safeguarding science
SAFEGUARDING-SCIENCE.EU

Glossary

Annotated list of safeguarding-science terms
Version June 2023

The Safeguarding-Science.eu glossary is compiled from documents and initiatives we observe. It serves us as an overview of terms, their definitions and related sources. It includes some supplementary comments, which reflect considerations or additions from the perspective of the Safeguarding-Science.eu team. The definitions in this glossary are "working definitions" for Safeguarding-Science.eu. As a rule, they are citations from relevant public and current sources. The terms listed here are defined differently in different countries and organisations. In some cases, we collect various definitions per term. The glossary does not claim to be complete or objective. The glossary is under continuous development. We are grateful for suggestions for the addition of relevant terminology and relevant programmes or documents. For comments and questions please contact safeguarding-science@dlr.de.

safeguarding science
SAFEGUARDING-SCIENCE.EU

Term	Definition	Source	Comment
Academic core values	Within the knowledge sector, core academic values (e.g. academic freedom, research integrity and openness) constitute the touchstones for our actions.	Academic core values: overview of core values | National Contact Point for Knowledge Security (loketkennisveiligheid.nl)	
Academic Freedom	We adopt the definition of academic freedom as freedom of academic staff and students to engage in research, teaching, learning and communication in and with society without interference nor fear of reprisal (Annex I)	Rome_Ministerial_Communique.pdf (ehea.info)	This is the definition currently used in the European Union.
Academic Freedom	Academic Freedom: The freedom to teach, conduct, and publish research in an academic environment with an emphasis on enabling the participation of all is a fundamental tenet of research. It is fundamental to the mandate of research institutions to pursue truth, provide education to students, and disseminate knowledge and understanding. Academic freedom requires an environment of enabled autonomy and job security where researchers are free from undue external influence or limitations on scholarly inquiry.	220812-g7-sigre-paper.pdf (bmbf.de)	Academic freedom has been a key success factor in the development of university research over the last 200 years in the industrialised countries. It is of considerable importance for the functioning of the liberal democratic open society. However, it should be borne in mind that even in open societies by far the major part of research investment is not subject to academic freedom (not open or transparent), but to economic (e.g. industrial research, industry-related research), socio-political (e.g. large-scale research) or military (e.g. the US agencies DARPA) constraints. It should also be considered that for less economically developed societies, academic freedom might not be affordable due to budgets constraints.
Academic Freedom	The Royal Netherlands Academy of Arts and Sciences (KNAW) defines academic freedom as 'the principle that staff members at academic institutions are free to conduct their scientific research, disseminate their findings and teach'. This freedom extends to aspects including the following: - The choice of topics to be investigated; - The choice and application of own research	Academic freedom | Academic core values: overview of core values | National Contact Point for Knowledge Security (loketkennisveiligheid.nl)	The definition of KNAW is more focused on freedom of research. However, academic freedom is more than just freedom of scientific research.

	questions and methods; - Access to sources of information; - The publication and sharing of information through conferences, lectures and membership of academic groups; - The choice to enter collaboration with academic partners; - The realisation of academic higher education.		
Academic Freedom Index	The Academic Freedom Index (AFI) assesses de facto levels of academic freedom across the world based on five indicators: freedom to research and teach; freedom of academic exchange and dissemination; institutional autonomy; campus integrity; and freedom of academic and cultural expression. The AFI currently covers 179 countries and territories, and provides the most comprehensive dataset on the subject of academic freedom.	Academic Freedom Index (academic-freedom-index.net)	This is seen as a valuable resource for a general view on suitable research partners worldwide. It is interesting to observe the development of the index over the years.
Academic Fundamental Values		European Higher Education Area and Bologna Process (ehea.info) na_daad_fundamental_academic_values.pdf	The term is used in the context of the Bologna Process in Europe.
Ambiguity / strategic or systematic ambiguity	Ambiguity in rules, laws (e.g. data laws, national security laws, NGO laws, etc.), expectations, etc. creates a diffuse fear and pressure, which ultimately leads to anticipatory obedience, in research, for example, to self-censorship in publications or in teaching or the restriction of research and cooperation to certain topics or partners. After all, no one knows where exactly the red lines run and what happens when rules are broken.		Strategic ambiguity is systematically used by states, for example, to force academics into certain forms of behaviour. This also affects cooperation partners in open societies. The open ambiguity of published rules is usually compounded by unwritten expectations of certain behaviour, which permanently force the person concerned to self-censor. A current example relevant for science is the revision of the PRC's Anti-Spying Law of April 2023: The offence of espionage was redefined. Now, not only state secrets are considered protected, but all documents and files that affect the "national interest". However, this is not sufficiently

			defined and leaves a lot of room for manoeuvre, and in the event of an arrest, trials take place behind closed doors, as it is a matter of national security. So, if a European scientist unwittingly conducts, for example, sociological research on a minority in the PRC, this may carry an unknown high risk.
Burglary	Most institutions see burglary as a major risk, not just in terms of the risk of losing hardware but also, just as importantly, the risk of losing valuable information.	Risk-analysis-HEIs.pdf (integraalveilig-ho.nl)	
Business Continuity Management (BCM)	The central goal of business continuity management is to enable companies to react quickly and purposefully in an emergency in order to minimise damage and ensure that important business processes continue or can be resumed as quickly as possible.	Business Continuity Management – Einführung | TÜV NORD (tuev-nord.de)	Business continuity management is not yet part of the management process of universities and research institutions. However, hacker attacks on universities in Europe have caused great damage in recent months. In the sense of a security by design solution to increase the resilience of research institutions, it seems sensible to adapt the BMC model of industry to academia.
Catch-all controls	Export controls for non-listed dual-use items according to the conditions referred to in Article 4 of the EU dual-use Regulation	consul_183.pdf (europa.eu)	EU compliance guidance for research involving dual-use items
Compliance	The act of obeying external or internal orders, rules, regulations or request. Compliance means doing what is required to operate in the declared system.		Up to now, compliance in universities and research institutions has essentially been an issue for the central administration departments - less an issue for the researchers. However, the risks of violating rules have grown significantly in recent years and so has the potential damage. E.g., law firms have specialised in compliance breaches in the public space. Simple, clear and organisation-specific compliance assistance applications should be developed.
Conditional (competitive) Cooperation	Start by analysing what each party will do if it chooses not to cooperate and how that will affect industry dynamics. Sometimes working together is a clear win, but even if it isn't, it may still be better than	The Rules of Co-opetition (hbr.org)	In contrast to industry, conditional cooperation in research is not a matter of course. Open interaction in the academic world has not promoted such approaches. In the current geopolitical situation, however, this approach appears to

