

Openness and security: two pillars, one system

Knowledge Security and Open Science

Project partners:

University of Bern (project leader):

- Piccina, Laura
- Brodersen, Kei Hannah
- Holländer, Nora
- Schlunegger, Sarah

Center for Security Studies (ETH)

- Eigner, Leo
- Wenger, Andreas

University of Applied Sciences and Arts Western Switzerland (HES-SO)

- Dougoud, Maya

Commissioned and supported by swissuniversities

Contents

Acknowledgements	4
Executive summary	5
Introduction	7
1. Regulatory framework for Open Science and Knowledge Security	10
1.1. European regulatory framework for Open Science and Knowledge Security	10
1.2. Swiss regulatory framework for Open Science	13
1.3. Swiss regulatory framework for Knowledge Security	14
2. Knowledge Security Risks in Open Science Practices	17
3. Factors leading to Knowledge Security risks in Open Science	22
3.1. Content	22
3.1.1. Export-controlled research	22
3.1.2. Critical technologies	23
3.1.3. Sensitive research areas	26
3.2. Partners	28
3.2.1. Legal sanctions and country-related embargoes	30
3.2.2. War and military activities	30
3.2.3. Human rights violations	32
3.2.4. Political influence and dependencies	33
3.2.5. Data imbalance in knowledge sharing	35
3.3. Infrastructure	37
4. Practical approaches to Knowledge Security and Open Science	40
4.1. Good practices for higher education institutions	41
4.2. Practical approaches: European higher education institutions	43
4.2.1. Delft University of Technology, Netherlands	43
4.2.2. KU Leuven, Belgium	44
4.2.3. Turku University of Applied Sciences, Finland	47
4.3. Practical approaches: Swiss higher education institutions	48
4.3.1. ETH Zurich	48
4.3.2. Lucerne University of Applied Sciences and Arts	49
4.3.3. University of Applied Sciences and Arts Northwestern Switzerland	50
4.3.4. University of Bern	51
4.3.5. University of Fribourg	52
4.3.6. University of Geneva	53
4.3.7. University of Zurich	55
4.3.8. Knowledge Security in Open Science in Switzerland	56
5. Open Science and Knowledge Security: Past and future trends	56
5.1. The circulation of knowledge	58
5.2. Circulation policies and their characteristics	59
5.3. International developments	60

u^b

5.4 International approaches..... 62

5.5 National developments and approaches 64

5.6. Future trends 67

6. Conclusions and recommendations _____ 68

Interviews _____ 73

Bibliography _____ 75

Acknowledgements

I would like to express my sincere gratitude to everyone who contributed to the development of this report.



I am deeply thankful to the project team for their expertise, collaboration, and commitment throughout the project. At the University of Bern, this includes colleagues from the Research Management Office – Laura Piccina, Sarah Schlunegger, and Nora Holländer – as well as the Open Science Team, in particular Federico Grasso Toro, Gero Schreier, Christine Krebs, and Dirk Verdicchio for their valuable feedback and brainstorming contributions. I would also like to thank Luisa Jansen and Malte Elson from the Psychology of Digitalisation division at the Institute of Psychology for their support and collaboration. Special acknowledgements go to Laura Piccina as the main author of this report.

My sincere thanks also go to our collaborators from the Center for Security Studies (CSS), especially Leo Eigner and Andreas Wenger, as well as to Maya Dougoud from the University of Applied Sciences and Arts of Western Switzerland. Special shoutout to Leo Eigner for assessing the future of Knowledge Security and Open Science in Chapter 5 of the report.

I would also like to sincerely thank everyone who contributed to the survey on institutional awareness and practices regarding Knowledge Security and Open Science, which laid the foundation for and helped initiate this project. The project would, furthermore, not have been feasible without all the interviewees in Switzerland and across Europe and Canada, who generously shared their expertise, perspectives, and experiences. Simone Rosenkranz and Aldina Camenisch from Lucerne University of Applied Sciences and Arts as well as Karin Hiltwein from the University of Applied Sciences and Arts Northwestern Switzerland kindly agreed to contribute the sections relating to their respective institutions in Chapter 4.

Finally, I would like to thank the members of several LERU working groups, the SRDSN, and the participants of a brainstorming workshop organised in the context of the Love Data Week. Their discussions, reflections, and feedback provided valuable inspiration and helped shape the development of this work.

I also gratefully acknowledge the trust in us and the financial support provided by swissuniversities, as well as the matching funds contributed by our respective institutions, which made this project possible. Thank you, Simon Zemp from swissuniversities, for your valuable feedback and support throughout the project.

Dr. Hannah Brodersen
University of Bern
Project leader

Executive summary

u^b

Openness has long been a cornerstone of higher education and scientific research, driving international collaboration, innovation, and the global exchange of knowledge. At the same time, an increasingly complex geopolitical environment, rapid technological advances, and growing concerns over foreign interference, misuse of research, and strategic competition have elevated Knowledge Security as a key policy priority. Rather than representing opposing objectives, Open Science and Knowledge Security are complementary principles: both seek to ensure that research remains accessible, trustworthy, and socially beneficial while protecting sensitive knowledge, technologies, and research infrastructures from unacceptable risks.

This report examines how Open Science and Knowledge Security can be implemented together within Swiss higher education institutions. Commissioned by swissuniversities under the Programme Open Science II Innovation Areas, it analyses the legal and policy landscape in Switzerland and Europe, identifies Knowledge Security risks arising in Open Science practices, and proposes practical approaches to support research that is both open and secure.

The report demonstrates that Open Science does not imply unrestricted access to all research outputs. Existing governance mechanisms, including data management plans, access controls, licensing arrangements, ethical review, and the FAIR principles already recognise that openness must be balanced with justified legal, ethical, commercial, and security-related restrictions. The challenge is, therefore, not whether research should be open or secure, but how to determine, through proportionate and evidence-based risk assessments, which knowledge can be shared openly and under which conditions.

Four principal categories of Knowledge Security risks in Open Science are identified: regulatory non-compliance in knowledge disclosure, misuse of scientific knowledge, unauthorised appropriation or exfiltration of knowledge, and undue influence, manipulation, or corruption of research outputs. These risks may arise from the nature of the research itself, the characteristics of research partners, or the digital and organisational infrastructures supporting Open Science.

The analysis highlights that Switzerland currently lacks a comprehensive legal framework dedicated specifically to Knowledge Security. Although existing legislation addresses export controls, data protection, intellectual property, and criminal offences, important gaps remain regarding the protection of sensitive research knowledge. Recent national initiatives, including the reports of the National Working Group and the Interdepartmental Working Group on Knowledge Security, as well as the implementation plan adopted by the Swiss Conference of Higher Education Institutions represent significant progress toward establishing coordinated national guidance, institutional compliance structures, and a National Contact Point for Knowledge Security.

To support implementation, the report presents examples of emerging practices from universities across Switzerland and Europe, illustrating how institutions are integrating Open Science and Knowledge Security through governance frameworks, due diligence procedures, awareness programmes, and responsible research policies. While implementation remains uneven, these experiences demonstrate that effective Knowledge Security measures can strengthen rather than undermine Open Science by enabling informed, proportionate, and transparent decision-making.

The report concludes that Open Science and Knowledge Security are mutually reinforcing rather than competing objectives. Many of the safeguards required for secure research – including data stewardship, FAIR data management, access controls, ethical review, secure digital infrastructures, and responsible international collaboration – are already embedded within Open Science practices. The principal challenge, therefore, lies not in reconciling openness with security, but in systematically integrating Knowledge Security considerations into existing research governance and Open Science frameworks.

u^b

Ultimately, maintaining scientific openness requires not fewer international collaborations or greater restrictions on research, but better governance. By embedding Knowledge Security within existing Open Science practices through a risk-based, proportionate, and country-agnostic approach, Swiss higher education institutions can preserve academic freedom, support international research excellence, and protect knowledge of strategic, societal, and scientific value. The recommendations presented in this report provide a practical framework for achieving these objectives while ensuring that Swiss research remains both open and secure.

Introduction

u^b

For several decades, openness has been a defining principle of higher education and research. Universities have promoted the free circulation of people, ideas, knowledge, and technology through international collaboration, academic mobility, the recruitment of foreign talent, open campuses, and the global dissemination of research results. This openness has been widely recognised as a key driver of scientific excellence, innovation, and economic development, enabling researchers to address increasingly complex societal challenges through cross-border cooperation.

Against this background, recent geopolitical shifts, global rearmament, and rapid technological change have made academic openness increasingly complex. While Western higher education institutions seek to protect the knowledge they produce from foreign interference and unwanted knowledge transfer, they also reaffirm openness as a fundamental condition for scientific progress and innovation. Even in times of conflict and geopolitical instability, international academic cooperation remains a defining feature of universities worldwide. This is because openness and collaboration are not merely advantageous but indispensable: cutting-edge research depends on the cross-border exchange of data, expertise, and specialised knowledge, as well as on the pooling of resources required to support costly research infrastructures and large-scale projects.

For the purposes of this report, it is important to distinguish between two related but distinct concepts that are often described using the same term. The first is **openness**, understood as a broad principle that encompasses the internationalisation of higher education and research through academic mobility, international collaboration, the recruitment of foreign talent, and the free circulation of knowledge and ideas. The second is **Open Science**, which refers to a set of concrete policies and practices designed to make scientific research and its outputs more accessible, transparent, and reusable.

Over the past two decades, Open Science has become a defining principle of research policy and academic excellence. By promoting open-access publishing, the sharing of research data, and greater transparency throughout the research process, it aims to make scientific knowledge more accessible and reusable across disciplines and borders. This global circulation of knowledge accelerates scientific progress by fostering collaboration, reducing duplication of effort, and enabling researchers to build on one another's work. At the same time, Open Science strengthens research quality by improving reproducibility, facilitating independent verification, and increasing transparency, thereby reinforcing the reliability and excellence of scientific research.

UNESCO identifies four pillars of Open Science: open scientific knowledge, open science infrastructures, open engagement of societal actors, and open dialogue with other knowledge systems (see Section 1.1).¹ In Switzerland, Open Science is primarily implemented through two strategic pillars: open-access publications and open research data. Both are supported by national strategic frameworks coordinated by swissuniversities in collaboration with other organisations. These two pillars are therefore also the focus of this project.

“Open”, in the context of Open Science, does not mean “uncontrolled”. All four pillars of Open Science indeed require varying degrees of governance, regulation, and, where appropriate, restriction. For example, the Data Management Plan, required by the Swiss National Science Foundation and by

¹ UNESCO. *UNESCO Recommendation on Open Science*. Paris: UNESCO, 2021. Accessed June 23, 2026. <https://www.unesco.org/en/open-science/about>.

many Swiss higher education institutions as part of project funding applications, ensures that sensitive data are identified and appropriately managed before publication. Data Transfer Agreements, publication plans, access controls, and licensing arrangements governing copyright and reuse are additional mechanisms that help keep science both open and secure.

In this context, the [FAIR principles](#) – Findability, Accessibility, Interoperability, and Reusability – play a fundamental role in operationalising Open Science. Accessibility itself recognises that “the protocol allows for an authentication and authorization procedure, where necessary,” while requiring that metadata remain accessible even when the underlying data are no longer available.² Consequently, FAIR does not imply that all data should be accessible to all users at all times or in all forms.

At the same time, the FAIR principles strengthen accountability, transparency, and trust in research. Data and metadata are registered or indexed in searchable repositories and assigned persistent identifiers that ensure their traceability. Comprehensive documentation accompanying open research data not only facilitates interoperability but also helps prevent misuse. As many advocates of Open Science argue, research that is openly shared and subject to broad scrutiny becomes more robust, transparent, and scientifically reliable.

As a consequence, we conclude that Open Science and Knowledge Security should not be understood as opposing concepts that contrast unrestricted openness with complete restriction. Rather, they are complementary approaches that jointly contribute to enabling research that is both open and secure.

The challenge is to determine which sensitive data, technologies, or research outputs can be shared openly, even under appropriate safeguards, without creating unacceptable risks. This is an inherently complex exercise that requires multifactorial risk assessments that consider research content, scientific partnerships, and compliance with regulatory frameworks, including export controls, intellectual property, and data protection legislation, as well as national and institutional priorities. Each case must therefore be evaluated carefully to avoid unnecessarily restricting the free circulation of knowledge. The absence of a national classification framework for research data further complicates the application of differentiated security requirements. Moreover, although openness often increases transparency and oversight, it may also expose research data to theft, manipulation, or corruption through distributed digital infrastructures.

To better understand these challenges, the project team conducted a kick-off survey³ during the summer of 2025 among representatives of Swiss higher education institutions. Respondents were asked about their perceptions of Knowledge Security risks associated with Open Science practices. The survey identified several ethical and security concerns, including unclear responsibilities for data ownership and integrity, the absence of well-defined policies for addressing ethical issues related to open data, and insufficient consideration of dual-use implications in open-access research. Respondents also highlighted weaknesses in data management, including inadequate data classification, insufficient access controls, and the lack of regular data security audits, all of which may expose sensitive or proprietary datasets to unintended disclosure.

² Wilkinson, Mark D., et al. “The FAIR Guiding Principles for Scientific Data Management and Stewardship.” *Scientific Data* 3 (2016): 4 <https://doi.org/10.1038/sdata.2016.18>.

³ Twenty-one accredited universities and universities of applied sciences participated, generating a total of fifty-five responses from professionals working in relevant areas, including open science, knowledge security, export control, technology transfer, international relations, legal affairs, research management, and IT. The survey generated quantitative raw data that have not been subjected to a statistical analysis, but that provide useful indications of general trends.

A recurring theme throughout the survey was the lack of Knowledge Security awareness and training among researchers and staff, accompanied by an incomplete understanding of Open Science itself. Respondents also identified uncertainty about what constitutes a Knowledge Security risk, limited institutional resources, and the absence of clear institutional policies as significant obstacles to implementing Knowledge Security effectively within Open Science. Organisational challenges, including administrative burdens and insufficient coordination between departments, were likewise emphasised.

Beyond targeted training initiatives, respondents identified several measures that would strengthen both Open Science and Knowledge Security. These include clearer guidance at both national and institutional levels, the development of secure digital tools and infrastructures for research data storage and sharing, and stronger coordination with national stakeholders, including swissuniversities, the Swiss National Science Foundation (SNSF), and the State Secretariat for Education, Research and Innovation (SERI).

The present report and its accompanying Toolbox, commissioned and funded by swissuniversities through its [Open Science Innovation II](#) programme, aim at addressing some of these identified needs. It thereby complements measures initiated following the [report of the National Working Group, led by swissuniversities, on Knowledge Security in Switzerland](#), for the Open Science context.⁴

Chapter 1 of the present report introduces the concepts of Open Science and Knowledge Security, and describes their legal and policy frameworks at both Swiss and European levels. Switzerland's close integration into the [European Research Area](#) (ERA), together with the European Union's leading role in shaping the development of Open Science, provides the rationale for adopting a European perspective throughout this Chapter.

Chapter 2 examines Knowledge Security risks as they could possibly arise in the context of Open Science practices.

Chapter 3 analyses the factors that could lead to risks to Knowledge Security and organises them into three main areas: research content, research partnerships, and research infrastructure.

Chapter 4 identifies key areas for action and presents examples of good practices demonstrating how Open Science and Knowledge Security can be successfully implemented in Switzerland and internationally. Even though implementation of Knowledge Security in Open Science still remains very fragmented, a variety of measures can already be observed at institutional level. Case studies are integrated throughout the chapter; fictional scenarios are marked with an asterisk (*).

Chapter 5, authored by Leo Eigner, examines Open Science and Knowledge Security as part of a broader context of strategic competition and explores their future developments.

The concluding chapter synthesises the report's main findings and presents recommendations for higher education institutions, drawing on the evidence and analysis developed throughout the preceding chapters.

⁴ swissuniversities. *Knowledge Security in Switzerland: A Strategic Framework for Higher Education Institutions and Authorities*. Bern: swissuniversities, 2025.

1. Regulatory framework for Open Science and Knowledge Security

1.1. European regulatory framework for Open Science and Knowledge Security

The European regulatory framework for Open Science builds on the UNESCO definition, officially recognised by 194 countries. This frames Open Science as

an inclusive construct that combines various movements and practices aiming to make 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. It comprises all scientific disciplines and aspects of scholarly practices, including basic and applied sciences, natural and social sciences and the humanities, and it builds on the following key pillars: open scientific knowledge, open science infrastructures, science communication, open engagement of societal actors and open dialogue with other knowledge systems.⁵

These four pillars are further described as:

1. “Open scientific knowledge”: open or partially open access to scientific publications, research data, metadata, educational resources, software, source code, and hardware.
2. “Open science infrastructure”: shared infrastructures (from repositories to open laboratories) that foster Open Science and support diverse research communities.
3. “Open engagement of societal actors” or “citizen science”: sharing of knowledge, methods, practices and tools between the scientific community and societal actors e.g, crowdfunding, crowdsourcing and scientific volunteering, research conducted by non-professionals.
4. “Open dialogue with other knowledge systems”: knowledge transfer to and from marginalised groups, local communities or individuals with different cultural canons.⁶



1 Pillars of Open Science, UNESCO 2021, <https://unesdoc.unesco.org/ark:/48223/pf0000383323>, p. 6

⁵ UNESCO Recommendation on Open Science: 7.

⁶ Ibidem, 9-15.

While UNESCO is widely regarded as a leading organization in shaping Open Science at the global level, European initiatives have also played a significant role in advancing its development. In Europe, Open Science had already gained significant momentum already in the 1990s and early 2000s through the Open Access movement, marked by milestones such as the [Budapest Open Access Initiative](#) and [the Berlin Declaration on Open Access to Knowledge in the Sciences and Humanities](#). Over time, its scope broadened considerably with topics such as Open Research Data and research transparency gaining increasing prominence. In the last fifteen years, the European Union has steadily advanced Open Science as a strategic priority, aiming at creating a research environment that is accessible, transparent, and collaborative across its Member States. This journey developed further with the establishment of [the European Commission's Open Science Policy Platform \(OSPP\)](#) in 2016. During the Horizon Europe 2020 programme, which ran from 2014 to 2020, mandatory open access policies for publications funded under the framework were introduced, laying a strong foundation for the dissemination of research outputs. Today, [Open Science remains a core principle of Horizon Europe](#), in which Switzerland also participates, and continues to be a key priority on the EU's research and innovation agenda.⁷

From the outset, discussions on Open Science have also taken into account the limits and constraints of making research open. In 2021, the [UNESCO Recommendation on Open Science](#), stated that:

Access to scientific knowledge should be as open as possible. Access restrictions need to be proportionate and justified. They are only justifiable on the basis of the protection of human rights, national security, confidentiality, the right to privacy and respect for human subjects of study, legal process and public order, the protection of intellectual property rights, personal information, sacred and secret indigenous knowledge, and rare, threatened or endangered species. Some data or code that is not openly available, accessible and reusable may nonetheless be shared among specific users according to defined access criteria made by local, national or regional pertinent governing instances. In cases where data cannot be openly accessible, it is important to develop tools and protocols for pseudonymizing and anonymizing data, as well as systems for mediated access, so that as much data as possible can be shared as appropriate. The need for justified restrictions may also change over time, allowing the data to be made accessible or restricting access to data at a later point.⁸

Echoing the *UNESCO Recommendation on Open Science*, the European Union's [Open Science Policy](#) underscores the importance of a balanced approach that promotes strategic autonomy and innovation-driven openness while simultaneously safeguarding sensitive knowledge and ensuring research security. While Open Science continues to be recognised as a vital factor in sustaining a competitive European market, as highlighted in Enrico Letta and Mario Draghi's 2024 reports,⁹ a new policy priority has emerged: Knowledge Security. A paradigmatic shift is underway: after years of strong incentives toward open-access publishing, free sharing of data and international collaboration, scientists are now encouraged to reflect more critically on the benefits and potential risks of sharing

⁷ See for example the upcoming [European Research Area Act](#) (ERA Act).

⁸ *UNESCO Recommendation on Open Science*: 10-11.

⁹ Letta, Enrico. *Much More Than a Market*. Report to the European Council. April 2024.

<https://institutdelors.eu/en/publications/much-more-than-a-market/>. Letta's report was commissioned by the Belgian government, led by Alexandre de Croo, the Spanish government, led by Pedro Sánchez, the European Council chaired by Charles Michel, and the President of the European Commission Ursula von der Leyen. Draghi, Mario. *The Future of European Competitiveness: A Competitiveness Strategy for Europe (Part A) and In-Depth Analysis and Recommendations (Part B)*. Brussels: European Commission, September 9, 2024. https://commission.europa.eu/topics/competitiveness/draghi-report_en. The report, tasked by the European Commission, produced some recommendations which served as basis for the European [Competitiveness Compass](#) presented in January 2025.

knowledge. Economic competitiveness and security appear now to be core priorities of European Commission President Ursula von der Leyen's agenda.¹⁰

According to the Council of the European Union, Knowledge Security (or Research Security) refers to

anticipating and managing risks related to: (a) the undesirable transfer of critical knowledge and technology that may affect the security of the Union and its Member States, for instance if channelled to military or intelligence purposes in third countries; (b) malign influence on research where research can be instrumentalised by or from third countries in order to inter alia create disinformation or incite self-censorship among students and researchers infringing academic freedom and research integrity in the Union; (c) ethical or integrity violations, where knowledge and technologies are used to suppress, infringe on or undermine Union values and fundamental rights, as defined in the Treaties.¹¹

Between 2021 and 2024, the European Union developed various Knowledge Security initiatives designed to enhance the integrity, resilience, and strategic autonomy of its research ecosystem. These measures seek to strike a balance between maintaining international collaborations and protecting against risks such as misuse of research and foreign interference. The 2023 [European Economic Security Strategy](#) marked a significant step by introducing systematic risk assessments targeting critical technology sectors, including artificial intelligence, semiconductors, and biotechnology. Building on this foundation, the [Council Recommendation on Enhancing Research Security](#), adopted in 2024, established guiding principles focused on safeguarding research integrity while ensuring openness. The European Commission and Member States shall

continue to promote and encourage international cooperation in research and innovation that is both open and secure, in line with the principle 'as open as possible, as closed as necessary', ensuring that research outputs are findable, accessible, interoperable and reusable (FAIR), with due consideration to applicable restrictions, including security concerns.¹²

In the same year, the European Research Area revised its [Charter for Access to Research Infrastructures](#), integrating FAIR data principles with reinforced research security requirements to promote responsible access and data sharing. Complementing these efforts, the [Cyber Resilience Act](#) introduced mandatory cybersecurity standards for digital products, aiming at fortifying the security and resilience of research infrastructures and digital networks.

The European Commission has also proposed creating a [European Centre of Expertise on Research Security](#), which could provide research institutions with tools (e.g., a common due diligence platform), guidance, and coordinated responses to emerging security challenges. Parallel to these developments, [European reforms to the dual-use export control regime](#) continue to address risks associated with intangible technology transfers and international research collaborations. Collectively, these initiatives underscore the EU's commitment to safeguarding knowledge assets while fostering innovation and international cooperation.

¹⁰ von der Leyen, Ursula. *Europe's Choice: Political Guidelines for the Next European Commission 2024–2029*. Strasbourg: European Commission, July 18, 2024. Accessed June 25, 2026. https://commission.europa.eu/document/download/e6cd4328-673c-4e7a-8683-f63ffb2cf648_en.

¹¹ Council of the European Union. *Council Recommendation of 23 May 2024 on Enhancing Research Security (C/2024/3510)*. *Official Journal of the European Union*, C/2024/3510, May 30, 2024: 4. <https://eur-lex.europa.eu/eli/C/2024/3510/oj>.

¹² *Council Recommendation of 23 May 2024 on Enhancing Research Security*: 5.

1.2. Swiss regulatory framework for Open Science

Open Science in Switzerland operates within a policy-driven framework, lacking binding federal legislation. Its implementation relies on voluntary adherence by institutions and researchers.

A key reference shaping Swiss Open Science policy is UNESCO's 2021 *Recommendation on Open Science*, whose definition of Open Science Switzerland has adopted. Beyond this, Swiss higher education institutions have also endorsed several international declarations promoting Open Science, including the [San Francisco Declaration on Research Assessment](#) (DORA), the [Coalition for Advancing Research Assessment](#) (CoARA), and the [Barcelona Declaration on Open Research Information](#). These instruments collectively advocate for reproducible, equitable, and transparent scientific practices supporting safe research globally.

In Switzerland, safeguarding the autonomy of higher education institutions and researchers is essential for the implementation of Open Science. Beyond the various institutional policies and bottom-up initiatives (see Section 4.3), the development of Open Science has been strongly driven by national strategic frameworks, such as the [National Open Access Strategy](#) and the [National Open Research Data Strategy](#).¹³ The former was adopted by the Plenary Assembly of swissuniversities in 2024,¹⁴ the latter by swissuniversities' Delegation Open Science in 2021.¹⁵

The National Open Access Strategy requires full open access (e.g., “a publication is immediately accessible in a machine-readable format at no charge, with no embargo, and with an open license”) for publicly funded research.¹⁶ The strategy defines six objectives, among which a strong full open access culture in scholarly publishing practices, as well as alignment with the global context. It implements rights retention policies (per cOAlition S, the largest Open Access international initiative of research funders to implement OS), and addresses the legal complexities of secondary publishing rights.¹⁷

The Swiss National Open Research Data Strategy also stipulates that, according to ORD principles, research data must be accessible: it must be possible to copy, use, distribute, transmit and present research findings. The strategy directly addresses the issue of Knowledge Security following the motto “as open as possible, as closed as necessary” by stating that “access restrictions according to good disciplinary practices regarding data may apply but are limited to justified legal and/or ethical constraints or security reasons and must not be extended to metadata.”¹⁸ In addition, due to the

¹³ swissuniversities. *Swiss National Open Research Data Strategy*. Bern: swissuniversities, 2021. Accessed February 12, 2026.

https://www.swissuniversities.ch/fileadmin/swissuniversities/Dokumente/Hochschulpolitik/Open_Access/Swiss_National_ORD_Strategy_en.pdf. swissuniversities. *Swiss National Open Access Strategy*. Bern: swissuniversities, 2024. Accessed February 12, 2026.

https://www.swissuniversities.ch/fileadmin/swissuniversities/Dokumente/Hochschulpolitik/Open_Access/Swiss-National-Open-Access-Strategy-2024-en.pdf.

¹⁴ The Open Access strategy revision has been approved by the Delegation Open Science on 10 April 2024.

