

2025

Wissenschaft und Sicherheit in Zeiten weltpolitischer Umbrüche

Positionspapier

IMPRESSUM

Wissenschaft und Sicherheit in Zeiten weltpolitischer Umbrüche | Positionspapier

Herausgeber

Wissenschaftsrat
Scheidtweilerstraße 4
50933 Köln
www.wissenschaftsrat.de
post@wissenschaftsrat.de

Drucksachennummer: 2485-25

DOI: <https://doi.org/10.57674/9tr5-kn29>

Lizenzhinweis: Diese Publikation wird unter der Lizenz Namensnennung – Weitergabe unter gleichen Bedingungen 4.0 International (CC BY-SA 4.0) veröffentlicht. Den vollständigen Lizenztext finden Sie unter <https://creativecommons.org/licenses/by-sa/4.0/legalcode.de>.



Veröffentlicht

Köln, Mai 2025

INHALT

Vorbemerkung	5
Kurzfassung	6
A. Wissenschaftsfreiheit in Zeiten hoher Unsicherheit	9
A.I Krise der liberalen und regelbasierten Nachkriegsordnung	10
A.II Wissenschaftsfreiheit als wesentliches Element offener Gesellschaften	12
B. Konzepte und Analysen	15
B.I Sicherheit	16
B.II Sicherheitsrelevante Forschung	18
B.III Wissenssicherheit	23
B.IV Recht und Selbstverpflichtung	28
IV.1 Exportkontrolle	28
IV.2 Zivilklauseln	30
C. Empfehlungen zum Umgang mit Wissensrisiken und sicherheitsrelevanter Forschung	32
C.I Gemeinsame Verantwortung geteilt wahrnehmen	33
C.II Governance-Leitlinien für den Umgang mit Wissensrisiken und Sicherheitsrelevanz	35
C.III Wissensrisiken erkennen und managen	37
III.1 Fallbezogene Einzelprüfung und kollegialer Austausch	38
III.2 Strategische Leitungsaufgabe: Risikobetrachtung strukturell verankern	42
III.3 Nationale Plattform für Wissenssicherheit einrichten	44
C.IV Sicherheitsrelevante Forschung vorantreiben	50
IV.1 Sicherheitsrelevante Forschung strategisch planen	52
IV.2 Sicherheitsrelevante Forschung integrativ und systemisch anlegen	55
D. Ausblick auf die Folgen für das Wissenschaftssystem	64
Anhang	69
Anhang 1: Fragen zur Erläuterung von Wissensrisikotypen	69
Anhang 2: Finanzierung militärischer Forschung in Deutschland	72
Abkürzungsverzeichnis	73
Mitwirkende	75

Vorbemerkung

Gravierende Veränderungen der weltpolitischen Lage, der Umgang mit zahlreichen Unsicherheiten in der verteidigungspolitischen und ökonomischen Situation sowie die Entwicklung von Forschungsergebnissen und Technologien mit einem inhärenten Dual-Use-Potenzial stellen Deutschland, Europa und viele andere demokratische Staaten vor neue sicherheitspolitische Herausforderungen. Diesen Entwicklungen kann sich das Wissenschaftssystem nicht entziehen, mehr noch: Mit seinen Forschungs- und Lehrleistungen, seiner internationalen Vernetzung und seinen Beiträgen zu technologischen Entwicklungen und Innovationen trägt es wesentlich zur Bewältigung dieser Herausforderungen bei.

Diese Konstellation bedingt, dass sich das Wissenschaftssystem in Deutschland und Europa in einer bisher nicht gekannten Weise mit sicherheitsrelevanten Fragen auseinanderzusetzen hat – und zwar in zweifacher Hinsicht: Zum einen müssen Maßnahmen ergriffen werden, um das Wissenschaftssystem in angemessener Weise zu schützen und zugleich die Wissenschaftsfreiheit zu gewährleisten. Zum anderen tragen auch Akteure im Wissenschaftssystem Verantwortung, um zur Sicherheit und Resilienz einer offenen demokratischen Gesellschaft beizutragen. Mit diesem Papier entwickelt der Wissenschaftsrat eine Positionierung in zweifacher Hinsicht. Er erarbeitet Antworten auf die Frage, wie das Wissenschaftssystem gut geschützt werden kann, ohne einer unangemessenen Bürokratisierung von Forschung und Lehre Vorschub zu leisten. Und er entwickelt Antworten darauf, wie die unterschiedlichen Akteure im Wissenschaftssystem, die einzelnen Forschenden, die Leitungen wissenschaftlicher Einrichtungen, die Wissenschafts- und Förderorganisationen sowie die wissenschaftspolitische Ebene Verantwortung zum Schutz und zum Resilienzaufbau unserer Gesellschaft übernehmen können.

Bei der Erarbeitung der Empfehlungen haben Expertinnen und Experten mitgearbeitet, die nicht Mitglieder des Wissenschaftsrats sind. Auch der Bundesnachrichtendienst (BND) hat im Rahmen seines gesetzlichen Auftrages mitgewirkt. Ihnen ist der Wissenschaftsrat zu besonderem Dank verpflichtet. Ebenso dankt der Wissenschaftsrat weiteren Sachverständigen aus dem In- und Ausland, die für den Beratungsprozess in Gesprächen mit dem Ausschuss oder in Einzelgesprächen zur Verfügung standen. Der Wissenschaftsrat hat das Positionspapier am 9. Mai 2025 in Mainz verabschiedet.

Kurzfassung

Eine zunehmend konfrontative Sicherheitspolitik, die deutliche Zunahme sicherheitspolitischer Risiken und Bedrohungen sowie das Erstarken und die steigende Anzahl autokratischer Systeme lässt die **liberale regelbasierte Nachkriegsordnung erodieren**. Das westlich geprägte demokratische Modell hat sich global bisher nicht in erwartetem Maße durchgesetzt. Zugleich entwickeln Forschungsarbeiten und Technologien in einem steigenden Maße einen inhärenten Dual-Use-Charakter, nicht allein, aber besonders in Feldern wie der Bio- und Quantentechnologie oder der Künstlichen Intelligenz (KI). Über sehr gute bis exzellente Forschungskapazitäten in diesen avancierten Bereichen verfügen auch Staaten außerhalb des demokratischen Spektrums.

Der Wissenschaftsrat hat in seinem Positionspapier Empfehlungen **zum Umgang mit Wissensrisiken und zum Beitrag der Wissenschaft für den Schutz sowie den Aufbau einer resilienten Gesellschaft** entwickelt.

Beide Ziele sind von besonderer Bedeutung: Einerseits ist das Wissenschaftssystem aufgrund seiner Offenheit besonders vulnerabel, andererseits leistet es aufgrund seiner hohen Innovationskraft wesentliche Beiträge für die Sicherheit des Gemeinwesens. Allerdings ist es derzeit noch nicht in einem ausreichenden Maße auf diese Herausforderung und die damit verbundenen Aufgaben vorbereitet. **Deutschland hat hier in zweifacher Hinsicht Nachholbedarf.**

Sicherheit wird heute umfassend und integrierend verstanden – nicht allein im Sinne der Verteidigung äußerer Grenzen, sondern auch zum Aufbau von Sicherheit und Resilienz im Inneren. Sicherheitsrelevant ist damit Forschung, insofern sie zur Aufrechterhaltung der inneren und äußeren Sicherheit sowie zum Aufbau der Resilienz und Erhaltung der natürlichen Lebensgrundlagen des Gemeinwesens beiträgt und beitragen soll, diese jedoch auch gefährden kann. Im Wissenschaftssystem bedarf es sowohl einer **höheren Aufmerksamkeit für Wissenssicherheit** – ein Begriff, der im Positionspapier entwickelt wird – (vgl. B.III) als auch **für die Bedeutung sicherheitsrelevanter Forschung**.

Mit Blick auf Fragen der Wissenssicherheit sieht der Wissenschaftsrat im Sinne einer gestuften Zuständigkeit zunächst jede Wissenschaftlerin, jeden Wissenschaftler in der Verantwortung, die Risiken ihrer bzw. seiner eigenen Arbeiten realistisch einzuschätzen. Dazu bedarf es der Bereitstellung von ausreichenden Informationen und Unterstützungsstrukturen. Falls Zweifel bestehen, sollten

im nächsten Schritt gemeinsam mit anderen Forschenden oder einer/einem Beauftragten der Einrichtung fünf unterschiedliche Risikotypen, die der Wissenschaftsrat identifiziert hat (vgl. B.III), geprüft werden. Es liegt in der Verantwortung der Leitungen von Hochschulen und Forschungseinrichtungen, die dafür notwendige Unterstützung bereitzustellen. Der Wissenschaftsrat empfiehlt jeder Einrichtung, eine **schlanke, handhabbare und zugleich klare Risikobetrachtung zu erarbeiten und zu implementieren** (vgl. C.III.2). Je nach Risikoprofil und Größe der Einrichtung kann sie unterschiedlich ausgestaltet sein. Einrichtungsübergreifende Modelle sollten dabei geprüft werden.

Der Wissenschaftsrat empfiehlt, **zügig eine Nationale Plattform für Wissenssicherheit** (vgl. C.III.3) einzurichten, in der die unterschiedlichen wissenschaftlichen Akteure und politisch Verantwortlichen vertrauensvoll zusammenarbeiten. Subsidiär zu den bestehenden dezentralen Strukturen soll sie als One-Stop-Shop auf nationaler Ebene wissenschaftliche Akteure in der Einschätzung von Wissensrisiken unterstützen, indem sie als schlanke, rasch reagierende Einrichtung kompetent und möglichst umfassend Informationen für die Risikobetrachtung zur Verfügung stellt. Zugleich soll sie auf nationaler Ebene eine kohärente Positionierung erarbeiten und beratend breit in das Wissenschaftssystem hineinwirken.

Um die **sicherheitsrelevante Forschung** zu stärken, empfiehlt der Wissenschaftsrat, das **derzeit fragmentierte Feld** besser zu **integrieren** und **systemische Forschungsansätze** gezielt zu **fördern**. Die Integration kann selbstorganisiert gelingen, sollte aber möglichst über Förderlinien und die Einrichtung eines Synthesezentrums (vgl. C.IV.2) gezielt unterstützt werden. Mit einer solchen systemischen und integrierten Sichtweise ist auch ein Kulturwandel nicht allein im engeren Feld der sicherheitsrelevanten Forschung, sondern im gesamten Wissenschaftssystem verbunden. Der Wissenschaftsrat empfiehlt, diesen Diskurs auch in den Hochschulen und Forschungseinrichtungen mit allen Beteiligten zu führen.

In den nächsten Jahren werden voraussichtlich deutlich **mehr Mittel für sicherheitsrelevante Forschungs- und Entwicklungsarbeiten** eingesetzt werden. Um das effektiv und effizient tun zu können, muss ein deutlich **breiteres Spektrum an Akteuren** im System adressiert werden. Nur so können ein systemisches Vorgehen gestärkt und die Synergien im bestehenden Wissenschaftssystem gehoben werden. Für die einzelnen Einrichtungen sind damit Herausforderungen hinsichtlich einzuhaltender Sicherheitsstandards zu bewältigen, insbesondere bei Arbeiten, die auf einen militärischen Einsatz zielen. Darüber hinaus bedarf es angesichts der sich zuspitzenden sicherheitspolitischen Lage Strukturen, in denen mit hoher Geschwindigkeit geforscht und entwickelt werden kann – bis hin zu Innovationen, die technologischer, strategischer und sozialer Natur sein sollten. Auch hier kommt es auf das Zusammenführen der unterschiedlichen

8 Perspektiven an. Der Wissenschaftsrat empfiehlt dazu die Einrichtung von **Innovation Hubs** (vgl. C.IV.2).

Andere Länder haben bereits Prozesse der multiperspektivischen Risikoanalyse entwickelt. In Deutschland sollte ein **Strategisches Dialogforum** etabliert werden, das, sofern es zur Einrichtung eines **Nationalen Sicherheitsrats** kommt, dort angesiedelt werden sollte. Ein solches Forum kann einen Strategiezyklus aufsetzen und basierend auf den regelmäßig aktualisierten Risikoanalysen in systematischer Form auch den notwendigen Forschungsbedarf artikulieren.

Der Wissenschaftsrat empfiehlt den politischen Akteuren, angesichts vergleichbarer Herausforderungen und Chancen innerhalb Europas die hier angeregten Anstrengungen eng im Austausch mit der EU und anderen europäischen Partnern voranzutreiben. So können Potenziale und Synergien – sowohl hinsichtlich des Umgangs mit Wissensrisiken wie auch zur Förderung sicherheitsrelevanter Forschung – besser ausgeschöpft werden.

Die hier skizzierten Entwicklungen und empfohlenen Veränderungen werden das Wissenschaftssystem in Deutschland und Europa deutlich verändern. Der Wissenschaftsrat hebt ausdrücklich den **hohen Wert der Wissenschaftsfreiheit** hervor, der es erfordert, dass alle Akteure im System sich ihrer Verantwortung zur Aufrechterhaltung von Wissenssicherheit im wissenschaftlichen Arbeiten bewusst sind und bereit sind, zur Sicherheit und zur Resilienz des Gemeinwesens beizutragen.

A. Wissenschaftsfreiheit in Zeiten hoher Unsicherheit

Das Wissenschaftssystem in Deutschland ist mit herausfordernden Entwicklungen auf europäischer und weltpolitischer Ebene konfrontiert. Seit mehreren Jahren lassen sich eine zunehmend **konfrontative Sicherheitspolitik** und eine massive Steigerung an Gewaltkonflikten beobachten. Dazu zählt auf weltpolitischer Ebene aktuell zum Beispiel der Angriffskrieg Russlands gegen die Ukraine, die Verschärfung des Konflikts zwischen der Volksrepublik China und Taiwan sowie die eskalierenden Krisen im Mittleren und Nahen Osten. | ¹ Zugleich sehen sich Deutschland und Europa heute mit einem breiten Spektrum sicherheitspolitischer Risiken konfrontiert, die bis in den Alltag der Menschen hinein unsere offene und demokratische Gesellschaft direkt herausfordern. Zentral dafür sind Szenarien hybrider Kriegsführung im Sinne der Kombination aus unterschiedlichen Bedrohungen vor allem in wirtschaftlicher, medialer und cybertechnischer Hinsicht. Hinzu kommen gravierende sicherheitspolitische Ungewissheiten angesichts des 2025 vollzogenen politischen Führungswechsels in den Vereinigten Staaten von Amerika und der damit verbundenen Implikationen für die Zukunft Europas und der NATO.

Gleichzeitig sind **wissenschaftliche Kooperation und Austausch** – auch über Systemgrenzen hinweg – **notwendiger denn je**, um globale Herausforderungen erforschen und Lösungsstrategien erarbeiten zu können. Ohne eine wissenschaftliche Zusammenarbeit lässt sich der schnell voranschreitende Klimawandel nicht bewältigen. Letzterer verlangt wie andere große gesellschaftliche Herausforderungen, z. B. die Ernährungssicherheit, mehr statt weniger internationale Zusammenarbeit. In der Kombination stellen diese globalen Trends das deutsche, auf Kooperation ausgerichtete, offene Wissenschaftssystem vor große neue Aufgaben.

| ¹ Weltweit gesehen lässt sich ein Höchststand an Kriegen und Gewaltkonflikten beobachten. Die jüngste Konflikttrendsanalyse auf der Grundlage des Uppsala Conflict Data Programm (UCDP) am Department of Peace and Conflict Research der Universität Uppsala zeigt 2023 den höchsten Stand an staatlich organisierten Konflikten seit 1946, vgl. <https://ucdp.uu.se/>. Für eine detaillierte Analyse vgl. Rustad, S. A. (2024): Conflict Trends: A Global Overview, 1946–2023; Oslo, <https://www.prio.org/publications/14006>. Alle Weblinks in diesem Positionspapier wurden zuletzt am 06.05.2025 abgerufen.

Hinzu kommt, dass einige Staaten außerhalb des demokratischen Spektrums über exzellente Forschungs- und Entwicklungskapazitäten verfügen, die für Forschende aus Deutschland und Europa hoch attraktiv sind. Zuvorderst strebt China seit einer guten Dekade die globale Dominanz in strategischen Wissenschafts- und Technologiefeldern an. |² Zugleich weisen immer mehr **Forschungsarbeiten und Technologien einen inhärenten Dual-Use-Charakter** auf, so dass sicherheitsrelevante Fragen sowie Fragen der technologischen und wirtschaftlichen Souveränität in einem hohen Maß sicherheitspolitische Implikationen bergen. Dies betrifft insbesondere, aber nicht allein Felder wie etwa Quanten- und Biotechnologie oder KI, die sich zudem mit einer enormen Dynamik entwickeln.

Zur Illustration der sicherheitsrelevanten Aspekte unterschiedlicher wissenschaftlicher Arbeiten finden sich im Positionspapier Beispiele für aktuelle Entwicklungen. Sie zeugen davon, dass sich **wissenschaftliche Akteure in einem Spannungsfeld zwischen Wissenschaftsfreiheit und Sicherheit bewegen. Die Balance zwischen den beiden Polen gilt es neu zu verhandeln.** Das Positionspapier entwickelt Leitlinien, Strategien und Strukturen für einen Umgang damit.

A.1 KRISE DER LIBERALEN UND REGELBASIERTEN NACHKRIEGSORDNUNG

Nach dem Ende des Kalten Kriegs dominierte in der westlichen Welt die Erwartung, dass auch weitere autokratisch regierte Länder den Weg hin zu demokratischen Gemeinwesen mit einer Marktwirtschaft einschlagen würden. Wissenschaftliche Kooperationen sollten den Prozess der Öffnung unterstützen und letztlich die Entwicklung hin zu liberalen Demokratien befördern. Allerdings hat sich diese Erwartung als **Fehleinschätzung** erwiesen. Heute sehen sich offene Gesellschaften gefordert, ihr grundlegendes Paradigma, dass sich das **westlich geprägte demokratische Modell mittel- oder langfristig durchsetzen** werde, zu überprüfen. |³

| ² Schon 2008 hat China im Law of the People's Republic of China on Progress of Science and Technology (§ 6) dargelegt, dass Technologien sowohl militärisch als auch zivil eingesetzt werden sollen. Auch soll entsprechend geforscht werden, vgl. 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>. Mit dem National Intelligence Law von 2017 wird die staatliche Steuerung deutlich, vgl. China Law Translate (2017): PRC National Intelligence Law; <https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/>.

| ³ Die dominante Erwartung nach dem Fall der Mauer war, dass auch autokratisch regierte Länder „were all on an inevitable path toward 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 organizations (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

Vielmehr lässt sich derzeit eine **Erosion der liberalen und regelbasierten Weltordnung** beobachten, verbunden mit einer **Stärkung autokratischer Kräfte** in verschiedenen Staaten. |⁴ Die liberale Nachkriegsordnung und das System der Vereinten Nationen befinden sich in einer tiefen Krise. Diese Entwicklungen schreiten mit hoher Geschwindigkeit voran. Offene Gesellschaften haben viele Stärken – auch mit Blick auf ihre Resilienz im Krisenfall. Allerdings ist ihr auf Wissenschaftsfreiheit beruhendes Wissenschaftssystem in mehreren Dimensionen möglichen Angriffen ausgesetzt: auf der Ebene des Wissens selbst hinsichtlich Zugänglichkeit und Qualität, auf der Ebene der Wissenschaftlerinnen und Wissenschaftler als Personen, auf der Ebene der Funktionsfähigkeit des Systems und auf der Ebene seiner Rolle und Verankerung in der Gesellschaft. Diese unterschiedlichen Dimensionen werden in der Folge unter dem Begriff der Vulnerabilität zusammengefasst. Mehr noch: Die **Anstrengungen** der letzten Jahrzehnte, sich international wissenschaftlich auszutauschen und **global über Systemgrenzen hinweg zusammenzuarbeiten, haben die Verletzlichkeit deutlich erhöht**. Gerade über lange Zeit gewachsene Kooperationen und persönliche Beziehungen können die Einsicht von Wissenschaftlerinnen und Wissenschaftler in die geänderte Situation und die damit notwendig gewordenen Veränderungen be- oder gar verhindern.

Und umgekehrt sieht sich die Gesellschaft angesichts neuester Technologien Gefahren und Risiken ausgesetzt, die ohne Rückgriff auf wissenschaftliches Wissen nicht zu bewältigen sind. Die **Entwicklungen im digitalen Raum** als „neuer, hybrider Einflussbereich“, in dem die „Grenzen zwischen wirtschaftlich und politisch motivierter Cyberaggression verschwimmen“ |⁵, sind hier von besonderer Brisanz. Dieser Raum wird nicht allein von Straftaten mit finanziellen Interessen (Cyber Crime) bedroht, sondern auch von staatlich gelenkten Angriffen mit ideologischem, politischem oder militärischem Hintergrund (Cyber Conflict) ebenso wie von großen Technologieunternehmen über digitale Produkte, die

underpinning these efforts.“ Baykal, A.; Benner, T. (2020): Risky Business: Rethinking Research Cooperation and Exchange with Non-Democracies. Strategies for Foundations, Universities, Civil Society Organizations, and Think Tanks; Berlin, S. 4, <https://gppi.net/2020/10/22/rethinking-research-cooperation-and-exchange-with-non-democracies>.

|⁴ Die Rede ist von einer „Autokratisierungswelle“, vgl. Nord, M.; Lundstedt, M.; Altmann, D. et al. (2024): Democracy Report 2024: Democracy Winning and Losing at the Ballot; Gothenburg, S. 6, https://www.v-dem.net/documents/43/v-dem_dr2024_lowres.pdf. Weltweit lässt sich ein solcher Trend des Abbaus und der Erosion demokratischer Rechte und Institutionen anhand bestimmter Indikatoren zeigen. So leben mittlerweile 38 % der Weltbevölkerung – 3,1 Mrd. Menschen – in Autokratien in Unterschied zu den 80er und 90er Jahren des letzten Jahrhunderts, in der weniger als 5 % in solchen Regimen lebten. Vgl. Nord, M.; David Altman, F.; Angiolillo, et al. (2025): Democracy Report 2025: 25 Years of Autocratization – Democracy Trumped?; Gothenburg, S. 20, <https://www.v-dem.net/publications/democracy-reports>. Vgl. auch Ikenberry, G. (2018): The end of liberal international order?, in: International Affairs, 94 (1), S. 7-23, <https://doi.org/10.1093/ia/iix241>.

|⁵ 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>.

Als Beispiel sei hier auf KI-Methoden für die Aufdeckung und Beseitigung von Softwareschwachstellen in Betriebssystemen von WLAN-Routern, Smartphones und Laptops hingewiesen. Ein Forschungsprojekt hat es ermöglicht, automatische Abwehrmaßnahmen zu entwickeln, gleichzeitig aber auch Schwachstellen in zahlreichen Geräten, die keiner regelmäßigen Kontrolle und Aktualisierung unterliegen, zu identifizieren und auszunutzen. So wurde das Software-Paket „WannaLaugh“ – als Gegenentwurf zum bösartigen „WannaCry“ – entwickelt, um Angriffe mit Ransomware, also Erpresserangriffe, durchzuführen und zu analysieren, ohne tatsächlichen Schaden zu verursachen oder schädliche Software zu verbreiten. Allerdings kann auch dieses Werkzeug selbst zur Zielscheibe werden und wie jede andere Software missbraucht werden. So könnte beispielsweise der vermeintliche Schadcode Schwachstellen in WannaLaugh ausnutzen und schädliche Aktionen ausführen, sodass es letztlich doch für Erpresserangriffe genutzt werden könnte. |⁷

A.II WISSENSCHAFTSFREIHEIT ALS WESENTLICHES ELEMENT OFFENER GESELLSCHAFTEN

Wissenschaftsfreiheit ist völkerrechtlich verankert |⁸ und bildet in vielen demokratischen Ländern einen zentralen Wert, auch wenn sich in den letzten Jahren global und regional der Grad an Wissenschaftsfreiheit vielerorts besorgniserregend verschlechtert hat. Entwicklungen wie Kriege und bewaffnete Konflikte können ganze Hochschulsysteme zerstören; Forschende können aufgrund ihrer Arbeiten oder politischen Ansichten aus dem akademischen System entlassen oder gar verhaftet werden. Solche Entwicklungen zerstören die Bedingungen für freie Wissenschaft. Die Gestaltung von Lehrplänen unterliegt in Ländern wie

|⁶ Ebd.

|⁷ Vgl. hierzu auch: Gemeinsamer Ausschuss zum Umgang mit sicherheitsrelevanter Forschung (GA) von Deutscher Forschungsgemeinschaft (DFG) und Nationale Akademie der Wissenschaften Leopoldina (2024): Wissenschaftsfreiheit und Sicherheitsinteressen in Zeiten geopolitischer Polarisierung – Fünfter Tätigkeits- und Sachstandsbericht; Berlin, S. 73, <https://www.sicherheitsrelevante-forschung.org/publikation-taetigkeitsbericht2024/>. Vgl. auch Brundage, M.; Avin, S.; Clark, J. et al. (2018): The malicious use of artificial intelligence: forecasting, prevention, and mitigation, S. 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 Abs. 3, https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-3&chapter=4&clang=_en.

Russland, Nicaragua, China, aber zum Teil auch in den USA politischen Eingriffen. Die **Wissenschaftsfreiheit** ist daher **weltweit** betrachtet **unter Druck** geraten. |⁹

Deutschland gehört zu den wenigen Ländern, in denen ein sehr hohes Maß an Wissenschaftsfreiheit gewährleistet ist. Ein Grund dafür ist, dass **Wissenschaftsfreiheit in Deutschland verfassungsrechtlich verankert** ist. |¹⁰ Sie gehört zu den wenigen Grundrechten, die keinem Gesetzesvorbehalt unterliegen. Einschränkungen der Wissenschaftsfreiheit kann es in Deutschland allein aus Gründen geben, die aus der Verfassung selbst stammen, „überwiegend aus anderen Grundrechten oder aus demselben Grundrecht anderer Wissenschaftler“. |¹¹ Auf *individueller Ebene* wird der oder dem Einzelnen Wissenschaftsfreiheit zugesichert – unabhängig von der Zugehörigkeit zu einer wissenschaftlichen Einrichtung. Auf *organisationaler Ebene* gilt sie für Forschungseinrichtungen |¹² und Hochschulen, ohne an einen bestimmten Organisationstypus von Hochschule gebunden zu sein. |¹³ Für die deutsche Verfassung ist eine weitere spezifische Bedeutung von Relevanz, nämlich das Verständnis von **Wissenschaftsfreiheit als Funktionsgrundrecht**. |¹⁴ Dies bedeutet, dass

|⁹ Vgl. die neueste Ausgabe des The Academic Freedom Index. In seinem Update 2025 wurden 34 Länder und Gebiete identifiziert, „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>, und vgl. Free to think: 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 Abs. 3 GG: „(3) Kunst und Wissenschaft, Forschung und Lehre sind frei. Die Freiheit der Lehre entbindet nicht von der Treue zur Verfassung.“ Grundgesetz für die Bundesrepublik Deutschland vom 23. Mai 1949 (BGBl. S. 1), zuletzt geändert durch Artikel 1 des Gesetzes zur Änderung des Grundgesetzes (Artikel 93 und 94) vom 20. Dezember 2024 (BGBl. I Nr. 439): Artikel 9 Absatz 3, <https://www.bundestag.de/parlament/aufgaben/rechtsgrundlagen/grundgesetz#>.

|¹¹ Dieter Grimm (2021): Wissenschaftsfreiheit als Funktionsgrundrecht, in: Berlin-Brandenburgische Akademie der Wissenschaften (Hrsg.): Wissenschaftsfreiheit in Deutschland. Drei rechtswissenschaftliche Perspektiven. Reihe Wissenschaftspolitik im Dialog, Nr. 14/2021, S. 17-23, hier S. 23, <https://edoc.bbaw.de/frontdoor/index/index/searchtype/series/id/13/start/4/rows/20/yearfq/2021/docId/3445>. Sog. verfassungsimmanente Schranken, Bundesverfassungsgericht, BVerfGE 47, 327 (368ff), <https://www.servat.unibe.ch/tools/DfInfo?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/rs20160217_1bvl000810.

|¹² Für den außeruniversitären Bereich bedeutet dies, dass dieser – trotz einer bisher noch nicht vorliegenden Entscheidung aus Karlsruhe und unabhängig von der privatrechtlichen Organisation – dem Grundrechtsschutz verpflichtet ist, sofern er überwiegend vom Staat finanziert wird; vgl. Dieter Grimm (2021): Wissenschaftsfreiheit als Funktionsgrundrecht, in: Berlin-Brandenburgische Akademie der Wissenschaften (Hrsg.): Wissenschaftsfreiheit in Deutschland. Drei rechtswissenschaftliche Perspektiven. Reihe Wissenschaftspolitik im Dialog, Nr. 14/2021, S. 17-23, hier S. 22 f., <https://edoc.bbaw.de/frontdoor/index/index/searchtype/series/id/13/start/4/rows/20/yearfq/2021/docId/3445>.

|¹³ Als Hintergrund sei darauf verwiesen, dass das Urteil im Zuge der Auseinandersetzungen um die sogenannte Gruppenuniversität erarbeitet wurde. Wörtlich heißt es: „Die Garantie der Wissenschaftsfreiheit hat weder das überlieferte Strukturmodell der deutschen Universität zur Grundlage, noch schreibt sie überhaupt eine bestimmte Organisationsform des Wissenschaftsbetriebs an den Hochschulen vor.“ BVerfGE 35, 79 (79), <https://www.servat.unibe.ch/tools/DfInfo?Command=ShowPrintVersion&Name=bv035079>.

|¹⁴ Vgl. Dieter Grimm (2021): Wissenschaftsfreiheit als Funktionsgrundrecht, in: Berlin-Brandenburgische Akademie der Wissenschaften (Hrsg.): Wissenschaftsfreiheit in Deutschland. Drei rechtswissenschaftliche

auf *systemischer Ebene* der Staat die Aufgabe hat, „einen funktionierenden Sach- und Wirkungsbereich unabhängiger Wissenschaft“ |¹⁵ zu gewährleisten, um den ständig wachsenden Wissensbedarf der Gesellschaft zu befriedigen und zugleich eine „kritische Distanz zu den gesellschaftlichen (und staatlichen) Interessen und Machtansprüchen“ |¹⁶ zu schaffen.