	allowing someone else to take your place in the deal—which could leave you at a disadvantage. Next, it's critical to figure out how to cooperate without giving away your "secret sauce"—your current advantages. Once you've done that, you'll need to craft an agreement that clearly outlines the deal's scope, who is in charge, how the arrangement could be unwound if needed, and how gains will be divided.		be of great advantage for one's own security. European research institutions should specify clear conditions for cooperation.
Conflicts of interest (COI) & conflicts of commitment (COC)	A conflict of interest is a set of circumstances that create a risk that professional judgment or actions regarding a primary interest will be unduly influenced by a secondary interest (American Association of University Professors, 2014[4]; UK Research and Innovation, n.d.[5]). A conflict of commitment is a situation in which an individual accepts excessive workloads or conflicting duties from multiple employers (Office of Science and Technology Policy, 2020[6]).	Integrity and security in the global research ecosystem (oecd-ilibrary.org)	A typical situation in international cooperation is when a researcher receives research funding from an authoritarian state, for example, and sits on university committees or evaluation teams in Europe on issues such as academic freedom. Or when funding from international business is accepted with expectations that are not in line with the goals of one's own research organisation.
Cost-benefit analysis	Risk Assessment and Quantitative Approaches: …, it will be essential to have robust engagement with economists and others in the risk analysis research community…. USDA has … an Office of Risk Assessment and Cost-Benefit Analysis (ORACBA), which sponsors a Science, Policy and Risk Forum. These government efforts are similar to private sector efforts focused on decision making with respect to economic risks, which are often regulatory in nature. Fundamental research presents different challenges, with the benefits often playing out over many years, and the risks less defined.	Research Program on Research Security (nsf.gov)	The limited resources at research institutions and even more so at universities in Europe force a very cost-efficient form of knowledge protection. It is therefore important to know the actual costs of damage or to estimate them as best as possible in order to implement appropriate risk prevention measures. See also => risk assesment
Counter Foreign	EU-COM Staff Working Document on tackling R&I foreign	Tackling R&I foreign interference	This report, written as a working document of the EU Commission, provides

interference / tackling foreign interference	interference: Foreign interference occurs when activities are carried out by, or on behalf of, a foreign state-level actor, which are coercive, covert, deceptive, or corrupting and are contrary to the sovereignty, values, and interests of the European Union (EU). EU Higher Education Institutions (HEIs) and Research Performing Organisations (RPOs) can benefit from a comprehensive strategy for tackling foreign interference that covers key areas of attention grouped into the following four categories: values, governance, partnerships and cybersecurity. The document contains a nonexhaustive list of possible mitigation measures that can help HEIs and RPOs to develop a comprehensive strategy, tailored to their needs.	- Publications Office of the EU (europa.eu)	concrete advice on safeguards to be taken by actors in the research sphere.
Cybersecurity	In language terms 'Cybersecurity' or 'cyber security', depending on the organization and the spelling of the word within its context, is a rather young term. Originated on the term 'Cyber Space', the term 'Cybersecurity' was crafted and used by IT professionals, consultants, lobbyists and politics to address security concerns in the 'Cyber Space'. But what does this mean? Does 'Cybersecurity' only address risks originating in the 'Cyber Space'? Does 'Cyber security' only consider the protection of virtual assets within the 'Cyber Space'? Does 'Cyber security' also apply to physical assets, such as Industrial Control Systems, production lines, power plants, etc. although they are not primarily designed to be in the 'Cyberspace'? The first purpose of this document is to raise and describe these diverging understandings in more detail and provide a guide for determining an appropriate understanding of the term 'Cybersecurity' to be	Definition of Cybersecurity - Gaps and overlaps in standardisation — ENISA (europa.eu)	Cybersecurity measures are among the mandatory duties of academic institutions and are being worked on intensively. However, in many cases they only establish passive security, i.e. protection against attacks, but do not pay similar attention to the leakage of data and information from their own systems. These can be detected and limited through own regular applications.

	used in the context of the intended use of the stakeholders and policy makers		
Defence of Democracy package	In 2020, under the headline ambition 'A new push for European Democracy', the European Commission presented the European Democracy Action Plan, with the aim of protecting and strengthening EU democracies by safeguarding the integrity of elections, strengthening media freedom and pluralism, and fighting against disinformation. In the 2022 State of the Union address, President von der Leyen announced an initiative to defend democracy from covert foreign influence…. The package will complement actions already taken at EU level under the European Democracy Action Plan. It will focus on transparency measures to prevent covert foreign interference.	Defending European democracy – Communication (europa.eu)	The objective of the 'Defence of Democracy' package is to bring together legislative and non-legislative measures to strengthen resilience to covert foreign interference. There will be effects for the research landscape in Europe, like new transparency regulations to enforce e.g. the disclosure of foreign financial benefits. In the near future Universities and Research Organisation will be asked/forced to disclose the sources of grants and financial benefits from third countries.
DESCA MODEL CONSORTIUM AGREEMENT	The signature of a Consortium Agreement between the partners of a research project is mandatory for most EU research projects. DESCA (Development of a Simplified Consortium Agreement) is a comprehensive Model Consortium Agreement for such projects…. DESCA… has been updated for use in Horizon Europe projects. The revised model considers requirements stemming from the rules of the new EU Framework Programme Horizon Europe and experience of the user community in working with DESCA 2020, as well as other legal developments.	DESCA Model Consortium Agreement - DESCA 2020 Model Consortium Agreement (desca-agreement.eu)	For conditional international cooperation good contracts are one safety measure for reliable cooperation. The EU´s templates are one key source for cross-border contractual arrangements for cooperation. The templates address EU funded projects but provide valuable example texts addressing relevant topics. They can be adapted to own needs.
Detrimental research practices	Detrimental research practices are actions that violate traditional values of the research enterprise and that may be detrimental to the research process (Committee on Responsible Science et al., 2017[7]).	Integrity and security in the global research ecosystem (oecd-ilibrary.org) Integrity and	

	Detrimental research practices include misrepresentation, breach of duty of care, and improperly dealing with allegations of misconduct (Purdue University, n.d.[8]). Theft, deception, and coercion are detrimental research practices that are more directly of concern in relation to research security (section 5).	security in the global research ecosystem (oecd-ilibrary.org)	
De-coupling	De-coupling is not a short-term phenomenon, but a long-term trend that has been fuelled by "America First" and China's "dual circulation" strategy in recent years. Decoupling is multifaceted and on the rise.	Resilienz in Zeiten des Decouplings und geopolitischer - KPMG Deutschland	Statement of a former high representative of European industry in China at a conference in spring 2023 regarding European industry position in China: There is no de-coupling! There is rather a higher diversification in individual components.
Dependency	Dependencies are mainly discussed in the area of the economy or in the area of the availability of raw materials – in the context of reducing European dependencies from others.		It remains unclear how dependent education and research in Europe is on foreign partners. It is in the very nature of cooperation that partners depend on the results of each other's, obviously e.g. when it comes to large scale research facilities. Students and researchers from less developed systems depend on opportunities in industrialised countries. Thus, the term dependency in the context of education and research need to be addressed always specific – and not in the way of a catch-all-term: "we need to reduce dependency from … "
De-risking	Managing this relationship and having an open and frank exchange with our Chinese counterparts is a key part of what I would call the de-risking through diplomacy of our relations with China…. This is why – after de-risking through diplomacy – the second strand of our future China strategy must be economic de-risking.	Speech by the President on EU-China relations (europa.eu)	Statement of a former high representative of European industry in China at a conference in spring 2023 regarding European industry position in China: We have to invest more in China, cooperate more - so de-risking does not mean less with China, but more, but in a more controlled and clear way. You also have to pay very close attention to what the Americans are doing and adapt early on. We also have to analyse very carefully how Chinese companies are developing and where they are investing, for example in South East Asia. When Chinese companies leave China, our customers go after them.