¹⁵ In 2021 the policy has been supported by the plenary assembly of swissuniversities, the ETH, the board of directors and delegates of the Swiss Academies of Arts and Sciences and the presiding board of the National Research Council of the SNSF.

¹⁶ *Swiss National Open Research Data Strategy*: 3.

¹⁷ More information on [‘Plan S’ and ‘cOAlition S’ – Accelerating the transition to full and immediate Open Access to scientific publications](#) and [SNSF joins cOAlition S – immediate Open Access to scientific articles](#).

¹⁸ *Swiss National Open Research Data Strategy*: 6

application of the FAIR principles (Findability, Accessibility, Interoperability and Reusability), the strategy encourages safe data management. It also mentions, among its goals, the improvement of researchers' ORD practices and capabilities, including on "legal requirements and principles of scientific integrity."¹⁹

Swiss institutional and national Open Science policies often mention the principle of "as open as possible, as closed as necessary", and recommend restrictions in terms of privacy issues, commercial interests, copyright and ethics. However, they do not generally address concerns of national security and misuse, and they provide little practical guidance on criteria for data closure. As a result, researchers may unintentionally publish or share data that ought to be protected under existing security, ethical, or other legal standards.

1.3. Swiss regulatory framework for Knowledge Security

In Switzerland, there is currently no federal regulatory framework or legislation that addresses Knowledge Security as a distinct and autonomous policy field. Risks to Knowledge Security are addressed in the Swiss criminal code, in export control legislation, data privacy laws, or intellectual property laws. Existing norms that address Knowledge Security, though, often leave room for interpretation, grey zones and gaps.

For examples, [export controls](#) regulate the export of items with dual-use potential (i. e. with both civilian and military use, or items that could contribute to the development of weapons of mass destruction and their delivery systems, or might be used for human rights abuses or acts of terrorism). While export control laws are well-defined for tangible goods, software, and technologies, they explicitly exempt fundamental research that lacks a specific practical aim or objective. This creates grey zones because even theoretical research can produce results with misuse potential. In addition, outside the items listed in federal export control lists, the concept of "dual-use" remains inherently ambiguous, as many technologies could be repurposed for military applications.²⁰ The risk, therefore, does not lie in the classification of research as "dual-use", but in the absence of a clear framework for assessing whether open dissemination may lead to harmful applications.

Other examples are [federal](#) and cantonal data protection laws that, although concrete in their requirements, their focus is narrowly confined to personal data and ethics in human, animal and medical research, or to commercial data in the case of the [Unfair Competition Act](#) (UCA). This creates a blind spot in data legislation and leaves it up to researchers to evaluate what data should not be shared because of other reasons, such as risks to Knowledge Security.

Since 2023, this legislative gap has been highlighted to the Federal Council through several parliamentary interpellations and motions.²¹ To address the emerging need for a national regulatory

¹⁹ Ibidem, 9.

²⁰ Stanton, Noah. *Dual-use Research and Innovation in Europe and Switzerland*. Brussels: SwissCore, 2026. EARTO – European Association of Research and Technology Organisations. (2024, April 30). *EARTO answer to EC consultation on technologies with dual-use potential (Final)*. <https://www.earto.eu/wp-content/uploads/EARTO-Answer-to-EC-Consultation-on-Technologies-with-dual-use-potential-Final.pdf>

²¹ 1) Interpellation no. 23.4203, deposited by Céline Weber on 28 September 2023, [23.4203 | Sollte es nicht eine nationale Kontaktstelle für die Sicherheit von Schweizer Wissen und Technologie geben? | Geschäft | Das Schweizer Parlament](#), last consulted on 12 February 2026: The interpellation asks how the Federal Council supports universities and companies in identifying opportunities and risks in international research

framework on Knowledge Security, federal institutions have initiated several measures. In November 2024, the Council of the Swiss Conference of Higher Education Institutions and the Federal Department of Economic Affairs, Education and Research established two national working groups on Knowledge Security.

The first, the so-called National Working Group (NWG), brought together representatives from several academic institutions and was chaired by Prof. Günther Dissertori, Rector of ETH Zurich. The second, referred to as the IDAG (*Interdepartementale Arbeitsgruppe*) on Knowledge Security, was led by the State Secretariat for Education, Research and Innovation (SERI) and included representatives from federal bodies such as the Federal Department of Defence, Civil Protection and Sport (DDPS), the Federal Department of Foreign Affairs (FDFA), and the Federal Department of Justice and Police (FDJP).

In September 2025, the NWG published the report [Knowledge Security in Switzerland: A Strategic Framework for Higher Education Institutions and Authorities](#). Therein, it defines Knowledge Security as

the prevention of the unwanted transfer of sensitive information, know-how, and technology, the mitigation of foreign interference in higher education and research, and the reduction of dependencies that could endanger national security and competitiveness. Ethical concerns are also important aspects²²

In relation to the potential misuse of knowledge. This definition covers several dimensions: institutional security, information security, personnel security, technology security and collaborative security.²³

partnerships, particularly given growing geopolitical tensions and Switzerland's increased cooperation outside Europe. It also asks whether Switzerland should create a national contact point for knowledge security, similar to the Netherlands. The Federal Council points to existing measures, including the intelligence service's "Prophylax" prevention program, guidance from swissuniversities on responsible international cooperation, and Switzerland's participation in European and bilateral research initiatives. It also refers to plans for a national center for scientific integrity, which would provide advice to universities, but stops short of proposing a separate national contact point for knowledge security.

2) Interpellation no. 24.4364, deposited by Anna Rosenwasser on 26 February 2025, [24.4364 | Globale Talente unerwünscht? Konsequenzen der neuen ETH-Prüfkriterien | Geschäft | Das Schweizer Parlament](#), last consulted on 12 February 2026: In October 2024, ETH Zurich introduced stricter security checks for Master's and doctoral admissions, as well as for guests and staff, particularly for applicants from around twenty countries and in sensitive fields subject to export controls. A parliamentary interpellation questioned whether these broad criteria are proportionate, potentially discriminatory, and likely to exclude talented individuals without security risks. The Federal Council replied that research security is a global priority and that ETH Zurich must comply with export control and sanctions laws. It considers the measures proportionate, as applications are assessed individually and no single criterion leads automatically to exclusion.

3) Motion no. 25.3315 deposited by Reto Nause on 21 March 2025: The motion calls on the Federal Council to amend the law to require security checks for students and researchers from high-risk countries who seek access to university programs with potential military (dual-use) applications. It argues that Switzerland's strong research sector is vulnerable to espionage and unwanted knowledge transfer. The Federal Council recognizes the importance of research security and notes that measures and working groups are already underway to address the issue while protecting academic freedom. It therefore recommends rejecting the motion.

²² *Knowledge Security in Switzerland: A Strategic Framework for Higher Education Institutions and Authorities*: 6; NWG's definition is based on Eigner, Leo. "Knowledge Security at Stake." *CSS Analyses in Security Policy*, no. 338. Zurich: Center for Security Studies, March 2024.

²³ *Knowledge Security in Switzerland: A Strategic Framework for Higher Education Institutions and Authorities*: 6-7.

The IDAG report,²⁴ also completed in late 2025, defined Knowledge Security as follows:

Knowledge security aims to protect scientific knowledge and national interests against specific risks by internal and external factors whilst creating a responsible and secure environment for international cooperation. This concept is embedded within a framework of national security, in which knowledge and technology management has become a key strategic issue. Technological progress and the internationalisation of scientific exchange present new challenges to which states must respond – on the one hand, to ensure knowledge and research security, and on the other, to safeguard academic freedom and scientific integrity. Knowledge security is intended to help prevent risks that could jeopardise national sovereignty, scientific integrity, and economic interests.²⁵

The IDAG report divided risks into six categories: (1) knowledge leakage and technology acquisition, (2) scientific integrity being undermined, (3) lack of reciprocity, transparency, and compliance in international partnerships, (4) financial and technological dependencies, (5) disruption of international partnerships, and (6) lack of coherence in the implementation of knowledge security measures.²⁶

To address the risks associated with Knowledge Security, the two reports formulated three main recommendations:²⁷

1. Strengthening the legal framework to enable higher education institutions to implement effective Knowledge Security measures, including through a clear legal basis for admission restrictions, export control and technology transfer regulations, and enhanced information sharing between higher education institutions, government agencies, and security services to support the assessment and mitigation of Knowledge Security risks.
2. Enhancing institutional awareness and compliance structures by ensuring that higher education institutions systematically raise awareness of Knowledge Security risks, establish dedicated compliance offices with clear internal procedures and guidelines, and participate in a coordination network to improve alignment and the effective implementation of Knowledge Security measures.
3. Establishing a national coordination and advisory mechanism to support higher education institutions on Knowledge Security risks, practices, and developments. This mechanism, potentially structured as a National Contact Point, would facilitate information exchange among relevant stakeholders, provide guidance and advisory support, and contribute to strategic planning and policy coherence at the national level.

The reports of both the NWG and the IDAG were reviewed by the Council of Higher Education on 27 November 2025. The Council agreed with both groups' assessment that action is required at all levels.

The Swiss Conference of Higher Education Institutions (*Schweizerische Hochschulkonferenz, SHK*) presented an [implementation plan](#) on 26 February 2026 for those measures that fall into its remit. Based on a neutral, country-agnostic, and principle-based framework, this document took note of the recommendations by NWG and IDAG and underlined that higher education institutions are primarily

²⁴ Schweizerische Eidgenossenschaft. *Bericht der IDAG Knowledge Security*. Bern: Schweizerische Eidgenossenschaft, November 10, 2025.

²⁵ Ibidem, 3.

²⁶ Ibidem.

²⁷ *Knowledge Security in Switzerland: A Strategic Framework for Higher Education Institutions and Authorities*: 14-18, and *Bericht der IDAG Knowledge Security*: 10-11.

responsible for identifying, assessing, and managing Knowledge Security risks in their teaching, research, and collaboration activities.

The implementation plan of the SHK comprises the following points:

- Establish a national contact point for Knowledge Security: The SHK is currently leading and coordinating a working group mandated to establish the national contact point. A final decision on the scope, mandate, and institutional anchorage of the national contact point is expected to be taken by the end of 2026.
- Appoint compliance officers in accordance with institutional size and needs: Each institution should establish a dedicated role, position, or specialised unit responsible for Knowledge Security. This body should support researchers and administrative staff in conducting risk assessments, coordinate sensitive cases and document related decisions, serve as a point of contact for cantonal and federal authorities, and ensure that internal procedures remain up to date.
- Develop a network of compliance officers: Such a network would facilitate the harmonisation of institutional processes and promote the exchange of expertise and experience with federal authorities and the National Contact Point. It would also contribute to the development of further national recommendations and guidance documents.
- Establish standardised internal procedures for addressing Knowledge Security issues: These procedures should include systematic, project-by-project risk assessments, particularly in the context of international collaborations; oversight of admissions and mobility involving individuals from sensitive contexts in coordination with cantonal and federal authorities; management of transfers of technology, data, and know-how in accordance with federal regulations, particularly those administered by SECO; and the review of sensitive institutional partnerships. To support the implementation of these measures, the adoption of a Code of Conduct on Knowledge Security is recommended. Institutions should also ensure that export control requirements are properly integrated into their internal procedures.
- Raise awareness and provide training on Knowledge Security matters: Researchers and administrative staff should receive targeted awareness-raising measures and training on Knowledge Security risks and compliance obligations.

The State Secretariat for Migration (SEM) has been requested to

- Examine a possible legal basis for taking Knowledge Security aspects into account when deciding on residence permits.
- Promote awareness and training on Knowledge Security issues.

2. Knowledge Security Risks in Open Science Practices

As defined by UNESCO, Open Science is a broad and multifaceted concept that requires further specification to be operationalised in practice. In this report, it is understood primarily as *open scientific knowledge*, encompassing open or partially open access to scientific publications, research data, metadata, software, source code, and hardware. Other dimensions of Open Science, such as open infrastructure, are considered only insofar as they support or enable access to scientific knowledge. This delimitation reflects the Swiss policy context, where Open Science is primarily framed through the National Open Research Data Strategy and the National Open Access Strategy (see Section 1.2). By contrast, other dimensions of Open Science, including citizen science and open

innovation, feature in policy discussions but do not currently constitute core elements of the national policy framework.

In order to fulfil the mandate of addressing Knowledge Security risks in an Open Science context, this report first examines how and where such risks may emerge within open scientific practices. By intersecting the nationally defined Knowledge Security risks as unwanted knowledge transfer, foreign interference, strategic dependencies, and misuse (see Section 1.3) with practices related to *open scientific knowledge*, at least four distinct areas of risk can be identified for this particular context:

1. Regulatory non-compliance in knowledge disclosure
Or, to put it simple, “knowledge sharing is itself a regulatory infringement”, e.g. a publication (data, software, papers) violates export control, data protection or IP laws.
2. Misuse of knowledge
or “open knowledge gets misused”, e.g. open data is decontextualised and misused for human rights violations or used to develop technologies that threaten national security.
3. Misappropriation or unauthorised exfiltration of knowledge
or “knowledge gets stolen”, e.g. closed data employed in an Open Science project is stolen via a cyberattack.
4. Undue influence, manipulation or corruption of knowledge
or “open knowledge gets influenced, altered, manipulated, corrupted, or faked”, e.g. published open data is altered to fit a political narrative; open data is erased because of political censorship; open data is falsified and later employed by a foreign country to train open AI models.

Risk 1: Regulatory non-compliance in knowledge disclosure

Regulatory non-compliance in knowledge disclosure (e.g. the open-access publication of a software with military applications) is a form of unwanted knowledge transfer because information is transmitted without authorisation, in breach of the law or of a contract (for instance, data protection and privacy laws, intellectual property laws, national security regulations, export control laws, contract agreements, commercial restrictions, codes of conducts, juvenile protection statutes, the Swiss Criminal Code, the Swiss Unfair Competition Act or other regulations). Publishing scientific output or data is unwanted by either the legislator or the contractual partner. The problem, in this case, is often not related to Open Science itself, but more to the question of whether to publish or not publish at all, and, if something is published, who has access to it.

Scenario 1 – Unwanted knowledge transfer due to breaches of privacy laws

A university research team publishes a supposedly anonymized dataset containing patient records (e.g., diagnoses, genomic information, and treatment histories) in an open repository; later, researchers show that individuals can be re-identified by combining the dataset with external

information. This could trigger privacy-law violations because health data is treated as highly protected personal information.²⁸

Scenario 2 – Example of unwanted knowledge transfer due to breaches of export control laws

A group of space scientists designs a telescope for an international space mission. They published clear instructions to build this new tool, which was not already in the public domain, in an open-access journal. Space optics, precision sensors, and aerospace components, though, are commonly listed under export control regimes (e.g., dual-use lists), because they can be used for surveillance, missile guidance, or military space systems. Since the telescope qualifies as controlled technology, publishing detailed instructions without access controls can be a regulatory infringement of export control laws.

Scenario 3 – Example of unwanted knowledge transfer due to breaches of copyright rules

A team of researchers jointly publishes two related datasets: one containing architectural measurements and another comprising accompanying drawings. While the measurements were not subject to copyright protection, the drawings were, and potentially included sensitive information. Because a single publishing license, which defines copyright and publication conditions, is applied to both datasets despite their differing legal status, the publication results in a copyright infringement and raises potential concerns regarding building security.

At its core, however, the problem stems from misclassification: the two datasets are not supposed to be bundled or treated as a single entity.

Risk 2: Misappropriation or unauthorised exfiltration of knowledge

Misappropriation or unauthorised exfiltration of knowledge is a form of unwanted knowledge transfer because information is transmitted without consent. “Open”, in fact, does not necessarily mean uncontrolled or accessible to everyone. Open data and publications can be protected by access controls, such as registration requirements, or full access might be granted only in reading rooms. When these safeguards are trespassed by malicious actors, the risk of appropriation or theft of publications or data through open or collaborative platforms arises.

Moreover, projects that promote open data and open-access publications frequently also generate closed data (e.g. sensitive material that cannot be shared openly). For example, publicly funded research on civil rights in Central Africa may disseminate its findings in open-access formats while restricting access to datasets containing the identities of human sources for security and ethical reasons. Such closed data may nevertheless remain vulnerable. Malicious actors could attempt to obtain it through cyberattacks, unauthorised access to restricted systems, or even through the aggregation of seemingly non-sensitive information that, when combined, enables inferences about protected data.

²⁸ Case scenarios have been collected from both bibliographical sources, media reports and direct accounts gathered through a series of interviews with experts in the fields of Knowledge Security and Open Science (see *Introduction*, p. 7). Scenarios marked with an asterisk* are hypothetical; however, they are grounded in real-world cases. For security reasons, all scenarios have been anonymised. Information about the underlying sources may be made available upon request.

Scenario 4* – Example of unwanted knowledge transfer as misappropriation

A public academic institution provides access to its holdings through a virtual reading room that allows users to consult materials remotely. Within this environment, digital documents, such as public building planimetries or infrastructure drawings protected by intellectual property rights, can be consulted by everyone upon request but not reproduced. If safeguards do not work properly (e.g. insufficient monitoring of user activity), once access is granted, documents may be copied, downloaded through screen capture, or redistributed without authorisation.

Scenario 5* – Example of unwanted knowledge transfer as misappropriation

A group of researchers receives public funding to study genetic diseases affecting a marginalised Asian community living under significant political pressure. In line with funding requirements, they are expected to publish their findings in open access, unless compelling reasons justify restrictions. Accordingly, the researchers disseminate their scientific results openly, while restricting access to the underlying genomic data for security and ethical reasons, protecting it through strict access controls. Despite these safeguards, a malicious actor succeeds in breaching the system, exfiltrates the genomic data, and subsequently misuses it for human rights violations.

Risk 3: Misuse of scientific knowledge

This risk arises when open publications and open data are or might be applied in unintended, unethical, or harmful ways due to manipulation, misinterpretation, and decontextualisation. The potential for misuse increases with large-scale dissemination of knowledge through platforms like social media, where information can be easily distorted or taken out of context. As a paywall does not represent a real obstacle for misuse, this risk exists irrespective of open-access publishing and open research data. The issue, once again, lies on access control, good scientific practices and safe collaborations – factors that enable research to be rooted in its original context and keep its purposes.

Scenario 6 – Example of potential misuse of scientific knowledge

A university researcher submits a paper about a new software-based method to improve drone flight stability in difficult weather conditions. The study was done entirely in computer simulations using a virtual model of a small consumer drone. No real drone was used or tested. The research focuses on general flight-control methods that are already widely used in civilian engineering and combined them with AI-based automatic adjustment techniques. The approach is not designed for any specific drone or military purpose.

During the publication review, however, concerns are raised that such methods could potentially be misused to improve small drones used in the Russia-Ukraine war and thereby create military risks.

Scenario 7* – Example of potential misuse of scientific knowledge

A researcher publishes on X data concerning vaccines. A political entity re-publishes the post with an opposite message reaching a massive audience; the political entity instrumentalised knowledge so that it could fit its political agenda.

Risk 4: Undue interference, manipulation or corruption of knowledge

The term “interference” comprises “malign activity by another state or those acting on its behalf that is designed to have a detrimental effect” on the interests of a given country.²⁹ “This activity can be deceptive, coercive or corruptive. It includes the use of agents of influence, leverage of investments, financial inducement, disinformation and disruptive or malicious cyber-activities”.³⁰ Reasons for interference are diverse, for instance, political, ideological, or economic. Interference can be direct or indirect and can take several forms such as knowledge alteration, removal, falsification, and (self-)censorship.

Published datasets or publications on public repositories, for example, could be modified to fit a political narrative; in other cases, publications financed by governmental entities could carry fake information that reinforce their agenda, while creating a high impact on public opinion.

Open data and open publications stored in open repositories could be deliberately erased because of political reasons or by strategic interests. Even when backup copies exist elsewhere, large-scale accessibility can be temporarily or permanently disrupted, undermining visibility of knowledge.

Scenario 8 – Example of undue interference

In early 2025, data that was not aligned with the US presidential administration’s priorities was removed by public federal databases without notice. Among others, interested datasets are: the Federal Workforce Data (FedScope), where race and ethnicity columns were removed; the Inmate statistics, where data on transgender inmates was removed; the National Crime Victimization Survey (NCVS) where three gender identity questions were removed.

Other data, such as those made available by the US National Oceanic and Atmospheric Administration (Noaa), were removed with notice.

As it becomes clear from these practical examples, Knowledge Security risks arising from Open Science practices can create serious vulnerabilities affecting national security and strategic competitiveness. They may compromise the integrity, reliability, and reproducibility of research, and ultimately erode public trust in science and innovation.

At the same time, such risks can have profound consequences for individuals and institutions alike. These may include legal liability, regulatory sanctions, loss of funding, and substantial reputational harm.

²⁹ Universities UK (UUK). *Managing Risks in International Research and Innovation*. London: Universities UK, 2020: 23. https://www.universitiesuk.ac.uk/sites/default/files/field/downloads/2022-06/managing-risks-in-international-research-and-innovation-uuk-cpni-ukri_1.pdf.

³⁰ Ibidem

3. Factors leading to Knowledge Security risks in Open Science

In order to understand why the Knowledge Security risks described in Chapter 2 materialise in the Open Science context, the following Chapter discusses the factors that may lead to or increase these risks.

u^b

Three main categories of factors can be identified as leading to or increasing the risk that the publication of knowledge is a regulatory infringement, that knowledge be misused, stolen, influenced, altered, manipulated, corrupted, or faked:

- a) The *content* of open data and open publications
- b) The *partners* with whom open data and publications are produced, managed and shared
- c) The *infrastructure* that supports and enables open data and open publications.

Identifying risk factors also helps defining risk mitigation strategies which will be addressed in the Toolbox that accompanies this report.

3.1. Content

The first risk factor is the nature of the dataset or the content of a publication. This section presents three approaches for assessing whether a research topic should be considered sensitive or pose Knowledge Security risks. The first approach focuses on the legal concept of dual-use research, specifically research involving items listed in federal Goods Control Lists within the framework of export control regulations. The second and third approaches – critical technologies and sensitive research areas – extend beyond this legal definition by identifying additional categories of research that may warrant heightened attention from a Knowledge Security perspective, even where no export control obligations apply.

3.1.1. Export-controlled research

Content with strategic value, whether for economic competitiveness, scientific advancement, or military applications, is particularly vulnerable to misuse. Such content may be stolen, manipulated, falsified, altered, erased, or exploited for purposes that conflict with the intentions of the researchers or their institutions.

Research data and publications involving dual-use items – that is, items with both civilian and military applications, or items that could contribute to the development of weapons of mass destruction and their delivery systems, facilitate human rights abuses, or support acts of terrorism – are at an elevated Knowledge Security risk.

In Switzerland, dual-use items are defined in the [federal Goods Control Lists](#) under the export control regime. Data, technology, software, and publications relating to these controlled items may not be shared openly without prior authorisation from the State Secretariat for Economic Affairs (SECO), where required.³¹

³¹ Export controls are based on international agreements and resolutions, such as the Chemical and Biological Weapons Convention, the Treaty on the Non-Proliferation of Nuclear Weapons and the four international export control regimes which are the Wassenaar Arrangement, Nuclear Suppliers Group, Missile Technology

Examples of controlled dual-use items include:

- Advanced machine tools (e.g., high-precision CNC machines)
- Electronics and microprocessors
- Telecommunications and encryption systems
- Sensors and lasers
- Navigation and avionics systems
- Marine equipment
- Aerospace components
- Chemicals and biological agents
- Nuclear-related materials and equipment.

In addition to the listed items, the “catch-all clause” in Article 3(4) of the Goods Control Ordinance extends export controls to non-listed goods, technology, and software if they are intended for the development, manufacture, use, transfer, or deployment of nuclear, biological, or chemical weapons or their means of delivery.

Export control regulations therefore constitute an important Knowledge Security measure by reducing the risk of unintended transfers of strategically sensitive knowledge. A list of tools for identifying dual-use and export-controlled goods, technology, and software in research outputs is provided in the Toolbox that accompanies this report.

3.1.2. Critical technologies

Not all research with potential military or criminal applications is covered by export controls, though. This is partly due to the fact that the concept of “dual use” is extremely broad and not coherently defined by a common methodology. As highlighted by Stanton,

[a] recurrent approach frames dual-use in relation to Technology Readiness Levels (TRLs), where dual-use potential is seen as becoming more meaningful at higher TRLs closer to end-user application, while early-stage or low-TRL research is considered difficult to classify as dual-use. Another strand conceptualises dual-use as knowledge or technology transfer between civilian and military domains, often emphasising spillovers from civil research into defence applications rather than the reverse. [...] Several documents highlight the need to clarify boundaries between civilian, dual, and military research (5), reflecting concerns about blurred categories and regulatory uncertainty.³²

Publications, research results, technical reports, designs, source code, and open-source software that are already in the public domain, as well as the outcomes of fundamental research, generally fall outside the scope of export control regulations. However, the absence of export control restrictions does not automatically mean that openly sharing such knowledge is without risk. Research that

Control Regime, and Australia Group. National implementing legislation has been adopted in all state parties. In Switzerland, export controls are regulated through the War Material Act (SR 514.51) and the War Material Ordinance (SR 514.511); the Goods Control Act (SR 946.202) and the Goods Control Ordinance (SR 946.202.1); the Chemical Weapons Control Ordinance (SR 946.202.21); the Ordinance on the Export and Brokerage of Goods for Internet and Mobile Communication Surveillance (SR 946.202.3); the Intelligence Service Act (SR 121); and the Embargo Act (SR 946.231). Other laws may apply, such as coercive measures enacted by the Federal Council.

³² *Dual-use Research and Innovation in Europe and Switzerland*: 23.

appears harmless today may acquire strategic significance or enable unintended applications as scientific capabilities and geopolitical circumstances evolve.

It is, therefore, important to consider not only whether the dissemination of research is legally permissible, but also whether the knowledge could pose security concerns despite falling outside the legal framework. Researchers should reflect on how their work could reasonably be expected to be used – or misused – in the future. For this reason, a Knowledge Security assessment should extend beyond export-controlled technologies to include broader categories of critical technologies and sensitive research areas.

To support such assessments, several jurisdictions and international organisations, including the European Union, Australia, and Canada, have published lists of critical technologies.³³ Although these technologies are not necessarily subject to export controls, they are considered strategically important because they have a high potential for misuse or could significantly affect national security, economic competitiveness, or the protection of human dignity, life, health, freedom, property, the environment, or international peace.

