relevant restrictions on the provision of such technical assistance are respected" (Commission Opinion, C(2019) 5883 final, 5 August 2019).

A supreme court in the Netherlands already ruled in December 2012, that universities in the Netherlands could no longer refuse admittance to Iranian nationals who might come into contact with nuclear expertise (Hoge Raad, 14 December 2012). In the Dutch situation, this makes it complex for universities to understand whether they are expected by the EU or their national authorities to ban students with particular nationalities from particular classes, courses or studies to avoid they might come into contact with specific technology, when a national court has ruled that an example of such an activity is illegal.

4.4 Securitisation

The security discourse in relation to science and technology has another effect. Countries in parts of Europe have a history of being subject to security measures (such as large parts of Eastern Europe before 1989); when the activities of foreign staff and students, as well as opponents, were closely monitored. This history also provides lessons for the future as does even more modern history in other parts of the world.

In a workshop on 'the role of universities in promoting democracy' (29 sept. 2022, Utrecht, Netherlands), one of the speakers explored a neo-nationalist trend that has emerged during the last decade and analysed how today's right-wing populist movements and authoritarian governments are threatening higher education (Douglass, 2021). Douglass used comparative case studies with China, Hong Kong and Singapore, Russia, Turkey, Poland, Hungary, Germany, Netherlands, Denmark, the UK, the US and Brazil to provide a conceptual framework for analysis.

[51] Russian Federation: dual-use technology (Annexes II, VII, X, XI, XVI, XXI en XXIII to Regulation (EU) 833/2014, version 05/02/2023), oil refinery and energy sector, aviation and aerospace, maritime navigation technology, IT and IT consulting services, financial assistance, investments, loans; Belarus: dual-use technology, defence and security (Annex Va of Regulation (EC) 765/2006, version 28/02/2023), machinery and electrical equipment, financial assistance, investments and loans. Myanmar: dual-use technology, technology that can be used for internal repression, telecommunications and interception equipment. Iran: dual-use technology (Annex II to Regulation 267/2012, version 29/06/2022), proliferation sensitive nuclear activities, enterprise resource planning software (described in Annex VIIA to Council Regulation 267/2012), designed for use in nuclear and military industries. Syria: equipment or technology as listed in Annex VII of Council Regulation (EU) No 36/2012; construction of new power plants, equipment and technology that can be used for internal repression, telecommunication and interception equipment. North Korea: too much to be listed here. Based on lists accessed 3 june 2023. This list is not exhaustive and can change any time.

He observes how 'anti-immigrant sentiments, anti-international students, anti-globalism and spreading doubts about the value of Higher Education' are signs of nascent populist movements or political parties, and - based on the analysis of this list of countries - identifies which measures are likely to be present under nascent populists movements, under nationalist leaning governments, illiberal democracies or authoritarian regimes.

The restriction on student and faculty visas, an increased focus on IP and national security, threats to reduction in funding and restrictions on international cooperation are manifest in some of the mentioned countries, and some EU member states, with a more nationalist-leaning government.

Based on experiences and case studies from these countries, he concludes that "the national political history and contemporary context is the dominant factor for shaping the role of universities in society" (Douglass, 2022). They are operating within a spectrum of a national and geopolitical environment in which neo-nationalist parties, movements or governments are becoming more dominant[52]. In various member states of the EU one can see some manifestations of anti-globalism, anti-internationalisation, or populist movements casting doubts about the value of higher education and scientific research. Scientists are sometimes at risk, as became even more clear during the COVID pandemic when several virologists received death threats.

Not only domestic groups are looking for information about individual scientists. Foreign entities might also be interested in the data that are collected for (national) security reasons, or in ongoing discussions across and between universities and authorities. Proper safeguards (IT, cybersecurity, encryption, GDPR, authorisation, authentication, communication) to protect relevant communication are therefore increasingly important.

The line between passive and active monitoring or reporting is, however, very thin. Universities are aware of their role and responsibilities - in line with the Magna Charta Universitatum - and the autonomy needed for universities in relation to political and economic considerations. Both universities and authorities have a role in the protection of democratic and academic values and to be alert for efforts to undermine democracy.

The (side-) effects of some policy instruments are critically questioned by some researchers and staff members, in particular when such measures are deemed to go against some academic[53] or democratic values. It is especially because of this, that an open dialogue between universities and authorities to anticipate and mitigate any potential side-effects of

[52] One example being a right-wing political party in the Netherlands that opened a "left-wing indoctrination hotline for students who suspect left-wing political bias on their campus" during the provincial election campaign of 2019 (van der Wende, in Douglass, 2021, p. 129). The same party won the provincial elections in that year.

[53] E.g. The Guild (a network of universities), the Swedish Rectors Association and the Association of Swedish Higher Education Institutes protested in 2023 against "Swedish government's decision to shorten the terms of office of the external members of Swedish university boards from three years to 17 months. This action, taken to enable the government to make direct appointments of security experts to the Boards of Swedish universities, circumvents a well-established process to ensure a proper, careful balance between the government's right to overview public universities, and the institutional autonomy and self-governance necessary to ensure academic freedom in the pursuit of knowledge". (The Guild, 15 May 2023)

security measures[54]. The side-effects of security measures are not born out of naivety (as it is sometimes argued) but out of serious and carefully considered concerns.