Dilemma **"dilemma-management"**	Every day, managers have to make decisions - even unpopular ones. They are often forced to choose the lesser of several evils. Decision-making is generally a complex process. In an ethical dilemma situation, moral norms must also be considered and weighed in order to arrive at a valid - ethically sound - decision. Central questions in dilemma management: How do I deal with ethical dilemmas? Who and what do I have to consider? How can I prevent dilemmas in the future? In dilemma management, one deals with individual factors and influences as well as with those that depend on the situation.	Dilemma Management - Center for Responsible Management (responsible-management.at)	Statement of a former high representative of European industry in China at a conference in spring 2023 regarding European industry position in China: If we want to do world trade we have to cooperate with China - you can't think of our social system without China. You have to do dilemma-management.
Diplomatic Resilience	Building diplomatic resilience should enable universities to navigate the global scientific landscape responsibly, self-determinedly and successfully, even in times of geopolitical tensions and worldwide threats to academic freedom. Such resilience consists, on the one hand, in developing specific and well-informed responses to acute science diplomacy crises by systematically drawing on their own scientific expertise and networks. On the other hand, diplomatic resilience means that universities promote internal reflection beyond the crisis mode and define with diverse stakeholders what their role and position can be in a world increasingly marked by conflict.	Wissenschaftsdiplomatie in Krisenzeiten • Berlin University Alliance (berlin-university-alliance.de)	The Volkswagen Foundation approved a project entitled" "Facing Challenges of Internationalisation Together: A Network for Diplomatic Resilience at the Berlin University Alliance" in March 2023. Universities and research institutions should build diplomatic resilience into their security strategy - a quasi-workflow for handling crises. (similar to the way crisis intervention teams work in German schools - only thought of on a much larger scale).
DISARM - Disinformation Analysis and Risk Management	Disinformation Analysis and Risk Management is an open-source framework designed for describing and understanding the behavioural parts of FIMI/disinformation. It sets out best practices for fighting disinformation through sharing data & analysis, and can inform effective action. The Framework has been	EEAS-DataTeam-ThreatReport-2023..pdf (europa.eu) Framework (disarm.foundation	

	developed, drawing on global cybersecurity best practices. The development of the DISARM Framework and the Foundation are currently being supported by non-profit Alliance4Europe.	20221129_Hybrid_CoE_Research_Report_7_Disarm_WEB.pdf (hybridcoe.fi)	
Disclosure ***disclosure policy for public-funded research***	NSPM-33 directs a series of actions for Federal research agencies, with an emphasis on developing standardized policies and practices for disclosing information to assess conflicts of interest and conflicts of commitment among researchers and research organizations applying for Federal R&D awards. Standardized disclosures are an optimal approach for increasing clarity, transparency, and equity while streamlining requirements and decreasing burden to the research community. They also enable Federal science funding agencies to identify potential conflicts of interest and commitment more rapidly and accurately, enabling them to make funding decisions that mitigate potential threats to research security and integrity.	An Update on Research Security: Streamlining Disclosure Standards to Enhance Clarity, Transparency, and Equity | OSTP | The White House NSF Pre-award and Post-award Disclosures - January 30, 2023 Proposal & Award Policies & Procedures Guide (PAPPG) (NSF 23-1) | NSF - National Science Foundation	For government funding in the US, an important change in the revised version of the NSF Proposal and Award Policies and Procedures Guide (PAPPG) (NSF 23-1) has come into effect as of 2023 with regard to the information to be provided to applicants about themselves (Biographical Sketches) and other funding received (Current & Pending (C&P) Support). See also => defence of democracy package
Dual-use research of concern	Dual-use research of concern can (based on current understanding) be reasonably anticipated to generate knowledge or technology that has the potential to be exploited to purposely cause harm and threaten public health or national security, although the research itself is conducted for beneficial purposes (Public Safety Canada, 2020[9]; BBSRC, MRC and Wellcome Trust, 2015[10])	Integrity and security in the global research ecosystem (oecd-ilibrary.org)	
Due diligence	Due diligence is analysis of an organization done in preparation for a transaction with that organization (Merriam-Webster, n.d.[11]). In	Integrity and security in the global research	For research institutions, it can be examined whether the cost of access to a professional credit agency is worthwhile to be able to make a quick due diligence

	international research collaboration, due diligence includes enquiry into a partner's past activities, the sector that it operates in, commercial and ethical standing of its governing body, and the legal and regulatory environment of the partner (Universities UK, 2020[12])	ecosystem (oecd-ilibrary.org) About ESMA (europa.eu)	scan. Large agencies offer background information not only from companies, but also from research institutions and universities worldwide. An option for an externalised due diligence check are the European or national Chamber of Commerce in the target country.
EDI - *Equity, diversity, and inclusion*	Equity, Diversity, and Inclusion: Equity, diversity, and inclusion (EDI) is the active promotion of the principles of access, diversity, and non-discrimination in all research activities – including recruitment procedures and career prospects. These are necessary for all aspects of research. EDI contributes to the diversity of identity and thought, with room for a variety of ideas, cultures, and views. Ensuring that everyone is able to freely participate in the research community, ecosystem, or enterprise will help to build an innovative, prosperous, and inclusive world.	220812-g7-sigre-paper.pdf (bmbf.de)	
Elicitation	A threat actor may try to elicit information by using flattery, indicating interest, asking leading questions, claiming a mutual interest or feigning ignorance. These techniques may be employed in both professional and personal settings.	Protect your research - British Columbia (science.gc.ca)	
EU Global Approach		The EU's global approach to research and innovation (europa.eu)	
Export control regimes	Multilateral arrangements seeking to prevent the proliferation of nuclear, biological and chemical weapons and their means of delivery as well as to prevent the destabilizing accumulation of conventional arms and dual-use items, e.g. by establishing lists of items which should be under control. The export	consul_183.pdf (europa.eu)	EU compliance guidance for research involving dual-use items.