Across these lists, the following technology areas consistently emerge as critical:

- Artificial intelligence / AI & machine learning
- Quantum technologies (quantum computing / communications / sensors)
- Biotechnologies / life sciences
- Advanced materials, advanced manufacturing and recycling technologies (including semiconductors / microelectronics)
- Robotics and autonomous systems
- Advanced sensing / surveillance / positioning / timing (sensors, PNT, advanced imaging, etc.)
- Space / aerospace / satellite technologies)
- Advanced energy technologies / energy storage / clean energy
- Advanced information & communications / digital infrastructure (5G/6G, high-performance computing, cloud/edge, cyber / cryptography).

The European Union identifies artificial intelligence, quantum technologies, semiconductors, and biotechnologies as particularly critical because of their strategic importance and high potential for misuse.

Scenario 9 – Example of potential misuse of scientific knowledge in open access publishing

³³ European Commission. *Annex to the Commission Recommendation on Critical Technology Areas for the EU's Economic Security for Further Risk Assessment with Member States*. C(2023) 6689 final. Strasbourg, October 3, 2023. [C_2023_6689_1_EN_annexe_acte_autonome_part1_v9.pdf](#); See also European Commission. *Commission Recommendation (EU) 2023/2113 of 3 October 2023 on Critical Technology Areas for the EU's Economic Security for Further Risk Assessment with Member States*. Official Journal of the European Union L, 2023/2113, October 11, 2023. [Commission Recommendation \(EU\) 2023/2113 of 3 October 2023 on critical technology areas for the EU's economic security for further risk assessment with Member States](#) Australia, actually, has developed four lists: a [List of Critical Technologies in the National Interest](#) | Department of Industry Science and Resources; a list of [critical minerals](#); a list of [strategic materials](#); a list of [defence and strategic goods](#). [Sensitive Technology List - Canada.ca](#);

A group of researchers publishes an open access article on pathogen detection in aquaculture, with the stated objective of enhancing biosecurity, animal health, and the economic competitiveness of the sector. The article provides an overview of molecular and technological innovations for pathogen detection and monitoring, focusing on recently developed point-of-care and on-site diagnostic systems. They also discuss techniques from other disciplines, such as CRISPR-Cas protocols for pathogen detection. While these methods demonstrate to be effective for pathogen surveillance and mitigation, they also create potential avenues for misuse.

By systematically describing diagnostic platforms that function independently of complex laboratory infrastructure and cold chain logistics, the publication lowers technical and logistical barriers to advanced pathogen detection, thus enabling malign actors to map pathogen prevalence, antimicrobial resistance markers, or microbial vulnerabilities in aquaculture.

Switzerland has not yet adopted an official list of critical technologies. Nevertheless, the National Working Group on Knowledge Security has recommended establishing a comprehensive framework for assessing the security implications of research and emerging technologies. Such a framework should consider factors including potential military applications, technology readiness level (TRL), strategic economic value, vulnerability to foreign exploitation, and relevance to Swiss national interests.³⁴

As an institutional example, ETH Zurich has developed a non-exhaustive list of technology areas used in its internal [security screenings](#) process. The list reflects the university's research profile and includes additive manufacturing, applied chemistry and physics, biochemistry, biotechnology, blockchain, chemical technology, cybersecurity and cyber surveillance, digital technologies, electrical and mechanical engineering, advanced manufacturing, advanced and intelligent materials, artificial intelligence, aerospace technologies, measurement technologies and sensors, nanotechnology, nuclear technologies, photonics, production and process engineering, quantum technologies, and telecommunications and information technology.

At ETH Zurich, security screening is generally required for applied research within these technology areas once a project reaches Technology Readiness Level 4, where the technology has been validated in a laboratory environment. The [Technology Readiness Level framework](#), originally developed by NASA and later adopted by the European Union in the Horizon research programmes, provides a standardised method for assessing the maturity of a technology, from basic scientific principles (TRL 1) to fully operational systems (TRL 9):

At Technology Readiness Level (TRL) 1, work is still at the stage of fundamental research. Scientific inquiry has only just begun, and early findings primarily serve to inform and shape subsequent research and development activities. At TRL 2, the underlying scientific principles have been explored in more depth, and initial experimental concepts or test approaches are formulated on the basis of those preliminary insights. At this point, the technology remains largely theoretical and exploratory in nature. Once experimental or test results provide empirical support for the original concept, the technology progresses to TRL 3. This stage typically involves both analytical investigations and controlled laboratory studies to determine whether the concept has

³⁴ *Knowledge Security in Switzerland: A Strategic Framework for Higher Education Institutions and Authorities: 16. See also Hufschmid, Manon. Enhancing Knowledge Security in Switzerland: Providing a Source of Inspiration for SwissCore Funders and Partners. Brussels: SwissCore, 2025.*

sufficient validity to justify further development. A proof-of-concept model is usually developed at this level. Achieving TRL 3, therefore, indicates that, from a scientific perspective, the proposed technology is feasible.³⁵

Following the German Science and Humanities Council,

u^b

up to and including TRL 3, it is often assumed that a possible use is still too unpredictable to carry out a meaningful risk assessment. However, there are fields, such as cryptography or AI, in which the time between basic discovery and development of a prototype can be less than a year, making the TRL less meaningful in these areas. [...] Indications cannot be considered in isolation in the sense of a checklist, but must be assessed in an overall view. In the case of a TRL 2 in a non-critical field of research, pure cooperation without personnel exchange could be categorised as unproblematic, even with partners from critical countries.³⁶

Lists of critical technologies can be useful tools for higher education institutions, as they help define areas that require attention in terms of Knowledge Security risk screening. However, such lists can be no more than a starting point or a way to narrow down the areas where particular attention is required, for instance, in recruitment or international collaborations, as they do not actually determine the potential misuse of a given technology. In addition, they are necessarily constantly outdated as science is often faster than politics and diplomacy. They are also incomplete because Knowledge Security risks can also occur in the humanities and social sciences – and not only in the natural sciences.

3.1.3. Sensitive research areas

Therefore, in addition to considering dual-use and critical technologies, assessing the research area itself provides a complementary perspective on Knowledge Security risks. In fact, some fields of research are inherently more exposed to geopolitical sensitivities, foreign interference and political pressure. In such cases, research outputs may be particularly vulnerable to misuse, manipulation, misrepresentation, or appropriation, even when they do not fall within the scope of export control or dual-use regulations. Consequently, Knowledge Security assessments should also take into account research areas that, due to their subject matter or societal implications, are especially susceptible to political influence or exploitation, such as:

- Climate and environment
- Public health and epidemiology
- Gender, sexuality and minority studies
- Human rights and governance research
- Migration and demographic data
- Historical studies

Some of these categories have in fact been defined as constituting “sensitive personal data” in the Federal Act on Data Protection (art. 5 lit. c):

- data relating to religious, philosophical, political or trade union-related views or activities
- data relating to health, the private sphere or affiliation to a race or ethnicity

³⁵ European Commission. *Guiding Notes to Use the TRL Self-Assessment Tool*. Horizon Europe. Brussels: European Commission, 2021. [trl-assessment-tool-guide-final.pdf](#)

³⁶ German Science and Humanities Council. *Science and Security in Times of Global Political Upheaval*. Position Paper. Cologne: German Science and Humanities Council, 2025:38-39. [Science and security in times of global political upheaval | Position paper, Cologne \(Drs.-2485-25_en\), May 2025](#)

- genetic data
- biometric data that uniquely identifies a natural person
- data relating to administrative and criminal proceedings or sanctions
- data relating to social assistance measures.

There is currently no nationally agreed mapping of sensitive data types or shared categorisation for research data across higher education institutions. The Swiss Research Data Stewardship Network (SRDSN) has initiated discussions on a common classification.

Scenario 10 – Example of potential misuse of scientific knowledge in open access publishing

An open access 2021 publication examines the consumption of online jihadist media among young adults and assesses how exposure relates to cognitive radicalisation, while considering moral disengagement, prior involvement in petty crime, and socio-demographic factors. The findings indicate that beheading videos – although the most widely consumed content among the target group (36% of consumers) – have a lower radicalisation potential than online magazines produced by the so-called Islamic State and Al-Qaeda, despite the latter being read by only a small minority (10–11%).

As noted by the German National Academy of Sciences Leopoldina, that highlighted this case, while such insights are valuable for understanding and preventing online radicalisation, they could also be exploited by extremist and terrorist groups to refine and enhance their online recruitment strategies.³⁷

Scenario 11* – Example of potential misuse of scientific knowledge in open access publishing

A group of researchers conducts a study on homosexuality in Uganda to map patterns of discrimination since the introduction of the Anti-Homosexuality Act (2023). The project is funded by public sources and, in line with the funding requirements, had to be published open access.

During fieldwork, the researchers collected qualitative and quantitative information from local sources, including testimonies from affected individuals, community representatives, and local NGOs. They identified geographic areas where discrimination was reported to be more frequent, described typical contexts in which abuses occurred (e.g., housing, employment, healthcare), and analysed the profiles of key victims (e.g., gender identity, age group, social position).

Although all sources were formally anonymised, the combination and cross-referencing of data points, such as specific geographic areas, detailed discrimination contexts, gender identity, age, occupation, and time of incident, created a significant risk of indirect identification. In a context where homosexuality is criminalised and socially stigmatised, even partial re-identification could expose individuals to severe consequences, including arrest, social exclusion, violence, or loss of livelihood.

³⁷ German National Academy of Sciences Leopoldina, and German Research Foundation (DFG). *Scientific Freedom and Security Interests in Times of Geopolitical Polarisation: Fifth Report of the Joint Committee of DFG and Leopoldina*. Halle (Saale): German National Academy of Sciences Leopoldina, November 1, 2024: 67.

Open access publication of granular data (for example, maps highlighting specific neighbourhoods, detailed case descriptions, or small-sample statistics for narrowly defined groups) may unintentionally increase the risk to participants. Moreover, local authorities or hostile non-state actors could potentially use the published information to target specific communities or individuals.

u^b

In conclusion, when data or the content of a scientific article contains export-controlled technology or software or otherwise protected information (for instance under privacy or intellectual property laws, or under a contract), there is a risk that their publication constitutes a form of unwanted knowledge transfer as it would violate legislative or contractual rules. In addition, data or publications referring to critical technologies or other sensitive research areas are prone to be misused, stolen, influenced, altered, manipulated, corrupted, or faked.

Therefore, it is advisable to conduct case-by-case assessments of the risks around research projects involving protected or controlled information, or involving critical technologies or otherwise sensitive information. Useful tools for conducting such assessments will be proposed in the Toolbox that accompanies this report.

3.2. Partners

International collaboration is a fundamental component of modern research and contributes significantly to scientific excellence, innovation, and the exchange of knowledge. At the same time, the increasing complexity of geopolitical contexts and research ecosystems requires researchers and institutions to consider potential Knowledge Security risks arising from international partnerships.

Research data and publications may be vulnerable to misuse, theft, alteration, falsification, manipulation, or deletion when researchers collaborate with partners operating under political or military pressure, or in contexts where standards of transparency, security, academic freedom, or research integrity differ from those upheld in Switzerland. Such risks cannot be assessed solely on the basis of a partner's country of origin or affiliation. Instead, these factors should be evaluated case by case, applying a country-agnostic and risk-based approach as suggested by the national report *Knowledge Security in Switzerland: A Strategic Framework for Higher Education Institutions and Authorities*.

Though, as general indicators, potential risk factors related to partners may include:

- Countries: Countries subject to applicable sanctions or embargoes; countries involved in armed conflicts or systematic human rights violations; and countries with particularly low scores in internationally recognised indicators of academic freedom, democracy, or human rights.
- Institutions: Institutions located in sanctioned or embargoed countries; institutions with links to military actors or defence-related activities; and institutions operating in countries affected by armed conflict or systematic human rights violations.
- Individuals: Individuals subject to applicable sanctions; individuals with military affiliations; and individuals who are based in, operate in, or have significant links to countries affected by armed conflict or systematic human rights violations.

These three categories are described in greater detail in the following sections. Beyond sanctions, military links, conflicts, and human rights concerns, partnership assessments could also consider additional factors, including limited transparency regarding academic affiliations, institutional interests, or contractual arrangements; reputational risks (for example, previous breaches of scientific integrity); persistent asymmetries in knowledge exchange; and structural dependencies that may affect research autonomy – depending on one’s institution’s priorities and values.

u^b

Knowledge Security risks arising from scientific relations with academic partners apply to both formal and informal collaborations, including publicly funded research projects that are often subject to Open Science requirements, particularly regarding open access to publications and open data practices. Openness is a fundamental principle of scientific progress; however, it also requires consideration of how, with whom, and under what conditions research knowledge is shared. To effectively define and manage risks in both open science and non-open science activities, several contextual factors need to be considered and balanced through an integrated risk assessment approach.

To navigate this balance between openness and security, research projects with international partners are increasingly encouraged to follow the principle of Responsible Internationalisation. Responsible Internationalisation is a process “for identifying, assessing, managing, and monitoring opportunities and risks in research collaborations,”³⁸ and ultimately ensuring safe international collaborations. Although the term does not yet have a fully standardised framework with clearly defined objectives and assessment processes, it has become an established principle among universities, research funders, and policymakers, both nationally and internationally (e.g., at the University of Zurich; see Section 4.3.7; see also swissuniversities’ guidelines [Towards Responsible International Collaborations: A Guide for Swiss Higher Education Institutions](#)).

According to Shih,

responsible internationalization focuses on the discretionary responsibilities that researchers have when building international relationships. This means that researchers need to develop their ability to reflect on contextual factors so that a complex portfolio of risks encountered when national borders are crossed can be proactively and realistically managed. For responsible practices to be effective they also need to be co-created in relationships, rather than representing the expectations of one side only.³⁹

Responsible internationalisation, therefore, aims to increase “knowledge of foreign interference, while also safeguarding fundamental rights and values of academic freedom, integrity and autonomy.” Openness remains a key element of responsible internationalisation, together with transparency, security, freedom, and integrity. The objective is not to limit international collaboration, but to enable researchers and institutions to engage in partnerships in a way that preserves the benefits of openness while reducing vulnerabilities.

Applying responsible internationalisation requires an integrated assessment of contextual factors throughout the lifecycle of a collaboration. This applies both to Open Science activities and to other forms of research cooperation. Practical guidance for conducting such assessments is provided in the Toolbox that accompanies this report.

³⁸ Council of the European Union. *Knowledge Security and Responsible Internationalisation*. Brussels: Council of the European Union, 2023: 3. <https://data.consilium.europa.eu/doc/document/ST-8824-2023-INIT/en/pdf>.

³⁹ Shih, Tommy. "Points of Departure and Developing Good Practices for Responsible Internationalization in a Rapidly Changing World." *Accountability in Research* 32, no. 5 (2025): 848.

3.2.1. Legal sanctions and country-related embargoes

International collaborations may give rise to legal risks when they involve partners that are subject to sanctions or are located in countries subject to sanctions or embargoes. These risks extend beyond financial transactions and may also affect common research activities, including the transfer of research data, the sharing of technology or software, access to laboratory infrastructure, and other forms of scientific cooperation. Depending on the circumstances, different sanctions regimes – such as Swiss, European Union, or U.S. measures – may apply simultaneously, each imposing distinct legal restrictions on collaborations involving particular countries, institutions, or individuals.

From a Knowledge Security perspective, sanctioned partners warrant particular attention because sanctions are generally imposed in response to activities that are considered to threaten international peace and security, involve serious human rights violations, support military capabilities, or otherwise conflict with the foreign and security policy objectives of the sanctioning jurisdiction. While the existence of sanctions does not, in itself, determine the nature or intentions of an individual researcher, institution, or country, it is an important indicator that a collaboration may involve heightened legal, ethical, and security risks.

A distinction should, nevertheless, be made between sanctioned individuals or entities and partners located in sanctioned or embargoed countries, as the associated legal risks differ. Collaborations involving sanctioned persons or organisations are affected by the prohibition on making funds or economic resources available (“*Bereitstellungsverbot*”), which significantly limits the scope for lawful cooperation. By contrast, collaborations with partners located in sanctioned or embargoed countries are primarily governed by country-specific restrictions, which may limit or prohibit the transfer of goods, technology, software, services, or other research-related activities depending on the applicable sanctions regime.

Resources for identifying sanctioned countries and individuals can be found in the Toolbox that accompanies this report.

3.2.2. War and military activities

Armed conflicts and military involvement can constitute significant risk factors in international research collaborations. Collaborations involving partners located in countries affected by armed conflict, territories under military occupation, or regions experiencing international or non-international armed conflicts may increase the likelihood that research outputs, technologies, or expertise are diverted to military purposes or other unintended applications. Likewise, collaborations with individuals or organisations that have military affiliations or are linked to defence activities may increase the risk that research with civilian objectives acquires dual-use relevance. In addition to potential Knowledge Security concerns, such collaborations may expose researchers and institutions to legal, ethical, and reputational risks.

For these reasons, many research institutions examine whether prospective collaborators have current or previous military affiliations or maintain relationships with defence organisations. Such assessments may consider international affiliations, collaboration networks, funding sources, publication records, patent activities, data management practices, and participation in research

projects or clinical trials. Resources for identifying potential military connections of academic partners are provided in the Toolbox that accompanies this report.

Several countries have also developed lists of organisations considered to present elevated national security risks. Examples include Canada's [Named Research Organizations List \(NRO\)](#), and the Hague Centre for Strategic Studies' [checklist](#) for assessing risks associated with cooperation with Chinese research institutions. These resources can support preliminary screening by highlighting organisations that may warrant enhanced due diligence.

Switzerland has not adopted a comparable national list. Moreover, even where such lists exist, they should be regarded as complementary tools rather than definitive assessments. They require continuous updating, may not capture changes in organisational structures or affiliations, and can be circumvented where links to military or security actors are not transparent. Consequently, while institutional watchlists can assist in identifying potential risk factors, they cannot replace a contextual, project-specific assessment. The relevance of military links or conflict-related factors should always be evaluated on a case-by-case basis, taking into account the nature of the collaboration, the research involved, and the applicable legal and Knowledge Security considerations.

Scenario 12 – Example of research cooperation with a country at war and possible export control violation

In 2009, a partnership between a European institute and a Russian institution was launched, funded jointly by a European (national) space agency and the Russian Space Agency (Roscosmos). Several other partnership proposals had been rejected by other funding agencies, which made the Russian collaboration particularly appealing. In addition, Russia shared similar scientific interests and could contribute critical expertise in areas such as launch capabilities, data transmission, and spacecraft engineering. The initiative was also strongly supported by Russian scientists working in the EU. At that time, international scientific cooperation with Russia was broadly encouraged. Given the extremely high cost of space astronomy, forming a partnership seemed both strategic and necessary.

The mission was designed to survey the entire sky over four years using two telescopes, a European one and a Russian one. Costs for the mission were shared equally. A first Memorandum of Understanding (MoU) signed in 2009 stipulated that Europe's 50% share of the proprietary data had to be made public no later than two years after achieving a robust and stable instrument calibration. Russia's 50% would be released on a schedule to be determined following launch.

A second agreement signed in 2011 reaffirmed that each partner would receive 50% of the mission's scientific data, corresponding to the portion of the sky allocated to them for analysis. The telescopes themselves from the European telescope, along with essential technical information required for calibration, were shared between the partners.

The European telescope was successfully launched in 2019 and operated for three years. However, following Russia's invasion of Ukraine in February 2022, the European institution's leadership recommended that the EU team halt all cooperation with Russian partners, who were now subject to sanctions. Although that specific telescope was not classified as a dual-use instrument according to the EU team, continuing collaboration risked violating restrictions on assisting Russia

in the collection of telescopic data – particularly given that the Russian Space Agency includes a military division. Reputational concerns also played a major role: maintaining cooperation during the war would have damaged the public image of both the European institution and the European space agency. Moreover, EU scientists had already acquired a substantial amount of data and were confident they could achieve most of their scientific goals independently. According to the European team, data-publication imbalance between EU and Russia should have also been considered.

For these reasons, the EU team decided to suspend further data collection and cease all technical and scientific collaboration with Russia. Nevertheless, calibration, data processing, and publication of the existing telescopic data will continue until 2028.

Scenario 13 – Example of research cooperation with a country at war

A Swiss researcher plans to apply for a Horizon Europe grant, which requires open access to publications, together with a collaborator from an Israeli university. Before proceeding, the university assesses the collaboration from a Knowledge Security perspective. Although the researcher notes that the collaborator does not personally support Israeli government policies, the assessment finds that the university maintains links with the military. This raises concerns about the reputational implications of supporting an institution that contributes to Israeli defence capabilities and increases the perceived risk of unintended military applications, given the dual-use potential of the research. On this basis, the university recommends placing the collaboration on hold.

3.2.3. Human rights violations

The involvement of academic partners in serious human rights violations can constitute an important Knowledge Security risk in international research collaborations. Beyond ethical and reputational concerns, collaborations with institutions, organisations, or individuals implicated in human rights abuses may increase the likelihood that research outputs, expertise, data, or technologies are used in ways that facilitate repression, discrimination, surveillance, or other violations of fundamental rights.

Although international human rights standards are well established through international treaties and domestic legislation, their application to research partnerships often requires contextual evaluation. As highlighted in the University of Lausanne’s report [Ethical considerations in external collaborations](#), higher education institutions should establish clear principles governing international collaborations before assessing individual cases. These principles provide a framework for evaluating whether a particular collaboration is compatible with the institution’s ethical responsibilities and knowledge security objectives.

In this context, it is also useful to distinguish between institutional agreements and project-specific collaborations. Institutional partnerships create privileged and long-term relationships between organisations and, therefore, carry a stronger political and symbolic significance.⁴⁰ By contrast,

⁴⁰ Schmid, Evelyne. “Ethical Considerations in External Collaborations: The Report of a Working Group at the University of Lausanne (7/9).” *Oxford Human Rights Hub* (blog), May 30, 2026. <https://ohrh.law.ox.ac.uk/ethical-considerations-in-external-collaborations-the-report-of-a-working-group-at-the-university-of-lausanne-7-11/>.

individual research projects are more diverse and may, in some circumstances, justify collaboration with partners operating in challenging contexts, provided that the associated legal, ethical, and Knowledge Security risks are carefully assessed and appropriately mitigated.

This differentiated approach is also reflected in the [Foreign Policy Strategy of the Swiss Confederation](#), which recognises that Switzerland may maintain scientific and diplomatic relations with strategically important countries despite disagreements on human rights, while continuing to promote respect for fundamental rights and international law.⁴¹

Accordingly, the existence of human rights concerns should not automatically preclude scientific collaboration. Rather, it should be regarded as a significant Knowledge Security risk factor requiring a thorough, case-by-case assessment of the partner's role, the nature of the research, the potential for misuse of research outputs, and the broader legal, ethical, and geopolitical context.

3.2.4. Political influence and dependencies

Political influence in higher education institutions refers to

attempts by a foreign actor to influence the perceptions of staff, scholars and students [...] with the aim of aligning research, education and the international academic debate with the strategic visions, opinions, interests or political system of a foreign actor, which are not supported by the receiving side and or are contrary to the receiving side's norms and values.⁴²

In the context of Knowledge Security, political influence represents a risk when external actors are able to affect the independence, integrity, or direction of knowledge production and dissemination. Such influence is often shaped by structural dependencies in terms of funding, infrastructure, access to data, or specialised know-how. In these contexts, Swiss-based actors – including researchers, scientific officers, technical staff, and students – may become vulnerable to pressure from foreign partners on whom they rely for critical resources or knowledge, for example through participation in talent programmes involving scholarships and specific affiliations.

Within Open Science collaborations, particularly those involving public institutions abroad, these power dynamics can manifest in various ways, including:

- Censorship and self-censorship in open access publications and open research data;
- False, incomplete, or biased knowledge in Open Access publications and open research data;
- Violation of non-disclosure obligations through Open Access publications and open data;
- Theft of protected knowledge through open science infrastructures or academic collaborations fostered by Open Science, including funding and networking activities;
- Erasure of knowledge through Open Science infrastructures or academic collaborations fostered by open science, including funding and networking activities.

Open Access publications – even when issued by established international publishers – may, in certain collaborative contexts, become subject to de facto censorship constraints. This risk can arise,

⁴¹ Swiss Confederation, *Foreign Policy Strategy 2024–2027* (Bern: Federal Department of Foreign Affairs, 2024: 26.

⁴² d'Hooghe, Ingrid, and Jonas Lammertink. *Towards Sustainable Europe-China Collaboration in Higher Education and Research*. Leiden: Leiden Asia Centre, 2020: 58.

for example, when editorial responsibilities involve individuals affiliated with critical institutions and when articles address politically sensitive topics related to critical countries. Attention should also be paid to the framing of acknowledgements. In some cases, collaborators may propose including politically framed statements, such as references to the role of the state or political leadership, even in technical or scientific outputs.

u^b

The central Knowledge Security concern is that dependencies within international collaborations may affect the integrity, independence, and availability of scientific knowledge. External pressure may influence not only what knowledge is produced, but also what knowledge is published, how it is framed, and who has access to it. These risks are particularly relevant in Open Science environments, where transparency and accessibility facilitate the dissemination of knowledge but may also create additional pathways for unintended influence, appropriation, or manipulation. Maintaining openness therefore requires consideration of the conditions under which knowledge is shared and the dependencies that may affect research autonomy.

A specific dimension of strategic dependency concerns the digital infrastructures that increasingly support research and knowledge exchange. As noted by Baums and Butts,⁴³ organisations are deeply dependent on IT infrastructures controlled by a small number of dominant technology oligopolies. These actors effectively govern access, usability, and transparency across digital systems. Such concentration of power not only enables the largely unchecked flow of data but also creates conditions for targeted influence and manipulation.

This dynamic is often described as a “tech cold war,” reflecting intensifying competition over digital dominance. The stakes are rising further with the growing centralisation of AI development within major technology firms. These companies are increasingly positioned to control not just the software itself, but also the datasets that underpin and shape AI systems – granting them unprecedented influence over how knowledge is produced, distributed, and applied.

As highlighted by the Royal Society, “[c]entralisation of AI development under large technology firms (e.g. Google, Microsoft, Amazon, Meta and Alibaba) could lead to corporate dominance over infrastructure critical for scientific progress. This includes ownership over massive datasets for training AI models, vast computing infrastructures, and top AI talent.”⁴⁴

The increasing influence of major multinational data companies and the growing number of cyberattacks against higher education institutions by foreign entities highlight the potential for the digital space to be used as an instrument of power in political, economic, and academic contexts.