Wenn der Staat aus sicherheitspolitischen Gründen der Wissenschaft gegenüber neue Erwartungen entwickelt, bleibt er in seiner **Doppelrolle**, insofern er als potenzieller Gefährder von Wissenschaftsfreiheit Eingriffe unterlassen sollte (*Freiheit vom Staat – Abwehrrecht*) und gleichzeitig als Garant der Freiheit die Bedingungen dafür zu schaffen hat, dass Wissenschaftsfreiheit im Sinne des Funktionsrechts realisiert werden kann (*Freiheit durch den Staat – Gewährleistungsrecht*).

Angesichts sich verstärkender Systemkonkurrenzen und der damit verbundenen sicherheitsrelevanten Herausforderungen betont der Wissenschaftsrat, dass die **Balance zwischen Wissenschaftsfreiheit und berechtigten Einschränkungen** durch verfassungsrechtlich geschützte Güter, namentlich andere Grundrechte, stets **auszutariert** ist. Für die einzelne Wissenschaftlerin, den einzelnen Wissenschaftler besteht eine „Pflicht zum Mitbedenken“ |¹⁷ allein im Sinne einer im Einzelfall zu treffenden Abwägung grundgesetzlich verankerter Werte, nicht bezogen auf alle gesellschaftlichen Folgen. Damit ist es verfassungsrechtlich nicht ausgeschlossen, dass Hochschulleitungen grundsätzlich Selbstreflexionsprozesse und Risikobetrachtungen etablieren. Der Wissenschaftsrat versteht sein Positionspapier als einen Beitrag im Zuge eines erneuten Austarierens dieser Balance angesichts globaler sicherheitsrelevanter Herausforderungen.

Perspektiven. Reihe Wissenschaftspolitik im Dialog, Nr. 14/2021, S. 17–23, hier S. 21, <https://e-doc.bbaw.de/frontdoor/index/index/searchtype/series/id/13/start/4/rows/20/yearfq/2021/docId/3445>.

| ¹⁵ Britz, G. (2013): Freiheit der Wissenschaft, in: Dreier, H. (Hrsg.): Grundgesetz. Kommentar Band I, Artikel 1–19; Tübingen, S. 792–838.

| ¹⁶ Hailbronner, K. (1979): Freiheit der Forschung und Lehre als Funktionsgrundrecht; Hamburg, S. 156, zitiert nach Häberle, P. (1986): Besprechungen. Kay Hailbronner: Freiheit der Forschung und Lehre als Funktionsgrundrecht, in: Archiv des öffentlichen Rechts, 111 (1), S. 165–170, hier S. 170, <https://www.jstor.org/stable/44308941>.

| ¹⁷ BVerfGE 47, 327 (377 f.), <https://www.servat.unibe.ch/tools/DfInfo?Command=ShowPrintVersion&Name=bv047327>.

B. Konzepte und Analysen

Schutz und Verteidigung offener demokratischer Gesellschaften und die Erhöhung ihrer **Resilienz** zur Bewältigung unabsehbarer Entwicklungen sind zu zentralen Herausforderungen geworden. Resilienz einer Gesellschaft meint die Fähigkeit, auf unerwartete Krisen und Schocks nicht nur reagieren, sondern sich aktiv anpassen und sich entsprechend verändern zu können, um die eigene Handlungs- und Funktionsfähigkeit zu erhalten und weiterzuentwickeln. Während Schutz, Verteidigung und Prävention auf die Verhinderung absehbarer negativer Entwicklungen zielt, stellen resiliente Gesellschaften sich zudem darauf ein, „Nichterwartbares [zu] erwarten.“ |¹⁸

Im **Wirtschaftssektor** spielen dabei Aspekte wie **wirtschaftliche Stärke, technologische Souveränität und Wissensschutz** eine wichtige Rolle. Denn Spionage und Sabotage sowie Datendiebstahl richten allein in Deutschland einen hohen wirtschaftlichen Schaden von mehr als 250 Mrd. Euro jährlich an, rund zwei Drittel aufgrund von Cyberattacken. |¹⁹ Wissensintensive Unternehmen schützen sich daher schon länger vor Wissensabfluss, Beeinflussung von außen und anderen Risiken. Staatliche Ziele wie technologische Souveränität und wirtschaftliche Unabhängigkeit erlauben im Rechtsrahmen des Grundgesetzes in

| ¹⁸ Ulrich Bröckling hat auf den Begriff der Resilienz als ein Schlüsselkonzept unserer Zeit verwiesen, vgl. Bröckling, U. (2017): Resilienz. Über einen Schlüsselbegriff des 21. Jahrhunderts, in: Soziopolis – Gesellschaft beobachten, hier S. 3, <https://www.ssoar.info/ssoar/handle/document/80731>. Für eine Rekonstruktion der Geschichte des Begriffs „Resilienz“ bis hin zum aktuellen politischen Diskurs vgl. auch Szöllösi-Janze, M. (2024): Resilienz. Zur Geschichte eines allgegenwärtigen Begriffs – Thesen zu den Herausforderungen einer modernen Zeitgeschichte, in: Vierteljahrshefte für Zeitgeschichte, 72 (3), S. 559–589, <https://doi.org/10.1515/vfzg-2024-0030>.

| ¹⁹ Vgl. Finsterbusch, S.; Sachse, M.: Hacker greifen aus China deutsche Unternehmen an, in: FAZ, 28.08.2024, <https://www.faz.net/aktuell/wirtschaft/mehr-wirtschaft/china-warum-hacker-gerade-von-dort-aus-deutsche-unternehmen-angreifen-19947534.html>. Dem Artikel liegen Ergebnisse des Bitkom e. V. zugrunde, vgl. Bitkom e. V. (2024): Wirtschaftsschutz 2024; Berlin, <https://www.bitkom.org/sites/main/files/2024-08/240828-bitkom-charts-wirtschaftsschutz-cybercrime.pdf>. Auch das Wissenschaftssystem ist von Cyberattacken betroffen: In den Jahren 2022 bis 2024 sind dem Bundeskriminalamt (Stand 19. Juni 2024) 42 Cyberangriffe auf Hochschulen und Wissenschaftseinrichtungen bekannt geworden, welche teilweise zu hohen finanziellen Schäden führten, vgl. Deutsche Bundesregierung (Drucksache 20/12259, 10.07.2024): Deutscher Bundestag (2024). Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion der CDU/CSU – Drucksache 20/11830 – Cyberangriffe auf Wissenschaft und Forschung in Deutschland, S. 3 f., <https://dip.bundestag.de/vorgang/cyberangriffe-auf-wissenschaft-und-forschung-in-deutschland/313002>. „Die festgestellten Schäden reichen von Ausfällen der Hochschul-Website über zeitweise Beeinträchtigungen von IT-gestützten Diensten und Hochschulangeboten, dem Ausleiten von Daten bis hin zu großflächigen Verschlüsselungen von IT-Servern und längerfristigen Ausfällen.“ Ebd., S. 8.

der Regel keine Einschränkungen der Wissenschaftsfreiheit. Daher werden diese Fragen hier nur am Rande adressiert.

Die Herausforderungen der Wissenssicherheit und der Sicherheitsrelevanz von Forschung verlangen Veränderungen der Praxis und Governance des Wissenschaftssystems sowie des Selbstverständnisses insbesondere von Lehrenden sowie Forschenden, aber auch von Studierenden. Diese Anpassungen sind von hoher Dringlichkeit, denn das **Wissenschaftssystem** ist **besonders vulnerabel**, weil es als **offenes System** in Demokratien ein begehrtes und vielfach noch leicht zugängliches Ziel etwa für ungewollten Wissensabfluss oder unerwünschte Einflussnahme ist. Zugleich tragen Forschungsaktivitäten wesentlich dazu bei, die Gesellschaft vor Angriffen von außen und innen zu schützen sowie ihre Resilienz zu stärken.

Vor diesem Hintergrund wird im Folgenden ein **erweitertes Sicherheitskonzept und ein breites Verständnis von Sicherheitsrelevanz in der Wissenschaft** zugrunde gelegt. In einem ersten Schritt werden die Begriffe Sicherheit, sicherheitsrelevante Forschung und Wissenssicherheit genauer beschrieben, um aufbauend auf dieser Klärung und der damit verbundenen Analyse Empfehlungen zu entwickeln.

B.1 SICHERHEIT

Mit der Moderne wird es als zentrale **Aufgabe des Staates** verstanden, die **Sicherheit** der Menschen, ihrer Lebensgrundlagen, ihrer Güter und auch der zentralen politischen Werte **zu gewährleisten**. |²⁰ Was allerdings genau unter Sicherheit zu verstehen ist, wird in Gesellschaften immer wieder neu ausgehandelt und ist auch abhängig von subjektivem Empfinden. |²¹ In der letzten Dekade lässt sich eine deutliche Veränderung beobachten. Noch zu Beginn des 21. Jahrhunderts standen Vulnerabilitäten etwa durch Naturkatastrophen und Terroranschläge im Vordergrund. Sicherheit zu gewähren, zielte auf zuverlässig funktionierende Infrastrukturen einer global vernetzten Gesellschaft: von

| ²⁰ Seit dem 17. Jahrhundert entwickelte sich die „positive Idee der Sicherheit“ als erstrebenswerter Zustand des Gemeinwesens, den zu „gewährleisten der neuzeitliche Staat beansprucht bzw. von ihm gefordert wird. Nicht mehr dieses oder jenes Gut, dieser oder jener Verkehrsweg, oder das Leben dieser oder jener Person gilt es, vor bestimmten Gefahren zu schützen, vielmehr soll die Herrschaft das gesamte Gebiet, auf das sie sich erstreckt, schützen.“ Kaufmann, F.-X. (2015): Sozialstaat als Kultur; Bonn, S. 280, https://doi.org/10.1007/978-3-531-94244-5_11.

| ²¹ „Sicherheit in politisch-sozialen Kontexten lässt sich nicht abstrakt definieren [...], sondern wird in Gesellschaften und von Gesellschaften als Orientierungs- und Handlungshorizont immer wieder neu bestimmt, und zwar nicht zuletzt über die Identifikation von Unsicherheit, von Bedrohungen oder Gefährdungen. Sicherheit, respektive Unsicherheit, ist gesellschaftlich und kulturell und damit auch im historischen Prozess variabel.“ Conze, E. (2023): Sicherheit. Wert, Fiktion und Versprechen, in: Saam, N. J.; Heiner, B. (Hrsg.): Die Idee der Freiheit und ihre Semantiken. Zum Spannungsverhältnis von Freiheit und Sicherheit; Bielefeld, S. 51–68, hier S. 55, <https://doi.org/10.1515/9783839461884-004>.

Versorgungsketten bis zu Kommunikationssystemen. Insbesondere mit dem Angriffskrieg Russlands auf die Ukraine rücken Fragen der äußeren Sicherheit, das heißt des Schutzes von Leben und Freiheit angesichts kriegerischer Auseinandersetzungen oder Bedrohungen, auch in Deutschland wieder in den Fokus. Zugleich wird auch dieser Aspekt von Sicherheit durch den Begriff der hybriden Kriegsführung, der auch nicht-militärische Formen von Gewaltausübung als Mittel der zwischenstaatlichen Konfliktaustragung begreift, selbst entgrenzt. In der Sicherheitsstrategie der Bundesregierung von 2023 wird **Sicherheit umfassend und integrierend verstanden** als „Schutz vor Krieg und Gewalt; als Freiheit, unser Leben im Rahmen unserer freiheitlichen demokratischen Grundordnung zu gestalten; als Sicherung unserer Lebensgrundlagen“. |²²

Angesichts der sich mit hoher Geschwindigkeit verändernden weltpolitischen Lage, ihrer schon jetzt sichtbar werdenden Konsequenzen für die gesellschaftliche Bedrohungslage sowie der technologischen Entwicklungen stehen demokratisch gewählte Regierungen derzeit unter verstärktem Druck, die Sicherheit ihrer Bürgerinnen und Bürger zu gewährleisten. Heute muss der Staat zunehmend andere gesellschaftliche Akteure einbeziehen, um diese Aufgabe erfüllen zu können. **Alle gesellschaftlichen Bereiche** müssen sich **mit dieser Herausforderung auseinandersetzen**, auch das Wissenschaftssystem. Zudem lässt sich eine solche Aufgabe nur bewältigen, wenn Abstimmung, Koordinierung und Vernetzung innerhalb und über die unterschiedlichen politischen, wirtschaftlichen und gesellschaftlichen Bereiche hinweg deutlich verbessert wird. Diese Abstimmungs-, Koordinierungs- und Vernetzungsprozesse müssen bis auf europäischer Ebene erfolgen.

Schutzziel ist die **Erhaltung der freiheitlich demokratischen Grundordnung unseres Gemeinwesens** – einschließlich ihrer Voraussetzungen. Für die Verteidigung dieses Ziels sind nicht allein äußere Bedrohungen von Relevanz. Die Verteidigung nach außen hängt mit dem Schutz sowie dem Aufbau von Resilienz im Innern zusammen. Denn Resilienz zielt auf die Fähigkeit einer Gesellschaft, mit komplexen Auswirkungen nicht absehbarer Krisen oder Schocks – einschließlich all ihrer befürchteten Schäden – flexibel umzugehen sowie diese Erfahrungen in Innovationen zu transformieren. Resiliente Gesellschaften, so die Erwartung, sind für eine unabsehbare und unsichere Zukunft besser gerüstet.

Das **Wissenschaftssystem** ist ein Teil der Gesellschaft, der in Abstimmungs-, Koordinierungs- und Vernetzungsprozesse zur Gewährleistung von Sicherheit zu integrieren ist. Wissenschaft spielt dabei **in mehrfacher Hinsicht eine besondere Rolle**. Zunächst treibt sie eine Vielzahl von Entwicklungen voran, die sowohl die Sicherheit gefährden als auch dazu beitragen können, Sicherheit und

| ²² Auswärtiges Amt (2023): Wehrhaft. Resilient. Nachhaltig. Integrierte Sicherheit für Deutschland: Nationale Sicherheitsstrategie; Berlin, S. 19, <https://www.nationalesicherheitsstrategie.de/>.

Resilienz im Inneren und nach außen zu schaffen. So kann informationstechnische Forschung sowohl zu Attacken auf kritische Infrastrukturen beitragen (Stichwort: Cyberkriege |²³) als auch umgekehrt deren Schutz erhöhen. Zudem wird der Wissenschaft – vor allem vor dem Hintergrund von Wissenschaftsfreiheit als Funktionsgrundrecht (vgl. A.II) – die Rolle einer kritischen Instanz gegenüber staatlichen und wirtschaftlichen Akteuren mit ihren jeweiligen (Macht)Interessen zugewiesen. Darüber hinaus eröffnet der wissenschaftliche Diskurs einen deliberativen Raum, in dem disziplinübergreifend Wissen und Handlungsstrategien für die Bewältigung akuter Krisen wie Pandemien oder andauernden Herausforderungen wie dem demographischen Wandel erarbeitet werden können – unabhängig von politischen Interessens- und Konfliktlagen. In einem solchen Raum kann die Komplexität unvorhergesehener Entwicklungen etwa im Zuge akuter oder andauernder Krisen angemessen erfasst und reflektiert werden. Damit wird der wissenschaftliche Diskurs zu einem Element der Resilienz, um innovativ auf Unvorhergesehenes reagieren zu können.

Es wird immer deutlicher, dass das Wissenschaftssystem, dessen sicherheitspolitische Relevanz sich bislang insbesondere auf umgrenzte, im Exportkontrollrecht definierte Bereiche sowie auf gezielte Forschung zu militärischen Zwecken beschränkte, nunmehr zu **einem zentralen sicherheitsrelevanten Teil der Gesellschaft geworden ist**. Es trägt einerseits mit den Arbeiten seiner Akteure wesentlich zur Gewährleistung von Sicherheit und Resilienz bei, was intendiert stärker befördert werden sollte (vgl. C.IV). Andererseits ist es zunehmend ein Angriffsziel für Staaten und andere, auch nichtstaatliche Akteure wie Terrorgruppen und kriminelle Vereinigungen, die von den wissenschaftlichen und technologischen Errungenschaften in unredlicher Weise militärisch profitieren oder auch Fortschritte verhindern wollen.

B.II SICHERHEITSRELEVANTE FORSCHUNG

Mit der Entwicklung des Sicherheitsbegriffs hin zu einem umfassenden und unterschiedliche Bereiche integrierenden Verständnis hat sich auch das Konzept von **sicherheitsrelevanter Forschung** verändert. Sicherheitsrelevant ist Forschung, insofern sie zur **Aufrechterhaltung der inneren und äußeren Sicherheit sowie zum Aufbau der Resilienz und Erhaltung der natürlichen Lebensgrundlagen des Gemeinwesens** beiträgt und beitragen soll oder diese gefährden kann. Folglich sind nicht allein Arbeiten sicherheitsrelevant, die der Aufrechterhaltung der äußeren (militärischen) Verteidigungsfähigkeit dienen. Vielmehr zählen auch wissenschaftliche Arbeiten dazu, die darauf abzielen, „Verwundbarkeiten zu erkennen, zu analysieren und Vorschläge bzw. Technologien zur

| ²³ Vgl. Wörner, J.-D.; Schmidt, Christoph M. (Hrsg.) (2022): Sicherheit, Resilienz und Nachhaltigkeit (acatech IMPULS), hrsg. v. acatech – Deutsche Akademie der Technikwissenschaften; München, S. 8, https://doi.org/10.48669/aca_2022-2.

Minderung oder Vermeidung der Risiken zu entwickeln, ohne in die Freiheit oder die Rechte des Bürgers einzugreifen“. |²⁴

Angesichts der politischen, gesellschaftlichen, wissenschaftlichen und technologischen Dynamik ist eine **klare Abgrenzung** zwischen wissenschaftlichen Arbeiten, die von Sicherheitsrelevanz sind, und solchen, in denen kein Bezug zu Fragen von Sicherheit und Resilienz besteht, **kaum möglich**. Es handelt sich um ein **Kontinuum**, das sich in **fast allen Disziplinen sowie Forschungsbereichen** beobachten lässt – auch in den Rechts-, Geistes- und Sozialwissenschaften, wie folgendes Beispiel illustriert.

Eine Studie untersucht, wie Jugendliche extremistisches (islamistisches) Material im Internet konsumieren und ob es einen Zusammenhang zur Radikalisierung gibt. Letzteres konnte nachgewiesen werden. Dabei fand man heraus, dass nicht die Darstellung von Gewalt, sondern die Intensität der Ansprache relevant ist. So wird etwa Videomaterial von Enthauptungen unter Jugendlichen zwar vielfach angeschaut. Das Radikalisierungspotenzial ist jedoch gering. Im Unterschied dazu besuchen nur wenige Menschen Online-Magazine des sogenannten Islamischen Staats oder von Al-Qaida – allerdings mit einem größeren kognitiven Effekt. Aufbauend auf diesen Erkenntnissen können Strategien der Deradikalisierung entwickelt werden. Gleichzeitig jedoch können sie extremistischen und terroristischen Gruppen helfen, ihre Rekrutierungsstrategien zu verbessern. Studien dieser Art können folglich sowohl Wege zur De-Radikalisierung aufzeichnen als auch eine Rekrutierungshilfe für Terrorgruppen darstellen. |²⁵

Auch grundlagenorientierte Aktivitäten sind betroffen, selbst wenn sie lange Zeit aufgrund der Bestimmung des Außenwirtschaftsrechts nicht als sicherheitsrelevant betrachtet wurden. Im Wesentlichen standen solche Forschungs- und Entwicklungsarbeiten im Fokus, die auf einem höheren Technology Readiness Level (TRL) |²⁶ als 3 betrieben wurden. Allerdings gab es schon in den 1950er Jahren Schutzmaßnahmen in der Grundlagenforschung, sofern das Potenzial

|²⁴ Klaus, T.; Drees, B.; Leismann, T. (2009): Zukunftstechnologien in der Sicherheitsforschung, in: Winzer, P.; Schnieder, E.; Bach, F.-W. (Hrsg.): Sicherheitsforschung – Chancen und Perspektiven (Reihe acatech DISKUSSION); Berlin/Heidelberg, S. 13-38, hier S. 13, <https://www.acatech.de/publikation/sicherheitsforschung-chancen-und-perspektiven/>.

|²⁵ Vgl. GA von DFG und Leopoldina (2024): Wissenschaftsfreiheit und Sicherheitsinteressen in Zeiten geopolitischer Polarisierung – Fünfter Tätigkeits- und Sachstandsbericht; Berlin, S. 71, <https://www.sicherheitsrelevante-forschung.org/publikation-taetigkeitsbericht2024/>. Vgl. auch Frissen, T. (2021): Internet, the great radicalizer? Exploring relationships between seeking for online extremist materials and cognitive radicalization in young adults, in: Computers in Human Behavior, 114, Artikel 106549, <https://doi.org/10.1016/j.chb.2020.106549>.

|²⁶ Technology Readiness Level (TRL) „ist ursprünglich ein Begriff, der in der Luft- und Raumfahrttechnik geprägt wurde (für Software: Software Technology Readiness Level). Es ist eine Skala zur Bewertung des Entwicklungsstandes von neuen Technologien auf der Basis einer systematischen Analyse.“ Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) (2024): Immaterieller Technologietransfer (ITT); Eschborn, https://www.bafa.de/SharedDocs/Downloads/DE/Aussenwirtschaft/afk_merkblatt_itt.html, S. 18.

des Missbrauchs bestand. So wurde etwa im Gründungsvertrag des Kernforschungszentrums Karlsruhe von 1956 auf Betreiben der Alliierten die erste Zivilklausel aufgenommen, um die Entmilitarisierung der atomaren Grundlagenforschung in Deutschland sicherzustellen. Angesichts der Beschleunigung in Forschungs- und Entwicklungsprozessen genügt ein bloßer Verweis auf Grundlagenforschung auch in anderen Feldern häufig nicht mehr, um Forschungsaktivitäten als nicht sicherheitsrelevant zu klassifizieren. Im Bereich der Informatik beispielsweise sind Forschungs- und Entwicklungsarbeiten bis zur Marktreife so eng miteinander verzahnt, dass Neuerungen bereits innerhalb weniger Monate in Produkte eingebaut werden, auch wenn sie noch nicht von allen genutzt werden können. Das eingangs beschriebene Spannungsverhältnis, Freiheit und Verantwortung gleichermaßen gewährleisten zu wollen, wird an dieser Stelle besonders deutlich.

Das **Konzept der Dual-Use-Technologien** und die Forderung nach Dual-Use Politiken ist ursprünglich in den 1970er Jahren entstanden im Zuge der Erkenntnis, dass die Begrenzung der unkontrollierten Proliferation von militärischen Technologien aus dem Bereich der Nuklear-, chemischen oder biologischen Waffen sowie den zugehörigen Trägertechnologien in einem Spannungsverhältnis zur zivilen Nutzung solcher Technologien steht. |²⁷ In der Folge wurde zunehmend die ökonomische Verwertung militärischer Technologien durch zivile Anwendungen in den Blick genommen, auch als Rechtfertigung hoher militärischer Forschungs- und Entwicklungsausgaben.

In den letzten drei Dekaden hat der Begriff „Dual Use“ eine **über die Unterscheidung zwischen militärischer und ziviler Forschung hinausgehende Bedeutung** entwickelt. |²⁸ Insbesondere vor dem Hintergrund der virologischen Gain of Function-Forschung (GoF) |²⁹ in den Lebenswissenschaften weitete sich die Bedeutung aus. Denn hier spielen neben der militärischen Nutzung auch moralische Bedenken und andere Risiken, etwa der Ausbruch aus einem Labor, eine Rolle, wie das folgende Fallbeispiel verdeutlicht:

In einer Studie wurden fünf genetische Veränderungen identifiziert, die es erlauben, dass die für Vögel hochpathogenen Influenzaviren vom Typ H5N1 (sogenannte Vogelgrippeviren) auch zwischen Säugern über die Luft übertragen werden. Diese Erkenntnisse können dazu beitragen, besser vorherzusagen, wie sich solche Viren schrittweise zu einer Bedrohung für den Menschen ent-

|²⁷ Vgl. Molas-Gallart, J. (1997): Which way to go? Defence technology and the diversity of 'dual-use' technology transfer, in: Research policy, 26 (3), S. 367–385, [https://doi.org/10.1016/S0048-7333\(97\)00023-1](https://doi.org/10.1016/S0048-7333(97)00023-1).

|²⁸ Vgl. Oltmann, S. (2015): Dual Use Research: Investigation Across Multiple Science Disciplines, in: Science and Engineering Ethics, 21, S. 327–341, hier S. 328, <https://doi.org/10.1007/s11948-014-9535-y>.

|²⁹ Virologische Gain-of-function-Forschung (GoF) bezieht sich auf Forschung, die darauf abzielt, die Übertragbarkeit und Virulenz von Krankheitserregern zu erhöhen. Diese Forschung war im Genfer Protokoll (1925) und in der Biowaffenkonvention (BWC von 1975) nicht klar adressiert, weil Viren nicht alle Merkmale des Lebens aufweisen. Heute wird GoF-Forschung etwa zur Impfstoff-Entwicklung eingesetzt.

wickeln könnten. Damit können das Pandemiepotenzial von in der Natur regelmäßig neu auftretenden krankmachenden Virusvarianten besser eingeschätzt werden, Erkenntnisse für die frühzeitige Unterbrechung von Infektionsketten gewonnen und gegebenenfalls Impfstoffe gezielt entwickelt werden. Risiken solcher GoF-Experimente an Vogelgrippeviren bestehen sowohl hinsichtlich unbeabsichtigter Pandemieausbrüche durch fahrlässiges Handeln im Labor, wodurch die Viren in die Umwelt gelangen, als auch hinsichtlich ihres Missbrauchs für die Entwicklung neuer biologischer Waffen. |³⁰

Mittlerweile geht man davon aus, dass **fast alle Forschungsfelder potenziellen Dual-Use-Charakter** haben. Vor allem die rasante Entwicklung der KI, die immer mehr Forschungsfelder durchdringt, hat dazu beigetragen. Hier stellen sich seit der EU-Verordnung (AI Act) von 2024 nicht allein ethische Fragen, sondern auch rechtliche. |³¹ Angesichts der vielfältigen Einsatzmöglichkeiten und des mehrfachen missbräuchlichen Potenzials von Forschungsarbeiten ist – über einen militärischen Einsatz hinaus – vom **Multiple Use-Charakter** der Forschung die Rede.

Neben die Ausweitung auf immer mehr Disziplinen und Forschungsfelder tritt die fortschreitende **Konvergenz unterschiedlicher Disziplinen**. Dies trifft vor allem, aber nicht allein auf die Durchdringung der Forschung mit Informations- und KI-Technologien zu, die in fast allen Disziplinen zu beobachten ist. |³² Auch andere Forschungsbereiche wie die Nanotechnologie sind hier zu nennen. |³³ Beide Entwicklungen, Ausweitung von Forschungsfeldern mit Potenzialen des Missbrauchs und Konvergenz unterschiedlicher Disziplinen, führen dazu, dass von einem **inhärenten Dual-Use-Charakter eines erheblichen Teils wissenschaftlicher Arbeiten** auszugehen ist.

Diese Analyse könnte dazu führen, sich vom **Dual-Use-Begriff** zu verabschieden. Allerdings bleibt er in bestimmten Kontexten, etwa zur Regelung der Exportkontrolle, hilfreich. Hier kann eine *gegenstandsbezogene Perspektive* hilfreich sein,

| ³⁰ Vgl. GA von DFG und Leopoldina (2024): Wissenschaftsfreiheit und Sicherheitsinteressen in Zeiten geopolitischer Polarisierung – Fünfter Tätigkeits- und Sachstandsbericht; Berlin, S. 74, <https://www.sicherheitsrelevante-forschung.org/publikation-taetigkeitsbericht2024/>. Vgl. auch Herfst, S.; Linster, M.; Chutinimitkul, S. et al. (2012): Airborne transmission of influenza A/H5N1 virus between ferrets, in: Science, 336 (6088), S. 1534–1541, <https://doi.org/10.1126/science.1213362>, sowie 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), S. 420–428, <https://doi.org/10.1038/nature10831>.

| ³¹ Vgl. <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>.

| ³² Vgl. Oltmann, S. (2015): Dual Use Research: Investigation Across Multiple Science Disciplines, in: Science and Engineering Ethics, 21, S. 327–341, hier S. 331, <https://doi.org/10.1007/s11948-014-9535-y>.

| ³³ Die Nanotechnologie umfasst Aspekte aus der Physik, Chemie, Biologie etc. und lässt die Grenzen zwischen biomedizinischer und Elektrotechnik verschwimmen, vgl. ebd., hier S. 329 f. Vgl. hierzu auch Hähnel, M. (2024): Conceptualizing dual use: A multidimensional approach, in: Research Ethics, 0 (0), hier S. 2, <https://doi.org/10.1177/17470161241261466>.

die wie in der 2021 novellierten EU-Dual-Use-Verordnung |³⁴ darauf abhebt, dass es sich bei Gütern „mit doppeltem Verwendungszweck“ auch um „Datenverarbeitungsprogramme (Software) und Technologie [handelt], die **sowohl für zivile als auch für militärische Zwecke** verwendet werden können“. |³⁵ Der Dual-Use-Begriff bezieht sich hier auf den möglichen Einsatz in einem militärischen oder zivilen Kontext. Darüber hinaus wird der Begriff auch bezogen auf die tatsächliche Intention der Nutzerin, des Nutzers, die oder der etwa Forschungsergebnisse zum Einsatz bringt. Diese *intentionale Perspektive* koppelt den Dual-Use-Charakter an die Akteursabsicht, die hinter dem Rückgriff auf wissenschaftliche Forschungsergebnisse steht. |³⁶ Allerdings sind die Intentionen der Akteure vielfach nicht offensichtlich, sondern bleiben implizit und opak. Daher besteht ein hoher Grad an Unsicherheit, will man den Dual-Use-Charakter von Gütern und Technologien allein in Bezug auf den intentionalen Einsatz von Forschungs- und Entwicklungsergebnissen bestimmen. Vermehrt nutzen auch kollektive Akteure wie terroristische Gruppen, organisierte kriminelle Banden oder supranationale Organisationen solche Güter und Technologien. Diese **Ausweitung von**

|³⁴ Vgl. BAFA (2021): Die neue EU-Dual-Use-Verordnung (Verordnung (EU) 2021/821), https://www.bafa.de/SharedDocs/Downloads/DE/Aussenwirtschaft/afk_merkblatt_eu-dual-use-vo.html.

|³⁵ Europäische Union (EU) (2021): Empfehlung (EU) 2021/1700 der Kommission vom 15. September 2021 zu internen Compliance-Programmen für die Kontrolle von Forschung im Zusammenhang mit Gütern mit doppeltem Verwendungszweck gemäß der Verordnung (EU) 2021/821 des Europäischen Parlaments und des Rates über eine Unionsregelung für die Kontrolle der Ausfuhr, der Vermittlung, der technischen Unterstützung, der Durchfuhr und der Verbringung betreffend Güter mit doppeltem Verwendungszweck, S. 7, <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32021H1700>. Die EU schließt darin auch Güter ein, „die zur Konstruktion, Entwicklung, Herstellung oder zum Einsatz von nuklearen, chemischen oder biologischen Waffen oder ihren Trägersystemen verwendet werden können, einschließlich aller Güter, die sowohl für nicht-explosive Zwecke als auch für jedwede Form der Unterstützung bei der Herstellung von Kernwaffen oder sonstigen Kernsprengkörpern verwendet werden können.“ Ebd., S. 7. In diesem Sinne hat auch die Expertenkommission für Forschung und Innovation (EFI) den Begriff verwendet: „Dual Use bzw. Dual-Use-Güter (Güter mit doppeltem Verwendungszweck) sind Waren, Software und Technologie, die üblicherweise für zivile Zwecke verwendet werden, darüber hinaus jedoch auch im militärischen Bereich verwendet werden können.“ EFI (2025): Gutachten zu Forschung, Innovation und technologischer Leistungsfähigkeit Deutschlands 2025; Berlin, S. 127, <https://www.e-fi.de/publikationen/gutachten>. Ähnlich auch der Deutsche Akademische Austauschdienst (DAAD): „Mit ‚Dual-Use‘ wird die grundsätzliche Verwendbarkeit von Technologien oder Gütern zu zivilen als auch zu militärischen Zwecken bezeichnet. Hierunter fallen nicht nur materielle, sondern auch intangible Güter wie Informationen, Daten und Wissensbestände verschiedenster Art, deren Weitergabe gesetzlichen Regelungen unterworfen ist.“ <https://www.daad.de/de/infos-services-fuer-hochschulen/kompetenzzentrum/kiwi-themen/risiko-und-sicherheit/dual-use/>. Dabei wird explizit auf gesetzliche Regelungen verwiesen.

|³⁶ In diesem Sinne argumentiert beispielsweise der GA der DFG und Leopoldina, der „unter dem Begriff besorgniserregende sicherheitsrelevante Forschung“ wissenschaftliche Arbeiten fasst, die missbraucht werden können, „um Menschenwürde, Leben, Gesundheit, Freiheit, Eigentum, Umwelt oder ein friedliches Zusammenleben erheblich zu schädigen.“ GA von DFG und Leopoldina (2024): Umgang mit sicherheitsrelevanter Forschung in Deutschland – auf einen Blick; Berlin, S. 5, <https://www.sicherheitsrelevante-forschung.org/publikation-informationsbroschuere2024/>. Vgl. auch GA der DFG und Leopoldina (2022): Wissenschaftsfreiheit und Wissenschaftsverantwortung – Empfehlungen zum Umgang mit sicherheitsrelevanter Forschung; Berlin, S. 10, <https://www.sicherheitsrelevante-forschung.org/publikation-wissenschaftsfreiheit2022/>. Weiter erläutert der GA, dass damit „[i]m Forschungskontext [...] meist solche Forschungsergebnisse und -methoden [gemeint sind], die sowohl für friedliche bzw. nützliche Zwecke als auch zum absichtlichen Schädigen oder Unterdrücken von Gesellschaft bzw. der Umwelt eingesetzt werden können.“ <https://www.sicherheitsrelevante-forschung.org/faq/>.

Akteuren und Akteurstypen ist in den letzten Jahren bzw. Jahrzehnten zu beobachten.

Allein eine **multiperspektivische Betrachtung** des Dual-Use-Konzepts erlaubt es, die unterschiedlichen Potenziale von Forschungsarbeiten und Technologien zu erkennen und sie in der Zusammenschau von Gegenstand sowie Akteursintentionen und -konstellationen angemessen einzuschätzen. Eine trennscharfe Abgrenzung sicherheitsrelevanter Forschung von nicht sicherheitsrelevanter ist weder vor dem Hintergrund des erweiterten Sicherheitsbegriffs möglich noch mit Bezug auf den Dual-Use-Charakter wissenschaftlicher Arbeiten. Um dieser Situation begegnen zu können, bedarf es einer neuen Governance im Umgang mit sicherheitsrelevanter Forschung und Wissenssicherheit im Wissenschaftssystem.

B.III WISSENSSICHERHEIT

Die weltpolitischen Spannungen und der inhärente Dual-Use-Charakter von Forschungs- und Technologiearbeiten haben zur Entwicklung eines **neuen querschnittlichen Politikbereichs** geführt: **Knowledge Security** (Wissens- und Forschungssicherheit). Er hat sich in den letzten Jahren in unterschiedlichen Ländern – neben der Wirtschaftssicherheit – etabliert. Länder wie Australien, Kanada, die USA, aber auch Großbritannien und die Niederlande adressieren diese Herausforderung schon seit längerem.

Verschiedene Begriffe werden hier verwendet: von der Forschungssicherheit („research security“ |³⁷) bis zu dem vor allem in Großbritannien aus historischen Gründen gewählten Begriff von „trusted research and innovation“. |³⁸ Der Wissenschaftsrat spricht im Kontext seines Positionspapiers von **Wissenssicherheit**, da dieser Begriff nicht allein Forschungsaktivitäten, sondern alle wissenschaftlichen Aktivitäten einschließlich des Austauschs von Personal und Studierenden umfasst. Wissenssicherheit als Wert zielt darauf, sowohl bestimmte nationale Interessen und Werte zu wahren als auch den Kern wissenschaftlichen Arbeitens weiterhin zu schützen, nämlich unter Bedingungen einer garantierten Wissenschaftsfreiheit arbeiten und international kooperieren zu können.

|³⁷ Vgl. unter anderem das im Mai 2024 verabschiedete Empfehlungspapier „Enhancing Research Security“ der Europäischen Kommission: „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.“ Rat der Europäischen Union (2024): Empfehlungen des Rates vom 23. Mai 2024 zur Stärkung der Forschungssicherheit (C/2024/3510); Brüssel, S. 4, <http://data.europa.eu/eli/C/2024/3510/oj>.

|³⁸ Vgl. <https://www.ukri.org/manage-your-award/good-research-resource-hub/trusted-research-and-innovation/>.

Dabei umfasst Wissenssicherheit mehrere Dimensionen, die sich auf **unterschiedliche Risiken** beziehen:

1 – Unerwünschter Wissensabfluss: Damit ist der aus unterschiedlichen Gründen unerwünschte Abfluss oder die Weitergabe von Wissen einschließlich Technologien gemeint. Dies kann sowohl aus militärischem bzw. im engeren Sinne sicherheitspolitischem Interesse als auch aus ökonomischem oder technologischem Interesse problematisch sein. Während für den Wissensabfluss aus militärischem Interesse schon immer Vorkehrungen bestanden, rückt der Wissensabfluss, um die jeweilige wirtschaftliche Macht zu stärken und die eigene technologische Souveränität zu befördern, nunmehr in den Fokus. Die Rede ist von einer „Non-Professionalisierung“ von Spionage, womit gemeint ist, dass Gastwissenschaftlerinnen und -wissenschaftler oder Studierende während ihres Aufenthalts an ausländischen Universitäten oder Forschungseinrichtungen zur Ausforschung beauftragt sind. |³⁹ Also nicht das persönliche, sondern das Interesse des jeweiligen Auftraggebenden ist für unerwünschten Wissensabfluss entscheidend. Hinzukommt, dass Gastwissenschaftlerinnen und -wissenschaftler auch ohne vorherigen Auftrag nach ihrer Rückkehr gedrängt oder gezwungen werden (können), Wissen mit staatlichen Stellen zu teilen.

Unerwünschter Wissens- und Datenabfluss ist nicht an Personen gebunden, sondern kann auch technisch durch Cyberattacken oder über kommerzielle Anbieter von Dienstleistungen (z. B. Cloud- oder Sequenzierungsangeboten) erfolgen und über Datentracking unterstützt werden. |⁴⁰ Die Nutzung digitaler Angebote hinterlässt Spuren, so dass die Anbieter mit entsprechenden Analyseinstrumenten Zugang zu allen Stufen des Research Life Cycle von der Literaturrecherche bis zur strukturierten Forschungsinformation haben.

2 – Unerwünschte Einflussnahme, die sich sowohl auf Forschung und Lehre selbst als auch auf einzelne Personen und deren gesellschaftliche Rolle beziehen kann. Sie reicht von der bewussten oder unbewussten Übernahme und Verbreitung bestimmter Meinungen über die Beschränkung von Publikationsaktivitäten bis hin zur Selbstzensur im wissenschaftlichen Arbeiten, so dass das Vertrauen in wissenschaftliches Arbeiten und die damit verbundene gute wissenschaftliche Praxis unterminiert wird.

|³⁹ Vgl. hierzu die Einschätzung des Bundesamtes für Verfassungsschutz (BfV) „Chinas neue Wege der Spionage“ <https://www.verfassungsschutz.de/SharedDocs/hintergruende/DE/wirtschafts-wissenschaftsschutz/chinas-neue-wege-der-spionage.html>.

|⁴⁰ 2021 hat die DFG auf die Implikationen des Datentrackings im Sinne der Analyse von Nutzungsspuren in der Wissenschaft hingewiesen, vgl. DFG-Ausschuss für Wissenschaftliche Bibliotheken und Informationssysteme (2021): Datentracking in der Wissenschaft: Aggregation und Verwendung bzw. Verkauf von Nutzungsdaten durch Wissenschaftsverlage. Ein Informationspapier des Ausschusses für Wissenschaftliche Bibliotheken und Informationssysteme der Deutschen Forschungsgemeinschaft; Bonn, <https://doi.org/10.5281/zenodo.5900759>.

Als ein Beispiel sei auf Berichte von chinesischen Studierenden verwiesen, die an ihren Gastuniversitäten Vorlesungen aufzeichnen und an Behörden melden, so etwa, wenn Dozierende aus Sicht Chinas „unerwünschte“ Inhalte lehren (z. B. Taiwan als unabhängiges Land bezeichnen). |⁴¹ Und umgekehrt gibt es Hinweise auf eine Einflussnahme der Volksrepublik China auf Wissenschaftseinrichtungen im Kontext von Konfuzius-Instituten, die auf verschiedene Weise auch mit Hochschulen verbunden sind. So kam es etwa zu Absagen virtueller Lesungen oder Versuchen, die Tour der Dokumentation „In the name of Confucius“ über die wachsende weltweite Kontroverse zum Wirken der Konfuzius-Institute zu verhindern. Dies hat zu Presseberichten und zu weitergehenden politischen Aktivitäten und Beobachtungen durch das Bundesamt für Verfassungsschutz (BfV) geführt. |⁴²

Auch an dieser Stelle läuft die Einflussnahme nicht allein über menschliche Akteure. Derzeit besteht ein besonders hohes Maß an Abhängigkeit von IT-Infrastrukturen, die marktbestimmende Oligopole zur Verfügung stellen. Sie kontrollieren den Zugang sowie ihre Benutzbarkeit und Transparenz. Dadurch können nicht nur Daten unkontrolliert abfließen, sondern grundsätzlich besteht auch die Möglichkeit der gezielten Manipulation. Die Rede ist vom „Tech Cold War“. |⁴³ Dieser Aspekt gewinnt insbesondere im Zuge der Zentralisierung der KI-Entwicklung unter dem Dach großer Technologieunternehmen eine noch höhere Brisanz, insofern sie nicht allein die Kontrolle über die zugrunde liegende Software, sondern auch über die zu Trainingszwecken eingesetzten Datensätze haben können. |⁴⁴

| ⁴¹ Vgl. 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>. Vgl. auch Deutsche Bundesregierung (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.

| ⁴² Ersteres betraf das Buch Aust, S.; Geiges, A. (2023): Xi Jinping. Der mächtigste Mann der Welt, 2. Aufl.; München, vgl. <https://www.spiegel.de/panorama/bildung/chinas-einfluss-auf-deutsche-universitaeten-der-lange-arm-peking-a-f6567e46-508f-4d64-a830-3816296dad79>. Eine genauere Darstellung ist aus Gründen der Geheimhaltung nicht möglich. Vgl. hierzu auch Deutsche Bundesregierung (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, insbesondere S. 5, <https://dip.bundestag.de/vorgang/stand-des-ausbaus-der-asien-und-china-kompetenz-im-wissenschaftssystem-und/286049?f.deskriptor=Technologietransfer&rows=25&pos=16&ctx=a>.

| ⁴³ Baums, A.; Butts, N. (2025): Tech Cold War. The Geopolitics of Technology; Boulder, <https://doi.org/10.1515/9781962551571>.

| ⁴⁴ Vgl. hierzu die Einschätzung der Royal Society: „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

3 – Finanzielle und wissenschaftliche Abhängigkeiten, die entstehen, wenn Partner ihre eigenen Kooperationsinteressen bewusst verschleiern und über finanzielle Anreize die Zusammenarbeit oder den Personalaustausch vorantreiben wollen. Abhängigkeiten können deutsche Einrichtungen auch indirekt betreffen, wenn mit unterschiedlichen Ländern kooperiert wird, deren Wissenschaftssystem in seiner Finanzierung – bis hin zur Gewährleistung von Studienangeboten – auf ausländische Investoren oder Studiengebühren ausländischer Studierender angewiesen ist.

Abhängigkeiten bestehen jedoch auch bezüglich Forschungs- und Dateninfrastrukturen, die von anderen Ländern finanziert oder bereitgestellt werden. Es ist unstrittig, dass die Bedeutung dieser Infrastrukturen in allen Wissenschaftsgebieten in den letzten Jahren deutlich gestiegen ist. |⁴⁵ Wenn Länder oder auch Wirtschaftsunternehmen, insbesondere Oligopole, in der Lage sind, aufgrund einseitiger Abhängigkeiten Akteure im Wissenschaftssystem unter Druck setzen zu können, erhöht sich die Vulnerabilität des Wissenschaftssystems in erheblichem Maße. Bereits 2023 hat der Wissenschaftsrat empfohlen, Abhängigkeiten zu reduzieren und eigene Handlungsmöglichkeiten zu erhöhen. |⁴⁶

Als Beispiel für wissenschaftliche Abhängigkeiten und Unwägbarkeiten auch mit Blick auf bislang unverbrüchlich eingestufte Partner kann das Argo-Programm |⁴⁷ gelten, das mittels frei treibender Messbojen (sogenannte Argo-Floats, von denen rund 4.000 aktuell in Betrieb sind) seit den frühen 2000er Jahren ozeanographische Daten aus den Tiefen der Meere sammelt und mittels Satelliten an Datenzentren in den USA und Frankreich überträgt. |⁴⁸

An diesem Programm beteiligt sich u. a. auch Deutschland mit aktuell weniger als 7 % der Argo-Floats, die vorrangig im Atlantik ausgesetzt werden. Insgesamt stellt die USA mehr als die Hälfte aller Bojen bereit (56 %, Stand Mai 2025). Diese Abhängigkeit birgt große Risiken für die Modellierung in der Klimaforschung sowie aktuelle Vorhersagedienste, |⁴⁹ wenn der Zugang zu den Daten nicht länger gewährleistet, bzw. die gegenwärtige Netzwerkdichte nicht aufrechterhalten wird.

intelligence is changing the nature and method of scientific research; London, S. 72, <https://royalsociety.org/news-resources/projects/science-in-the-age-of-ai/>.

|⁴⁵ Hintergrund für diesen Bedeutungszuwachs ist, dass nicht länger eine klare Grenze zwischen Forscherhandeln und Infrastrukturen zu ziehen ist, vgl. dazu u. a. Gehring, P. (2018): Viele Fronten. Forschungsdatenmanagement als Ermöglichungspolitik, in: *Forschung & Lehre*, 25. Jg., 9/18, S. 754–756, <https://www.forschung-und-lehre.de/heftarchiv/ausgabe-9/18>; und Barlösius, E. (2019): *Infrastrukturen als soziale Ordnungsdienste*. Ein Beitrag zur Gesellschaftsdiagnose, Frankfurt a. M./New York, v. a. S. 157 ff.

|⁴⁶ Vgl. Wissenschaftsrat (2023): *Empfehlungen zur Souveränität und Sicherheit der Wissenschaft im digitalen Raum*; Köln, <https://doi.org/10.57674/m6pk-dt95>.

|⁴⁷ Vgl. https://www.bsh.de/EN/TOPICS/Monitoring_systems/Argo_floats/argo_floats_node.html.

|⁴⁸ Vgl. <https://www.aoml.noaa.gov/two-decades-argo-program/>.

|⁴⁹ Vgl. <https://globalocean.noaa.gov/research/argo-program/>, <https://argo.ucsd.edu>.

4 – Interferenzen wissenschaftlicher Aktivitäten mit anderen gesellschaftlichen Bereichen, so dass wissenschaftlicher Austausch und Zusammenarbeit mit einem kritischen Land |⁵⁰ sich auf andere etwa politische und/oder wirtschaftliche Beziehungen mit diesem oder anderen Ländern auswirkt. Beispielsweise kann die Existenz einer wissenschaftlichen Beziehung zu politischem Reputationsgewinn genutzt werden. In den internationalen Beziehungen scheint sich im Zuge der Erosion einer regelbasierten Ordnung ein solcher transaktional genannter Ansatz immer stärker durchzusetzen, der zu „Deals“ über die Grenzen der unterschiedlichen gesellschaftlichen Bereiche und damit auch der Politikfelder hinweg führt. |⁵¹ Die Orientierung erfolgt an nationalen Interessen und weniger an übergeordneten Prinzipien oder Werten, so dass kurzfristig erzielte Ergebnisse und Vorteile anstelle langfristiger strategischer oder wertebasierter Partnerschaften handlungsleitend sind. Wissenschaftliche Beziehungen können gezielt genutzt werden, um sie mit politischen oder wirtschaftlichen Interessen zu „verrechnen“ – und sei es nur auf einer symbolischen Ebene. Dies ist insbesondere deswegen kritisch, weil die Auswirkungen in den nichtakademischen Bereichen für den einzelnen Wissenschaftler oder die einzelne Wissenschaftlerin nicht immer erkennbar sind.

5 – Verletzung forschungsethischer oder ethischer Prinzipien, so dass die Integrität des wissenschaftlichen Arbeitens in Frage gestellt wird (z. B. Unterdrückung unerwünschter Daten) oder ethische Werte verletzt werden (z. B. durch die Verlagerung von Experimenten in Länder mit geringerem rechtlichen Schutzniveau, die Nutzung wissenschaftlicher Technologien zu Überwachungszwecken in autokratischen Staaten oder der Missbrauch menschlicher Quellen zur Datenerhebung).

Quellenschutz ist ein Beispiel für eine zunehmend wichtiger werdende ethische Herausforderung, wenn es um Forschungsprojekte in Weltregionen geht, aus denen Menschen auf legalen oder illegalen Wegen nach Europa migrieren. Hier werden nicht allein Migrationsfragen, sondern auch Fragen politischer Dynamiken in der Region oder andere sensible Rahmenbedingungen thematisiert. So können über den Kreis der Personen, die diese Forschung gemeinsam diskutieren, vertrauliche Informationen oder Positionen abfließen und zu politischen Zwecken eingesetzt werden. Das Anonymisieren von Quellen ist unabdingbar und zugleich schwierig – vor allem bei bekannten Orten und Institutionen, über die gegebenenfalls in den Medien berichtet wird.

| ⁵⁰ Vgl. zur Einordnung eines Landes als kritisch die Aufgabe der Nationalen Plattform (siehe Fußnote 69 und C.III.3).

| ⁵¹ Zur Einordnung des transaktionalen Ansatzes im Kontext der von Ländern des Globalen Südens als „westliche Doppelstandards“ wahrgenommenen Bezugnahme auf eine regelbasierte internationale Ordnung, vgl. Eisentraut, S. (2025): Westliche Doppelstandards: Prinzipien unter Beschuss, in: Internationale Politik 1/2025, S. 76–81, <https://internationalepolitik.de/de/westliche-doppelstandards-prinzipien-unter-beschuss>.

Der Wissenschaftsrat legt den hier entwickelten **umfassenden Begriff von Wissensrisiken und Wissenssicherheit** seinen weiteren Analysen und Empfehlungen **zugrunde**. Er plädiert dafür, im wissenschaftspolitischen Diskurs nicht allein Forschungsrisiken zu adressieren, sondern im Sinne der fünf explizierten Risikotypen von Wissensrisiken zu sprechen. In einem dynamischen Feld wie diesem, das in enger Wechselwirkung mit den weltpolitischen Entwicklungen steht, ist es möglich, dass weitere Risikotypen hinzukommen. Dies ist derzeit noch nicht absehbar.

B.IV RECHT UND SELBSTVERPFLICHTUNG

Der Umgang mit sicherheitsrelevanten Themen ist in der deutschen Wissenschaft partiell reguliert. Von zentraler Bedeutung für den Umgang mit einem Teil der sicherheitsrelevanten Forschung ist das System der Exportkontrolle (vgl. B.IV.1). Darüber hinaus können Zivilklauseln eine Rolle spielen, bei denen es sich allerdings in der Regel um Selbstverpflichtungen von Hochschulen und Forschungseinrichtungen handelt, die rechtlich nicht bindend sind (vgl. B.IV.2).

IV.1 Exportkontrolle

In der Nachkriegszeit richteten sowohl die westlichen als auch die östlichen Mächte einen signifikanten Teil der Forschung dezidiert auf militärische Innovationen aus – in der Regel in eigenständigen Organisationen oder Organisationseinheiten unter entsprechenden Sicherheitsvorkehrungen. Als Schutz wurde in der westlichen Welt ein **System der Exportkontrolle**, dem auch wissenschaftliche Einrichtungen unterliegen, ausgearbeitet. Entsprechende Exportkontrollsysteme wie das Coordinating Committee on Multilateral Export Controls (COCOM) wurden etabliert, um insbesondere den Zugriff der Sowjetunion auf avancierte Technologien zu verhindern. Während früher häufig militärische Technologien in entsprechend entschärfter Form auch für zivile Systeme genutzt wurden, setzt die militärische Forschung mittlerweile auf zivile Arbeiten auf, da hier eine deutlich höhere Innovationsgeschwindigkeit zu beobachten ist. Vor diesem Hintergrund entwickelten sich die Exportkontrollmechanismen weiter. Das **Wassenaar Arrangement von 1995, dem auch die postsowjetischen Länder und Russland selbst beitraten**, folgte auf die im kalten Krieg entwickelte Exportkontrolle über COCOM.

In Deutschland und Europa haben **Exportkontrollregelungen Gesetzeskraft** und sind **strafbewehrt**. Hintergrund ist, dass Deutschland sich international dazu verpflichtet hat, die Verbreitung von Massenvernichtungswaffen und die unkontrollierte Anhäufung von konventionellen Rüstungsgütern zu verhindern. Dazu zählt auch die Kontrolle sensibler Güter, einschließlich Technologien und Software, als wichtiger Bestandteil dieser Nichtverbreitungsstrategie. Neben Wirt-

schaftsunternehmen sind auch Hochschulen und Forschungseinrichtungen Adressaten der Kontrollvorschriften für den Umgang mit potentiell kritischen Gütern |⁵² und den Transfer von sensitivem Know-how: „Dies betrifft einerseits die Ausfuhr von Waren (z. B. Laborequipment, Testausrüstung), dabei insbesondere auch die Ausfuhr von verkörperter Technologie (in E-Mails, auf Datenträgern, in Clouds etc.), sowie andererseits die unverkörperte („intangible“) Weitergabe von Wissen, den Know-how-Transfer, also die sog. „Technische Unterstützung““. |⁵³ Hierbei sind in erster Linie national oder in der EU-Dual-Use-Verordnung gelistete Güter oder Technologien sowie Länderembargos, d. h. Beschränkungen im Zuge internationaler Wirtschaftssanktionen von Interesse. Hauptfokus lag und liegt bisher auf proliferationsrelevanten Sachverhalten. Schlüsseltechnologien im Rahmen der Elektronischen Datentransfers (EDT) sind zum Teil (noch) nicht gelistet und unterliegen damit nicht explizit der Exportkontrolle. Gleichwohl können sie ein Sicherheitsrisiko darstellen.

Im Bereich der Exportkontrolle, deren Vorschriften sowohl für die einzelne Wissenschaftlerin, den einzelnen Wissenschaftler als auch für die Hochschule bzw. Forschungseinrichtung gelten, ist primär – gegenstandsbezogen – das **objektive Missbrauchspotenzial** entscheidend – unabhängig von der Motivation und Zielrichtung der eigenen Tätigkeit. |⁵⁴ Dabei gilt es auch, die Kooperation mit Personen zu bedenken, die gegebenenfalls auf Sanktionslisten aufgeführt werden.

Die Entwicklung des sogenannten Khan-Netzwerks gilt als bekanntester Fall für den Abfluss von Wissen und seinen Missbrauch. Nach seiner Ausbildung an europäischen Universitäten konnte Abdul Quadeer (A. Q.) Khan zum „Vater der pakistanischen Atombombe“ werden. Über sein Proliferationsnetzwerk konnte er Nuklearexpertise und -technologie an weitere Staaten wie Iran, Nordkorea und Libyen sowie an nichtstaatliche Akteure weitergeben. |⁵⁵

Die **umfassendste Exportkontrolle** einschließlich eines restriktiven Datenregimes hat derzeit **China** errichtet. Als autokratischer Staat ist ihm dies möglich. Dabei richtet es seine Exportkontrolle nicht allein auf die Möglichkeit der militärischen Nutzung von Forschung und Technologie aus, sondern hat eine Vielzahl von Maßnahmen zur Kontrolle mit unterschiedlichen strategischen Zielen

|⁵² Dazu zählen auch verbaute Teile. Das BAFA verweist zum Beispiel auf Schaltfunkenstrecken aus der Medizintechnik, die prinzipiell auch eingesetzt werden können, um Kernsprengköpfe zu zünden.

|⁵³ BAFA (2019): Exportkontrolle in Forschung & Wissenschaft; Eschborn, S. 12, https://www.bafa.de/SharedDocs/Downloads/DE/Aussenwirtschaft/afk_aca_broschuere_awareness.html?nn=1466914. Kriegswaffen unterliegen einer eigenen Gesetzgebung (Kriegswaffenkontrollgesetz).

|⁵⁴ Vgl. hierzu: BAFA (2019): Exportkontrolle in Forschung & Wissenschaft; Eschborn, v. a. S. 9, https://www.bafa.de/SharedDocs/Downloads/DE/Aussenwirtschaft/afk_aca_broschuere_awareness.html?nn=1466914.

|⁵⁵ Vgl. hierzu: Heupel, M. (2008): Das A. Q.-Khan-Netzwerk. Transnationale Proliferationsnetzwerke als Herausforderung für die internationale Nichtverbreitungspolitik, SWP-Studie, Stiftung Wissenschaft und Politik, Deutsches Institut für Internationale Politik und Sicherheit; Berlin, https://www.swp-berlin.org/publications/products/studien/2008_S14_hpl_ks.pdf.

entwickelt. Ziel ist es, die nationale Sicherheit in einem sehr umfassenden Sinne sicherzustellen, so dass nach Einschätzung von Beobachtern „Beijing’s strategic motives, means and constraints will significantly shape the nexus of geopolitics and technology in the years to come“. |⁵⁶

IV.2 Zivilklauseln

In Deutschland ist aus historischen Gründen in weiten Teilen der akademischen Welt eine „**Kultur der Friedensorientierung**“ fest verankert, die vielerorts die Etablierung von Zivilklauseln einschloss. Auch diese Entwicklung beruht auf der Annahme, zwischen Forschung zu zivilen und militärischen Zwecken oder aus friedlichen und nichtfriedlichen Motiven heraus klar unterscheiden zu können. Heute wird Deutschland eine „Kultur der militärischen Zurückhaltung“ attestiert, die sich als „Produkt außen- und sicherheitspolitischer Entwicklungen sowie innenpolitischer Aushandlungsprozesse“ |⁵⁷ herausgebildet hat.

Zivilklauseln |⁵⁸ sind in der Regel Selbstverpflichtungen von Hochschulen, nur in Einzelfällen Verpflichtungen in Hochschulgesetzen, die sich an das in Art. 26 GG |⁵⁹ verankerte Friedensgebot anlehnen. Demnach sollen Forschung, Lehre und Studium allein zivilen bzw. friedlichen Zwecken dienen. |⁶⁰ Mehr als

| ⁵⁶ „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, localization 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.; Hmaid, 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, S. 3, <https://merics.org/en/report/keeping-value-chains-home>.

| ⁵⁷ 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), S. 327–353, <https://doi.org/10.1515/sirius-2023-4002>.

| ⁵⁸ Ein Vorläufer der Zivilklausel war bereits im Gründungsvertrag des Kernforschungszentrums Karlsruhe 1956 aufgenommen worden, in diesem Fall auf Betreiben der Alliierten, die Wert auf die Entmilitarisierung der Forschung in Deutschland gelegt haben. Die Friedensbewegung hat in der Folge zur zivilen Ausrichtung öffentlicher Forschungseinrichtungen beigetragen – nicht zuletzt befördert von Studierenden.

| ⁵⁹ Artikel 26 Absatz 1 des Grundgesetzes lautet: „Handlungen, die geeignet sind und in der Absicht vorgenommen werden, das friedliche Zusammenleben der Völker zu stören, insbesondere die Führung eines Angriffskrieges vorzubereiten, sind verfassungswidrig. Sie sind unter Strafe zu stellen.“ <https://www.bundestag.de/parlament/aufgaben/rechtsgrundlagen/grundgesetz#1>.

| ⁶⁰ Untergesetzliche Zivil- oder Friedensklauseln finden sich an unterschiedlichen Stellen: im Leitbild einer Hochschule oder Forschungseinrichtung, in ihrer Grundordnung oder als Selbstverpflichtung des Senats. In der Grundordnung einzelner Hochschulen erfolgt ein ausdrücklicher Verweis auf die Wahrung der verfassungsrechtlich garantierten Wissenschaftsfreiheit, so in der Präambel der Universität Bielefeld (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>). Einzelne Hochschulen weisen ihrer Ethikkommission die Aufgabe zu, sich mit Fragestellungen zum möglichen Einsatz von Forschungsergebnissen für nicht-friedliche Zwecke auseinanderzusetzen, vgl. Grundordnung der Europa-Universität Viadrina Frankfurt (Oder) in der Fassung der ersten Änderungssatzung vom 06.11.2019, § 10 Abs. 8,

die Hälfte der Bundesländer, nämlich Baden-Württemberg, Bayern, Hamburg, Mecklenburg-Vorpommern, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, das Saarland und Sachsen, haben derzeit in ihren allgemeinen Hochschulgesetzen keine Zivilklausel verankert. Seit Juli 2024 hat Bayern in seinem Hochschulinnovationsgesetz „eine Beschränkung der Forschung auf zivile Nutzung (Zivilklausel)“ sogar für „unzulässig“ erklärt. |⁶¹ In den Hochschulgesetzen der anderen Länder ist eine Orientierung an einem friedlichen Zusammenleben vorgesehen, so in Berlin, Brandenburg, |⁶² Hessen, Bremen, Sachsen-Anhalt, Schleswig-Holstein und Thüringen. Die Länder Bremen und Thüringen haben zudem gesetzlich festgeschrieben, dass Hochschulen sich selbst eine Zivilklausel zu geben haben. |⁶³ **Die Wirkung von Zivilklauseln ist aus einer rechtlichen Perspektive angesichts der grundgesetzlich gewährleisteten Wissenschaftsfreiheit in der Praxis begrenzt**, wie Beispiele der Zusammenarbeit mit Akteuren aus dem militärischen Bereich wie z. B. der Bundeswehr zeigen. Gleichwohl sehen sich viele Akteure in Einrichtungen mit einer Zivil- oder Friedensklausel dieser auch verpflichtet.

https://www.europa-uni.de/de/universitaet/einrichtungen/stabsstellen/justizariat/zentrale-ordnungen/_dateien/grundordnung-2019.pdf. In Ausnahmefällen wird darüber hinaus dargelegt, wie in Konfliktfällen zu verfahren sei: „Die sich aus dieser Ordnung und dem Leitbild der Universität ergebende Beschränkung der Universität auf zivile Forschung stellt auch eine individuelle Verpflichtung für alle an der Universität forschenden Mitglieder und Angehörigen dar. Die Anzeige von Forschungsvorhaben gemäß § 66 Abs. 3 ThürHG muss die Einschätzung enthalten, dass der Forschungsgegenstand nicht unmittelbar Militär- oder Rüstungsforschung ist. Der Präsident oder eine von ihm beauftragte Stelle prüfen diese Einschätzung. Erfolgt diese Einschätzung nicht oder bestehen Zweifel an deren Begründetheit, ist der Antrag der Ethikkommission der Universität vorzulegen. Diese wird durch den Forschungsausschuss gemäß § 13 Abs. 3 gebildet. Der Ausschuss muss den Antragsteller anhören und auf dessen Vorschlag oder eigenen Beschluss zur Entscheidungsfindung weitere sachverständige Personen hinzuziehen. Der Präsident hat Antrags-, Teilnahme- und Rederecht. Der Präsident entscheidet abschließend auf Grundlage der Bewertung der Ethikkommission über die Unvereinbarkeit des Forschungsvorhabens mit der Zivilklausel gemäß § 5 Abs. 3 ThürHG. Der Präsident unterrichtet die Öffentlichkeit jährlich und in geeigneter Weise.“ 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.

|⁶¹ Bayerisches Hochschulinnovationsgesetz (BayHIG) vom 5. August 2022 (GVBl. S. 414, BayRS 2210-1-3-WK), das zuletzt durch § 14 des Gesetzes vom 23. 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>. Das Gesetz ist verfassungsrechtlich umstritten.

|⁶² Im Hochschulgesetz findet sich eine sehr offene Formulierung: „Die Hochschulen [...] setzen sich im Bewusstsein ihrer Verantwortung gegenüber der Gesellschaft und der Umwelt mit den möglichen Folgen einer Nutzung ihrer Forschungsergebnisse auseinander und wirken auf eine nachhaltige Ressourcennutzung an der Hochschule hin“ 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>.

|⁶³ 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>, und 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 und § 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. Empfehlungen zum Umgang mit Wissensrisiken und sicherheitsrelevanter Forschung

In den letzten Jahrzehnten ist das deutsche Wissenschaftssystem deutlich internationaler geworden. Es bestehen intensive globale Netzwerke, die vom Studierendenaustausch bis zur formalen Kooperation ganzer Einrichtungen reichen. Sich **international auszutauschen und zu kooperieren**, gehört – und gehörte immer schon – zum **Kern wissenschaftlichen Arbeitens**. Zudem wurde die Internationalisierung politisch gefordert und gefördert, nicht zuletzt, um die Qualität wissenschaftlichen Arbeitens im eigenen Land zu erhöhen. Sie gilt mittlerweile vermehrt als Wert an sich und fungiert als Indikator im Rahmen von Evaluationen.

In der neuen weltpolitischen Lage, die durch Systemrivalitäten in politischer, gesellschaftlicher, wirtschaftlicher und wissenschaftlicher Hinsicht geprägt ist, laufen offene Gesellschaften und ein offenes, international vernetztes Wissenschaftssystem jedoch Gefahr, sich zu gefährden, indem diese Offenheit gezielt genutzt und missbraucht wird (**Vulnerabilität offener Systeme**). Zugleich kann es auf Seiten der Wissenschaftlerinnen und Wissenschaftler zu einer zu weit gehenden Zurückhaltung kommen, wenn sie aus Sorge um die Wissenssicherheit und angesichts vielfach noch ungeklärter Rahmenbedingungen in dem in seiner Breite noch wenig ausgearbeiteten Feld der Wissenssicherheit Kooperationen nicht weiterführen, keine neue Zusammenarbeit suchen oder den Austausch verweigern (**Überreaktion/overprotection**).

Der Wissenschaftsrat sieht es als **dringliche Aufgabe an, in diesem Feld Handlungssicherheit zu schaffen**. Ansonsten besteht die **Gefahr des doppelten Verlusts**: Einerseits geht aus Unsicherheit die Bereitschaft zurück, mit Partnern in kritischen Ländern zusammenzuarbeiten, und andererseits zögern bestimmte Länder, mit Einrichtungen in Deutschland zusammenzuarbeiten – in beiden Fällen, weil die Rahmenbedingungen nicht geklärt und Prozesse in den Einrichtungen noch nicht implementiert sind.

Deutschland hat an dieser Stelle Nachholbedarf. Es bedarf einer **höheren Aufmerksamkeit für Wissenssicherheit** im Wissenschaftssystem. Andere Länder wie Kanada, die Niederlande oder Dänemark haben entsprechende Strategien und Maßnahmen zum Umgang mit Wissensrisiken bereits implementiert. |⁶⁴ Deutschland hat zudem einen Nachholbedarf, wenn es um die **Bedeutung sicherheitsrelevanter Forschung** geht. Auch an dieser Stelle gehen andere Länder schon weiter und wollen sicherheitsrelevante Forschung gezielter fördern. |⁶⁵

Für den Wissenschaftsrat ist entscheidend, dass kein Akteur im Wissenschaftssystem sich der geänderten weltpolitischen Lage und der neuen Wettbewerbssituation – bis hin zu systemischer Rivalität – in wissenschaftlicher, technologischer, wirtschaftlicher oder gesellschaftlicher Hinsicht vollständig entziehen kann. **Die unterschiedlichen Akteure im Wissenschaftssystem** – vom einzelnen Forschenden bis hin zum Gesetzgeber (vgl. C.I) – **sind gefordert, Verantwortung in diesem querschnittlichen Feld**, dessen Bedeutung massiv zugenommen hat, **zu übernehmen**, um sich über die Relevanz der eigenen Arbeiten für die Sicherheit und Resilienz des Gemeinwesens Rechenschaft abzulegen und um Wissenssicherheit herzustellen. Dabei ist sich der Wissenschaftsrat bewusst, dass es sich um ein in dieser Reichweite neues Feld handelt und es einer gemeinsamen Anstrengung bedarf, die durchaus mit zeitlichem und finanziellem Ressourcenaufwand verbunden ist. Diese Anstrengung wird das Wissenschaftssystem verändern und es stärker als bisher mit anderen Politikbereichen verbinden.

C.I GEMEINSAME VERANTWORTUNG GETEILT WAHRNEHMEN

Die Ausweitung von Forschungsfeldern, die potenziell sicherheitsrelevant sind oder inhärent einen Dual-Use-Charakter haben, die Konvergenz von Disziplinen, insbesondere im Zuge der Durchdringung wissenschaftlicher Arbeiten mit KI und Informationstechnologie, sowie die Proliferation von Akteuren mit unterschiedlichen strategischen Interessen verlangen nach einer **gestuften und vom Verständnis her subsidiären Zuständigkeit im Wissenschaftssystem**, um mit den gestiegenen Anforderungen an Wissenssicherheit und Sicherheitsrelevanz von Forschung umgehen zu können. Bindende rechtliche Vorgaben wie die der Exportkontrolle, seien sie auf nationaler, seien sie auf supranationaler Ebene, sind nur Teil einer Sicherheitsarchitektur. Es bedarf einer umfassenderen syste-

| ⁶⁴ Vgl. für einen knappen und aktuellen Überblick über die internationale Situation: GA von DFG und Leopoldina (2024): Wissenschaftsfreiheit und Sicherheitsinteressen in Zeiten geopolitischer Polarisierung. Fünfter Tätigkeits- und Sachstandsbericht; Berlin, S. 11 ff., <https://www.sicherheitsrelevante-forschung.org/publikation-taetigkeitsbericht2024/>.

| ⁶⁵ Vgl. 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>.

mischen Sicherheitsarchitektur. In einer solchen Governance haben die unterschiedlichen Ebenen jeweils ihre Verantwortung wahrzunehmen. Vor diesem Hintergrund empfiehlt der Wissenschaftsrat,

– dass die einzelnen **Wissenschaftlerinnen und Wissenschaftler sich explizit mit der Sicherheitsrelevanz ihrer Arbeiten auseinandersetzen** – und zwar in beide Richtungen: in Richtung einer Prüfung von Risiken sowie in Richtung einer Prüfung ihres möglichen Beitrags zur Schaffung von Sicherheit und Resilienz in Deutschland und Europa. Es sind die einzelnen Wissenschaftlerinnen und Wissenschaftler, die ihre Arbeiten am besten unter diesen beiden Gesichtspunkten einschätzen können, auch wenn sie nicht immer gleich die Potenziale ihrer technologischen Einsatzmöglichkeiten vor Augen haben. Gleichwohl haben sie eine tiefe Kenntnis ihres Forschungsgegenstands und ihrer Kooperationsbeziehungen. Ihr Engagement ist daher unerlässlich; sie können von dieser Aufgabe nicht entlastet werden. Allerdings kann eine einzelne Wissenschaftlerin oder ein einzelner Wissenschaftler diese Aufgabe ohne wirksame Unterstützungsleistungen und -strukturen nicht hinreichend bewältigen. Die Leitung muss Informationen bereitstellen, welche die Wissenschaftlerinnen und Wissenschaftler befähigt, ihre Verantwortung wahrzunehmen (vgl. C.II).

– dass die **Leitungen der unterschiedlichen wissenschaftlichen Einrichtungen und Organisationen sich strategisch auf die neue Situation einstellen** und sich intern darüber verständigen, welche Standards in der eigenen Einrichtung gelten sollen. Der Wissenschaftsrat betrachtet es als eine dringliche Leitungsaufgabe, Leitlinien zum Umgang mit Risiken und Potenzialen für die Organisation zu entwickeln sowie einen Prozess der Risikobetrachtung aufzusetzen und Ressourcen dafür bereitzustellen (vgl. C.III). Diese Maßnahmen beziehen sich auf unterschiedliche Leistungsdimensionen: von der Forschung über Lehre und Ausbildung bis zum Transfer. Ein besonderes Augenmerk ist auf Infrastrukturen zu legen, die – wie dargelegt (vgl. B.I) – in unterschiedlichen Hinsichten ein Wissensrisiko bergen können, insbesondere hinsichtlich ihrer informationstechnischen Möglichkeiten eines unerwünschten Wissensabflusses und unerwünschter Einflussnahme. Teil des Umgangs mit Wissenssicherheit sollte es auch sein, sich über eine Thematisierung in Forschung und Lehre zu verständigen. Studierende und Promovierende müssen frühzeitig sensibilisiert werden, zum Beispiel in Modulen zur guten wissenschaftlichen Praxis, um eine neue Selbstverständlichkeit im Umgang mit Fragen von Sicherheitsrelevanz und Wissenssicherheit zu schaffen.

– dass **Förderer Fragen nach Wissensrisiken und Sicherheitsrelevanz in ihre eigenen Verfahren integrieren.** Angesichts der geschilderten wissenschaftsinternen Entwicklungen als auch der weltpolitischen Veränderungen sollte geprüft werden, wie die Forderung nach Wissenssicherheit Teil des jeweiligen Fördersystems werden kann und wie der Umgang damit in die Leitlinien guter

wissenschaftlicher Praxis zu integrieren ist. |⁶⁶ Gleichfalls sollte auch auf unterschiedlichen Ebenen ein Bewusstsein dafür entwickelt werden, ob und in welchem Maße Förderprogramme und -formate sicherheitsrelevante Forschung im oben entwickelten umfassenden Sinne mit ermöglichen können (vgl. C.IV.2).

- dass die **staatliche Seite ressortübergreifend die notwendigen Voraussetzungen im Sinne von möglichst kohärenten Rahmenbedingungen** schafft (vgl. C.III.3). Dadurch können die übrigen Akteure im Wissenschaftssystem ihre Verantwortung – sowohl zum Schutz des Wissenschaftssystems als auch zur Mitwirkung bei sicherheitsrelevanten Fragen – auf einer verlässlichen politischen und transparenten Informationsgrundlage wahrnehmen. Dabei plädiert der Wissenschaftsrat für ein abgestimmtes Vorgehen von Bund und Ländern. Gleichmaßen notwendig ist es, sich europäisch abzustimmen.

Die Wahrnehmung der Verantwortung auf den unterschiedlichen Ebenen ist eine **dringliche Aufgabe**, die mit Aufwand verbunden ist. |⁶⁷ Dieser **Aufwand** sollte für die einzelnen Wissenschaftlerinnen und Wissenschaftler **möglichst begrenzt** sein und nicht bloß als ein weiteres Element einer wachsenden Bürokratie in Erscheinung treten. Ziel ist es, Handlungssicherheit zu schaffen. Allein im Sinne einer gemeinsamen Verantwortung lässt sich diese Aufgabe bewältigen.

C.II GOVERNANCE-LEITLINIEN FÜR DEN UMGANG MIT WISSENSRISIKEN UND SICHERHEITSRELEVANZ

Der Umgang mit Fragen von Wissenssicherheit und Sicherheitsrelevanz verlangt danach, **zwei Perspektiven miteinander zu verschränken**. Übergeordnet bedarf es politischer Rahmenbedingungen, um auch über die unterschiedlichen gesellschaftlichen Teilbereiche hinweg eine Kohärenz herzustellen. Die Perspektive der Wissenschaftlerinnen und Wissenschaftler ist zentral, insofern sie – bei ausreichender Sensibilität – mit ihrer Feldexpertise Risiken und Potenziale der Arbeiten am besten einschätzen können.

| ⁶⁶ Einige Förderer haben bereits darauf reagiert, so z. B. DFG (2023): Umgang mit Risiken in internationalen Kooperationen. Empfehlungen der DFG; Bonn, <https://www.dfg.de/resource/blob/289702/457ab05c902a521e6772bc5a25f0cd4d/risiken-int-kooperationen-de-data.pdf>. Vgl. auch Rat der Europäischen Union (2024): Empfehlungen des Rates vom 23. Mai 2024 zur Stärkung der Forschungssicherheit (C/2024/3510), <http://data.europa.eu/eli/C/2024/3510/oj>.

| ⁶⁷ Darauf hat auch das Bundesministerium für Forschung, Technologie und Raumfahrt (BMFTR) mit einem Positionspapier aufmerksam gemacht, vgl. ehemals Bundesministerium für Bildung und Forschung (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>.

Um in produktiver Weise zusammenwirken zu können, schlägt der Wissenschaftsrat **drei Leitlinien** für die **Governance** im Umgang mit Wissenssicherheit und Sicherheitsrelevanz vor:

1 – Prozesse entwickeln: Einschätzungen zu Fragen von Wissenssicherheit und Sicherheitsrelevanz von Wissenschaft unterliegen einem kontinuierlichen gesellschaftlichen Aushandlungsprozess. |⁶⁸ Eine Prozessorientierung ist auf allen Ebenen erforderlich, um rasch, flexibel und kontinuierlich auf eine sich dynamisch verändernde Situation reagieren zu können. Zugleich erhöhen etablierte Prozesse die Transparenz, schaffen Sicherheit für die einzelnen Wissenschaftlerinnen und Wissenschaftler und geben Raum für kontinuierliche Verbesserung. Zudem können sich Risiken und Potenziale von Forschungsarbeiten oder Kooperationsvorhaben im Laufe der Zeit verändern. Daher reicht es nicht aus, allein zu Beginn eines Vorhabens, eines Austauschs oder einer Kooperation einen Sicherheitscheck durchzuführen. Es bedarf einer hohen Sensibilität für die weitere Entwicklung der Aktivitäten im Laufe der Zeit. Dabei ist es erforderlich, die auf den unterschiedlichen Ebenen etablierten Prozesse gut miteinander zu verzahnen, um ein möglichst hohes Maß an Konsistenz und Kohärenz jenseits der Grenzen von Einrichtungen – bis hin zur staatlichen Ebene – zu schaffen.

2 – Unterstützung schaffen und vorhalten: Die einzelnen Wissenschaftlerinnen und Wissenschaftler sind in der Regel diejenigen, die das sicherheitsrelevante Potenzial und mögliche Sicherheitsrisiken ihrer Arbeiten am besten einschätzen können. Allerdings sind sie nicht immer in der Lage, die unterschiedlichen Risiken im Austausch und in der Kooperation mit der Vielfalt der Partner angemessen beurteilen zu können. Daher bedarf es Unterstützungsstrukturen auf unterschiedlichen Ebenen, die dazu beitragen, Risiken und Potenziale einschätzen und einen angemessenen Umgang damit entwickeln zu können. Der Wissenschaftsrat sieht sowohl die Leitungen der Einrichtungen in der Verantwortung, solche Unterstützungsangebote zu schaffen und vorzuhalten, als auch die Förderer und politisch Verantwortlichen (vgl. C.III). Eine angemessene Struktur auf nationaler Ebene erlaubt es, sich einrichtungsübergreifend zu verständigen, sich europäisch und international zu vernetzen und gegebenenfalls abzustimmen sowie auf Veränderungen der weltpolitischen Lage zügig zu reagieren (vgl. C.III.3). Dadurch können Konsistenz und Kohärenz auf übergeordneter Ebene gestärkt werden. Der Wissenschaftsrat weist auf Probleme der Abhängigkeit von kommerziellen Anbietern hin. Er empfiehlt, möglichst auf europäischer Ebene ein von der öffentlichen Hand bereitgestelltes Angebot zu entwickeln.

| ⁶⁸ Vgl. hierzu die Einschätzung von Wolfgang Bonß (2014): „Bei Risikoproblemen hingegen gibt es keine eindeutige und endgültige Lösung; Risikoprobleme zeichnen sich vielmehr dadurch aus, dass die anvisierten Lösungen stets insofern ‚suboptimal‘ sind, als sie nicht ‚endgültig‘ sind. Sie ziehen vielmehr selbst wieder Unsicherheiten nach sich, die entweder neu erzeugt oder jetzt erst sichtbar werden.“ Ders.: (Un-)Sicherheit in der Moderne, in: Zoche, P.; Kaufmann, S.; Haverkamp, R. (Hrsg.) : Zivile Sicherheit. Gesellschaftliche Dimensionen gegenwärtiger Sicherheitspolitiken; Bielefeld, S. 43–70, hier S. 46, <https://doi.org/10.14361/transcript.9783839414354.43>.

3 – Ländersensibel vorgehen: Vielfach wird bisher im Umgang mit Fragen der Wissenssicherheit ein länderagnostisches Vorgehen favorisiert. Angesichts der weltpolitischen Situation einerseits und der Ausweitung von Forschungsfeldern mit einem inhärenten Dual-Use-Potenzial andererseits empfiehlt der Wissenschaftsrat ein ländersensibles Vorgehen. Dies ermöglicht, lokale, regionale und nationale Kontexte angemessen zu berücksichtigen, rechtliche und politische Interessen des Gegenübers gut einzuschätzen sowie gegebenenfalls kritische Länder zu identifizieren. |⁶⁹ Ziel ist es, den Austausch möglichst sicher zu gestalten und im eigenen – strategischen oder wissenschaftlichen – Interesse liegende Kooperationen auch mit solchen Partnern zu ermöglichen, die in unterschiedlichen Hinsichten herausfordernd sind.

C.III WISSENSRISIKEN ERKENNEN UND MANAGEN

Wissenschaftliches Arbeiten ist hier umfassend verstanden und zielt nicht allein auf Forschungsarbeiten, sondern auch auf Personalaustausch oder Kooperationsvereinbarungen ab. Nach Auffassung des Wissenschaftsrats ist in weiten Teilen des deutschen Wissenschaftssystems das **Bewusstsein davon, welche Risiken bestehen** und wie wissenschaftliches Arbeiten zur Sicherheit sowie Resilienz des Gemeinwesens beitragen können, **noch nicht deutlich genug ausgeprägt**. Wenn es vorhanden ist, dann bezieht es sich vor allem auf Nutzungsoptionen, die im militärischen Bereich liegen. Hier besteht in der Regel eine erste Intuition bei den verantwortlich Forschenden. Allerdings ist eine vertiefte Bewusstseinsbildung in der Breite erforderlich, um mögliche Risiken und Potenziale der eigenen Arbeiten frühzeitig zu identifizieren.

Der Wissenschaftsrat empfiehlt jeder Einrichtung, eine **schlanke und zugleich klare Risikobetrachtung zu erarbeiten und zu implementieren**. Je nach Risikoprofil und Größe der Einrichtung kann diese unterschiedlich ausgestaltet sein. Dies obliegt der einzelnen Hochschule oder der einzelnen Forschungseinrichtung. Entscheidend ist, dass Wissenschaft und Verwaltung gemeinsam einen **pragmatisch handhabbaren Prozess** entwickeln. Ein pragmatisches Vorgehen schafft Akzeptanz auf der wissenschaftlichen Seite und erhöht die Bereitschaft, die Risikobetrachtung zu durchlaufen. Ohne die Bereitschaft der

| ⁶⁹ Vgl. hierzu auch die Aufgabe der empfohlenen nationalen Plattform (C.III.3). Hilfreich sind an dieser Stelle dynamisch sich entwickelnde Listen kritischer Länder, wie z. B. die Staatenliste im Sinne von § 13 Abs. 1 Nr. 17 SÜG vom Bundesministeriums des Innern und für Heimat (BMI), <https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/sicherheit/staatenliste-para-13-anleitung-sicherheitserklaerung.html>. Oder die Embargoliste der BAFA, https://www.bafa.de/SharedDocs/Downloads/DE/Aussenwirtschaft/afk_embargo_uebersicht_laenderbezogene_embargos.html. Auch auf europäischer Ebene und in anderen Ländern existieren solche Listen, so etwa die EU Sanction Map, vgl. <https://www.sanctions-map.eu/#/main>.

einzelnen Wissenschaftlerin, des einzelnen Wissenschaftlers, sich mit den Risiken auseinanderzusetzen, läuft der Prozess – vor allem jenseits der verbindlichen rechtlichen Vorgaben seitens des Zoll- und Exportkontrollrechts – ins Leere.

III.1 Fallbezogene Einzelprüfung und kollegialer Austausch

Wissensrisiken können – wie eingangs erläutert (vgl. B.III) – fünf unterschiedliche Dimensionen haben. Dazu zählen (1) der unerwünschte Wissensabfluss und (2) die unerwünschte Einflussnahme auf das Wissenschaftssystem. Zudem gilt es (3) zu fragen, ob die eigene Forschung hinreichend unabhängig erfolgt – sowohl in finanzieller wie auch in wissenschaftlicher Hinsicht. Darüber hinaus sind (4) Interferenzen mit anderen gesellschaftlichen Bereichen zu bedenken sowie (5) (forschungs)ethische Prinzipien zu wahren. Grundlage angemessener Wissenssicherheit ist, dass die einzelne Wissenschaftlerin, der einzelne Wissenschaftler die **Wissensrisiken** des eigenen Arbeitens prüft und erkennt. Exemplarische Leitfragen (vgl. Anhang 1) können im Rahmen dieser **fallbezogenen Einzelprüfung** (vgl. auch Abbildung 1) helfen, diese Risiken besser einschätzen zu können und hinreichend risikobewusst vorzugehen.

In einem ersten Schritt obliegt es folglich der einzelnen Wissenschaftlerin, dem einzelnen Wissenschaftler, hier Verantwortung zu übernehmen. Der Wissenschaftsrat hat **fünf Anhaltspunkte** identifiziert, die eine **weitergehende Risikobetrachtung nahelegen**:

1 – Besonders sensible Forschungsthemen: Ein Anhaltspunkt kann der Bezug des Themas zu Feldern sein, die als besonders sensibel gelten. Bisher erfolgt eine Identifikation von solchen Feldern noch nicht konsequent über Ressort- und Landesgrenzen hinweg. Der Wissenschaftsrat empfiehlt, zentral für Deutschland und möglichst im Einklang mit den europäischen Partnern solche Forschungsfelder zu identifizieren, auch wenn es kaum möglich sein wird, sich gerade angesichts der enormen Geschwindigkeit, mit der sich bestimmte Felder entwickeln, abschließend zu verständigen. Vielmehr ist dies eine kontinuierliche Aufgabe, die auf eine möglichst konsistente Informationsbasis – im Sinne eines living document – für das Wissenschaftssystem zielt (vgl. hierzu auch C.III.3).

Als Beispiel für ein sensibles Thema in der medizinischen Forschung sei auf KI-gestützte Systeme der virtuellen Toxizitätsprüfung von Wirkstoffkandidaten mit Blick auf Medikamentenentwicklungen verwiesen. Solche Systeme sind in der Lage, auch besonders schädliche Moleküle zu identifizieren. Mit wenig Aufwand lassen sich in der Folge innerhalb weniger Stunden sowohl bekannte Gifte wie Sarin oder Tabun auffinden als auch bislang größtenteils unbekannte hochtoxische und potenziell waffentaugliche Substanzen entdecken. Selbst wenn es weiterer Forschung bedarf, um solche Moleküle zu stabilisieren und ihre Wirkung im Organismus zu prüfen, birgt der Einsatz einer

2 – Kooperationspartner aus kritischen Ländern: Ein weiterer Anhaltspunkt für erhöhte Aufmerksamkeit ist durch Akteure und Akteurskonstellationen gegeben, wie im Rahmen der Reflexion zum Dual-Use-Begriff erläutert wurde (vgl. B.II). Die persönlichen Motive, die staatlichen Interessen oder die Interessen von Unternehmen wie etwa großen Technologieunternehmen sind nicht immer offensichtlich. Daher kann der Studierendenaustausch oder die Kooperation mit wissenschaftlichen oder wirtschaftlichen Kooperationspartnern aus kritischen Ländern Risiken bergen. Für eine fundierte Einschätzung sind umfassende Informationen erforderlich (vgl. C.III.3).

Voraussetzung ist, dass man sich immer wieder darüber verständigt, welches Land bzw. welches Unternehmen national und gegebenenfalls europäisch hier von Relevanz ist – vergleichbar dem Austausch über sensible Forschungsfelder (vgl. C.III.3). |⁷¹

Als Beispiel sei auf den geplanten Besuch eines ausländischen Wissenschaftlers aus einem als kritisch eingestuften Land verwiesen, der an einem elektrotechnischen Vorhaben zur Optimierung von Strom-, Gas- oder Wassernetzen, m. a. W. kritischer Infrastruktur, in Deutschland unter Anwendung von KI-Methoden mitwirken wollte. Ein Risiko von Wissensabfluss besteht dabei in zwei Hinsichten: Zum einen können die den KI-Methoden zugrundeliegenden Modelle so modifiziert werden, dass sie anstelle einer effizienten Gestaltung des Systems die Infrastruktur beschädigen oder sogar lahmlegen können. Zum anderen beruht eine KI-basierte Optimierung auf detaillierten Datenbeständen, so dass ein Zugriff darauf eine umfassende Einsicht in die strukturellen Eigenschaften der Infrastruktur ermöglicht. Damit werden der Aufbau und die Funktionsgrundlage der kritischen Infrastruktur in Deutschland und/oder in Europa offengelegt und verwundbar(er).

3 – Mittelbare Zusammenarbeit mit kritischen Partnern: Die Zusammenarbeit mit Einrichtungen – seien es akademische oder seien es Unternehmen –, deren Muttersitz sich in einem der als kritisch identifizierten Länder befindet,

|⁷⁰ Urbina, F.; Lentzos, F.; Invernizzi, C. et al. (2022). Dual use of artificial-intelligence-powered drug discovery, in: *Nature Machine Intelligence*, 4, S. 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>. Laut Aussage des 5. Tätigkeitsberichts des GA haben die Autoren die Studie durchgeführt, um auf potenzielle Missbrauchsrisiken von Systemen Künstlicher Intelligenz (KI) aufmerksam zu machen, vgl. GA von DFG und Leopoldina (2024): Wissenschaftsfreiheit und Sicherheitsinteressen in Zeiten geopolitischer Polarisierung. Fünfter Tätigkeits- und Sachstandsbericht; Berlin, S. 73, <https://www.sicherheitsrelevante-forschung.org/publikation-taetigkeitsbericht2024/>.

|⁷¹ Vgl. auch die Hinweise auf Länderlisten in Fußnote 69.

kann Anlass für eine Prüfung sein. Denn auch wenn diese Forschungs- und Bildungseinrichtungen oder Unternehmen Dependancen in Europa unterhalten, kann die Kooperation risikobehaftet sein. Intendiert oder indirekt können hier strategische Interessen eine Rolle spielen, etwa wenn der Hauptpartner nicht offengelegt wird oder abhängige Beteiligte unter Druck gesetzt werden können. Dabei kann es sich um Personalaustausch, um Kooperationen oder auch um klassische Auftragsforschung handeln. Vertiefte Informationen dazu sind unerlässlich, um die Situation angemessen einschätzen zu können.

Als Beispiel für eine Zusammenarbeit „über Bande“ kann der im Januar 2025 bekannt gewordene Fall gelten, in dem ein Deutscher über mehrere Jahre (2017–2024) für einen chinesischen Geheimdienstmitarbeiter gearbeitet hat, um Erkenntnisse zu Bootsmotoren, Sonarsystemen, Flugzeugschutzsystemen, Antrieben für Panzerfahrzeuge sowie militärisch nutzbaren Drohnen zu erlangen. Dabei wurden Kontakte zur Forschungseinrichtung über ein in Deutschland ansässiges Unternehmen hergestellt. Das Kooperationsabkommen der Universität wurde dann mit dem in Deutschland ansässigen Unternehmen abgeschlossen, das jedoch mit dem chinesischen Geheimdienst zusammenarbeitete. |⁷²

4 – Forschungsstandort mit sensitiven Technologien: Der Einsatz sensibler Technologien wie etwa Geräte oder Methoden ist ebenfalls ein Anhaltspunkt für die Notwendigkeit, der Sicherheitsrelevanz eine erhöhte Aufmerksamkeit zu schenken. Dabei kann es sich um explizit gelistete und exportregulierte Güter wie beispielsweise Laser- oder Linsenanlagen handeln. Aber auch relativ einfache Laboraufbauten, um sensitive Forschungsergebnisse zu erzielen, gehören dazu.

So gibt es den Fall, dass eine Besuchsdelegation die Möglichkeit erhielt, Einblick in Ausstattung und Methodik einer Einrichtung zu gewinnen. Auch wenn das Forschungsthema selbst nicht sensibel ist, könnte die Ausstattung von Interesse sein. So ließ sich beobachten, dass unangekündigt weitere ausländische Delegationsmitglieder erschienen und sich von der Führung entfernten. Dadurch konnten sie Aufnahmen von der Ausstattung der Forschungsabteilung machen und wertvolle Hinweise für andere Aktivitäten gewinnen. |⁷³

|⁷² Vgl. Generalbundesanwalt beim Bundesgerichtshof (2025): Anklage wegen mutmaßlicher geheimdienstlicher Agententätigkeit erhoben, 09.01.2025, <https://www.generalbundesanwalt.de/SharedDocs/Pressemitteilungen/DE/2025/Pressemitteilung-vom-09-01-2025.html>.

|⁷³ Vgl. u. a. BfV (2022): Informationsblätter zum Wirtschaftsschutz. Spionage in Wissenschaft und Forschung; Berlin, S. 4, <https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/wirtschafts-wissenschaftsschutz/2023-01-17-infoblatt-spionage-in-wissenschaft-und-forschung.pdf>.

5 – **Anwendungsnähe:** Um das Potenzial des möglichen unmittelbaren Missbrauchs zu erfassen, kann das TRL als Anhaltspunkt dienen. Bis einschließlich TRL 3 wird oft davon ausgegangen, dass eine mögliche Nutzung noch zu unvorhersehbar sei, um eine sinnvolle Risikobewertung vorzunehmen. Allerdings gibt es Felder, wie das der Kryptographie oder das der KI, in denen die Zeit zwischen grundlegender Entdeckung und Entwicklung eines Prototyps unter einem Jahr liegen kann, so dass auf diesen Gebieten das TRL weniger aussagekräftig ist. Aber nicht allein in diesen Feldern sollte die Beschleunigung der Umsetzung mit bedacht werden.

Als Beispiel kann auf den Wunsch eines chinesischen Wissenschaftlers verwiesen werden, der an einem Forschungsvorhaben zu Verbundwerkstoffen und Fertigungskonzepten auf einem TRL 3–5 mitarbeiten wollte. Das Forschungsvorhaben ermöglicht eine Massereduktion mittels Ersatzes metallischer durch polymere Werkstoffe in Trägertechnologien wie etwa dem Flugzeugbau. Der Mitarbeiter hat die Nanjing University of Aeronautics and Astronautics (NUAA) besucht, die zu den Seven Sons of National Defence gehört und dem Ministry of Industry and Information Technology untergeordnet ist. Wäre diesem Wunsch entsprochen worden, so hätte eine Zusammenarbeit mit dem chinesischen Militär bei großer Anwendungsnähe bestanden.

Diese **Anhaltspunkte** können nicht isoliert im Sinne einer Checkliste betrachtet werden, sondern sind **in einer Gesamtschau zu beurteilen**. Bei einem TRL 2 in einem unkritischen Forschungsfeld könnte eine reine Kooperation ohne Personalaustausch auch mit Partnern aus kritischen Ländern als unproblematisch eingestuft werden. Sollte die Gesamtschau der Anhaltspunkte aber nahelegen, dass sicherheitsrelevante Aspekte vorliegen, so empfiehlt der Wissenschaftsrat den einzelnen Wissenschaftlerinnen und Wissenschaftlern, eine **weitere Risikobetrachtung** zu durchlaufen. Gilt ein Risiko im Anschluss als wahrscheinlich, so sollte das Vorhaben nicht oder allein unter klar definierten Randbedingungen – in Rücksprache mit den Kommissionen für Ethik sicherheitsrelevanter Forschung (KEF) – realisiert werden.

Ist ein oder sind mehrere Anhaltspunkte gegeben und der oder die Einzelne ist sich unsicher, ob ein Risiko besteht, so sollte als nächste Stufe ein **kollegialer Austausch – im Folgenden als dialogisches Verfahren bezeichnet** – erfolgen. Ein Gespräch mit Kolleginnen und Kollegen kann zu einer klareren Einschätzung von Risiken und Potenzialen der eigenen Arbeiten führen. Der Wissenschaftsrat empfiehlt es daher **als zweiten Schritt der Risikobetrachtung**. Denn eine solche Einschätzung ist vielschichtig und läuft in der Regel – mit Ausnahme des rechtlich geregelten Bereichs der Exportkontrolle – nicht auf einfache Ja-Nein-Entscheidungen hinaus. Ohne direkt in einen formalisierten Prozess einzusteigen, kann der kollegiale Austausch helfen, eigene Interessen und mögliche Risiken besser zu reflektieren. Ob Ansprechpersonen für Wissensrisiken auf Fachbereichs- oder Fakultätsebene oder auf höheren Ebenen etabliert werden

oder ob solche Aufgaben durch Ombudspersonen für andere Fragen übernommen werden können, muss in der einzelnen Einrichtung oder Organisation entschieden werden. Dies hängt vom Risikoprofil und der Größe der Einrichtung ab (vgl. C.III.2). Entscheidend ist, dass die Einrichtungsleitung gegebenenfalls Ansprechpersonen bestimmt, die in der Hochschule oder dem Forschungsinstitut bekannt gemacht und ihrerseits geschult und unterstützt werden sollten.

Ein solches **dialogisches Verfahren** wie das hier vorgeschlagene, das auf Sensibilisierung und kollegialen Austausch setzt, ermöglicht es, dass weitere Prozessschritte nur dann angestoßen werden, wenn sie erforderlich sind und nicht allein, um sich abzusichern. Dadurch werden Verwaltung und/oder die in den Einrichtungen vorhandenen Gremien wie etwa die an vielen Einrichtungen vorhandenen KEFs nicht überlastet. Sie werden erst in einem dritten Schritt eingeschaltet (vgl. C.III.3).

In Zukunft ist es wichtig, dass eine **Sensibilisierung für Fragen der Wissenssicherheit und Sicherheitsrelevanz systematisch in Lehre und Ausbildung** – spätestens in der Promotionsphase – integriert wird, wie zum Beispiel in Modulen zur guten wissenschaftlichen Praxis.

III.2 Strategische Leitungsaufgabe: Risikobetrachtung strukturell verankern

Im Sinne der gemeinsamen Verantwortung (vgl. C.I) trägt auch die Leitung einer Hochschule oder Forschungseinrichtung Verantwortung für den Umgang mit den Themen Wissenssicherheit und sicherheitsrelevante Forschung in der eigenen Einrichtung. Sie ist gefordert, dafür Sorge zu tragen, an der Einrichtung **Kompetenzen aufzubauen, Beratung anzubieten und einen Abwägungsprozess zu etablieren.**

Die großen Hochschulen und Forschungseinrichtungen sind bereits so aufgestellt, dass Fragen der **Exportkontrolle**, die auch von (straf)rechtlicher Relevanz sind, im Zusammenspiel mit dem Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) behandelt werden können. Die **Initiative**, die Risikobetrachtung zu starten, liegt in der Regel bei der einzelnen Wissenschaftlerin, dem einzelnen Wissenschaftler (vgl. C.III.1). Einige Hochschulen und Forschungseinrichtungen haben die Identifikation von Risiken – insbesondere mit Blick auf die Exportkontrolle – in ihre formalen Abläufe wie Rekrutierungs- oder Dokumentenmanagementprozesse integriert. Dadurch kann die Einrichtung die Initiative übernehmen und muss es in bestimmten Fällen auch, um möglichen Schaden niedrig zu halten, sich nicht dem Vorwurf eines Organisationsverschuldens auszusetzen

und die einzelnen Forschenden zu entlasten. Einige Hochschulen und Forschungseinrichtungen haben die Position eines bzw. einer Beauftragten etabliert. |⁷⁴

An diese Strukturen oder andere noch zu etablierende (vgl. C.III.3) können Forschungseinrichtungen oder einzelne Hochschulen anknüpfen, um auch die sicherheitsrelevanten Fragen, die im Wesentlichen im vorrechtlichen Bereich liegen, behandeln zu können. Aus Sicht des Wissenschaftsrats kann es keine „one-size-fits-all“-Lösung geben. Vielmehr sind die **Leitungen** von Hochschulen und Forschungseinrichtungen **gefordert, angepasst an Größe und Risikoprofil ihrer Einrichtung entsprechende Unterstützungsstrukturen und Prozesse aufzubauen** und dabei auch Fragen der Daten- und Cybersicherheit zu berücksichtigen.

Der Wissenschaftsrat plädiert für schlanke Lösungen und empfiehlt ausdrücklich aus Gründen des effizienten Ressourceneinsatzes sowie der Bündelung von Kompetenzen **einrichtungsübergreifende Modelle**. |⁷⁵ In jedem Fall liegt es in der Verantwortung der Leitung, die einzelnen Wissenschaftlerinnen und Wissenschaftler hinreichend zu unterstützen. Der Aufbau schlanker Strukturen und Prozesse – an den Einrichtungen oder einrichtungsübergreifend – ist notwendig und sollte so rasch wie möglich erfolgen, sofern noch nicht geschehen. Keinesfalls sollte aber die formelle Befassung einer Kommission mit Forschungsprojekten der Regelfall sein; die Selbstprüfung und das dialogische Verfahren sollten als wirksame Filter fungieren.

Viele Hochschulen und Forschungseinrichtungen haben bereits **Ansprechpersonen** für sicherheitsrelevante Forschung benannt oder eine KEF gebildet, deren Kernkompetenz in der ethischen Bewertung von und Beratung zu Missbrauchspotenzialen konkreter Forschungsergebnisse und -methoden an den jeweiligen Einrichtungen liegt. Aufgrund des steigenden Bedarfs richten immer mehr Hochschulen und Forschungseinrichtungen KEFs ein oder beauftragen Personen mit einer solchen Aufgabe der Risikobetrachtung. |⁷⁶

| ⁷⁴ Diese Position sollte – so die Empfehlung der BAFA – „organisatorisch und personell außerhalb der unmittelbar im Bereich der wissenschaftlichen Forschung tätigen Personen stehen. Bei kleineren Organisationen kann die Aufgabe einer bestehenden Organisationseinheit (z. B. Rechtsabteilung, Revision) übertragen werden“ BAFA (2022): Handbuch Exportkontrolle und Academia, 2. Aufl.; Eschborn, S. 107, https://www.bafa.de/SharedDocs/Downloads/DE/Aussenwirtschaft/afk_aca_broschuere_handbuch.html.

| ⁷⁵ Mit Blick auf die digitale Sicherheit haben die bayrischen Universitäten 2023 den Grundstein für ein einrichtungsübergreifendes Netzwerk gelegt, vgl. <https://www.utn.de/2023/03/21/forschungsnetzwerk-fur-digitale-sicherheit/>. Bezogen auf ethische Fragen haben sich die bayrischen Hochschulen für angewandte Wissenschaften zu einem Netzwerk zusammengeschlossen und eine gemeinsame Ethikkommission zur Bewertung ethischer und rechtlicher Aspekte von Forschungsarbeiten geschaffen, vgl. <https://www.gehba.de/home>.

| ⁷⁶ Vgl. hierzu die Analyse des GA von DFG und Leopoldina (2024): Wissenschaftsfreiheit und Sicherheitsinteressen in Zeiten geopolitischer Polarisierung. Fünfter Tätigkeits- und Sachstandsbericht; Berlin, S. 37 ff., <https://www.sicherheitsrelevante-forschung.org/publikation-taetigkeitsbericht2024/>.

Der Wirtschaftssektor hat sich bereits umfassender auf die sich seit einigen Jahren zuspitzende Risikolage eingestellt. So haben Unternehmen vielfach entsprechend ihrem Risikoprofil sog. Compliance-Management-Systeme (CMS) aufgebaut. |⁷⁷ Mit Blick auf die gesetzlichen Bestimmungen im Bereich der Exportkontrolle werden sie als **Internal Compliance Programme (ICP)** bezeichnet. Auch im Wissenschaftssystem könnten solche ICP, die der proaktiven Verhinderung von Verstößen gegen das Außenwirtschaftsrecht dienen, aufgebaut werden. Mit einem entsprechend adaptierten System könnten sich auch Hochschulen und Forschungseinrichtungen systematisch vor einer straf- oder ordnungswidrigkeitsrechtlichen Verantwortung im Exportrecht und vor Reputationsschäden schützen. Mittel- bis langfristig könnte sich – vergleichbar der Situation für Wirtschaftsunternehmen – die **Möglichkeit einer Zertifizierung** eines auf das Wissenschaftssystem zugeschnittene ICP anbieten. |⁷⁸ Wirtschaftsunternehmen können privilegierte Verfahren beim BAFA und Zoll so nutzen, dass straf- und ordnungswidrigkeitsrechtliche Risiken im Umgang mit Dual-Use-Gütern minimiert werden und die Effizienz im Prozess erhöht wird. Eine solche Zertifizierung ist für Einrichtungsleitungen attraktiv und entlastend, insofern im Zweifelsfall nachgewiesen werden kann, dass kein Organisationsverschulden vorliegt.

III.3 Nationale Plattform für Wissenssicherheit einrichten

In den letzten Jahren sind innerhalb des Wissenschaftssystems **unterschiedliche Initiativen der Selbststeuerung** entstanden, um mit ethischen Herausforderungen sowie Risiken internationaler Kooperation und Mobilität umgehen zu können. So haben die Deutsche Forschungsgemeinschaft (DFG) und die Nationale Akademie der Wissenschaften Leopoldina 2015 den **Gemeinsamen Ausschuss zum Umgang mit sicherheitsrelevanter Forschung (GA)** geschaffen, der sich mit ethischen Fragen wie etwa Missbrauchspotenzialen bestimmter Forschungen beschäftigt und zunehmend mit sicherheitsrelevanten – auch rechtlich relevanten – Aspekten von Forschung konfrontiert ist. |⁷⁹ Der GA kooperiert mit den an vielen Hochschulen und Forschungseinrichtungen gegründeten KEFs.

Mit Blick auf internationale Kooperationen ist 2019 das **Kompetenzzentrum für Internationale Wissenschaftskooperationen (KIWi)** – angebunden an den

|⁷⁷ Vgl. hierzu auch BAFA (2022): Handbuch Exportkontrolle und Academia, 2. Aufl.; Eschborn, S. 101 f., https://www.bafa.de/SharedDocs/Downloads/DE/Aussenwirtschaft/afk_aca_broschuere_handbuch.html.

|⁷⁸ Vgl. BAFA (2022): Firmeninterne Exportkontrolle. Betriebliche Organisation im Außenwirtschaftsverkehr, 3. Aufl.; Eschborn, v. a. S. 21. https://www.bafa.de/SharedDocs/Downloads/DE/Aussenwirtschaft/afk_merkblatt_icp.html.

|⁷⁹ Der GA verfügt über eine Geschäftsstelle in Berlin, die dem Präsidialbüro der Leopoldina angegliedert ist. Neben Aufwendungen der Leopoldina wird die Geschäftsstelle auch von der DFG, Fraunhofer-Gesellschaft (FhG), Helmholtz-Gemeinschaft, Leibniz-Gemeinschaft und der Max-Planck-Gesellschaft auf der Grundlage einer Kooperationsvereinbarung getragen, vgl. <https://www.sicherheitsrelevante-forschung.org/geschaeftsstelle/>.

Deutschen Akademischen Austauschdienst e. V. (DAAD) – gegründet worden. |⁸⁰ Vornehmlich aufbauend auf der Regionalexpertise des DAAD berät das KIWi deutsche Hochschulen in Fragen internationaler Kooperationen und berücksichtigt zunehmend die damit verbundenen sicherheitsrelevanten Risiken. Alle Initiativen, der GA im Zusammenspiel mit den KEFs wie auch das KIWi, leisten neben der **Beratungsarbeit** auch wertvolle und dringend notwendige **Sensibilisierungs- und Vernetzungsarbeit**.

Der Wissenschaftsrat würdigt diese unterschiedlichen Aktivitäten ausdrücklich. Sie sind unabdingbar für das deutsche Wissenschaftssystem. Allerdings sieht er – gerade vor der eingangs geforderten subsidiären Zuständigkeit (vgl. C.I) – **auf nationaler Ebene eine Leerstelle**. Denn derzeit mangelt es erstens an einer nationalen Positionierung, um einen möglichst hohen Grad an Kohärenz über alle wissenschaftlichen Einrichtungen im Umgang mit sicherheitsrelevanten Fragen schaffen zu können. Zweitens sind die Wissenschaftlerinnen und Wissenschaftler sowie die Einrichtungen darauf angewiesen, sich spezifische Informationen zu sicherheitsrelevanten Aspekten ihrer Vorhaben selbst zu beschaffen. Derzeit müssen sie dabei auf Quellen zurückgreifen, die – wie etwa der ASPI-Tracker |⁸¹ – nur von begrenztem Informationsgehalt sind |⁸² oder bei denen unklar ist, welchen Qualitätsstandards sie genügen. Zudem fehlt eine koordinierte und übergreifende Unterstützung auf nationaler Ebene, wenn wissenschaftliche Einrichtungen oder Organisationen sich insbesondere strategisch hinsichtlich ihrer internationalen Zusammenarbeit informiert aufstellen wollen. Daher plädiert der Wissenschaftsrat dafür, **eine Nationale Plattform für Wissenssicherheit** einzurichten, die folgende Funktionen übernehmen soll:

1 – Abstimmung und Positionierung: Die Dynamik und Unübersichtlichkeit weltpolitischer Entwicklungen einerseits und technologischer Fortschritte andererseits verlangen nach einem **kontinuierlichen Austausch, um die Perspek-**

| ⁸⁰ Aufbauend auf einer Empfehlung des Wissenschaftsrats von 2018 wurde das Kompetenzzentrum für Internationale Wissenschaftskooperationen (KIWi) als zentrale Beratungsstelle zu internationalen Kooperationen insbesondere für Hochschulen gegründet. Seitdem hat sich das Aufgabenportfolio hinsichtlich der Einschätzung von Wissensrisiken und forschungsrelevante Rechtsfragen erweitert. Das Auswärtige Amt und das BMFTR unterstützen die Arbeit des KIWi finanziell, vgl. <https://www.daad.de/de/infos-services-fuer-hochschulen/kompetenzzentrum/ueber-uns/#special> und den ausführlicheren Bericht in der DUZ – Magazin für Wissenschaft und Gesellschaft: DAAD (Hrsg.) (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.

| ⁸¹ Tracker des Australian Strategic Policy Institutes. Dieser bezieht sich ausschließlich auf China und wurde 2019 zum letzten Mal aktualisiert (vgl. <https://unitracker.aspi.org.au/>). Zu bedenken ist auch die Finanzierung des Trackers, so dass es sich nicht um eine neutrale Instanz handelt.

| ⁸² Eine solche Leerstelle wird auch von anderen Akteuren im Wissenschaftssystem gesehen. Die DFG hat in ihren Impulsen für die neue Legislaturperiode die „Finanzierung einer zentralen Beratungsstelle für die Wissenschaft“ gefordert, DFG (2025): Erkenntnisgeleitete Forschung als Fundament für die internationale Wettbewerbsfähigkeit Deutschlands. Impulse der DFG für die 21. Legislaturperiode des Deutschen Bundestages; Bonn, S. 12, <https://www.dfg.de/resource/blob/352134/908b9ec587e758a0e5d25f8f0c317706/250226-impulspapier-legislaturperiode-data.pdf>.

tiven der verschiedenen Akteure auf der wissenschaftlichen und der staatlichen Seite zusammenzubringen. Verantwortliche in Ressorts und Ressortforschungseinrichtungen, gegebenenfalls auch Vertreterinnen und Vertreter der Sicherheitsdienste sowie Vertreterinnen und Vertreter der Länder gewinnen einen vertieften Einblick in aktuelle Forschungsstände in sensiblen Feldern und ein breiteres Verständnis für die Logik und Interessenlage der wissenschaftlichen Akteure. Umgekehrt gewinnen die wissenschaftlichen Akteure Einblicke in die übergeordneten politischen Implikationen. Eine Positionierung zum Umgang mit Wissensrisiken unter Einbeziehung der unterschiedlichen wissenschaftlichen und staatlichen Akteure erlaubt es damit, **orientierend** in das deutsche Wissenschaftssystem hineinzuwirken und eine **Positionierung Deutschlands** in dieser Hinsicht **im europäischen Kontext** fundiert vorzubereiten.

In dieser Weise werden die Rahmenbedingungen geschaffen, die einen möglichst hohen Grad an **Abstimmung im Zusammenwirken der staatlichen Seite mit der wissenschaftlichen Seite** herzustellen helfen. Diese Rahmenbedingungen schaffen eine verlässliche und transparente Grundlage für das Handeln wissenschaftlicher Akteure, so dass sie ihre Verantwortung im System der gestuften Zuständigkeiten angemessen wahrnehmen können (vgl. C.I).

2 – Kompetenzaufbau auf der Basis umfassender Informationen: Voraussetzung für die Positionierung ist eine umfassende Information über bestehende Risiken. Wissen und Einschätzungen aus unterschiedlichen Quellen sollen hier zusammengeführt werden: von der Regionalexpertise, etwa aus dem sehr großen Lektorennetzwerk des DAAD, über die Einschätzungen zu bestimmten Technologien seitens des GA bis hin zu den Informationen und Einschätzungen der verschiedenen Ressorts, die auch Zugang zu nachrichtendienstlichen Informationen (BfV, BND, Bundesamt für den Militärischen Abschirmdienst (MAD)) haben und deren Wissen kontrolliert einbringen können.

Der Wissenschaftsrat erinnert an die bereits geäußerten Hinweise auf Probleme angesichts einer **Abhängigkeit von kommerziellen Anbietern** und deren Informationsbereitstellung (vgl. C.II). Sofern kein entsprechendes Angebot auf europäischer Ebene entwickelt wird, sollten relevante Informationen auf nationaler Ebene gebündelt bereitgestellt werden. Diese sollten für Wissenschaftseinrichtungen eine möglichst umfassende Datengrundlage zur Einschätzung des Risikopotenzials von Personen oder Einrichtungen zur Nutzung durch die Wissenschaftseinrichtungen zur Verfügung stellen.

3 – Beratung von Einrichtungen und Forschungsorganisationen: Zugleich kann eine solche Plattform die bereits bestehenden Strukturen im Sinne eines One-Stop-Shop beratend unterstützen und damit in das Wissenschaftssystem hineinwirken. Die Beratung kann strategischer Art im Kontext der Erarbeitung von Internationalisierungsstrategien sein oder die Ausgestaltung von Kooperationsverträgen unterstützen.

Nach Einschätzung des Wissenschaftsrats kann eine solche Struktur organisatorisch in unterschiedlicher Weise realisiert werden. Dabei erscheint es sinnvoll, dass die **Plattform in ihrer Arbeitsweise folgende Randbedingungen** erfüllt:

- _ **staatliche Akteure** sind breit eingebunden;
- _ die Plattform ist politisch **mandatiert**;
- _ die Struktur arbeitet **subsidiär**;
- _ sie **antwortet rasch** auf Anfragen, um der Dynamik im wissenschaftlichen Prozess gerecht zu werden;
- _ die **Teilnehmenden treffen sich regelmäßig**, um kontinuierlich auf die sich dynamisch verändernden Rahmenbedingungen reagieren zu können, und
- _ die Plattform wird von einer **schlanken administrativen Einheit** unterstützt.

Der Unterschied und **Mehrwert gegenüber rein wissenschaftsinternen Strukturen** wie dem KIWi und dem GA, die bereits sehr gute Arbeit leisten, liegt in der Beteiligung der staatlichen Akteure. Dadurch erhält die **Plattform Zugang zu spezifischen Informationen und politischen Einschätzungen**. Funktionen und Arbeitsweise bestimmen die Organisation und den Ressourcenbedarf.

Dem Wissenschaftsrat ist bewusst, dass übergreifende Plattformen dieser Art in der Regel erst geschaffen werden, wenn neben dem offensichtlichen Bedarf auch der politische Wille vorhanden ist, da unter anderem gegebenenfalls gesetzliche Rahmenbedingungen angepasst oder entsprechende rechtliche Voraussetzungen geschaffen werden müssen. Vielfach befördert ein Schockereignis maßgeblich den politischen Druck und den Willen zu gemeinsamem Handeln. Der Wissenschaftsrat warnt davor, bis zu einem solchen Schockereignis für Deutschland zu warten und plädiert vielmehr dafür, eine **solche Plattform so rasch wie möglich einzurichten**. Ihre Einrichtung auf nationaler Ebene unter Einbeziehung unterschiedlicher Ressorts ist dringend erforderlich und sollte zeitnah realisiert werden.

Aus Sicht des Wissenschaftsrats werden alle Beteiligten von der Einrichtung einer solchen Plattform profitieren. Denn sie fördert die Vernetzung von Wissenschaftssystem und Politik, sie trägt zu einer Koordination der Aktivitäten einzelner Ressorts bei und hilft den Sicherheitsdiensten bei der Einschätzung von cutting edge-Technologien. Auch die EU hat ihren Mitgliedstaaten empfohlen,

„gegebenenfalls eine neue Unterstützungsstruktur oder einen neuen Unterstützungsdienst zu schaffen oder die bereits bestehenden zu stärken.“ |⁸³

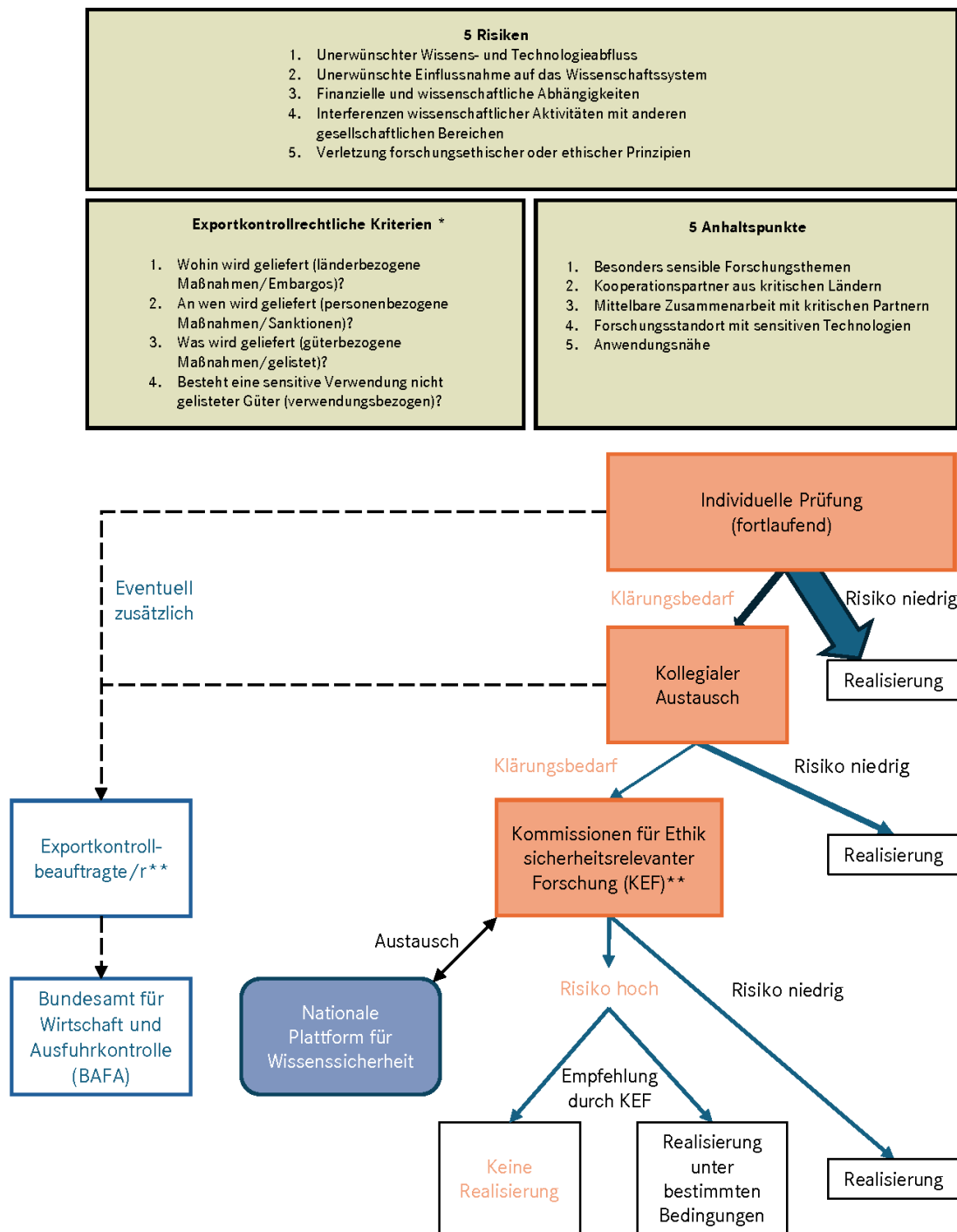
Eine solche Plattform kann zudem als zentraler **Ansprechpartner auf europäischer oder internationaler Ebene** – vergleichbar Einrichtungen wie etwa dem Contact Point for Knowledge Security in den Niederlanden |⁸⁴ oder dem SECURE Center der US-National Science Foundation |⁸⁵ – dienen. Eine europäische und internationale Zusammenarbeit ist erforderlich, um die internationale wissenschaftliche Kooperation – vor allem mit gleichgesinnten bzw. Wertepartnern – möglichst unbürokratisch und barrierefrei aufrechtzuerhalten.

Die folgende Abbildung fasst die Risikobetrachtung idealtypisch – von der primären Ebene des oder der Einzelnen bis zu der noch einzurichtenden nationalen Plattform für Wissenssicherheit – zusammen.

|⁸³ Rat der Europäischen Union (2024): Empfehlung des Rates vom 23. Mai 2024 zur Stärkung der Forschungssicherheit (C/2024/3510); Brüssel, S. 6, <https://eur-lex.europa.eu/eli/C/2024/3510/oj>.

|⁸⁴ Vgl. <https://english.loketkennisveiligheid.nl/>.

|⁸⁵ Safeguarding the Entire Community in the U. S. Research Ecosystem (SECURE), Vgl. <https://new.nsf.gov/research-security>.



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

** In der wissenschaftlichen Einrichtung oder einrichtungsübergreifend

Quelle: Eigene Darstellung. Die Dicke der Pfeile soll die Größenordnung der Fallzahlen illustrieren.

Sicherheitsrelevante Forschung umfasst – aufbauend auf einem umfassenden Sicherheitsbegriff – nicht nur militärische Forschung, sondern den gesamten Bereich von **Forschungsarbeiten, die zur Sicherheit und Resilienz der Gesellschaft beitragen** (vgl. B.II). Sicherheitsrelevant ist damit die wissenschaftliche Auseinandersetzung mit Risiken, Bedrohungen und Schutzmaßnahmen für die innere und äußere Sicherheit. Dies umfasst die Entwicklung neuer Technologien, Methoden, Verfahren und Dienstleistungen zur Prävention, Detektion und Bewältigung von unterschiedlichen Gefahrenarten. Dementsprechend ist sicherheitsrelevante Forschung in verschiedenen Disziplinen und Forschungsfeldern (z. B. von der Friedens- und Konfliktforschung über die Cybersicherheitsforschung bis hin zur zivilen Sicherheitforschung) in unterschiedlichen Ausprägungen und normativen Orientierungen präsent.

Während das Feld der militärischen Forschung – nicht zuletzt aufgrund seiner hohen Sicherheits- und Geheimhaltungsstandards – weitestgehend auf klar definierte Standorte begrenzt ist, findet Forschung zu sicherheitsrelevanten Fragen **verstreut an außeruniversitären Einrichtungen** inkl. Ressortforschungseinrichtungen unterschiedlicher Ressorts **und an Hochschulen** statt. Ein relevantes Feld unter mehreren, nämlich die an verschiedenen Standorten etablierte Friedens- und Konfliktforschung, befasst sich mit Ursachen, Formen, Dynamiken und Folgen von Gewaltkonflikten und kriegerischer Gewalt, mit deren Prävention, Einhegung oder Beilegung sowie mit der dauerhaften Stabilisierung von Frieden. |⁸⁶ Demgegenüber sind die im angelsächsischen Raum verbreiteten Sicherheitsstudien (Security Studies) und die militärisch orientierten strategischen Studien (Strategic Studies) in Deutschland vergleichsweise schwächer vertreten. |⁸⁷ Allerdings lassen sich nicht alle Wissenschaftlerinnen und Wissenschaftler, die sich aus politikwissenschaftlicher oder auch soziologischer Perspektive mit Fragen der inneren Sicherheit, zum Beispiel mit Phänomenen wie Extremismus oder terroristischer Gewalt, oder der äußeren Sicherheit, wie

| ⁸⁶ Der Analyse des Wissenschaftsrats von 2019 folgend handelt es sich um ein interdisziplinär arbeitendes Feld mit offenen Grenzen und zahlreichen Schnittflächen zu anderen Forschungsfeldern und Disziplinen. Es gibt mehrere außeruniversitäre Einrichtungen und ein Mindestmaß an Institutionalisierung in Form von Professuren mit entsprechender Denomination an Hochschulen, einer wissenschaftlichen Fachgesellschaft und eigenen Fachzeitschriften, ohne dass von einer eigenen Disziplin die Rede sein kann. Vgl. Wissenschaftsrat (2019): Empfehlungen zur Weiterentwicklung der Friedens- und Konfliktforschung; Gießen, v. a. S. 8 & 15, <https://www.wissenschaftsrat.de/download/2019/7827-19>.

| ⁸⁷ Vgl. ebd., S. 35.

etwa mit Fragen von Abschreckung und kollektiver Sicherheit, befassen, eindeutig einem dieser Felder zurechnen. Vielfach verorten sie sich im Feld der internationalen Beziehungen. |⁸⁸

Die in Fragen der sicherheitsrelevanten Forschung zu beobachtende **Fragmentierung ist primär historisch begründet**. In Zeiten konfrontativer Sicherheitspolitik und des Auftretens direkter, multidimensionaler Bedrohungen, die von Cyberattacken bis hin zu Naturkatastrophen reichen (vgl. A), sollten Fragen von **Frieden und Sicherheit aus einer systemischen und stärker integrierenden Perspektive heraus bearbeitet werden**. Mit dem Angriffskrieg Russlands auf die Ukraine sowie im Zuge des Machtwechsels der USA steht zudem „ein deutlicher Wandel der deutschen strategischen Kultur wie auch der außenpolitischen Kultur an.“ |⁸⁹ Um diese sicherheitspolitischen Herausforderungen angemessen erfassen sowie den anstehenden strategischen Wandel adäquat vorbereiten und begleiten zu können, sollte sich das wissenschaftliche Feld und das Zusammenspiel von Wissenschaft mit politischen, wirtschaftlichen und gesellschaftlichen Akteuren deutlich erweitern und weiterentwickeln. Eine Kooperation mit Disziplinen und Feldern, die nicht zu den historisch gewachsenen, oben genannten Teildisziplinen gehören, ist problem- und themenbezogen gefordert. Dies ist nicht allein notwendig, um die Themen wissenschaftlich angemessen zu durchdringen, sondern auch um den dringend erforderlichen Wissenstransfer in hoher Qualität leisten zu können.

Vor diesem Hintergrund schlägt der Wissenschaftsrat Instrumente und Maßnahmen vor, um sowohl die **strategische Planung voranzutreiben** (vgl. C.IV.1) als **auch neue Strukturen zu schaffen** (vgl. C.IV.2), die der Integration des Feldes dienen sowie die Geschwindigkeit der strategischen und technologischen Entwicklungen und deren produktive Nutzung erhöhen sollen.

| ⁸⁸ Jüngst wurde dem Bereich der internationalen Beziehungen attestiert, die Implikationen der technologischen Entwicklungen für sicherheitsrelevante Fragen nicht ausreichend zu reflektieren. Die Rede ist von einem „blinden Fleck“, insofern der Einfluss und das Potenzial von Technologien zur radikalen Veränderung von politischer Macht und Geopolitik nicht systematisch berücksichtigt werde, vgl. Baums, A.; Butts, N. (2024): Die Geopolitik der Technologie, in: Internationale Politik, 6, S. 88–93, <https://internationalepolitik.de/de/die-geopolitik-der-technologie>. Vgl. auch Baums, A.; Butts, N. (2025): Tech Cold War. The Geopolitics of Technology; Boulder, <https://doi.org/10.1515/9781962551571>.

| ⁸⁹ Daase, C.; Deitelhoff, N.; Geis, A. (2024): Wer hat uns verraten? Friedens- und Sicherheitsforschung in Kriegszeiten, in: Geis, A.; Deitelhoff, N.; Masala, C. (Hrsg.): Der russische Angriffskrieg gegen die Ukraine und die Internationalen Beziehungen, Sonderheft der Zeitschrift für Internationale Beziehungen (zib), 31 (2), 82–105, hier S. 97, <https://doi.org/10.5771/0946-7165-2024-2-82>.

Derzeit lassen sich unterschiedliche Ansätze in der Forschungsplanung beobachten. Im militärischen Bereich setzt die Forschung in Deutschland aus Effizienzgründen auf der zivilen Forschung auf. Das Bundesministerium der Verteidigung (BMVg) prüft, ob Forschungsergebnisse gegebenenfalls direkt für militärische Anwendungen im Sinne des Dual-Use-Potenzials genutzt oder Technologien bis zum militärischen Einsatz weiterentwickelt werden können (sogenannte Add-On-Forschung). Dabei orientiert sich die Forschungsplanung primär an dem seitens der **Bundeswehr artikulierten Erkenntnis- und Technologiebedarf**.^{| 90} Letzterer wird jährlich erhoben und führt über einen Priorisierungsprozess zu Forschungs- und Entwicklungsmaßnahmen, zu denen neben der eigenen Forschung auch Studienaufträge oder Zuwendungen an Dritte zählen.^{| 91} Um Ideen für die Weiterentwicklung der Bundeswehr zu generieren, nehmen Vertreterinnen und Vertreter aus Bundeswehr und BMVg regelmäßig an wissenschaftlichen Konferenzen oder Tagungen teil. Sie können Anregungen aus dem wissenschaftlichen Diskurs gewinnen und an die relevanten Dienststellen weiterleiten. In Einzelfällen arbeiten einzelne Wissenschaftlerinnen oder Wissenschaftler für eine bestimmte Zeit in Ministerien mit oder umgekehrt werden Personen aus der Verwaltung auf Zeit an (Ressort)Forschungseinrichtungen abgeordnet.

In der Friedens- und Konfliktforschung orientieren sich die öffentlich finanzierten universitären und außeruniversitären Einrichtungen nicht allein an Erkenntnisinteressen der Grundlagenforschung,^{| 92} sondern arbeiten in ausgeprägter

| 90 Die Wehrwissenschaftliche Forschung, zu der im Sinne des Ressortforschungsplans auch die Wehrpharmazie, Wehrveterinärmedizin und Wehrzahnmedizin gehören, „setzt im Rahmen ihrer Forschungsaktivitäten grundsätzlich auf den Erkenntnissen der zivilen Forschung auf, wenn nationale Sicherheitsinteressen und das angestrebte Fähigkeitsprofil der Bundeswehr es erfordern. Sind entsprechende Ergebnisse der zivilen Forschung nicht verfügbar, müssen sie im Rahmen der Ressortforschung erarbeitet werden.“ BMVg (2023): Ressortforschungsplan des Bundesministeriums der Verteidigung für 2023 ff.; Berlin, S. 6 f., <https://www.bmvg.de/resource/blob/5637696/555527115f817d20ad9a2c7f49456765/ressortforschungsplan-bmvg-2023-data.pdf>.

| 91 In den Prozess der Bedarfsermittlung und der Ideengenerierung aus unterschiedlichen Quellen (Hochschulen, außeruniversitäre Einrichtungen, Wirtschaft, internationale Partnerschaften, Streitkräfte etc.) spielen neben dem Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr in Koblenz (BAAINBw, inoffiziell Beschaffungsamt genannt) auch die Fachtechniken eine Rolle. Dabei handelt es sich um teilweise an Ressortforschungseinrichtungen beheimatete Dienststellen, drei wehrwissenschaftliche und fünf wehrtechnische. Sie haben einen fachlichen Fokus, etwa für Waffen und Munition oder auch Informationstechnologie und Elektronik. Forschende können sich zudem mit Ideen und Forschungsvorschlägen direkt an das BMVg, etwa das BAAINBw, wenden.

| 92 Für einige der Einrichtungen spielt die nachfragegetriebene (Auftrags)Forschung für die Forschungsplanung und Schwerpunktsetzung durchaus eine Rolle. Thematische Ausschreibungen der Bundesministerien oder Förderorganisationen beeinflussen, so hat die Analyse des Wissenschaftsrats gezeigt, die Schwerpunktsetzungen der Arbeiten von universitären Einrichtungen, vgl. hierzu: Wissenschaftsrat (2019): Empfehlungen zur Weiterentwicklung der Friedens- und Konfliktforschung; Gießen, S. 70, <https://www.wissenschaftsrat.de/download/2019/7827-19>.

Weise problem-, praxis- und anwendungsorientiert. |⁹³ In der Sicherheitsforschung spielen Beobachtung und Reflexion aktueller (gesellschafts)politischer Entwicklungen im In- und Ausland neben dem genuin grundlagenorientierten Erkenntnisinteresse eine Rolle. Forschungsprogramme entwickeln sich in diesen Bereichen folglich in einem **Wechselspiel von eigenen Erkenntnisinteressen und dem Anspruch, problemorientiert zu arbeiten.**

Allerdings fehlt in Deutschland ein **institutionalisierter systematischer und regelmäßiger Austausch zwischen der wissenschaftlichen Seite und anderen Stakeholdern in sicherheitsrelevanten Fragen.** „Scouting“ auf Tagungen, der persönliche Austausch, die Problemorientierung sowie die an perzipierten Sicherheitsbedarfen orientierte Anlage von Forschungsarbeiten sind hilfreich, aber angesichts der systemischen Herausforderungen und des Geschwindigkeitsbedarfs nicht länger ausreichend.

Vor dem Hintergrund dieser Analyse empfiehlt der Wissenschaftsrat, ein **Strategisches Dialogforum von wissenschaftlichen und sicherheitspolitisch verantwortlichen Akteuren** einzurichten. Zu letzteren zählen politisch Verantwortliche aus dem Bundeskanzleramt und den unterschiedlichen Ressorts, wie dem Auswärtigen Amt (AA), dem BMVg und der Bundeswehr, dem Bundesministerium für Forschung, Technologie und Raumfahrt (BMFTR), dem Bundesministerium für Wirtschaft und Energie (BMWE), dem Bundesministerium des Innern (BMI), dem Bundesministerium für Umwelt, Klimaschutz, Naturschutz und nukleare Sicherheit (BMUKN) oder dem Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung (BMZ). Ebenfalls beteiligt sein sollten Unternehmen, gegebenenfalls auch Rüstungsunternehmen, und Akteure wie Feuerwehr, Polizei, das Technische Hilfswerk (THW) und andere Hilfs- und Rettungsorganisationen. Das Dialogforum sollte eng mit der Nationalen Plattform (vgl. C.III.3) zusammenarbeiten.

Ein Strategisches Dialogforum unter Beteiligung der genannten Akteure könnte dazu beitragen, dem formulierten Anspruch einer integrierten Sicherheit gerecht zu werden. Als Teil eines deutschen Strategiezyklus könnten Risikoanalysen und sicherheitspolitische Szenarien entworfen werden. Auf Basis **multidisziplinär gewonnener Risikoanalysen** könnten dort mittel- und langfristige Perspektiven für den Umgang mit einer sich kontinuierlich verändernden Bedrohungslage entwickelt sowie darauf aufbauend Forschungsbedarfe artikuliert

| ⁹³ Politische Relevanz und der Wunsch, zur Lösung praktischer Fragen der Konfliktbearbeitung und -transformation beizutragen, prägen die Auswahl der Themen, vgl. ebd., S. 35. Die Friedens- und Konfliktforschung ist „im Wissenstransfer engagiert und steht vor allem mit der Politik, aber auch mit zivilgesellschaftlichen Organisationen in engem Austausch.“ Ebd. S. 28.

werden. Großbritannien etwa ist diesen Weg einer integrierten Risikoanalyse bereits gegangen und hat 2023 einen aktualisierten Bericht vorgelegt. |⁹⁴

Auf der Grundlage einer solchen Risikoanalyse kann der **sicherheitsrelevante Forschungsbedarf systematischer als derzeit identifiziert und abgeleitet** werden. Der Wissenschaftsrat ist davon überzeugt, dass ein allein entlang der Ressortlogiken oder der Bedürfnisse von Unternehmen oder anderen Akteuren ermittelter Forschungsbedarf der komplexen Sicherheitslage nicht länger gerecht wird. Das empfohlene Strategische Dialogforum kann im vertrauensvollen Austausch der verschiedenen Beteiligten und unter Einsatz von neuen Techniken mögliche Zukunftsszenarien entwickeln und darauf aufbauend Forschungsbedarf formulieren. Ausschreibungen der einschlägigen Ministerien zur Forschungsförderung könnten sich auf diese gemeinsame Bedarfsermittlung beziehen. Auch Akteure im Wissenschaftssystem können sich daran orientieren. Der Wissenschaftsrat empfiehlt, die bisherige Verwendung von Forschungsmitteln kritisch zu analysieren und in Zukunft stärker abzustimmen, um die inhaltliche Förderausrichtung und gegebenenfalls den effizienten Einsatz der Mittel anzupassen.

Die **Zusammensetzung eines solchen Dialogforums** gilt es im Laufe der Zeit immer wieder zu überdenken und der jeweils neuen Situation anzupassen. Allerdings bedarf es auch einer gewissen Stabilität, um in einem solchen sensiblen Feld ausreichend Vertrauen aufzubauen. Im Falle der Einrichtung eines Nationalen Sicherheitsrats sollte das Dialogforum dort angegliedert sein. In einem ersten Schritt könnte die Nationale Plattform die Einrichtung des Dialogforums unterstützen. Dem Wissenschaftsrat ist bewusst, dass ein Austausch im Rahmen des Dialogforums mit Blick auf die Fragen der äußeren Verteidigung oder des Aufbaus einer resilienten kritischen Infrastruktur allein in einem geschützten Raum stattfinden kann, um keine Fähigkeitslücken auf deutscher Seite offenzulegen oder neue Vulnerabilitäten zu schaffen.

Andere europäische Länder haben bereits entsprechende Instrumente entwickelt, um im Sinne eines **Strategiezyklus** ihre Risikoanalysen regelmäßig zu aktualisieren und im Rahmen der eigenen Nationalen Sicherheitsstrategie zeitnah darauf reagieren zu können. Die Niederlande haben schon mehrere solcher Zyklen durchlaufen und eine anspruchsvolle Methodik entwickelt, die als Vorbild für andere Länder gilt. |⁹⁵ Auch im Vereinigten Königreich etwa koordiniert der National Security Council (NSC) ein solches Vorgehen, das die Bereiche Verteidi-

| ⁹⁴ Vgl. <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>.

| ⁹⁵ Vgl. <https://fourninesecurity.de/2023/03/09/ein-anfang-nicht-das-ende-die-nationale-sicherheitsstrategie-als-auftakt-eines-regelmaessigen-strategiezyklus>.

gung, Sicherheit, Resilienz, Diplomatie, Entwicklung und Handel sowie Wirtschafts-, Wissenschafts- und Technologiepolitik adressiert. Die Umsetzung der Ziele wird kontinuierlich beobachtet und evaluiert. |⁹⁶

Der Wissenschaftsrat empfiehlt, in Zukunft die auf deutscher und europäischer Ebene **bereitgestellten Mittel für sicherheitsrelevante Forschung gezielt und strategisch einzusetzen** – möglichst auf Grundlage der Beratungen in einem Strategischen Dialogforum. Sofern die Etablierung eines solchen Dialogforums längerer Vorbereitungen bedarf, empfiehlt der Wissenschaftsrat, übergangsweise eine ressortübergreifende Ad-hoc-Gruppe einzurichten, um erste Förderentscheidungen beratend vorzubereiten. Ein solcher strategischer Dialog sollte nicht allein zu einer systematischen Identifikation des Forschungsbedarfs führen, sondern zudem verbindlicher als bisher die Rolle des Staates als Nachfrager für sicherheitsrelevante Innovationen in den Blick nehmen, so dass Förder- und Forschungsaktivitäten stärker an die Nachfrage gekoppelt werden können (vgl. auch C.IV.2). |⁹⁷

IV.2 Sicherheitsrelevante Forschung integrativ und systemisch anlegen

Die Forschung in sicherheitsrelevanten Feldern folgt häufig historisch gewachsenen Teilbereichen der Forschung und ist auch auf unterschiedliche Akteure verteilt. So fördert das **BMVg** vor allem **militärische Forschung und Entwicklung** im Jahr 2024 mit rund 3,6 Mrd. Euro (vgl. Tabelle 1 in Anhang 2). |⁹⁸ Hier gilt es zu berücksichtigen, dass ein großer Teil aus dem Sondervermögen in Höhe von rund 2 Mrd. Euro für die Entwicklung und Erprobung von Kampfflugzeugen und Kampfpanzern eingesetzt wurde. |⁹⁹ Ein geringer Anteil von rund

| ⁹⁶ Das 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.“ Darauf aufbauend erfolgte 2023 eine Aktualisierung (Refresh, IR2023), die eine „greater integration of IR2023 into the Government Planning and Performance Framework (GPPF)“ betont. „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>. Vgl. auch 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>.

| ⁹⁷ Im Europäischen Verteidigungsfonds werden Fördermaßnahmen sowohl mit als auch ohne Beschaffungsabsicht vergeben, vgl. https://germany.representation.ec.europa.eu/news/europaischer-verteidigungsfonds-12-milliarden-euro-fur-innovationen-und-bessere-2023-03-30_de.

| ⁹⁸ Dabei handelt es sich um Soll-Ausgaben des Bundes in Forschung und Entwicklung in das Ressort des BMVg, vgl. <https://www.datenportal.bmbf.de/portal/de/grafik-1.1.4.html>.

| ⁹⁹ Neben den rd. 668 Mio. Euro, die aus dem Sondervermögen in die wehrtechnische Entwicklung und Erprobung geflossen sind, wurden weitere Investitionen in die Entwicklung des Kampfflugzeugs MRCA (Multi-Role Combat Aircraft, Soll 2024 rd. 114 Mio. Euro), des Waffensystems Eurofighter (Soll 2024 rd. 897 Mio. Euro), des Main Ground Combat System (MGCS) (Soll 2024 rd. 84 Mio. Euro) und der Next Generation Weapon

50 Mio. Euro des Sondervermögens flossen in die wehrtechnische Auftragsforschung |¹⁰⁰ und weitere rund 668 Mio. Euro in die wehrtechnische Entwicklung und Erprobung – über die eigens genannten Projekte hinaus. |¹⁰¹ Weitere 565 Mio. Euro wurden für die wehrtechnische Forschung und Technologie im Sinne von Auftragsforschung aus dem Haushalt aufgewendet und rund 216 Mio. Euro für die wehrtechnische Entwicklung und Erprobung, die mit einer Beschaffungsabsicht und Prototypentwicklung verbunden ist. |¹⁰² Zu diesen Ausgaben zählen nicht allein die Förderung von Forschungsprojekten an Hochschulen, Forschungseinrichtungen und Unternehmen; darüber hinaus ist darin auch die Grundfinanzierung von Forschungseinrichtungen i. H. v. rund 178 Mio. Euro enthalten, zu denen mehrere Institute des Deutschen Zentrums für Luft- und Raumfahrt e. V. (DLR), |¹⁰³ der Fraunhofer-Gesellschaft (FhG) |¹⁰⁴ und das Deutsch-Französische Forschungsinstitut Saint- Louis (ISL) |¹⁰⁵ zählen.

Für **nichtmilitärische sicherheitsrelevante Forschung liegen keine vergleichbar belastbaren Zahlen** vor. Denn dieses Feld ist – wie geschildert – nicht klar eingrenzbar. |¹⁰⁶ Es gibt spezifische Programme, mit denen Aktivitäten in dieser Richtung gefördert werden. Zu nennen ist etwa das Rahmenprogramm „Forschung für die zivile Sicherheit“, welches das damalige Bundesministerium für Bildung und Forschung (BMBF) 2007 erstmalig aufgelegt hat; 2024 ist es in der vierten Programmphase unter dem Titel „Forschung für die zivile Sicherheit – gemeinsam für ein sicheres Leben in einer resilienten Gesellschaft“ fortgeführt worden. Seit dem Start des Programms konnten „mehr als 520 Forschungsprojekte mit über 2.200 Teilvorhaben gefördert“ (Stand 2024) werden, was einem Fördervolumen von insgesamt rund 915 Mio. Euro entspricht. Zusätzliche Mittel in der Höhe von 165 Mio. Euro kamen als Eigenmittel aus der Industrie. |¹⁰⁷ Hintergrund ist, dass in rund der Hälfte der Vorhaben Praxispartner wie Feuerwehr,

Systems (NGWS) in einem Future Combat Air System (FCAS) (Soll 2024 516 Mio. Euro) finanziert. Vgl. Bundesministerium der Finanzen (BMF) (2024): Bundeshaushaltsplan 2024, Einzelplan 14. Bundesministerium der Verteidigung; Berlin, S. 74, S. 77 und S. 80, <https://www.bundeshaushalt.de/static/daten/2024/soll/epl14.pdf>.

|¹⁰⁰ Vgl. ebd., S. 73.

|¹⁰¹ Vgl. ebd., S. 74.

|¹⁰² Vgl. ebd., S. 44 & 47.

|¹⁰³ Vgl. DLR Programmkoordination Sicherheits- und Verteidigungsforschung, <https://www.dlr.de/de/forschung-und-transfer/sicherheit/zivile-sicherheitsforschung-und-dual-use>.

|¹⁰⁴ Vgl. Fraunhofer-Leistungsbereich Verteidigung, Vorbeugung und Sicherheit (VVS), <https://www.vvs.fraunhofer.de/de/mitglieder.html>.

|¹⁰⁵ Vgl. Wissenschaftliche Dienste des Deutschen Bundestages (2024): Wehrtechnische Forschung in ausgewählten Ländern. Finanzen, Verantwortlichkeiten, Verfahren; Berlin, S. 5, <https://www.bundestag.de/resource/blob/1032720/4ec2c18ad1aa3ee397241bf58e418947/WD-2-050-24-pdf.pdf>.

|¹⁰⁶ Vgl. hierzu auch die Untersuchung des Wissenschaftsrats zur Friedens- und Konfliktforschung in Deutschland, die auch Teile der Sicherheitsforschung mit umfasst. Personalausstattung und Drittmiteleinwerbungen beziehen sich auf die Jahre 2017 und 2018, vgl. hierzu: Wissenschaftsrat (2019): Empfehlungen zur Weiterentwicklung der Friedens- und Konfliktforschung; Gießen, v. a. Anhang 2, S. 117, <https://www.wissenschaftsrat.de/download/2019/7827-19>.

|¹⁰⁷ <https://www.sifo.de/sifo/de/programm/zahlen-und-fakten/zahlen-und-fakten-zum-sicherheitsforschungsprogramm.html?nn=248276>.

Polizei, THW und andere Hilfs- und Rettungsorganisationen eingebunden sind. Im Rahmen seines Programms „Maritime Sicherheit“ förderte das damalige Bundesministerium für Wirtschaft und Klimaschutz (BMWK) sicherheitsrelevante Forschung, so zum Beispiel mit dem Programm „Echtzeittechnologien für die Maritime Sicherheit“, das sich an Unternehmen richtet. | ¹⁰⁸ Auch die Deutsche Stiftung Friedensforschung unterstützt Projekte in sicherheits- und verteidigungspolitischen Feldern. | ¹⁰⁹ Vor einigen Jahren ist zudem die Agentur für Innovation in der Cybersicherheit GmbH, kurz Cyberagentur, gegründet worden. Ihr Auftrag ist es, bahnbrechende Innovationen auf dem Gebiet der Cybersicherheit – vor allem für die Bedarfe der inneren und äußeren Sicherheit – zu fördern. | ¹¹⁰

Der Wissenschaftsrat hat bereits in seinen zurückliegenden Evaluationen feststellen müssen, dass die **Forschungsmittel, die in die Ressortforschungseinrichtungen des BMVg geflossen sind, vielfach weder zielführend noch effizient** eingesetzt worden sind. Defizite lassen sich in unterschiedlichen Hinsichten beobachten: (1) hinsichtlich unklarer und sehr langwieriger Beschaffungsprozesse, | ¹¹¹ (2) hinsichtlich der Rekrutierung und des Einsatzes von wissenschaftlichem Personal, | ¹¹² (3) hinsichtlich der notwendigen Infrastruktur – bis hin zum WLAN-Zugang | ¹¹³ – sowie (4) hinsichtlich der effizienten Nutzung von Forschungsinfrastrukturen wie zum Beispiel Forschungsschiffen. | ¹¹⁴ Ein

| ¹⁰⁸ Vgl. <https://www.bmwk.de/Redaktion/DE/Textsammlungen/Technologie/Schlüsseltechnologien/forschung-entwicklung-innovation-in-der-maritimen-wirtschaft.html>.

| ¹⁰⁹ Vgl. <https://bundesstiftung-friedensforschung.de/>.

| ¹¹⁰ Vgl. <https://www.cyberagentur.de/agentur/>.

| ¹¹¹ Als Beispiel sei auf das Institut für Präventivmedizin der Bundeswehr verwiesen, das „nur die aus den Vorgängereinrichtungen vorhandene Geräteausstattung nutzen und für die neuen Aufgaben keine Beschaffung, Instandhaltung und Regeneration von Geräten durchführen [kann]. Aus diesem Grund konnten zwei bei der Gründung geplante Labore [...] bislang nicht eingerichtet sowie Messgeräte bzw. -systeme und IT-Ausstattung nicht erworben werden. Bislang ist es nicht gelungen zu klären, welche vorgesetzte Stelle dieses Defizit beheben kann. Für dieses Problem muss unbedingt auf höherer Ebene eine Lösung gefunden werden. Die Beschaffungsprozesse sind umständlich und langwierig.“ Wissenschaftsrat (2022): Stellungnahme zum Institut für Präventivmedizin der Bundeswehr (InstPrävMedBw), Andernach; Köln, S. 63, <https://doi.org/10.57674/14pe-fn68>.

| ¹¹² So hat der Wissenschaftsrat festgestellt, dass das „Bundesamt für das Personalmanagement der Bundeswehr [...] dem Institut gelegentlich für die experimentelle Laborarbeit ungeeignetes technisches Personal zugewiesen“ hat, so dass empfohlen wurde, dem Institut mehr Mitsprache- und Auswahlrechte einzuräumen, vgl. Wissenschaftsrat (2020): Stellungnahme zum Institut für Pharmakologie und Toxikologie der Bundeswehr (InstPharmToxBw), München; Köln, S. 12, <https://www.wissenschaftsrat.de/download/2020/8521-20>.

| ¹¹³ So fehlt etwa im Institut für Pharmakologie und Toxikologie der Bundeswehr ein leistungsstarker und zeitgemäßer Internetzugang, vgl. ebd., S. 13 & 64.

| ¹¹⁴ Aufgrund fehlenden Personals sind Forschungsschiffe nicht ausgelastet, wie der Wissenschaftsrat in seiner Stellungnahme zur Wehrtechnischen Dienststelle für Schiffe und Marinewaffen, Maritime Technologie und Forschung (WTD 71), Eckernförde, noch 2022 feststellte, vgl. Wissenschaftsrat (2022): Stellungnahme zur Wehrtechnischen Dienststelle für Schiffe und Marinewaffen, Maritime Technologie und Forschung (WTD 71), Eckernförde; Köln, S. 13 & 64, <https://doi.org/10.57674/y345-ca97>.

Grund dafür liegt in der Organisation des Beschaffungsprozesses. | ¹¹⁵ Angesichts dieser vielfältigen Defizite fehlen nach Einschätzung des Wissenschaftsrats in vielen Fällen die strukturellen Voraussetzungen für wissenschaftliches Arbeiten auf hohem Niveau und mit hoher Geschwindigkeit. | ¹¹⁶ Die bisherigen Akteure im Feld, so der Eindruck, können die geforderten Forschungsarbeiten nicht so rasch leisten, wie es jetzt geboten ist.

Daher empfiehlt der Wissenschaftsrat nachdrücklich, die leistungsstarken und profilierten Akteure zu stärken und zu vernetzen sowie den Kreis der Akteure für Arbeiten in der sicherheitsrelevanten Forschung zu erweitern. Mit der Erweiterung des Akteurskreises können auch die **vorhandenen Potenziale und Synergien in der vielgestaltigen deutschen Wissenschaftslandschaft, namentlich den Hochschulen, besser gehoben** werden. Dies ist mit einem Kulturwandel verbunden, der auch die gesamte Gesellschaft betrifft (vgl. D). Die zur Verfügung stehenden Mittel sollten klug eingesetzt werden, indem (1) die ganze Breite und Vielfalt der sicherheitsrelevanten Forschung ins Auge gefasst und darüber hinaus in der Förderung adressiert werden, (2) ein Fokus auf Anstrengungen zur Integration des Feldes gelegt wird und (3) die Innovationskraft in einem weiten, nicht allein technologischen Sinne substanziell gesteigert wird.

Der Wissenschaftsrat sieht es als eine Aufgabe des **Strategischen Dialogforums** an, die strategische Forschungsplanung auf Basis der multidisziplinär gewonnenen Risikoanalysen mit den drei genannten Zielen zu verschränken. In dieser Weise können die drängenden **sicherheitsrelevanten Probleme** in einem umfassenden und integrierten Sinne bearbeitet und die Mittel effizient und effektiv eingesetzt werden. Der Wissenschaftsrat konzentriert sich im Folgenden auf strategische und strukturelle Neuerungen, die auf eine Integration des Feldes zielen und in der Folge auch zu Innovationen im weiten Sinne, nicht allein im technologischen Sinne, führen.

1 – Integration des wissenschaftlichen Feldes fördern: Der Wissenschaftsrat stellt mit **Sorge fest, dass sich die unterschiedlichen Bereiche der sicherheitsrelevanten Forschung in Deutschland in getrennten Räumen bewegen**. Grenzbeziehungen sind im Wesentlichen historisch und nicht oder nur in geringen Teilen aus dem Gegenstand heraus begründet. Schon jetzt lässt sich beobachten, dass im Zuge der wissenschaftlichen Entwicklung und Professionalisierung der

| ¹¹⁵ So stellte der Wissenschaftsrat mit Blick auf das Zentrum für Geoinformationswesen fest, dass der „Prozess für die Beantragung von Mitteln für Geräte und Material beim Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) [...] so langwierig und aufwändig [ist], dass es vorkommen kann, dass [eine Einrichtung] [...] erforderliche Geräte nicht mehr während der Laufzeit des Projektes erhält, für das sie benötigt werden. Auch Vertragsabschlüsse mit extramuralen Auftragnehmern [...] unterliegen häufig langen Verzögerungen.“ Wissenschaftsrat (2019): Stellungnahme zum Zentrum für Geoinformationswesen der Bundeswehr (ZGeoBw), Euskirchen; Köln, S. 12, <https://www.wissenschaftsrat.de/download/2019/7489-19>. Vergleichbare Beobachtungen wurden auch im Zuge der Evaluation anderer Ressortforschungseinrichtungen des BMVg gemacht.

| ¹¹⁶ Vgl. exemplarisch die zusammenfassende Einschätzung zum Zentrum für Geoinformationswesen der Bundeswehr: Ebd., S. 13.

Friedens- und Konfliktforschung zunehmend eine Öffnung gegenüber der sicherheitspolitischen Forschung stattgefunden hat, so dass sich diese beiden Perspektiven deutlich wieder annähern. |¹¹⁷

Diese Integration des Feldes sollte sowohl selbstorganisiert vorangetrieben als auch strategisch durch Fördermaßnahmen unterstützt werden. Der Wissenschaftsrat hält es für unerlässlich, die im breiten Feld vorhandenen Wissens- und Datenbestände, die aus unterschiedlichen Quellen und in unterschiedlichen Forschungskontexten gewonnen wurden, zugänglich zu machen und stärker miteinander zu verschränken. Dies kann im Rahmen etablierter Formate wie zum Beispiel über Ausschreibungen befördert werden. In anderen Feldern, etwa in der Biodiversitäts- und Klimaforschung sind bereits Strukturen entwickelt worden, die dazu beitragen, die **Wissens- und Datenbestände systematisch zu integrieren**. Dazu wurden eigens Strukturen geschaffen: In sogenannten **Synthesezentren** führen Wissenschaftlerinnen und Wissenschaftler – mit Unterstützung von informationstechnischer Expertise – ihre disparaten Wissens- und Datenbestände zusammen, um komplexe Themen wie Klima oder eben auch Sicherheit aus einer systemischen Perspektive heraus angemessen zu analysieren. Besonders ertragreich ist eine solche Zusammenarbeit in Präsenz. Allerdings sind auch andere, virtuelle Formate denkbar.

In Synthesezentren führen Expertinnen und Experten aus unterschiedlichen Disziplinen ihre Daten und Ergebnisse im Sinne einer weiterentwickelten Metaanalyse zusammen. Dazu arbeiten sie für eine begrenzte Zeit, zum Beispiel jeweils mehrere Male im Jahr für eine Woche, an einem Ort zusammen. Datenexpertinnen und -experten unterstützen die Forschenden, um die disparaten Daten- und Wissensbestände aus den verschiedenen Forschungsfeldern und Disziplinen zusammenführen zu können. Die bestehenden 14 **Synthesezentren** aus Australien, China, Europa, Nord- und Südamerika haben sich 2013 zu einem informellen Netzwerk, dem **International**

| ¹¹⁷ Heute handelt es sich eher um unterschiedliche Schwerpunktsetzungen und in weiten Teilen komplementäre Zugänge. Während die Sicherheitsforschung häufig „ein stärkerer Zugriff auf militärische Formen der Sicherheit“ auszeichnet, legt die Friedensforschung einen Schwerpunkt auf „zivile Krisenbearbeitung und fundamentalere Ordnungsfragen.“ Daase, C.; Deitelhoff, N.; Geis, A. (2024): Wer hat uns verraten? Friedens- und Sicherheitsforschung in Kriegszeiten, in: Geis, A.; Deitelhoff, N.; Masala, C. (Hrsg.): Der russische Angriffskrieg gegen die Ukraine und die Internationalen Beziehungen, Sonderheft der Zeitschrift für Internationale Beziehungen (zib), 31 (2), 82–105, hier S. 86, <https://doi.org/10.5771/0946-7165-2024-2-82>. „Die scharfe Entgegensetzung von positivem und negativem Frieden und das Bekenntnis zu einem weiten Begriff der strukturellen Gewalt hatte für die kritische Friedensforschung die gleiche identitätsstiftende Bedeutung wie das Festhalten an einem engen Begriff der Sicherheit und der Vorstellung struktureller Anarchie für die Sicherheitsforschung. Das hatte zur Folge, dass in der Sicherheitsforschung lange das Kooperationsparadigma vernachlässigt und in der Friedensforschung die Beschäftigung mit Krieg, Militär und Rüstungskontrolle mit Argwohn betrachtet wurde.“ Ebd., hier S. 90.

Synthesis Consortium (ISC) | ¹¹⁸ zusammengeschlossen, sechs der Synthesezentren bestehen in den USA, eines in Deutschland, ein weiteres ist in Deutschland geplant. | ¹¹⁹

2 – Innovation Hubs einrichten: Zahlreiche Hochschulen und Forschungsinstitute tragen schon jetzt wesentlich zum Erkenntnisgewinn in sicherheitsrelevanten Forschungsfragen bei – selbst in militärisch relevanten Bereichen. Allerdings stellen Forschungsaktivitäten, die gegebenenfalls auch auf einen militärischen Einsatz zielen, Hochschulen und Forschungseinrichtungen insofern vor **Herausforderungen, als strenge Sicherheitsstandards einzuhalten oder zu schaffen** sind. Dazu zählen Vorkehrungen in den Gebäuden (z. B. Kontrolle des Zugangs), in den Rechnerinfrastrukturen (z. B. physisch getrennte Netzwerke, Datensicherheit, Maßnahmen zur Erkennung von Datenmanipulation) und im Mitarbeiterstab (z. B. Sicherheitsüberprüfung des Personals). Eine intensivere Kooperation mit auf diesen Gebieten erfahrenen Einrichtungen, etwa der FhG oder dem DLR, kann dazu beitragen, den sicherheitstechnischen Herausforderungen zu begegnen.

Um jedoch der Geschwindigkeit der technologischen und weltpolitischen Entwicklungen, der Diversität der Bedrohungslage sowie den strategischen Erfordernissen gerecht zu werden, empfiehlt der Wissenschaftsrat die **Einrichtung mehrerer Innovation Hubs** in Deutschland. Sie sollen sich durch eine flexible und dynamische Arbeitsweise auszeichnen. Solche Hubs müssen unternehmerisch gemanagt und sollten langfristig, jedoch nicht institutionell, gefördert werden. Unterschiedliche Perspektiven und Expertisen sollen hier in einer eigenen Organisationseinheit zusammengeführt werden. Forschende unterschiedlicher Provenienz, auch auf Ebene von Promovierenden, aber auch Praxispartnerinnen und -partner bringen ihr Wissen ein und forschen gemeinsam an einem Thema.

Ziel ist es, mit den Hubs einen **kreativen Raum zu schaffen, der von der Forschung bis hin zur Innovation und Anwendung** reichen muss und in dem zügig Ergebnisse erzielt werden. Strategische Überlegungen gehen Hand in Hand mit technologischen Entwicklungen. Die Hubs können auch eine **Inkubatorfunktion** übernehmen. Die dafür erforderlichen Unterstützungsleistungen sollten bereitgestellt werden. Dazu zählen der Zugang zur notwendigen Technik, zu

| ¹¹⁸ Vgl. hierzu das Netzwerk bestehender Synthesezentren mit ihren unterschiedlichen Modellen: <https://synthesis-consortium.org/>.

| ¹¹⁹ Seit langem existiert ein Synthesezentrum im Bereich der Biodiversität, <https://www.idiv.de/de/forschung/sdiv-synthesis-centre/>. Weitere, sogenannte Synthesis and Solutions Labs der Senckenberg Gesellschaft für Naturforschung (SGN), sind in Gründung befindlich. Sie sollen zum „erste[n] Ort eines transdisziplinären Synthesezentrums in Deutschland“ werden, Wissenschaftsrat (2022): Stellungnahme zum Antrag auf strategische Erweiterung der Senckenberg Gesellschaft für Naturforschung (SGN), Frankfurt am Main, großer strategischer Sondertatbestand im Rahmen der Ausführungsvereinbarung WGL; Köln, S. 56, <https://doi.org/10.57674/530t-ps77>.

(Forschungs)Infrastrukturen und geschützter Kommunikationstechnologie. Neben der technischen Ausstattung spielt auch die fachliche Unterstützung bei der Konzeptentwicklung und Ausarbeitung von Business-Plänen eine Rolle. Dadurch werden positive Spillover-Effekte befördert – sei es in den zivilen Sektor, sei es in den militärischen hinein. | ¹²⁰

Der Wissenschaftsrat sieht in der Einrichtung von **Innovation Hubs große Potenziale** mit Blick auf strategische Fragen der äußeren Sicherheit und hinsichtlich des Aufbaus von Resilienz im Innern. An unterschiedlichen Orten sollten solche, nicht allein auf technologische Entwicklungen ausgerichtete Hubs gefördert werden, gegebenenfalls mit unterschiedlichen inhaltlichen Schwerpunkten. | ¹²¹ Innovation Hubs tragen dazu bei, strategisches Wissen zu neu entstehenden sicherheitsrelevanten Technologien (zum Beispiel Quantentechnologie) für Politik und Gesellschaft zu entwickeln und bereitzustellen. Außerdem helfen sie, die vielfach in Deutschland und Europa zu beobachtende kritische Phase im Innovationsprozess von der Entwicklung zur Marktinnovation, das „**Tal des Todes**“ | ¹²², **strukturell zu überbrücken**. Wissenschaftlerinnen und Wissenschaftler können dadurch gegebenenfalls geeignete Partner für die Weiterentwicklung oder Validierung ihrer Ergebnisse finden. Wünschenswert und für die Umsetzung von besonderer Bedeutung sind die oben genannten Praxispartner. Denn über die unmittelbare Interaktion in einem solchen Hub kann die gemeinsame Orientierung im Sinne einer Abstimmung von Innovationsangebot und -nachfrage deutlich verbessert werden. Allerdings bedarf es darüber hinaus auch weiterer Instrumente der innovativen Beschaffung. Dazu zählen Innovationspartnerschaften ebenso wie eine vorwettbewerbliche Beschaffung. Der Begriff „Staat als Ankerkunde“ | ¹²³ bezieht sich auf eine Strategie, bei der der Staat eine aktive Rolle in der Förderung und Entwicklung bestimmter Wirtschaftssektoren oder Technologien einnimmt. Dies geschieht, indem er als wichtiger Auftraggeber oder Kunde für Unternehmen in diesen Bereichen auftritt. Auf diese Weise fördert die öffentliche Hand Unternehmen, insbesondere Start-ups, mit dem Ziel, Innovationen zu beschleunigen und die Wettbewerbsfähigkeit in strategisch wichtigen Bereichen zu stärken. Dies kann vor allem in Schlüsseltechnologien wie etwa der Raumfahrt erfolgen. Als eigene Organisati-

| ¹²⁰ Ilzetki, E. (2025): Guns and Growth: The Economic Consequences of Defense Buildups, in: Kiel Report No. 2, Kiel Institute for the World Economy, S. 38, <https://www.ifw-kiel.de/publications/guns-and-growth-the-economic-consequences-of-defense-buildups-33747/>.

| ¹²¹ Boris Pistorius hat den Aufbau eines Innovationszentrums in Erding angekündigt: <https://www.bmvg.de/de/aktuelles/pistorius-innovation-night-muenchner-sicherheitskonferenz-5889354>.

| ¹²² Vgl. European Investment Bank (EIB) (Hrsg.); Europäische Kommission (2024): fi-compass ERDF [European Regional Development Fund]. ERDF Equity financial instruments. Factsheet; Luxemburg, S. 22, <https://www.fi-compass.eu/library/how-to/erdf-equity-financial-instruments>.

| ¹²³ Vgl. Weber, T.; Süssenguth, F. (2024): Innovationsfähigkeit in der Zeitenwende (acatech IMPULS), hrsg. v. acatech – Deutsche Akademie der Technikwissenschaften; München, S. 64, https://doi.org/10.48669/aca_2024-14.

onseinheit können die Innovation Hubs so gestaltet sein, dass sie den erforderlichen Standards in der Wissenssicherheit und den Geheimhaltungsanforderungen für militärisch relevante Vorhaben gerecht werden.

In den Hubs sollten **Vertreterinnen und Vertreter der sicherheitsrelevanten Forschung aus unterschiedlichen Einrichtungen auf Zeit unter einer systemischen Perspektive zusammenarbeiten** – zum Beispiel auf Zeit abgeordnet von einer Hochschule oder Forschungseinrichtung. Lediglich die Struktur und eine Grundausrüstung an Betriebspersonal würden bereitgestellt. Der Wissenschaftsrat empfiehlt nachdrücklich, auch die politik-, rechts-, sozial- und kulturwissenschaftlichen Teile der Sicherheitsforschung mit einzubeziehen. Eine ausschließliche Konzentration auf technologische Forschungs- und Entwicklungsarbeiten greift zu kurz.

In dieser Weise können Forschende aus ganz unterschiedlichen Kontexten in ein hoch dynamisches Geschehen eintreten. Die enge und fokussierte Kooperation sollte die **Innovationsgeschwindigkeit erhöhen**. | ¹²⁴ Sicherheitsstandards, die heute selbstverständlich an einzelnen Instituten der FhG oder des DLR herrschen, können in Hubs ebenfalls sichergestellt werden. Die Förderung sollte koordiniert über die unterschiedlichen Ressorts erfolgen. In den Hubs können dadurch in besonderer Weise systemische Fragen adressiert werden. Diese reichen von der Entwicklung neuer Technologien für eine moderne (hybride) Kriegsführung über die Erarbeitung von Resilienzkonzepten auf regionaler oder nationaler Ebene bis hin zu innovativen strategischen Antworten auf die Vielzahl von bewaffneten und kalten Konflikten.

Der Wissenschaftsrat hält es für essenziell, Forschung und Entwicklung auch im **europäischen Kontext** zu sehen. Derzeit entwickelt sich Förderung und Organisation sicherheitsrelevanter Forschung auf europäischer Ebene mit hoher Geschwindigkeit. | ¹²⁵ Es ist noch nicht genau absehbar, welche Auswirkungen diese Veränderungen haben werden. Während bisher das Förderprogramm Horizon Europe ausschließlich auf zivile Projekte zielte, sollte sich der Europäische Verteidigungsfonds (EDF) der Verteidigungsforschung und ihren Anwendungen widmen. Diese klaren Grenzziehungen sind in Zukunft nicht länger zu erwarten. Allerdings war es immer schon möglich, sicherheitsrelevante Forschung in dem hier zugrunde gelegten breiten Sinne im Rahmen von Horizon Europe zu

| ¹²⁴ Die fehlende Innovationsgeschwindigkeit wurde zuletzt noch einmal deutlich kritisiert: Trotz des angekündigten transformativen Richtungswechsels sei dieser viel zu langsam umgesetzt worden. „Diese Langsamkeit resultiert gleichermaßen aus Priorisierungs- und Koordinierungsdefiziten sowie Umsetzungsdefiziten.“ EFI (2025): Gutachten zu Forschung, Innovation und Technologischer Leistungsfähigkeit Deutschlands; Berlin, S. 24, https://www.e-fi.de/fileadmin/Assets/Gutachten/2025/EFI_Gutachten_2025_30125.pdf.

| ¹²⁵ Für die militärische Forschung und Entwicklung ist auf europäischer Ebene ein „Hub for Defence Innovation (HEDI)“ gegründet worden, „to foster innovative solutions for military capabilities“, <https://dirs.be/e-das-hub-for-defence-innovation-hedi/>.

fördern, so etwa für den Cluster „Zivile Sicherheit für die Gesellschaft“. | ¹²⁶ Der Wissenschaftsrat empfiehlt den wissenschaftspolitischen Akteuren, den Förderorganisationen und den Forschenden nachdrücklich, gemeinsame europäische Lösungen im Sinne des Positionspapiers zu suchen, zu unterstützen und zu nutzen.

| ¹²⁶ https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe/cluster-3-civil-security-society_en.

D. Ausblick auf die Folgen für das Wissenschaftssystem

Eingangs wurde unterstrichen, dass die beobachtbaren weltpolitischen Entwicklungen im Zusammenspiel mit der enormen Dynamik der emergierenden Technologien Praxis und Governance des Wissenschaftssystem verändern werden. Wie für die gesamte Gesellschaft steht auch für das Wissenschaftssystem eine **intensive Debatte vor der Tür, wie angesichts begrenzter Ressourcen neue Prioritäten und Orientierungen zur Schaffung einer sicheren sowie nach außen und innen resilienten Gesellschaft** gesetzt werden können und sollten. Der Wissenschaftsrat spricht sich dafür aus, dass diese Debatte auch und gerade in Hochschulen und Forschungseinrichtungen geführt wird. Dabei sollte explizit auch die Frage der Angemessenheit von Zivilklauseln für wissenschaftliche Einrichtungen diskutiert werden. Denn letztere sind Orte, an denen Lehrende und Studierende öffentlich oder im geschützten Raum akademischer Lehre einen solchen Diskurs führen können und sollten.

In der Debatte darf der **Fokus nicht auf Deutschland allein gerichtet** sein. Sicherheit und Resilienz sind letztlich allein in einem größeren Kontext, vor allem im Zusammenspiel mit den unterschiedlichen europäischen Partnerländern, zu erreichen. Dies gilt für beide zentralen Zielrichtungen des Positionspapiers: Der effektive Schutz vor Wissensrisiken gelingt besser in Abstimmung mit europäischen Partnern oder anderen Partnern, die gleichermaßen eine regelbasierte liberale Ordnung im eigenen Land und weltweit verfolgen. Qualität und Wirkungsmächtigkeit sicherheitsrelevanter Forschung kann gesteigert werden, wenn Kooperationen über Institutionen- und Ländergrenzen hinweg ge- und befördert werden – insbesondere vor dem Hintergrund der Empfehlung, die Forschung stärker zu integrieren und systemisch auszurichten.

Die hier vorgeschlagenen **Strategien und Maßnahmen** zum Umgang mit Wissensrisiken und zur Förderung sicherheitsrelevanter Forschung **sollten in regelmäßigen Abständen auf ihre Wirksamkeit und Effektivität überprüft** werden. Die gesammelten Erfahrungen und die Ergebnisse einer solchen Überprüfung sollten zu ihrer Anpassung und Weiterentwicklung genutzt werden. Wesentlicher Gesichtspunkt der Evaluation sollte der Aufwand auf Seiten von Wissenschaftlerinnen und Wissenschaftlern wie auch Einrichtungen sein. Standards und bürokratische Prozesse können rasch ein Eigenleben entwickeln, so dass sie

für viele Organisationen zu einer Belastung werden, ohne dass sie zu den gewünschten Erfolgen führen – etwa zur effektiven Identifikation von Sicherheitsrisiken in Forschungsvorhaben oder Austauschprojekten.

Darüber hinaus zeichnet sich schon jetzt ab, dass dieser Wandel im Umgang mit Wissensrisiken und sicherheitsrelevanten wissenschaftlichen Arbeiten **weitergehende Auswirkungen** auf das Wissenschaftssystem zeitigen wird – bis ins Selbstverständnis von Forschenden, Lehrenden und Studierenden hinein und vor allem hinsichtlich Arbeiten zu militärischen Zwecken. Vor dem Hintergrund der unterschiedlichen bisher gewonnenen Erfahrungen hebt der Wissenschaftsrat drei Auswirkungen exemplarisch hervor:

1 – Verschiebungen im globalen Netzwerk von Wissenschaft: In Zukunft werden sich internationale Netzwerke in anderer Weise entwickeln. **Nicht allein Qualität und Innovationskraft werden die Attraktivität wissenschaftlicher Partnerinnen und Partner bestimmen.** Vielmehr spielen auch genuin politische Motive für deren Wahl eine Rolle, wie im Anschluss an den Angriffskrieg Russlands auf die Ukraine zu beobachten war. Die Wissenschaftsorganisationen haben das Kooperationsverbot mit russischen Akteuren mitgetragen und umgesetzt. Diese Veränderungen wirken sich etwa auf Rekrutierung und Auswahl internationaler Kräfte, vor allem junger Kräfte, sowie auf Reisebeschränkungen für Wissenschaftlerinnen und Wissenschaftler aus. Gegebenenfalls verlieren sie den Zugang zu ihren Forschungsgegenständen oder dieser wird eingeschränkt. Damit sind nur einige der möglichen, derzeit in ihren Wirkungen noch nicht absehbaren Folgen für das Handeln der wissenschaftlichen Akteure im internationalen Kontext aufgezeigt.

Das globale System wissenschaftlicher Kooperationen ist auch ein Element in der diplomatischen Zusammenarbeit. Dabei darf nicht übersehen werden, dass sich die Voraussetzungen so geändert haben, dass dieses gewachsene System internationaler wissenschaftlicher Kooperationen sowohl für die unerwünschte Einflussnahme im eigenen Land als auch jenseits unserer nationalen Grenzen ausgenutzt werden kann. | ¹²⁷ Der Wissenschaftsrat hält es daher für geboten, sich rasch über diese Folgen klar zu werden mit dem Ziel, ein **neues Verständnis von Wissenschaftsdiplomatie** zu entwickeln. Dazu sollte der Austausch auf europäischer Ebene gesucht werden. Dabei gilt es zu berücksichtigen, dass vermehrt nichtstaatliche Akteure wie große, global agierende Technologieunternehmen Wissenschaftsdiplomatie einsetzen, um ihre eigenen Interessen zu

| ¹²⁷ Vgl. The Royal Society; American Association for the Advancement of Science (AAAS) (2025): Science diplomacy in an era of disruption; London, S. 5, <https://royalsociety.org/-/media/about-us/international/science-diplomacy/science-diplomacy-in-an-era-of-disruption.pdf>.

verfolgen, die durchaus von denen der nationalen Regierung divergieren können. | ¹²⁸ Die Herausforderung besteht darin, wissenschaftliche Kooperationen, die – wie eingangs formuliert (vgl. A) – nötiger denn je sind, um große gesellschaftliche Herausforderungen zu bearbeiten, auch als eine Chance des Austausches und des Aufbaus von gegenseitigem Vertrauen zu sehen – gerade in langwierigen Konfliktsituationen. Ziel sollte es keineswegs sein, solche Kooperationsstränge einfach zu kappen.

Mit Blick auf Europa kann das Wissenschaftssystem weiterhin dazu beitragen, die Verbindungen zwischen den unterschiedlichen Staaten Europas zu stärken. Entscheidend ist hier, dass alle **Akteure im Wissenschaftssystem** – einzelne Forschende, wissenschaftliche Einrichtungen und Wissenschaftsorganisationen sowie die politische Ebene – sich in der **Verantwortung** sehen, **die europäische Dimension in ihrem Handeln mit zu berücksichtigen**. Wissenschaftliche Aktivitäten und wissenschaftspolitische Initiativen tragen dazu bei, im europäischen Raum Vertrauen aufzubauen und sich im Handeln besser abzustimmen.

2 – Weiterentwicklung des Reputationssystems: **Reputation** ist die entscheidende Währung im Wissenschaftssystem. Sie gilt als **Indiz für wissenschaftliche Leistungen von hoher Qualität und steuert Aufmerksamkeit und Rezeptionsbereitschaft** im Wissenschaftssystem. | ¹²⁹ Zudem trägt sie wesentlich zur Anerkennung einer Person, Gruppe oder Organisation auch in anderen gesellschaftlichen Zusammenhängen bei und kann in Ressourcen (Budget, Stellen, Ausstattung) konvertiert werden.

Reputation hängt mit dem zugrundeliegenden Bewertungsregime zusammen, in dem vielfach Zahl und Qualität der **Publikationen** sowie die Höhe der wettbewerblich eingeworbenen **Drittmittel eine Schlüsselrolle** spielen. Wenn eine Publikation über Forschungsergebnisse in sicherheitsrelevanten Bereichen aus guten Gründen nicht möglich ist, kann sich dies folglich negativ auf Reputation und Karrierechancen des oder der Einzelnen auswirken. Um dieses Problem abzumildern, gibt es beispielsweise in den USA der Geheimhaltung unterliegende begutachtete Fachzeitschriften für Arbeiten aus den sicherheitsrelevanten Bereichen der National Laboratories. Ein solcher Weg ist für das relativ überschaubare Wissenschaftssystem in Deutschland aber nicht realisierbar, wohl auch

| ¹²⁸ Vgl. dazu: 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>. Die großen Unternehmen „[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“, ebd., S. 5.

| ¹²⁹ Vgl. grundlegend zu Reputation in der Wissenschaft: Luhmann, N. (1990): Die Wissenschaft der Gesellschaft; Frankfurt a. M. Und kritisch weiterführend: Schimank, U. (2010): Reputation statt Wahrheit: Verdrängt der Nebencode den Code?, in: Soziale Systeme 16 (2010), Heft 2, S. 233–242, <https://doi.org/10.1515/so-sys-2010-0204>. Schimank spricht von einer „Quantifizierung der Reputation“, ebd., S. 235.

kaum im europäischen Raum. Möglicherweise ließe es sich im Rahmen einer derzeit diskutierten Europäischen Verteidigungsunion (EVU) realisieren. | ¹³⁰

Schon seit längerer Zeit wird auf deutscher Ebene, etwa von Seiten der DFG, und auf europäischer Ebene versucht, das **Bewertungssystem weiterzuentwickeln**. Die von der Coalition for Advancing Research Assessment (CoARA) | ¹³¹ formulierte Vision, die unterschiedlichen Formate wissenschaftlichen Arbeitens in ihrer Qualität und mit ihren diversen Wirkungen wertzuschätzen, ist in diesem Feld wichtiger denn je. Wenn sich junge Wissenschaftlerinnen und Wissenschaftler nicht auf ein angemessenes Bewertungsregime verlassen können, werden sie sich mittel- und langfristig nicht für eine solche Arbeit begeistern.

Reputationssysteme entwickeln sich nur sehr langsam. Hier bedarf es eines **Bewusstseinswandels auf Seiten der Bewertenden**. In den Ingenieurwissenschaften zählt die Tätigkeit in einem Industrieunternehmen – verbunden mit wissenschaftlichen Aktivitäten – als Leistung im Lebenslauf. Analog sollten Tätigkeiten in Innovation Hubs oder anderen geschützten Orten explizit in der Bewertung berücksichtigt werden – auch in Berufungsverfahren oder im Zuge der Vergabe von Fördergeldern. Gegebenenfalls sind andere Wege zu suchen, um eine Person und ihre Leistungsfähigkeit einschätzen zu können. In jedem Fall bedarf es einer angemessenen Würdigung der Arbeiten, die nicht oder nur in geringerem Maße zu Publikationen führen. Darüber hinaus regt der Wissenschaftsrat an, neue Instrumente wie spezifische Preise zu entwickeln, um Anreize für die Arbeit in sicherheitsrelevanten Bereichen und an Orten wie den erwähnten Innovation Hubs zu schaffen.

3 – Überprüfung von Open Science-Policies: Austausch, Kooperation und Innovation gelingen am besten unter Bedingungen der Offenheit. Wissen, Infrastrukturen, Methoden etc. so früh und so weit wie möglich zu teilen – auch über den akademischen Kreis hinaus – galt lange Zeit als Garant für eine dynamische Entwicklung von Wissenschaft und Gesellschaft. Daher wurde **in den letzten Jahrzehnten eine Open Science-Policy wissenschaftspolitisch gefordert und gefördert**. Deutschland hat sich zu Open Access bekannt und trägt die UNESCO-Empfehlung | ¹³² grundsätzlich mit, ohne eine nationale Open Science-Strategie

| ¹³⁰ Die EVU soll die NATO ergänzen und die strategische Autonomie Europas stärken. Sie zielt auf eine engere militärische Zusammenarbeit und Integration innerhalb der EU. Dies soll nicht allein zu einer koordinierten Verteidigungsstrategie führen, sondern auch zur Unterstützung von Forschung und Entwicklung im Verteidigungssektor (Europäischer Verteidigungsfonds).

| ¹³¹ Vgl. <https://coara.eu/>.

| ¹³² Vgl. United Nations Educational, Scientific and Cultural Organization (UNESCO); Canadian Commission for UNESCO (2022): An introduction to the UNESCO Recommendation on Open Science; Paris, <https://doi.org/10.54677/XOIR1696>. Nach Auffassung der UNESCO soll wissenschaftliches Wissen so offen wie möglich sein. Aber unter bestimmten Bedingungen sind Einschränkungen auch gerechtfertigt, wozu auch die nationale Sicherheit gehört: „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

entwickelt zu haben. Eine solche Policy impliziert nicht einen völlig freien Fluss von Wissen und Daten. Denn es gibt gute Gründe, bestimmte Erkenntnisse nicht sofort oder nicht in vollem Umfang mit anderen zu teilen, etwa zum Schutz legitimer Interessen von Forschenden und Forschungseinrichtungen, wenn diese ihr Wissen wirtschaftlich verwerten wollen.

Vor dem Hintergrund der internationalen Entwicklungen sollte über die konkrete **Ausgestaltung der Formel „so offen wie möglich, so geschlossen wie nötig“ noch einmal reflektiert** werden. In Deutschland könnte – insbesondere bezogen auf den Umgang mit Daten – die Nationale Forschungsdateninfrastruktur e. V. (NFDI) ein Forum für eine solche Reflexion sein. Angesichts der sich verschärfenden Systemkonkurrenzen ist nach Auffassung des Wissenschaftsrats eine solche Reflexion nicht allein auf deutscher, sondern auch auf europäischer Ebene geboten. Ziel sollte es sein, sich in Zukunft darauf zu verständigen, was es bedeutet, kontrolliert und gemanagt offen vorzugehen.

Der Wissenschaftsrat ist davon überzeugt, dass ein offenes und freies Wissenschaftssystem, wie es derzeit in Deutschland und in den meisten europäischen Ländern gelebt wird, ein Wert an sich ist. Es schafft, wie eingangs dargestellt (vgl. A.II), mit seinem Wissen eine Grundlage für die Bewältigung der komplexen Herausforderungen unserer Zeit und fungiert zugleich als unabhängige und kritische Instanz gegenüber Machtansprüchen des Staates, aber auch anderer Akteure wie zum Beispiel großer Technologieunternehmen. Im internationalen Kontext entwickelt ein solches System eine hohe Attraktivität für kreative Köpfe und kann daher einen Wettbewerbsvorteil darstellen. Dafür sollten die Rahmenbedingungen wie etwa aussichtsreiche Karrierewege, ausreichende und souveräne Forschungs- und Dateninfrastrukturen sowie attraktive Studienangebote stimmen. Der Wissenschaftsrat sieht hier auch eine **Verantwortung der öffentlichen Hand, das Wissenschaftssystem in einer Weise zu gestalten und zu fördern, dass Wissenschaft auch in Zukunft diese grundlegende Funktion für eine freie Gesellschaft übernehmen kann**. Von einem offenen und freien Wissenschaftssystem, in dem Wissenssicherheit gewährleistet und sicherheitsrelevante Forschung zum Schutz und zur Resilienz der Gesellschaft betrieben wird, profitieren alle: von den einzelnen Bürgerinnen und Bürgern über eine prosperierende Wirtschaft bis hin zu einer stabilen demokratischen Gesellschaft.

and public order, the protection of intellectual property rights, personal information, sacred and secret indigenous knowledge, and rare, threatened or endangered species.“ United Nations Educational, Scientific and Cultural Organization (UNESCO); Canadian Commission for UNESCO (2022): An introduction to the UNESCO Recommendation on Open Science; Paris, S. 11, <https://doi.org/10.54677/XOIR1696>. Und <https://www.unesco.org/en/open-science>; zur Situation in Deutschland: Deutsche UNESCO-Kommission (2020): Open Science. Perspektiven aus Deutschland auf die Erarbeitung der geplanten Empfehlung der UNESCO; Bonn, <https://www.unesco.de/themen/wissenschaft/open-science/>.

Anhang

ANHANG 1: FRAGEN ZUR ERLÄUTERUNG VON WISSENSRISIKOTYPEN

Um für Themen der Wissenssicherheit und der Sicherheitsrelevanz wissenschaftlichen Arbeitens zu sensibilisieren, regt der Wissenschaftsrat an, systematisch die genannten fünf Risikotypen (vgl. B.III) anhand von Leitfragen zu prüfen. Die folgenden Listen sind nicht vollständig und sind allein als exemplarische Fragen zu verstehen, um den jeweiligen Risikotyp zu erläutern.

Zu 1: Unerwünschter Wissens- und Technologieabfluss

- _ Besteht zwischen den Akteuren eine signifikante Technologie- und/oder Wissenslücke? Könnte die Schließung dieser Lücke das primäre Interesse des oder der Kooperationspartner sein?
- _ Handelt es sich bei der Forschung um die Kronjuwelen | ¹³³ eines Akteurs?
- _ Gibt es eine vertragliche Kooperationsvereinbarung, in der alle beteiligten Akteure gleichermaßen den Zugang und die Nutzung der Forschungsdaten sicherstellen? Beinhaltet diese auch Regularien zu Verschwiegenheitspflicht, Verbreitung und Publikation?
- _ In welcher Weise werden bestehende IP-Rechte, Forschungsdaten oder vertrauliche Daten des Projektes oder zurückliegender Projekte Dritten zur Verfügung gestellt (auch im Sinne des remote access) oder geteilt? Wie werden sie geschützt?
- _ Zu welchen Gebäuden, Informationen oder internen Netzwerken werden Kooperationspartner oder Gäste Zugang haben?

| ¹³³ Der Begriff der Kronjuwelen stammt aus dem wirtschaftlichen Kontext. Dort sind damit „besonders attraktive Vermögensgegenstände eines Unternehmens im Sinne ihres gegenwärtigen sowie potenziellen zukünftigen Wertes“ gemeint, <https://www.gabler-banklexikon.de/definition/crown-jewels-56809>. Er wird zunehmend auch im Kontext der wissenschaftspolitischen Diskussion verwendet, so etwa in den Guidelines der Niederlande, wonach damit Folgendes gemeint ist: „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, S. 29, <https://english.loketkennisveiligheid.nl/documents/publications/2022/04/07/national-knowledge-security-guidelines>.

- _ Ist mit patentierbaren oder anderweitig kommerziell relevanten Ergebnissen zu rechnen?
- _ Umfasst die Forschung sog. Emerging Technologies, die ausgenutzt werden könnten?

Zu 2: Unerwünschte Einflussnahme auf das Wissenschaftssystem

- _ Besteht die Möglichkeit, dass Publikationsaktivitäten und die Nutzung von Daten eingeschränkt oder behindert werden?
- _ Gehen von Gästen (Wissenschaftlerinnen und Wissenschaftler, Studierende etc.) oder Kooperationspartnern Risiken aus, die bestehenden Werte und die Kultur der Einrichtung unangemessen beeinflussen?
- _ Werden im Zuge der Austausch- und/oder Kooperationsaktivitäten biometrische, genetische oder andere Daten erfasst, die mit den Werten und Standards der eigenen Einrichtung nicht im Einklang stehen?

Zu 3: Finanzielle und wissenschaftliche Abhängigkeiten

- _ Gibt es finanzielle oder materielle Zuwendungen (Fördermittel, Stipendien, Vergütung, Ausstattung etc.), die direkt oder indirekt (z. B. über Unternehmen) aus kritisch eingestuften Ländern stammen, und werden diese gemeldet?
- _ Wie sieht die finanzielle Beteiligung der einzelnen Akteure aus und könnte dadurch ein Ungleichgewicht bezüglich Kontrolle und Mitspracherecht entstehen?
- _ Werden Kooperationspartner oder -partnerinnen durch staatliche Stipendien- oder Förderprogramme aus dem Ausland finanziert? Um welche Art von Förderprogramm handelt es sich (z. B. um ein malign foreign talent recruitment program)?

Zu 4: Interferenzen wissenschaftlicher Aktivitäten mit anderen gesellschaftlichen Bereichen

- _ Was sind die konkreten Ziele der Kooperation und welcher Nutzen ergibt sich daraus für die eigene und die kooperierenden Institutionen?
- _ Welche Ziele könnten jenseits der wissenschaftlichen Kooperationen verfolgt werden und welcher Nutzen ergibt sich daraus für das kooperierende Land oder Unternehmen?
- _ Welche symbolischen Implikationen hat ein wissenschaftlicher Austausch, eine wissenschaftliche Kooperation?

- _ Könnten die Forschungsergebnisse zu unethischen oder unmoralischen Zwecken missbraucht werden?
- _ Vertreten alle Akteure vergleichbare akademische Werte, ethische Standards sowie Grund- und Menschenrechte?
- _ Werden sämtliche gesetzlichen Vorschriften und Regelungen von allen Akteuren eingehalten und mitgetragen? Dazu gehören etwa die Bestimmungen zur Exportkontrolle oder zum Datenschutz.
- _ Wurde ein Kooperationspartner, eine Kooperationspartnerin oder eine kooperierende Institution illegaler Tätigkeiten beschuldigt, angeklagt oder verurteilt? Dazu gehören insbesondere Betrug, Erpressung, Spionage und Korruption sowie Diebstahl geistigen Eigentums, Urheberrechtsverletzungen und Patentdiebstahl, aber auch Verletzungen im Umgang mit Gütern unter Exportkontrolle oder anderweitigem Schutz.

Dem Wissenschaftsrat ist durchaus bewusst, dass es bereits elaborierte Prüfprozesse gibt, in die die Identifizierung dieser Risiken eingeflossen ist. Zu verweisen ist hier auf die Mitte 2024 erschienene „Handreichung für einen Prüfprozess zum Wissenschafts- und Kooperationsschutz in der internationalen Zusammenarbeit von Hochschulen und Forschungseinrichtungen“. | ¹³⁴

| ¹³⁴ Vgl. DLR Projektträger Safeguarding Science Team (2024): Due Diligence in Science. Handreichung für einen Prüfprozess zum Wissenschafts- und Kooperationsschutz in der internationalen Zusammenarbeit von Hochschulen und Forschungseinrichtungen; Bonn, https://www.safeguarding-science.eu/wp-content/uploads/Due-Diligence-in-Science_German-Handreichung2024.pdf.

Tabelle 1: Ausgaben des Bundesministeriums der Verteidigung für Forschung und Entwicklung sowie für wehrtechnische Forschung und Technologie sowie Entwicklung und Erprobung, in Mio. Euro (Stand März 2025)

	Forschung und Entwicklung	wehrtechnische Forschung und Technologie		wehrtechnische Entwicklung und Erprobung*		Grundfinanzierung (DLR, FhG, ISL)
		Haushalt	Sondervermögen	Haushalt	Sondervermögen	
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

Quellen: Forschung und Entwicklung: <https://www.datenportal.bmbf.de/portal/de/K1/grafik-1.1.4.html>; Wehrtechnische Forschung und Technologie sowie Entwicklung und Erprobung: <https://www.bundeshaushalt.de/DE/Bundeshaushalt-digital/bundeshaushalt-digital.html>, sowie Grundfinanzierung (DLR, FhG, ISL) Bundeshaushaltspläne Einzelpläne 14 der Jahre 2017-2024, bspw. <https://www.bundeshaushalt.de/static/daten/2024/soll/epl14.pdf>. *Im Sondervermögen und im Haushaltskapitel zur Wehrforschung sind neben den Ausgaben für die Entwicklung und Erprobung auch die Ausgaben für die Entwicklung (nicht Beschaffung) des Waffensystems Eurofighter, Kampfflugzeuges Multi-Role Combat Aircraft (MRCA), Main Ground Combat System (MGCS), Next Generation Weapon Systems (NGWS) in einem Future Combat Air System (FCAS). Soll-Zahlen sind kursiv gesetzt.

Tabelle 2: Grundfinanzierung von Forschungsinstituten aus dem Einzelplan 14, in Mio. Euro (Stand März 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

Bei der Förderung des Deutsch-Französischen Forschungsinstitutes Saint-Louis (ISL) liegt keine Zuwendung nach §§ 23, 44 Bundeshaushaltsordnung (BHO) vor. Die Zahlungsgrundlage ist stattdessen der deutsch-französische Staatsvertrag vom 31. März 1958, der jährlich durch einen Regierungszusatzvertrag ergänzt wird.

Quelle: Bundeshaushaltspläne Einzelpläne 14 der Jahre 2017-2024, bspw. <https://www.bundeshaushalt.de/static/daten/2024/soll/epl14.pdf>, Soll-Zahlen sind kursiv gesetzt.

BAFA	Bundesamt für Wirtschaft und Ausfuhrkontrolle
BfV	Bundesamt für Verfassungsschutz
BMFTR	Bundesministerium für Forschung, Technologie und Raumfahrt
BMF	Bundesministerium für Finanzen
BMVg	Bundesministerium der Verteidigung
DAAD	Deutscher Akademischer Austauschdienst e. V.
DFG	Deutsche Forschungsgemeinschaft
DLR	Deutsches Zentrum für Luft- und Raumfahrt e. V.
EFI	Expertenkommission Forschung und Innovation
FhG	Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e. V.
GA	Gemeinsamer Ausschuss zum Umgang mit sicherheitsrelevanter Forschung
GoF	Gain of Function
ISL	Deutsch-Französisches Forschungsinstitut Saint-Louis
KEF	Kommissionen für Ethik sicherheitsrelevanter Forschung
KI	Künstliche Intelligenz
KIWi	Kompetenzzentrum Internationale Wissenschaftskooperationen
NOAA	National Oceanic and Atmospheric Administration
TRL	Technology Readiness Level; Technologiereifegrad
WR	Wissenschaftsrat

Mitwirkende

Im Folgenden werden die an den Beratungen im Wissenschaftsrat und in dem Ausschuss Forschung beteiligten Personen sowie die beteiligten Mitarbeiterinnen und Mitarbeiter der Geschäftsstelle aufgelistet.

Die von Arbeitsgruppen und Ausschüssen erarbeiteten Entwürfe werden bei den einstufigen Verfahren in den Kommissionen des Wissenschaftsrats diskutiert und können gegebenenfalls auch verändert werden. Im Ergebnis ist damit der Wissenschaftsrat Autor der veröffentlichten Empfehlungen, Stellungnahmen und Positionspapiere.

Vorsitzender

Professor Dr. Wolfgang Wick
Universitätsklinikum Heidelberg | Deutsches Krebsforschungszentrum
Heidelberg (DKFZ)

Generalsekretär

Thomas May
Geschäftsstelle des Wissenschaftsrats

Wissenschaftliche Kommission des Wissenschaftsrats

Professorin Dr. Jutta Allmendinger
Humboldt-Universität zu Berlin | Freie Universität Berlin

Professorin Dr. Julia C. Arlinghaus
Otto-von-Guericke-Universität Magdeburg | Fraunhofer-Institut
für Fabrikbetrieb und -automatisierung IFF, Magdeburg
Vorsitzende der Wissenschaftlichen Kommission

Professorin Dr. Liane G. Benning
Freie Universität Berlin | Deutsches GeoForschungsZentrum (GFZ) Potsdam

Dr. Ulrich A. K. Betz
Merck KGaA

Professor Dr. Folkmar Bornemann
Technische Universität München

Professorin Dr. Eva-Lotta Brakemeier
Universität Greifswald

Professorin Dr. Alena Michaela Buyx
Technische Universität München

Professorin Dr. Petra Dersch
Universität Münster

Professorin Dr. Nina Dethloff
Rheinische Friedrich-Wilhelms-Universität Bonn

Professor Dr. Jakob Edler
Fraunhofer-Institut für System- und Innovationsforschung ISI |
Manchester Institute of Innovation Research

Professor Dr. Christian Facchi
Technische Hochschule Ingolstadt

Professorin Dr. Christine Falk
Medizinische Hochschule Hannover

Professorin Dr. Uta Gaidys
Hochschule für Angewandte Wissenschaften Hamburg

Professor Dr. Michael Hallek
Universität zu Köln

Dr.-Ing. Frank Heinrich

Professor Dr. Frank Kalter
Universität Mannheim | Deutsches Zentrum für Integrations- und Migrations-
forschung (DeZIM) e. V.

Dr. Stefan Kampmann
Unternehmensberater, Knetzgau

Professor Dr. Wolfgang Lehner
Technische Universität Dresden

Professorin Dr. Anne Lequy
Hochschule Magdeburg-Stendal

Andrea Martin
IBM DACH

Professorin Dr. Gabriele Metzler
Humboldt-Universität zu Berlin

Professorin Dr. Friederike Pannewick
Philipps-Universität Marburg

Professorin Dr. Ursula Rao
Max-Planck-Institut für Ethnologische Forschung, Halle |
Universität Leipzig

Professorin Dr. Gabriele Sadowski
Technische Universität Dortmund

Professor Dr. Ferdi Schüth
Max-Planck-Institut für Kohlenforschung, Mülheim/Ruhr
Stellvertretender Vorsitzender der Wissenschaftlichen Kommission

Dr. Harald Schwager
EVONIK Leading Beyond Chemistry

Professorin Dr. Christine Silberhorn
Universität Paderborn

Professor Dr. Thomas S. Spengler
Technische Universität Braunschweig

Professorin Dr. Birgit Spinath
Universität Heidelberg

Professor Dr. Klement Tockner
Goethe-Universität Frankfurt am Main | Senckenberg Gesellschaft für Natur-
forschung Frankfurt

Professor Dr. Wolfgang Wick
Universitätsklinikum Heidelberg | Deutsches Krebsforschungszentrum (DKFZ)
Vorsitzender des Wissenschaftsrats

Professor Dr. Oliver Zielinski
Universität Rostock | Leibniz-Institut für Ostseeforschung Warnemünde

Verwaltungskommission (Stand: Mai 2025)

Von der Bundesregierung entsandte Mitglieder

N. N.
Bundesministerium für Forschung, Technologie
und Raumfahrt

N. N.
Bundesministerium für Forschung, Technologie
und Raumfahrt

N. N.
Bundesministerium der Finanzen

N. N.
Bundesministerium des Innern

N. N.
Bundesministerium für Landwirtschaft, Ernährung und
Heimat

N. N.
Bundesministerium für Wirtschaft und Energie

Von den Länderregierungen entsandte Mitglieder

Baden-Württemberg

Petra Olschowski
Ministerin für Wissenschaft, Forschung und Kunst

Markus Blume
Staatsminister für Wissenschaft und Kunst
Vorsitzender der Verwaltungskommission

Berlin

Dr. Ina Czyborra
Senatorin für Wissenschaft, Gesundheit und Pflege

Brandenburg

Dr. Manja Schüle
Ministerin für Wissenschaft, Forschung und Kultur

Bremen

Kathrin Moosdorf
Senatorin für Umwelt, Klima und Wissenschaft

Hamburg

Dr. Andreas Dressel
Präses der Behörde für Finanzen und Bezirke

Hessen

Timon Gremmels
Minister für Wissenschaft und Forschung, Kunst und Kultur

Mecklenburg-Vorpommern

Bettina Martin
Ministerin für Wissenschaft, Kultur, Bundes- und Europaangelegenheiten

Niedersachsen

Falko Mohrs
Minister für Wissenschaft und Kultur

Nordrhein-Westfalen

Ina Brandes
Ministerin für Kultur und Wissenschaft

Rheinland-Pfalz

Clemens Hoch
Minister für Wissenschaft und Gesundheit

Jakob von Weizsäcker
Minister der Finanzen und für Wissenschaft

Sebastian Gemkow
Staatsminister für Wissenschaft im Staatsministerium für Wissenschaft,
Kultur und Tourismus

Professor Dr. Armin Willingmann
Minister für Wissenschaft, Energie, Klimaschutz und Umwelt
Stellvertretender Vorsitzender der Verwaltungskommission

Dr. Dorit Stenke
Ministerin für Allgemeine und Berufliche Bildung, Wissenschaft,
Forschung und Kultur

Christian Tischner
Minister für Bildung, Wissenschaft und Kultur

Professor Dr. Ferdi Schüth

Max-Planck-Institut für Kohlenforschung, Mülheim/Ruhr

Stellvertretender Vorsitzender der Wissenschaftlichen Kommission des WR

Vorsitzender des Ausschusses

Professorin Dr. Julia C. Arlinghaus

Otto-von-Guericke-Universität Magdeburg | Fraunhofer-Institut

für Fabrikbetrieb und -automatisierung IFF, Magdeburg

Vorsitzende der Wissenschaftlichen Kommission des WR

Ministerialdirigentin Dr. Christine Burtscheidt

Hessisches Ministerium für Wissenschaft und Forschung, Kunst und Kultur

Professor Dr. Jakob Edler

Fraunhofer-Institut für System- und Innovationsforschung ISI |

Manchester Institute of Innovation Research

Mitglied der Wissenschaftlichen Kommission des WR

Professor Dr. Michael Hallek

Universität zu Köln

Mitglied der Wissenschaftlichen Kommission des WR

Professor Dr. Wolfgang Lehner

Technische Universität Dresden

Mitglied der Wissenschaftlichen Kommission des WR

Ministerialrat Dr. Florian Leiner

Bayerisches Staatsministerium für Wissenschaft und Kunst

Ministerialrat Ralf Maier

Bundesministerium für Forschung, Technologie und Raumfahrt

(vormals Bundesministerium für Bildung und Forschung)

Professorin Dr. Gabriele Metzler

Humboldt-Universität zu Berlin

Mitglied der Wissenschaftlichen Kommission des WR

Als Gäste:

Dr. Svenja Gertheiss

Bundesministerium für Forschung, Technologie und Raumfahrt

(vormals Bundesministerium für Bildung und Forschung)

Ministerialrätin Esther Seng

Bundesministerium für Forschung, Technologie und Raumfahrt

(vormals Bundesministerium für Bildung und Forschung)

Professorin Dr. Birgit Spinath

Universität Heidelberg

Mitglied der Wissenschaftlichen Kommission des WR

Professor Dr. Wolfgang Wick

Universitätsklinikum Heidelberg | Deutsches Krebsforschungszentrum (DKFZ)

Vorsitzender des Wissenschaftsrats

Als externe Sachverständige:

Professor Dr. Volker Epping

Leibniz Universität Hannover

Professor Dr. Michael Lauster

Fraunhofer-Institut für Naturwissenschaftlich-Technische Trendanalysen INT,
Euskirchen

Professorin Dr. Ursula Schröder

Universität Hamburg

Dr. Annette Barkhaus (stellvertretende Abteilungsleiterin)

Miriam Betge (Sachbearbeiterin)

Gudrun Hilles (Sachbearbeiterin)

Dr. Rainer Lange (Abteilungsleiter)

Britta Philippsen (Teamassistentin)

Leila Young (Sachbearbeiterin)