	control regimes refer to Nuclear Suppliers Group, Zangger Committee, Missile Technology Control Regime, Australia Group and Wassenaar Arrangement.		
Freedom of scientific research	Freedom of scientific research encompasses the right to freely define research questions, choose and develop theories, gather empirical material, devise and employ sound academic research methods, to question accepted wisdom and bring forward new ideas. It entails the right to share, disseminate, and publish research results openly, including through training and teaching. It is the freedom of researchers to express their opinion without being disadvantaged by the system in which they work or by governmental or institutional censorship and discrimination. It is also the freedom to associate in professional or representative academic bodies and associated scientific meetings (Ministerial Conference on the European Research Area, 2020[13]).	Integrity and security in the global research ecosystem (oecd-ilibrary.org) 10_2_2_bonn_declaration_en_final.pdf (bmbf.de)	By signing the Bonn Declaration in October 2020, the EU member states sent out a strong political message about the freedom of scientific research as a fundamental value of the European Union and as a principle of international research cooperation. See => academic freedom
Foreign interference vs foreign influence	Foreign interference is carried out by, or on behalf of a foreign actor and is contrary to national sovereignty, values, and interests. It is coercive, covert, deceptive, or corrupting. This is in contrast to foreign influence, which is part of normal diplomatic relations and is normally conducted in an open and transparent manner (University Foreign Interference Taskforce, 2021[14]). Whilst it can be useful in some circumstances to make the distinction between interference and influence, the line between these two is not always clear.	Integrity and security in the global research ecosystem (oecd-ilibrary.org)	
FIMI - Foreign Information	Foreign Information Manipulation and Interference (FIMI) describes a mostly non-illegal pattern of behaviour that threatens or has the	1st EEAS Report on Foreign Information Manipulation and	This first edition of the report on Foreign Information Manipulation and Interference (FIMI) threats by the European External Action Service's (EEAS) is based on

Manipulation and Interference Threats	potential to negatively impact values, procedures and political processed. Such activity is manipulative in character, conducted in an intentional and coordinated manner, by state or non-state actors, including their proxies inside and outside of their own territory.	Interference Threats | EEAS (europa.eu)	100 FIMI incidents detected between October and December 2022. It informs about FIMI activities, actors and threats. Although Knowledge Security is not in the focus of the report - Russia's invasion of Ukraine dominates observed FIMI activities - there are a number of serious indications that can be adapted to the research and innovation landscape: diplomatic channels are an integral part of FIMI incidents (e.g. Foreign embassies force the cancellation of lectures), impersonation techniques become more sophisticated (e.g. could be the unauthorised use University logos). FIMI intends to direct attention to a different actor or narrative or to shift blame ("distract") or change the framing and narrative ("distort"). Examples for these two aspects are known in Europe´s academia.
Hybrid threats / Countering Hybrid Threads / EU Hybrid Toolbox	Hybrid attacks and campaigns are often coordinated actions across different domains… To respond in a comprehensive manner to these threats, we need to be ready to mobilise all the tools and instruments that the EU has. Acting as an overall framework, the EU hybrid toolbox will bring together relevant mechanisms, such as the cyber diplomacy toolbox and the Foreign Information Manipulation and Interference toolbox. It will improve the effectiveness and coherence of different actions, and therefore bring added value to the EU's capacity to respond to hybrid threats.	Questions and answers: a background for the Strategic Compass | EEAS Website (europa.eu)	The EU Hybrid Tool Box is planned as one of the implementation measures of the European Strategic Compass which proposes actions in four domains (ACT, SECURE, INVEST and PARTNER). The Toolbox shall bring together instruments to detect, prepare for, and respond in a coordinated manner to a broad range of hybrid threats. In parallel, a toolbox to address and counter foreign information manipulation and interference is planned too. Knowledge Security related instruments are planned to become part of the Toolbox.
Hybrid Threats	Resilience is one key component to counter Hybrid Threats. Resilience against hybrid threats can take an advantage of the resilience measures of different domains. It needs to be thoroughly designed and implemented. Developing resilience against hybrid threats requires not only looking at resilience in each area but how to build it systemically considering dependencies and interdependencies between the	JRC Publications Repository - Hybrid Threats: A Comprehensive Resilience Ecosystem (europa.eu)	See also => diplomatic resilience

	different parts of society. This report examines what is particular about resilience against Hybrid Threats. In this report, the comprehensive approach to resilient ecosystem (CARE) model which is a system-thinking representation of the society as a whole is proposed.		
Hostile Foreign Investment	While the vast majority of the foreign investment in Canada is carried out in an open and transparent manner, a number of State-Owned Enterprises (SOEs) and private firms with close ties to a foreign government and / or intelligence services can pursue corporate acquisition bids in Canada or other economic activities. Corporate acquisitions by these entities pose potential risks related to vulnerabilities in critical infrastructure, control over strategic sectors, espionage and foreign influenced activities, and illegal transfer of technology and expertise.	Protect your research - British Columbia (science.gc.ca)	In the European academic world, investments are known that can at least be suspected of being hostile. For example, universities or cultural and language institutes have been founded by foreign states at European universities that represent a non-democratic narrative. Hence, In the case of investments from third countries, the intentions behind them must always be clarified.
Insider Risk /Thread	Threat actors can use trusted insiders (employees, contractors, suppliers, partners, etc.) to gain access to your organization's most valuable information. You can also hear these individuals referred to as "non-traditional collectors". These insiders can also be coerced, manipulated, compelled or incentivized to provide information or access.	https://science.gc.ca/site/science/en/safeguarding-your-research/general-information-research-security/who-are-you-risk/protect-your-research-regional-fact-sheets/british-columbia	
Integral Safety Management / Integral Safety Plan	All universities participating within VSNU have agreed with regard to safety to: - Take responsibility for organizing an integrated safety policy to guarantee a safe living, learning and working environment and safeguard business continuity also in the case of extreme circumstances. - Compare costs and	An organization design to implement and monitor Integral Safety Management at the University of Twente — University of Twente Research	The Netherlands have a Whole of Government approach that involves not only different ministries, but also the actors of the research and innovation system. This is expressed in the basic document of the security guidelines. In our view, the Netherlands has an exemplary holistic and practical approach. It involves various activities, guidance and support measures,

Manual MISH	benefits of safety measures with each other so that only the most sensible ones are given a place. To implement Integral Safety Management in accordance with the above made agreements, a proposal is being developed for the organization and monitoring of Integral Safety Management at the UT.	Information (utwente.nl) Manual-MISH-Safe-and-Open.pdf (integraalveilig-ho.nl)	legislative initiatives and structural changes. Many relevant documents have been openly published.
MARSEILLE DECLARATION ON INTERNATIONAL COOPERATION IN RESEARCH AND INNOVATION	The objective was to move forward with the implementation of the new strategy for international cooperation in R&I of the European Union and to better concert the Union and Member States' approaches to third countries.	marseille-declaration.pdf (europa.eu)	
Internal Compliance Programme (ICP)	Effective, appropriate and proportionate policies and procedures, adopted by research organisations to facilitate compliance with the provisions and objectives of the EU dual-use Regulation and additional national measures	consul_183.pdf (europa.eu)	EU compliance guidance for research involving dual-use items
ISAC - Information Sharing and Analysis Centres	Information Sharing and Analysis Centres are trusted entities to foster information sharing and good practices about threats and their respective mitigation. In the context of a FIMI-ISAC, the purpose is to pool insights from the many organizations that expose manipulative activity using common frameworks and standards	EEAS-DataTeam-ThreatReport-2023..pdf (europa.eu)	As far as we understood, this is a suggestion only so far (June 2023). It might become an extension of STIX in the near future. See also => STIX
Knowledge security	Knowledge security means preventing the unauthorized transfer of knowledge and technology. It also includes preventing covert influence by state actors on higher education and research, which can impair the freedom of scientific research either directly or via self-censorship.	Integrity and security in the global research ecosystem (oecd-ilibrary.org)	Knowledge security is a term used by the Dutch government (and increasingly by universities) to refer to the risks of working with research partners from countries such as China but also Iran and Russia. (https://www.nato.int/docu/review/articles/2022/09/30/knowledge-security-insights-for-nato/index.html)

Non-discrimination	Especially with regard to a subject like knowledge security, in which threat analyses and risk profiles play an important role, there is a danger that an approach will 'go overboard' and lead to forms of arbitrary exclusion, imputation and discrimination. This should be avoided at all times. Any measures taken should always be objective, proportional and related to an actual danger. Engage in open discussion about this within your institution and take any and all signals seriously.	Non-discrimination | Academic core values: overview of core values | National Contact Point for Knowledge Security (loketkennisveiligheid.nl)	
Norm diffusion **Norm divergence**	The Koselleck project explores how the meaning of norms changes when they are "translated" from one arena to another. In particular, countries in Latin America, Africa and Asia with different colonial traditions, regime types and degrees of (limited) statehood will be studied, leading to different manifestations of norm resonance, legal cultures, public arenas and legal or normative pluralism.	Die Übersetzung internationaler Normen zwischen globalen und lokalen Arenen • Informationen für Medien und Journalist*innen • Freie Universität Berlin (fu-berlin.de)	The German Research Foundation (DFG) is funding a project at the Otto Suhr Institute for Political Science at Freie Universität Berlin for the translation of international norms between global and local arenas. The question of norm-setting and the respective interpretation of norms plays an increasingly important role in research and innovation. Which norms enter into a cooperation and how they are interpreted must be part of every project planning.
Open Science	Open Science can be defined as efforts by researchers, governments, research funding agencies or the scientific community to make the primary outputs of publicly funded research results – publications and the research data – publicly accessible in a digital format with no or minimal restriction as a means for accelerating research (OECD, 2015[15]).	Integrity and security in the global research ecosystem (oecd-ilibrary.org)	
Open Science	Within the European Union, it has been agreed that open science should become the standard in scientific research, and this practice is already becoming more commonplace within the knowledge sector. This does not mean, however, that	Open science | Academic core values: overview of core values | National Contact Point for Knowledge	

	all international partners also practice open science. Moreover, there may be legitimate reasons to protect some research results and to make them public only in part, if at all. These include privacy, national security, intellectual property and commercial reasons.	Security (loketkennis-veiligheid.nl)	
Operations Security (OPSEC)	OPSEC stands for Operations Security. The plain English definition is: "A systematic process of identifying and protecting sensitive, critical information to deny or mitigate an adversary's ability to access that information." Universities and colleges are caretakers of valuable research and other institutional information, as well as personal, confidential, or private information belonging to students, faculty, and other employees that someone could use to harm an individual or your institution. …. Raising awareness among students and staff that their information may be targeted, and promoting appropriate OPSEC practices ….	College_OPSEC_Packet_Final.pdf (dni.gov)	
Outsider threats	Outsider threats encompass individuals or groups that do not have authorized access to an organization's assets, but who act in a way that could lead to the illegitimate acquisition of assets and to subsequent harm…. Threat actors can use a variety of methods that include, but are not limited to, taking pictures of the facility or documents housed within, theft of digital information through portable storage devices (e.g. USB), or gaining access to restricted areas by taking advantage of ineffective physical security barriers.	Guidance for Research Organizations and Funders on Developing a Research Security Plan (science.gc.ca)	
Personnel Security	Counterintelligence reporting essentials (CORE) - A Practical Guide for Reporting Counterintelligence	Microsoft Word - TR 05-6 Reporting CI and Security	That might be interesting in Europe for staff working in security research or dual-use-research of concern.

	and Security Indicators - Defense Personnel Security Research Center (PERSEREC)	Indicators 24 May.doc (dhra.mil)	
Platform 'Safe and Open Higher Education´ (Dutch platform)	Higher Education Institutions (HEIs) have a unique 'open' character, due to their social assignment, both in physical space and in mentality. … In the Netherlands, this challenge is addressed by the Platform 'Safe and Open Higher Education', a cooperation of HEIs in the Netherlands…. Therefore, the participants in this Platform have developed an integrated safety & security management system that HEIs can use to help design their safety & security systems with which board members can carefully weigh choices to balance safety and openness.	About us - Platform Integrale Veiligheid Hoger Onderwijs (integraalveilig-ho.nl)	The Dutch platform is a very helpful blueprint for universities in other regions of Europe to develop their own approaches.
Preemployment Screening	Pre-employment screening is part of a security-oriented personnel selection. On the basis of the application documents and with the publicly available sources, the qualification of applicants is the qualifications of applicants are objectively the employer objectively. A conscientious examination according to the principle "authentic, complete and conclusive" is recommended.	bfv_Infoblatt_Pre Employment Screening_DIN A4_1122.indd (verfassungsschutz.de)	
Programme Security Instruction for Horizon Europe (PSI)	This Programme Security Instruction (PSI) establishes the security procedures to be applied and the common security procedures and processes to be followed for the management of a classified grant awarded under the Horizon Europe Programme, as well as assigns the responsibilities for the protection of classified information generated or exchanged in connection with the Programme.	https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/psi_he_en.pdf	These processes must be applied to research that involves security-relevant or secret-protection-relevant aspects. This is security research.
Proportionality	Proportionality is essential when taking measures. The guiding	Proportionality | Academic core values: overview of core values |	See => cost-benefit analysis