These developments raise the question of digital sovereignty, defined by the Swiss Federal Council in the report [Souveraineté numérique de la Suisse](#), as « la capacité de contrôle et d’action nécessaire dont dispose l’État dans l’espace numérique afin de garantir l’accomplissement de ses tâches. »⁴⁵

⁴³ Baums, Ansgar, and Nicholas Butts. *Tech Cold War: The Geopolitics of Technology*. Boulder, CO: Lynne Rienner Publishers, 2025.

⁴⁴ The Royal Society. *Science in the Age of AI: How Artificial Intelligence Is Changing the Nature and Method of Scientific Research*. London: The Royal Society, October 2024:72.

⁴⁵ Swiss Federal Council. *Souveraineté numérique de la Suisse*. Bern: Swiss Federal Council, 2025: 1. The Federal Council’s 2021–2024 *Digital Foreign Policy Strategy* already identified several key dimensions of Switzerland’s digital sovereignty, including geopolitical tensions, the global technology race, and increasing

To enhance Switzerland's independence and strategic autonomy in the digital domain, several measures have been implemented, including the promotion of open-source software to reduce reliance on proprietary technologies and external providers while promoting transparency, interoperability, security, and innovation.

L'utilisation et l'autorisation de mise à disposition de logiciels à code source ouvert permettent de réduire les dépendances à l'égard des fournisseurs et, partant, d'accroître la liberté d'action. [...] La création et le renforcement des capacités en matière de logiciels ouverts permettront à la Confédération d'établir un marché de prestataires pour les développements répondant à ses besoins propres et de réduire ainsi les dépendances à l'égard des fabricants. Par ailleurs, le secteur TNI de la Chancellerie fédérale a lancé en 2024 une étude de faisabilité sur l'utilisation de logiciels à code source ouvert pour la bureautique de l'administration fédérale. Cette étude évalue l'adéquation des logiciels à code source ouvert en tant que solution de secours pour le traitement des données sensibles en cas de défaillance de la solution bureautique principale.⁴⁶

A similar approach is reflected in the European Union's [Open Source Strategy](#), unveiled on 3 June 2026 as part of the [EU Technological Sovereignty Package](#), which promotes the use of open technologies to reduce dependence on non-European technology providers.

In conclusion, Open Science increases the circulation and accessibility of knowledge, but this openness can create vulnerabilities when research ecosystems depend on actors that have the capacity or incentive to influence what knowledge is produced, shared, suppressed, or controlled. Reducing strategic dependencies does not imply limiting international collaboration or openness. Rather, it aims to preserve the conditions necessary for Open Science by ensuring that researchers and institutions retain sufficient autonomy, control, and resilience over the infrastructures, partnerships, and resources on which knowledge production depends.

3.2.5. Data imbalance in knowledge sharing

Successful international research collaborations rely on reciprocity in the exchange of knowledge, data, expertise, and research infrastructure. In the context of Open Science, where openness and data sharing are fundamental principles, asymmetries may arise when partners are unable or unwilling to contribute equally to the exchange of research outputs. Such imbalances may allow one partner to benefit disproportionately from the collaboration while limiting reciprocal access to data, publications, or scientific resources. They may also reduce transparency, hinder reproducibility, create structural dependencies, and increase the risk of unintended knowledge transfer. Similar asymmetries have been observed in scientific collaborations with countries such as China and Russia (see scenarios below).

China illustrates how differences in national legal and regulatory frameworks can shape the reciprocity of international research collaborations. Restrictions on data sharing form part of a broader and highly controlled governance system that includes extensive export control regimes covering both dual-use items and civilian technologies, the use of entity blacklists, data localisation requirements, constraints on talent mobility, and closely managed trade and investment frameworks.

legal uncertainty. Since 2023, digital sovereignty has also been recognized as a priority theme in the Federal Council's *Digital Switzerland Strategy*. Furthermore, strengthening digital sovereignty is a key objective of the Federal Council's 2024–2027 *Foreign Policy Strategy*. It is also one of the seven strategic priorities of the *Digital Public Administration Strategy*, adopted in December 2023. See *Souveraineté numérique de la Suisse*, p. 2-3.

⁴⁶ Ibidem, 14-15.

Together, these measures may limit reciprocal openness and influence the conditions under which international scientific cooperation takes place. As Arcesati, Chimits and Hmadi observe, “China is not the only country seeking to manage foreign access to ‘sensitive’ technology and the associated value chains, but it stands out for its comprehensive and opaque approach.”⁴⁷

This regulatory environment is also reflected in China’s approach to Open Science.

u^b

Although China has several decades of national open science initiatives and widespread support behind it, the outcomes of open science appear low. The Chinese government’s attitude towards open access publishing and open data can be seen as contradictory. Even though the government appears to be motivated to make research accessible to the public, it also views open access research as a national security risk.⁴⁸

According to Ahlers and Lattu, Open Science in China is becoming increasingly securitised.⁴⁹ This trend is reflected in measures such as the temporary closure and subsequent partial reopening of the [China National Knowledge Infrastructure](#) (CNKI) between 2022 and 2024, while access for foreign researchers remains restricted; the adoption of the Data Security Law ([DSL](#), 2021) and tighter rules governing cross-border data transfers; stricter regulation of health, genetic, human-subject, and other categories of data designated as “core data”; and restrictions on access to international research databases in the context of growing geopolitical tensions.

These developments illustrate how national regulatory frameworks can produce asymmetrical openness in international research collaborations. According to Ahlers and Lattu, they contribute not only to unequal data sharing between international partners, but also to restricted data mobility, creating obstacles for joint projects and cross-border datasets, and to fragmented openness, whereby research fields considered sensitive are excluded from data-sharing practices and repository initiatives. More broadly, such asymmetries may reduce reciprocity within Open Science collaborations and increase Knowledge Security risks by limiting mutual access to research data and scientific outputs while allowing uneven flows of knowledge between partners.

International data transfers as a Knowledge Security risk (China as an example)

Cross-border research collaborations frequently involve the transfer of research data, including personal data. When collaborators operate under different legal frameworks governing access to, disclosure of, and protection of data, these transfers may create both legal compliance obligations and knowledge security risks. In particular, jurisdictions that grant public authorities broad powers to access research data, or that restrict researchers’ control over information, may increase the risk of unintended disclosure, governmental access, or loss of control over valuable research outputs.

China illustrates these challenges. The temporary closure and subsequent partial reopening of the China National Knowledge Infrastructure (CNKI) between 2022 and 2024, together with the

⁴⁷ Arcesati, Rebecca, Chimits, François, and Hmadi, Antonia. *Keeping Value Chains at Home: How China Controls Foreign Access to Technology and What It Means for Europe*. MERICS Report. Berlin: Mercator Institute for China Studies (MERICS), August 2024: 3. <https://merics.org/en/report/keeping-valuechains-home>.

⁴⁸ Lattu, Annina Sofia. *Open Science in China: An Open and Closed Case. Observations: Short Working Papers on Science and Society in China and the World*, no. 13. Berlin: Max Planck Institute for the History of Science, 2023. <https://doi.org/10.17617/2.3553727>; Ye, Josh. “Chinese Authority Launches Probe into Chinese Academic Database CNKI.” *Reuters*, June 24, 2022. <https://www.reuters.com/world/china/chinese-authority-launches-probe-into-chinese-academic-database-cnki-2022-06-24/>.

⁴⁹ Ahlers, Anna Lisa, and Annina Sofia Lattu. “Open Science in China.” Presentation at *Open Science Days 2025*, Berlin, November 10, 2025.

continuing restrictions on access for foreign researchers, reflects the broader regulatory framework established by China's Data Security Law (DSL), which reinforces state control over data and knowledge infrastructures. In parallel, China's Personal Information Protection Law (PIPL) governs the processing of personal data relating to individuals located in China, including cross-border transfers. Consequently, unauthorised transfers of personal data from China to Switzerland may expose researchers and institutions to significant legal consequences, including the application of extraterritorial sanctions.

These differences also have implications under Swiss law. The revised Federal Act on Data Protection (FADP), in force since 1 September 2023, permits international transfers of personal data only where the receiving jurisdiction ensures an adequate level of protection (Art. 16 para. 1 FADP). The Federal Council maintains the list of jurisdictions considered adequate in Annex 1 of the Data Protection Ordinance (DPO). China is not included on that list and is generally regarded as providing an insufficient level of protection.⁵⁰ Consequently, transfers of personal data to China require additional legal safeguards.

Pursuant to Article 16 paragraph 2 FADP, transfers remain permissible in the absence of an adequacy decision where an equivalent level of protection is ensured through appropriate safeguards, such as international treaties, contractual clauses notified to the FDPIC, approved standard contractual clauses, binding corporate rules, or other recognised mechanisms. In decision A-2727/2023 (para. 4.3.4), the Federal Administrative Court confirmed that, although the Federal Council's adequacy list has binding legal effect, cross-border transfers remain lawful where appropriate safeguards have been implemented.

Responsibility rests with the data controller. The Swiss Federal Supreme Court (FSC 6B_219/2022) emphasised that data controllers must evaluate each international transfer on a case-by-case basis. Similarly, the Federal Data Protection and Information Commissioner (FDPIC) has confirmed that the FADP – including its provisions on data security, international transfers, data subject rights, and processing by third parties – applies fully to research activities.⁵¹ Consistently, the [University of Zurich recommends](#) that research collaborations involving controller-to-controller transfers be governed by supplementary data protection agreements.

Beyond compliance with data protection legislation, transfers of research data to jurisdictions where public authorities enjoy extensive access powers may present broader Knowledge Security risks. Researchers and institutions may have limited control over how transferred data are accessed, further processed, or disclosed once they fall under the legal jurisdiction of another state. Given the risk of governmental access to data and the limited legal remedies available to data subjects in China, supplementary technical and organisational measures are often necessary to prevent unauthorised access and maintain effective control over research data.

3.3. Infrastructure

According to UNESCO's 2021 *Recommendation on Open Science*, open infrastructure comprises the virtual and physical facilities needed to support Open Science and serve the needs of different research communities. These include scientific equipment, repositories, archives, journals and open

⁵⁰ Rosenauer, Philipp. "Wenn Sensitive Daten Grenzen Überschreiten." *Procure Swiss Magazin*. procure.ch. Accessed July 17, 2026 <https://www.procure.ch/magazin/artikel/wenn-sensible-daten-grenzen-ueberschreiten>

⁵¹ See federal information sheet [Research \(unrelated to health\) and data protection](#).

access publication platforms, scientific databases, current research information systems, computational infrastructures, virtual research environments, digital research services, and other facilities that enable the creation, management, analysis, preservation, and dissemination of scientific knowledge.⁵²

Open Science infrastructure provides the technical foundation for open access to publications and research data. According to UNESCO, it should offer interoperable and standardised services that enable the management, sharing, discovery, analysis, and long-term preservation of scientific information while ensuring that research outputs remain discoverable and reusable by both humans and machines. Among the different components of Open Science infrastructure, repositories, archives, and open access publication platforms are particularly important because they are specifically designed to facilitate the dissemination of research results.⁵³

The infrastructure supporting Open Science can itself become a Knowledge Security risk. A common misconception is that Open Science infrastructure is “fully open” by definition and therefore of limited interest to malicious actors. In reality, many components of research infrastructures contain valuable information that is not yet publicly available. Research data are rarely released immediately; before publication they typically undergo validation, quality control, interpretation, and legal or ethical review. During these stages, infrastructures may host sensitive information, including source identifiers, personal data, copyrighted material, commercially valuable information, or research with strategic value. These assets may become targets for theft, manipulation, corruption, ransomware attacks, or unauthorised access.

The collaborative nature of Open Science infrastructures also creates specific vulnerabilities. Large federated research infrastructures connect thousands of users and numerous institutions, allowing cyberattacks or technical failures to propagate rapidly across interconnected systems.⁵⁴ As Peisert et al. observe, computing systems supporting scientific research may suffer disruptive security incidents without being specifically targeted, simply because they are connected to exploitable networks.⁵⁵ Such incidents may compromise research data, interrupt scientific activities, or even affect remotely operated scientific instruments.

At the same time, openness can strengthen security when it is implemented appropriately. Public scrutiny increases transparency and enables continuous review by a broad scientific community. As highlighted by the Open Research Community Accelerator (ORCA), transparency has practical implications for software security. The open-source model – illustrated by projects such as Linux and widely used cryptographic libraries – allows vulnerabilities to be identified and corrected more rapidly than is often possible in proprietary environments. Collaborative review improves reproducibility, accountability, and resilience while reducing duplication of effort and facilitating the early detection of errors.⁵⁶

⁵² Ibidem.

⁵³ Ibidem.

⁵⁴ Altunay, Melike, Avery, Patricia, Blackburn, Keith et al. "A Science Driven Production Cyberinfrastructure — the Open Science Grid." *Journal of Grid Computing* 9, 2011: 201–218

⁵⁵ Peisert, Sean, Von Welch, Andrew Adams, Ruth Anne Bevier, Michael Dopheide, Rich LeDuc, Pascal Meunier, Steve Schwab, and Karen Stocks. *Open Science Cyber Risk Profile (OSCRP)*, Version 1.3.3. October 2022. DOI: [10.5281/zenodo.7268749](https://doi.org/10.5281/zenodo.7268749), par. 4 “Introduction”.

⁵⁶ Open Research Community Accelerator (ORCA). 2025. *Fostering Innovation Through Open Science: A Cross-Sector Roadmap for Impact*:19-20. DOI: [10.5281/zenodo.16877389](https://doi.org/10.5281/zenodo.16877389)

Beyond cybersecurity, the governance of research infrastructures is itself a Knowledge Security consideration. Dependence on external platforms for storing, processing, or accessing research data may reduce institutional autonomy and increase exposure to foreign legal regimes or political influence. For this reason, the European Open Science Cloud Federation ([EOSC Node](#)) was established to provide sustainable, secure, and trusted access to research data within a European governance framework. EOSC supports interoperability with other European data spaces while complying with legislative frameworks such as the GDPR, the Data Governance Act, the Data Act, the AI Act, and the European Health Data Space. Through services including secure storage, virtual machines, collaborative workspaces, and controlled data access, EOSC aims to reduce strategic dependencies while supporting Open Science.

Switzerland is participating in this effort through the development of the [Swiss EOSC Node Prototype](#) (SENPro), funded by swissuniversities and coordinated by ETH Zurich. As part of the wider EOSC Federation, SENPro will provide federated research infrastructure and resource discovery services for the Swiss research community. This initiative aligns with the Swiss Foreign Policy Strategy, which promotes trustworthy data spaces, digital self-determination, and digital sovereignty.⁵⁷

By strengthening national and European research infrastructures, Switzerland seeks to preserve secure access to scientific knowledge while reducing dependence on external digital platforms and ensuring that research data remain protected throughout their lifecycle.

Scenario 14 – Example of vulnerabilities of the Open Science infrastructure

A European research centre strengthens the cybersecurity of the light source supporting its synchrotron facilities. To achieve this, the centre conducts a vulnerability analysis and develops corresponding risk mitigation measures. The analysis identifies several existing vulnerabilities:

- **Open connectivity model:** User groups are able to connect complete experimental setups directly to beamlines. Collaborating research groups may also build and operate beamlines, provided that they enable shared access for other users. While this model supports scientific collaboration and flexibility, it requires support for a Bring-Your-Own-Device (BYOD) approach, introducing externally managed systems into the institutional network and increasing potential attack surfaces.
- **Relatively flat network architecture:** The network structure relies on decentralised oversight, which facilitates flexibility but complicates the implementation of modern cybersecurity practices, including segmentation, access control, and monitoring.
- **Active Directory/Domain Controller (AD/DC) services:** These services manage user identities, system assets, and software lifecycles across general-purpose networks. While they simplify IT administration, they represent a critical security dependency: if compromised, attackers may gain extensive control over institutional systems.
- **Project-based implementation of scientific instruments:** Experimental instruments are often developed through project-based initiatives that prioritise rapid prototyping and customised workflows under tight timelines. As a result, security measures have traditionally focused on perimeter protection, such as firewalls and routers, while many

⁵⁷ *Foreign Policy Strategy: 38.*

network-connected devices within experimental areas remain accessible from internal subnets.

Scenario 15* – Example of cyberattack on Open Science infrastructure

A dataset used in an economics research project contains sensitive financial records with personally identifiable information. The dataset is stored on a university server specifically designed for handling highly confidential data. Access is restricted to a small group of researchers and students through a secure enclave incorporating multiple layers of security controls.

The research team intends to publish the study under an open access model once the data have been appropriately anonymised, or to exclude sensitive data from publication where anonymisation is not possible. However, parts of the restricted dataset are discovered on the dark web. Given the strong technical safeguards protecting the server, investigators suspect that the breach likely originates either from an internal source or from an “analog” vulnerability, such as unauthorised copying or extraction of data outside the secure environment.

Scenario 16* – Example of manipulation

A foreign political actor deliberately trains openly accessible AI models on falsified or manipulated open data. As a result, the models generate biased and unreliable outputs that appear credible but are based on distorted information. This contamination undermines reproducibility, erodes trust in digital knowledge systems, and poses significant risks to scientific integrity and the long-term advancement of knowledge in the targeted country.

Scenario 17 – Example of misuse of Open Science infrastructure

The research efforts of other countries in the Arctic present concerns for Canada’s national security [...] because physical geoscientific data collected in the course of research activities can be used to assert presence or dominance in northern geopolitically contested areas [...]. The expansion of unmanned sensing infrastructure and the establishment of satellite ground stations – ostensibly used for scientific purposes (e.g., to facilitate data transfer from sensing infrastructure) – is one example of sensitive research activities in the Arctic, as collected data can be used for military surveillance purposes.⁵⁸

4. Practical approaches to Knowledge Security and Open Science

The following Chapter presents institutional approaches for implementing Knowledge Security while supporting Open Science in higher education institutions at both the Swiss and European levels. The practices described are based on interviews with practitioners in Knowledge Security and Open Science from Swiss, European, and Canadian institutions, complemented by desk research.

Section 4.1 outlines common approaches adopted to reconcile Knowledge Security with Open Science. Section 4.2 provides an overview of selected national Knowledge Security frameworks –

⁵⁸ Whole text quoted from: Council of Canadian Academies (CCA). *Balancing Research Security and Open Science*. Ottawa, ON: Expert Panel on Sensitive Research of Concern, Council of Canadian Academies, 2025:24-25.

namely those of the Netherlands, Germany, and the United Kingdom – to illustrate different models of coordination between governments, research funders, and higher education institutions.

Sections 4.2 and 4.3 examine in greater detail how Knowledge Security and Open Science are implemented in a range of Swiss and European universities and universities of applied sciences.

The institutions covered are:

- Delft University of Technology (Netherlands)
- KU Leuven (Belgium)
- Turku University of Applied Sciences (Finland)
- ETH Zurich
- Lucerne University of Applied Sciences and Arts
- University of Applied Sciences and Arts Northwestern Switzerland
- University of Bern
- University of Fribourg
- University of Geneva
- University of Zurich

The report concludes with a discussion of the strengths and limitations of the approaches adopted by higher education institutions, identifies remaining challenges, and highlights opportunities for further development (see Chapter 6).

4.1. Good practices for higher education institutions

Higher education institutions in Switzerland and abroad have implemented a range of measures to identify, prevent, and manage Knowledge Security risks, including those arising in the context of Open Science – often not necessarily under a “Knowledge Security”-label. In fact, several of these measures such as access controls, publication licensing, and data management practices have long been integral components of Open Science. Their purpose is to ensure that research outputs remain both accessible and secure, recognising that openness may, in some cases, require carefully justified restrictions. Although these measures are not always embedded within a dedicated Knowledge Security strategy, they, nonetheless, make an important contribution to protecting research while preserving the benefits of openness. They can be grouped into the following categories.

- **Due diligence:** In the context of higher education, due diligence refers to the assessment of prospective research partners, funding sources, data-sharing arrangements, technology transfers, and other collaboration-related factors in order to identify potential legal, ethical, reputational, or security risks. Its objective is to ensure that research collaborations and related decisions are based on an informed assessment of opportunities and risks.
- **Export controls:** Export controls constitute a specific form of due diligence. They regulate the transfer of goods, software, and technologies with dual-use characteristics. Researchers, technical staff, and developers involved in sharing controlled items are responsible for verifying whether the relevant goods appear on applicable control lists and, where necessary, obtaining an export licence from the competent licencing authority before any transfer takes place. Swiss higher education institutions are legally required to implement Internal Compliance Programmes (ICPs) to ensure compliance with export control legislation. Violations may result in criminal liability for both the institution and the individuals involved.

- Access controls: Access to research data is managed through repositories but is also governed by legal and institutional requirements. For example, datasets containing personal or other sensitive information may be required to remain on servers located in Switzerland. The Swiss National Science Foundation, together with most Swiss higher education institutions, requires research data to be managed in repositories that comply with the FAIR principles. Within these frameworks, institutions may apply different levels of access depending on the sensitivity of the information.

Examples include:

- openly available datasets that have been anonymised or pseudonymised
 - access upon user registration
 - openly available datasets accompanied by warnings or usage restrictions
 - selective openness, where only metadata, parts of datasets, or specific access rights (e.g. read-only or execution access) are provided
 - embargo periods before publication
 - controlled access through secure reading rooms
 - access restricted to specific IP addresses or locations and
 - “closed but FAIR” datasets, where metadata remain publicly available to support discovery and citation while the underlying data are not openly accessible.
- Publication licences: The openness of publications, datasets, and software is regulated through licences that determine how research outputs may be shared and reused. Only the copyright holder, or another party authorised to act on their behalf, may apply licences such as [CC BY](#) or [CC0](#). While licencing decisions ultimately rest with the rights holder, institutions can provide guidance on selecting an appropriate licence and determining the appropriate level of openness in light of Knowledge Security considerations. These issues are ideally addressed at the outset of a research project and documented in a publication or dissemination plan.
 - Other data management practices: Sound data governance significantly reduces Knowledge Security risks while supporting Open Science.

Relevant measures include:

- established data stewardship structures and professional support from data stewards
 - publication and dissemination plans
 - data management plans addressing collaboration-specific risks, including data-sharing asymmetries
 - effective data classification, including metadata classification according to sensitivity
 - the use of sustainable and non-proprietary file formats where appropriate
 - reliable preservation strategies, including trusted repositories and regular backups and
 - secure procedures for handling, transferring, and storing large or sensitive datasets.
- Research integrity and ethics: Assessing the potential misuse of research requires both scientific and ethical evaluation. Researchers must balance the expected benefits of their work against potential risks to human dignity, life, health, freedom, property, the environment, and other fundamental values. Institutional mechanisms such as research ethics committees,

technology assessment procedures, and clear standards of scientific integrity support researchers in addressing these challenges. Several European organisations, including the German National Academy of Sciences Leopoldina, also recommend integrating ethics and Knowledge Security considerations into relevant university curricula.

- Awareness-raising and capacity building: Researchers are often best placed to recognise Knowledge Security risks within their own disciplines, although they may be less familiar with broader geopolitical developments or the legal and institutional obligations associated with Knowledge Security. Many European universities, therefore, support researchers through training, guidance, and advisory services that promote informed decision-making, self-assessment, and responsible research practices. Clear communication about the objectives and rationale of Knowledge Security measures, combined with the active involvement of researchers and other stakeholders, has also been shown to improve acceptance and facilitate implementation.

Although many of these measures are common across Swiss and international higher education institutions, their implementation varies considerably with respect to governance structures, scope, maturity, and strategic objectives.

4.2. Practical approaches: European higher education institutions

4.2.1. Delft University of Technology, Netherlands

Knowledge Security at Delft University of Technology is governed by an [institutional policy](#) aligned with Dutch and European legislation, as well as the [Dutch National Knowledge Security Guidelines](#). Recognising the importance of international collaboration and Open Science, the university's approach to Knowledge Security does not seek to eliminate risks entirely, but rather to identify, prevent, and mitigate them. Key risks identified by TU Delft include unwanted knowledge transfer, covert influence, and misuse of research outcomes.

Knowledge Security is implemented through a hybrid governance model that combines central coordination with decentralized responsibilities across faculties and organisational units. To support staff, TU Delft provides a comprehensive set of tools, guidance materials, and an internal platform that consolidates relevant resources.

These include:

- Guidelines for assessing whether international collaborations are both allowed and desirable.
- A related advisory process with both decentralised (1st line of support) and centralised (2nd line of support) elements
- Threat analyses outlining common forms of covert influence and unwanted knowledge transfer
- Access rights management mechanisms
- Training sessions and symposia aimed at awareness-raising and capacity building
- Guidance on secure use of digital devices during business travel
- Designated Knowledge Security contact persons within all faculties
- A pilot project exploring the ethical dimensions of Knowledge Security decisions (see *Knowledge Security as a Moral Challenge* by Governance & Integrity International)

TU Delft's risk assessment methodology considers both (1) the sensitivity of the research topic and technologies involved as well as (2) the affiliation risks of prospective collaboration partners or candidates. Risks are not determined by a single factor in isolation; rather, they arise from the interaction between research content and partner characteristics. At the same time, very high risks associated with only one of the parameters can outweigh low risks associated with the other. As such, partnerships with China's so-called "Seven Sons of National Defence" universities are treated as highly undesirable regardless of the research topic.

When establishing collaborations or recruiting new staff, TU Delft conducts systematic Knowledge Security risk assessments, typically at the final stages of selection processes. These assessments draw on information such as CVs and motivation letters, and take into account both the sensitivity of the research area and the professional affiliations of the individuals involved as based on their CVs.

Guiding questions include:

- Does the collaboration fall under EU sanctions regimes?
- Is the research subject to enhanced Knowledge Security oversight or embargo measures?
- Does the collaboration fall under export control regulations?
- Is the partner institution or individual affiliated with a military organisation outside the EU or NATO?
- Is the research considered sensitive from a Knowledge Security perspective?
- Is the individual involved through externally funded hospitality or sponsorship arrangements?
- Is there a credible risk of misuse of the knowledge or technology generated?

With regard to the relationship between Knowledge Security and Open Science, TU Delft has taken steps to ensure alignment between the two domains. A Knowledge Security representative participates in the steering board of the Open Science programme, and several Open Science-related policies explicitly incorporate Knowledge Security considerations. For example, the Research Software Policy includes provisions related to export control, while the Data Classification Policy and Guidelines define permissible uses of different data categories, taking into account Knowledge Security alongside other considerations such as privacy, intellectual property rights, and export control requirements. In addition, Data Management Plans are mandatory for obtaining ethical approval from the Human Research Ethics Committee.

Other challenges remain – particularly in relation to digital sovereignty. Ensuring sufficient institutional control and ownership over data in an Open Science environment continues to be a key concern for TU Delft.

4.2.2. KU Leuven, Belgium

KU Leuven is an autonomous Belgian university structured around three main academic domains: Science, Engineering and Technology; Biomedical Sciences; and Humanities and Social Sciences.

The university promotes Knowledge Security while maintaining a strong commitment to openness, internationalisation, and academic integrity. It actively addresses key risks such as the unintended transfer of sensitive knowledge, foreign interference, and the misuse of research outcomes. To raise awareness, KU Leuven provides introductory guidance on its website, including practical examples and questions designed to help researchers identify and assess Knowledge Security concerns.

Dedicated sections on unwanted knowledge transfer and foreign interference are publicly accessible:

- [Unwanted transfer of sensitive knowledge](#)

KU Leuven provides illustrative examples such as:

- Agreements with entities from countries with authoritarian regimes seeking particular knowledge
- Phishing campaigns or cyberattacks funded by a foreign government
- Bribery or coercion of employees to obtain sensitive information
- Requirements imposed on researchers to disclose all knowledge acquired at a foreign institution upon return

To support risk identification, researchers are encouraged to consider questions such as:

- Is the technology I am working on critical?
- Could it help advance a country whose values oppose those of KU Leuven, Belgium and/or European Union?
- Is this collaboration mutually beneficial for both parties?

- [Foreign interference and restriction of academic freedom](#)

KU Leuven also provides examples of foreign interference, including:

- Pressure from foreign partners to suppress or delay publication of research that may be politically sensitive
- Funding of university-affiliated cultural centres used to disseminate state-aligned propaganda
- Coordinated disinformation campaigns targeting research groups to undermine credibility
- Monitoring of nationals abroad to discourage dissenting academic or political views

Researchers are prompted to reflect on questions such as:

- Could the subject I am working on influence the public debate on a certain controversial topic?
- Are any students or researchers in my classes or research group experiencing restrictions to their academic freedom?
- Do PhD students need to report on their research to the embassy of their home country?
- Has the funder of my research proposal voiced concerns about the contents of my publication?

To mitigate risks of knowledge misuse, KU Leuven provides [guidance on sensitive technologies](#) and end-use considerations on its website. These guidelines align with the European Commission's *Recommendation on critical technology areas for the EU's economic security, supporting structured risk assessment by Member States*.⁵⁹ The university also offers information on [export control](#) and international [sanctions](#).

To address potential human rights violations, some of which intersect with Knowledge Security concerns, KU Leuven has adopted a [Human Rights Policy](#). A [Human Rights Assessment](#) is required for all agreements with external academic and non-academic partners in the areas of research, education, and societal engagement, including open science collaborations. A dedicated Human Rights Contact Point provides additional information and support.

When it comes specifically to Open Science, as declared by the institution in its [Open Science Vision](#),

⁵⁹ See p. 22.

KU Leuven applies the principle of the European Commission: As open as possible, as closed as necessary. We support open and early sharing of research findings, in order to foster innovation and bring research closer to society. However, to facilitate innovation, it will be necessary to strike a balance between benefits for the public interests and business potential, with respect for intellectual property rights.

The need to balance openness in science with the protection of economic interests, intellectual property, data protection requirements, and ethical standards is also reflected in the university's Research Data Management policy, even though it does not explicitly address Knowledge Security.

In practice, KU Leuven places particular emphasis on preventing the misuse of knowledge for military or malevolent purposes. Open publication itself is in most cases not considered to be the most important risk; instead greater concern may arise when published research attracts unsolicited collaboration or funding proposals, particularly from foreign institutions or researchers who initiate contact after identifying relevant outputs.

To prevent and mitigate such risks in the context of Open Science, KU Leuven provides targeted training on identifying potential misuse of research.

Where necessary, access control mechanisms are applied. For instance, restrictions may be requested for the publication of sensitive data, such as genomic datasets. Once published, access requests to such data are reviewed by researchers and data management teams, and applicants must specify their intended use. Risk assessments consider factors such as the requester's country of origin, available background information, and the nature of the data. A dedicated Data Access Committee, trained in geopolitics, risk assessment, and country-risk analysis, takes the final decision. Support services play a central role in this process, ensuring that researchers are not solely responsible for complex security assessments.

KU Leuven has also established two decision-making bodies with binding authority on Knowledge Security matters. Depending on the nature of the case, decisions are either taken by the Ethical Committee on Dual Use, Military Use and Misuse of Research (EC DMM) or by the Committee on Knowledge Security (CKS). For both Committees, there is an appeal procedure with the university Executive Board. The EC DMM assesses agreements between KU Leuven and foreign partners where dual-use, military use, or human rights concerns arise, including research collaborations, student exchanges, and societal service agreements.

All other Knowledge Security-related matters fall under the remit of the CKS, including staff recruitment, student admissions, and incoming and outgoing academic visits. The Single Point of Contact (SPOC) for Knowledge Security supports the CKS by preparing cases for decision, developing and implementing institutional policies, raising awareness across the university, and advising researchers and central support services.

Researchers can consult the EC DMM either for formal ethical assessment or for advisory support via a helpdesk function. A mandatory [self-assessment](#) is required to determine whether a case must be submitted to the EC DMM. This applies across all types of research and collaboration, including publicly funded projects, contract research funded by industry, and partnerships between academic institutions. A separate [self-assessment](#) procedure is also in place for staff recruitment.

4.2.3. Turku University of Applied Sciences, Finland

Openness and internationalisation are core values at Turku University of Applied Sciences, a relatively small institution where participation in international collaboration is considered essential for scientific advancement and innovation. Prior to the war in Ukraine and the subsequent deterioration of relations with Russia, the whole Finland was widely regarded as a leader in Open Science, characterised by extensive openness in research data and materials. In recent years, however, geopolitics has influenced the national approach to research security. While openness remains the default principle, restrictions are now applied where risk assessments indicate that protective measures are necessary.

At the Turku University of Applied Sciences, Knowledge Security is closely linked to the concept of responsible internationalisation, as defined by the Finnish Ministry of Education and Culture.⁶⁰ Within this framework, institutional policies address both the physical and digital protection of information and expertise across key activities, including recruitment, travel, and project evaluation. Security considerations are integrated into recruitment processes from an early stage, particularly in sensitive or high-risk fields. Formal procedures are also in place for visitors, including controlled access to research infrastructures and laboratories. Travel security is another key area, with researchers travelling to certain destinations required to use clean or “empty” laptops to reduce exposure risks.

Research projects are evaluated through a risk-based approach, with mitigation measures adapted to the level of identified risk. Each project begins with a kick-off meeting organised by the project management office within the research management structure. At this stage, Knowledge Security considerations are explicitly addressed, including their implications for Open Science. Researchers receive guidance on publication practices and conference participation, and they are required to complete a checklist to determine whether aspects of their research require restriction or can be shared openly. Because these considerations are integrated early in the project lifecycle, additional checks at the publication phase are generally not necessary.

To support the evaluation of international collaborations, the University has implemented a “know-your-partner” process. Information on partners is stored in an internal system that also feeds into project-level risk assessment, including a database designed to flag potential concerns.

The University has developed both policies and practical tools to help researchers identify sensitive or critical aspects of their work. Researchers are required to complete a checklist to assess whether their research falls under dual-use or export control regulations. A dedicated helpdesk service provides guidance and support, while a research security group brings together expertise from legal services, security management, partnership and project management, cybersecurity, human resources, and national research security networks.

Researchers are further supported through structured data management planning and tailored data management solutions. Tools such as the national DMP platform ([DMPTuuli](#)) are used alongside a shared glossary for sensitive data. A range of services is available to manage data at different sensitivity levels, including in international contexts such as EU-funded projects. The Finnish IT Center

⁶⁰ Finnish Ministry of Education and Culture. *Recommendations of the Working Group on Responsible International Cooperation in Higher Education and Research*. Helsinki: Ministry of Education and Culture, 2025. [MUISTIO_20250506081203.PDF](#)

for Science (CSC) plays a key role in this ecosystem by providing high-performance computing infrastructure and facilitating discussions on export control and dual-use issues.

With about one thousand staff members, the Turku University of Applied Sciences benefits from a relatively high level of institutional awareness regarding ongoing activities due to internal Knowledge Security trainings for top management and research group leaders. In addition, recent training on dual-use and export control has been delivered to research management professionals across Finnish universities.

Despite these robust processes, certain Knowledge Security challenges remain. One area of concern involves researchers presenting their work abroad, particularly when sensitive technologies are involved. For highly classified projects, such as those related to defence, access is strictly controlled through specialised facilities, and even senior leadership may have limited visibility. Additional challenges relate to the use of high-performance computing resources provided by CSC. As these systems are sourced from the United States, they are subject to licensing restrictions that may affect researchers from certain countries. This has raised questions regarding access for researchers from critical countries, the sharing of sensor data in international collaborations, and the use of artificial intelligence tools, particularly in relation to data processing and storage locations.

4.3. Practical approaches: Swiss higher education institutions

4.3.1. ETH Zurich

In Switzerland, ETH Zurich has played a pioneering role in implementing export control compliance and Knowledge Security measures while maintaining its commitment to academic freedom and international collaboration. For several years, the [Export Control Unit](#) has supported the ETH community in interpreting and applying Swiss export control legislation.

In 2024, [ETH Zurich introduced security screening measures](#) to manage risks associated with international collaborations in an evolving geopolitical environment. These screenings apply to applications for Master's and doctoral studies, employment, and guest stays involving individuals from countries subject to sanctions imposed by the United Nations Security Council, the European Union, or the United States, as well as countries identified by Switzerland as presenting proliferation risks. Where several [screening criteria](#) are met, ETH Zurich may recommend against proceeding with an application. However, no decision is made automatically: every case is assessed individually, and no single criterion is sufficient, on its own, to justify rejection.

In February 2026, the ETH Board approved revised regulations governing the ETH Zurich Ethics Committee. The revised mandate expands the Committee's remit beyond research involving humans and animals to include ethical issues arising from security-relevant research. In parallel, ETH Zurich is developing a proposal for a dedicated Knowledge Security Specialist Unit, which is expected to be presented to the university leadership during the second half of 2026.

Open Science is a core institutional value at ETH Zurich and is embedded across a broad range of activities, including Open Access, FAIR and open research data, citizen science, and open innovation. The university's commitment is further reflected in its endorsement of the Agreement on Reforming

Research Assessment and its membership in the Coalition for Advancing Research Assessment (CoARA), both of which recognise Open Science as a fundamental principle of research assessment.⁶¹

Within this broader commitment, knowledge security considerations are increasingly integrated into Open Science practices. The [ETH Guidelines for Research Data Management](#), published in 2022, explicitly recognise the need to balance openness with legal and security requirements:

u^b

The ideal to be strived for is Open Research Data (ORD) — the practice of making Research Data publicly available, accessible and reusable while always respecting legal and ethical framework conditions ('as open as possible, as closed as necessary'). [...] Applicable national and international law always takes precedence (e.g. personal data protection, export control of dual-use technology, archiving, copyright)".⁶²

In 2025, ETH Zurich launched the [ETH FAIR Coalition](#), an institutional initiative aimed at implementing the FAIR principles across all digital research assets, including data, software, code, metadata, laboratory notes, and images. Through an open charter, researchers and staff commit to making FAIR the default standard for digital research outputs, using infrastructures and policies that support FAIR practices, strengthening community engagement and data governance, and contributing to the institution-wide transition towards FAIR research.

Several complementary initiatives launched in 2026 further strengthen this approach. These include embedding FAIR principles within individual research units, expanding institutional expertise in research data management, and reinforcing links with the European Open Science Cloud (EOSC) Federation. ETH Zurich also plans a FAIR Summit to showcase successful projects and facilitate knowledge exchange through workshops and community events. At the national level, the university leads the development of the [the Swiss EOSC Node Prototype \(SENPro\)](#), which aims to provide a federated research infrastructure together with training and secure services supporting Open Science.

To facilitate the transition towards FAIR data practices, ETH Zurich is also piloting the **FAIR Competence Funding Grants**. These grants, of up to CHF 50,000 over a maximum period of 18 months, support the advanced training of research data management specialists and the expansion of institutional support services for FAIR data.

While ETH Zurich provides the institutional framework, guidance, and infrastructure necessary to fulfil its duty of care, responsibility for managing research data ultimately remains with researchers. They are responsible for determining which data can be openly shared, which should remain restricted, and which repositories are appropriate and trustworthy for the publication, preservation, and long-term stewardship of their research outputs.

4.3.2. Lucerne University of Applied Sciences and Arts

Based on its research profile, Knowledge Security is relevant to the Lucerne University of Applied Sciences and Arts (HSLU), particularly in departments with a focus on computer science, engineering, and technology. To address this, HSLU's Executive Board adopted a Knowledge Security Guideline co-developed by the Standing Committee on Research and Development and the Legal Services in autumn 2025. The guideline covers topics such as export control regulations and security screening

⁶¹ See [Research assessment | ETH Zurich](#)

⁶² ETH Zurich. *Guidelines for Research Data Management at ETH Zurich (RDM Guidelines)*. RSETHZ 414.2. Zurich: ETH Zurich, July 1, 2022

procedures for individuals. The guideline is complemented by an information sheet and corresponding procedures. While the guideline provides an overview of the topic and defines the overall framework for action, the information sheet includes questionnaires that enable the responsible units to conduct an initial assessment of specific categories of individuals. If this preliminary assessment indicates the need for enhanced security screening during a staff recruitment process, dedicated procedures and forms developed by Human Resources are applied to support the further review while the Directorate of each department is responsible for further review of potential students, cooperation partners and guests

Since 2024, HSLU has also had an [Open Science Policy](#) in place, covering in particular open access to scientific publications and research data management. This policy replaced the Open Access Policy adopted in 2016. While Knowledge Security is not explicitly addressed in the Open Science Policy, the document states that data should be made accessible according to the principle of “as open as possible, as closed as necessary.” The policy also clearly states that data protection requirements and ethical principles must be observed.

The Open Science team, which provides services to both the University of Lucerne and HSLU, is currently building expertise in the area of Knowledge Security. The aim is to integrate relevant aspects of Knowledge Security into research data management advice and training activities where appropriate.

In addition, the Head of Open Science and the Head of the Research Office maintain a regular exchange, which also provides an opportunity to discuss issues related to Knowledge Security. HSLU has initiated discussions with the University of Lucerne and the Lucerne University of Teachers' Education on this topic.

4.3.3. University of Applied Sciences and Arts Northwestern Switzerland

In 2025, FHNW conducted a comprehensive review of Knowledge Security and subsequently adopted Knowledge Security Directive in January 2026. The directive, which entered into force on March 1, 2026, establishes principles and procedures to strengthen protection against the misuse of knowledge generated and acquired at FHNW. The directive addresses the balance between Open Science, international collaboration, non-discrimination, and Knowledge Security. Rather than prescribing detailed rules for these potentially conflicting objectives, it requires a careful case-by-case assessment of the relevant legal and institutional interests.

Key measures include security screening procedures and regulations governing the export of tangible and intangible assets. Individuals from designated critical countries who seek employment in areas involving listed technologies or admission to a master's degree program are subject to a security screening and may only be employed or admitted following a positive assessment. Security screening is also mandatory whenever there is a concrete suspicion of a potential violation of the Goods Control Act. Furthermore, the directive sets out requirements relating to employee travel to critical countries and visits by guests from such countries.

Security screenings for master's students have been introduced as part of a pilot project for students commencing their studies in September 2026. Security screenings for employees will be implemented from January 1, 2027.

To support implementation of the directive, FHNW will launch an internal awareness campaign in 2027 to inform employees about Knowledge Security, associated risks, and their responsibilities.

The FHNW Secretary General serves as the Knowledge Security Officer and is responsible for overseeing the security screening process.



4.3.4. University of Bern

At the University of Bern, Knowledge Security is addressed through a combination of export control compliance, institutional advisory services, and research data management practices that support both security and Open Science.

The Export Control Contact Point advises researchers and the University Board on matters relating to Swiss, EU, and U.S. export controls, embargoes, and sanctions. It administers the University's [Internal Compliance Programme](#), assists researchers in classifying goods and technologies, and supports applications for export licences where required.

To strengthen institutional compliance, the University introduced export control, embargo, and sanctions screenings for staff in summer 2025 and for students in January 2026. In selected cases, these screenings also consider indicators of potential knowledge security risks that extend beyond strict legal compliance.

Knowledge Security advice is further provided through a dedicated Knowledge Security Contact Point within the Research Management Office of the Vice-Rectorate for Research. The Contact Point supports researchers and the University Board in assessing security risks related to international collaborations, the recruitment of foreign staff, visiting researchers and guests, foreign research funding, and participation in foreign talent programmes. Rather than imposing binding rules or predefined red lines, the university follows an advisory approach based on case-by-case risk assessment.

To further strengthen researchers' awareness, the university is developing a self-assessment tool for international research collaborations. The tool is intended to help researchers identify potential Knowledge Security risks at an early stage and support informed decision-making throughout the collaboration.

The University of Bern likewise integrates Knowledge Security considerations into its broader Open Science and research data management framework. Researchers receive support from faculty-specific data stewards through individual consultations, courses, and training covering the entire research data lifecycle, including ethical and legal aspects of data collection, storage, sharing, and preservation.

The University's Open Science policy follows the principle of "as open as possible, as closed as necessary", recognising that openness must be balanced against legal, ethical, and security requirements.

Accordingly, the university's [Guidelines on Research Data Management](#) state:

Research data and programming code both are relevant and requested to be shared along with the publication under a “Research Data and Code Availability Statement”. They should be published and deposited in a FAIR research data repository along with rich metadata information. If data cannot be openly published due to ethical or legal restrictions then a Data Transfer and Use Agreement is recommended to upload along with the metadata and supplementary documentation material about the dataset, which will allow other researchers to understand and reuse the data.

u^b

Researchers are expected to document systematically the structure, provenance, and processing of research data in digital form to ensure compliance with both the FAIR and CARE (Collective Benefit, Authority to Control, Responsibility, and Ethics) principles. Although Data Management Plans are not generally mandatory, applications to the university’s central Research Ethics Commission require a DMP that has been reviewed by a data steward.

To support good research data management practices, the Open Science team has developed a [Research Data Management Checklist](#), which researchers are encouraged to complete as early as possible, ideally before submitting a funding application. The checklist includes questions that help identify potential knowledge security risks and data protection issues at the planning stage of a project.

In 2026, the University further published its [Recommendations on Ethics in Research Data Management](#),⁶³ which explicitly address Knowledge Security considerations alongside research ethics. The recommendations discuss, among other topics, dual-use research and export control requirements, and introduce a framework for research data classification and risk assessment to assist researchers in selecting appropriate data management and protection measures. The recommendations also provide detailed guidance on publication licences.

Finally, the recommendations outline criteria for selecting trusted FAIR-compliant repositories and describe several good practices for responsible data sharing. These include maintaining public access wherever legal and ethical constraints permit; publishing personal or health-related data only after effective anonymisation and in the absence of contractual restrictions; recognising that anonymised datasets relating to rare conditions may nevertheless require restricted access; and publishing metadata together with supplementary documentation, such as ReadMe files, whenever full data sharing is not possible.⁶⁴ The recommendations also provide practical guidance on secure data processing, including anonymisation, pseudonymisation, and secure data storage.⁶⁵

4.3.5. University of Fribourg

At the University of Fribourg, a working group was established in 2025 to address issues at the intersection of export control and Knowledge Security. During this initial phase, a draft export control policy was developed, alongside a *cahier des charges* outlining the role of a compliance officer. Early awareness-raising efforts included the creation of an informational leaflet, the identification of research groups with potential dual-use risks through targeted risk analyses, and direct outreach to these groups.

⁶³ Churakova, O., et al. *Recommendations on Ethics in Research Data Management*. Bern, University of Bern, 2026.

⁶⁴ Ibidem: 6.

⁶⁵ Ibidem: 5.

In 2026, efforts have shifted toward consolidating and implementing these initiatives and an awareness training by Prophylax on espionage in academia took place. The export control policy is currently being revised, with several open questions still under consideration, and the recruitment of a compliance officer remains under discussion. Furthermore, an AI-based tool has been developed and is already in use to screen for war materials and dual-use items.

The University of Fribourg has also adopted an [Open Access Policy](#) which currently does not explicitly address Knowledge Security. However, its institutional [Research Data Management Policy](#) states that “les données de la recherche produites à l’Université de Fribourg sont aussi ouvertes que possible et protégées que nécessaire.” The policy also clearly defines researchers’ responsibilities, including the requirement to respect data protection – particularly for sensitive data – while complying with applicable legislation and codes of conduct. It further emphasizes the importance of considering copyright, as well as ethical and societal implications.

The university explicitly encourages researchers to address data security and integrity considerations at the stage of developing their Data Management Plans.

4.3.6. University of Geneva

At the University of Geneva, the interconnection between Open Science and Knowledge Security is more explicitly addressed in official policy documents than at other Swiss institutions of higher education.

The 2025-2028 [Roadmap to Open Science](#) identifies data security and digital sovereignty as one of the current challenges,⁶⁶ and formulates “the implementation of a coherent policy for the security and governance of sensitive data, aligned with scientific sovereignty and Knowledge Security” as one of five strategic priorities for the period of 2025 to 2028.⁶⁷

To achieve the goal of ensuring a consistent policy for the security and governance of sensitive data, the *Roadmap* suggests the following measures, categorised into three pillars:

- Implementation of an “Open & Safe” Program
 - Development of a FAIR + SAFE best practices guide based on the “[Five Safes](#)” framework (UK Data Service): safe data, trained to protect any confidentiality concerned; safe projects, which are approved by data owners for the public good; safe people: researchers can use data safely; safe setting: secure infrastructure prevents unauthorised use; safe outputs.
 - Targeted training on risks related to sensitive international partnerships, personal data, and misuse of research.
- Integration of Knowledge Security into Institutional Governance
 - Connection with the National Working Group and the Swiss Knowledge Security strategy (SHK).
 - Inclusion of security considerations in ethical reviews, Data Management Plans (DMPs), and research agreements (in collaboration with the Research and Grants Office, Legal Service, and the Commission for Ethical Research in Geneva (CUREG)).
- Capacity Building
 - Establishment of a “Data Security and Open Science” advisory service.⁶⁸

⁶⁶ University of Geneva. *Roadmap to Open Science 2025–2028*. Geneva: University of Geneva, 2025: 3-4.

⁶⁷ Ibidem, 6.

⁶⁸ Ibidem.

While the university's [Open Science Charter](#) postulates the principle of “as open as possible, as closed as necessary”, researchers are required to respect legal and ethical requirements for data handling. In particular, the [Institutional Policy on Research Data Management](#), which endorses “the principle of proper stewardship of such data throughout their lifecycle in accordance with prevailing standards,” is aligned with the [Institutional Data Management Policy](#), ensuring the security, quality, and availability of data.

u^b

In support, the university provides a [Research Data Portal](#), with a [dedicated information page](#) (in French) containing a research data classification matrix based on different levels of data sensitivity level (low, medium, high), illustrated through practical examples. Moreover, the [Data Portal](#) provides general information on Data Security and Data Protection.

In order to implement specific measures related to Research Data Management and Knowledge Security, an action plan has been established for 2026.

Within this framework, the following actions are currently underway:

- Deploy roles and responsibilities applicable to research data, as defined in the Institutional Data Management Policy, in order to ensure compliant research data management at all levels of the institution.
- Establish coordination for research data with the Data Office in order to ensure the security, protection, openness, and management of research data, and to develop appropriate strategies.
- Provide information (rights and obligations related to research data management, services) as part of the researchers' onboarding programme.
- Support entities in the implementation of an ORD process, by providing guidance and examples.
- Conduct an inventory of tools for the anonymisation, pseudonymisation, and encryption of personal and sensitive data.
- Propose an audio and video transcription tool, also tailored to the processing of personal and sensitive data (already [available](#) to researchers).

As part of its ethics and compliance strategy, the University of Geneva has developed a dedicated webpage on [research ethics](#) that provides guidance on risks associated with environmental impact, dual-use research, animal experimentation, research on and with human beings, potential human rights violations, personal data, and research integrity.

Researchers are required to complete an online [ethical risk declaration](#) before initiating any new research project. This declaration process is intended to systematically identify potential ethical risks prior to the conclusion of research-related agreements. Depending on the nature of the project, the review is completed by either the Research and Grants Office, the tech-transfer office (UNITEC), the legal affairs department, or the ethics commission (CUREG) – and ultimately, the vice-rector for research.

Efforts to strengthen research integrity and responsible research practices have recently been expanded at the University of Geneva through a series of awareness-raising initiatives targeting researchers across different faculties. In particular, faculty-level events such as “*LERU into Action*” organized within the Faculty of Science have contributed to improving understanding of Knowledge Security, export control regulations and their implications for academic activities. The university has

also recently hired an export control officer who helps researchers navigate administrative procedures and obtaining export licences, where necessary.

4.3.7. University of Zurich

The University of Zurich (UZH) has established an internal Policy on Responsible Internationalization, which builds on existing institutional principles, practices, and practical tools. The policy provides information and guidance to support UZH staff in addressing emerging questions and considerations related to international collaborations, ranging from research collaborations to travel safety and security or cybersecurity.

As part of this project, UZH has published an internal self-evaluation questionnaire and a [due diligence flowchart](#), with links to the relevant contact points and resources at UZH. This document guides researchers through the checks and steps they have to consider to ensure compliance with national, cantonal and university legal principles and guidelines, as well as the requirements of research funding institutions.

Researchers can seek guidance on sanctions, embargos and export controls from UZH's Export Control Officer, who was appointed in late 2024 and is part of the legal service. Governance structures have been established, and [information, guidelines and trainings](#) have been provided to support UZH staff in ensuring compliance with respective applicable laws.

The University of Zurich's [Open Science Policy](#) dates from 2021 and is entitled *Open by Default*. Open Science is presented as a core institutional value and is supported through both top-down and bottom-up initiatives. The university distinguishes between two complementary approaches: "Open by Design," through which it provides the infrastructure, support, and guidelines necessary to implement Open Science practices, and "Open by Desire" which seeks to encourage and support the engagement of individual researchers and research communities.

Within this framework, knowledge transfer is regarded as a key benefit of Open Science and is generally seen as something to promote rather than restrict. However, UZH

recommends openness in all research phases following the principle "as open as possible, as protected as necessary". This includes all research stages prior to publication (e.g. making data available, publishing data analysis plans, preprints). [...] How research data is being managed and shared depends on the kind of data and the culture within different disciplines and domains. Open data means making data available without restriction. Data and metadata should, therefore, be machine-readable and in non-proprietary file formats. Open Data is subject to data protection and must comply with legal requirements (e.g. sensitive data). UZH expects the entire research community to make research data (incl. source materials, records, datasets, etc.) as openly available as possible and as closed as necessary; concretely, this means:

- Data (at least the metadata) on which a publication is based should be openly accessible.
- Data should be shared as early as possible, at the time of first publication at the latest.
- Data should be FAIR and comply with good scientific and legal practice (anonymization etc).⁶⁹

In addition, the University of Zurich provides researchers [legal and ethical guidelines for research data management](#). These guidelines, which are intended to assist researchers in handling personal data,

⁶⁹ Hermans, Katherine, Höfler, Manuela, Robinson, Mark and Thommen, Marc. *Open by Default: Open Science at the University of Zurich*. Zurich: University of Zurich, 2021: 5.

are complemented by services and support for managing research data accordingly, including a [data protection and ethics self-assessment tool](#).

The University of Zurich complements its guidelines and support services with targeted awareness-raising and capacity-building activities, including presentations, for example to the UZH Open Science Working Group, short practice-oriented Lunch & Learn sessions for researchers, and dedicated workshops and exchange sessions within the Data Stewards Network.

4.3.8. Knowledge Security in Open Science in Switzerland

Swiss higher education institutions have already introduced a broad range of measures that contribute to Knowledge Security, Open Science, and the integration of Knowledge Security into Open Science, although these measures are implemented with varying degrees of maturity and coordination.

Most institutions have established robust Open Science frameworks, including policies based on the principle of “as open as possible, as closed as necessary”, FAIR research data management, trusted repositories, data stewardship services, Open Access publishing, data management planning, and guidance on licensing, anonymisation, and secure data sharing.

At the same time, many universities have strengthened Knowledge Security through export control compliance programmes, sanctions and security screenings, due diligence procedures for international collaborations, internal compliance structures, researcher self-assessment tools, ethics review mechanisms, and specialised advisory services on security-related research.

Increasingly, these two areas are being connected. Several institutions explicitly recognise legal and security considerations – such as export controls, data protection, dual-use research, and ethical constraints – within their Open Science policies and research data management guidelines. They also encourage researchers to integrate Knowledge Security considerations into data management planning, publication decisions, repository selection, and international collaborations.

Overall, Swiss higher education institutions have already laid many of the building blocks required for integrating Knowledge Security and Open Science. The remaining challenge is not the creation of entirely new mechanisms, but the development of a more coherent, institution-wide governance framework that systematically embeds Knowledge Security across existing Open Science policies and research practices. Awareness-raising is a first necessary step in that direction.

5. Open Science and Knowledge Security: Past and future trends

Since the mid-2010s, science, technology, and innovation (STI) have been increasingly treated as strategic components of a broader geopolitical competition.⁷⁰ Europe, China, and the US are all vying for control of key STI assets and capabilities to ensure long-term economic, military, and political power. These assets and capabilities span the entire value chain – from research and development (R&D) to manufacturing and deployment – and depend on globally interconnected innovation ecosystems and commercial markets.

⁷⁰ Jensen, Benjamin, Yasir Atalan, Can Mutlu, and Jose M. Macias III. "Competition in the Shadow of Technology." Center for Strategic and International Studies, December 2024.

To further their aims, states are pursuing a triple-track approach. First, they are steering their national innovation systems towards a strategic orientation that will lead to the development and retention of key STI assets and capabilities. Second, states are diversifying their supply chains as well as building capabilities in vulnerable spots along the value chain to reduce current and future dependencies. Third, states are setting guardrails to the circulation of knowledge to safeguard national interests over key STI assets and capabilities and ensure a risk-aware engagement with strategic competitors.

u^b

Three macro-historical developments explain this approach. First, human society is in the midst of a new industrial revolution, sometimes called industry 4.0, characterised by a rapid convergence of physical, digital, and biological systems.⁷¹ Since the 1990s and the rise of information and communication technologies (ICT), scientific and technological progress has advanced to a point where entire sectors could now be transformed by a suite of general-purpose critical technologies, such as artificial intelligence, robotics, biotechnology, and others. In the current era of strategic competition, the disruptive potential of these critical technologies conditions their development to that of a ‘tech race’ principally contested by private companies in consort with national governments.⁷²

Second, the way innovations occur has fundamentally changed since the 1980s and 1990s. Globalisation and market-driven capitalism have led to the rise of a handful of oligopolistic companies that concentrate capital and key technological capabilities in private hands as well as enabled them to flexibly operate across jurisdictions to their own and not necessarily to their ‘home country’s’ advantage.⁷³ This has reinforced a correlated trend, namely that the ability to perform R&D has shifted from the publicly funded academic sector to the privately funded corporate sector.⁷⁴ In the US, for example, the corporate sector’s share of the country’s total R&D expenditure has risen from 50 to 75 per cent since 1980.⁷⁵ As a result, national governments struggle to regulate and steer companies in ways that benefit national interests and the public good.

Third, globalisation and market liberalisation policies, which have enabled China’s rise as well as the US’ continued pre-eminence, no longer serve the interests of the two largest economic and political powers. In response to China’s rapid economic and technological development over the past two decades, the US has, since the mid-2010s, pursued a third offset strategy to limit or contain China’s development.⁷⁶ At the same time, China has intensified its statist and securitised approach under President Xi Jinping, gearing the academic and corporate sectors towards technological self-reliance.⁷⁷ In addition to Russia’s invasion of Ukraine and worsening transatlantic relations, these developments have impelled European states and the EU to view their own strengths and weaknesses through a strategic lens requiring a reappraisal of core political assumptions, particularly in the realm of security and economic policy.

⁷¹ Schwab, Klaus. *The Fourth Industrial Revolution*. World Economic Forum, 2016.

⁷² Girishankar, Navin (ed). "Staying Ahead in the Global Technology Race: A Roadmap for Economic Security." Center for Strategic and International Studies, October 2024.

⁷³ Petit, Nicolas. *Big Tech and the Digital Economy: The Moligopoly Scenario*. Oxford University Press, 2020.

⁷⁴ Borges, Chris. "Public and Private R&D Are Complements – Not Substitutes." Center for Strategic and International Studies, August 2025.

⁷⁵ National Science Foundation. "Discovery: R&D Activity and Research Publications." National Center for Science and Engineering Statistics, NSB-2025-7. Accessed June 15, 2026:

⁷⁶ Gentile, Gian, Michael Shurkin, Alexandra T. Evans, Michelle Grisé, Mark Hvizda, and Rebecca Jensen. "A History of the Third Offset, 2014–2018." RAND Corporation, 2021.

⁷⁷ Cheung, Tai Ming. *Innovate to Dominate: The Rise of the Chinese Techno-Security State*. Cornell University Press, 2022; Eigner, Leo. "China’s Vision for Science and Technology." CSS Analyses in Security Policy, no. 364. Center for Security Studies, July 2025.

Open Science and Knowledge Security are affected by as well as implement states' triple-track approach, since they both address the benefits and risks inherent in the circulation of knowledge. While Open Science seeks to make scientific knowledge widely accessible to promote inclusivity, equity, and collaboration within a hitherto globally interconnected and apolitical STI sector, Knowledge Security seeks to manage sensitive knowledge transfer through derisking practices within a globally interconnected yet increasingly politicised STI sector.⁷⁸

This chapter examines Open Science and Knowledge Security neither as opposites nor as complementary policy concepts but as part of the broader context of strategic competition. It first relates Open Science and Knowledge Security as well as dual-use and defence R&D policies to the function of knowledge circulation based on economic, normative, and security rationales. It then identifies the main international and national trends that explain and shape the adaptation of the STI sector(s) to the new political realities. By way of conclusion, the chapter examines what future trends are likely to affect the STI sector in Switzerland.

5.1. The circulation of knowledge

The circulation of knowledge is central to scientific and technological progress.⁷⁹ Throughout history, the exchange of ideas, information, and methods with a greater diversity of talent has a proven track record of improving and accelerating the innovation cycle.⁸⁰ STI policies therefore generally seek to encourage a frictionless circulation of knowledge wherever possible. This can be done by various means and depends on where the circulation is meant to occur. For instance, circulation can occur within as well as between disciplines, as it can within and between organizations, sectors, or national jurisdictions.

Academic mobility, international cooperation, and Open Science therefore became established STI policies in Europe and the US, the main centres of knowledge production until the 1990s, before spreading to create a globally interconnected system of exchange. In this international context, the more unimpeded the circulation of knowledge, the freer, more dynamic, and ultimately more innovative the STI sector is considered to be. By contrast, policies that impede knowledge circulation are seen as slowing down or even curtailing innovation because the freedom of STI actors to exchange ideas and information is restraint.

The circulation of knowledge has always been limited to a greater or lesser extent, either due to technical constraints or to political contexts. Following the mobilisation of science during the Second World War, a tacit agreement, known as the social contract of science, emerged in Europe and the US that established academic freedom and self-regulation as cornerstones of STI policy and as laws.⁸¹ While this protected academic actors from undue domestic political interference, it also empowered them to pursue their own policies and research agendas. This was done to shore up legitimacy for the post-war liberal democratic state as well as to promote the innovative capabilities of academic actors

⁷⁸ "UNESCO Recommendation on Open Science". UNESCO. Accessed June 23, 2026:

<https://www.unesco.org/en/open-science/about>

⁷⁹ Keim, Wiebke, Leandro Rodriguez Medina, and Rigas Arvanitis (eds). *Routledge Handbook of Academic Knowledge Circulation*. Routledge, 2023.

⁸⁰ Fara, Patricia. *Science: A Four Thousand Year History*. Oxford University Press, 2010.

⁸¹ Guston, David H. *Between Politics and Science: Assuring the Integrity and Productivity of Research*. Cambridge University Press, 2000.

in exchange for public returns on investment – be it in social welfare, cultural enrichment, economic growth, or security capabilities.

The extent to which knowledge can or should be circulated is therefore negotiable according to the tenets of the social contract for science. It is also shaped by three distinct yet interrelated rationales that academic, corporate, and policy actors as well as society at large often employ during such negotiations. First, the economic rationale encourages knowledge circulation to enhance the productivity and thus the overall economic value of the STI sector. In this conception, knowledge is ownable by the inventor and the investor, at least for a certain period, and equated with other productive forces, such as goods, services, capital, and labour.

Second, the normative rationale encourages knowledge circulation for its own intrinsic value as well as to promote equal access and opportunity. In this conception, knowledge is not ownable and thus considered a global public good in line with United Nations principles, such as the right to science, to education, and to development. The normative rationale also connects with the economic rationale, since greater and fairer access would make the global STI system more integrated, diverse, and dynamic.

Third, the security rationale seeks neither to encourage nor discourage knowledge circulation. Instead, it views circulation critically depending on what is being circulated with or through whom. In other words, the object, agent, and method of circulation are scrutinised on the basis of national security and strategic concerns and requirements. This applies to both domestic contexts (e.g., civil-military R&D cooperation) and international contexts (e.g., restricting exports to strategic competitors).

5.2. Circulation policies and their characteristics

Seen in this light, Open Science and Knowledge Security as well as dual-use and defence R&D policies all address the circulation of knowledge, albeit from different vantage points. While Open Science and Knowledge Security are system-wide policies that seek to address circulation issues holistically, policies in dual-use and defence R&D have a sector-based focus, as they seek to promote spillovers between the civil and military domains.⁸² All three policy concepts are differently influenced by the economic, normative, and security rationales underpinning the circulation of knowledge.

Open Science encourages knowledge circulation mainly through open access measures, which makes scientific research, data, and methods accessible in physical and online repositories.⁸³ It is underpinned by the economic rationale, typically if circulation is encouraged within national or like-minded jurisdictions, and by the normative rationale, if circulation is encouraged across all borders. This indiscriminate circulation of knowledge, which applies both to the content being circulated as well as to the jurisdictions it is being disseminated across, is currently being problematised by the spread of Knowledge Security, since it raises the question not only of what but also to whom sensitive knowledge is available through Open Science practices and systems.⁸⁴

⁸² Molas-Gallart, Jordi. "Which Way to Go? Defence Technology and the Diversity of 'Dual-Use' Technology Transfer." *Research Policy* 26, no. 3 (October 1997): 367–385.

⁸³ Moradi, Sh, and S. Abdi. "Open Science–Related Policies in Europe." *Science and Public Policy* 50, no. 3 (June 2023): 521–530.

⁸⁴ Pannier, Alice. "Software Power: The Economic and Geopolitical Implications of Open Source Software." Institut français des relations internationales, December 2022.

Knowledge Security neither encourages nor discourages but filters knowledge circulation through risk mitigation measures based on scientific values and national interest.⁸⁵ It is mainly underpinned by the security rationale, since Knowledge Security seeks to protect national STI assets and capabilities as well as the integrity of the STI sector more generally from unwanted knowledge transfer and political interference. But it is also influenced by the economic rationale, because Knowledge Security accepts that trade-offs must be weighed beyond mere security concerns, and by the normative rationale, because Knowledge Security seeks to uphold ethical standards in international law and research integrity in line with national interests, values, and laws.

Dual-use and defence R&D policies encourage a sectorial circulation of knowledge between civil and military innovation ecosystems typically (but not exclusively) within national jurisdictions.⁸⁶ Dual-use and defence R&D policies are mainly underpinned by the economic rationale, as they seek to maximise the returns of public investment in the STI and defence sectors alike by promoting spin-offs (i.e., applying military innovations to civilian contexts) and spin-ins (i.e., applying civil innovations to military contexts). The security rationale is also germane, and applies in two ways: first, when dual-use and defence R&D, as sectorial policies, go beyond national jurisdictions, as this raises security issues around what knowledge is circulated with whom, how, and why; second, when dual-use and defence R&D is conducted among national partners from different sectors, e.g., among academic, corporate, and defence actors, as this raises security issues around the institutional and operational forms of cooperation to prevent knowledge leakages.

5.3. International developments

National STI sectors have experienced numerous upheavals in recent years. In the US, the government has simultaneously intensified its support for as well as its interference in the STI sector.⁸⁷ In China, the STI sector has been aligned to the corporate and defence sectors with the Military-Civil Fusion and Made in China 2025 strategies as well as regulated more heavily with new laws.⁸⁸ In Europe, national governments are deepening civil-military R&D ties, while the EU is turning dual-use R&D into a structural feature of its various R&D funds and programmes. These developments, which are captured in diverse Open Science, Knowledge Security, and dual-use and defence R&D policies, can be traced back to broader geoeconomic and geopolitical developments.

Since the late 2010s, geoeconomic developments have raised global awareness of strategic vulnerabilities and dependencies. In the context of the US-China trade war, both countries successively imposed tariffs and other trade restrictions, particularly in strategic domains such as

⁸⁵ Eigner, Leo. "Knowledge Security at Stake." CSS Analyses in Security Policy, no. 338. Center for Security Studies, March 2024.

⁸⁶ Eigner, Leo. "Dual-use and Defence Research in Europe." CSS Policy Briefs, no. 2. Center for Security Studies, May 2026.

⁸⁷ Tollefson, Jeff, and Max Kozlov. "US Congress Set to Reject Trump's Sweeping Science Budget Cuts." *Nature*, January 20, 2026; Garisto, Dan. "Entire NSF science advisory board fired by Trump administration." *Nature*, April 28, 2026.

⁸⁸ McFaul, Cole, Sam Bresnick, and Daniel Chou. "Pulling Back the Curtain on China's Military-Civil Fusion: How the PLA Mobilizes Civilian AI for Strategic Advantage." Center for Security and Emerging Technology, September 2025; Wübbeke, Jost, Mirjam Meissner, Max J. Zenglein, Jaqueline Ives, and Björn Conrad. "Made in China 2025: The Making of a High-Tech Superpower and Consequences for Industrial Countries." MERICS, December 2016.

semiconductors and rare earth elements, to hamper each other's development.⁸⁹ The economic disruption that resulted raised widespread concerns over supply chain dependencies and raised the spectre of economic coercion.⁹⁰ Other developments, notably the covid-19 pandemic, highlighted additional vulnerabilities and underscored the urgency that ultimately impelled states to minimise current and future disruptions through derisking strategies. These span STI, economic, and industrial policy and encompass investment screenings, export controls, and the reshoring or 'friend-shoring' of critical assets and capabilities along the entire value chain.

As a result, states also began to prioritise their national STI sectors. While still globally interconnected, the aim is to intentionally promote and retain key STI assets and capabilities to assure the ongoing capacity of a country to conduct breakthrough innovation that enables it to compete in global markets and global power struggles. Public investments in basic and applied research, aggressive talent acquisition programmes, or the deregulation of certain innovative sectors – examples of which can be found in Europe, China, the US, as well as further afield – are all policies that seek to strengthen what in China at least is called "indigenous innovation".⁹¹ Owing to the integrated nature of national STI sectors, this 'indigenous' quality is never exclusively nation-based, but remains fluid and hard to police, even for authoritarian states like China. Yet the awareness and willingness among policymakers to promote their national STI sectors for geoeconomic reasons has risen among developed, scientifically leading countries.

Since the early 2020s, geopolitical developments have intensified these trends in derisking and 'indigenous innovation,' particularly in Europe. Following Russia's invasion of Ukraine, which marked the return of large-scale conventional warfare involving major powers, European states recognised the vulnerabilities to and in their individual and collective security architectures. In response, European states raised defence budgets and deepened cross-border partnerships with the aim of restocking, expanding, and upgrading military capabilities after decades of underinvestment, addressing the fragmentation of Europe's defence technological and industrial base, and catching up on emerging STI capabilities through the promotion of defence innovation.⁹² The urgency of Europe's defence policy turn has drastically increased due to American revisionism and unwillingness to continue to underwrite European security.⁹³

As a result, the emphasis of European derisking strategies has shifted, altering Europe's approach to STI policy as well. Europe's dependence on US civil and military technology, from which it procures up to two-thirds of its defence equipment, and on China for green transition technologies and rare earth

⁸⁹ Grgić, Gorana, Michiel Foulon, and Névine Schepers. "Europe's Semiconductor Strengths and Strains." CSS Analyses in Security Policy, no. 360. Center for Security Studies, May 2025; Schepers, Névine. "China's Strategic Use of Trade Controls." CSS Policy Briefs, no. 1. Center for Security Studies, April 2026.

⁹⁰ OECD. *Economic Security in a Changing World. New Approaches to Economic Challenges*. OECD Publishing, 2025; Hackenbroich, Jonathan, Filip Medunic, and Pawel Zerka. "Tough Trade: The Hidden Costs of Economic Coercion." European Council on Foreign Relations, February 2022.

⁹¹ Cao, Cong, Richard P. Suttmeier, and Denis Fred Simon. "China's 15-Year Science and Technology Plan." *Physics Today* 59, no. 12 (December 2006): 38–43.

⁹² The Economist. "Europe Is Going on a Huge Military Spending Spree." December 1, 2025; Grgić, Gorana. "The Changing Nature of the EU's and NATO's Partnerships." CSS Analyses in Security Policy, no. 348. Center for Security Studies, October 2024; Clapp, Sebastian, and Martin Höflmayr, with Falk Vambrie. "Building a Common Market for European Defence." EPRS Briefing, PE 775.924, September 2025.

⁹³ Möckli, Daniel. "Rudderless World: American Neo-revisionism and the Demise of Global Order." In *Strategic Trends 2025*, edited by Gorana Grgić and Daniel Möckli, 11–31. Center for Security Studies, 2025; Everts, Steven, Giuseppe Spatafora, and Alice Ekman (eds). "Low Trust: Navigating Transatlantic Relations under Trump 2.0". Chaillot Paper, no. 187. European Union Institute for Security Studies, October 2025.

elements can be partly traced back to Europe's relative underperformance in STI.⁹⁴ This is due to a variety of factors, such as lower R&D spending, a focus on mature rather than frontier technologies, and fragmented capital and commercial markets that limit economies of scale. European states are therefore attempting to enhance their digital and technological sovereignty vis-à-vis the US and China through the wholesale promotion of a European value chain in critical technologies.⁹⁵ This spans STI, economic, industrial, and defence policy and encompasses R&D investment, particularly in dual-use and defence R&D, infrastructure projects, and supply chain diversification.

These geoeconomic and geopolitical developments have compounded over the past decade, and impelled states to reassess the globalised, diversified nature of resources, competences, and supply chains as well as to revise systemic, asymmetric dependencies wherever possible. Given the interdependent nature of global innovation systems and commercial markets, total self-reliance is neither possible nor desirable. Instead, states are seeking to expand their strategic agency, on the one hand, by minimising vulnerabilities and dependencies, and on the other, by identifying and maximising key chokepoints in global markets that they control and can therefore use as leverage in interstate negotiations. International relations are thus increasingly characterised by an intensified form of politicised and at times coercive interdependence where states constantly exert pressure on one another to tip the balance of power in their favour.⁹⁶

5.4 International approaches

Despite the intensely politicized and interdependent nature of strategic competition, Europe, China, and the US continue to promote the circulation of knowledge domestically and internationally. Even China, which officially pursues a policy of "technological self-reliance," is still seeking to balance "openness and self-reliance".⁹⁷ But Europe, China, and the US also regulate and restrict knowledge circulation. In this sense, the principle, popularized by the European Commission in 2019 and adopted by UNESCO in 2021, that STI sectors should be "as open as possible, as closed as necessary" defines a global approach.⁹⁸ How states interpret this principle of balanced openness naturally differs, and depends on their political systems, laws, and political aims.

In China's authoritarian system, a series of laws passed in 2021, like the Data Security Law and Personal Information Protection Law, as well as a statist, securitized conception of STI assets and

⁹⁴ Clapp, Sebastian. "European Defence Industrial Strategy." EPRS Briefing, PE 762.402, September 2024; Schepers, Névine. "China's Strategic Use of Trade Controls." CSS Policy Briefs, no. 1. Center for Security Studies, April 2026; Draghi, Mario. "The Future of European Competitiveness." European Commission, September 2024.

⁹⁵ Burwell, Frances, and Kenneth Propp. "Digital Sovereignty: Europe's Declaration of Independence?" Atlantic Council, January 2026; García Bercero, Ignacio, Antoine Mathieu Collin, Ben McWilliams, Niclas Poitiers, and Simone Tagliapietra. "'Made with Europe' Not 'Made in Europe' Should Guide EU Industrial Policy." Bruegel, February 2026.

⁹⁶ Drezner, Daniel W., Henry Farrell, and Abraham L. Newman (eds). *The Uses and Abuses of Weaponized Interdependence*. Brookings Institution Press, 2021.

⁹⁷ You, Xiaoying. "China Seeks Self-Reliance in Science in Next Five-Year Plan." *Nature* 647 (October 24, 2025): 11–12; Xi Jinping. "Speech at the Work Conference for Cybersecurity and Informatization." Translated by Rogier Creemers. China Copyright and Media, April 19, 2016. Accessed June 10, 2026: <https://chinacopyrightandmedia.wordpress.com/2016/04/19/speech-at-the-work-conference-for-cybersecurity-and-informatization/>.

⁹⁸ Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on "Open Data and the Re-use of Public Sector Information". Official Journal of the European Union L 172 (June 26, 2019): 56–83; "UNESCO Recommendation on Open Science." UNESCO, 2021.

capabilities filter and sometimes limit the international circulation of knowledge. The government's conception of "comprehensive national security" leads to a perception of knowledge, especially in strategic domains, as state property when it affects national security.⁹⁹ Since this can be interpreted broadly, this provides the government with considerable leeway to screen and intervene in knowledge circulation. The government thus regulates the circulation of knowledge on the basis of an overcautious precautionary approach that civilian actors must comply with.

u^b

In Europe's and the US' liberal democratic systems, laws around academic freedom and self-regulation, property rights, and transparency rights as well as a liberal, civilian-driven conception of innovation shape the circulation of knowledge. Security related laws, like export controls, secrecy, and extraterritorial laws, like the US CLOUD Act (2018), also affect knowledge circulation but are applied conservatively.¹⁰⁰ The regulation of knowledge circulation thus assembles civilian actors and the government in a process of mutual consultation in which risks and benefits are weighed against competing interests. However, the current Trump administration's persistent attempts to undermine academic freedom and self-regulation signal a programmatic intention to intervene in established STI policies.¹⁰¹

However, there are also similarities between the US and China as there are differences between the US and Europe. With respect to the domestic, sectorial circulation of knowledge, the US and China have traditionally kept their civil and military innovation ecosystems strongly interlinked and invested heavily in dual-use and defence R&D. In Europe, especially after the collapse of the Soviet Union, similar interlinkages have become much less pronounced. European states and the EU are now seeking to reverse this partial separation of the civil and military domains through various national and EU dual-use and defence R&D policies.

There are additional differences when it comes to Open Science and Knowledge Security. Unlike in the US, Open Science received not just institutional but also political backing in Europe. In 2016, the EU announced its "open innovation, Open Science, open to the world" policy and made Open Science a legal obligation for recipients of EU funds in 2021.¹⁰² As an important funder of R&D, the EU's regulations thus helped to promote the widespread adoption of institutional Open Science policies that was situationally reinforced by national policies encouraging Open Science practices. In the US, Open Science received government backing under the Biden administration and has become mandatory, if funded by federal R&D agencies, since 2025 / 2026.¹⁰³ However, the current Trump administration may reverse this.

⁹⁹ Matthews, David. "Foreign Researchers in China Face Tightening Restrictions." *Nature*, March 6, 2025; Li, Xiaojie, Yali Cong, and Zheng Yi. "Research under China's Personal Information Law." *Science* 378, no. 6622 (November 25, 2022): 713–715; Drinhausen, Katja, and Helena Legarda. "Confident Paranoia: Xi's 'Comprehensive National Security' Framework Shapes China's Behavior at Home and Abroad." *China Monitor*, no. 75. MERICS, September 2022.

¹⁰⁰ Bundesamt für Justiz. «Bericht zum US CLOUD Act: Gutachten des Bundesamts für Justiz». Schweizerische Eidgenossenschaft, September 17, 2021. Accessed June 15, 2026: <https://www.bj.admin.ch/bj/de/home/publiservice/publikationen/berichte-gutachten/2021-09-17.html>.

¹⁰¹ Garisto, Dan, and Mariana Lenharo. "White House Proposes Vast Overhaul of US Science Funding: What You Need to Know." *Nature*, June 3, 2026.

¹⁰² European Commission, Directorate-General for Research and Innovation. "Open Innovation, Open Science, Open to the World: A Vision for Europe". Publications Office of the European Union, 2016; European Research Executive Agency. "Open Science." European Commission. Accessed June 10, 2026: https://rea.ec.europa.eu/open-science_en.

¹⁰³ Lenharo, Mariana. "NIH-Funded Science Must Now Be Free to Read Instantly: What You Should Know." *Nature*, June 26, 2025; Nelson, Alondra. "Ensuring Free, Immediate, and Equitable Access to Federally Funded

In Knowledge Security, the US has adopted a more top-down approach compared to European states. The National Security Presidential Memorandum-33 (2021) and the CHIPS and Science Act (2022) made the reception of federal funding contingent on the institutional implementation of cybersecurity, foreign travel, awareness-raising, and other Knowledge Security measures.¹⁰⁴ European states have not yet tied R&D funding to Knowledge Security requirements. Instead, they have mostly reinforced the compliance to national and international export controls at academic institutions as well as emphasized their responsibility, as autonomous institutions that rely on public funding, to implement Knowledge Security measures for their own sake as much as for national interests. It is likely, however, that the European Commission, which plans to revise the European Research Area Act by the end of 2026, will include Knowledge Security in its regulations, thereby making compliance legally binding for European universities and research performing institutions.

Overall, Europe and the US agree on the principle of tighter knowledge circulation. Key principles, such as balanced openness, promoting risk-aware cooperation, and adopting a proportional, targeted, and precautionary approach, are shared on both sides of the Atlantic. In the context of greater domestic political interference in the US STI sector, however, European states have, by comparison, generally adopted a more liberal, collaborative approach to their respective STI sectors and shown greater respect for academic freedom and self-regulation. However, the geoeconomic and geopolitical pressures have also compelled European states to demand more from their STI sectors by incentivizing academic actors to address and manage the pressures that governments are facing.

5.5 National developments and approaches

Compared to the rest of Europe and the US, Switzerland has a more liberal approach to STI policy. This is due to the country's liberal conception of the constitutional state and to its federalist, decentralised political system that empowers subsidiary actors.¹⁰⁵ Policy decisions of a historically formative nature are also relevant. Following the Second World War, Switzerland combined a maximalist foreign economic policy with a minimalist foreign policy approach to promote economic growth and escape the political isolation that characterised the war and postwar years. This approach, which has since become a hallmark of Switzerland's international posture, discourages political positioning while encouraging engagement and cooperation on the international stage and is widely considered central to Switzerland's economic and political model.

These foundations thus predispose the country, and the STI and corporate sectors in particular, towards openness. The government does not steer these sectors with technology or industrial strategies but seeks to co-design ideal framework conditions with the relevant academic and

Research." Memorandum for the Heads of Executive Departments and Agencies. Office of Science and Technology Policy, Executive Office of the President, August 25, 2022. Accessed June 10, 2026: <https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/08/08-2022-OSTP-Public-Access-Memo.pdf>.

¹⁰⁴ Trump, Donald J. "Presidential Memorandum on United States Government-Supported Research and Development National Security Policy." The White House, January 14, 2021. Accessed June 10, 2026: <https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/>; United States Congress. "CHIPS and Science Act." Pub. L. No. 117-167, H.R. 4346, 117th Cong. Signed into law August 9, 2022.

¹⁰⁵ Papadopoulos, Yannis, Pascal Sciarini, Adrian Vatter, Silja Häusermann, Patrick Emmenegger, und Flavia Fossati (eds). *Handbuch der Schweizer Politik = Manuel de la politique suisse*, 7. Auflage. NZZ Libro, 2023.

corporate actors so as to enable them to flourish.¹⁰⁶ In the case of the STI sector, this liberal, consensual approach to policymaking is conditioned by laws on academic freedom and institutional autonomy, which limits governmental authority by empowering academic actors to pursue their own institutional policies to fulfil their mandate. Being thus system-relevant and autonomous, academic actors must routinely cooperate with one another as well as with policy actors to define nationally coherent STI policy approaches wherever necessary.

u^b

The subsidiarity principle additionally influences how academic and policy actors interact.¹⁰⁷ This states that political issues are addressed directly at their source by the actors concerned who may, if the issues surpass the scope of their mandate and competences, call on cantonal and/or federal government for support. Given the numerous, diverse, and autonomous actors that characterise the Swiss STI sector, this means that a degree of alignment within the sector must be achieved before the subsidiarity principle can be invoked for the sector as a whole. By responding to the call for support, the government thus recognises that there is a shared responsibility for the issue which needs to be addressed collectively.

These characteristics of the Swiss political system and STI sector are key to understanding Switzerland's approach to knowledge circulation policies. Since the emergence of the geoeconomic and geopolitical developments in the late 2010s, academic as well as corporate actors have invoked the subsidiarity principle and called on the government for support in addressing knowledge and economic security respectively. In the case of the STI sector, the government engaged with the issue at the behest of the actors concerned and because of additional pressure from parliament (see Section 1.3), thereby acknowledging that Knowledge Security was a national and not just an institutional challenge that required a coordinated response. A similar development did not occur with respect to Open Science.

A two-tier approach to Knowledge Security – one institutional, one national – thus emerged in Switzerland. Being exposed to Knowledge Security risks as well as being responsible for their management, it was academic actors who initially addressed the issue at the institutional level, initiated discussions within the STI sector, and subsequently incited policy actors to take coordinated action. In late 2024, the government created an interdepartmental working group (*Interdepartementale Arbeitsgruppe*, IDAG) on Knowledge Security that assembled policy actors, and which worked alongside the national working group (NWG) on Knowledge Security that assembled academic actors (see Section 1.3). Both reports, published in late 2025, shared a common threat perception and conception of Knowledge Security, namely that openness and security must be balanced and any restrictions must be proportional, targeted, and precautionary in nature.

The two reports also broadly aligned on policy recommendations, which can be divided along three tracks (see Section 1.3). First, academic actors remain the chief 'owners' of Knowledge Security and must, therefore, ensure their own risk management, compliance, and awareness-raising measures as well as coordinate with other academic actors to align institutional policies. For academic actors to achieve this, however, two sets of policies at national level must be implemented. The second track relates to legal modifications of cantonal and federal laws and regulations that would facilitate the

¹⁰⁶ Staatssekretariat für Bildung, Forschung und Innovation. «Internationale Strategie der Schweiz im Bereich Bildung, Forschung und Innovation». Schweizerische Eidgenossenschaft, July 2018. Accessed June 10, 2026: https://www.sbfi.admin.ch/dam/de/sd-web/stJ1sWncEgw9/internationale_strategie_bfi_d.pdf.

¹⁰⁷ Bieri, Matthias, and Wenger, Andreas. "Subsidiarität und die Schweizer Sicherheitspolitik". CSS Analysen zur Sicherheitspolitik, Nr. 227. Center for Security Studies, May 2018.

implementation of institutional measures. The third track relates directly to national coordination. Since Knowledge Security risks evolve, and actors need to share and access classified information to make decisions, a National Contact Point for Knowledge Security is expected to be created to facilitate this exchange as well as support national policy coherence more generally.

By contrast, Open Science and its relation to Knowledge Security remains within the purview of institutional autonomy, since the subsidiarity principle was not invoked in this case. Like in the US and Europe, it was academic actors who implemented institutional policies for their own aims and interests, in part to comply with EU and domestic research funding requirements – the Swiss National Science Foundation (SNSF) and the Framework Programme having made open access publication mandatory in 2018 and 2021 respectively.¹⁰⁸ While the SNSF is an autonomous actor who co-designs policies with Swiss academic actors, the Framework Programme regulations are shaped by EU policymakers. Meanwhile, the Swiss government did not have a national Open Science policy, since this was an institutional and STI sector responsibility, although it did financially support Open Science policies at institutional level. The question of if and how Open Science policies and practices must adapt to accommodate Knowledge Security measures is one that academic actors must therefore self-determine as well as co-determine with other actors at national and international level with ad hoc support from policy actors.

Dual-use and defence R&D policy also remains an institutional policy decision. In this case, it is not academic actors who can invoke the subsidiarity principle but the government, as the ‘owner’ of security issues, that approached academic and corporate actors for support. In its 2025 armaments strategy, Armasuisse announced its intention to double its annual R&D budget and to enhance synergies in dual-use and defence R&D with civil actors, notably the ETH Domain.¹⁰⁹ In October 2025, Armasuisse and the ETH Domain initiated the Research Program Security with 2 million CHF and have since launched eight research projects in critical technologies.¹¹⁰ In April 2026, Armasuisse and Innosuisse launched joint funding calls in dual-use R&D.¹¹¹ The question of whether or not and indeed how to engage in dual-use and defence R&D remains an institutional decision.

Switzerland’s approach to knowledge circulation policies thus broadly aligns with the rest of Europe. Owing to the country’s political system, however, the measures that are and will be put in place emphasize limited state intervention in line with liberal policymaking, academic freedom, and institutional autonomy with the aim of preserving the STI sector’s and Switzerland’s overall openness as much as possible.

¹⁰⁸ "Open Access Publications." Swiss National Science Foundation. Accessed June 10, 2026: <https://www.snf.ch/en/VyUvGzptStOEPUoC/topic/open-access-publications>; EURAXESS. "The EU’s Open Science Policy." European Commission. Accessed June 10, 2026: <https://euraxess.ec.europa.eu/worldwide/asean/eus-open-science-policy>.

¹⁰⁹ armasuisse, Bundesamt für Rüstung. «Rüstungspolitische Strategie des Bundesrates.» Schweizerische Eidgenossenschaft, June 20, 2025. Accessed June 10, 2026: <https://www.ar.admin.ch/de/ruestungspolitikbundesrates>.

¹¹⁰ armasuisse, Bundesamt für Rüstung. «Research Program Security: Das VBS und der ETH-Bereich stärken Forschung im Bereich Sicherheit und Verteidigung.» Schweizerische Eidgenossenschaft, May 22, 2026. Accessed June 10, 2026: <https://www.ar.admin.ch/de/newsb/YOj8z3xJzfT5>.

¹¹¹ «Innosuisse und armasuisse lancieren eine Projektausschreibung im Bereich Dual-Use-Technologien». Innosuisse, April 30, 2026. Accessed June 10, 2026: <https://www.innosuisse.admin.ch/de/newsb/xMNk0LL66iDuYIrinwy7m>.

5.6. Future trends

u^b

Geoeconomic and geopolitical developments will continue to affect the Swiss and global STI sectors for the foreseeable future. How long this will last is unclear, because the existing world order based on multilateralism, liberalism, and market-based capitalism is in transition. What is clear, however, is that this transition period is characterised by a multi-domain strategic competition exercised in grey zones through the tactical exploitation of diverse forms of interdependence. Dominance in general-purpose, critical technologies will remain a key feature, meaning that the entire value chain from basic research to deployment and diffusion will continue to be contested and thus highly politicised. It is likely that this strategic competition continues to periodically abate and intensify, hopefully by avoiding major crises, before settling into a new world order that is, at present, impossible to foresee. Due to this protracted period of volatility and uncertainty, academic and policy actors in Switzerland would do well to take the long view when taking action today. Seen in the light of strategic competition, Open Science, Knowledge Security, and dual-use and defence R&D policies are not random aberrations but structural features of the STI sector impacted by strategic rivals competing with one another and will therefore persist in some shape or form. The prevailing principle of balancing openness with security ensures that established STI principles, such as academic freedom and self-regulation, and established STI policies, such as international cooperation and academic mobility, remain intact. Their practice, however, will change due to derisking measures designed to offset current and future geoeconomic and geopolitical challenges as far as possible.

Concretely, the strategic encouragement or discouragement of knowledge circulation in Europe, China, and the US, which is part of broader derisking efforts, will likely lead to regional and ideological convergences and divergences within the global STI sector. In other words, cooperation and exchange is likely to increase among strategic partners, whether geographically near or far, and decrease between strategic competitors, as it has in recent years between China and the US.¹¹² That said, cooperation and exchange among leading academic actors is likely to continue, albeit with a heightened risk and strategic awareness of the knowledge circulation taking place.

Europe may benefit the most from this trend. It is not only in a position to benefit from bilateral cooperation with China and the US respectively, but can also benefit from intensified intra-European cooperation, especially through dual-use and defence R&D policies, as well as through cooperation with global strategic partners. For instance, the EU has intensified its science diplomacy efforts in recent years and expanded third-country association to the Framework Programme to New Zealand (2023), Canada (2024), South Korea (2025), Japan (2026), and Australia (2027) amongst others.¹¹³ This suggests a more strategic awareness of Europe's STI assets and one it may develop and wield more expansively.

In a high-performing, globally integrated, and self-regulating STI sector like that of Switzerland, academic actors, whether institutions or individuals, will not only be exposed to geoeconomic and geopolitical challenges but also be expected to manage them in line with their academic freedom and institutional autonomy. Capacity-building and awareness-raising are therefore essential to empower institutions as well as the individuals in their care. Given the STI sector's numerous, diverse, autonomous academic actors, it is likely that, apart from setting best practices in Switzerland's

¹¹² Stoye, Emma. "China-US Research Collaborations Are in Decline – This Is Bad News for Everyone." *Nature*, July 19, 2024.

¹¹³ European Commission, Directorate-General for Research and Innovation. "A European Framework for Science Diplomacy." News article. European Commission, February 13, 2025.

approach to Knowledge Security, there will be a plethora of institutional policies in Open Science and Knowledge Security as well as dual-use and defence R&D.

Owing to the magnitude of the challenges in addition to the autonomy of academic actors in Switzerland, relations between academic and policy actors are likely to grow closer during this transition period. As threat landscapes, national interests, and scientific and technological developments rapidly evolve, academic and policy actors will need to engage in mutual consultation to understand each other's shifting priorities and come to tacit, often case by case agreements on how to manage certain challenges. In this sense, the National Contact Point for Knowledge Security might fulfil an important role beyond Knowledge Security issues.

Overall, the Swiss political system and the STI sector is agile enough to manage the uncertainty and volatility of strategic competition. This ability, however, depends on the strength of Switzerland's social contract for science. This is not defined by academic or policy actors alone but is shaped through broad societal debate and ultimately determined through political processes. Given the high degree of autonomy, responsibility, and that academic actors enjoy to fulfil their mandate, it is in their interest to actively address societal expectations and engage with policy actors. In this way, they may continue to act as global institutions, supporting the global enterprise of scientific and technological development throughout the world, while aligning their efforts in ways that serve national interests and the public good.

6. Conclusions and recommendations

The previous Chapters of this report have defined the concepts of Knowledge Security and Open Science, outlined the European and Swiss regulatory frameworks governing both fields, identified the Knowledge Security risks associated with Open Science, analysed the factors that give rise to or increase these risks, and presented good practices and risk mitigation measures adopted by higher education institutions across Switzerland and Europe. Building on these findings, several key conclusions can be drawn.

First, Open Science and Knowledge Security are not only compatible but can also reinforce one another when implemented effectively. While tensions may arise between the unrestricted dissemination of knowledge and the need to limit access for security reasons, these tensions do not apply to Open Science as it is currently understood and implemented by Swiss institutions (see Section 1.3) – namely, according to the principle “as open as possible, *as closed as necessary*”, which has always supposed the possibility to restrict openness. Although Knowledge Security is not explicitly addressed in many Swiss national and institutional Open Science policies, most recognise that access to research outputs may need to be restricted to comply with legal, ethical, or contractual requirements.

Consequently, the central question is often not whether a publication or dataset should be made openly or restrictively accessible, but whether it should be published at all and, if not, according to which criteria. Restricting access through paywalls alone is rarely sufficient to prevent misuse or undue influence. Moreover, the Knowledge Security risks discussed in this report are not unique to Open Science; they arise equally in research conducted outside an Open Science framework. Open Science should therefore not be regarded as the source of Knowledge Security risks, but rather as one of several research contexts in which such risks must be identified and managed responsibly.

Indeed, many established Open Science practices already incorporate safeguards that contribute to the secure and responsible conduct of research. Measures such as data stewardship, FAIR data management, access controls, licensing schemes, ethical review, and secure research infrastructures demonstrate that openness and protection are complementary rather than contradictory objectives. From this perspective, Open Science, together with Knowledge Security, can be understood as a fundamental component of responsible research.

u^b

The challenges at the intersection of Open Science and Knowledge Security arise primarily for two reasons. First, Open Science principles are not always implemented effectively in practice. Weak data classification, insufficient data protection measures, the absence of Knowledge Security requirements in research workflows, non-compliance with applicable legislation (including data protection, export control, and copyright law), inadequate access controls, poor data management practices, insufficient cybersecurity of research infrastructures, limited consideration of the ethical implications of knowledge sharing, and inadequate awareness of the risks associated with collaborations involving critical partners all increase the likelihood of Knowledge Security incidents (see Chapter 3).

Second, given that Knowledge Security emerged rather recently at the horizon of higher education institutions, the topic and its implications remain insufficiently understood and incompletely embedded within institutions, both among researchers and at the level of institutional governance.

Across Switzerland, not even one institution of higher education has adopted a coherent and comprehensive approach to Knowledge Security. Most institutions currently address selected aspects of the topic according to their own priorities and capacities, while recognising that further development is needed. There is, therefore, a clear need for institution-wide governance frameworks that integrate Knowledge Security across all relevant areas of academic activity, including recruitment, international collaborations, travel, research funding, data management, digital infrastructure, and the dissemination of research results. Reconciling the commitment to openness with the responsibility to protect knowledge against legal, ethical, reputational, and strategic risks requires robust governance structures, clear institutional policies, and a strong culture of awareness, responsibility, and accountability.

In this context, the establishment of a National Contact Point for Knowledge Security, as recommended by both the National Working Group (NWG) and the Interdepartmental Working Group (IDAG), would represent a significant step forward for the Swiss higher education sector. The Dutch National Contact Point for Knowledge Security provides a valuable model for such an initiative.

A national contact point would enable higher education institutions to access specialised expertise that is often unavailable internally, particularly on issues requiring national coordination. As Knowledge Security is closely linked to national security, geopolitical developments, foreign interference, and strategically sensitive technologies, it is neither realistic nor desirable to expect individual institutions to address these issues independently without support from the federal authorities, including guidance based on information that cannot be made publicly available. Furthermore, because Knowledge Security assessments are inherently context-dependent and require case-by-case evaluation, a central source of expertise would promote greater consistency in institutional practice across Switzerland. Establishing a National Contact Point would also align Switzerland with emerging European developments. The European Union has already announced the creation of a European Knowledge Security Expert Centre, reflecting the growing importance of

coordinated national and international support structures for Knowledge Security governance (see Section 1.1).

u^b

In light of these considerations, this report endorses the recommendations formulated by the National Working Group in *Knowledge Security in Switzerland: A Strategic Framework for Higher Education Institutions and Authorities*, as well as those set out by the Interdepartmental Working Group (IDAG) in the *Bericht der IDAG Knowledge Security*. Together, these recommendations provide a solid foundation for developing a coherent Swiss approach that strengthens both Knowledge Security and Open Science, ensuring that scientific openness continues to support research excellence while safeguarding knowledge of strategic, societal, and scientific values.

In particular, institutions are encouraged to:

1. Develop a comprehensive Knowledge Security policy.

Institutions should establish clear Knowledge Security policies covering key areas such as due diligence procedures for international collaborations, technology transfer protocols, information security measures, and mechanisms for reporting Knowledge Security concerns. These policies should be developed in consultation with the research community to ensure that they are practical, proportionate, and transparent. At the same time, they should minimise unnecessary administrative burdens while remaining sufficiently flexible to respond to evolving risks and regulatory requirements.¹¹⁴

2. Establish dedicated Knowledge Security officers or specialised internal units.

Given its complex national and international regulatory environment, as well as its cross-cutting relevance across multiple areas of academic activity, Knowledge Security requires dedicated expertise and professional oversight. Effective Knowledge Security governance also depends on close collaboration across all levels of institutional management and, in particular, with researchers who are best positioned to identify and assess the risks associated with their own work.¹¹⁵

3. Implement Knowledge Security training and awareness programmes.

Institutions should provide tailored training for students, researchers and administrative staff to strengthen awareness of Knowledge Security principles and risks. In addition to the recommendations of the National Working Group, specialised training should also be offered to personnel with specific responsibilities related to Open Science, such as data stewards and Open Science officers. Such training should address dual-use research and other Knowledge Security issues relevant to their roles.¹¹⁶

4. Strengthen international and national cooperation on Knowledge Security.

Institutions should strengthen international cooperation through formal agreements, strategic partnerships, and participation in relevant Knowledge Security networks. International collaborations

¹¹⁴ See also: *Knowledge Security in Switzerland: A Strategic Framework for Higher Education Institutions and Authorities*, Section 4.1, recommendation under Axis 1. Section 1.1 of the Toolbox accompanying this report provides more details.

¹¹⁵ See also: *Knowledge Security in Switzerland: A Strategic Framework for Higher Education Institutions and Authorities*, Section 4.1, recommendation under Axis 1.

¹¹⁶ See also: *Knowledge Security in Switzerland: A Strategic Framework for Higher Education Institutions and Authorities*, Section 4.1, recommendation under Axis 1. Section 1.3 of the Toolbox accompanying this report provides inspiration.

should be approached strategically, with careful consideration of partners' profiles and the establishment of cooperation with institutions that share comparable standards, values, and commitments to responsible research and Knowledge Security. In addition, it is important to define a Swiss "way to Knowledge Security", that takes into account our unique position globally and within Europe, as well as national priorities, strengths and constraints. Not only can collaboration create valuable synergies, but it should also contribute to creating a level playing field.¹¹⁷

u^b

5. Integrate Knowledge Security into existing Open Science policies and strategies.

Institutions are encouraged to explicitly incorporate Knowledge Security principles into their existing Open Science policies and strategies in order to strengthen responsible research practices. This would address current gaps in Open Science governance, such as the absence of clear criteria for restricting access to certain research outputs, while requiring only limited adjustments to existing frameworks. Such integration would minimise additional administrative burdens and reinforce the principle that responsible research requires both openness and appropriate safeguards.¹¹⁸

6. Improve Open Science practices in light of Knowledge Security considerations.

Researchers, who retain primary responsibility for their research data and publications, together with data stewards and Open Science officers, should strengthen the integration of Knowledge Security considerations into Open Science practices.

In particular:

- Knowledge Security considerations should be incorporated into data management planning from the earliest stages of each research project.
- Data Management Plans should be carefully reviewed before publication to ensure that data sharing complies with applicable federal, cantonal, and institutional data protection requirements, as well as other relevant legal and regulatory obligations.
- Institutions should develop data classification frameworks that categorise research data according to their sensitivity and associated protection requirements. Such frameworks would support researchers and data stewards in selecting appropriate measures for data management, storage, sharing, and access throughout the research lifecycle.
- Access control mechanisms should be regularly reviewed, updated, and proportionately calibrated to the sensitivity of the data and the risks associated with the research activity.
- Institutions should ensure that Open Science infrastructures provide adequate protection against cyber threats and other security risks.
- Open Science projects involving sensitive research areas identified by each institution should undergo a proportionate Knowledge Security assessment before research activities begin. Such assessments should consider the sensitivity of the research topic, the nature of international collaborations, the applicable legal and regulatory framework, and the potential for misuse or unintended knowledge transfer. Rather than relying on predefined categories of research that are automatically excluded from Open Science, institutions should adopt a case-by-case, risk-based approach that balances openness with the protection of sensitive knowledge, research integrity, and legitimate security interests.

¹¹⁷ See also: *Knowledge Security in Switzerland: A Strategic Framework for Higher Education Institutions and Authorities*, Section 4.1, recommendation under Axis 3.

¹¹⁸ A practical tool is suggested in Section 1.2 of the Toolbox accompanying this report ("Knowledge Security Management Plan").

Criteria that define under which circumstances data can be shared or not should be as precise as possible. Otherwise, researchers will remain in the dark and, when in doubt, will decide against publishing data, even if this is not at all necessary.

7. Use Open Science practices as Knowledge Security measures.

Open Science practices can also contribute to strengthening Knowledge Security.

u^b

For example, institutions and researchers should:

- Use Data Management Plans to assess data storage, access, and transfer arrangements throughout the research lifecycle.
- Ensure that data transfers are supported by appropriate contractual safeguards and comply with applicable legal and institutional requirements.
- Apply proportionate access controls to research outputs where necessary to protect sensitive information while enabling responsible sharing.
- Promote transparency and collaboration within Open Science infrastructures to enhance reproducibility and accountability according to the many-eyes principle.

Practical instruments for implementing these measures are provided in the Toolbox on Knowledge Security and Open Science.

Interviews

u^b

Name	First name	Institution	Country	Job title
Aagaard	Kaare	Aarhus University	Denmark	Open Science Coordinator
Anonymous researcher			Switzerland	
Bach	Felix		Germany	Hochschule Karlsruhe
Bosman	Ryan	TNO	Netherlands	Security Advisor
Caron	Florence	EPFL	Switzerland	Project Manager, International Affairs
Castelltort	Sébastien	University of Geneva	Switzerland	Vice-rector Research and Sustainability
de Bast	Anouk	ETHZ	Switzerland	Head International Affairs
de Halleux	Véronique	imec	Belgium	Principal Expert, Research Library & Open Access
Dubochet	Gilles	EPFL	Switzerland	Head of Open Science
Dunning	Alastair	TU Delft	Netherlands	Head, Research Services (Library)
Eechaudt	Vincent	University of Gent	Belgium	Senior policy advisor – Research security, export control, dual-use research, human rights policy
Fritsch	Johannes	Leopoldina	Germany	Leiter der Geschäftsstelle
Girardin	Jordan	SNSF	Switzerland	Scientific Officer Knowledge Security
Janssen	Katleen	KU Leuven	Belgium	Head of the Knowledge Security Office
Jeney	Sylvia	SNSF	Switzerland	Head of Open Research Data
Krappe	Johanna	University of Turku	Finland	Head of RDI & Global Engagement
Marino	Mario	University of Bologna	Italy	Data Steward
Merloni	Andrea	Max Planck Institute for Extraterrestrial Physics (MPE)	Germany	Senior Scientist
Nast	Silvia	ETHZ	Switzerland	Head of Export Control
Omitted	Omitted	Radboud University	Netherlands	Research Security Officer at Radboud University
Omitted	Omitted	Federal Intelligence Service	Switzerland	Head of the Technopol module within the FIS' Prophylax awareness programme
Proudman	Vanessa	Sparc Europe	Netherlands	Director

u^b

Singh	Akshay	University of British Columbia	Canada	Director Research Security
Sommer	Job	National Contact Point KS	Netherlands	Knowledge security advisor
Strebel	Ignaz	ETHZ	Switzerland	Coordinator for Open Science
Thomas	Beatrijs	imec	Belgium	Compliance Manager Export Controls, Sanctions and Knowledge Security
van der Molen	Franke	Radboud University	Netherlands	policy officer (Open Science)
van der Molen	Irna	University of Twente	Netherlands	Policy-advisor knowledge security
van Gils	Aart	TU Delft	Netherlands	Policy Advisor, Knowledge Security
Vasone	Filippo	University of Bologna	Italy	Data Steward
Vermaas	Pieter	TU Delft	Netherlands	Professor in philosophy of quantum technologies
Westensee	John	Aarhus University	Denmark	Senior Advisor Knowledge Security

Bibliography

Ahlers, Anna Lisa, and Annina Sofia Lattu. "Open Science in China." Presentation at *Open Science Days 2025*, Berlin, November 10, 2025.