Such a dialogue will strengthen the effectiveness of, and support, for security measures. In the context of increased securitisation, universities also receive advice or requests from the authorities. Universities can benefit from expertise and intelligence of the authorities, and vice-versa. In some countries, a front office is created to support universities with their questions, or meetings are arranged with security officers (AWTI, 2022).

[54] For example, when universities in one of the member states were recently asked 'whether they keep an overview of staff, guests and guest-researchers that form a risk in terms of knowledge security' and whether they keep 'a central overview of students and staff from high risks countries', they declined with reference to their core responsibility, their compliance with GDPR and to avoid nationality profiling.

Chapter 5. Keeping science open? Conclusions and recommendations

The previous chapters have elaborated a complex set of factors, dimensions and instruments that play a role in making sure that science is 'as open as possible, as restricted as necessary'.

We started with the changed geopolitical landscape, and concluded with a positioning of knowledge security in historic context and potential safety risks for students and scientists. Based on the analyses in previous chapters, we can observe that:

1. Export control, sanctions, and other knowledge security measures are starting to have an effect, in particular on human resources, choice of partnerships, external funding and on some of the operational processes in universities of science & technology. These effects are more visible in some countries than in others, and depend on the domain, the technologies involved, the type of university, and the type of collaboration. The lack of policy-relevant data and comparative studies makes it difficult to generalise on the impact of measures.

2. Open access publications, open data and/or FAIR data are, at present, only in a minor way affected by export control and other knowledge security measures. Other aspects - such as IP and trade secrets, research integrity, data sovereignty, benefit sharing, or administrative burden - play a more prominent role for open data and/or FAIR data. As the example of Digital Sequencing of genome Information showed, a simplistic trade-off between 'closed' and 'open' is therefore neither helpful nor realistic.

3. The recruitment of scientists and students is mostly affected in those countries that have a security-screening related to particular topics or research groups. Although not intentional, this results according to some, in *de facto* discriminatory practices at the level of universities.

4. The admittance of PhD students is gradually affected through screening, visa-vetting procedures and debates about PhDs coming in with state-sponsored scholarships.

5. Sanctions and export control (and country-specific sanctions on dual-use technology) are not affecting teaching, instruction and training much yet, as the scenarios to which this applies are very specific. Furthermore, there is a lack of guidance by authorities on the legal interpretation of these measures, and universities are reluctant to take measures that require monitoring of individuals or that are likely to result in *de facto* discrimination.

Previous chapters also show how open science is affected in the day-to-day reality of universities.

Government measures are differentially impacting universities. This is due to the diverse nature of universities and the type of measures involved. There is some controversy around such measures, as universities (and scientists) recognise the need for research security, but

are also afraid of limits to their institutional autonomy, the effect on academic freedom, and the impact on their core-business and operational processes.

This is more so when they have not been engaged early in the design process, or when they have concerns about the lack of resources (funding, human resources, ICT systems), both for their own institute or the competent authorities. A robust process for design, implementation, and resourcing, is therefore key for the success of new measures. (see recommendation 1 and 2 for national authorities).

The changes of the geopolitical situation show that the EU, its member states, and universities and research organisations should take a proactive approach. To avoid confusion about the commitment to open science and the openness of science (reiterated over and again by the European Commission), efforts of the relevant Directorates-General to discuss the impact of the global approach with representatives of scientific and university networks is well appreciated and should continue (recommendation 1 for the EU).

The openness of science to scientists from non-European countries will be more restricted in case of screening and visa vetting procedures, or with measures that restrict the inflow of (PhD) students and staff from non-EU countries on sensitive technologies. While this is in line with the EU global approach, it might have negative side-effects, in particular when these procedures are causing long delays and uncertainty. Earlier screening measures have shown that in case of long delays and uncertainty, the risk of *de facto* discrimination increases, in particular to applicants from certain high-risk countries. Another side-effect that has been mentioned multiple times by scientists (e.g. in public debates, round tables, seminars or workshops on knowledge security), is that excellent researchers from non-EU countries start to apply elsewhere in or outside Europe, where such measures do not (yet) exist. A coordinated European approach would be helpful to avoid the ‘waterbed’ effect. (recommendation 2 for the EU)

One of the measures that has had little impact until now - for reasons as described in chapter 4 – but has the potential to affect the scientific process significantly and negatively, is the suggestion in Recommendation (EU) 2021/1700 that scientific presentations, publications and seminars and conferences on dual-use items are potentially subject to export control with the conditions and exceptions as discussed. The uncertainty thus created, affects universities in their core-business and operational processes; it reflects a significant future barrier for (open) scientific processes. After all, as confirmed by the authors in the same Recommendation (EU) 2021/1700, it is very rare that a publication meets the export control thresholds in its entirety. Exemption of export control on publications and presentations - in combination with a helpdesk for researchers who want to avoid misuse of their knowledge - is expected to be more effective and proportionate (recommendation 3 for the EU).

Alternatively, a standard and easy-to-use risk assessment and classification tool is required, to be developed together with the EU research community and the EU Coordination Group for Dual-use Goods. By accepting this new tool as part of a revision of the Commission Recommendation (EU) 2021/1700 on Internal Compliance Programs - the open scientific

process is less at risk. The TIM Dual-use tool might be instrumental in the development of such a tool. (recommendation 3 for the EU).

Open science (and its elements) is both facilitated and restricted through policy and regulatory measures from national authorities and the EU, for example in the area of data, data governance, open science, digital services and cybersecurity. The European Commission reiterates in almost all its publications its commitment to the openness of trade and the openness of science. The mix of measures, policies, practices and legal requirements as described in this paper, makes it a challenge for researchers, support staff and management at universities to navigate between 'as open as possible' and 'as restricted as necessary'. A help desk for researchers and universities could be helpful for universities to grasp the complexity of these regulations in relation to each other and particularly in relation to how authorities envision their implementation (including when thresholds are considered met) and to assist universities with choices to keep science as open as possible. It could also help individual researchers and support staff of universities who have concerns that their knowledge or international collaboration can be misused (recommendation 4 EU). The collection of policy-relevant data and comparative studies can shed more light on how export control and knowledge security policies impact operational processes of universities. (recommendation 5 for the EU).

Open science (and its elements) is further affected by operational practices and policy conditions from the university. Reviewing existing practices and procedures, e.g. with regard to pre-employment screening, data management, research integrity, risk management and/or contract management, provide entries for universities to balance open science more naturally and more structurally with knowledge security.

Open science and openness of science is differentially affected by measures on knowledge security or export control within universities. Sometimes these measures are not in line with, or informed by, other university policies. A clear positioning of universities on openness, transparency, security, freedom and integrity, the alignment of the relevant policies, accompanied with the right tools and instruments, will help scientists, support staff and management to align and communicate their policies more clearly (recommendation 1 for universities).

Research integrity and data management are both examples that would support knowledge security at the level of individual researchers. By adhering to the European code of conduct on research integrity (ALLEA) and by encouraging the use of data management plans, researchers will be guided to make informed choices on 'as open as possible' and 'closed or restricted when necessary' (recommendation 2 and 3 for universities).

Open science (and its elements) is differentially restricted by existing instruments in the commercial sector to protect confidentiality, IP clauses and other measures to safeguard future commercialisation. The access to data, technology, equipment, infrastructure and IT, can also be restricted through technical (security) measures or technical safeguards. Exchanging views with relevant partners in the commercial sector (including toolboxes used) is an interesting way for universities to further expand and professionalise their services

related to knowledge or research security, due diligence, data protection, IP, and export control. (recommendation 4 for universities)

The discourse on knowledge security, on strategic autonomy and technological sovereignty, and the framing of countries, actors, and science, are manifestations of the further securitisation of science and technology. This requires extra attention for the impact of measures on individual researchers and personal freedoms (recommendation 1 on securitisation). It also requires attention for the cybersecurity of the collection and transfer of sensitive data on persons and procedures (recommendation 2 on securitisation). The recommendations mentioned above are summed up below.

5.1 Recommendations for national authorities

1. Formulate the necessary pre-conditions for effective implementation, before measures enter in-force: ensure sufficient (human, financial, technical, digital) resources by the authorities, ensure the quality of the process and engagement of implementing authorities, encourage support from universities and university networks, ensure flexibility and robustness and share good practices. Avoid the creation of 'autonomy traps' [55]. Take adequate measures and funding - both for the implementing authorities and the universities - to ensure these conditions over a longer period of time.

2. Given the potential impact on the core business of universities and in order to avoid a trade-off between fundamental rights, conduct early impact assessments and a risk analysis at the design-stage of policies and regulatory changes. Be explicit about the underlying assumptions, uncertainties and potential ambiguities. Make sure there is sufficient time for adjusting policies and regulatory changes based on the findings of these risk analyses and early impact assessments.

5.2 Recommendations for the EU institutions

1. Advance the global approach based on strategic, open, reciprocal towards a global framework for science & technology cooperation. Discuss with representatives of university and scientific networks, what this means for open science and the openness of science, departing from guiding principles previously outlined.

2. Measures that affect the inflow of (PhD) students and staff, should be taken at EU level to avoid undesirable ('waterbed') effects amongst member states.

3. On export control: three options are identified:

[55] Autonomy traps are situations "in which universities may seem to be autonomous but are not provided the resources and the means to effectively exercise it, or are encumbered with autonomy and responsibilities in areas not related to their core mission" (Björnmalm in Science Business, 27 June 2023)

a. Continue with business as usual without further adjustments. All publications that might include specific information on dual-use topics are subject to checks on export controls in the preprint phase of a project. All NCAs responsible for implementation discuss the criteria for (de)controls on publications with the higher education sector in their country.

b. (Preferred option) Scientific publications rarely meet the threshold criteria from the dual-use regulation. Therefore, follow the US Export Administration Regulations (EAR) approach in exempting published information and information intended to be published from export controls and to allow for an unrestricted publishing in publicly available scientific journals – print or online - including sharing information with co-authors and reviewers abroad, to enable a smooth and timely peer review process and thereby keep science open (EECARO) (see recommendation 4 under 5.3)

c. Alternatively (that is: if 3b is not acceptable) develop a standard and easy-to-use risk assessment or classification tool together with the EU research community and the EU Coordination Group for Dual-use Goods. This new toolkit should become part of a revision of the Commission Recommendation (EU) 2021/1700 on Internal Compliance Programs - both for publications and presentations.