	principle is always: 'open where possible, protected where necessary'.	National Contact Point for Knowledge Security (loketkennisveiligheid.nl)	See => reciprocity
Reciprocity	Reciprocity is the practice of exchanging research materials, outputs, and knowledge in a manner that benefits all collaborating partners. It is necessary for effective cooperation because it helps to ensure that cooperation is mutually beneficial even if there may be asymmetries in the capacity of research partners to reciprocate cooperation or exploit its benefits.	Integrity and security in the global research ecosystem (oecd-ilibrary.org)	Reciprocity is one of the buzzwords transferred from business to research without considering the incredibly diverse nature of cooperation. Research cooperation per se is not geared towards reciprocity, but towards joint knowledge gain, whereby it matters less who invests how much and gets it back afterwards. Research with less developed research systems cannot be reciprocal at all – and should nevertheless not be stopped. The term should only be used very specifically, for example "equal, i.e. reciprocal, access to research data" or more appropriate research terms should be used, for example "fair" or "balanced" cooperation.
Research ecosystem	Research systems involve different actors, including research funders, different types of research institutions and universities and individual researchers. These actors are interdependent, operating together in a dynamic ecosystem…. The global research ecosystem is characterised by interactions between actors in different countries that have different national interests.	Integrity and security in the global research ecosystem (oecd-ilibrary.org)	A research system by its nature is cooperative and whatever knowledge security measures are put in place must first and foremost aim at supporting cooperative principles.
Research integrity	Research integrity is an overarching term that refers to the ethos of research (Sutrop, Parder and Juurik, 2020[16]). Integrity may be attributed to individual researchers, but also to institutions or the entire research ecosystem. In this project, "research integrity" refers specifically to certain values, norms, and principles that constitute good scientific practice (freedom of scientific research, openness, honesty, accountability, etc.) and regulate international research collaboration	Integrity and security in the global research ecosystem (oecd-ilibrary.org)	The here listed three definitions on research integrity overlap partly. However, we list them because there are indeed differences in the focus looking at it from different perspectives: e.g. a high-income country point of view (freedom, openness, accountability) vs. a stronger global point of view (diversity and inclusivity, fair practice from conception to implementation, mutual respect as a pathway to trust)

	(reciprocity, equity, nondiscrimination, etc.).	
Research integrity	We – the G7 members – believe the common values of research integrity apply broadly to all members of the research community, including governments, research funders, research institutions, and researchers themselves. These values include academic freedom, institutional autonomy, and the ethical conduct of research, the latter of which entails respecting the rights of those who develop ideas, research outcomes, and intellectual property throughout the lifecycle of the research project, including their publication rights. Adherence to research integrity also includes a commitment to transparency.	220812-g7-sigre-paper.pdf (bmbf.de)
Research integrity	Good research practices are based on fundamental principles of research integrity…. These principles are: Reliability in ensuring the quality of research, reflected in the design, the methodology, the analysis and the use of resources. Honesty in developing, undertaking, reviewing, reporting and communicating research in a transparent, fair, full and unbiased way. Respect for colleagues, research participants, society, ecosystems, cultural heritage and the environment. Accountability for the research from idea to publication, for its management and organisation, for training, supervision and mentoring, and for its wider impacts	The European Code of Conduct for Research Integrity - ALLEA
Research integrity	Goals for Research Integrity:Research should deliver accurate, replicable, and unbiased results reported responsibly, with the appropriate acknowledgement of all stakeholders. … Diversity and Inclusivity as a pathway to fair practice and attribution, Fair Practice from	Cape Town Statement - WCRIF - The World Conferences on Research Integrity Foundation

	conception to implementation, Mutual Respect as a pathway to trust, Shared Accountability, Indigenous Knowledge Recognition and Epistemic justice		
	Research Integrity is adherence to accepted values and principles — objectivity, honesty, openness, accountability, fairness, and stewardship — that guide the conduct of research and recognize the expectations of funding agencies, research institutions, and the research community.	Research Program on Research Security (nsf.gov)	Jason Report: Proposal to the National Science Foundation to set up a research program to study research security scientifically
Research misconduct	Research misconduct can be narrowly defined as fabrication, falsification, or plagiarism (FFP) in proposing, performing, or reviewing research, or in reporting research results. Fabrication is making up data or results and recording or reporting them. Falsification is manipulating research materials, equipment, or processes, or changing or omitting data or results such that the research is not accurately represented in the research record. Plagiarism is the appropriation of another person's ideas, processes, results, or words without giving appropriate credit (Office of Science and Technology Policy, 2000[17]).	Integrity and security in the global research ecosystem (oecd-ilibrary.org)	
Research security	In a globalised research ecosystem, ensuring research security means preventing undesirable foreign state or non-state interference with research. The main goal of research security is to protect the research ecosystem and thus protect legitimate national and economic interests (see Figure 2.1).	Integrity and security in the global research ecosystem (oecd-ilibrary.org)	See => STIP compass OECD
Research security	Research Security refers to the ability to identify possible risks to your work through unwanted access, interference, or theft and the measures that minimize these risks	Why safeguard your research? (science.gc.ca)	

	and protect the inputs, processes, and products that are part of scientific research and discovery.		
Research security	Research Security is protecting the means, know-how, and products of research until they are ready to be shared, by approval of the leader(s) of the research program and other stakeholders in their security.	Research Program on Research Security (nsf.gov)	Jason Report: Proposal to the National Science Foundation to set up a research program to study research security scientifically
Research Security by Design			The term "Security By Design" or "Secure By Design" describes a development approach, especially in the IT sector, in which the security features of a system are already systematically considered in the design phase. In other words, it is not left to chance or the assessments of individual developers whether and to what extent security functions are implemented in a system. Instead, the threats to which a system is specifically exposed are determined by modelling the threats ("threat modelling"). From this, targeted measures can be derived to minimise the security risk. See also => Integral Safety Management
Research Security Plan	Guidance to support science stakeholders to maintain research security, foundational principles of open science and academic freedom.	guidance_for_research_organizations_and_funders_on_developing_a_research_security_plan.pdf (science.gc.ca)	
Risk Analysis	Since Openness, accessibility and transparency are values that we do not want to give up in our HEIs, it is inevitable that absolute safety at HEIs is not possible. Incidents cannot be excluded at the cost of everything…. Because you can spend every euro only once, HEIs need to make a cost-benefit analysis for investments in their risk	Risk-analysis-HEIs.pdf (integraalveilig-ho.nl)	This Dutch report from 2017 compiles aspects of risk analysis in academia and comes up with recommendations: e.g. - Organize for resilience - Conduct an integral risk analysis - Collaborate in safety and security networks

	management. Risk management for HEIs is therefore a complex balancing act that requires strategic decisions at the board level of HEIs and at the level of national and European safety and security networks.		- Monitor input and output as well as processes - Balance regulation - Facilitate the sharing of knowledge on safety and security between HEIs in Europe
Risk-assessment techniques / cost-benefit analysis	Assessment of risk associated with the know-how and methods for acquiring and analyzing new data, as well as building new theoretical frameworks based on those data is also essential. 1. Risk assessment via objective functions to provide quantitative measures of the risks and costs of various research security infractions and prevention methodologies. Risk assessment should be carried out for individual scientific fields. 2. Controlled experiments (red team, blue team) involving risk assessment of research security incidents. 3. Game theoretic risk assessment of research security breaches for various scientific fields. 4. Analysis of which types of breaches of research security pose actual economic or national security threats. 5. Algorithms and tools for detection of breaches of research security.	Research Program on Research Security (nsf.gov)	Jason Report: Proposal to the National Science Foundation to set up a research program to study research security scientifically. See => cost-benefit analysis
Risk Management	ETH Zurich's university-wide risk management system takes a holistic approach that considers both potential internal and external risks. The systematic process is based on the internationally established risk management standard ISO 31000. The purpose of risk management is to protect the tangible and intangible assets on which the success of ETH Zurich depends, in particular human capital, infrastructure and reputation.	GB22-eth-zu-erich-risikoma-nage-ment_EN.pdf (ethz.ch)	Risk Management is processed in various forms and from various actors. The ETH example shows a very comprehensive 3 page risk management document.
Risk Mitigation	Risk mitigation is the strategy that organizations use to lessen the effects of business risks. It's similar to	What is Risk Mitigation & Why is it	Risk mitigation is a day-today business of cyber security or laboratory safety teams at universities and Research

	the risk reduction process, wherein potential business threats are identified before the organization takes the necessary steps to lessen the effects of these factors. Some of the threats and risks that modern organizations deal with include cybersecurity threats, natural disasters, and anything that may cause damage to the equipment, personnel, and facilities of an organization.	Important? | SafetyCulture	organisations. Risk mitigation should be applied n Research cooperation. Risk mitigation should also be considered in fields of international research cooperation, for example through pre-cooperation screening, due diligence, etc..
Safeguarding Science	The National Counterintelligence and Security Center (NCSC) has partnered with multiple federal agencies to develop an outreach initiative, "Safeguarding Science," designed to raise awareness of the spectrum of risk in emerging technologies and to help stakeholders in these fields to develop their own methods to protect research and innovation. The initiative focuses on emerging technology sectors where the stakes are potentially greatest for U.S. economic and national security…	Safeguarding Science (dni.gov)	
Safeguarding Science	Safeguarding Science: Canadian institutions are at the forefront of innovation, research and development in several areas, including science, technology, and engineering. Due to its advanced nature, research is a target for adversaries who may want to use it for malicious purposes. The transfer of our cutting-edge research can result in: - damage to the integrity of Canadian academic and research institutions; - advancements in the military and intelligence capabilities of threat actors; the possible violation of Canadian law(s) or regulation(s); and; -the loss of valuable intellectual property, which could have a negative commercial impact on Canada.	Safeguarding Science (publicsafety.gc.ca)	

Science Diplomacy	Science diplomacy is broadly understood as a series of practices that stand at the intersection of science and diplomacy. Science diplomacy has been divided into three phenomena: - science for diplomacy – the use of science to advance diplomatic objectives; - diplomacy for science – the use of diplomatic action to further scientific and technological progress; - science in diplomacy – the direct involvement of science or scientific actors in diplomatic processes (European Union Science Diplomacy Alliance, n.d.[18])	Integrity and security in the global research ecosystem (oecd-ilibrary.org)	
Scientific integrity	Scientific integrity is the adherence to professional practices, ethical behavior, and the principles of honesty and objectivity when conducting, managing, using the results of, and communicating about science and scientific activities. Inclusivity, transparency, and protection from inappropriate influence are hallmarks of scientific integrity.	A Framework for Federal Scientific Integrity Policy and Practice (whitehouse.gov)	Scientific Integrity is a term that was recently introduced into the debate by the USA and also includes science communication.
Secrecy protection	The protection of state secrets includes all measures to keep secret information that is classified by a state agency. In this context, classified information is all facts, objects or findings that must be kept secret in the interest of the public. The form of presentation is not important, only the content.	BMI - Staatlicher Geheimschutz (bund.de) Protection of European Union classified information (EUCI) - Consilium (europa.eu) classification-of-information-in-he-projects_he_en.pdf (europa.eu)	There are cases in which secrecy protection is relevant for research and cooperation. Entities should have appropriate processes and a “who-to-go-to” information for scientist in place
Security and Integrity of the Global Research	The G7 Working Group on the Security and Integrity of the Global Research Ecosystem (SIGRE) was established in the 2021 G7 Research Compact to develop principles, best practices, and a virtual academy	220812-g7-sigre-paper.pdf (bmbf.de)	

Ecosystem (SIGRE)	and toolkit for research security and integrity. These products will outline the behaviours, systems, and processes needed to preserve the openness and integrity of the research ecosystem through the protection of valuable knowledge and technology assets where necessary. In doing so, it will inform how international collaboration can continue with confidence. So far SIGRE published the G7 Common Values and Principles on Research Security and Research Integrity under the German G7 presidency in June 2022 and the G7 Best Practices for Secure & Open Research under the Japanese G7 presidency in May 2023. The Virtual Academy with an integrated Toolkit will be released in Autumn 2023.	
Security Appraisal	All actions funded under Horizon Europe shall comply with the applicable security rules and in particular rules on the protection of classified information against unauthorised disclosure, including compliance with any relevant Union and national law. DG HOME coordinates the Security Appraisal process providing a corporate service for all the parts of the Horizon Europe Programme. Where appropriate, the Commission carries out, with the national security experts, the security appraisal process for proposals raising security issues. This can lead to security recommendations, which may include, among others, the classification of certain deliverables by the project.	Innovation and security research (europa.eu)
Security Appraisal Procedure	The Security Appraisal Procedure concerns all activities funded under Horizon Europe and includes three main steps: the Security Self-assessment, performed by the applicants at the proposal preparation stage, the Security Review Procedure, conducted before the start of the	programme-guide_horizon_en.pdf (europa.eu)

	project, as well as the Security checks, conducted during or after the life of the project.	
Security Review	Only proposals above threshold and considered for funding will undergo a Security Review carried out by granting authority and Commission qualified staff, as well as by national security experts. The Security Review includes three steps: the Security Pre-screening performed by the granting authority, the Security Screening performed by the Commission and the Security Scrutiny conducted by national security experts. The Security Review is organised based on whether the call or topic, under which a proposal is submitted, is security sensitive or not and it can lead to security requirements that become contractual obligations.	programme-guide_horizon_en.pdf (europa.eu)
Security Self-assessment	When preparing a proposal to be submitted under any of the Horizon Europe calls, the applicant is required to conduct a Security Self-assessment starting with the completion of a Security Issues Table. In case the proposal is submitted under a call or topic, which is a priori flagged by the Commission as security sensitive, the applicant is also required to complete a Security Section.	programme-guide_horizon_en.pdf (europa.eu)
Security (Pre-) Screening	The first phase of the Security Review Procedure, the Security Pre-Screening, is carried out by qualified staff of the granting authority, during the scientific evaluation or soon after…. All the proposals that have gone through the Security Pre-screening will be automatically sent to the second phase of the Security Review. During this phase, the Commission (DG HOME) will assess the results of the pre-screening and decide whether the launch of the third	programme-guide_horizon_en.pdf (europa.eu)

	phase of the procedure, the Security Scrutiny, is needed.		
Security Scrutiny	The Security Scrutiny is the last phase of the Security Review and it is conducted by the Security Scrutiny Group, comprised of national security experts appointed in close cooperation with the relevant Programme Committee and the competent National Security Authorities…. The objective of the Security Scrutiny is to identify security concerns in a certain proposal,…. The possible outcomes of the Security Scrutiny are: 1. No security concern 2. Security recommendations and/or security classification3. Proposal too sensitive to be funded	programme-guide_horizon_en.pdf (europa.eu)	
Security Union Strategy 2020	Security is an issue that pervades all spheres of life. For this reason, the EU has decided to take a holistic approach to security. This communication provides an overall framework to support national policies by anticipating and tackling evolving threats whether they be online/offline, digital/physical or internal/external.	https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:4472345	EU Security Union Strategy (July 2020): Document by the European Commission addressing a comprehensive range of security issues including issues relevant for research and innovations stakeholders like cybersecurity, hybrid threads, foreign interference, security of public spaces. It also addresses the need for more research on security measures.
Sensible openness	Europe's International Higher Education and Research Cooperation in Times of Uncertainty - The Quest for Sensible Openness	Reflection-Paper-Template-final-edit-1-2-1.pdf (aca-secretariat.be)	This Academic Association Cooperation (AAC) reflection paper aims to contribute to current discussions on the role, nature and consequences of international cooperation in higher education and research. It puts five broad principles to underpin Europe's future global cooperation in higher education and research. see => conditional cooperation

Sensitive Research Areas/ Sensitive dual-Use	Research Areas Covered by Export Controls: Some fields of research (for example, nuclear, chemical, biological, radiological, or space applications) have a clear link to advancing military or intelligence capabilities and, therefore, have laws and regulations in place that must be followed for the conduct of research and export of any resulting knowledge.	national_security_guidelines_for_research_partnerships.pdf (science.gc.ca)	Similar to Dual-use-research
Sensitive dual—use research of concern	Some of these laws and regulations do not apply to new and emerging technologies since their potential military, security, and intelligence applications are less clear and well known, and/or because international arms and export control regimes have yet to reach consensus. These technologies can be sensitive or sometimes can be referred to as dual-use in that they have military, intelligence, or dual military/civilian applications	national_security_guidelines_for_research_partnerships.pdf (science.gc.ca)	Similar to Dual-use-research of concern
Sensitive Technologies		Guidance for the Control of Sensitive Technologies for Security Export for Academic and Research Institutions Revised (meti.go.jp)	Sensitive technologies have so far been pursued primarily in connection with direct investment screening and export control or embargo regimes - i.e. in economic issues. In research cooperation, these regulations are also relevant and must be considered.
STIP-Compass OECD Thematic portal Research Security	Research security: A portal that shares policy initiatives to safeguard national and economic security whilst protecting freedom of enquiry, promoting international research cooperation, and ensuring openness and non-discrimination.	Research security portal | STIP Compass (oecd.org)	The OECD STIP-Compass with the thematic sub portal on research security gives an overview on existing documents in some OECD countries, which is a good basic information however the list is not complete so far but should be updated regularly.
STIX – Structured Threat Information	The Structured Threat Information Expression (STIX™) is a data format used to encode and exchange cyber threat intelligence (CTI). It can also be used to share insights on FIMI	EEAS-DataTeam-ThreatReport-2023..pdf (europa.eu)	

Expression (STIX™)	incidents, by breaking them down into their different constitutive elements into the STIX format)	Introduction to STIX (oasis-open.github.io	
Strategic Compass for Security and Defence EU	A Strategic Compass for Security and Defence - For a European Union that protects its citizens, values and interests and contributes to international peace and security	pdf (europa.eu)	The Strategic compass is an umbrella document published by the Council of the European Union to express the European stance in an era of growing strategic competition, complex security threats and the direct attack on the European security order. The spectrum of threats has grown more diverse and unpredictable. This also effects scientific cooperation: cooperation remains important but it is increasingly politicised: research on vaccines, free exchange of scientific data and technology standards are becoming instruments of political competition. The academic world is becoming less free.
Supply Chain Risk Management	The National Counterintelligence Strategy of the United States 2020-2022 strategic objective for supply chain security is to: "Reduce threats to key U.S. supply chains to prevent foreign attempts to compromise the integrity, trustworthiness, and authenticity of products" and services purchased and integrated into the operations of the U.S. Government, the Defense Industrial Base, and the private sector.	20200925-NCSC-Supply-Chain-Risk-Management-tri-fold.pdf (dni.gov)	Supply chains might include research
Technology Readiness Levels (TRL)	Technology Readiness Levels is a non-discipline specific measurement system with indicators of the maturity level of particular technologies.	consul_183.pdf (europa.eu)	EU compliance guidance for research involving dual-use items
Technological sovereignty	Technological sovereignty has been at the heart of recent political debate in the EU. ….Key enabling technologies (KETs) – advanced manufacturing and materials, lifescience technologies, micro/nano-electronics and photonics, artificial intelligence, and security and	EPRS_STU(2021)697184_EN.pdf (europa.eu)	

	connectivity technologies – are crucial for an interconnected, digitalised, resilient and healthier European society, as well as being important for the EU's competitiveness and position in the global economy.		
Travel Risk Management		ISO 31030:2021(en), Travel risk management — Guidance for organizations	
Trusted research and innovation	Trusted research and innovation is our work programme designed to support cross-sector campaigns which protect all those working in our thriving and collaborative international research and innovation sector.	Trusted research and innovation – UKRI	The approach is mainly transported by United Kingdom Research and Innovation (UKRI), an umbrella entity covering the main funding and innovation agencies. Various supporting materials, including podcast and videos and a helpful FAQ are public.
University Autonomy / University Autonomy Scorecard	Institutional autonomy is widely considered an important prerequisite for modern universities to develop institutional profiles and deliver efficiently on their missions. The EUA Autonomy Scorecard (latest report 2023), which was first launched in 2011, offers a methodology to collect, compare and weight data on university autonomy. The Scorecard is based on more than 30 different core indicators in four key dimensions of autonomy. These include: • Organisational autonomy • Financial autonomy • Staffing autonomy • Academic autonomy	Publications (eua.eu)	
Whistleblowing	For the purpose of preventing or combating corruption and to ensure compliance at ETH Zurich ... professors and employees of ETH Zurich who, in the course of their official activities, become aware of crimes	Whistleblowing – Staffnet | ETH Zürich	A university or research institution should have an ombudsperson for critical reports. This should also have responsibilities for international cooperation.

or misdemeanours of ETH Zurich that are to be prosecuted ex officio are obliged to report the matter to their direct or next higher superior.