All European Academies (ALLEA). *The European Code of Conduct for Research Integrity*. Revised ed. Berlin: ALLEA, 2017. <https://allea.org/code-of-conduct/>.

Altunay, Melike, Avery, Patricia, Blackburn, Keith et al. "A Science Driven Production Cyberinfrastructure — the Open Science Grid." *Journal of Grid Computing* 9, 2011: 201–218. <https://doi.org/10.1007/s10723-010-9176-6>

Arcesati, Rebecca, Chimits, François, and Hmaidi, Antonia. *Keeping Value Chains at Home: How China Controls Foreign Access to Technology and What It Means for Europe*. MERICS Report. Berlin: Mercator Institute for China Studies (MERICS), August 2024. <https://merics.org/en/report/keeping-valuechains-home>.

armasuisse. "Research Program Security: Das VBS und der ETH-Bereich stärken Forschung im Bereich Sicherheit und Verteidigung." Swiss Confederation, May 22, 2026. <https://www.ar.admin.ch/de/newsb/YOj8z3xJzFT5>.

armasuisse. *Rüstungspolitische Strategie des Bundesrates*. Bern: Swiss Confederation, June 20, 2025. <https://www.ar.admin.ch/de/ruestungspolitikbundesrates>.

Association of Research Managers and Administrators (ARMA). *Complex Collaborations: Efficiency, Equity, Quality and Security in International Research*. Final Report. 2023.

Baums, Ansgar, and Nicholas Butts. *Tech Cold War: The Geopolitics of Technology*. Boulder, CO: Lynne Rienner Publishers, 2025.

Bieri, Matthias, and Andreas Wenger. "Subsidiarität und die Schweizer Sicherheitspolitik." *CSS Analysen zur Sicherheitspolitik*, no. 227. Zurich: Center for Security Studies, May 2018.

Borges, Chris. "Public and Private R&D Are Complements – Not Substitutes." Center for Strategic and International Studies, August 2025.

Brenneis, Andreas. "Assessing Dual Use Risks in AI Research: Necessity, Challenges and Mitigation Strategies." *Research Ethics* 21, no. 2, 2024: 302–330. <https://doi.org/10.1177/17470161241267782>.

Bundesamt für Justiz. *Bericht zum US CLOUD Act: Gutachten des Bundesamts für Justiz*. Bern: Schweizerische Eidgenossenschaft, September 17, 2021. <https://www.bj.admin.ch/bj/de/home/publiservice/publikationen/berichte-gutachten/2021-09-17.html>.

Burwell, Frances, and Kenneth Propp. *Digital Sovereignty: Europe's Declaration of Independence?* Washington, DC: Atlantic Council, January 2026.

Cao, Cong, Richard P. Suttmeier, and Denis Fred Simon. "China's 15-Year Science and Technology Plan." *Physics Today* 59, no. 12, 2006: 38–43.

Carroll, Stephanie Russo, Ibrahim Garba, Oscar L. Figueroa-Rodríguez, James Holbrook, et al. "The CARE Principles for Indigenous Data Governance." *Data Science Journal* 19, 2020. <https://doi.org/10.5334/dsj-2020-043>.

CESAER. *Keeping science open? Current challenges in the day-to-day reality of universities*. White paper, 2023, <http://doi.org/10.5281/zenodo.8355324>.

CESAER. *Research Security as a Collective Responsibility: Empowering Universities, Enabling Europe*, 2025. <https://doi.org/10.5281/zenodo.17453941>.

Cheung, Tai Ming. *Innovate to Dominate: The Rise of the Chinese Techno-Security State*. Ithaca, NY: Cornell University Press, 2022.

Churakova, O., et al. *Recommendations on Ethics in Research Data Management*. Bern, University of Bern, 2026.

- Clapp, Sebastian, Martin Höflmayr, and Falk Vambrie. *Building a Common Market for European Defence*. EPRS Briefing PE 775.924. Brussels: European Parliamentary Research Service, September 2025.
- Clapp, Sebastian. *European Defence Industrial Strategy*. EPRS Briefing PE 762.402. Brussels: European Parliamentary Research Service, September 2024.
- Council of Canadian Academies (CCA). *Balancing Research Security and Open Science*. Ottawa, ON: Expert Panel on Sensitive Research of Concern, Council of Canadian Academies, 2025. <https://doi.org/10.60870/fmt9-9559>.
- Council of the European Union. *Council Recommendation of 23 May 2024 on Enhancing Research Security (C/2024/3510)*. *Official Journal of the European Union*, C/2024/3510, May 30, 2024. <https://eur-lex.europa.eu/eli/C/2024/3510/oj>
- Council of the European Union. *Knowledge Security and Responsible Internationalisation*. Brussels: Council of the European Union, 2023. <https://data.consilium.europa.eu/doc/document/ST-8824-2023-INIT/en/pdf>.
- d'Hooghe, Ingrid, and Jonas Lammertink. *Towards Sustainable Europe-China Collaboration in Higher Education and Research*. Leiden: Leiden Asia Centre, 2020. [20-10-01-Towards-Sustainable-Europe-China-Collaboration-in-Higher-Education-and-Research.pdf](https://www.leiden.nl/asia-centre/publications/20-10-01-Towards-Sustainable-Europe-China-Collaboration-in-Higher-Education-and-Research.pdf)
- Draghi, Mario. *The Future of European Competitiveness: A Competitiveness Strategy for Europe (Part A) and In-Depth Analysis and Recommendations (Part B)*. Brussels: European Commission, September 9, 2024. https://commission.europa.eu/topics/competitiveness/draghi-report_en.
- Drezner, Daniel W., Henry Farrell, and Abraham L. Newman, eds. *The Uses and Abuses of Weaponized Interdependence*. Washington, DC: Brookings Institution Press, 2021.
- Drinhausen, Katja, and Helena Legarda. *Confident Paranoia: Xi's "Comprehensive National Security" Framework Shapes China's Behavior at Home and Abroad*. China Monitor, no. 75. Berlin: Mercator Institute for China Studies (MERICS), September 2022.
- EARTO – European Association of Research and Technology Organisations. *EARTO answer to EC consultation on technologies with dual-use potential (Final)*, 2024. <https://www.earto.eu/wp-content/uploads/EARTO-Answer-to-EC-Consultation-on-Technologies-with-dual-use-potential-Final.pdf>
- Eigner, Leo. "China's Vision for Science and Technology." *CSS Analyses in Security Policy*, no. 364. Zurich: Center for Security Studies, July 2025.
- Eigner, Leo. "Dual-Use and Defence Research in Europe." *CSS Policy Briefs*, no. 2. Zurich: Center for Security Studies, May 2026.
- Eigner, Leo. "Knowledge Security at Stake." *CSS Analyses in Security Policy*, no. 338. Zurich: Center for Security Studies, March 2024.
- Eiterjord, T. "Securitize the Volume: Epistemic Territorialisation and the Geopolitics of China's Arctic Research." *Territory, Politics, Governance* 12, no. 1, 2024: 93–111. <https://doi.org/10.1080/21622671.2023.2179535>.
- EOSC. *Empowering Europe's Trusted, Secure and Sovereign Research Data Ecosystem*. April 2026. <https://doi.org/10.5281/zenodo.19368164>.
- ETH Zurich. *Guidelines for Research Data Management at ETH Zurich (RDM Guidelines)*. RSETHZ 414.2. Zurich: ETH Zurich, July 1, 2022. [414.2en.pdf](https://www.ethz.ch/en/research-data-management/414.2en.pdf)
- EURAXESS. "The EU's Open Science Policy." European Commission. <https://euraxess.ec.europa.eu/worldwide/asean/eus-open-science-policy>.
- European Commission, Directorate-General for Research and Innovation. *Open Innovation, Open Science, Open to the World: A Vision for Europe*. Luxembourg: Publications Office of the European Union, 2016.

European Commission, Directorate-General for Research and Innovation. "A European Framework for Science Diplomacy." News article. European Commission, February 13, 2025.

European Commission. *Annex to the Commission Recommendation on Critical Technology Areas for the EU's Economic Security for Further Risk Assessment with Member States*. C(2023) 6689 final. Strasbourg, October 3, 2023. [C_2023_6689_1_EN_annexe_acte_autonome_part1_v9.pdf](#)

European Commission. *Commission Recommendation (EU) 2023/2113 of 3 October 2023 on Critical Technology Areas for the EU's Economic Security for Further Risk Assessment with Member States*. Official Journal of the European Union L, 2023/2113, October 11, 2023. [Commission Recommendation \(EU\) 2023/2113 of 3 October 2023 on critical technology areas for the EU's economic security for further risk assessment with Member States](#)

European Commission. *Guiding Notes to Use the TRL Self-Assessment Tool*. Horizon Europe. Brussels: European Commission, 2021. [trl-assessment-tool-guide-final.pdf](#)

European Parliament and Council of the European Union. *Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on Open Data and the Re-use of Public Sector Information*. Official Journal of the European Union L 172, June 26, 2019: 56–83.

European Research Executive Agency. "Open Science." European Commission. https://rea.ec.europa.eu/open-science_en.

Everts, Steven, Giuseppe Spatafora, and Alice Ekman, eds. *Low Trust: Navigating Transatlantic Relations under Trump 2.0*. Chaillot Paper no. 187. Paris: European Union Institute for Security Studies, October 2025.

Falco, Gregory, Boschetti, Nicola and Nikas, Ioannis. *Undercover Infrastructure: Dual-Use Arctic Satellite Ground Stations*. Waterloo, ON: Centre for International Governance Innovation, 2024. <https://www.cigionline.org/publications/undercover-infrastructure-dual-use-arctic-satellite-ground-stations/>.

Fara, Patricia. *Science: A Four Thousand Year History*. Oxford: Oxford University Press, 2010.

Finnish Ministry of Education and Culture. *Recommendations of the Working Group on Responsible International Cooperation in Higher Education and Research*. Helsinki: Ministry of Education and Culture, 2025.

Freilich, Janet, et al. "Data Manipulation within the US Federal Government." *The Lancet* 406, no. 10500, 2025: 227–228.

García Bercero, Ignacio, Collin, Antoine Mathieu, McWilliams, Ben, Poitiers Niclas, and Tagliapietra, Simone. "'Made with Europe,' Not 'Made in Europe,' Should Guide EU Industrial Policy." Brussels: Bruegel, February 2026.

Garisto, Dan, and Lenharo, Mariana. "White House Proposes Vast Overhaul of US Science Funding: What You Need to Know." *Nature*, June 3, 2026.

Garisto, Dan. "Entire NSF Science Advisory Board Fired by Trump Administration." *Nature*, April 28, 2026.

Gentile, Gian, Shurkin, Michael, Evans, Alexandra T., Grisé, Michelle, Hvizda, Mark and Jensen, Rebecca. *A History of the Third Offset, 2014–2018*. Santa Monica, CA: RAND Corporation, 2021.

German National Academy of Sciences Leopoldina, and German Research Foundation (DFG). *Scientific Freedom and Security Interests in Times of Geopolitical Polarisation: Fifth Report of the Joint Committee of DFG and Leopoldina*. Halle (Saale): German National Academy of Sciences Leopoldina, November 1, 2024.

German Research Foundation (DFG). *Dealing with Risks in International Research Collaborations*. Bonn: German Research Foundation, 2023.

German Science and Humanities Council. *Science and Security in Times of Global Political Upheaval*. Position Paper. Cologne: German Science and Humanities Council, 2025.

- Girishankar, Navin, ed. *Staying Ahead in the Global Technology Race: A Roadmap for Economic Security*. Washington, DC: Center for Strategic and International Studies, October 2024.
- Grgić, Gorana, Foulon, Michiel and Schepers, Névine. "Europe's Semiconductor Strengths and Strains." *CSS Analyses in Security Policy*, no. 360. Zurich: Center for Security Studies, May 2025.
- Grgić, Gorana. "The Changing Nature of the EU's and NATO's Partnerships." *CSS Analyses in Security Policy*, no. 348. Zurich: Center for Security Studies, October 2024.
- Guston, David H. *Between Politics and Science: Assuring the Integrity and Productivity of Research*. Cambridge: Cambridge University Press, 2000.
- Hackenbroich, Jonathan, Medunic, Filip and Zerka, Paweł. *Tough Trade: The Hidden Costs of Economic Coercion*. London: European Council on Foreign Relations, February 2022.
- Hermans, Katherine, Höfler, Manuela, Robinson, Mark and Thommen, Marc. *Open by Default: Open Science at the University of Zurich*. Zurich: University of Zurich, 2021.
- Hufschmid, Manon. *Enhancing Knowledge Security in Switzerland: Providing a Source of Inspiration for SwissCore Funders and Partners*. Brussels: SwissCore, 2025.
- Innosuisse. "Innosuisse und armasuisse lancieren eine Projektausschreibung im Bereich Dual-Use-Technologien." April 30, 2026. <https://www.innosuisse.admin.ch/de/newsb/xMNk0LL66iDuYlrinwy7m>.
- Karásková, Ivana, Šebok, Filip and Blablová, Veronika. *How to Do Trusted Research: China-Specific Guidelines for European Stakeholders*. Prague: Association for International Affairs (AMO), 2022.
- Keim, Wiebke, Rodriguez Medina, Leandro and Arvanitis, Rigas eds. *Routledge Handbook of Academic Knowledge Circulation*. London: Routledge, 2023.
- Lattu, Annina Sofia. *Open Science in China: An Open and Closed Case. Observations: Short Working Papers on Science and Society in China and the World*, no. 13. Berlin: Max Planck Institute for the History of Science, 2023. <https://doi.org/10.17617/2.3553727>
- Lenharo, Mariana. "NIH-Funded Science Must Now Be Free to Read Instantly: What You Should Know." *Nature*, June 26, 2025.
- Letta, Enrico. *Much More Than a Market*. Report to the European Council. April 2024. <https://institutdelors.eu/en/publications/much-more-than-a-market/>
- Li, Xiaojie, Cong, Yali and Yi, Zheng. "Research under China's Personal Information Law." *Science* 378, no. 6622, 2022: 713–715.
- Marwaha, Sapna, et al. *Stronger Cooperation, Safer Collaboration: Driving Research Security Cooperation across Europe*. 2025.
- Matthews, David. "Foreign Researchers in China Face Tightening Restrictions." *Nature*, March 6, 2025.
- McFaul, Cole, Bresnick, Sam, and Chou, Daniel. *Pulling Back the Curtain on China's Military-Civil Fusion: How the PLA Mobilizes Civilian AI for Strategic Advantage*. Washington, DC: Center for Security and Emerging Technology, September 2025.
- Möckli, Daniel. "Rudderless World: American Neo-Revisionism and the Demise of Global Order." In *Strategic Trends 2025*, edited by Gorana Grgić and Daniel Möckli, 11–31. Zurich: Center for Security Studies, 2025.
- Molas-Gallart, Jordi. "Which Way to Go? Defence Technology and the Diversity of 'Dual-Use' Technology Transfer." *Research Policy* 26, no. 3, 1997: 367–385.
- Moradi, Sh., and S. Abdi. "Open Science-Related Policies in Europe." *Science and Public Policy* 50, no. 3, 2023: 521–530.
- Müller, Roland, et al. "Cybersecurity Efforts Undertaken at BESSY II." *Journal of Physics: Conference Series* 3010, 2025: 012022. <https://doi.org/10.1088/1742-6596/3010/1/012022>.

- National Science Foundation, National Center for Science and Engineering Statistics. *Discovery: R&D Activity and Research Publications*. NSB-2025-7. Alexandria, VA: National Science Foundation, 2025. <https://ncses.nsf.gov/pubs/nsb20257>.
- Nelson, Alondra. *Ensuring Free, Immediate, and Equitable Access to Federally Funded Research*. Memorandum for the Heads of Executive Departments and Agencies. Washington, DC: Office of Science and Technology Policy, Executive Office of the President, August 25, 2022. <https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/08/08-2022-OSTP-Public-Access-Memo.pdf>.
- OECD. "Integrity and Security in the Global Research Ecosystem." *OECD Science, Technology and Industry Policy Papers*, no. 130. Paris: OECD Publishing, 2022. <https://doi.org/10.1787/1c416f43-en>.
- OECD. *Economic Security in a Changing World: New Approaches to Economic Challenges*. Paris: OECD Publishing, 2025.
- Oltmann, Shannon M. "Dual Use Research: Investigation Across Multiple Science Disciplines." *Science and Engineering Ethics* 21 (2015): 327–341.
- Open Research Community Accelerator (ORCA). *Fostering Innovation Through Open Science: A Cross-Sector Roadmap for Impact*. 2025. <https://doi.org/10.5281/zenodo.16877389>.
- Pannier, Alice. *Software Power: The Economic and Geopolitical Implications of Open Source Software*. Paris: Institut français des relations internationales (IFRI), December 2022.
- Papadopoulos, Yannis, Sciarini, Pascal, Vatter, Adrian, Häusermann, Silja, Emmenegger, Patrick and Fossati, Flavia eds. *Handbuch der Schweizer Politik = Manuel de la politique suisse*. 7th ed. Zurich: NZZ Libro, 2023.
- Peisert, Sean, Von Welch, Andrew Adams, Ruth Anne Bevier, Michael Dopheide, Rich LeDuc, Pascal Meunier, Steve Schwab, and Karen Stocks. *Open Science Cyber Risk Profile (OSCRP)*, Version 1.3.3. October 2022. DOI: [10.5281/zenodo.7268749](https://doi.org/10.5281/zenodo.7268749).
- Petit, Nicolas. *Big Tech and the Digital Economy: The Moligopoly Scenario*. Oxford: Oxford University Press, 2020.
- Rosenauer, Philipp. "Wenn Sensitive Daten Grenzen Überschreiten." *Procure Swiss Magazin*. procure.ch. <https://www.procure.ch/magazin/artikel/wenn-sensible-daten-grenzen-ueberschreiten>
- Safeguarding Science Team. *Due Diligence in Science: Manual for an Assessment Process – Safeguarding Science and Scientific Cooperation*. Bonn, 2024.
- Schepers, Névine. "China's Strategic Use of Trade Controls." *CSS Policy Briefs*, no. 1. Zurich: Center for Security Studies, April 2026.
- Schmid, Evelynne. "Ethical Considerations in External Collaborations: The Report of a Working Group at the University of Lausanne (7/9)." *Oxford Human Rights Hub* (blog), May 30, 2026. <https://ohrh.law.ox.ac.uk/ethical-considerations-in-external-collaborations-the-report-of-a-working-group-at-the-university-of-lausanne-7-11/>.
- Schwab, Klaus. *The Fourth Industrial Revolution*. Geneva: World Economic Forum, 2016.
- Shih, Tommy. "Points of Departure and Developing Good Practices for Responsible Internationalization in a Rapidly Changing World." *Accountability in Research* 32, no. 5, 2025: 845–851. <https://doi.org/10.1080/08989621.2024.2318789>.
- Stanton, Noah. *Dual-use Research and Innovation in Europe and Switzerland*. Brussels: SwissCore, 2026.
- State Secretariat for Education, Research and Innovation (SERI). *Internationale Strategie der Schweiz im Bereich Bildung, Forschung und Innovation*. Bern: Swiss Confederation, July 2018. https://www.sbf.admin.ch/dam/de/sd-web/stJ1sWncEgw9/internationale_strategie_bfi_d.pdf.
- Stoye, Emma. "China–US Research Collaborations Are in Decline—This Is Bad News for Everyone." *Nature*, July 19, 2024.

- Swiss Academies of Arts and Sciences. *Code of Conduct for Scientific Integrity*. Bern: Swiss Academies of Arts and Sciences, 2021. <https://doi.org/10.5281/zenodo.4707560>.
- Swiss Academy of Sciences (SCNAT). *Guide for Global Research Partnerships: Six Principles for More Effective and Equitable Research*. Bern: Swiss Academy of Sciences, 2025.
- Swiss Confederation, State Secretariat for Education, Research and Innovation (SERI). *Research and Innovation in Switzerland: Interim Report 2022*. Bern: State Secretariat for Education, Research and Innovation, 2022. https://www.sbf.admin.ch/rapport_r-i.
- Swiss Confederation. *Bericht der IDAG Knowledge Security*. Bern, November 10, 2025.
- Swiss Confederation. *Foreign Policy Strategy 2024–2027*. Bern: Federal Department of Foreign Affairs, 2024.
- Swiss Federal Council. *Souveraineté numérique de la Suisse*. Bern: Swiss Federal Council, 2025 [7a265759-84df-4915-82e8-5af9ea8f5a57.pdf](https://www.sbf.admin.ch/rapport_r-i)
- Swiss National Science Foundation (SNSF). "Open Access Publications." <https://www.snf.ch/en/VyUvGzptStOEpUoC/topic/open-access-publications>.
- swissuniversities. *Knowledge Security in Switzerland: A Strategic Framework for Higher Education Institutions and Authorities*. Bern: swissuniversities, 2025.
- swissuniversities. *Swiss National Open Access Strategy*. Bern: swissuniversities, 2024. https://www.swissuniversities.ch/fileadmin/swissuniversities/Dokumente/Hochschulpolitik/Open_Access/Swiss-National-Open-Access-Strategy-2024-en.pdf.
- swissuniversities. *Swiss National Open Research Data Strategy*. Bern: swissuniversities, 2021. https://www.swissuniversities.ch/fileadmin/swissuniversities/Dokumente/Hochschulpolitik/Open_Access/Swiss_National_ORD_Strategy_en.pdf.
- Tatlow, Didi Kirsten. "China's Expanding Arctic Ambitions Challenge the U.S. and NATO." *Newsweek*, July 21, 2024. <https://www.newsweek.com/2024/08/09/china-russia-us-arctic-north-pole-strategy-svalbard-norway-sea-route-1916641.html>.
- The Economist*. "Europe Is Going on a Huge Military Spending Spree." December 1, 2025.
- The Royal Society. *Science in the Age of AI: How Artificial Intelligence Is Changing the Nature and Method of Scientific Research*. London: The Royal Society, October 2024. <https://royalsociety.org/news-resources/projects/science-in-the-age-of-ai/>.
- Thomson, John. "Canadian Military Developing Surveillance System to Monitor Arctic Waters." *CBC News*, August 2, 2017. <https://www.cbc.ca/news/canada/north/cause-array-drdc-test-1.4232348>.
- Tollefson, Jeff, and Max Kozlov. "US Congress Set to Reject Trump's Sweeping Science Budget Cuts." *Nature*, January 20, 2026.
- Trump, Donald J. *Presidential Memorandum on United States Government-Supported Research and Development National Security Policy*. Washington, DC: The White House, January 14, 2021. <https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/>.
- UNESCO. *UNESCO Recommendation on Open Science*. Paris: UNESCO, 2021. <https://www.unesco.org/en/open-science/about>.
- United States Congress. *CHIPS and Science Act*. Pub. L. No. 117-167, H.R. 4346, 117th Cong. Signed into law August 9, 2022.
- Universities UK (UUK). *Managing Risks in International Research and Innovation*. London: Universities UK, 2020. https://www.universitiesuk.ac.uk/sites/default/files/field/downloads/2022-06/managing-risks-in-international-research-and-innovation-uuk-cpni-ukri_1.pdf.
- University of Geneva. *Roadmap to Open Science 2025–2028*. Geneva: University of Geneva, 2025.

- van der Lee, M., C. Peters, M. van Berlo, et al. "A Holistic Framework for Assessing the Uptake Potential of EU-Funded Security Research and Innovation Project Results." *Open Research Europe* 5, 2026: 115. Version 2. <https://doi.org/10.12688/openreseurope.19711.2>.
- Vermaas, Pieter, et al. "Toward a Code of Conduct for Technology Ethics Practitioners." *Journal of Responsible Innovation* 12, no. 1, 2025: 2440958. <https://doi.org/10.1080/23299460.2024.2440958>.
- von der Leyen, Ursula. *Europe's Choice: Political Guidelines for the Next European Commission 2024–2029*. Strasbourg: European Commission, July 18, 2024. https://commission.europa.eu/document/download/e6cd4328-673c-4e7a-8683-f63ffb2cf648_en.
- Wilkinson, Mark D., Michel Dumontier, IJsbrand Jan Aalbersberg, et al. "The FAIR Guiding Principles for Scientific Data Management and Stewardship." *Scientific Data* 3 (2016): 160018. <https://doi.org/10.1038/sdata.2016.18>.
- Wübbeke, Jost, Meissner, Mirjam, Zenglein, Max J., Ives, Jaqueline and Conrad, Björn. *Made in China 2025: The Making of a High-Tech Superpower and Consequences for Industrial Countries*. Berlin: Mercator Institute for China Studies (MERICS), December 2016.
- Xi Jinping. "Speech at the Work Conference for Cybersecurity and Informatization." Translated by Rogier Creemers. *China Copyright and Media*, April 19, 2016. <https://chinacopyrightandmedia.wordpress.com/2016/04/19/speech-at-the-work-conference-for-cybersecurity-and-informatization/>.
- Ye, Josh. "Chinese Authority Launches Probe into Chinese Academic Database CNKI." *Reuters*, June 24, 2022. <https://www.reuters.com/world/china/chinese-authority-launches-probe-into-chinese-academic-database-cnki-2022-06-24/>
- You, Xiaoying. "China Seeks Self-Reliance in Science in Next Five-Year Plan." *Nature* 647, 2025: 11-12.