4. Create a help desk for researchers, reviewers and publishers to provide guidance on the regulatory context, and provide support to those who have concerns about the potential (mis)use of their knowledge or publications. The intention to create a virtual academy and toolkit on research security are welcome.

5. Support the collection of policy-relevant data and comparative studies, to shed more light on the question how export control and knowledge security policies impact universities' operational processes.

5.3 Recommendations for universities and research organisations:

1. Openness, transparency, security, freedom and integrity are crucial elements for responsible internationalisation, in particular when the internationalisation of higher education is contested in the political debate (see also Van de Walle, 2023). Position the university vis-a-vis these principles or values. Be explicit about any trade-offs if and when they emerge. Use this program to balance and clarify decisions.

2. Push for transparency and other good practices of research integrity by researchers in their research processes in order to keep science open. As a university, develop incentives, training and communication that facilitate the take-up of the European code of conduct on research integrity.

3. Encourage the use of adequate data management plans amongst all scientists as these encourage the scientist to think carefully about the protection and openness of

data. There are several tools available, including the EOSC-Pillar Guidelines for Legal Compliance of Researchers, that are valid for all EU member states.

4. Ask author(s) in the regular research cycle (for example as part of their data management plan), whether they consider that specific information, or underlying data, may be likely to be used by embargoed or sanctioned countries, end-users, for prohibited end-uses. Such due diligence should be done in an early phase of a research project. If so, take appropriate measures.

5. To foster a culture of responsible internationalisation, emphasize the importance of institutional peer learning. Exchange views with, and learn from, the commercial sector. This can substantially enrich the 'toolbox' currently available.

5.4 Recommendations for all stakeholders in the light of increased securitisation

1. Take mitigating measures to assure that individual researchers or students, and academic freedom, will not be at risk. In this light, also discuss the risks related to monitoring, screening, registration and possible violation of personal freedoms.

2. Push for adequate measures for cybersecurity for all communication, collection, and processing of data in the light of new measures (both for universities and authorities). Protect personal data (adhere to the GDPR) and ensure sufficient IT security measures / cybersecurity on information and data provided by students, researchers, universities and research organisations to the authorities.

List of resources

Literature

Advisory Council for Science, Technology and Innovation (2022). *Knowledge in conflict: striking a balance between security and liberty*. https://www.awti.nl/documenten/adviezen/2022/11/29/advice-knowledge-in-conflict

Anderson, J., (2022). *Europe needs high-tech talent* (Foundation for European Progressive Studies Policy Brief July 2022). https://feps-europe.eu/wp-content/uploads/2022/07/Final_6.7.22_Europe-needs-high-tech-talent.pdf

Baker, L., Cristea, I., Errington, T., Jaśko, K., Lusoli, W., MacCallum C. J., Parry, V., Pérignon, C., Šimko, T., Winchester, C. (2020). *Reproducibility of scientific results in the EU : scoping report*. Publications Office of the European Union. https://data.europa.eu/doi/10.2777/341654

Barker, M., Manola, N., Gaillard, V., Kuchma, I., Lazzeri, E., Story, L. (2021). *Digital skills for FAIR and Open Science: report from the EOSC Executive Board Skills and Training Working Group*. Publications Office of the European Union. https://doi.org/10.2777/59065

Bateman, J. (2022). *US-China technological "decoupling": a strategy and policy framework.* Carnegie Endowment for International Peace. https://carnegieendowment.org/files/Bateman_US-China_Decoupling_final.pdf

Bauer, M. (2022). The Impacts of EU Strategy Autonomy Policies – A Primer for Member State. *ECIPE Policy Brief 09/2022*, 1-34. https://ecipe.org/publications/eu-strategy-autonomy-policies-impact/

Bjerkem, J., Harbour, M. (2020). *Europe as a global standard-setter: The strategic importance of European standardisation* (Discussion Paper). European Policy Center. https://www.epc.eu/content/PDF/2020/EPE_JB_Europe_as_a_global_standard-setter.pdf

Brown, A. (2022). *What's next for national security and research?* (HEPI Report 147). Higher Education Policy Institute. https://www.hepi.ac.uk/wp-content/uploads/2022/02/Whats-next-for-national-security-and-research_HEPI-Report-147.pdf

Bundesverband der Deutschen Industrie (2022). *Comparison and experiences US vs. EU Chips Act: 11 lessons from the US Chips Act for the EU Chips Act.* https://issuu.com/bdi-berlin/docs/20221118_position_bdi_comparison_us_eu_chips_act

Buzan, B., Wæver, O., de Wilde, J. (1998). *Security: A New Framework for Analysis.* Lynne Riever Publishers.

CESAER (2020). *Next generation metrics.* https://www.cesaer.org/content/5-operations/2020/20200610-white-next-generation-metrics.pdf

CESAER, Royal Academy of Engineering (2022). *Key Technologies Shaping the Future.* https://doi.org/10.5281/zenodo.5865414

Curaj, A., Deca, L., Pricopie, R. (eds) (2018). European Higher Education Area: The Impact of Past and Future Policies. Springer, Cham. https://doi.org/10.1007/978-3-319-77407-7

Damiano, J-P. (2017). Protection of the scientific potential and technology of the Nation: utopia or reality to find the right balance: foster innovation, protect knowledge. *URSI-France Workshop Radio Science for Humanity 2017*. https://hal.science/hal-01639556

Douglass, J.A. (2021). *Neo-nationalism and Universities*: *Populists, Autocrats, and the Future of Higher Education*. Johns Hopkins University Press., doi:10.1353/book.85165.

d'Hooghe, I., Lammertink, J. (2022). How National Governments and Research Institutions Safeguard Knowledge Development in Science and Technology. Leiden Asia Centre and AWTI. https://leidenasiacentre.nl/publication-how-national-governments-and-research-institutions-safequard-knowledge-development-in-science-and-technology

European Commission, Directorate-General for Research and Innovation, (2021). *Towards a reform of the research assessment system: scoping report*. Publications Office of the European Union. https://data.europa.eu/doi/10.2777/707440

European Commission, Directorate-General for Research and Innovation, (2022). *Open science and intellectual property rights: How can they better interact? : state of the art and reflections : executive summary*, Publications Office of the European Union. https://data.europa.eu/doi/10.2777/347305

European Commission, European Innovation Council and SMEs Executive Agency (2022). *Study on the legal protection of trade secrets in the context of the data economy: final report.* Publications Office of the European Union. https://data.europa.eu/doi/10.2826/021443

European Parliamentary Research Service (2020*). On the path to 'strategic autonomy': the EU in an evolving geopolitical environment* (PE 652.096). https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652096/EPRS_STU(2020)652096_EN.pdf

European University Association (2021). *Research and innovation as drivers of open international cooperation: EUA response to the European Commission Communication on a Global Approach to Research and Innovation.* https://eua.eu/downloads/publications/policy%20input_global%20approach.pdf

Frontier Economics (2022). Measuring the impacts of the European Union's approach to open strategic autonomy. https://ecipe.org/wp-content/uploads/2022/11/Strategic-Autonomy-Impacts.pdf

Global science must not be treated as a diplomatic pawn. (2022). *Nature 612*(7941), 589–590. https://doi.org/10.1038/d41586-022-04477-8

Gownaris, NJ, Vermeir, K, Bittner, M-I, Gunawardena, L, Kaur-Ghumaan, S, Lepenies, R, Ntsefong, GN and Zakari, IS. 2022. Barriers to Full Participation in the Open Science Life Cycle among Early Career Researchers. Data Science Journal, 21: 2, pp. 1–15. DOI: https://doi.org/10.5334/dsj-2022-002

Hodson, Jones et al. (2018). *FAIR Data Action Plan: interim recommendations and actions from the European Commission Expert Group on FAIR data*. https://doi.org/10.5281/zenodo.1285290

Institute for Security & Development Policy (2018). *Made in China. Backgrounder June 2018.* https://isdp.eu/content/uploads/2018/06/Made-in-China-Backgrounder.pdf

Matei, L., Iwinska, J. (2018). Diverging Paths? Institutional Autonomy and Academic Freedom in the European Higher Education Area. In: Curaj, A., Deca, L., Pricopie, R. (eds) European Higher Education Area: The Impact of Past and Future Policies. Springer, Cham. https://doi.org/10.1007/978-3-319-77407-7_22

Molloy, L., Nordling, J., Grootveld, M., van Horik, R., Whyte, A., Davidson, J., Herterich, P., Martin, I., Méndez, E., Principe, P., Vieira, A., & Asmi, A. (2020). D3.4 Recommendations on practice to support FAIR data principles (1.1). Zenodo. https://doi.org/10.5281/zenodo.5357329

Netherlands Institute of International Relations Clingendael (2021). *Technologische samenwerking met China: risico's voor en belangen van Nederland op de terreinen halfgeleiders, fotonica en medicijn-/vaccinontwikkeling*. https://www.clingendael.org/sites/default/files/2021-11/Rapport_Technologische_samenwerking_met_China.pdf

NATO Science & Technology Organization (2020). *Science & technology trends 2020-2040: exploring the S&T edge*. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf

Pannier, A. (2022). *Critical technologies and industrial capabilities: national definition and policy implications. The French case* (Comment #78). Armament Industry European Research Group. https://www.iris-france.org/wp-content/uploads/2022/09/ARES-78-Comment.pdf

Patrahau, I., Singhvi, A., Rademaker, M., van Manen, H., Kleijn, R., van Geuns, L. (2020). *Securing critical materials for critical sectors: policy options for the Netherlands and the European Union.* The Hague Centre for Strategic Studies. https://hcss.nl/wp-content/uploads/2021/01/Securing-Critical-Materials-for-Critical-Sectors.pdf

Patrahau, I., van Manen, H., de Feijter, T., Rademaker, M. (2020). *Standards for critical raw materials: strategic standard setting in China, the EU and the Netherlands.* The Hague Centre for Strategic Studies. https://hcss.nl/wp-content/uploads/2021/01/Standards-for-Critical-Raw-Materials.pdf

Scholz, A.H., Freitag, J., Lyal, C.H.C. et al. (2022). Multilateral benefit-sharing from digital sequence information will support both science and biodiversity conservation. *Nat Commun* 13, 1086. https://doi.org/10.1038/s41467-022-28594-0

Science|Business (2023). *Strategic autonomy: A guide for the perplexed*. https://sciencebusiness.net/report/strategic-autonomy-guide-perplexed

SPARC Europe (2021). *An Analysis of Open Science Policies in Europe, v7*. Zenodo. https://doi.org/10.5281/zenodo.4725817

Stewart, I. (2023). Export Controls in an era of strategic competition: implications for the existing landscape and the need for a new multilateral trade review regime. *Strategic Trade Review 9*(10), 37-50.

Störmer, E., Muench, S., Vesnic-Alujevic, L., Vesnic-Alujevic, L., Scapolo, F., Cagnin, C. (2021). *Shaping and securing the EU's open strategic autonomy by 2040 and beyond* (European Commission Joint Research Centre Science for Policy Report). Publications Office of the European Union. https://data.europa.eu/doi/10.2760/877497

Teleanu, S. (2021). The geopolitics of digital standards: China's role in standard-setting organisations. DiploFoundation/Geneva Internet Platform and Multilateral Dialogue Konrad Adenauer Foundation Geneva. https://www.diplomacy.edu/wp-content/uploads/2021/12/Geopolitics-of-digital-standards-Dec-2021.pdf

Wilkinson, M., Dumontier, M., Aalbersberg, I. et al. (2016). The FAIR Guiding Principles for scientific data management and stewardship. *Sci Data* 3, 160018. https://doi.org/10.1038/sdata.2016.18

OECD (2023), *OECD Science, Technology and Innovation Outlook 2023: Enabling Transitions in Times of Disruption*, OECD Publishing, Paris, https://doi.org/10.1787/0b55736e-en

Policy documents

All European Academies (ALLEA) (2023). *The European Code of Conduct for Research Integrity* (revised edition 2023). https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/european-code-of-conduct-for-research-integrity_horizon_en.pdf

Coalition for Advancing Research Assessment (2022). *Agreement on reforming research assessment.* https://coara.eu/app/uploads/2022/09/2022_07_19_rra_agreement_final.pdf

European Higher Education Area Rome 2020 (2020). *Rome Ministerial Communiqué, 19 November 2020*, https://www.ehea.info/Upload/Rome_Ministerial_Communique.pdf

European Higher Education Area Rome 2020 (2020). *Rome Ministerial Communiqué, Annex I*, https://www.ehea.info/Upload/Rome_Ministerial_Communique.pdf

European Commission (2016). *Open Innovation, Open Science, Open to the World. A vision for Europe*. Publications Office of the European Union, https://ec.europa.eu/newsroom/dae/redirection/document/16236

European Commission (2019). Commission opinion of 5.8.2019 on a request for interpretation concerning the provision of higher education and the undertaking of applied research in the framework of a prohibition to provide technology or technical assistance to a third country (C(2019) 5883 final). https://finance.ec.europa.eu/system/files/2020-01/190805-opinion-technical-assistance-prohibition_en.pdf

European Commission (2019). *Open Science*, https://research-and-innovation.ec.europa.eu/system/files/2019-12/ec_rtd_factsheet-open-science_2019.pdf

European Commission (2021). C*ommunication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Global Approach to Research and Innovation: Europe's strategy for international cooperation in a changing world*, COM(2021) 252 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2021:252:FIN

European Commission (2021). C*ommunication from the Commission to the European Parliament and the Council: 2021 Strategic Foresight Report*, COM(2021) 750 final. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2021:750:FIN

European Commission (2022). C*ommunication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Roadmap on critical technologies for security and defence*, COM(2022) 61 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022DC0061

European Commission (2022). *Horizon Europe (HORIZON), Euratom Research and Training Programme (EURATOM), General Model Grant Agreement EIC Accelerator Contract* (Version 1.1).

European Commission (2023). *Annotated Grant Agreement. EU Funding Programmes 2021-2027* (Version 1.0).

European Commission (2023). *Joint communication to the European Parliament, the European Council and the Council on "European economic security strategy"* (JOIN/2023/20 final). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023JC0020

European Commission, Directorate-General for Migration and Home Affairs and Directorate-General for Research and Innovation (2021). *Guidance note — Potential misuse of research*,

https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/guidance-note-potential-misuse-of-research-results_he_en.pdf

European Commission, Directorate-General for Research and Innovation (2016). *H2020 Programme Guidelines on FAIR Data Management in Horizon 2020* (Version 3.0), 26.7.2016. https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf

European Commission, Directorate-General for Research and Innovation (2021). *European Research Area policy agenda: overview of actions for the period 2022-2024*. Publications Office of the European Union. https://doi.org/10.2777/52110

European Commission, Directorate-General for Research and Innovation (2022). *Tackling R&I foreign interference – Staff working document*. Publications Office of the European Union, https://data.europa.eu/doi/10.2777/513746

European Council (2023). *European Council meeting (29 and 30 June 2023) – Conclusions* (EUCO 7/23). https://data.consilium.europa.eu/doc/document/ST-7-2023-INIT/en/pdf

European Parliament (2023). *Parliamentary question E-002069/2023(ASW): answer given by Executive Vice-President Vestager on behalf of the European Commission*. https://www.europarl.europa.eu/doceo/document/E-9-2023-002069-ASW_EN.html

European Research Council Executive Agency (2017). *European Research Council (ERC) guidelines on implementation of open access to scientific publications and research data in projects supported by the European Research Council under Horizon 2020* (Version 1.1). https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/oa-pilot/h2020-hi-erc-oa-guide_en.pdf

French Presidency of the Council of the European Union (2022). *Marseille declaration on international cooperation in research and innovation (R&I)*. https://presidence-francaise.consilium.europa.eu/media/xi1khxzg/marseille-declaration.pdf

Germany's Presidency of the Council of the European Union (2020). *Bonn Declaration on Freedom of Scientific Research, adopted at the Ministerial Conference on the European Research Area on 20 October 2020 in Bonn*, https://www.bmbf.de/bmbf/shareddocs/downloads/files/_drp-efr-bonner_erklaerung_en_with-signatures_maerz_2021.pdf?__blob=publicationFile&v=1

Ministerie van Buitenlandse Zaken (2021). *Betreft Evaluatie en voortgang verscherpt toezicht op studenten en onderzoekers in gevoelige onderwijs- en onderzoeksgebieden.* https://open.overheid.nl/documenten/ronl-3aa28a42-d873-4d54-9e4b-818f1253ff34/pdf

Observatory Magna Charta Universitatum, Magna Charta Universitatum 2020, https://www.magna-charta.org/magna-charta-universitatum/mcu2020

Overheid.nl (2022). *Besluit toepassingsbereik sensitieve technologie.* https://www.internetconsultatie.nl/sensitievetechnologievifo/b1

UNESCO (2021). *UNESCO Recommendation on Open Science*, https://unesdoc.unesco.org/ark:/48223/pf0000379949#:~:text=For%20the%20purpose%20of%20this,sharing%20of%20information%20for%20the

Russell Group, Universities UK International, UK Council for International Student Affairs, Universities & Colleges Employers Assocation (2023). *Sector letter on ATAS March 2023*. https://russellgroup.ac.uk/media/6124/joint-letter-atas-010323.pdf

The Guid (2023). *The Guild supports Sweden's Rectors in defence of Academic Freedom and Institutional Autonomy.* https://www.the-guild.eu/publications/statements/the-guild-supports-sweden%E2%80%99s-rectors-in-defence-of-academic-freedom-and-institutional-autonomy.pdf

Universiteiten van Nederland (2022), *National knowledge security guidelines. Secure international collaboration*, https://open.overheid.nl/documenten/ronl-5379d1b4f8b9784bf518251032507a965be9c92d/pdf

U.S. Department of Commerce, Bureau of Industry and Security (2018). *Review of controls for certain emerging technologies: a proposed rule by the Industry and Security Bureau on 11/19/2018*. National Archives. https://www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies

U.S. Department of Commerce, Bureau of Industry and Security (2022). *Implementation of Additional Export Controls: Certain Advanced Computing and Semiconductor Manufacturing Items; Supercomputer and Semiconductor End Use; Entity List Modification*. https://www.bis.doc.gov/index.php/documents/product-guidance/3182-2022-10-28-bis-written-presentation-public-briefing-on-advanced-computing-and-semiconductor-manufacturing-items-rule/file

Legal instruments and jurisprudence

Commission Recommendation (EU) 2021/1700 of 15 September 2021 on internal compliance programmes for controls of research involving dual-use items under Regulation (EU) 2021/821 of the European Parliament and of the Council setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items, OJ L 338, 23.9.2021

Common Military List of the European Union adopted by the Council on 20 February 2023, OJ C 72, 28.2.2023

Council Regulation (EC) 765/2006 of 18 May 2006 concerning restrictive measures in view of the situation in Belarus and the involvement of Belarus in the Russian aggression against Ukraine. OJ L 134, 20.5.2006.

Council Regulation (EU) No 36/2012 of 18 January 2012 concerning the restrictive measures in view of the situation in Syria and repealing Regulation (EU) No 442/2011. OJ L 16, 19.1.2012.

Council Regulation (EU) No 267/2012 of 23 March 2012 concerning restrictive measures against Iran and repealing Regulation (EU) No 961/2010. OJ L 88, 24.3.2012.

Council Regulation (EU) No 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilizing the situation in Ukraine. OJ L 229, 05.02.2023.

ECLI:NL:HR:2012:BX8351, Case number 11/03521 Hoge Raad 2012, https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:HR:2012:BX8351

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

Grey literature / websites / other sources

Center for Open Science. *Open Science*. https://www.cos.io/open-science

CESAER (2020), *Balancing 'as open as possible' and 'as closed as necessary'*. https://www.cesaer.org/news/balancing-as-open-as-possible-and-as-closed-as-necessary-758

Council of the European Union (2021). *New Pact and governance structure for the European Research Area (ERA)*. https://www.consilium.europa.eu/en/press/press-releases/2021/11/26/new-pact-and-governance-structure-for-the-european-research-area-era

DSI Scientific Network. *Get informed about DSI and global policy developments.* https://www.dsiscientificnetwork.org/resources

DSI Scientific Network (2022). *DSI Scientific Network - CBD COP15 Outcome Statement*. https://www.dsiscientificnetwork.org/elementor-4601

European Commission, *An EU approach to enhance economic security*. https://ec.europa.eu/commission/presscorner/detail/en/IP_23_3358

European Commission, EU sanctions map. https://sanctionsmap.eu

European Commission. *European Chips Act*. https://digital-strategy.ec.europa.eu/en/policies/european-chips-act

European Commission, *Open access*. https://research-and-innovation.ec.europa.eu/strategy/strategy-2020-2024/our-digital-future/open-science/open-access_en

European Commission, *Open science*. https://research-and-innovation.ec.europa.eu/strategy/strategy-2020-2024/our-digital-future/open-science_en

European Commission. *Overview of sanctions and related resources*. https://finance.ec.europa.eu/eu-and-world/sanctions-restrictive-measures/overview-sanctions-and-related-resources_en

European Commission (2021). *Strengthened EU export control rules kick in*. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_4601

European Commission (2021). Commission welcomes approval of the Pact for Research and Innovation in Europe and future governance of the European Research Area. https://ec.europa.eu/commission/presscorner/detail/en/IP_21_6270

European Commission, Directorate-General for Research and Innovation. Open Science monitor. https://research-and-innovation.ec.europa.eu/strategy/strategy-2020-2024/our-digital-future/open-science/open-science-monitor_en

European Commission, Directorate-General for Research and Innovation. *Past research and innovation policy goals*. https://research-and-innovation.ec.europa.eu/strategy/past-research-and-innovation-policy-goals_en

European Commission, Directorate-General for Research and Innovation. *Rapid & transparent publishing*. https://open-research-europe.ec.europa.eu/

European Commission Joint Research Centre. *Citizen Science for EU policies*. https://joint-research-centre.ec.europa.eu/scientific-activities-z/citizen-science-eu-policies_en

European Open Science Cloud. *European Open Science Cloud portal.* https://eosc-portal.eu

European Science Foundation. *Plan S*. https://www.coalition-s.org/

European Union External Action (2022). *Science diplomacy*. https://www.eeas.europa.eu/eeas/science-diplomacy_en

Follow The Money (2022). *China Science Investigation*. https://www.ftm.eu/chinascienceinvestigation

Foreign & Commonwealth Office, Foreign, Commonwealth & Development Office (2023). *Guidance: Academic Technology Approval Scheme (ATAS)*. https://www.gov.uk/guidance/academic-technology-approval-scheme

JISK, *Sherpa Juliet: Juliet statistics*. https://v2.sherpa.ac.uk/view/funder_visualisations/1.html

Kinas hemliga avtal med studenter i Sverige – kräver lojalitet med regimen (2023, January 12). *Dagens Nyheter*, https://www.dn.se/sverige/kinas-hemliga-avtal-med-studenter-i-sverige-kraver-lojalitet-med-regimen

Open Science for Open Societies (2020). *National Open Science policies in Europe: find and compare information on national Open Science policies in Europe*. https://openscience.eu/find-and-compare-information-on-specific-national-open-science-policies-in-europe

OpenAIRE. *Open Science overview in Europe by country*. https://www.openaire.eu/os-eu-countries

Secrétariat général de la défense et de la sécurité nationale (2022). *Protéger le potentiel scientifique et technique de la nation*. https://www.sgdsn.gouv.fr/nos-missions/proteger/proteger-le-potentiel-scientifique-et-technique-de-la-nation

SPARC Europe, *SPARC Europe papers*. https://sparceurope.org/what-we-do/sparc-europe-key-resources/sparc-europe-documents

The Hague Centre for Strategic Studies (2022). *Critical raw materials for semiconductor supply next 10 years*. https://hcss.nl/wp-content/uploads/2022/11/Reaching-Breaking-Point-Master-Map.pdf

The State Council of the People's Republic of China (2021). *Full Text: China's Export Controls*. https://english.www.gov.cn/archive/whitepaper/202112/29/content_WS61cc01b8c6d09c94e48a2df0.html

U.S. Department of Commerce, Bureau of Industry and Security. *Deemed Exports FAQs - I plan to publish in a foreign journal a scientific paper describing the results of my research, which is in an area listed in the EAR as requiring a license to all countries except Canada. Do I need a license to send a copy to my publisher abroad.*

Link to annexes