WR

WISSENSCHAFTSRAT

Saarbrücken 20 10 2023

Empfehlungen zur Souveränität und Sicherheit der Wissenschaft im digitalen Raum

IMPRESSUM

Empfehlungen zur Souveränität und Sicherheit der Wissenschaft im digitalen Raum

Herausgeber

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

Drucksachennummer: 1580-23

DOI: https://doi.org/10.57674/m6pk-dt95

Veröffentlicht

Köln, Oktober 2023

Vorbemerkung

Die vorliegenden Empfehlungen knüpfen an das im Jahr 2021 verabschiedete Positionspapier des Wissenschaftsrats „Impulse aus der COVID-19-Krise für die Weiterentwicklung des Wissenschaftssystems in Deutschland“ an. Darin hat der Wissenschaftsrat betont, wie wichtig Souveränität und Sicherheit im digitalen Raum sind, wenn ein resilientes Wissenschaftssystem sichergestellt werden soll, und erhebliche Kraftanstrengungen in dieser Hinsicht angemahnt. Zudem forderte er die Akteure des Wissenschaftssystems auf, den digitalen Raum aktiv mitzugestalten und die sich eröffnenden Potenziale gewinnbringend zu nutzen.

Im Bewusstsein, dass Fragen der digitalen Souveränität und Sicherheit einer ausgesprochenen Dynamik unterworfen sind und in eine Vielzahl von Politik- und Gesellschaftsbereichen hineinreichen, zielen die Empfehlungen darauf, wissenschaftsspezifische Aspekte in den Blick zu nehmen und daran anknüpfend Leitlinien und Prinzipien zu formulieren, wie diese Herausforderungen adressiert werden sollten. Im Zentrum steht dabei die Souveränität und Sicherheit wissenschaftlicher Einrichtungen, der in ihnen tätigen Personen sowie des (deutschen) Wissenschaftssystems insgesamt. Übergeordnete Überlegungen zur technologischen Souveränität Deutschlands und Europas spielen hierbei zwar mit hinein, sind jedoch nicht Gegenstand der Empfehlungen.

Zur Vorbereitung der Empfehlungen hat der Wissenschaftsrat eine Arbeitsgruppe eingerichtet, die im März 2022 ihre Arbeit aufgenommen hat. Mitgewirkt haben in ihr auch Sachverständige, die nicht Mitglieder des Wissenschaftsrats sind. Ihnen gilt der besondere Dank des Wissenschaftsrats. Ebenso dankt der Wissenschaftsrat weiteren Gesprächspartnerinnen und -partnern, die den Beratungsprozess im Rahmen von Anhörungen und Gesprächen konstruktiv unterstützt haben. Hierzu zählen Vertreter von Digitalverbänden, wissenschaftlichen Rechenzentren und außerhochschulischen Forschungsorganisationen, Hochschulleitungen und -CIOs, Repräsentantinnen und Repräsentanten wissenschaftlicher IT-Dienstleister aus dem In- und Ausland sowie Vertreter öffentlich geförderter Dateninfrastrukturangebote, Clouddienste und Kompetenzzentren.

Der Wissenschaftsrat hat die vorliegenden Empfehlungen am 20. Oktober 2023 in Saarbrücken verabschiedet.

Kurzfassung

Lehre, Forschung und Transfer wie auch die damit verbundenen Verwaltungs- und Managementtätigkeiten sind auf eine zuverlässige, leistungsfähige digitale Infrastruktur und auf hochwertige digitale Dienste und Werkzeuge angewiesen. Wie Wissenschaft die digitalen Möglichkeiten nutzen und weiterentwickeln kann, wirkt sich sowohl auf ihre Praxis als auch auf ihre Gestaltungsfreiheit aus.

Fragen der digitalen Souveränität und Sicherheit werden deshalb immer wichtiger. Forschende, Lehrende und Wissenschaftseinrichtungen | [1] brauchen im digitalen Raum ausreichend Selbstbestimmung und Handlungsfreiheit. Dies betrifft etwa den Zugang zu digitalen Diensten, Infrastrukturen und Daten, die Überprüfbarkeit wissenschaftlicher Ergebnisse oder den Schutz vor Cyberangriffen, der in einem wissenschaftlichen Umfeld, das sich durch Offenheit und Heterogenität auszeichnet, besonders schwierig ist. Andernfalls geraten wesentliche Rahmenbedingungen und Grundprinzipien wissenschaftlichen und wissenschaftsnahen Arbeitens in Gefahr.

Souveränität und Sicherheit im digitalen Raum sind aus Sicht des Wissenschaftsrats zentral für ein resilientes Wissenschaftssystem. Er spricht deshalb folgende Empfehlungen aus:

1 – Die **digitale Selbstbefähigung von Wissenschaftseinrichtungen** muss gestärkt und gefördert werden.

Dies bedeutet insbesondere, die Verantwortung für die digitalen Voraussetzungen des Wissenschaftsbetriebs in jeder Einrichtung klar festzulegen. Diese **Steuerungsaufgaben sollten auf Leitungsebene** verankert und in speziellen Organisationseinheiten (bspw. CIO) abgebildet werden. Auch in einrichtungsinternen Strategie- und Planungsprozessen sollten Fragen der digitalen Souveränität und Sicherheit mehr Beachtung finden. Dazu zählt unter anderem, sich über Zugangs- und Nutzungsrechte für Daten und Software Klarheit zu verschaffen.

Angehörige wissenschaftlicher Einrichtungen sind gefordert, sich mit Chancen und Risiken digitaler Werkzeuge für die Souveränität und Sicherheit wissenschaftlichen Handelns auseinanderzusetzen und ihre Eigenverantwortung kritisch auszuüben. Dieses **Problem- und Risikobewusstsein** gilt es gezielt zu fördern.

| [1] Der Begriff steht für die Gesamtheit der Hochschulen und außerhochschulischen Forschungseinrichtungen im öffentlichen Sektor.

Zudem sind **Personalstrukturen** erforderlich, die den Bedarf für die Planung, den Betrieb und die Absicherung der eigenen IT-Infrastruktur auf professionellem Niveau abdecken. Hier sind Personalverantwortliche und Einrichtungsleitungen gefordert; zugleich wird an Bund und Länder appelliert, auf Anpassungen der Eingruppierungs- und Vergütungssysteme hinzuwirken und den Einrichtungen eine stärkere Orientierung an den marktüblichen Verdienstmöglichkeiten zu ermöglichen.

2 – Dringender Handlungsbedarf besteht im Bereich der **Cybersicherheit** von Wissenschaftseinrichtungen.

Um sich besser vor Cyberangriffen zu schützen, ist der Aufbau leistungsfähiger und professionell aufgestellter Organisations- und Governancestrukturen erforderlich. Erster Schritt ist die Ernennung einer oder eines **IT-Sicherheitsverantwortlichen**.

Jede Einrichtung muss über ein **aktuelles Cybersicherheitskonzept** verfügen, das den Arbeitsweisen und Freiheitsbedürfnissen des wissenschaftlichen Kontextes Rechnung trägt. Neben technischen Vorkehrungen und einer Cybersicherheitsarchitektur, die sich an unterschiedlichen, jeweils angemessenen Schutzniveaus orientiert, sind entsprechende Notfallpläne (Business Continuity) sowie individuelle Schulungs- und Sensibilisierungsmaßnahmen nötig.

3 – **Kooperation und Vernetzung** sollten ausgebaut werden, um Synergie- und Skaleneffekte zu nutzen.

Übergreifende Strukturen und Kooperationen können die Effizienz sowie die Position der Wissenschaft bei der **Beschaffung und dem Betrieb digitaler Infrastrukturen und Dienste** stärken. Bundesweite oder zumindest länderübergreifende Strukturen sollten deshalb, wo Einsatzgebiet, Funktion sowie erforderliche Fertigungstiefe dies zulassen, genutzt und ausgebaut werden.

Der Wissenschaftsrat spricht sich dafür aus, das Potenzial von zentral bereitgestellten **Beratungsangeboten und Kompetenzzentren auf Landes- oder Bundesebene** zu prüfen, um IT-Verantwortliche mit Knowhow zu unterstützen, das vor Ort nicht oder nur eingeschränkt vorhanden ist.

4 – Bei der Auswahl und Gestaltung digitaler Angebote sollten **Pluralität und Offenheit** angestrebt werden, um Abhängigkeiten zu reduzieren und die Handlungsfähigkeit der Wissenschaft zu erhöhen.

Beschaffungs- und Vergabeprozesse sind so zu gestalten, dass ein Anbieterwechsel möglich bleibt sowie definierte Mindeststandards für Pluralität und Offenheit eingehalten werden. Nutzerfreundlichkeit und Funktionalität gilt es dabei stets im Blick zu behalten.

Zur Stärkung von Pluralität und Offenheit ist ein ausreichendes Angebot **öffentlich geförderter Infrastrukturen und Plattformen**, wie NFDI und EOSC, unabdingbar. Diese Angebote müssen möglichst nahtlos an bestehende Strukturen anknüpfen und nutzerfreundlich ausgestaltet sein. Ihre Bekanntheit gilt es zu erhöhen.

Bei der Gestaltung des Softwareangebots können **Open-Source-Lösungen** zu mehr Offenheit und Selbstbestimmtheit beitragen. Angesichts des Betreuungs- und Ressourcenaufwands kann nicht pauschal zum Umstieg geraten werden; dennoch gilt es, wo möglich und sinnvoll, den Einsatz von Open-Source-Software auszubauen und zu fördern. Dies beinhaltet, verlässliche Strukturen und Finanzierungsmöglichkeiten für die nachhaltige Bereitstellung, Pflege und Entwicklung zu etablieren.

Knowhow und Innovationspotenzial der Wissenschaft sollten für die (Weiter-) Entwicklung digitaler Angebote **gezielt genutzt und gefördert werden**. Wenn dadurch Souveränität und Sicherheit gesteigert werden, kann nicht nur die Wissenschaft, sondern auch die Handlungs- und Wettbewerbsfähigkeit der Wirtschaft und anderer Gesellschaftsbereiche profitieren.

5 – Souveränität und Sicherheit lassen sich langfristig nur sichern, wenn auch die strukturellen und finanziellen Rahmenbedingungen des digitalen Wissenschaftsbetriebs weiterentwickelt werden. Daher bekräftigt der Wissenschaftsrat seine Position, dass die **Gestaltung des digitalen Raumes als Daueraufgabe von Wissenschaftseinrichtungen** zu verankern und dem auch in finanzieller Hinsicht Rechnung zu tragen ist. Zugleich sind alle Angehörigen der Einrichtungen gefordert, sich dieser Aufgabe anzunehmen und daran mitzuwirken.

A. Digitale Souveränität und Sicherheit der Wissenschaft – Status quo

A.I HINTERGRÜNDE UND ZIELE

Im Staats- und Völkerrecht sowie der politischen Theorie hat der Souveränitätsbegriff eine lange Tradition. |[2] Im Vergleich dazu ist seine **Verwendung als Leitgedanke für die Ausgestaltung des digitalen Raumes** ein noch recht junges Phänomen. Weil wenige, zumeist US-amerikanische Internet- und Technologiekonzerne als übermächtig wahrgenommen werden, sind Fragen der Datensammlung und -hoheit sowie Abhängigkeiten im Hinblick auf IT-Produkte, digitale Dienstleistungen und grundlegende Kommunikationsinfrastrukturen in den Fokus geraten. In jüngster Zeit haben der technologische Aufstieg Chinas, begleitet von einer zunehmend autoritär ausgerichteten Konnektivitätspolitik, und die Folgen des russischen Angriffs auf die Ukraine die geopolitische Dimension der Diskussion unterstrichen. |[3] Auch die zunehmende Bedrohung durch Cyberangriffe wird heute als Einschränkung der digitalen Souveränität diskutiert.

Mittlerweile ist die Übertragung des Souveränitätsbegriffs auf den digitalen Raum Gegenstand einer breiten Zahl an Veröffentlichungen, die sich der Thematik auch auf einer theoretischen Ebene annähern. Eine einheitliche Definition von digitaler Souveränität hat sich allerdings noch nicht durchgesetzt. |[4] Die meisten Definitionsversuche stellen auf eine grundlegende Selbstbestimmtheit und

| 2 Hierzu ausführlich: Grimm, D. (2009): Souveränität. Herkunft und Zukunft eines Schlüsselbegriffs, Berlin.

| 3 Pohle, J.; Thiel, Th. (2019): Digitale Vernetzung und Souveränität: Genealogie eines Spannungsverhältnisses, S. 58–60, in: Borucki, I.; Schünemann, W. (Hrsg.): Internet und Staat. Perspektiven auf eine komplizierte Beziehung, Baden-Baden, S. 57–80; Ritzi, C.; Zierold, A.: Souveränität unter den Bedingungen der Digitalisierung, S. 35 f., in: Borucki/Schünemann, a. a. O., S. 35–56.

| 4 Einen detaillierten Überblick über verschiedene Definitionsversuche bietet Bundesministerium für Wirtschaft und Energie – BMWi (2021): Schwerpunktstudie Digitale Souveränität. Bestandsaufnahme und Handlungsfelder 2021, Berlin, S. 61–64, https://www.bundesregierung.de/breg-de/service/publikationen/schwerpunktstudie-digitale-souveraenitaet-1981176.

Alle Weblinks in dieser Empfehlung wurden zuletzt am 18.10.2023 abgerufen.

– in unterschiedlichem Ausmaß – auch Unabhängigkeit von Akteuren im digitalen Raum ab. So definiert der IKT-Branchenverband Bitkom digitale Souveränität als „Fähigkeit zu selbstbestimmtem Handeln und Entscheiden im digitalen Raum". |[5] Die Akademie der Technikwissenschaften acatech versteht darunter die „Fähigkeit von Individuen, Unternehmen und Politik, frei zu entscheiden, wie und nach welchen Prioritäten die digitale Transformation gestaltet werden soll." |[6] Und in einer Veröffentlichung des Kompetenzzentrums Öffentliche IT (ÖFIT) wird digitale Souveränität beschrieben als „die Summe aller Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können." |[7]

Die meisten öffentlichen Stellungnahmen zur digitalen Souveränität weisen eine **wirtschafts- und technologiepolitische, teils auch geo- bzw. sicherheitspolitische Stoßrichtung** auf. So werden sowohl Defizite hinsichtlich der selbstbestimmten Steuerung und Ausgestaltung von digitalen Prozessen aller Wirtschafts- und Gesellschaftsbereiche benannt als auch Abhängigkeiten von wenigen privatwirtschaftlichen Unternehmen angeprangert, die noch dazu aus dem außereuropäischen Ausland stammen. Die vielfach artikulierten Forderungen nach (mehr) digitaler Souveränität sind somit Teil breiterer Bestrebungen, die neben einem (Rück-)Gewinn an individueller, gesellschaftlicher und staatlicher Gestaltungshoheit und -freiheit vor allem darauf zielen, die Handlungsfähigkeit sowie die Innovations- und Wettbewerbsfähigkeit der heimischen Wirtschaft zu stärken. |[8] Wesentliche Bezugs- und Rechtfertigungsrahmen bilden geopolitische Handels- und Ressourcenkonflikte sowie der globale Wettbewerb um Technologieführerschaft. |[9]

Digitale Souveränität überschneidet sich, ist aber nicht identisch mit „Technologiesouveränität" |[10], einem Begriff, der vor allem geopolitische Verhältnisse adressiert und mit dem vielfach eine Schwerpunktsetzung auf so genannte Schlüsseltechnologien, wie Künstliche Intelligenz oder Quantencomputer, einhergeht. |[11] So

| 5 Bitkom (2018): Digitale Souveränität. Positionsbestimmung und erste Handlungsempfehlungen für Deutschland und Europa, 05.05.2015, S. 296, in: Datenschutz und Datensicherheit 5 (2018), S. 294–300.

| 6 Kagermann, H.; Streibich, K.; Suder, K. (2021): Digitale Souveränität. Status quo und Handlungsfelder. acatech Impuls, München, S. 8.

| 7 Goldacker, G. (2017): Digitale Souveränität. Diskussionspapier des Kompetenzzentrums Öffentliche IT, Berlin, S. 3.

| 8 Pohle, J.; Thiel, Th. (2019): Digitale Vernetzung und Souveränität: Genealogie eines Spannungsverhältnisses, S. 70 f., in: Borucki, I.; Schünemann, W. (Hrsg.): Internet und Staat. Perspektiven auf eine komplizierte Beziehung, Baden-Baden, S. 57–80.

| 9 Bundesministerium für Wirtschaft und Energie – BMWi (2021): Schwerpunktstudie Digitale Souveränität. Bestandsaufnahme und Handlungsfelder 2021, Berlin, S. 6, https://www.bundesregierung.de/breg-de/service/publikationen/schwerpunktstudie-digitale-souveraenitaet-1981176.

| 10 Hierzu u. a. Edler, J. et al. (2020): Technologiesouveränität. Von der Forderung zum Konzept, Fraunhofer ISI Policy Brief 02/2020, Karlsruhe.

| 11 Zur Identifikation und Auswahl von Schlüsseltechnologien hat Bitkom einen Kriterienkatalog entwickelt, Bitkom (2022): Kriterien zur Identifikation von digitalen Schlüsseltechnologien. Positionspapier 11. Februar 2022,

adressiert das Bundesministerium für Bildung und Forschung (BMBF) unter dem Schlagwort der technologischen Souveränität die Leistungsfähigkeit deutscher und europäischer Entwickler und Hersteller im internationalen Technologiewettbewerb – insbesondere im Verhältnis zu USA, China und Indien – sowie die Versorgungssicherheit mit leistungsfähiger Technologie für nationale Anwender. Als Kern dieses technologisch interpretierten Souveränitätsverständnisses gilt hier, „die souveräne Entwicklung und Anwendung von Schlüsseltechnologien international auf Augenhöhe und im Sinne unserer Werte mitzugestalten." | [12]

Häufig wird der Leitgedanke der digitalen Souveränität nicht nur auf die **kollektive Handlungs- und Gestaltungsfähigkeit von Staat und Wirtschaft**, | [13] sondern auch auf die **digitale Selbstbestimmung Einzelner** bezogen. Forderungen in diese Richtung zielen insbesondere auf den Ausbau interoperabler technischer Angebote, ein Mehr an Verschlüsselung, transparentere Geschäftsmodelle oder auch auf eine Förderung der Medien- und Digitalkompetenz der Bürgerinnen und Bürger. | [14] Auch das Stichwort der „Datensouveränität" fällt in diesem Kontext immer wieder. Es meint den Zugang zu sowie die Bereitstellung und die verantwortungsvolle Nutzung von Daten und bezieht Kompetenzen zum Umgang mit Daten (so genannte Data Literacy) ein. Zugleich hat Datensouveränität eine wirtschaftliche Dimension, gilt der Zugang zu und der Umgang mit Daten doch als ein zentrales Element, um Volkswirtschaften zukunfts- und konkurrenzfähig aufzustellen. | [15]

Ganz im Sinne des staats- und völkerrechtlichen Verständnisses von Souveränität orientieren sich auch die politischen Bestrebungen zur Gestaltung des digitalen Raumes an territorialen Bezugsgrößen. Für den deutschen Fall ist dies neben der nationalen vor allem die europäische Ebene, wo die Stärkung der digitalen Souveränität mehr und mehr zu einem zentralen Handlungsbereich gemeinschaftlicher Politik wird. | [16] Dahinter steht die Überzeugung, dass erst in einem euro-

https://www.bitkom.org/Bitkom/Publikationen/Kriterien-zur-Identifikation-und-Auswahl-von-digitalen-Schluesseltechnologien.

| [12] Bundesministerium für Bildung und Forschung – BMBF (2021): Technologisch souverän die Zukunft gestalten. BMBF-Impulspapier zur technologischen Souveränität, Bonn/Berlin, S. 2 f, https://www.bmbf.de/SharedDocs/Publikationen/de/bmbf/5/24032_Impulspapier_zur_technologischen_Souveraenitaet.html.

| [13] Digitale Souveränität ist bspw. fester Bestandteil der Digitalstrategie der Bundesregierung. Der IT-Planungsrat unterhält eine gemeinsame Arbeitsgruppe von Bund und Ländern zu Cloud Computing und Digitaler Souveränität. Bund, Länder und Kommunen haben ein Zentrum für Digitale Souveränität der Öffentlichen Verwaltung (ZenDiS) ins Leben gerufen, https://www.cio.bund.de/Webs/CIO/DE/digitale-loesungen/digitale-souveraenitaet/digitale-souveraenitaet-node.html.

| [14] Pohle/Thiel (2019), a. a. O., S. 70 f.

| [15] Dazu grundlegend Gehring, P.: Datensouveränität versus Digitale Souveränität: Wegweiser aus dem konzeptionellen Durcheinander, in: Augsberg, St.; Gehring, P. (Hrsg.): Datensouveränität. Positionen zur Debatte, Frankfurt a. M. 2022, S. 19–44.

| [16] So war der Ausbau digitaler Souveränität sowohl im Rahmen der letzten deutschen als auch der französischen EU-Ratspräsidentschaft ein wesentliches Anliegen. Siehe hierzu bspw.: Berlin Declaration on Digital Society and Value-Based Digital Government at the ministerial meeting during the German Presidency of the

päischen Rahmen ein wirkmächtiges Gegengewicht zur technologischen und wirtschaftlichen Übermacht von Akteuren aus den USA und zunehmend auch aus China erreicht werden kann. |[17] Eine vollständige Unabhängigkeit im Sinne einer Autarkie in allen (Technologie-)Bereichen und ausschließlich im eigenen Land produzierter Lösungen ist dabei aber in aller Regel nicht intendiert. Vielmehr wird eine „goldene Mitte zwischen Fremdbestimmung und Autarkie“ |[18] angestrebt. Bisweilen wird damit auch die Überzeugung verbunden, dass sich die Mitgliedstaaten der Europäischen Union als eine Wertegemeinschaft liberaler Demokratien verstehen, die eigene Akzente in der Entwicklung und Nutzung digitaler Dienste setzen möchten. |[19]

Gleichrangig mit dem Souveränitätsgedanken richten sich politische Bestrebungen, den digitalen Raum zu gestalten, spätestens seit der COVID-19-Pandemie und dem russischen Angriff auf die Ukraine auf den **Bereich der Cybersicherheit**. |[20] Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat die Bedrohungslage für Deutschland in seinem letzten Lagebericht so hoch eingeschätzt wie noch nie. Demnach nimmt die Quantität und Qualität von Cyberangriffen kontinuierlich zu und trifft auf vielfach unzureichend gesicherte IT-Systeme. Ursprünge und Hintergründe solcher Attacken lassen sich immer häufiger nicht oder nur mit großem Aufwand und erheblicher Zeitverzögerung ermitteln. Neben dem Diebstahl von Daten und der (Industrie-)Spionage zielen diese Angriffe darauf, Rechenzeit und Bandbreiten für eigene Zwecke zu nutzen, Lösegeld zu erpressen oder auch die öffentliche Meinung zu beeinflussen. |[21]

Vielfach werden **digitale Souveränität und Cybersicherheit** in Strategie- und Positionspapieren zur Ausgestaltung des digitalen Raumes zusammen behandelt. So sehen etwa das ÖFIT, |[22] das Bundesministerium für Wirtschaft und Energie (nun-

Council of the European Union on 8 December 2020, https://digital-strategy.ec.europa.eu/en/news/berlin-declaration-digital-society-and-value-based-digital-government.

| 17 Besonders eindringlich: Fokusgruppe „Digitale Souveränität in einer vernetzten Gesellschaft“ (2018): Digitale Souveränität und Künstliche Intelligenz – Voraussetzungen, Verantwortlichkeiten und Handlungsempfehlungen, Digital Gipfel der Bundesregierung, Nürnberg 2018, S. 2, https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2018/p2-digitale-souveraenitaet-und-kuenstliche-intelligenz.pdf.

| 18 Pohle, J. (2021): Digitale Souveränität. Das Ringen um Handlungs- und Entscheidungsfreiheit im Netz, S. 7, in: WZB-Mitteilungen 171 (2021), S. 6–8.

| 19 Steiner, F.; Grzymek, V. (2020): Digitale Souveränität in der EU. Bertelsmann-Stiftung – Europäische Öffentliche Güter, Juli, https://www.bertelsmann-stiftung.de/de/publikationen/publikation/did/digitale-souveraenitaet-in-der-eu-all; Kagermann, H.; Wilhelm, U. (Hrsg.) (2020): European Public Sphere. Gestaltung der digitalen Souveränität Europas. acatech IMPULS, München.

| 20 Die Begriffe „Cybersicherheit“ und „IT-Sicherheit“ werden in diesem Dokument entsprechend gängiger Praxis (so bspw. auch vom Bundesamt für Sicherheit in der Informationstechnik - BSI) synonym verwendet.

| 21 Bundesamt für Sicherheit in der Informationstechnik (2022): Die Lage der IT-Sicherheit in Deutschland 2022, Bonn, S. 11 f., https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/Archiv-Lageberichte/archiv-lagebericht_node.html.

| 22 Goldacker, G. (2017): Digitale Souveränität. Diskussionspapier des Kompetenzzentrums Öffentliche IT, Berlin, S. 5.

mehr Bundesministerium für Wirtschaft und Klimaschutz) |[23] oder auch die Gesellschaft für Informatik |[24] Cybersicherheit als wesentlichen Teil und Grundvoraussetzung digitaler Souveränität an. Demnach werden die verschiedenen Dimensionen digitaler Souveränität durch einen systematischen Schutz gegen Fehlfunktionen und äußere Angriffe komplementiert. Bestrebungen zur Abgrenzung und Selbstbestimmung im internationalen Rahmen spielen hier ebenfalls eine Rolle. Denn die Sicherheit von IT-Infrastrukturen soll unter anderem dadurch gesteigert werden, sich unabhängiger von ausländischen – insbesondere chinesischen und US-amerikanischen – Technologie- und Dienstanbietern aufzustellen sowie die Förderung von inländischen bzw. europäischen Sicherheitslösungen voranzutreiben. |[25] Umgekehrt orientieren sich auch Strategiepapiere zur Ausgestaltung von Cybersicherheit am Ziel, digitale Souveränität zu stärken, allerdings zumeist ohne sich auch konzeptionell mit dieser Zielforderung auseinanderzusetzen. |[26]

A.II HERAUSFORDERUNGEN IN LEHRE, FORSCHUNG, ADMINISTRATION UND TRANSFER

Wissenschaftliches Arbeiten ist sowohl in Lehre, Forschung und Transfer als auch im Rahmen von Verwaltungs- und Managementtätigkeiten auf eine zuverlässige, leistungsfähige digitale Infrastruktur und auf hochwertige digitale Dienste, Plattformen und Werkzeuge angewiesen. Zugleich beeinflusst die Digitalisierung – je nach Disziplin in unterschiedlichem Ausmaß – die Art und Weise, wie Wissenschaft betrieben wird. Im Bereich der Lehre verändern virtuelle Kommunikationsumgebungen und der Einsatz digitaler Werkzeuge die Möglichkeiten und Formen der Wissensvermittlung. |[27] Und für die Forschung ermöglichen neue algorithmi-

| 23 Bundesministerium für Wirtschaft und Energie – BMWi (2021): Schwerpunktstudie Digitale Souveränität. