WR

WISSENSCHAFTSRAT

2025

Science and security in times of global political upheaval

Position paper

IMPRINT

Science and security in times of global political upheaval | Position paper

Publisher

German Science and Humanities Council | Wissenschaftsrat (WR)
Scheidtweilerstraße 4
50933 Cologne
www.wissenschaftsrat.de
post@wissenschaftsrat.de

Document number: 2485-25_en

DOI: https://doi.org/10.57674/v8dp-8269

Published

Cologne, May 2025

CONTENT

Preliminary remarks **5**

Summary **6**

A. Academic freedom in times of great uncertainty **9**

A.I Crisis of the liberal and rules-based post-war order **10**

A.II Academic freedom as an essential element of open societies **12**

B. Concepts and analyses **15**

B.I Security **16**

B.II Security-relevant research **18**

B.III Knowledge security **22**

B.IV Law and voluntary commitment **26**

IV.1 Export control 26

IV.2 Civil clauses 28

C. Recommendations for dealing with knowledge risks and security-relevant research **31**

C.I Sharing responsibility **32**

C.II Governance guidelines for dealing with knowledge risks and security relevance **34**

C.III Recognising knowledge risks and managing them **35**

III.1 Case-related individual examination and collegial exchange 36

III.2 Strategic management task: structurally anchoring risk assessment 40

III.3 Establish a National Platform for knowledge security 41

C.IV Advancing security-relevant research **47**

IV.1 Strategic planning of security-relevant research 48

IV.2 Integrative and systemic approach to security-relevant research 51

D. Outlook on the consequences for the system of research and higher education **59**

Appendix **64**

Appendix 1: Questions to explain knowledge risk types 64

Appendix 2: Funding of military research in Germany 67

List of abbreviations 69

Contributors **71**

Preliminary remarks

Serious changes in the global political situation, dealing with numerous uncertainties in the defence policy and economic situation as well as the development of research results and technologies with an inherent dual-use potential present Germany, Europe and many other democratic states with new security policy challenges. The system of research and higher education cannot escape these developments, and even more: with its research and teaching achievements, its international networking and its contributions to technological developments and innovations, it makes a significant contribution to overcoming these challenges.

This constellation means that the system of research and higher education in Germany and Europe has to deal with security-relevant issues in an unprecedented way – in two respects: on the one hand, measures must be taken to adequately protect the system of research and higher education and at the same time guarantee academic freedom. On the other hand, actors in the system of research and higher education also have a responsibility to contribute to the security and resilience of an open democratic society. With this paper, the German Science and Humanities Council (Wissenschaftsrat, WR) is developing a position in two respects. It provides answers to the question of how the system of research and higher education can be well protected without encouraging an inappropriate bureaucratisation of research and teaching. And it develops answers to the question of how the various actors in the system of research and higher education, individual researchers, the management of scientific institutions, scientific and funding organisations, as well as the science policy level can take responsibility for protecting and building resilience in our society.

Experts who are not members of the WR contributed to the development of the recommendations. The Foreign Intelligence Service of Germany (Bundesnachrichtendienst, BND) also contributed within the scope of its legal mandate. The WR owes them all a special debt of gratitude and would also like to thank other experts from Germany and abroad who have supported the consultation process through discussions with the committee or in individual meetings. The WR adopted the position paper on 9 May 2025 in Mainz.

Summary

An increasingly confrontational security policy arena, the significant increase in security risks and threats as well as the strengthening and growing number of autocratic systems are **eroding** the **liberal, rules-based post-war order**. The Western-style democratic model has not yet prevailed globally to the extent expected. At the same time, research activities and technologies are increasingly developing an inherent dual-use character, not only, but especially in fields such as biotechnology, quantum technology and artificial intelligence (AI). Countries outside the democratic spectrum also have very good to excellent research capacities in these advanced areas.

In its position paper, the WR has developed recommendations **for dealing with knowledge risks and the contribution of science and humanities to protecting and building a resilient society**.

Both objectives are of particular importance: on the one hand, the science system is particularly vulnerable due to its openness; on the other hand, it makes significant contributions to the security of the community due to its high level of innovation. However, it is not yet sufficiently prepared for this challenge and the associated tasks. **Germany has a lot of catching up to do in both respects**.

Today, security is understood in a comprehensive and integrative way – not only in terms of the defence of external borders, but also in terms of building internal security and resilience. Security Research is therefore relevant insofar as it contributes and should contribute to the maintenance of internal and external security as well as to the development of resilience and the protection of the natural living conditions of the community, but can also jeopardise these. The system of research and higher education needs to **pay greater attention to knowledge security** – a term developed in this position paper – (cf. B.III) and **to the importance of security-relevant research**.

With regard to questions of knowledge security, the WR believes that first and foremost, every scientist is responsible for realistically assessing the risks of her or his own work. This requires the provision of sufficient information and support structures. If there are any doubts, the next step should be to examine together with other researchers or a representative of the institution five different types of risk identified by the WR (cf. B.III). It is the responsibility of the management of higher education institutions and research institutions to provide

the necessary support. The WR recommends that every institution **develops and implements** a **lean, manageable and at the same time clear risk assessment** (cf. C.III.2). It can be organised differently depending on the risk profile and size of the institution. Cross-institutional models should be examined.

The WR recommends the **swift** establishment **of a National Platform for Knowledge Security** (cf. C.III.3), in which the various scientific stakeholders and political decision-makers work together in a spirit of trust. Subsidiary to the existing decentralised structures, it should function as a one-stop shop at national level to support scientific stakeholders in the assessment of knowledge risks by providing competent and comprehensive information for risk assessment as a lean, rapid-response institution. At the same time, it should develop a coherent positioning at national level and have a broad advisory effect on the system of research and higher education.

In order to strengthen **security-relevant research**, the WR recommends better **integrating** the **currently fragmented field** and specifically **promoting systemic research approaches**. Integration can be self-organised, but should be specifically supported via funding lines and the establishment of a synthesis centre (cf. C.IV.2). Such a systemic and integrated view is also associated with a cultural change not only in the narrower field of security-relevant research, but in the entire system of research and higher education. The WR recommends that this discourse should also be conducted in higher education institutions and research organisations with all stakeholders.

In the coming years, significantly **more funds** are likely to be provided **for security-relevant research and development work**. In order to do this effectively and efficiently, a much **broader spectrum of actors** in the system must be addressed. This is the only way to strengthen a systemic approach and leverage synergies in the existing system of research and higher education. For the individual institutions, this means overcoming challenges with regard to the security standards to be complied with, particularly in the case of work aimed at military deployment. Furthermore, in view of the escalating security policy situation, structures are needed in which research and development can be carried out at high speed – including innovations that should be of a technological, strategic and social nature. Here, too, it is important to bring together the different perspectives. To this end, the WR recommends the establishment of **innovation hubs** (cf. C.IV.2).

Other countries have already developed processes for multi-perspective risk analysis. In Germany, a S**trategic Dialogue Forum** should be established, which, if a **National Security Council** is set up, should be located there. Such a forum can set up a strategy cycle and also articulate the necessary research requirements in a systematic form based on the regularly updated risk analyses.

In view of the comparable challenges and opportunities within Europe, the WR recommends that the political players work closely with the EU and other European partners to advance the efforts suggested here. In this way, potentials and synergies – both in terms of dealing with knowledge risks and promoting security-relevant research – can be better utilised.

The developments and recommended changes outlined here will significantly change the system of research and higher education in Germany and Europe. The WR expressly emphasises **the high value of academic freedom**, which requires all actors in the system to be aware of their responsibility to maintain knowledge security in scientific work and to be prepared to contribute to the security and resilience of the community.

A. Academic freedom in times of great uncertainty

The system of research and higher education in Germany is confronted with challenging developments on a European and global political level. An increasingly **confrontational security policy arena** and a massive increase in violent conflicts have been observed for several years. On a global political level, this currently includes Russia's war of aggression against Ukraine, the intensification of the conflict between the People's Republic of China and Taiwan and the escalating crises in the Middle East. |[1] At the same time, Germany and Europe are now confronted with a broad spectrum of security policy risks that directly challenge our open and democratic society, even in people's everyday lives. Central to this are scenarios of hybrid warfare in the sense of a combination of different threats, particularly in economic, media and cyber-technological terms. In addition, there are serious uncertainties in terms of security policy in view of the change of political leadership in the United States of America in 2025 and the associated implications for the future of Europe and NATO.

At the same time, **scientific cooperation and exchange** – also across system boundaries – are **more necessary than ever** in order to research global challenges and develop solution strategies. The rapidly advancing climate change cannot be overcome without scientific cooperation. The climate change, like other major societal challenges such as food security, requires more rather than less international cooperation. In combination, these global trends confront the German system of research and higher education, which is open and geared towards cooperation, with major new tasks.

In addition, some **countries outside the democratic spectrum** have **excellent research and development capacities** that are highly attractive to researchers from Germany and Europe. First and foremost, China has been striving for

| [1] The number of wars and violent conflicts is at an all-time high worldwide. The latest conflict trend analysis based on the Uppsala Conflict Data Programme (UCDP) at the Department of Peace and Conflict Research at Uppsala University shows the highest level of state-organised conflicts since 1946 in 2023, cf. https://ucdp.uu.se/. For a detailed analysis cf. Rustad, S. A. (2024): Conflict Trends: A Global Overview, 1946-2023; Oslo, https://www.prio.org/publications/14006.
All web links in this position paper were last accessed on 06.05.2025.

global dominance in strategic fields of science and technology for a good decade. [2] At the same time, more and more **research activities and technologies** have **an inherent dual-use character**, so that security-relevant issues and questions of technological and economic sovereignty harbour a high degree of security policy implications. This applies in particular, but not exclusively, to fields such as quantum technology, biotechnology and AI, which are also developing at an enormous pace.

The position paper contains examples of current developments to illustrate the security-relevant aspects of various scientific endeavours. They show that **scientific actors are caught between the poles of academic freedom and security. The balance between these two poles needs to be renegotiated**. The position paper develops guidelines, strategies and structures for dealing with this.

A.I CRISIS OF THE LIBERAL AND RULES-BASED POST-WAR ORDER

After the end of the Cold War, the Western world was dominated by the expectation that other autocratically governed countries would also embark on the path towards democratic communities with a market economy. Scientific cooperation was supposed to support the process of opening up and ultimately promote the development towards liberal democracies. However, this expectation proved to be a **misjudgement**. Today, open societies see themselves challenged to review their fundamental paradigm that the **Western democratic model** will **prevail in the medium or long term**. [3]

Instead, we are currently seeing an **erosion of the liberal and rules-based world order**, combined with a **strengthening of autocratic forces** in various countries. [4] The liberal post-war order and the United Nations system are in a deep

[2] As early as 2008, China stated in the Law of the People's Republic of China on Progress of Science and Technology (§ 6) that technologies should be used for both military and civilian purposes. Research should also be conducted accordingly, cf. the State Council. The People's Republic of China (PRC) (2014): Law of the People's Republic of China on Progress of Science and Technology, https://perma.cc/72DS-9ERQ. The National Intelligence Law of 2017 makes state control clear, cf. China Law Translate (2017): PRC National Intelligence Law; https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/.

[3] The dominant expectation after the fall of the Berlin Wall was that even autocratically governed countries "were all on an inevitable path towards democracy and a free market economy. [...] One way to speed up that process of opening was through cooperation between universities, think tanks, foundations, and civil society organisations (CSOs) in the West and their counterparts in authoritarian contexts like China, the Middle East or the countries of the former Soviet Union. The assumption was that such cooperation would strengthen like-minded actors in these settings [...] "democratic change through engagement" was the basic theory of change underpinning these efforts." Baykal, A.; Benner, T. (2020): Risky Business: Rethinking Research Cooperation and Exchange with Non-Democracies. Strategies for Foundations, Universities, Civil Society Organisations, and Think Tanks; Berlin, p. 4, https://gppi.net/2020/10/22/rethinking-research-cooperation-and-exchange-with-non-democracies.

[4] There is talk of a "wave of autocratization", cf. Nord, M.; Lundstedt, M.; Altmann, D. et al. (2024): Democracy Report 2024: Democracy Winning and Losing at the Ballot; Gothenburg, p. 6, https://www.v-

crisis. These developments are progressing at a rapid pace. Open societies have many strengths – also with regard to their resilience in the event of a crisis. However, their system of research and higher education, which is based on academic freedom, is exposed to possible attacks in several dimensions: at the level of knowledge itself in terms of accessibility and quality, at the level of scientists as individuals, at the level of the system's ability to function and at the level of its role and anchoring in society. These different dimensions are subsequently summarised under the term vulnerability. Furthermore, the **efforts** of recent decades towards international scientific dialogue and **global cooperation across system boundaries have significantly increased the vulnerability**. Cooperations and personal relationships that have developed over a long period of time can hinder or even prevent scientists from recognising the changed situation and the changes that have become necessary as a result.

Conversely, society is exposed to dangers and risks in view of the latest technologies that cannot be overcome without recourse to scientific knowledge. **Developments in the digital space** as a "new, hybrid sphere of influence", in which the "boundaries between economically and politically motivated cyber aggression are blurred" [5] are particularly explosive here. This space is not only threatened by criminal offences with financial interests (Cyber Crime), but also by state-led attacks with an ideological, political or military background (Cyber Conflict) as well as by large technology companies via digital products that give manufacturers access to information and functions (Cyber Dominance). [6]

One example of this are AI methods for detecting and eliminating software vulnerabilities in the operating systems of Wi-Fi routers, smartphones and laptops. A research project has made it possible to develop automatic defence measures, but also to identify and exploit vulnerabilities in numerous devices that are not subject to regular checks and updates. For example, the "WannaLaugh" software package – as a counter-design to the malicious "WannaCry" – was developed to carry out and analyse ransomware attacks without causing any actual damage or spreading malicious software. However, this tool itself can also become a target and be misused like any other software. For example, the supposed malicious code could exploit vulnerabilities in

dem.net/documents/43/v-dem_dr2024_lowres.pdf. Such a trend of the dismantling and erosion of democratic rights and institutions can be seen worldwide on the basis of certain indicators. For example, 38 % of the world's population - 3.1 billion people - now live in autocracies, in contrast to the 1980s and 1990s, when less than 5 % lived in such regimes. Cf. Nord, M.; David Altman, F.; Angiolillo, et al. (2025): Democracy Report 2025: 25 Years of Autocratisation - Democracy Trumped?; Gothenburg, p. 20, https://www.v-dem.net/publications/democracy-reports. Cf. also Ikenberry, G. (2018): The end of liberal international order?, in: International Affairs, 94 (1), pp. 7-23, https://doi.org/10.1093/ia/iix241.

[5] [unofficial translation] Plattner, C. (2025): Cyberaggression: Hybride Bedrohungen des 21. Jahrhunderts und wie wir uns vor ihnen schützen, https://de.linkedin.com/pulse/cyberaggression-hybride-bedrohungen-des-21-und-wie-wir-plattner-yu2ue.

[6] Ibid.

WannaLaugh and carry out malicious actions so that it could ultimately be used for ransomware attacks. [7]

A.II ACADEMIC FREEDOM AS AN ESSENTIAL ELEMENT OF OPEN SOCIETIES

Academic freedom is enshrined in international law [8] and is a core value in many democratic countries, even though the degree of academic freedom has worsened alarmingly in many places globally and regionally in recent years. Developments such as wars and armed conflicts can destroy entire university systems; researchers can be dismissed from the academic system or even arrested because of their work or political views. Such developments destroy the conditions for free science. The design of curricula in countries such as Russia, Nicaragua and China, but also to some extent in the USA, is subject to political intervention. **Academic freedom** has therefore come **under pressure worldwide**. [9]

Germany is one of the few countries in which a very high degree of academic freedom is guaranteed. One reason for this is that **academic freedom is enshrined in the German constitution**. [10] It is one of the few fundamental rights that is not subject to any legal reservation. In Germany, academic freedom can only be restricted for reasons that are derived from the constitution itself, “predominantly from other fundamental rights or from the same fundamental right of other academics”. [11] At an *individual level,* academic freedom is guaranteed to

[7] Cf. also: Joint Committee on the Handling of Security-Relevant Research (GA) of the German Research Foundation (DFG) and the German National Academy of Sciences Leopoldina (2024): Scientific Freedom and Security Interests in Times of Geopolitical Polarisation – Fifth Report of the Joint Committee of DFG and Leopoldina; Berlin, p. 69, https://www.security-relevant-research.org/publication-progressreport2024/. Cf. also Brundage, M.; Avin, S.; Clark, J. et al. (2018): The malicious use of artificial intelligence: forecasting, prevention, and mitigation, p. 25 f., https://doi.org/10.48550/arXiv.1802.07228.

[8] United Nations (UN) General Assembly (1966): International Covenant on Economic, Social and Cultural Rights, Art. 15 para. 3, https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-3&chapter=4&clang=_en.

[9] Cf. the latest edition of The Academic Freedom Index. In its 2025 update, 34 countries and territories were identified “that have experienced a statistically significant and substantially meaningful decline in academic freedom compared to ten years ago, while only eight countries saw an increase in academic freedom” https://academic-freedom-index.net, and cf: Report of the Scholars at Risk Academic Freedom Monitoring Project (2024); New York, https://www.scholarsatrisk.org/resources/free-to-think-2024/.

[10] Art. 5 para. 3 Basic Law (GG): “(3) Art and science, research and teaching are free. Freedom of teaching shall not release from loyalty to the Constitution.” [unofficial translation] Basic Law for the Federal Republic of Germany of 23 May 1949 (BGBl. p. 1), last amended by Article 1 of the Act Amending the Basic Law (Articles 93 and 94) of 20 December 2024 (BGBl. I No. 439): Article 9 para. 3, https://www.bundestag.de/parlament/aufgaben/rechtsgrundlagen/grundgesetz#.

[11] [unofficial translation] Dieter Grimm (2021): Wissenschaftsfreiheit als Funktionsgrundrecht, in: Berlin-Brandenburg Academy of Sciences and Humanities (ed.): Wissenschaftsfreiheit in Deutschland. Drei rechtswissenschaftliche Perspektiven. Reihe Wissenschaftspolitik im Dialog, No. 14/2021, pp. 17-23, here p. 23, https://e-doc.bbaw.de/frontdoor/index/index/searchtype/series/id/13/start/4/rows/20/yearfq/2021/docId/3 445 . So-called constitutional barriers, Federal Constitutional Court, BVerfGE 47, 327 (368 ff), https://www.servat.unibe.ch/tools/DfrInfo?Command=ShowPrintVersion&Name=bv047327; BVerfGE 122, 89 (107), https://www.bverfg.de/e/rs20081028_1bvr046206; BVerfGE 126, 1 (24), https://www.bverfg.de/e/rs20100413_1bvr021607; BVerfGE 141, 143 (169), https://www.bverfg.de/e/ls20160217_1bvl000810.

the individual – regardless of their affiliation to an academic institution. At an *organisational level*, it applies to research institutions [12] and higher education institutions, without being tied to a specific type of organisation of the university. [13] Another specific meaning is relevant for the German constitution, namely the understanding of **academic freedom as a functional fundamental right.** [14] This means that, on a *systemic level*, the state is obliged to ensure "a functioning sphere of independent science", [15] in order to satisfy society's constantly growing need for knowledge and, at the same time, to create a "critical distance to social (and state) interests and claims to power". [16]

If the **state** develops new expectations towards science and humanities for security policy reasons, it remains in its **dual role**, insofar as it should refrain from interfering as a potential threat to academic freedom (*freedom from the state – right of defence*) and at the same time, as the guarantor of freedom, must create the conditions for academic freedom to be realised in the sense of functional right (*freedom by the state – right of guarantee*).

In view of the increasing competition between systems and the associated security-relevant challenges, the WR emphasises that the **balance between academic freedom and justified restrictions** due to constitutionally protected goods, namely other fundamental rights, **must** always **be struck**. For the individual scientist, there is a "duty to consider" [17] only in the sense of weighing up constitutionally enshrined values in individual cases, not in relation to all social consequences. Under constitutional law, this does not rule out the possibility of university management establishing self-reflection processes and risk

[12] For the non-university sector, this means that - despite a decision from Karlsruhe that is not yet available and regardless of the private-law organisation - it is obliged to protect fundamental rights if it is predominantly financed by the state, cf. Dieter Grimm (2021): Wissenschaftsfreiheit als Funktionsgrundrecht, in: Berlin-Brandenburg Academy of Sciences and Humanities (ed.): Wissenschaftsfreiheit in Deutschland. Drei rechtwissenschaftliche Perspektiven. Reihe Wissenschaftspolitik im Dialog, No. 14/2021, pp. 17-23, here pp. 22 f., https://edoc.bbaw.de/frontdoor/index/index/searchtype/series/id/13/start/4/rows/20/yearfq/2021/docId/3445.

[13] As background, it should be noted that the judgement was drafted in the course of the disputes surrounding the so-called group university. It states: "The guarantee of academic freedom is not based on the traditional structural model of the German university, nor does it prescribe a specific organisational form of academic life at higher education institutions." [unofficial translation] BVerfGE 35, 79 (79), https://www.servat.unibe.ch/tools/DfrInfo?Command=ShowPrintVersion&Name=bv035079.

[14] Cf. Dieter Grimm (2021): Wissenschaftsfreiheit als Funktionsgrundrecht, in: Berlin-Brandenburg Academy of Sciences and Humanities (ed.): Wissenschaftsfreiheit in Deutschland. Drei rechtswissenschaftliche Perspektiven. Reihe Wissenschaftspolitik im Dialog, No. 14/2021, pp. 17-23, here p. 21, https://edoc.bbaw.de/frontdoor/index/index/searchtype/series/id/13/start/4/rows/20/yearfq/2021/docId/3445.

[15] [unofficial translation] Britz, G. (2013): Freiheit der Wissenschaft, in: Dreier, H. (ed.): Grundgesetz. Kommentar Band I, Artikel 1-19; Tübingen, pp. 792-838.

[16] [unofficial translation] Hailbronner, K. (1979): Freiheit der Forschung und Lehre als Funktionsgrundrecht; Hamburg, p. 156, cited in Häberle, P. (1986): Besprechungen. Kay Hailbronner: Freiheit der Forschung und Lehre als Funktionsgrundrecht, in: Archiv des öffentlichen Rechts, 111 (1), pp. 165-170, here p. 170, https://www.jstor.org/stable/44308941.

[17] [unofficial translation] BVerfGE 47, 327 (377 f.), https://www.servat.unibe.ch/tools/DfrInfo?Command=ShowPrintVersion&Name=bv047327.

assessments. The WR sees its position paper as a contribution to a renewed balancing of this equilibrium in the face of global security challenges.

B. Concepts and analyses

The **protection and defence** of open democratic societies and increasing their **resilience** to cope with unforeseeable developments have become key challenges. The resilience of a society means the ability not only to react to unexpected crises and shocks, but also to actively adapt and change accordingly in order to maintain and further develop its own ability to act and function. While protection, defence and prevention aim to prevent foreseeable negative developments, resilient societies also prepare themselves to "expect the unexpected". |[18]

In the **business sector**, aspects such as **economic strength**, **technological sovereignty and knowledge protection** play an important role. This is because espionage and sabotage as well as data theft cause high economic damage of more than 250 billion euros annually in Germany alone, around two thirds of which is due to cyberattacks. |[19] Knowledge-intensive companies have therefore long been protecting themselves against knowledge leakage, external influence and other risks. However, state objectives such as technological sovereignty and economic independence generally do not permit any restrictions on academic freedom within the legal framework of the German Basic Law. These issues are therefore only addressed marginally here.

| [18] [unofficial translation] Ulrich Bröckling has referred to the concept of resilience as a key concept of our time, cf. Bröckling, U. (2017): Resilience. Über einen Schlüsselbegriff des 21. Jahrhunderts, in: Soziopolis - Gesellschaft beobachten, here p. 3, https://www.ssoar.info/ssoar/handle/document/80731. For a reconstruction of the history of the term "resilience" up to the current political discourse cf. also Szöllösi-Janze, M. (2024): Resilienz. Zur Geschichte eines allgegenwärtigen Begriffs – Thesen zu den Herausforderungen einer modernen Zeitgeschichte, in: Vierteljahrshefte für Zeitgeschichte, 72 (3), pp. 559-589, https://doi.org/10.1515/vfzg-2024-0030.

| [19] Cf. Finsterbusch, S.; Sachse, M.: Hackergreifen aus China deutsche Unternehmen an, in: FAZ, 28 August 2024, https://www.faz.net/aktuell/wirtschaft/mehr-wirtschaft/china-warum-hacker-gerade-von-dort-aus-deutsche-unternehmen-angreifen-19947534.html. The article is based on findings from Bitkom e. V., cf. Bitkom e. V. (2024): Wirtschaftsschutz 2024; Berlin, https://www.bitkom.org/sites/main/files/2024-08/240828-bitkom-charts-wirtschaftsschutz-cybercrime.pdf. The scientific system is also affected by cyberattacks: In the years 2022 to 2024, the Federal Criminal Police Office (as of 19 June 2024) became aware of 42 cyberattacks on higher education institutions and scientific institutions, some of which resulted in high financial losses, cf. German Federal Government (Drucksache 20/12259,10.07.2024): German Bundestag (2024). Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion CDU/CSU – Drucksache 20/11830 – Cyberangriffe auf Wissenschaft und Forschung in Deutschland, p. 3 f., https://dip.bundestag.de/vorgang/cyberangriffe-auf-wissenschaft-und-forschung-in-deutschland/313002. "The damage identified ranges from university website outages to temporary disruptions of IT-supported services and higher education offerings, the leaking of data, large-scale encryption of IT servers and longer-term outages." [unofficial translation] Ibid, p. 8.

The challenges of knowledge security and the security relevance of research require changes to the practice and governance of the academic system as well as the self-conception of teachers and researchers in particular, but also of students. These adjustments are of great urgency, as the **system of research and higher education** is **particularly vulnerable because**, as an **open system** in democracies, it is a coveted and often easily accessible target for undesirable knowledge transfer or influence. At the same time, research activities make a significant contribution to protecting society from external and internal attacks and strengthening its resilience.

Against this background, the following section is based on an **expanded security concept and a broad understanding of security relevance in science and humanities**. In a first step, the terms security, security-relevant research and knowledge security are described in more detail in order to develop recommendations based on this clarification and the associated analysis.

B.I SECURITY

In the modern age, it is seen as a central **task of the state to guarantee the security** of people, their livelihoods, their goods and also the central political values. |[20] However, what exactly is meant by security is constantly being renegotiated in societies and is also dependent on subjective perceptions. |[21] A clear change can be observed in the last decade. At the beginning of the 21st century, vulnerabilities caused by natural disasters and terrorist attacks, for example, still took centre stage. Ensuring security was aimed at reliably functioning infrastructures in a globally networked society: from supply chains to communication systems. With Russia's war of aggression against Ukraine in particular, issues of external security, i. e. the protection of life and liberty in the face of armed conflicts or threats, are once again taking centre stage in Germany. At the same time, this aspect of security is itself being delimited by the concept of hybrid warfare, which also recognises non-military forms of the use of violence as a means of pursuing conflicts between states. In the Federal Government's 2023 Security Strategy, **security is understood comprehensively and integratively** as "protection from war and violence, as the freedom to live within the

| [20] Since the 17th century, the "positive idea of security" has developed as a desirable state of the community, which "the modern state claims to guarantee or is required to guarantee. It is no longer this or that good, this or that transport route, or the life of this or that person that is to be protected from certain dangers, but rather the rule is to protect the entire territory to which it extends." [unofficial translation] Kaufmann, F.-X. (2015): Sozialstaat als Kultur; Bonn, p. 280, https://doi.org/10.1007/978-3-531-94244-5_11.

| [21] "Security in political-social contexts cannot be defined abstractly [...], but is constantly redefined in societies and by societies as a horizon for orientation and action, not least through the identification of insecurity, threats or dangers. Security, or insecurity, is socially and culturally variable and thus also variable in the historical process." [unofficial translation] Conze, E. (2023): Sicherheit. Wert, Fiktion und Versprechen, in: Saam, N. J.; Heiner, B. (eds.): Die Idee der Freiheit und ihre Semantiken. Zum Spannungsverhältnis von Freiheit und Sicherheit; Bielefeld, pp. 51-68, here p. 55, https://doi.org/10.1515/9783839461884-004.

framework of our free democratic order, and as safeguarding the very resources on which our lives depend." [22]

In view of the rapidly changing global political situation, its already visible consequences for the social threat situation and technological developments, democratically elected governments are currently under increased pressure to ensure the security of their citizens. Today, the state must increasingly involve other social actors in order to fulfil this task. **All areas of society** must **deal with this challenge**, including the system of research and higher education. Moreover, such a task can only be accomplished if harmonisation, coordination and networking within and across the various political, economic and social sectors are significantly improved. These harmonisation, coordination and networking processes must take place at the European level.

The defence objective is the **preservation of the free and democratic basic order of our community** – including its prerequisites. External threats are not the only relevant factor in the defence of this objective. External defence is linked to protection and the development of internal resilience. This is because resilience is aimed at a society's ability to deal flexibly with the complex effects of unforeseeable crises or shocks – including all their feared damage – and to transform these experiences into innovations. Resilient societies are expected to be better equipped for an unpredictable and uncertain future.

The **system of research and higher education** is a part of society that must be integrated into coordination, harmonisation and networking processes to ensure security. Science and humanities play **a special role** here **in several respects**. Firstly, they drive a large number of developments that can both jeopardise security and contribute to creating security and resilience both internally and externally. For example, IT research can both contribute to attacks on critical infrastructures (keyword: cyber wars [23]) and, conversely, increase their protection. In addition, science and humanities – especially against the background of academic freedom as a fundamental functional right (cf. A.II) – are assigned the role of a critical authority vis-à-vis state and economic actors with their respective (power) interests. Furthermore, scientific discourse opens up a deliberative space in which knowledge and action strategies for overcoming acute crises such as pandemics or ongoing challenges such as demographic change can be developed across disciplines – regardless of political interests and conflicts. In such a space, the complexity of unforeseen developments, for example in the course of acute or ongoing crises, can be adequately recognised and reflected

[22] Federal Foreign Office (2023): Robust. Resilient. Sustainable. Integrated Security for Germany: National Security Strategy; Berlin, p. 19, https://www.nationalesicherheitsstrategie.de/en.html.

[23] Cf. Wörner, J.-D.; Schmidt, Christoph M. (eds.) (2022): Security, Resilience and Sustainability (acatech IMPULSE), published by acatech – National Academy of Science and Engineering; Munich, p. 7, https://doi.org/10.48669/aca_2022-2.

upon. In this way, scientific discourse becomes an element of resilience in order to be able to react innovatively to the unforeseen.

It is becoming increasingly clear that the system of research and higher education, whose relevance to security policy was previously limited to specific areas defined in export control law and to targeted research for military purposes, **has** now **become a central security-relevant part of society**. On the one hand, the work of its actors makes a significant contribution to ensuring security and resilience, which should be promoted more strongly as intended (cf. C.IV). On the other hand, it is increasingly a target for attacks by states and other actors, including non-state actors such as terrorist groups and criminal organisations, who want to profit from scientific and technological achievements dishonestly in a military manner or prevent progress.

B.II SECURITY-RELEVANT RESEARCH

With the development of the concept of security towards a comprehensive understanding that integrates different areas, the concept of **security-relevant research** has also changed. Research is relevant to security insofar as it contributes and should contribute to **the maintenance of internal and external security as well as to the development of resilience and the protection of the natural living conditions of the community** or can jeopardise these. Consequently, these are not only acitivities that serve to maintain external (military) defence capabilities. Rather, also include scientific activities that aim to “identify and analyse vulnerabilities and develop proposals or technologies to reduce or avoid the risks without interfering with the freedom or rights of citizens”. |[24]

In view of the political, social, scientific and technological dynamics, **it is almost impossible to draw a clear line** between scientific activities that are relevant to security and those which have no connection to questions of security and resilience. It is **a continuum** that can be observed **in almost all disciplines and research areas** – including the legal sciences, humanities and social sciences, as the following example illustrates.

A study investigates how young people consume extremist (Islamist) material on the internet and whether there is a link to radicalisation. The latter could be proven. It was found that it is not the depiction of violence that is relevant, but the intensity with which it is addressed. For example, video footage of beheadings is often viewed by young people. However, the potential for radicalisation is low. In contrast, only a few people visit online magazines of the

| [24] [unofficial translation] Klaus, T.; Drees, B.; Leismann, T. (2009): Zukunftstechnologien in der Sicherheitsforschung, in: Winzer, P.; Schnieder, E.; Bach, F.-W. (eds.): Sicherheitsforschung – Chancen und Perspektiven (acatech DISKUSSION); Berlin/Heidelberg, pp. 13-38, here p. 13, https://www.acatech.de/publikation/sicherheitsforschung-chancen-und-perspektiven/.

so-called Islamic State or Al-Qaeda – albeit with a greater cognitive effect. De-radicalisation strategies can be developed on the basis of these findings. At the same time, however, they can help extremist and terrorist groups to improve their recruitment strategies. Studies of this kind can therefore both map out paths to de-radicalisation and provide a recruitment aid for terrorist groups. [25]

Basic research-orientated activities are also affected, even if they were not considered security-relevant for a long time due to the provisions of foreign trade law. Essentially, the focus was on research and development work that was conducted at a higher Technology Readiness Level (TRL) [26] than 3. However, protective measures for basic research were already in place in the 1950s if there was a potential for misuse. For example, the first civil clause [27] was included in the founding treaty of the Karlsruhe Nuclear Research Centre in 1956 at the instigation of the Allies in order to ensure the demilitarisation of basic nuclear research in Germany. In view of the acceleration in research and development processes, a mere reference to basic research in other fields is often no longer sufficient to classify research activities as non-security-relevant. In the field of IT, for example, research and development work are so closely interlinked until they are ready for the market that innovations are already being incorporated into products within a few months, even if they cannot yet be used by everyone. The tension between wanting to guarantee freedom and responsibility in equal measure, as described at the beginning, becomes particularly clear at this point.

The **concept of dual-use technologies** and the demand for dual-use policies originally emerged in the 1970s in the wake of the realisation that limiting the uncontrolled proliferation of military technologies in the field of nuclear, chemical or biological weapons and the associated carrier technologies was in tension with the civilian use of such technologies. [28] As a result, the economic utilisation of military technologies through civilian applications was increasingly taken into consideration, also as a justification for high military research and development expenditure.

[25] Cf. GA of the DFG and Leopoldina (2024): Scientific Freedom and Security Interests in Times of Geopolitical Polarisation - Fifth Report of the Joint Committee of DFG and Leopoldina; Berlin, p. 67, https://www.security-relevant-research.org/publication-progressreport2024/. Cf. also Frissen, T. (2021): Internet, the great radicaliser? Exploring relationships between seeking for online extremist materials and cognitive radicalisation in young adults, in: Computers in Human Behavior, 114, article 106549, https://doi.org/10.1016/j.chb.2020.106549.

[26] Technology Readiness Level (TRL) "is a term that was originally coined in the aerospace industry (for software: Software Technology Readiness Level). It is a scale for assessing the development status of new technologies on the basis of a systematic analysis." [unofficial translation] Federal Office for Economic Affairs and Export Control (BAFA) (2024): Immaterieller Technologietransfer (ITT); Eschborn, https://www.bafa.de/SharedDocs/Downloads/DE/Aussenwirtschaft/afk_merkblatt_itt.html , p. 18.

[27] In German the so-called Zivilklausel.

[28] Cf. Molas-Gallart, J. (1997): Which way to go? Defence technology and the diversity of 'dual-use' technology transfer, in: Research policy, 26 (3), pp. 367-385, https://doi.org/10.1016/S0048-7333(97)00023-1.

In the last three decades, the term “**dual use**” has developed a **meaning that goes beyond the distinction between military and civilian research**. |[29] The meaning has expanded, particularly against the backdrop of virological gain-of-function research (GoF) |[30] in the life sciences. In addition to military use, moral concerns and other risks, such as escape from a laboratory, also play a role here, as the following case study illustrates:

> A study has identified five genetic changes that allow H5N1 influenza viruses, which are highly pathogenic to birds, to be transmitted between mammals via the air. These findings can help to better predict how such viruses could gradually develop into a threat to humans. This will make it possible to better assess the pandemic potential of pathogenic virus variants that regularly emerge in nature, gain insights for the early interruption of infection chains and, if necessary, develop targeted vaccines. There are risks associated with such GoF experiments on bird flu viruses, both in terms of unintentional pandemic outbreaks due to negligent behaviour in the laboratory, resulting in the viruses being released into the environment, and in terms of their misuse for the development of new biological weapons. |[31]

It is now assumed that **almost all fields of research** have a **potential dual-use character**. In particular, the rapid development of AI, which is penetrating more and more fields of research, has contributed to this. Since the EU regulation (AI Act) of 2024, this has not only raised ethical questions, but also legal ones. |[32] In view of the wide range of possible applications and the multiple potential for misuse of research activities, there is talk of the **multiple use character** of research – over and above military applications.

In addition to the expansion into more and more disciplines and fields of research, there is also a progressive **convergence of different disciplines**. This applies above all, but not only, to the penetration of research with information and AI technologies, which can be observed in almost all disciplines. |[33] Other

|[29] Cf. Oltmann, S. (2015): Dual Use Research: Investigation Across Multiple Science Disciplines, in: Science and Engineering Ethics, 21, pp. 327-341, here p. 328, https://doi.org/10.1007/s11948-014-9535-y.

|[30] Virological gain-of-function (GoF) research refers to research that aims to increase the transmissibility and virulence of pathogens. This research was not clearly addressed in the Geneva Protocol (1925) and the Biological Weapons Convention (BWC of 1975) because viruses do not have all the characteristics of life. Today, GoF research is used for vaccine development, for example.

|[31] Cf. GA of the DFG and Leopoldina (2024): Scientific Freedom and Security Interests in Times of Geopolitical Polarisation - Fifth Report of the Joint Committee of DFG and Leopoldina; Berlin, p. 70, https://www.security-relevant-research.org/publication-progressreport2024/. Cf. also Herfst, S.; Linster, M.; Chutinimitkul, S. et al. (2012): Airborne transmission of influenza A/H5N1 virus between ferrets, in: Science, 336 (6088), pp. 1534-1541, https://doi.org/10.1126/science.1213362, and Imai M.; Watanabe, T.; Hatta, M. et al. (2012): Experimental adaptation of an influenza H5 HA confers respiratory droplet transmission to a reassortant H5 HA/H1N1 virus in ferrets, in: Nature, 486 (7403), pp. 420-428, https://doi.org/10.1038/nature10831.

|[32] Cf. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.

|[33] Cf. Oltmann, S. (2015): Dual Use Research: Investigation Across Multiple Science Disciplines, in: Science and Engineering Ethics, 21, pp. 327-341, here p. 331, https://doi.org/10.1007/s11948-014-9535-y.

areas of research such as nanotechnology should also be mentioned here. [34] Both developments, the expansion of research fields with potential for misuse and the convergence of different disciplines, mean that it can be assumed that **a significant proportion of scientific work has an inherent dual-use character**.

This analysis could lead us to abandon **the dual-use concept**. However, it remains helpful in certain contexts, such as for regulating export control. Here, an *object-related perspective* can be helpful, which, as in the EU Dual-Use Regulation amended in 2021, [35] emphasises that dual-use goods also include "software and technology, which can be used **for both civilian and military purposes**". [36] The dual-use term here refers to the possible use in a military or civilian context. In addition, the term also refers to the actual intention of the user who, for example, utilises research results. This *intentional perspective* links the dual-use character to the actor's intention behind the utilisation of scientific research results. [37] However, the intentions of the actors are often not obvious, but remain implicit and opaque. Therefore, there is a high degree of uncertainty when try-

[34] Nanotechnology encompasses aspects of physics, chemistry, biology etc. and blurs the boundaries between biomedical and electrical engineering, cf. ibid., here p. 329 f. Cf. also Hähnel, M. (2024): Conceptualising dual use: A multidimensional approach, in: Research Ethics, 0 (0), here p. 2, https://doi.org/10.1177/17470161241261466.

[35] Cf. BAFA (2021): Die neue EU-Dual-Use-Verordnung (Veordnung (EU) 2021/821), https://www.bafa.de/SharedDocs/Downloads/DE/Aussenwirtschaft/afk_merkblatt_eu-dual-use-vo.html.

[36] European Union (EU) (2021): Commission Recommendation (EU) 2021/1700 of 15 September 2021 on internal compliance programmes for the control of research involving dual-use items under Regulation (EU) 2021/821 of the European Parliament and of the Council setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items, p. 5, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021H1700. The EU also includes goods "which can be used for the design, development, production or use of nuclear, chemical or biological weapons or their means of delivery, including all items which can be used for both non-explosive uses and assisting in any way in the manufacture of nuclear weapons or other nuclear explosive devices." Ibid., p. 5. The Commission of Experts for Research and Innovation (EFI) has also used the term in this sense: "Dual-use goods are goods, software and technology that are normally used for civilian purposes but can also be used in the military sector." [unofficial translation] EFI (2025): Gutachten zu Forschung, Innovation und technologischer Leistungsfähigkeit Deutschlands 2025; Berlin, p. 127, https://www.e-fi.de/publikationen/gutachten. (An executive summary of the report can be found here: https://www.e-fi.de/fileadmin/Assets/Gutachten/2025/EFI_Summary_2025_17.pdf.) Similarly, the German Academic Exchange Service (DAAD): "Dual-use refers to the fundamental usability of technologies or goods for both civilian and military purposes. This includes not only material goods, but also intangible goods such as information, data and knowledge of various kinds, the transfer of which is subject to legal regulations." [unofficial translation] https://www.daad.de/de/infos-services-fuer-hochschulen/kompetenzzentrum/kiwi-themen/risiko-und-sicherheit/dual-use/. Explicit reference is made to legal regulations.

[37] The DFG and Leopoldina GA argues along these lines, for example, which defines "security-relevant research of concern as scientific work" that can be misused "to cause significant harm to human dignity, life, health, freedom, property, the environment or peaceful coexistence". GA of the DFG and Leopoldina (2024): The Handling of Security-Relavant Research in Germany – An Overwiew; Berlin, p. 3, https://www.security-relevant-research.org/publication-informationbrochure2025/. Cf. also GA of the DFG and Leopoldina (2022): Scientific Freedom and Scientific Responsibility - Recommendations for Handling of Security-Relevant Research; Berlin, p. 34, https://www.security-relevant-research.org/publication-scientificfreedom2022/. The GA further explains that "[i]n the research context [...] [this] usually refers to those research results and methods that can be used both for peaceful or beneficial purposes and for deliberately harming or suppressing society or the environment." https://www.security-relevant-research.org/faq-eng/.

ing to determine the dual-use character of goods and technologies solely in relation to the intentional use of research and development results. Increasingly, collective actors such as terrorist groups, organised criminal gangs or supranational organisations are also using such goods and technologies. This **expansion of actors and types of actors** has been observed in recent years and decades.

Only a **multi-perspective view** of the dual-use concept makes it possible to recognise the different potentials of research activities and technologies as well as to assess them appropriately in the context of the subject matter and the actors' intentions and constellations. A clear distinction between security-relevant and non-security-relevant research is neither possible against the background of the expanded concept of security nor with regard to the dual-use character of scientific work. In order to counter this situation, a new form of governance is needed in dealing with security-relevant research and knowledge security in the system of research and higher education.

B.III KNOWLEDGE SECURITY

Global political tensions and the inherent dual-use nature of research and technology work have led to the development of a **new cross-cutting policy area**: **Knowledge Security** (knowledge and research security). It has become established in various countries in recent years – alongside economic security. Countries such as Australia, Canada, the USA, but also the UK and the Netherlands have been addressing this challenge for some time.

Various terms are used here: from "research security" [38] to the term "trusted research and innovation", [39] which was primarily chosen in the UK for historical reasons. In the context of its position paper, the WR speaks of **knowledge security**, as this term encompasses not only research activities, but all scientific activities including the exchange of staff and students. Knowledge security as a **value** aims to protect specific national interests and values as well as to continue to protect the core of scientific work, namely to be able to work and cooperate internationally under conditions of guaranteed academic freedom. Knowledge security encompasses several dimensions that relate to **different risks**:

[38] Cf. the European Commission's recommendation paper "Enhancing Research Security" adopted in May 2024: "'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." Council of the European Union (2024): Council Recommendations of 23 May 2024 on enhancing research security (C/2024/3510); Brussels, p. 4, http://data.europa.eu/eli/C/2024/3510/oj .

[39] Cf. https://www.ukri.org/manage-your-award/good-research-resource-hub/trusted-research-and-innovation/.

1 – **Undesirable knowledge transfer**: This refers to the undesirable outflow or transfer of knowledge, including technologies, for various reasons. This can be problematic for military or, in the narrower sense, security policy reasons as well as for economic or technological reasons. While precautions have always been in place against the outflow of knowledge for military reasons, the focus is now shifting to countering undesireable knowledge transfer in order to strengthen the respective economic power and promote one's own technological sovereignty. There is talk of a "non-professionalisation" of espionage, by which is meant that visiting academics or students are commissioned to conduct research during their stay at foreign universities or research institutions. [40] In other words, it is not the personal interest but the interest of the respective commissioning party that is decisive for the undesirable knowledge transfer. In addition, visiting academics may be pressurised or forced to share knowledge with government agencies after their return, even without a prior commission.

Undesirable knowledge and data transfer is not tied to individuals, but can also occur technically through cyberattacks or via commercial service providers (e. g. cloud or sequencing services) and be supported by data tracking. [41] The use of digital services leaves traces so that the providers have access to all stages of the research life cycle, from literature searches to structured research information, using appropriate analysis tools.

2 – **Unwanted influence**, which can relate to research and teaching itself as well as to individuals and their role in society. It ranges from the conscious or unconscious adoption and dissemination of certain opinions to the restriction of publication activities and up to self-censorship in scientific work, undermining trust in scientific work and the good scientific practice associated with it.

One example reports from Chinese students who record lectures at their host universities and report them to the authorities, for example when lecturers teach content that is "undesirable" from China's point of view (e. g. referring to Taiwan as an independent country). [42] Conversely, there are indications

[40] Cf. the assessment of the German domestic intelligence services (BfV) "Chinas neue Wege der Spionag https://www.verfassungsschutz.de/SharedDocs/hintergruende/DE/wirtschafts-wissenschaftsschutz/chinas-neue-wege-der-spionage.html.

[41] In 2021, the DFG pointed out the implications of data tracking in terms of analysing usage traces in science, cf. DFG Committee on Scientific Library Services and Information Systems (2021): Data tracking in research: aggregation and use or sale of usage data by academic publishers. A briefing paperof the Committee on Scientific Library Services and Information Systems of the German Research Foundation; Bonn, https://doi.org/10.5281/zenodo.5937995.

[42] Cf. Amnesty International (2024): Roundtable on Transnational Repression in the UK: lived experience and recommendations from Hong Kong diaspora community groups. A Summary Report, https://www.amnesty.org.uk/resources/roundtable-transnational-repression-uk-lived-experience-and-recommendations-hong-kong. Cf. also German Federal Government (Drucksache 20/14938, 10.02.2025): Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Peter Heidt, Gyde Jensen, Michael Georg Link (Heilbronn) und der Fraktion der FDP – Drucksache 20/14592 – Transnationale Repressionen durch die Regierung der Volksrepublik China in Deutschland, https://dip.bundestag.de/vorgang/transnationale-repressionen-durch-die-regierung-der-volksrepublik-china-in-deutschland/319579?f.wahlperiode=20&f.herausgeber_dokumentart=Bundestag-Drucksache&rows=25&pos=21&ctx=a.

that the People's Republic of China is exerting influence on academic institutions in the context of Confucius Institutes, which are also linked to higher education institutions in various ways. For example, there have been cancellations of virtual readings or attempts to prevent the tour of the documentary "In the name of Confucius" about the growing global controversy surrounding the work of the Confucius Institutes. This has led to press reports and further political activities and observations by the German domestic intelligence services (BfV). [43]

Here, too, influence is not only exerted by human actors. There is currently a particularly high degree of dependence on IT infrastructures provided by market-determining oligopolies. They control access, usability and transparency. This not only allows data to flow uncontrollably, but also the possibility of targeted manipulation. We are talking about the "tech cold war". [44] This aspect is becoming even more explosive, particularly in the course of the centralisation of AI development under the umbrella of large technology companies, insofar as they can have control not only over the underlying software, but also over the data sets used for training purposes. [45]

3 – **Financial and academic dependencies** that arise when partners deliberately conceal their own cooperation interests and want to promote cooperation or staff exchanges through financial incentives. Dependencies can also affect German institutions indirectly when cooperating with countries whose academic systems are dependent on foreign investors or tuition fees from foreign students for their funding – including the provision of study programmes.

However, there are also dependencies with regard to research and data infrastructures that are financed or provided by other countries. It is undisputed that

[43] The former concerned the book Aust, S.; Geiges, A. (2023): Xi Jinping. Der mächtigste Mann der Welt, 2nd ed.; Munich, cf. https://www.spiegel.de/panorama/bildung/chinas-einfluss-auf-deutsche-universitaeten-der-lange-arm-pekings-a-f6567e46-508f-4d64-a830-3816296dad79. A more detailed description is not possible for reasons of confidentiality. Cf. also German Federal Government (20.04.2022): Deutscher Bundestag 20. Wahlperiode. Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion der CDU/CSU – Drucksache 20/1275 – Stand des Ausbaus der Asien- und China-Kompetenz im Wissenschaftssystem und Aktivitäten der Konfuzius-Institute in Deutschland, in particular p. 5, https://dip.bundestag.de/vorgang/stand-des-ausbaus-der-asien-und-china-kompetenz-im-wissenschaftssystem-und/286049?f.deskriptor=Technology transfer&rows=25&pos=16&ctx=a.

[44] Baums, A.; Butts, N. (2025): Tech Cold War. The Geopolitics of Technology; Boulder, https://doi.org/10.1515/9781962551571.

[45] Cf. the Royal Society's assessment: "Centralisation of AI development under large technology firms (eg 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." The Royal Society (2024): Science in the age of AI: How artificial intelligence is changing the nature and method of scientific research; London, p. 72, https://royalsociety.org/news-resources/projects/science-in-the-age-of-ai/.

the importance of these infrastructures in all scientific fields has increased significantly in recent years. [46] If countries or even commercial enterprises, especially oligopolies, are in the position to put pressure on actors in the science system due to one-sided dependencies, the vulnerability of the system of research and higher education increases considerably. As early as 2023, the WR recommended reducing dependencies and increasing its own scope for action. [47]

The Argo programme, [48] which has been collecting oceanographic data from the depths of the oceans since the early 2000s using free-drifting measuring buoys (known as Argo floats, of which around 4,000 are currently in operation) and transmitting it to data centres in the USA and France via satellites, is an example of scientific dependencies and uncertainties, even with regard to partners that have been classified as unbreakable to date. [49]

Germany is also participating in this programme with currently less than 7 % of the Argo floats, which are primarily deployed in the Atlantic. Overall, the USA provides more than half of all buoys (56 %, as of May 2025). This dependency poses major risks for modelling in climate research and current forecasting services, [50] if access to the data is no longer guaranteed or the current network density is not maintained.

4 – **Interference of scientific activities with other areas of society**, so that scientific exchange and cooperation with a critical country [51] has an impact on other political and/or economic relations with this or other countries. For example, the existence of a scientific relationship can be used to gain political reputation. In the course of the erosion of a rules-based order, such a transactional approach seems to be gaining increasing acceptance in international relations, leading to "deals" across the boundaries of different social areas and thus also political fields. [52] The orientation is towards national interests and less towards overarching principles or values, so that short-term results and benefits are guiding actions instead of long-term strategic or value-based partnerships. Scientific

[46] The background to this increase in importance is that it is no longer possible to draw a clear line between research activities and infrastructures, cf. e. g. Gehring, P. (2018): Viele Fronten. Forschungsdatenmanagement als Ermöglichungspolitik, in: Forschung & Lehre, 25. Jg., 9/18, pp. 754-756, https://www.forschung-und-lehre.de/heftarchiv/ausgabe-9/18; and Barlösius, E. (2019): Infrastrukturen als soziale Ordnungsdienste. Ein Beitrag zur Gesellschaftsdiagnose, Frankfurt a. M./New York, esp. p. 157 ff.

[47] Cf. WR (2023): Empfehlungen zur Soveränität und Sicherheit im digitalen Raum; Cologne, https://doi.org/10.57674/m6pk-dt95.

[48] Cf. https://www.bsh.de/EN/TOPICS/Monitoring_systems/Argo_floats/argo_floats_node.html.

[49] Cf. https://www.aoml.noaa.gov/two-decades-argo-program/.

[50] Cf. https://globalocean.noaa.gov/research/argo-program/, https://argo.ucsd.edu.

[51] Cf. the task of the National Platform for categorising a country as critical (see footnote 70 and C.III.3).

[52] For a classification of the transactional approach in the context of the reference to a rules-based international order perceived by countries of the Global South as "Western double standards", cf. Eisentraut, S. (2025): Westliche Doppelstandards: Prinzipien unter Beschuss, in: Internationale Politik 1/2025, pp. 76-81, https://internationalepolitik.de/de/westliche-doppelstandards-prinzipien-unter-beschuss.

relationships can be used in a targeted manner to "offset" them against political or economic interests – even if only on a symbolic level. This is particularly critical because the effects in non-academic areas are not always recognisable to the individual scientist.

5 – **Violation of research ethics or ethical principles**, calling the integrity of scientific work into question (e. g. suppression of unwanted data) or violating ethical values (e. g. by relocating experiments to countries with a lower level of legal protection, the use of scientific technologies for surveillance purposes in autocratic states or the misuse of human sources for data collection).

Source protection is an example of an increasingly important ethical challenge when it comes to research projects in regions of the world from which people migrate to Europe legally or illegally. Not only migration issues are addressed here, but also questions of political dynamics in the region or other sensitive framework conditions. This means that confidential information or positions can be transmitted via the circle of people discussing this research together and be used for political purposes. Anonymising sources is both essential and difficult – especially in the case of well-known places and institutions that may be reported on in the media.

The WR **bases** its further analyses and recommendations **on the comprehensive concept of knowledge risks and knowledge security** developed here. It advocates not only addressing research risks in the science policy discourse, but also speaking of knowledge risks in terms of the five types of risk explicated. In a dynamic field such as this, which interacts closely with global political developments, it is possible that further risk types will emerge. This is not yet foreseeable.

B.IV LAW AND VOLUNTARY COMMITMENT

The handling of security-relevant topics is partially regulated in German science. The export control system (cf. B.IV.1) is of central importance for the handling of some security-relevant research. In addition, civil clauses can play a role, although these are usually voluntary commitments by higher education institutions and research organisations that are not legally binding (cf. B.IV.2).

IV.1 Export control

In the post-war period, both the Western and Eastern powers focused a significant part of their research on military innovations – usually in independent organisations or organisational units under appropriate security precautions. In the western world, a **system of export control**, to which scientific institutions are also subject, has been developed as a protection. Export control systems such as the Coordinating Committee on Multilateral Export Controls (COCOM) were established to prevent the Soviet Union in particular from gaining access to advanced technologies. Whereas in the past military technologies were often also used for civilian systems in a suitably minimised form, military research is now based on civilian work, as a significantly higher speed of innovation can be observed here. Against this background, export control mechanisms have evolved. The **Wassenaar Arrangement of 1995, to which the post-Soviet countries and Russia itself also acceded**, followed on from the export control developed during the Cold War via COCOM.

In Germany and Europe, **export control regulations have the force of criminal law** and **are punishable under that law**. The background to this is that Germany has made an international commitment to prevent the proliferation of weapons of mass destruction and the uncontrolled accumulation of conventional armaments. This also includes the control of sensitive goods, including technologies and software, as an important part of this non-proliferation strategy. In addition to commercial enterprises, higher education institutions and research institutions are also addressees of the control regulations for the handling of potentially critical goods [53] and the transfer of sensitive know-how: “This concerns the export of goods (e. g. laboratory equipment, test equipment), in particular the export of embodied technology (in e-mails, on data carriers, in clouds, etc.), as well as the non-embodied (‘intangible’) transfer of knowledge, the transfer of know-how, i. e. so-called ‘technical assistance’”. [54] Goods or technologies listed nationally or in the EU Dual-Use Regulation as well as country embargoes, i. e. restrictions in the course of international economic sanctions, are of primary interest here. To date, the main focus has been on proliferation-related issues. Some key technologies in the context of electronic data transfers (EDT) are not (yet) listed and are therefore not explicitly subject to export control. Nevertheless, they can represent a security risk.

In the area of export control, whose regulations apply to both the individual scientist and the higher education institution or research institution, the **objective potential for misuse** is primarily decisive – in relation to the subject matter – regardless of the motivation and objective of the individual’s own activities. [55] It is also important to consider cooperation with persons who may be included on sanctions lists.

[53] This also includes installed parts. The BAFA refers, for example, to switching spark gaps from medical technology, which in principle can also be used to detonate nuclear warheads.

[54] [unofficial translation] BAFA (2019): Exportkontrolle in Forschung & Wissenschaft; Eschborn, p. 12, https://www.bafa.de/SharedDocs/Downloads/DE/Außenwirtschaft/afk_aca_broschuere_awareness.html?nn=1466914. War weapons are subject to their own legislation (War Weapons Control Act).

[55] Cf. on this: BAFA (2019): Exportkontrolle in Forschung & Wissenschaft; Eschborn, esp. p. 9, https://www.bafa.de/SharedDocs/Downloads/DE/Aussenwirtschaft/afk_aca_broschuere_awareness.html?nn=1466914.

The development of the so-called Khan network is considered the best-known case of the transfer of knowledge and its misuse. After his education at European universities, Abdul Quadeer (A. Q.) Khan was able to become the "father of the Pakistani nuclear bomb". Through his proliferation network, he was able to pass on nuclear expertise and technology to other states such as Iran, North Korea and Libya, as well as to non-state actors. [56]

China has currently established **the most comprehensive export control**, including a restrictive data regime. As an autocratic state, it is able to do this. It does not focus its export control solely on the possibility of using research and technology for military purposes, but has developed a variety of control measures with different strategic objectives. The aim is to ensure national security in a very comprehensive sense so that, according to observers, "Beijing's strategic motives, means and constraints will significantly shape the nexus of geopolitics and technology in the years to come". [57]

IV.2 Civil clauses

In Germany, for historical reasons, a "**culture of peace orientation**" is **firmly anchored** in large parts of the academic world, which in many places included the establishment of civil clauses. This development is also based on the assumption that a clear distinction can be made between research for civilian and military purposes or for peaceful and non-peaceful motives. Today, Germany is said to have a "culture of military restraint", which has emerged as a "product of foreign and security policy developments as well as domestic political negotiation processes". [58]

[56] Cf. on this: Heupel, M. (2008): Das A. Q.-Khan-Netzwerk. Transnationale Proliferationsnetzwerke als Herausforderung für die internationale Nichtverbreitungspolitik, SWP-Studie, Stiftung Wissenschaft und Politik, German Institute for International and Security Affairs; Berlin, https://www.swp-berlin.org/publications/products/studien/2008_S14_hpl_ks.pdf.

[57] "The party state's toolkit includes: Dual-use export controls (Export Control Law, ECL); Civilian technology export controls (Foreign Trade Law and Technology Import/Export Regulations, TIER); Other instruments (blacklists, localisation of data, technical information and intellectual property (IP), restrictions on talent mobility, managed trade and investment, and party-state control of S&T development). 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." Arcesati, R.; Chimits, F.; Hmaidi, A. (2024): Keeping value chains at home. How China controls foreign access to technology and what it means for Europe, MERICS (Mercator Institute for China Studies) Report; Berlin, p. 3, https://merics.org/en/report/keeping-value-chains-home.

[58] Barbin, J. L. S.; Konopka, T. (2023): Militärische Zurückhaltung oder militärisches Engagement? Entstehung und Entwicklung der strategischen Kultur der Bundesrepublik Deutschland bis 1990 im Lichte von Archivquellen, in: SIRIUS-Zeitschrift für Strategische Analysen, 7(4), pp. 327-353, https://doi.org/10.1515/sirius-2023-4002.

Civil clauses [59] are generally voluntary commitments on the part of higher education institutions, only in individual cases obligations in higher education laws that are based on the peace requirement enshrined in Article 26 of the German Basic Law (GG [60]). According to this, research, teaching and studies should only serve civil or peaceful purposes. [61] More than half of the federal states, namely Baden-Württemberg, Bavaria, Hamburg, Mecklenburg-Western Pomerania, Lower Saxony, North Rhine-Westphalia, Rhineland-Palatinate, Saarland and Saxony, do not currently have a civil clause enshrined in their general higher education laws. Since July 2024, Bavaria has even declared "a restriction of research to civilian use (civil clause)" to be "inadmissible" in its Hochschulinnovationsgesetz. [62] The higher education laws of the other federal states provide for an orientation towards peaceful coexistence, for example in Berlin,

[59] A forerunner of the civil clause had already been included in the founding treaty of the Karlsruhe Nuclear Research Centre in 1956, in this case at the instigation of the Allies, who attached importance to the demilitarisation of research in Germany. The peace movement subsequently contributed to the civilian orientation of public research institutions – not least promoted by students.

[60] Article 26 paragraph 1 of the Basic Law reads: "Acts which are suitable and carried out with the intention of disturbing the peaceful coexistence of peoples, in particular the waging of a war of aggression, are unconstitutional. They shall be punishable by law." [unofficial translation] https://www.bundestag.de/parlament/aufgaben/rechtsgrundlagen/grundgesetz#1.

[61] Sub-legal civil or peace clauses can be found in various places: in the mission statement of a higher education institution or research institution, in its constitution or as a voluntary commitment by the Senate. The basic regulations of some higher education institutions make explicit reference to the preservation of constitutionally guaranteed academic freedom, such as in the preamble of Bielefeld University (Grundordnung der Universität Bielefeld vom 1. September 2020 in Verbindung mit den Änderungen vom 1. März 2021 und 15. Januar 2025, https://verkuendungsblatt.uni-bielefeld.de/1/1/1/P000232830.pdf). Individual higher education institutions assign their ethics committee the task of dealing with issues relating to the possible use of research results for non-peaceful purposes, cf. Grundordnung der Europa-Universität Viadrina Frankfurt (Oder) in der Fassung der ersten Änderungssatzung vom 06.11.2019, § 10 Abs. 8, https://www.europa-uni.de/de/universitaet/einrichtungen/stabsstellen/justiziariat/zentrale-ordnungen/_dateien/grundordnung-2019.pdf.In exceptional cases, it is also stated how to proceed in cases of conflict: "The restriction of the university to civil research resulting from these regulations and the university's mission statement also represents an individual obligation for all members and affiliates conducting research at the university. The notification of research projects in accordance with Section 66 (3) ThürHG must contain the assessment that the subject of the research is not directly military or armaments research. The President or a body authorised by him shall review this assessment. If this assessment is not made or if there are doubts as to its justification, the application must be submitted to the university's ethics committee. This is formed by the Research Committee in accordance with Section 13 (3). The committee must hear the applicant and, at the applicant's suggestion or by its own decision, consult further experts for the decision-making process. The President has the right to apply, participate and speak. The President makes the final decision on the incompatibility of the research project with the civil clause in accordance with Section 5 (3) ThürHG based on the assessment of the Ethics Committee. The President shall inform the public annually and in an appropriate manner." [unofficial translation] Grundordnung der Technischen Universität Ilmenau vom 05.02.2019, § 2 Abs. 6, https://www.tu-ilmenau.de/fileadmin/Bereiche/Universitaet/Dokumente/Satzungen_und_Ordnungen/Grundordnung/Grundordnung_TU_Ilmenau_2019.pdf.

[62] [unofficial translation] Bayerisches Hochschulinnovationsgesetz (BayHIG) vom 5. August 2022 (GVBl. S. 414, BayRS 2210-1-3-WK), das zuletzt durch § 14 des Gesetzes vom 3. Dezember 2024 (GVBl. S. 605) und durch § 8 des Gesetzes vom 23. Dezember 2024 (GVBl. S. 632) geändert worden ist, Artikel 20 Abs. 4, https://www.gesetze-bayern.de/Content/Document/BayHIG-20. The law is constitutionally controversial.

Brandenburg, [63] Hesse, Bremen, Saxony-Anhalt, Schleswig-Holstein and Thuringia. The states of Bremen and Thuringia have also stipulated by law that higher education institutions must adopt a civil clause. [64] From a legal perspective, the **effect of civil clauses is limited in practice in view of the constitutionally guaranteed academic freedom**, as examples of cooperation with actors from the military sector, such as the Bundeswehr, show. Nevertheless, many actors in institutions with a civil or peace clause also consider themselves bound by it.

[63] The Hochschulgesetz contains a very open formulation: "The higher education institutions [...] are aware of their responsibility towards society and the environment and address the possible consequences of using their research results and work towards the sustainable use of resources at the higher education institution" [unofficial translation] Brandenburgisches Hochschulgesetz (BbgHG) vom 9. April 2024 (GVBl.I/24, [Nr. 12]) geändert durch Artikel 2 des Gesetzes vom 21. Juni 2024 (GVBl.I/24, [Nr. 30], S. 32), § 3 Abs. 3, https://bravors.brandenburg.de/gesetze/bbghg#3.

[64] Thüringer Hochschulgesetz (ThürHG) vom 10. Mai 2018, zuletzt geändert durch Gesetz vom 2. Juli 2024 (GVBl. S. 371), § 5 Abs. 3, https://landesrecht.thueringen.de/bsth/document/jlr-HSchulGTH2018V4P5, and Bremisches Hochschulgesetz (BremHG) vom 9. Mai 2007 (Brem.GBl. S. 339), zuletzt geändert durch Artikel 3 des Gesetzes vom 28. März 2023 (Brem.GBl. S. 305), § 4 Abs. 1 and § 7 b, https://www.transparenz.bremen.de/metainformationen/bremisches-hochschulgesetz-in-der-fassung-vom-9-mai-2007-190931?asl=bremen203_tpgesetz.c.55340.de&template=20_gp_ifg_meta_detail_d#jlr-HSchulGBR2007V6P7b.

C. Recommendations for dealing with knowledge risks and security-relevant research

In recent decades, the German system of research and higher education has become much more international. There are intensive global networks ranging from student exchanges to formal cooperation between entire institutions. **International exchange and cooperation** is – and always has been – at the **core of scientific activities**. Internationalisation has also been politically demanded and promoted, not least in order to increase the quality of academic work in one's own country. It is now increasingly recognised as a value in itself and acts as an indicator in the context of evaluations.

However, in the new global political situation, which is characterised by systemic rivalries in political, social, economic and scientific terms, open societies and an open, internationally networked system of research and higher education run the risk of their openness being deliberately exploited and abused (**vulnerability of open systems**). At the same time, scientists may be overly cautious if, out of concern for knowledge security and in view of the often still unclear framework conditions in the still poorly developed field of knowledge security, they do not continue collaborations, do not seek new collaborations or refuse to engage in exchange (**overreaction/overprotection**).

The WR considers it an **urgent task** to create **certainty in this field. Otherwise, there is a risk of a double loss**: on the one hand, uncertainty reduces the willingness to work with partners in critical countries, and on the other hand, certain countries are reluctant to work with institutions in Germany – in both cases because the framework conditions have not been clarified and processes have not yet been implemented in the institutions.

Germany has some catching up to do in this area. **More attention** needs to be **paid to knowledge security** in the system of research and higher education. Other countries such as Canada, the Netherlands and Denmark have already implemented corresponding strategies and measures to deal with knowledge risks. |[65] Germany also has some catching up to do when it comes to the **importance of security-relevant research**. Here too, other countries are already advancing and want to promote security-relevant research in a more targeted manner. |[66]

For the WR, it is crucial that no actor in the system of research and higher education can completely disregard the changed global political situation and the new competitive situation – including systemic rivalry – in scientific, technological, economic or social terms. **The various actors in the system of research and higher education** – from individual researchers to legislators (cf. C.I) – **are called upon to assume responsibility in this cross-sectional field**, the importance of which has increased massively, in order to account for the relevance of their own work for the security and resilience of the community and to establish knowledge security. The WR is aware that this is a new field in terms of its scope and that it will require a joint effort, which will certainly require time and financial resources. This endeavour will change the system of research and higher education and link it more closely than before with other policy areas.

C.I SHARING RESPONSIBILITY

The expansion of research fields that are potentially security-relevant or have an inherent dual-use character, the convergence of disciplines, especially in the course of the penetration of scientific work with AI and information technology, and the proliferation of actors with different strategic interests call for a **tiered and subsidiary responsibility in the system of research and higher education** in order to be able to deal with the increased requirements for knowledge security and the security relevance of research. Binding legal requirements such as export control, whether at national or supranational level, are only part of a security architecture. What is needed is a more comprehensive **systemic security architecture**. In such a system of governance, the different levels must each fulfil their respective responsibilities. Against this background, the WR recommends

_ that the individual **scientists explicitly address the security relevance of their activities** – in both directions: by examining risks and by examining their potential contribution to creating security and resilience in Germany and Europe. It is the individual scientists who are best able to assess their activities from these two perspectives, even if they do not always immediately realise

|[65] Cf. for a concise and up-to-date overview of the international situation: GA of DFG and Leopoldina (2024): Scientific Freedom and Security Interests in Times of Geopolitical Polarisation – Fifth Report of the Joint Committee of DFG and Leopoldina; Berlin, p. 10 ff., https://www.security-relevant-research.org/publication-progressreport2024/.

|[66] Cf. Ministry of Defense (2024): 2024 Defence White Paper. Strong, smart and together; The Hague, https://english.defensie.nl/downloads/publications/2024/09/05/defence-white-paper-2024.

the potential of their technological applications. Nevertheless, they have a deep knowledge of their research subject and their collaborative relationships. Their commitment is therefore essential; they cannot be relieved of this task. However, an individual researcher cannot adequately fulfil this task without effective support services and structures. The management must provide information that enables the researchers to fulfil their responsibilities (cf. C.II).

_ that the **management of the various scientific institutions and organisations adapt strategically to the new situation** and agree internally on which standards should apply in their own institution. The WR considers it an urgent management task to develop guidelines for dealing with risks and potentials for the organisation and to set up a risk assessment process and provide resources for this (cf. C.III). These measures relate to different dimensions of performance: from research to teaching and training up to transfer. Particular attention must be paid to infrastructures, which – as explained (cf. B.I) – can harbour a knowledge risk in various respects, particularly with regard to their IT-related potential for an undesirable transfer of knowledge and unwanted exertion of influence. Part of dealing with knowledge security should also be to agree on how to address the issue in research and teaching. Students and doctoral candidates must be sensitised at an early stage, for example in modules on good scientific practice, in order to create new routines in dealing with issues of security relevance and knowledge security.

_ that **funding organisations integrate questions about knowledge risks and security relevance into their own procedures**. In view of the internal scientific developments described above and the global political changes, it should be examined how the demand for knowledge security can become part of the respective funding system and how this can be integrated into the guidelines of good scientific practice. [67] At the same time, an awareness should be developed at various levels as to whether and to what extent funding programmes and formats can facilitate security-relevant research in the comprehensive sense developed above (cf. C.IV.2).

_ that the **government** creates the **necessary cross-departmental requirements in the sense of the most coherent possible framework conditions** (cf. C.III.3). This will enable the other actors in the system of research and higher education to fulfil their responsibility – both to protect the system and to participate in security-relevant issues – on a reliable political and transparent information basis. The WR advocates a coordinated approach by the federal and state governments. It is equally necessary to coordinate at European level .

[67] Some funding organisations have already responded to this, such as the DFG (2023): Dealing with Risks in International Research Cooperation. Recommendations from the Deutsche Forschungsgemeinschaft; Bonn, https://www.dfg.de/resource/blob/289704/585cb3b48bb8e9f5b6e57e0e0a0d700e/risiken-int-kooperationen-en-data.pdf. Cf. also Council of the European Union (2024): Council Recommendations of 23 May 2024 on enhancing research security (C/2024/3510), http://data.europa.eu/eli/C/2024/3510/oj.

The fulfilment of responsibility at the various levels is an **urgent task** that involves effort. [68] This **effort** should be **as limited as possible** for the individual scientists and not merely appear as another element of a growing bureaucracy. The aim is to create certainty of action. This task can only be accomplished through shared responsibility.

C.II GOVERNANCE GUIDELINES FOR DEALING WITH KNOWLEDGE RISKS AND SECURITY RELEVANCE

Dealing with issues of knowledge security and security relevance requires **two perspectives to be intertwined**. An overarching political framework is required in order to create coherence across the different areas of society. The perspective of scientists is central, insofar as they – given sufficient sensitivity – are best able to assess the risks and potential of the work with their field expertise.

In order to be able to work together in a productive manner, the WR proposes **three guidelines** for **governance** in dealing with knowledge security and security relevance:

1 – **Developing processes**: Assessments on questions of knowledge security and the security relevance of science and humanities are subject to a continuous social negotiation process. [69] Process-orientation is required at all levels in order to be able to react quickly, flexibly and continuously to a dynamically changing situation. At the same time, established processes increase transparency, create certainty of action for individual scientists and provide scope for continuous improvement. In addition, the risks and potential of research activitities or collaborative projects can change over time. It is therefore not enough to carry out a security check at the beginning of a project, an exchange or a collaboration. A high level of sensitivity is required for the further development of activities over time. It is necessary to interlink the processes established at the various levels in order to create the highest possible degree of consistency and coherence beyond the boundaries of institutions – right up to the state level.

2 – **Create and provide support**: The individual scientists are usually the ones who are best able to assess the security-relevant potential and possible security

[68] The Federal Ministry of Research, Technology and Space (BMFTR) has also drawn attention to this in a position paper, cf. formerly Federal Ministry of Education and Research (2024): Positionspapier des Bundesministeriums für Bildung und Forschung zur Forschungssicherheit im Lichte der Zeitenwende, https://www.bmbf.de/SharedDocs/Downloads/DE/2024/positionspapier-forschungssicherheit.pdf.

[69] Cf. the assessment by Wolfgang Bonß (2014): "In the case of risk problems, on the other hand, there is no clear and final solution; risk problems are characterised by the fact that the envisaged solutions are always 'suboptimal' in that they are not 'final'. Rather, they themselves entail uncertainties that are either newly created or are only now becoming visible." [unofficial translation] Bonß, W. (2014): (Un-)Sicherheit in der Moderne, in: Zoche, P.; Kaufmann, S.; Haverkamp, R. (eds.): Zivile Sicherheit. Gesellschaftliche Dimensionen gegenwärtiger Sicherheitspolitiken; Bielefeld, pp. 43-70, here p. 46, https://doi.org/10.14361/transcript.9783839414354.43.

risks of their work. However, they are not always in a position to adequately assess the different risks in exchange and cooperation with the diverse partners. Support structures are therefore needed at various levels to help them assess risks and potentials and develop an appropriate way of dealing with them. The WR believes that it is the responsibility of the heads of the institutions to create and provide such support services, as well as that of the funding bodies and political decision-makers (cf. C.III). An appropriate structure at national level makes it possible to communicate across institutions, to network at European and international level and, if necessary, to coordinate and react quickly to changes in the global political situation (cf. C.III.3). This can strengthen consistency and coherence at a higher level. The WR points to problems of dependence on commercial providers. It recommends that an offer provided by the public sector should be developed at European level, if possible.

3 – **Take a country-sensitive approach**: To date, a country-agnostic approach has often been favoured when dealing with questions of knowledge security. In view of the global political situation on the one hand and the expansion of research fields with an inherent dual-use potential on the other, the WR recommends a country-sensitive approach. This enables local, regional and national contexts to be taken into account appropriately, legal and political interests of the other party to be assessed well and, if necessary, critical countries to be identified. |[70] The aim is to organise the exchange as securely as possible and to enable cooperation that is in one's own – strategic or scientific – interest, even with partners that are challenging in different respects.

C.III RECOGNISING KNOWLEDGE RISKS AND MANAGING THEM

Scientific activities are understood comprehensively here and do not only include research, but also staff exchanges or cooperation agreements. In the opinion of the WR, **awareness of the risks that exist** and how scientific work can contribute to the security and resilience of the community **is not yet sufficiently pronounced** in large parts of the German system of research and higher education. If this awareness exists, then it primarily relates to utilisation options in the military sector. The responsible researchers generally have an initial intuition in this area. However, more in-depth awareness-raising is required across the board in order to identify the possible risks and potentials of their own work at an early stage

|[70] Cf. also the task of the recommended National Platform (C.III.3). Dynamically developing lists of critical countries are helpful in this matter, e. g. Staatenliste im Sinne von § 13 Abs. 1 Nr. 17 SÜG from the Federal Ministry of the Interior (BMI), https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/sicherheit/staatenliste-para-13-anleitung-sicherheitserklaerung.html. Or the embargo list of the BAFA, https://www.bafa.de/SharedDocs/Downloads/DE/Aussenwirtschaft/afk_embargo_uebersicht_laenderbezogene_embargos.html. Such lists also exist at European level and in other countries, such as the EU Sanction Map, cf. https://www.sanctionsmap.eu/#/main.

The WR recommends that every institution **develop and implement** a **lean and clear risk assessment.** Every institution can organise it in different ways depending on its risk profile and size. This is the responsibility of the individual higher education institution or research institution. It is crucial that science and administration work together to develop a **pragmatic**, **manageable process**. A pragmatic approach creates acceptance on the scientific side and increases the willingness to undergo the risk assessment. Without the willingness of the individual scientist to deal with the risks, the process – especially beyond the binding legal requirements of customs and export control law – will come to nothing.

III.1 Case-related individual examination and collegial exchange

As explained at the beginning (cf. B.III), knowledge risks can have five different dimensions. These include (1) the undesirable transfer of knowledge and (2) the undesirable exertion of influence on the system of research and higher education. In addition, (3) it is important to ask whether one's own research is sufficiently independent – both financially and scientifically. Furthermore, (4) interference with other areas of society must be considered and (5) (research) ethical principles must be upheld. The basis of appropriate knowledge security is that the individual scientist examines and recognises the **knowledge risks** of her or his own work. Exemplary guiding questions (cf. Appendix 1) can help in the context of this **case-related individual examination** (cf. also Figure 1) to better assess these risks and to proceed with sufficient risk awareness.

As a first step, it is therefore up to the individual scientist to take responsibility here. The WR has identified **five indications that suggest a more extensive risk assessment**:

1 – **Particularly sensitive research topics**: One clue can be the relation of the topic to fields that are considered particularly sensitive. So far, such fields have not been consistently identified across departmental and national borders. The WR recommends identifying such research fields centrally for Germany and, if possible, in agreement with European partners, even if it will hardly be possible to reach a final agreement, especially in view of the enormous speed at which certain fields are developing. Rather, this is an ongoing task that aims to create an information base as consistent as possible – in the sense of a living document – for the system of research and higher education (cf. also C.III.3).

As example of a sensitive topic in medical research AI-supported systems for virtual toxicity testing of drug candidates with a view to drug development shall be referred to. Such systems are also able to identify particularly harmful molecules. With little effort, known toxins such as sarin or tabun can be detected within a few hours, as can previously largely unknown, highly toxic substances and those potentially used as arms. Even if further research is needed to stabilise such molecules and test their effect in the organism, the use of such software harbours risks with regard to the design of new types of chemical warfare agents. |[71]

2 – **Cooperation partners from critical countries**: A further indication of increased attention is given by actors and actor constellations, as explained in the context of the reflection on the dual-use concept (cf. B.II). The personal motives, state interests or the interests of companies such as large technology companies are not always obvious. Therefore, student exchanges or cooperation with scientific or economic cooperation partners from critical countries can harbour risks. Comprehensive information is required for a well-founded assessment (cf. C.III.3).

The prerequisite is that there is always an agreement on which country or which company is relevant here at national and, if applicable, European level – comparable to the exchange on sensitive fields of research (cf. C.III.3). |[72]

An example of this is the planned visit of a foreign scientist from a country classified as critical, who wanted to participate in an electrical engineering project to optimise electricity, gas or water networks, in other words critical infrastructure, in Germany using AI methods. There is a risk of undesirable knowledge transfer in two respects: Firstly, the models on which the AI methods are based can be modified in such a way that they can damage or even paralyse the infrastructure instead of making the system more efficient. On the other hand, AI-based optimisation is based on detailed data sets, so that accessing them provides a comprehensive insight into the structural properties of the infrastructure. This exposes the structure and functional basis of the critical infrastructure in Germany and/or Europe and makes it (more) vulnerable.

3 – **Indirect collaboration with critical partners**: Collaboration with organisations – whether academic or corporate – whose headquarters are located in one of the countries identified as critical, can be cause for risk assessment. This is because even if these research and educational institutions or companies have branches in Europe, the cooperation can be risky. Intended or indirect strategic interests can play a role here, for example if the main partner is not disclosed or dependent parties can be put under pressure. This may involve personnel ex-

|[71] Urbina, F.; Lentzos, F.; Invernizzi, C. et al. (2022). Dual use of artificial-intelligence-powered drug discovery, in: Nature Machine Intelligence, 4, pp. 189-191, https://doi.org/10.1038/s42256-022-00465-9; Jakob, U.; Krämer, F.; Kraus, F. et al. (2024): Applying Ethics in the Handling of Dual Use Research: The Case of Germany, in: Research Ethics, 0(0), https://doi.org/10.1177/17470161241261044. According to the GA's 5th report, the authors conducted the study to draw attention to potential risks of misuse of artificial intelligence (AI) systems, cf. GA of DFG and Leopoldina (2024): Scientific Freedom and Security Interests in Times of Geopolitical Polarisation – Fifth Report of the Joint Committee of DFG and Leopoldina; Berlin, p. 69, https://www.security-relevant-research.org/publication-progressreport2024/.

|[72] Cf. also the references to country lists in footnote 70.

changes, collaborations or even traditional contract research. Detailed information on this is essential in order to be able to assess the situation appropriately.

One example of indirect cooperation is the case that came to light in January 2025, in which a German worked for a Chinese intelligence officer for several years (2017-2024) in order to gain knowledge about boat engines, sonar systems, aircraft protection systems, drives for armoured vehicles and drones for military use. Contacts were established with the research organisation via a company based in Germany. The university's cooperation agreement was then concluded with the German-based company, which was, however, working with the Chinese secret service. |[73]

4 – **Research location with sensitive technologies**: The use of sensitive technologies such as devices or methods is also an indication of the need to pay increased attention to security relevance. This may involve explicitly listed and export-regulated goods such as laser or lens systems. But even relatively simple laboratory setups for achieving sensitive research results could require special attention.

For example, a visiting delegation was given the opportunity to gain insights into the equipment and methodology of an institution. Even if the research topic itself is not sensitive, the equipment could be of interest. It was observed that other foreign delegation members appeared unannounced and left the guided tour for some time. This allowed them to take pictures of the research department's equipment and gain valuable information for other activities. |[74]

5 – **Application proximity**: The TRL can serve as a reference point for assessing the potential for direct misuse. 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. And it is not only in these fields that the acceleration of realisation should be considered.

An example of this is the request of a Chinese scientist who wanted to work on a research project on composite materials and manufacturing concepts on

|[73] Cf. Federal Public Prosecutor General at the Federal Court of Justice (2025): Anklage wegen mutmaßlicher geheimdienstlicher Agententätigkeit erhoben, 09.01.2025, https://www.generalbundesanwalt.de/SharedDocs/Pressemitteilungen/DE/2025/Pressemitteilung-vom-09-01-2025.html.

|[74] Cf. i. a. BfV (2022): Informationsblätter zum Wirtschaftsschutz. Spionage in Wissenschaft und Forschung; Berlin, p. 4, https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/wirtschafts-wissenschaftsschutz/2023-01-17-infoblatt-spionage-in-wissenschaft-und-forschung.pdf.

a TRL 3-5. The research project enables a reduction in mass by replacing metallic materials with polymer materials in carrier technologies such as aircraft construction. The employee visited the Nanjing University of Aeronautics and Astronautics (NUAA), which belongs to the Seven Sons of National Defence and is subordinate to the Ministry of Industry and Information Technology. If this request had been granted, there would have been cooperation with the Chinese military with a high degree of application proximity.

These **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. However, if the overall assessment of the evidence suggests that there are security-relevant aspects, the WR recommends that the individual researchers initiate a **further risk assessment**. If a risk is subsequently deemed probable, the project should not be realised or should only be realised under clearly defined boundary conditions – in consultation with the Committees for Ethics in Security-Relevant Research (KEF).

If one or more indications are present and the individual is unsure whether a risk exists, the next step should be a **collegial exchange – referred to below as a dialogue-based procedure**. A dialogue with colleagues can lead to a clearer assessment of the risks and potential of one's own work. The WR therefore recommends it **as the second step in risk assessment**. This is because such an assessment is complex and – with the exception of the legally regulated area of export control – does not usually boil down to simple yes/no decisions. Without directly entering into a formalised process, a collegial exchange can help to better reflect on one's own interests and possible risks. Whether contact persons for knowledge risks should be nominated at department or faculty level or at higher levels or whether such tasks can be taken over by ombudspersons for other issues must be decided in the individual institution or organisation. This depends on the risk profile and the size of the institution (cf. C.III.2). It is crucial that the management of the institution appoints contact persons, if necessary, who should be publicised within the higher education institution or research institute as well as trained and supported.

A **dialogue-based procedure** such as the one proposed here, which focuses on awareness-raising and collegial exchange, enables further process steps to be initiated only when they are necessary and not just to cover oneself. This means that the administration and/or existing committees in the facilities, such as the KEFs that exist in many facilities, are not overburdened. They are only involved in a third step (cf. C.III.3).

In the future, it is important that **sensitisation to issues of knowledge security and security relevance** is systematically integrated **into teaching and training**

– at the latest in the doctoral phase – such as in modules on good scientific practice.

III.2 Strategic management task: structurally anchoring risk assessment

In terms of shared responsibility (cf. C.I), the management of a higher education institution or research organisation also bears responsibility for dealing with the issues of knowledge security and security-relevant research at its own institution. They are required to ensure that **competences are built up** at the institution, **that advice is offered and a process of consideration is established**.

The major higher education institutions and research organisations are already set up in such a way that **export control** issues that are also of (criminal) legal relevance can be dealt with in cooperation with the Federal Office for Economic Affairs and Export Control (BAFA). The **initiative** to start the risk assessment usually lies with the individual scientist (cf. C.III.1). Some higher education institutions and research organisations have integrated the identification of risks – particularly with regard to export control – into their formal procedures such as recruitment or document management processes. This allows the institution to take the initiative, as it must do in certain cases in order to minimise potential damage, avoid accusations of organisational culpability and relieve the burden on individual researchers. Some higher education institutions and research organisations have charged special officers with this task. [75]

Research institutions or individual higher education institutions can build on these structures or others yet to be established (cf. C.III.3) in order to be able to deal with security-relevant issues, which essentially lie in the pre-legal area. In the view of the WR, there can be no "one-size-fits-all" solution. Rather, the **management** of higher education institutions and research institutions are **required to set up appropriate support structures and processes adapted to the size and risk profile of their institution** and to take data and cyber security issues into account.

The WR advocates lean solutions and expressly recommends **cross-institutional models** for reasons of efficient use of resources and the pooling of expertise. [76] In any case, it is the responsibility of the management to provide sufficient sup-

[75] According to the BAFA's recommendation, this position should be "organisationally and in terms of personnel independent from the research process. In smaller organisations, the task can be assigned to an existing organisational unit (e. g. legal department, auditor)" [unofficial translation] BAFA (2022): Handbuch Exportkontrolle und Academia, 2nd ed.; Eschborn, p. 107, https://www.bafa.de/SharedDocs/Downloads/DE/Aussenwirtschaft/afk_aca_broschuere_handbuch.html.

[76] With regard to digital security, the Bavarian universities laid the foundation for a cross-institutional network in 2023, cf. https://www.utn.de/2023/03/21/forschungsnetzwerk-fur-digitale-sicherheit/. With regard to ethical issues, the Bavarian universities of applied sciences have formed a network and created a joint ethics committee to evaluate ethical and legal aspects of research activities, cf. https://www.gehba.de/home.

port to the individual scientists. The establishment of lean structures and processes – at the institutions or across institutions – is necessary and should take place as quickly as possible, if not already done. Under no circumstances, however, should the formal referral of research projects to a commission be the rule; self-review and the dialogue-based procedure should act as effective filters.

Many higher education institutions and research institutions have already appointed **contact persons** for security-relevant research or a **KEF**, whose core competence lies in the ethical assessment of and counselling on the potential for misuse of specific research results and methods at the respective institutions. Due to the increasing demand, more and more higher education institutions and research institutions are setting up KEFs or appointing people to carry out such risk assessment tasks. [77]

The business sector has already adapted more comprehensively to the risk situation, which has been intensifying for several years. In many cases, companies have set up compliance management systems (CMS) in line with their risk profile. [78] With a view to the legal provisions in the area of export control, they are referred to as **Internal Compliance Programmes (ICP)**. Such ICP, which serve to proactively prevent violations of foreign trade law, could also be set up in the system of research and higher education. With an appropriately adapted system, higher education institutions and research organisations could also systematically protect themselves from criminal or administrative liability under export law and from reputational damage. In the medium to long term – similar to the situation for commercial enterprises – the **possibility of certification** of an ICP tailored to the scientific system could be considered. [79] Commercial enterprises can use privileged procedures at BAFA and customs to minimise criminal and administrative offence risks when dealing with dual-use goods and increase efficiency in the process. Such certification is attractive and relieves the burden on the management, insofar as it can be proven in cases of doubt that there is no organisational culpability.

III.3 Establish a National Platform for knowledge security

In recent years, **various self-regulatory initiatives** have emerged within the system of research and higher education to deal with ethical challenges and the risks of international cooperation and mobility. In 2015, for example, the German Research Foundation (DFG) and the German National Academy of Sciences

[77] Cf. the analysis of the GA of the DFG and Leopoldina (2024): Academic Freedom and Security Interests in Times of Geopolitical Polarisation – Fifth Report of the Joint Committee of DFG and Leopoldina; Berlin, p. 36 ff., https://www.security-relevant-research.org/publication-progressreport2024/

[78] Cf. also BAFA (2022): Handbuch Exportkontrolle und Academia, 2nd ed.; Eschborn, p. 101 f., https://www.bafa.de/SharedDocs/Downloads/DE/Aussenwirtschaft/afk_aca_broschuere_handbuch.html.

[79] Cf. BAFA (2022): Firmeninterne Exportkontrolle. Betriebliche Organisation im Außenwirtschaftsverkehr, 3rd ed.; Eschborn, esp. p. 21. https://www.bafa.de/SharedDocs/Downloads/DE/Aussenwirtschaft/afk_merkblatt_icp.html.

Leopoldina created the **Joint Committee on the Handling of Security-Relevant Research (GA)**, which deals with ethical issues such as the potential for misuse of certain research and is increasingly confronted with security-relevant – including legally relevant – aspects of research. [80] The GA cooperates with the KEFs established at many higher education institutions and research institutes.

The **Centre for International Academic Cooperation (KIWi)** – linked to the German Academic Exchange Service (DAAD) – was founded in 2019 with a view to international cooperation. [81] Primarily building on the DAAD's regional expertise, the KIWi advises German higher education institutions on international cooperation issues and increasingly takes into account the associated security-relevant risks. All initiatives, the GA in cooperation with the KEFs as well as the KIWi, provide valuable and urgently needed **awareness-raising and networking activities** in addition to their **advisory work**.

The WR expressly recognises these various activities. They are indispensable for the German system of research and higher education. However, it sees **a gap at the national level** – especially in view of the subsidiary responsibility called for at the beginning (cf. C.I). Firstly, there is currently a lack of national positioning in order to create the highest possible degree of coherence across all scientific institutions in dealing with security-relevant issues. Secondly, scientists and institutions are dependent on obtaining specific information on security-relevant aspects of their projects themselves. At present, they have to rely on sources that – such as the ASPI tracker [82] – only contain limited information [83] or for which it is unclear what quality standards they fulfil. In addition, there is a lack of coordinated and comprehensive support at national level if scientific institutions or organisations want to position themselves strategically, particularly

[80] The GA has an office in Berlin, which is affiliated to the President's Office of the Leopoldina. In addition to expenses incurred by the Leopoldina, the office is also supported by the DFG, Fraunhofer-Gesellschaft (FhG), Helmholtz Association, Leibniz Association and Max Planck Society on the basis of a cooperation agreement, cf. https://www.security-relevant-research.org/office/.

[81] Based on a recommendation by the WR in 2018, the Centre for International Academic Cooperation (KIWi) was founded as a central advisory centre for international cooperation, particularly for higher education institutions. Since then, the portfolio of tasks has expanded to include the assessment of knowledge risks and legal issues relevant to research. The Federal Foreign Office and the BMFTR support the work of the KIWi financially, cf. https://www.daad.de/en/information-services-for-higher-education-institutions/kiwi/about-us/ and the more detailed report in DUZ - Magazin für Wissenschaft und Gesellschaft: DAAD (ed.) (2024): Impulse für die internationale Hochschulzusammenarbeit. Das Kompetenzzentrum Internationale Wissenschaftskooperationen (KIWi) stellt sich vor; Bonn, https://static.daad.de/media/daad_de/pdfs_nicht_barrierefrei/infos-services-fuer-hochschulen/kompetenzzentrum/duz_special_daad_kiwi_2024.pdf.

[82] Tracker of the Australian Strategic Policy Institute. This relates exclusively to China and was last updated in 2019 (cf. https://unitracker.aspi.org.au/) The financing should also be considered, meaning that it is not a neutral body.

[83] Such a gap is also recognised by other players in the system of research and higher education. In its impulses for the new legislative period, the DFG has called for the "funding of a central advice centre for science", DFG (2025): Erkenntnisgeleitete Forschung als Fundament für die internationale Wettbewerbsfähigkeit Deutschlands. Impulse der DFG für die 21. Legislaturperiode des Deutschen Bundestages; Bonn, p. 12, https://www.dfg.de/resource/blob/352134/908b9ec587e758a0e5d25f8f0c317706/250226-impulspapier-legislaturperiode-data.pdf, for an English summary https://www.dfg.de/en/service/press/press-releases/2025/press-release-no-02.

with regard to their international cooperation. The WR therefore advocates the establishment of **a National Platform for knowledge security**, which should fulfil the following functions:

1 – **Coordination and positioning**: The dynamics and complexity of global political developments on the one hand and technological advances on the other call for a **continuous exchange in order to bring together the perspectives of the various stakeholders on the scientific and governmental side**. Those responsible in ministries and departmental research institutions, and possibly also representatives of the security services and representatives of the federal states, gain a deeper insight into the current state of research in sensitive fields and a broader understanding of the logic and interests of the scientific players. Conversely, the scientific stakeholders gain insights into the overarching political implications. A positioning on dealing with knowledge risks involving the various scientific and state actors thus makes it possible **to have an orientating** effect on the German system of research and higher education and to prepare a well-founded **positioning of Germany** in this respect **in the European context**.

In this way, the framework conditions are created that help to achieve the highest possible degree of **coordination between the state and the scientific community**. These framework conditions create a reliable and transparent basis for the actions of scientific actors so that they can adequately fulfil their responsibilities in the system of tiered competences (cf. C.I).

2 – **Building expertise on the basis of comprehensive information**: Comprehensive information about existing risks is a prerequisite for positioning. Knowledge and assessments from various sources should be brought together here: from regional expertise, for example from the DAAD's very large network of lecturers, to the assessments of certain technologies by the GA, to the information and assessments of the various departments, which also have access to intelligence information (BfV, BND, Military Counterintelligence Service (MAD)) and can contribute their knowledge in a controlled manner.

The WR recalls the points already made about the problematic **dependence on commercial providers** and their information services (cf. C.II). If no corresponding offer is developed at European level, relevant information should be bundled and made available at national level. These should provide scientific institutions with a data basis as comprehensive as possible for assessing the risk potential of persons or institutions.

3 – **Advice for institutions and research organisations:** At the same time, such a platform can provide advisory support to existing structures in the sense of a one-stop shop and thus have an impact on the system of research and higher education. The advice can be of a strategic nature in the context of developing

internationalisation strategies or supporting the drafting of cooperation agreements.

According to the WR, such a structure can be implemented in different organisational ways. It would appear reasonable for the **platform** to fulfil the **following boundary conditions in its mode of operation**:

_ **state actors** are broadly involved;

_ the platform is politically **mandated**;

_ the structure works **on a subsidiary basis**;

_ it **responds quickly** to enquiries in order to do justice to the dynamics of the scientific process;

_ the **participants meet regularly** in order to be able to react continuously to the dynamically changing framework conditions, and

_ the platform is **supported** by a **lean administrative unit**.

The difference and **added value compared to purely internal scientific structures** such as the KIWi and the GA, which are already doing very good work, lies in the involvement of state actors. This gives the **platform access to specific sources of information and to political assessments**. Functions and working methods determine the organisation and resource requirements.

The WR is aware that overarching platforms of this kind are usually only created when, in addition to the obvious need, the political will is also present, as, among other things, legal framework conditions may need to be adapted or corresponding legal requirements created. In many cases, a shock event significantly fosters political pressure and the will to act together. The WR warns against waiting for such a shock event in Germany and instead advocates **setting up such a platform as quickly as possible**. Its establishment at national level, involving various ministries, is urgently needed and should be realised as soon as possible.

The WR believes that all stakeholders will benefit from the establishment of such a platform. This is because it promotes networking between the system of research and higher education and politics, helps to coordinate the activities of individual departments and helps the security services to assess cutting-edge technologies. The EU has also recommended that its member states "[w]here relevant, create a new or reinforce an existing support structure or service." |[84]

Such a platform can also serve as a central **point of contact at European or international level** – comparable to institutions such as the Contact Point for

|[84] Council of the European Union (2024): Council Recommendation of 23 May 2024 on strengthening research security (C/2024/3510); Brussels, p. 6, https://eur-lex.europa.eu/eli/C/2024/3510/oj.

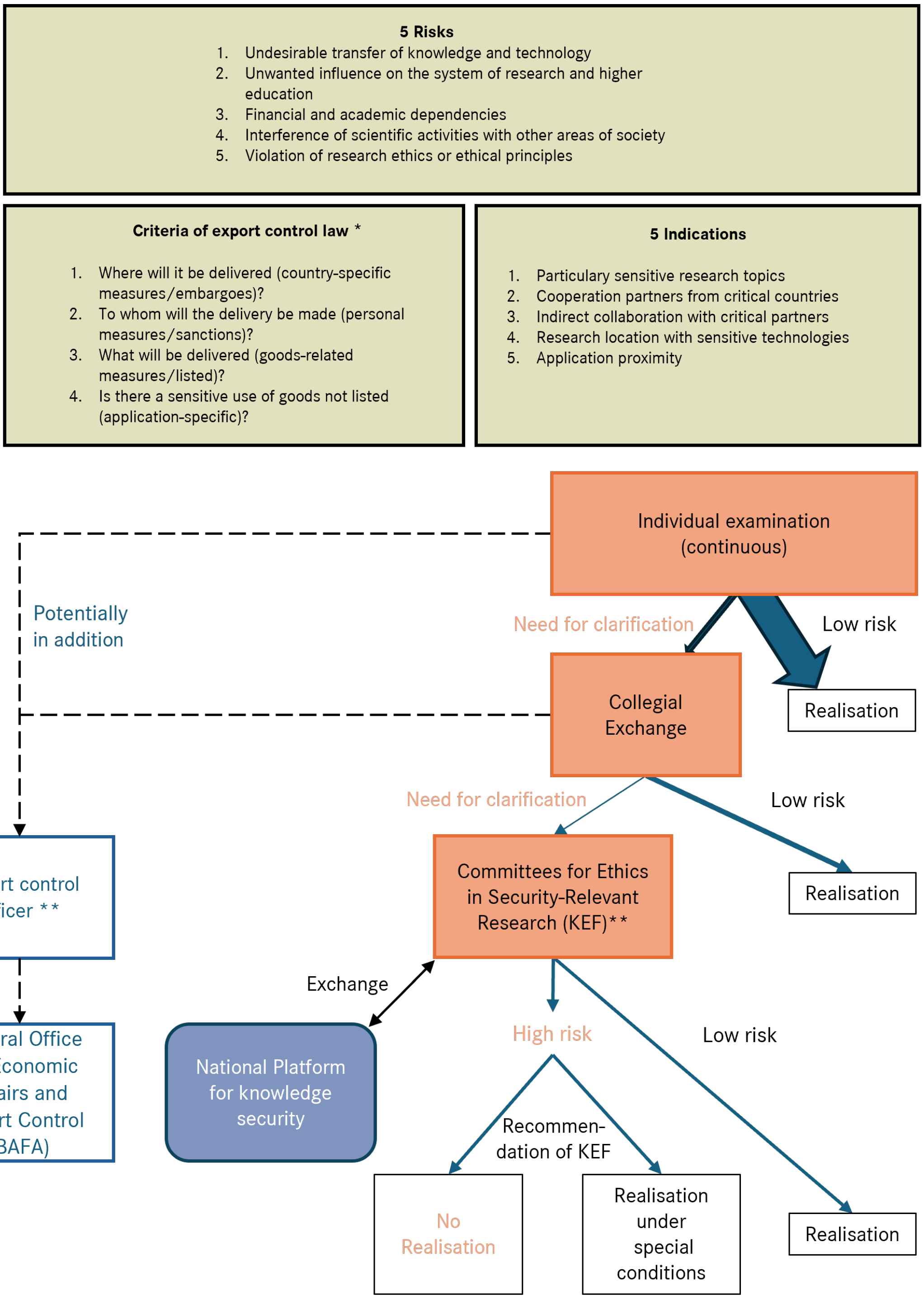
Knowledge Security in the Netherlands[85] or the SECURE Centre of the US National Science Foundation.[86] European and international cooperation is necessary in order to maintain international scientific cooperation – especially with like-minded partners – as unbureaucratically and barrier-free as possible.

The following figure summarises the risk assessment in an idealised manner – from the primary level of the individual to the National Platform for knowledge security that is yet to be established.

[85] Cf. https://english.loketkennisveiligheid.nl/.

[86] Safeguarding the Entire Community in the U.S. Research Ecosystem (SECURE), cf. https://new.nsf.gov/research-security.

Figure 1: Risk assessment



5 Risks

1. Undesirable transfer of knowledge and technology
2. Unwanted influence on the system of research and higher education
3. Financial and academic dependencies
4. Interference of scientific activities with other areas of society
5. Violation of research ethics or ethical principles

Criteria of export control law *

1. Where will it be delivered (country-specific measures/embargoes)?
2. To whom will the delivery be made (personal measures/sanctions)?
3. What will be delivered (goods-related measures/listed)?
4. Is there a sensitive use of goods not listed (application-specific)?

5 Indications

1. Particulary sensitive research topics
2. Cooperation partners from critical countries
3. Indirect collaboration with critical partners
4. Research location with sensitive technologies
5. Application proximity

Individual examination (continuous)
Potentially in addition
Need for clarification
Low risk
Collegial Exchange
Realisation
Need for clarification
Low risk
Export control officer **
Committees for Ethics in Security-Relevant Research (KEF)**
Realisation
Exchange
Federal Office for Economic Affairs and Export Control (BAFA)
National Platform for knowledge security
High risk
Low risk
Recommen-dation of KEF
No Realisation
Realisation under special conditions
Realisation

* BAFA (2022): Handbuch Exportkontrolle und Academia, 2nd ed.; Eschborn, p. 34 ff, https://www.bafa.de/SharedDocs/Downloads/DE/Aussenwirtschaft/afk_aca_broschuere_handbuch.html.

** In the scientific institution or across institutions

Source: Own illustration. The thickness of the arrows is intended to illustrate the order of magnitude of the case numbers.

Based on a comprehensive concept of security, security-relevant research encompasses not only military research, but also the entire field of **research that contributes to the security and resilience of society** (cf. B.II). Therefore, the scientific examination of risks, threats and protective measures both for internal and for external security is security-relevant. This includes the development of new technologies, methods, procedures and services for the prevention, detection and management of different types of danger. Accordingly, security-relevant research occurs in various disciplines and research fields (e. g. from peace and conflict research to cyber security research and civil security research) in different forms and normative orientations.

While the field of military research is largely limited to clearly defined locations – not least due to its high security and confidentiality standards – research on security-relevant issues is **scattered across non-university institutions**, including departmental research institutions of various ministries **and higher education institutions**. One relevant field among several, namely peace and conflict research which is established at various locations, deals with the causes, forms, dynamics and consequences of violent conflicts and armed violence, with their prevention, containment or resolution and with the lasting stabilisation of peace. |[87] In contrast, security studies, which are widespread in the Anglo-Saxon world, and military-oriented strategic studies are comparatively less well represented in Germany. |[88] However, not all academics who deal with questions of internal security, for example with phenomena such as extremism or terrorist violence, or external security, such as with questions of deterrence and collective security, from a political science or sociological perspective, can be clearly categorised as belonging to one of these fields. In many cases, they are located in the field of international relations. |[89]

The **fragmentation** that can be observed in security-relevant research **is primarily due to historical reasons**. In times of confrontational security policy and the

| [87] According to the WR's analysis in 2019, it is an interdisciplinary field with open boundaries and numerous intersections with other research fields and disciplines. There are several non-university institutions and a minimum degree of institutionalisation in the form of professorships with a corresponding denomination at higher education institutions, one scientific society and its own specialist journals, without it being possible to speak of a separate discipline. Cf. WR (2019): Empfehlungen zur Weiterentwicklung der Friedens- und Konfliktforschung; Giessen, esp. p. 8 & 15, https://www.wissenschaftsrat.de/download/2019/7827-19.

| [88] Cf. ibid., p. 35.

| [89] Recently, the field of international relations has been criticised for not sufficiently reflecting the implications of technological developments for security-relevant issues. There is talk of a "blind spot" insofar as the influence and potential of technologies to radically change political power and geopolitics is not systematically taken into account, cf. Baums, A.; Butts, N. (2024): Die Geopolitik der Technologie, in: Internationale Politik, 6, pp. 88-93, https://internationalepolitik.de/de/die-geopolitik-der-technologie. Cf. also Baums, A.; Butts, N. (2025): Tech Cold War. The Geopolitics of Technology; Boulder, https://doi.org/10.1515/9781962551571.

emergence of direct, multidimensional threats ranging from cyberattacks to natural disasters (cf. A), questions of **peace and security** should **be addressed from a systemic and more integrated perspective**. With Russia's war of aggression against Ukraine and the USA's transition of power, "a significant change in German strategic culture and foreign policy culture is also imminent." [90] In order to adequately grasp these security policy challenges and adequately prepare for and accompany the upcoming strategic change, the scientific field and the interaction of science and humanities with political, economic and social actors should be significantly expanded and further developed. Cooperation with disciplines and fields that do not belong to the historically grown sub-disciplines mentioned above is required in relation to problems and topics. This is not only necessary in order to adequately penetrate the topics scientifically, but also to be able to provide the urgently required high-quality knowledge transfer.

Against this background, the WR proposes instruments and measures to **drive forward strategic planning** (cf. C.IV.1) **as well as to create new structures** (cf. C.IV.2) that serve to integrate the field and increase the speed of strategic and technological developments and their productive utilisation.

IV.1 Strategic planning of security-relevant research

Different approaches can currently be observed in research planning. In the military sector, research in Germany is based on civilian research for reasons of efficiency. The Federal Ministry of Defence (BMVg) examines whether research results can be used directly for military applications in terms of dual-use potential or whether technologies can be further developed for military use (so-called add-on research). Research planning is primarily orientated **towards the knowledge and technology requirements articulated** by the **Bundeswehr**. [91] The latter is surveyed annually and leads to research and development measures via a prioritisation process, which, in addition to in-house research, also includes study commissions or grants to third parties. [92] In order to generate ideas for the further development of the Bundeswehr, representatives from the Bundeswehr and

[90] [unofficial translation] Daase, C.; Deitelhoff, N.; Geis, A. (2024): Wer hat uns verraten? Friedens- und Sicherheitsforschung in Kriegszeiten, in: Geis, A.; Deitelhoff, N.; Masala, C. (eds.): Der russische Angriffskrieg gegen die Ukraine und die Internationale Beziehungen, Sonderheft der Zeitschrift für Internationale Beziehungen (zib), 31 (2), 82-105, here p. 97, https://doi.org/10.5771/0946-7165-2024-2-82.

[91] Military science research, which according to the departmental research plan also includes military pharmacy, military veterinary medicine and military dentistry, "generally builds on the findings of civilian research as part of its research activities if national security interests and the desired capability profile of the Bundeswehr require so. If corresponding results from civilian research are not available, they must be developed as part of departmental research." [unofficial translation] BMVg (2023): Ressortforschungsplan des Bundesministeriums der Verteidigung für 2023 ff; Berlin, p. 7 f., https://www.bmvg.de/resource/blob/5637696/555527115f817d20ad9a2c7f49456765/ressortforschungsplan-bmvg-2023-data.pdf.

[92] In addition to the Federal Office of Bundeswehr Equipment, Information Technology and In-Service Support (BAAINBw, unofficially known as the Procurement Office) in Koblenz, the specialised technologies also play a role in the process of determining requirements and generating ideas from various sources (higher

BMVg regularly take part in scientific conferences or meetings. They can gain ideas from the scientific discourse and pass them on to the relevant departments. In individual cases, individual scientists work in ministries for a certain period of time or, conversely, people from the administration are seconded to (departmental) research institutions on a temporary basis.

In peace and conflict research, publicly funded universities and non-university institutions are not solely orientated towards the knowledge interests of basic research, |[93] but work in a distinctly problem-, practice- and application-oriented manner. |[94] In security research, observation of and reflection on current (socio)political developments in Germany and abroad play a role alongside the genuine interest in basic research. Research programmes in these areas therefore develop in an **interplay between their own research interests and the requirement to work in a problem-oriented manner**.

However, **Germany lacks an institutionalised, systematic and regular exchange between the scientific side and other stakeholders in security-relevant issues**. "Scouting" at conferences, personal exchange, problem-orientation and the design of research activities based on perceived security needs are helpful, but are no longer sufficient in view of the systemic challenges and the need for speed.

Against the background of this analysis, the WR recommends setting up a **Strategic Dialogue Forum of scientific and security policy stakeholders**. The latter include political decision-makers from the Federal Chancellery and the various ministries, such as the Federal Foreign Office (AA), the Federal Ministry of Defence (BMVg) and the Federal Armed Forces, the Federal Ministry of Research, Technology and Space (BMFTR), the Federal Ministry for Economic Affairs and Energy (BMWE), the Federal Ministry of the Interior (BMI), the Federal Ministry for the Environment, Climate Action, Nature Conservation and Nuclear Safety (BMUKN) and the Federal Ministry for Economic Cooperation and Development (BMZ). Companies, including defence companies where appropriate, and stakeholders such as the fire brigades, police, the Federal Agency for Technical Relief

education institutions, non-university institutions, industry, international partnerships, armed forces, etc.). Some of these are based at departmental research institutions, three military science and five military technology departments. They have a specialised focus, for example on weapons and ammunition or information technology and electronics. Researchers can also contact the BMVg, such as the BAAINBw, directly with ideas and research proposals.

|[93] For some of the institutions, demand-driven (contract) research certainly plays a role in research planning and prioritisation. The analysis of the WR has shown that thematic calls for proposals from federal ministries or funding organisations influence the focus of the work of universities, cf: WR (2019): Empfehlungen zur Weiterentwicklung der Friedens- und Konfliktforschung; Giessen, p. 70, https://www.wissenschaftsrat.de/download/2019/7827-19.

|[94] Political relevance and the desire to contribute to solving practical issues of conflict management and transformation characterise the selection of topics, cf. ibid., p. 35. Peace and conflict research is "engaged in knowledge transfer and is in close exchange with politics in particular, but also with organisations of the civil society." [unofficial translation] Ibid. S. 28.

(THW) and other aid and rescue organisations should also be involved. The Dialogue Forum should work closely with the National Platform (cf. C.III.3).

A Strategic Dialogue Forum involving the aforementioned stakeholders could help to fulfil the formulated claim of integrated security. Risk analyses and security policy scenarios could be developed as part of a German strategy cycle. On the basis of **multidisciplinary risk analyses**, medium and long-term perspectives for dealing with a constantly changing threat situation could be developed and research needs could be articulated on this basis. The UK, for example, has already gone down this path of integrated risk analysis and presented an updated report in 2023. [95]

On the basis of such a risk analysis, **security-relevant research needs** can be **identified and derived more systematically than at present**. The WR is convinced that research needs determined solely on the basis of departmental logic or the needs of companies or other stakeholders no longer do justice to the complex security situation. The recommended Strategic Dialogue Forum can develop possible future scenarios in a trusting exchange between the various stakeholders and using new technologies, and formulate research needs on this basis. Calls for proposals from the relevant ministries for research funding could be based on this joint needs assessment. Actors in the system of research and higher education can also orientate themselves on this. The WR recommends critically analysing the use of research funding to date and coordinating it more closely in future in order to adjust the focus of funding and, if necessary, the efficient use of funds.

The **composition of such a Dialogue Forum** needs to be reconsidered over time and adapted to the new situation. However, a certain degree of stability is also required in order to build sufficient trust in such a sensitive area. If a National Security Council is established, the Dialogue Forum should be linked to it. As a first step, the National Platform could support the establishment of the Dialogue Forum. The WR is aware that an exchange within the framework of the Dialogue Forum with regard to the issues of external defence or the development of a resilient critical infrastructure can only take place in a protected space in order to avoid exposing capability gaps on the German side or creating new vulnerabilities.

Other European countries have already developed corresponding instruments to regularly update their risk analyses in the sense of a **strategic cycle** and to be able to react promptly as part of their own national security strategy. The Neth-

[95] Cf. https://www.gov.uk/government/publications/integrated-review-refresh-2023-responding-to-a-more-contested-and-volatile-world/integrated-review-refresh-2023-responding-to-a-more-contested-and-volatile-world.

erlands has already gone through several such cycles and developed a sophisticated methodology that is considered a model for other countries. [96] In the United Kingdom, for example, the National Security Council (NSC) coordinates such an approach, which addresses the areas of defence, security, resilience, diplomacy, development and trade as well as economic, science and technology policy. The implementation of the objectives is continuously monitored and evaluated. [97]

The WR recommends that in future, the **funds made available** at German and European level **for security-relevant research** should be **used in a targeted and strategic manner** – if possible on the basis of consultations in a Strategic Dialogue Forum. If the establishment of such a Dialogue Forum requires longer preparations, the WR recommends setting up an interdepartmental ad hoc group on a transitional basis to prepare initial funding decisions in an advisory capacity. Such a strategic dialogue should not only lead to a systematic identification of research needs, but should also take a more binding view than before of the role of the state as a consumer of security-relevant innovations, so that funding and research activities can be more closely linked to demand (cf. also C.IV.2). [98]

IV.2 Integrative and systemic approach to security-relevant research

Research in security-relevant fields often follows historically evolved sub-areas of research and is also distributed among different actors. For example, the **BMVg** is primarily funding **military research and development** with around 3.6 billion euros in 2024 (cf. Table 1 in Annex 2). [99] It should be noted here that a large part from the special fund (Sondervermögen) of around 2 billion euros was

[96] Cf. https://fourninesecurity.de/2023/03/09/ein-anfang-nicht-das-ende-die-nationale-sicherheitsstrategie-als-auftakt-eines-regelmaessigen-strategiezyklus.

[97] The Integrated Review 2021 (IR2021) “set the UK’s overarching national security and international strategy, bringing together defence, security, resilience, diplomacy, development and trade, as well as elements of economic, and science and technology (S&T) policy.” Building on this, an update (Refresh, IR2023) was carried out in 2023, which emphasised a “greater integration of IR2023 into the Government Planning and Performance Framework (GPPF)”. “As set out in IR2021, this requires long-term cultural change so the Government is able to navigate a much more challenging operating environment. The IR strategic cycle will therefore require ongoing commitment from senior leaders across the national security community to strengthening culture, diversity and inclusion.” https://www.gov.uk/government/publications/integrated-review-refresh-2023-responding-to-a-more-contested-and-volatile-world/integrated-review-refresh-2023-responding-to-a-more-contested-and-volatile-world. Cf. also HM Government (2021): Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy, https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy.

[98] In the European Defence Fund, funding measures are awarded both with and without procurement intent, cf. https://germany.representation.ec.europa.eu/news/europaischer-verteidigungsfonds-12-milliarden-euro-fur-innovationen-und-bessere-2023-03-30_de.

[99] These are target expenditures by the Federal Government in research and development in the BMVg’s portfolio, cf. https://www.datenportal.bmbf.de/portal/en/K1/chart-1.1.4.html.

used for the development and testing of combat aircraft and battle tanks. [100] A small proportion of around 50 million euros of the special fund was used for military contract research [101] and a further 668 million euros for military development and testing – over and above the projects specifically mentioned. [102] A further 565 million euros were spent on military research and technology in the sense of contract research from the budget and around 216 million euros for military technology development and testing, which is linked to the intention to procure and prototype development. [103] This expenditure does not only include funding for research projects at higher education institutions, research institutions and companies; it also includes basic funding of research institutions amounting to around 178 million euros, which includes several institutes of the German Aerospace Centre (DLR), [104] of the Fraunhofer-Gesellschaft (FhG) [105] and the French-German Research Institute of Saint-Louis (ISL). [106]

No comparable, reliable figures are available for **non-military security-relevant research**. As described above, this field cannot be clearly delimited. [107] There are specific programmes that support activities in this area. One example is the framework programme "Research for civil security", which was first launched by the former Federal Ministry of Education and Research (BMBF) in 2007; it was continued in the fourth programme phase in 2024 under the title "Research for civil security – working together for a safe life within a resilient society". Since the start of the programme, "more than 520 research projects with over 2,200 sub-projects have been funded" (as of 2024), which corresponds

[100] In addition to the approx. 668 million euros that have been channelled from the special fund into military technology development and testing, further investments have been made in the development of the Multi-Role Combat Aircraft (MRCA) (target 2024: approx. 114 million euros), the Eurofighter weapon system (target 2024: approx. 897 million euros), the Main Ground Combat System (MGCS) (target 2024: approx. 84 million euros) and the Next Generation Weapon Systems (NGWS) in a Future Combat Air System (FCAS) (target 2024: 516 million euros). Cf. Federal Ministry of Finance (BMF) (2024): Bundeshaushaltsplan 2024, Einzelplan 14. Bundesministerium der Verteidigung; Berlin, p. 74, p. 77 and p. 80, https://www.bundeshaushalt.de/static/daten/2024/soll/epl14.pdf.

[101] Cf. ibid, p. 73.

[102] Cf. ibid., p. 74.

[103] Cf. ibid, pp. 44 & 47.

[104] Cf. DLR Programme Coordination for Security and Defence Research, https://www.dlr.de/en/research-and-transfer/security/civil-security-research-and-dual-use.

[105] Cf. Fraunhofer Segment for Defence and Security (VVS), https://www.vvs.fraunhofer.de/en/members.html.

[106] Cf. Wissenschaftliche Dienste des Deutschen Bundestages (2024): Wehrtechnische Forschung in ausgewählten Ländern. Finanzen, Verantwortlichkeiten, Verfahren; Berlin, p. 5, https://www.bundestag.de/resource/blob/1032720/4ec2c18ad1aa3ee397241bf58e418947/WD-2-050-24-pdf.pdf.

[107] Cf. also the WR's study on peace and conflict research in Germany, which also includes parts of security research. Staffing levels and third-party funding refer to the years 2017 and 2018, cf: WR (2019): Empfehlungen zur Weiterentwicklung der Fiedens- und Konfliktforschung; Giessen, esp. Annex 2, p. 117, https://www.wissenschaftsrat.de/download/2019/7827-19.

to a total funding volume of around 915 million euros. Additional funding totalling 165 million euros came from industry itself. [108] The background to this is that practical partners such as the fire brigades, police, THW and other aid and rescue organisations are involved in around half of the projects. As part of its “Maritime Sicherheit” programme, the former Federal Ministry for Economic Affairs and Climate Protection (BMWK) funded security-relevant research, for example with the “Echtzeittechnologien für die Maritime Sicherheit” programme, which is aimed at companies. [109] The German Foundation for Peace Research also supports projects in security and defence policy fields. [110] A few years ago, the Agentur für Innovation in Cybersicherheit GmbH, or Cyberagentur for short, was also founded. Its mission is to promote ground-breaking innovations in the field of cyber security – especially for the needs of internal and external security. [111]

In its previous evaluations, the WR has already found that the **research funds that have flowed into the BMVg’s departmental research institutions have in many cases** been used **neither effectivly nor efficiently**. Deficits can be observed in various respects: (1) with regard to unclear and very lengthy procurement processes, [112] (2) with regard to the recruitment and deployment of scientific personnel, [113] (3) with regard to the necessary infrastructure – up to WLAN access [114] – and (4) with regard to the efficient utilisation of research infrastructures such as research vessels. [115] One reason for this lies in the organisation of

[108] [unofficial translation] https://www.sifo.de/sifo/de/programm/zahlen-und-fakten/zahlen-und-fakten-zum-sicherheitsforschungsprogramm.html?nn=248276, an English version of the publication can be found here: https://www.sifo.de/sifo/en/home/home_node.html.

[109] Cf. https://www.bmwk.de/Redaktion/DE/Textsammlungen/Technologie/Schluesseltechnologien/research-development-innovation-in-the-maritime-economy.html.

[110] Cf. https://bundesstiftung-friedensforschung.de/.

[111] Cf. https://www.cyberagentur.de/en/cyberagentur/.

[112] One example of this is the Bundeswehr Institute of Preventive Medicine, which “can only use the existing equipment from the previous facilities and cannot procure, maintain and regenerate equipment for the new tasks. For this reason, two laboratories [...] planned when the centre was founded have not yet been set up and measuring devices and systems and IT equipment have not yet been acquired. So far, it has not been possible to clarify which superior body can remedy this deficit. It is essential that a solution to this problem is found at a higher level. The procurement processes are cumbersome and lengthy.” [unofficial translation] WR (2022): Stellungnahme zum Institut für Präventivmedizin der Bundeswehr (InstPrävMedBw), Andernach; Cologne, p. 63, https://doi.org/10.57674/14pe-fn68.

[113] For example, the WR found that the “Federal Office of Personnel Management of the Bundeswehr [...] occasionally assigned unsuitable technical personnel to the Institute for experimental laboratory work”, [unofficial translation] so that it was recommended that the Institute be given more say and selection rights, cf. WR (2020): Stellungnahme zum Institut für Pharmakologie und Toxikologie der Bundeswehr (InstPharmToxBw), Munich; Cologne, p. 12, https://www.wissenschaftsrat.de/download/2020/8521-20.

[114] For example, the Bundeswehr Institute of Pharmacology and Toxicology lacks high-performance, up-to-date Internet access, cf. ibid., pp. 13 & 64.

[115] Due to a lack of personnel, research vessels are not fully utilised, as the WR stated in its statement on the Wehrtechnische Dienststelle für Schiffe und Marinewaffen, Maritime Technologie und Forschung (WTD 71), Eckernförde, as recently as 2022, cf: Stellungnahme zur Wehrtechnischen Dienststelle für Schiffe und Marinewaffen, Maritime Technologie und Forschung (WTD 71), Eckernförde; Cologne, p. 13 & 64, https://doi.org/10.57674/y345-ca97.

the procurement process. [116] In view of these diverse deficits, the WR believes that in many cases the structural prerequisites for scientific activities at a high level and at high speed are lacking. [117] The impression is that the current players in the field are unable to carry out the required research as quickly as is now necessary.

The WR therefore strongly recommends strengthening and networking the high-performing and high-profile actors and expanding the circle of players involved in security-relevant research. By expanding the circle of players, the **existing potential and synergies in the diverse German scientific landscape, namely the higher education institutions**, can also be **better utilised**. This is associated with a cultural change that also affects society as a whole (cf. D). The available funds should be used wisely by (1) considering the entire breadth and diversity of security-relevant research and addressing it in funding, (2) focussing on efforts to integrate the field and (3) substantially increasing innovative strength in a broad, not just technological sense.

The WR sees it as a task of the **Strategic Dialogue Forum** to interlink strategic research planning with the three aforementioned objectives on the basis of the multidisciplinary risk analyses. In this way, the urgent **security-relevant problems** can be dealt with in a comprehensive and integrated manner and the resources can be utilised efficiently and effectively. In the following, the WR focuses on strategic and structural innovations that aim to integrate the field and subsequently lead to innovations in a broad sense, not just in the technological sense.

1 – **Promote integration of the scientific field**: The WR **notes** with **concern that the different fields of security-relevant research in Germany** operate **in separate arenas**. Boundaries are essentially historical and not, or only to a limited extent, based on the subject matter. It can already be observed that in the course of the scientific development and professionalisation of peace and conflict research, there has been an increasing opening towards security policy research, so that these two perspectives are clearly converging again. [118]

[116] With regard to the Centre for Geoinformation Systems, the WR noted that the "process for applying for funds for equipment and materials from the Federal Office of Bundeswehr Equipment, Information Technology and In-Service Support (BAAINBw) [...] is so lengthy and complex that it can happen that [an institution] [...] no longer receives the required equipment during the term of the project for which it is needed. Contracts with extramural contractors [...] are also often subject to long delays." [unofficial translation] WR (2019): Stellungnahme zum Zentrum für Geoinformationswesen der Bundeswehr (ZGeoBw), Euskirchen; Cologne, p. 12, https://www.wissenschaftsrat.de/download/2019/7489-19. Comparable observations were also made in the course of the evaluation of other departmental research institutions of the BMVg.

[117] Cf. the summary assessment of the Bundeswehr Geoinformation Centre as an example: ibid., p. 13.

[118] Today, it is more a question of different focal points and, to a large extent, complementary approaches. While security research is often characterised by "a stronger focus on military forms of security", peace research focuses on "civilian crisis management and more fundamental questions of order." [unofficial translation] Daase, C.; Deitelhoff, N.; Geis, A. (2024): Wer hat uns verraten? Friedens- und Sicherheitsforschung in

This integration of the field should be both self-organised and strategically supported by funding measures. The WR considers it essential to make the knowledge and data available in the broad field, which have been obtained from different sources and in different research contexts, accessible and more closely interlinked. This can be promoted within the framework of established formats such as calls for proposals. In other fields, such as biodiversity and climate research, structures have already been developed that contribute to the **systematic integration of knowledge and data**. Special structures have been created for this purpose: In so-called **synthesis centres**, scientists – with the support of IT expertise – bring together their disparate bodies of knowledge and data in order to appropriately analyse complex topics such as climate or even security from a systemic perspective. This type of collaboration is particularly fruitful in physical meetings. However, other virtual formats are also conceivable.

In synthesis centres, experts from different disciplines bring together their data and results in the sense of an advanced meta-analysis. To this end, they work together in one place for a limited period of time, for example several times a year for a week. Data experts support the researchers to bring together the disparate data and knowledge from the various research fields and disciplines. The existing 14 **synthesis centres** from Australia, China, Europe, North and South America joined together in 2013 to form an informal network, the **International Synthesis Consortium (ISC).** |[119] Six of the synthesis centres are in the USA, one in Germany and another is planned in Germany. |[120]

2 – **Set up innovation hubs**: Numerous higher education institutions and research institutes are already making a significant contribution to gaining knowledge in security-relevant research issues – even in militarily relevant areas. However, research activities that may also be aimed at military deployment pose **challenges** for higher education institutions and research facilities insofar as **strict security standards** must **be adhered to or created**. These include precautions in the buildings (e. g. access control), in the computer infrastructures

Kriegszeiten, in: Geis, A.; Deitelhoff, N.; Masala, C. (eds.): Der russische Angriffskrieg gegen die Ukraine und die Internationale Beziehungen, Sonderheft der Zeitschrift für Internationale Beziehungen (zib), 31 (2), 82-105, here p. 86, https://doi.org/10.5771/0946-7165-2024-2-82. “The sharp contrast between positive and negative peace and the commitment to a broad concept of structural violence had the same identity-forming significance for critical peace research as the adherence to a narrow concept of security and the idea of structural anarchy for security research. As a result, the cooperation paradigm was neglected in security research for a long time and the preoccupation with war, the military and arms control was viewed with suspicion in peace research.” [unofficial translation] Ibid., here p. 90.

| [119] Cf. the network of existing synthesis centres with their different models: https://synthesis-consortium.org/.

| [120] There has long been a synthesis centre in the field of biodiversity, https://www.idiv.de/de/forschung/sdiv-synthesis-centre/. Other centres, known as the Synthesis and Solutions Labs of the Senckenberg Society for Nature Research (SGN), are currently being founded. They are to become the “first location of a transdisciplinary synthesis centre in Germany” [unofficial translation], WR (2022): Stellungnahme zum Antrag auf strategische Erweiterung der Senckenberg Gesellschaft für Naturforschung (SGN), Frankfurt am Main, großer strategischer Sondertatbestand im Rahmen der Ausführungsvereinbarung; Cologne, p. 56, https://doi.org/10.57674/530t-ps77.

(e. g. physically separate networks, data security, measures to recognise data manipulation) and in the staff (e. g. security checks on personnel). More intensive cooperation with institutions experienced in these areas, such as the FhG or the DLR, can help to meet the security challenges.

However, in order to do justice to the speed of technological and global political developments, the diversity of the threat situation and strategic requirements, the WR recommends the **establishment of several innovation hubs** in Germany. They should be characterised by a flexible and dynamic way of working. Such hubs must be managed in an entrepreneurial manner and should be supported in the long term, but not institutionally. Different perspectives and expertise should be brought together here in a separate organisational unit. Researchers from different backgrounds, including doctoral students, as well as practice partners, contribute their knowledge and do research on a topic together.

The aim is to use the hubs **to establish** a **creative space that** must extend **from research to innovation and application** and in which results can be achieved quickly. Strategic considerations go hand in hand with technological developments. The hubs can also take on an **incubator function**. The support services required for this should be provided. These include access to the necessary technology, (research) infrastructures and protected communication technology. In addition to technical equipment, specialised support also plays a role in concept development and the preparation of business plans. This promotes positive spillover effects – be it into the civilian sector or the military sector. |[121]

The WR sees **great potential** in the establishment of **innovation hubs** with regard to strategic issues of external security and the development of internal resilience. Such hubs, which are not solely focussed on technological developments, should be promoted at different locations, possibly with different thematic focuses. |[122] Innovation hubs contribute to the development and provision of strategic knowledge on emerging security-relevant technologies (e. g. quantum technology) for politics and society. They also help to **structurally bridge** the critical phase in the innovation process from development to market innovation, the **"valley of death"** |[123], which can often be observed in Germany and Europe. This enables scientists to find suitable partners for the further development or validation of their results. The practice partners mentioned above are desirable and of particular importance for implementation. This is because

| [121] Ilzetzki, E. (2025): Guns and Growth: The Economic Consequences of Defence Buildups, in: Kiel Report No. 2, Kiel Institute for the World Economy, p. 38, https://www.ifw-kiel.de/publications/guns-and-growth-the-economic-consequences-of-defense-buildups-33747/.

| [122] Boris Pistorius has announced the establishment of an innovation centre in Erding: https://www.bmvg.de/en/news/pistorius-innovation-night-muenchner-sicherheitskonferenz-5889354.

| [123] Cf. European Investment Bank (EIB) (ed.); European Commission (2024): fi-compass ERDF [European Regional Development Fund]. ERDF Equity financial instruments. Factsheet; Luxembourg, p. 22, https://www.fi-compass.eu/library/how-to/erdf-equity-financial-instruments.

direct interaction in such a hub can significantly improve joint orientation in terms of harmonising innovation supply and demand. However, further instruments of innovative procurement are also required. These include innovation partnerships as well as pre-competitive procurement. The term "Staat als Ankerkunde" [124] refers to a strategy in which the state plays an active role in the promotion and development of certain economic sectors or technologies. It does this by acting as an important client or customer for companies in these areas. In this way, the public sector supports companies, in particular start-ups, with the aim of accelerating innovation and strengthening competitiveness in strategically important areas. This can take place primarily in key technologies such as aerospace. As a separate organisational unit, the innovation hubs can be designed in such a way that they meet the necessary standards of knowledge security and confidentiality requirements for militarily relevant projects.

In the hubs, **representatives of security-relevant research from different institutions** should **work together for a period of time from a systemic perspective** – for example, on a temporary secondment from a higher education institution or research organisation. Only the structure and a basic level of operational staff would be provided. The WR strongly recommends that the political, legal, social and cultural science aspects of security research should also be included. An exclusive focus on technological research and development work falls short of the mark.

In this way, researchers from very different contexts can enter into a highly dynamic process. The close and focussed cooperation should increase the **speed of innovation**. [125] The security standards that currently prevail at individual FhG or DLR institutes can also be ensured in hubs. Funding should be coordinated across the various departments. In the hubs, systemic issues can be addressed in a special way. These range from the development of new technologies for modern (hybrid) warfare and the development of resilience concepts at regional or national level up to innovative strategic responses to the multitude of armed and cold conflicts.

The WR considers it essential to view research and development in a **European context**. The funding and organisation of security-relevant research is currently

[124] "State as anchor customer" [unofficial translation] Cf. Weber, T.; Süssenguth, F. (2024): Innovationsfähigkeit in der Zeitenwende (acatech IMPULS), published by acatech - National Academy of Science and Engineering; Munich, p. 64, https://doi.org/10.48669/aca_2024-14.

[125] The lack of innovation speed was recently criticised once again: Despite the announced transformative change of direction, this had been implemented far too slowly. "This slowness results equally from prioritisation and coordination deficits as well as implementation deficits." EFI (2025): Gutachten zu Forschung, Innovation und Technologischer Leistungsfähigkeit Deutschlands; Berlin, p. 24, https://www.e-fi.de/fileadmin/Assets/Gutachten/2025/EFI_Gutachten_2025_30125.pdf. An executive summary of the report can be found here: https://www.e-fi.de/fileadmin/Assets/Gutachten/2025/EFI_Summary_2025_17.pdf.

developing at a rapid pace at European level. | [126] It is not yet possible to predict exactly what impact these changes will have. While the Horizon Europe funding programme has so far focused exclusively on civilian projects, the European Defence Fund (EDF) should be dedicated to defence research and its applications. These clear boundaries are no longer to be expected in the future. However, it has always been possible to fund security-relevant research in the broad sense used here within the framework of Horizon Europe, for example for the "Civil Security for Society" cluster. | [127] The WR strongly recommends that science policy actors, funding organisations and researchers seek, support and use joint European solutions in line with the position paper.

| [126] A "Hub for Defence Innovation (HEDI)" has been established at European level for military research and development "to foster innovative solutions for military capabilities", https://dirs.be/edas-hub-for-defence-innovation-hedi/.

| [127] https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe/cluster-3-civil-security-society_en.

D. Outlook on the consequences for the system of research and higher education

It was emphasised at the outset that the observable global political developments in conjunction with the enormous dynamics of emerging technologies will change the practice and governance of the system of research and higher education. As for society as a whole, the system is also facing an **intensive debate** on how **new priorities and orientations** can and should be set **to create a secure society that is resilient both internally and externally in the face of limited resources**. The WR is in favour of this debate being conducted in higher education institutions and research institutes in particular. The question of the appropriateness of civil clauses for academic institutions should also be explicitly discussed. After all, the latter are places where teachers and students can and should engage in such discourse in public or in the protected space of academic teaching.

The debate must **not focus on Germany alone**. Ultimately, security and resilience can only be achieved in a wider context, especially in cooperation with the various European partner countries. This applies to both central objectives of the position paper: effective protection against knowledge risks is better achieved in coordination with European partners or other partners that pursue a rules-based liberal order both in their own country and worldwide. The quality and effectiveness of security-relevant research can be increased if cooperation across institutional and national borders is encouraged and promoted – particularly in light of the recommendation to integrate research more closely and align it systemically.

The **strategies and measures** proposed here for dealing with knowledge risks and promoting security-relevant research **should** be **reviewed at regular intervals for their effectiveness and efficiency**. The experience gained and the results of such a review should be used to adapt and further develop them. A key aspect of the evaluation should be the effort required on the part of researchers and institutions. Standards and bureaucratic processes can quickly develop a life of their own, so that they become a burden for many organisations without leading to the desired results – such as the effective identification of security risks in research projects or exchange projects.

Furthermore, it is already becoming apparent that this change in dealing with knowledge risks and security-relevant scientific work will have **far-reaching effects** on the system of research and higher education – including the self-image of researchers, teachers and students and, above all, with regard to work for military purposes. Against the background of the different experiences gained to date, the WR emphasises three exemplary effects:

1 – **Shifts in the global network of science**: In future, international networks will develop in a different way. **Quality and innovative strength alone will not determine the attractiveness of scientific partners**. Genuinely political motives will also play a role in their choice, as was observed at the onset of Russia's war of aggression against Ukraine. The scientific organisations have supported and implemented the ban on cooperation with Russian actors. These changes have an impact on the recruitment and selection of international staff, especially young staff, as well as on travel restrictions for scientists. They may lose access to their research subjects or these may be restricted. These are just some of the possible consequences, the effects of which are not yet foreseeable, for the actions of scientific actors in an international context

The global system of scientific cooperation is also an element of diplomatic cooperation. It should not be overlooked that the conditions have changed in such a way that this evolved system of international scientific cooperation can be exploited both for unwanted influence at home and beyond our national borders. |[128] The WR therefore considers it necessary to quickly recognise these consequences with the aim of developing a **new understanding of science diplomacy**. To this end, dialogue should be sought at European level. It is important to bear in mind that non-state actors such as large, globally active technology companies are increasingly using science diplomacy to pursue their own interests, which may well diverge from those of national governments. |[129] The challenge is to see scientific cooperation, which – as formulated at the beginning (cf. A) – is more necessary than ever in order to tackle major societal challenges,

| [128] Cf. The Royal Society; American Association for the Advancement of Science (AAAS) (2025): Science diplomacy in an era of disruption; London, p. 5, https://royalsociety.org/-/media/about-us/international/science-diplomacy/science-diplomacy-in-an-era-of-disruption.pdf.

| [129] Cf: The Royal Society; AAAS (2025): Science diplomacy in an era of disruption; London, https://royalsociety.org/-/media/about-us/international/science-diplomacy/science-diplomacy-in-an-era-of-disruption.pdf. The big companies "[are] using science diplomacy to conduct their own equivalent of 'statecraft' in support of their company's objectives, which may be distinct from those of any national government", ibid., p. 5.

as an opportunity to exchange ideas and build mutual trust – especially in protracted conflict situations. The aim should by no means be to simply cut off such lines of cooperation.

With a view to Europe, the system of research and higher education can continue to contribute to strengthening the links between the different European countries. The decisive factor here is that all **players in the system of research and higher education** – individual researchers, scientific institutions and scientific organisations as well as the political level – see it as **their responsibility** to **take the European dimension into account in their actions**. Scientific activities and science policy initiatives help to build trust in the European area and to better coordinate their actions.

2 – **Further development of the reputation system**: **Reputation** is the decisive currency in the system of research and higher education. It is regarded as an **indication of high-quality scientific achievements and controls attention as well as receptiveness** in the scientific system. |[130] It also contributes significantly to the recognition of a person, group or organisation in other social contexts and can be converted into resources (budget, positions, equipment).

Reputation is linked to the underlying evaluation regime, in which the number and quality of **publications** as well as the amount of competitively acquired **third-party funding** often play **a key role**. If publication of research results in security-relevant areas is not possible for good reasons, this can therefore have a negative impact on the reputation and career opportunities of the individual. To mitigate this problem, in the USA, for example, there are confidential peer-reviewed journals for work from the security-relevant areas of the National Laboratories. However, such an approach is not feasible for the relatively manageable system of research and higher education in Germany, and probably not in Europe. It could possibly be realised within the framework of a European Defence Union (EDU) currently under discussion. |[131]

Attempts to **further develop** the **assessment system** have been underway for some time at German level, for example by the DFG, and at European level. The vision formulated by the Coalition for Advancing Research Assessment (CoARA) |[132] of valuing the different formats of scientific activities in their quality and with their various effects is more important than ever in this field. If

|[130] Cf. fundamentally on reputation in science: Luhmann, N. (1990): Die Wissenschaft der Gesellschaft; Frankfurt a. M. And critically further: Schimank, U. (2010): Reputation statt Wahrheit: Verdrängt der Nebencode den Code?, in: Soziale Systeme 16 (2010), Heft 2, pp. 233-242, https://doi.org/10.1515/sosys-2010-0204. Schimank speaks of a “quantification of reputation” [unofficial translation], ibid., p. 235.

|[131] The EDU is intended to complement NATO and strengthen Europe’s strategic autonomy. It aims to achieve closer military cooperation and integration within the EU. This should not only lead to a coordinated defence strategy, but also to support for research and development in the defence sector (European Defence Fund).

|[132] Cf. https://coara.eu/.

young scientists cannot rely on an appropriate assessment regime, they will not be enthusiastic about such work in the medium and long term.

Reputation systems are only developing very slowly. There needs to be a **change in awareness on the part of the evaluators**. In the engineering sciences, work in an industrial company – combined with scientific activities – counts as an achievement in a CV. Similarly, activities in innovation hubs or other protected locations should be explicitly taken into account in the assessment – also in appointment procedures or in the course of awarding funding. If necessary, other ways should be sought to assess a person and their performance. In any case, work that does not lead to publications or only to a lesser extent needs to be appropriately recognised. In addition, the WR suggests developing new instruments such as specific prizes to incentivise work in security-relevant areas and in places such as the innovation hubs mentioned above.

3 – **Review of open science policies**: Exchange, cooperation and innovation succeed best under conditions of openness. Sharing knowledge, infrastructures, methods, etc. as early and as widely as possible – even beyond academic circles – has long been seen as a guarantee for the dynamic development of science and society. For this reason, **an open science policy has been demanded and promoted in science policy in recent decades**. Germany has committed itself to Open Access and supports the UNESCO recommendation [133] in principle, without having developed a national Open Science strategy. Such a policy does not imply a completely free flow of knowledge and data. There are good reasons for not sharing certain findings immediately or in full with others, for example to protect the legitimate interests of researchers and research institutions if they wish to exploit their knowledge commercially.

Against the backdrop of international developments, the concrete **implications of the formula "as open as possible, as closed as necessary"** should be **considered once again**. In Germany, the Nationale Forschungsdateninfrastruktur e. V. (NFDI) could be a forum for such reflection, particularly with regard to the handling of data. In view of the intensifying competition between systems, the WR believes that such a reflection is necessary not only at German level, but also at European level. The aim should be to agree in future on what it means to proceed openly in a controlled and managed manner.

[133] Cf. United Nations Educational, Scientific and Cultural Organisation (UNESCO); Canadian Commission for UNESCO (2022): An introduction to the UNESCO Recommendation on Open Science; Paris, https://doi.org/10.54677/XOIR1696. According to UNESCO, scientific knowledge should be as open as possible. However, restrictions are also justified under certain conditions, including national security: "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." Ibid., p. 11, https://doi.org/10.54677/XOIR1696. And https://www.unesco.org/en/open-science; on the situation in Germany: German Commission for UNESCO (2020): Open Science. Perspektiven aus Deutschland auf die Erarbeitung der geplanten Empfehlung der UNESCO; Bonn, https://www.unesco.de/themen/wissenschaft/open-science/.

The WR is convinced that an open and free system of research and higher education, as it is currently practised in Germany and most European countries, is a value in itself. As outlined at the beginning (cf. A.II), its knowledge creates a basis for overcoming the complex challenges of our time and at the same time acts as an independent and critical authority vis-à-vis claims to power by the state, but also by other players such as large technology companies. In an international context, such a system is highly attractive to creative minds and can therefore represent a competitive advantage. The framework conditions for this, such as promising career paths, sufficient and sovereign research and data infrastructures as well as attractive study programmes, must be right. The WR also believes that **the public sector** has a **responsibility to shape and promote the system of research and higher education in such a way that science and humanities can continue to fulfil this fundamental function for a free society in the future**. Everyone benefits from an open and free system of research and higher education in which knowledge security is guaranteed and security-relevant research is carried out for the protection and resilience of society: from individual citizens to a prosperous economy and a stable democratic society.

Appendix

APPENDIX 1: QUESTIONS TO EXPLAIN KNOWLEDGE RISK TYPES

In order to sensitise people to issues of knowledge security and the security relevance of scientific work, the WR suggests systematically examining the five risk types mentioned (cf. B.III) using guiding questions. The following lists are not exhaustive and are to be understood solely as exemplary questions to explain the respective risk type.

Re 1: Undesirable transfer of knowledge and technology

_ Is there a significant technology and/or knowledge gap between the actors? Could closing this gap be the primary interest of the cooperation partner(s)?

_ Is the research the crown jewels [134] of an actor?

_ Is there a contractual cooperation agreement in which all stakeholders involved equally guarantee access to and use of the research data? Does this also include regulations on confidentiality, dissemination and publication?

_ In what way are existing IP rights, research data or confidential data of the project or previous projects made available to third parties (also in the sense of remote access) or shared? How are they protected?

_ Which buildings, information or internal networks will cooperation partners or guests have access to?

_ Can patentable or otherwise commercially relevant results be expected?

_ Does the research include so-called emerging technologies that could be exploited?

[134] The term “crown jewels” originates from the economic context. There, it refers to “particularly attractive assets of a company in terms of their current and potential future value”, [unofficial translation] https://www.gabler-banklexikon.de/definition/crown-jewels-56809. It is also increasingly being used in the context of science policy discussions, for example in the guidelines of the Netherlands, according to which it means: “the sensitive domains of knowledge within which your institution has built a reputation and within which research is conducted that is internationally recognised as excellent”, Contact Point for Knowledge Security of the Government of the Netherlands; the Universities of the Netherlands (VSNU); the Netherlands Federation of University Medical Centres (NFU) et al. (2022): National knowledge security guidelines. Secure international collaboration, p. 29, https://english.loketkennisveiligheid.nl/documents/publications/2022/04/07/national-knowledge-security-guidelines.

Re 2: Unwanted influence on the system of research and higher education

_ Is there a possibility that publication activities and the use of data will be restricted or hindered?

_ Do guests (academics, students, etc.) or cooperation partners pose risks that inappropriately influence the existing values and culture of the institution?

_ Are biometric, genetic or other data collected in the course of exchange and/or cooperation activities that are not in line with the values and standards of one's own organisation?

Re 3: Financial and scientific dependencies

_ Are there financial or material benefits (funding, scholarships, remuneration, equipment, etc.) that originate directly or indirectly (e. g. via companies) from countries classified as critical, and are these reported?

_ What is the financial involvement of the individual stakeholders and could this lead to an imbalance in terms of control and co-determination?

_ Are cooperation partners funded by government scholarship or funding programmes from abroad? What type of funding programme is involved (e. g. a malign foreign talent recruitment programme)?

Re 4: Interference of scientific activities with other areas of society

_ What are the concrete goals of the cooperation and what benefits does it bring for the cooperating institutions?

_ What goals could be pursued beyond scientific cooperation and what benefits does this bring for the cooperating country or company?

_ What are the symbolic implications of a scientific exchange, a scientific cooperation?

Re 5: Violation of research ethics or ethical principles

_ Could the research results be misused for unethical or immoral purposes?

_ Do all actors represent comparable academic values, ethical standards as well as fundamental and human rights?

_ Are all legal requirements and regulations complied with and supported by all stakeholders? This includes, for example, the provisions on export control or data protection.

_ Has a cooperation partner or a cooperating institution been accused, charged or convicted of illegal activities? This includes in particular fraud, extortion, espionage and corruption as well as theft of intellectual property, copyright infringements and patent theft, but also violations in the handling of goods under export control or other protection.

The WR is well aware that there are already elaborate review processes in which the identification of these risks has been incorporated. Reference should be made here to the "Manual for an assessment process: safeguarding science and scientific cooperation" published in mid-2024. [135]

[135] Cf. DLR Projektträger Safeguarding Science Team (2024): Due Diligence in Science. Manual for an assessment process: safeguarding science and scientific cooperation; Bonn, https://www.safeguarding-science.eu/wp-content/uploads/Due-Diligence-in-Science_Manual2024.pdf.

Table 1: Expenditure of the Federal Ministry of Defence on research and development and on military research and technology as well as development and testing, in million euros (as of March 2025)

	Research and development	Military research and development		Military development and testing*		Basic funding (DLR, FhG, ISL)
		Budget	Special fund	Budget	Special fund	
2015	916,6	346,4		361,4		116,5
2016	896,6	265,1		421,9		121,3
2017	1 174,8	477,6		463,4		121,3
2018	1 044,9	416,1		384,0		128,0
2019	1 314,2	525,4		527,5		*129,6*
2020	1 463,6	557,5		714,7		143,4
2021	1 762,1	564,4		825,2		145,1
2022	2 178,0	442,5	5,0	1 207,8		158,1
2023	1 870,4	320,4		*893,0*	*524,5*	*163,7*
2024	*3 600,7*	*565,0*	*49,8*	*215,5*	*2 277,6*	*178,1*

Sources: Research and development: https://www.datenportal.bmbf.de/portal/en/K1/chart-1.1.4.html; military research and technology and development and testing: https://www.bundeshaushalt.de/DE/Bundeshaushalt-digital/bundeshaushalt-digital.html, as well as basic funding (DLR, FhG, ISL) Federal budgets Section 14 for the years 2017-2024, e. g. https://www.bundeshaushalt.de/static/daten/2024/soll/epl14.pdf. *In addition to expenditure on development and testing, the special assets and the budget chapter on military research also include expenditure on the development (not procurement) of the Eurofighter weapon system, Multi-Role Combat Aircraft (MRCA), Main Ground Combat System (MGCS), Next Generation Weapon Systems (NGWS) in a Future Combat Air System (FCAS). Target figures are italicised.

Table 2: Basic funding of research institutes from Section 14, in million euros (as of March 2025)

	DLR	FhG	ISL
2015	31,1	64,3	21,1
2016	32,2	68,0	21,1
2017	32,6	67,6	21,1
2018	35,1	70,8	22,1
2019	36,5	71,0	*22,1*
2020	44,8	75,9	22,7
2021	45,1	76,7	23,3
2022	48,6	85,7	23,8
2023	*50,4*	*89,6*	*23,7*
2024	*61,6*	*89,4*	*27,1*

Funding for the French-German Research Institute of Saint-Louis (ISL) does not constitute a grant in accordance with Sections 23 and 44 of the Federal Budget Code (BHO). Instead, the basis for payment is the Franco-German State Treaty of 31 March 1958, which is supplemented annually by an intergovernmental supplementary agreement.

Source: Federal budget sections 14 for the years 2017-2024, e. g. https://www.bundeshaushalt.de/static/daten/2024/soll/epl14.pdf, target figures are italicised.

BAFA	Bundesamt für Wirtschaft und Ausfuhrkontrolle Federal Office for Economic Affairs and Export Control
BfV	Bundesamt für Verfassungsschutz German domestic intelligence services
BMFTR	Bundesministerium für Forschung, Technologie und Raumfahrt Federal Ministry of Research, Technology and Space
BMF	Bundesministerium für Finanzen Federal Ministry of Finance
BMVg	Bundesministerium der Verteidigung Federal Ministry of Defence
DAAD	Deutscher Akademischer Austauschdienst e. V. German Academic Exchange Service
DFG	Deutsche Forschungsgemeinschaft German Research Foundation
DLR	Deutsches Zentrum für Luft- und raumfahrt e. V. German Aerospace Centre
EFI	Expertenkommission Forschung und Innovation Commission of Experts for Research and Innovation
FhG	Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e. V.
GA	Gemeinsamer Ausschuss zum Umgang mit sicherheitsrelevanter Forschung Joint Committee on the Handling of Security-Relevant Research
GoF	Gain of function
ISL	Deutsch-Französisches Forschungsinstitut Saint-Louis French-German Research Institute of Saint-Louis
KEF	Kommissionen für Ethik sicherheitsrelevanter Forschung Committees for Ethics in Security-Relevant Research
AI	Artificial intelligence

KIWi	Kompetenzzentrum Internationale Wissenschaftskooperationen Centre for International Scientific Cooperation
NOAA	National Oceanic and Atmospheric Administration
TRL	Technology readiness level
WR	Wissenschaftsrat German Science and Humanities Council

Contributors

The following is a list of the people involved in the deliberations of the German Science and Humanities Council (WR) and the Research Committee, as well as the staff of the Head Office involved in the development process.

The drafts prepared by working groups and committees are discussed in the commissions of the WR during a one-step process and can also be changed if necessary. As a result, the WR is considered the author of the published recommendations, statements and position papers.

Members of the German Science and Humanities Council (as of May 2025)

Chair

Professor Dr Wolfgang Wick
Heidelberg University Hospital | German Cancer Research Center, Heidelberg (DKFZ)

Secretary General

Thomas May
WR Head Office

Scientific Commission of the WR

Professor Dr Jutta Allmendinger
Humboldt-Universität zu Berlin | Freie Universität Berlin

Professor Dr Julia C. Arlinghaus
Otto von Guericke University Magdeburg | Fraunhofer Institute for Factory Operation and Automation IFF, Magdeburg
Chair of the Scientific Commission

Professor Dr Liane G. Benning
Freie Universität Berlin | German Research Centre for Geosciences (GFZ) Potsdam

Dr Ulrich A. K. Betz
Merck KGaA

Professor Dr Folkmar Bornemann
Technical University of Munich

Professor Dr Eva-Lotta Brakemeier
University of Greifswald

Professor Dr Alena Michaela Buyx
Technical University of Munich

Professor Dr Petra Dersch
University of Münster

Professor Dr Nina Dethloff
University of Bonn

Professor Dr Jakob Edler
Fraunhofer Institute for Systems and Innovation Research ISI | Manchester Institute of Innovation Research

Professor Dr Christian Facchi
Technische Hochschule Ingolstadt

Professor Dr Christine Falk
Hannover Medical School

Professor Dr Uta Gaidys
Hamburg University of Applied Sciences

Professor Dr Michael Hallek
University of Cologne

Dr Frank Heinricht

Professor Dr Frank Kalter
University of Mannheim | German Center for Integration and Migration Research (DeZIM) e. V.

Dr Stefan Kampmann
Management consultant, Knetzgau

Professor Dr Wolfgang Lehner
Dresden University of Technology

Professor Dr Anne Lequy
Magdeburg-Stendal University of Applied Sciences

Andrea Martin
IBM DACH

Professor Dr Gabriele Metzler
Humboldt-Universität zu Berlin

Professor Dr Friederike Pannewick
University of Marburg

Professor Dr Ursula Rao
Max Planck Institute for Social Anthropology, Halle |
Leipzig University

Professor Dr Gabriele Sadowski
TU Dortmund University

Professor Dr Ferdi Schüth
Max-Planck-Institut für Kohlenforschung, Mülheim/Ruhr
Deputy Chair of the Scientific Commission

Dr Harald Schwager
EVONIK Leading Beyond Chemistry

Professor Dr Christine Silberhorn
Paderborn University

Professor Dr Thomas S. Spengler
Technische Universität Braunschweig

Professor Dr Birgit Spinath
Heidelberg University

Professor Dr Klement Tockner
Goethe University Frankfurt/Main | Senckenberg Society for Nature Research Frankfurt

Professor Dr Wolfgang Wick
Heidelberg University Hospital | German Cancer Research Center (DKFZ)
Chair of the WR

Professor Dr Oliver Zielinski
University of Rostock | Leibniz Institute for Baltic Sea Research Warnemünde

Administrative Commission (as of May 2025)

Members delegated by the Federal Government

N. N.
Federal Ministry of Research, Technology and Space

N. N.
Federal Ministry of Research, Technology and Space

N. N.
Federal Ministry of Finance

N. N.
Federal Ministry of the Interior

N. N.
Federal Ministry of Agriculture, Food and Regional Identity

N. N.
Federal Ministry for Economic Affairs and Energy

Members delegated by the federal state governments

Baden-Württemberg

Petra Olschowski
Minister of Science, Research and Arts

Bavaria

Markus Blume
Minister of State of Science and the Arts
Chair of the Administrative Commission

Berlin

Dr Ina Czyborra
Senator for Higher Education and Research, Health and Long-Term Care

Brandenburg

Dr Manja Schüle
Minister for Science, Research and Culture

Bremen

Kathrin Moosdorf
Senator for Environment, Climate and Science

Hamburg

Dr Andreas Dressel
President of the Ministry of Finance and Districts

Hesse

Timon Gremmels
Minister of Science and Research, Arts and Culture

Mecklenburg-Western Pomerania

Bettina Martin
Minister of Science, Culture, Federal and European Affairs

Lower Saxony

Falko Mohrs
Minister of Science and Culture

North Rhine-Westphalia

Ina Brandes
Minister of Culture and Science

Rhineland-Palatinate

Clemens Hoch
Minister for Science and Health

Saarland

Jakob von Weizsäcker
Minister of Finance and Science

Saxony

Sebastian Gemkow
Minister of State for Science in the State Ministry for Science, Culture and Tourism

Saxony-Anhalt

Professor Dr Armin Willingmann
Minister for Science, Energy, Climate Protection and the Environment
Deputy Chair of the Administrative Commission

Schleswig-Holstein

Dr Dorit Stenke
Minister for General Education and Vocational Training, Science, Research and Culture

Thuringia

Christian Tischner
Minister for Education, Science and Culture

Professor Dr Ferdi Schüth
Max-Planck-Institut für Kohlenforschung, Mülheim/Ruhr
Deputy Chair of the Scientific Commission of the WR
Chair of the committee

Professor Dr Julia C. Arlinghaus
Otto von Guericke University Magdeburg | Fraunhofer Institute for Factory Operation and Automation IFF, Magdeburg
Chair of the Scientific Commission of the WR

Deputy Director General Dr Christine Burtscheidt
Hessian Ministry of Science and Research, Arts and Culture

Professor Dr Jakob Edler
Fraunhofer Institute for Systems and Innovation Research ISI |
Manchester Institute of Innovation Research
Member of the Scientific Commission of the WR

Professor Dr Michael Hallek
University of Cologne
Member of the Scientific Commission of the WR

Professor Dr Wolfgang Lehner
Dresden University of Technology
Member of the Scientific Commission of the WR

Ministerial Councillor Dr Florian Leiner
Bavarian State Ministry of Science and the Arts

Ministerial Councillor Ralf Maier
Federal Ministry of Research, Technology and Space
(formerly Federal Ministry of Education and Research)

Professor Dr Gabriele Metzler
Humboldt-Universität zu Berlin
Member of the Scientific Commission of the WR

As guests:

Dr Svenja Gertheiss
Federal Ministry of Research, Technology and Space
(formerly Federal Ministry of Education and Research)

Ministerial Councillor Esther Seng
Federal Ministry of Research, Technology and Space
(formerly Federal Ministry of Education and Research)

Professor Dr Birgit Spinath
Heidelberg University
Member of the Scientific Commission of the WR

Professor Dr Wolfgang Wick
Heidelberg University Hospital | German Cancer Research Center, Heidelberg (DKFZ)
Chair of the WR

As external experts:

Professor Dr Volker Epping
Leibniz University Hanover

Professor Dr Michael Lauster
Fraunhofer Institute for Technological Trend Analysis INT, Euskirchen

Professor Dr Ursula Schröder
University of Hamburg

Dr Annette Barkhaus (deputy head of research department)

Miriam Betge (administrative officer)

Gudrun Hilles (administrative officer)

Dr Rainer Lange (head of research department)

Britta Philippsen (team assistant)

Leila Young (administrative officer)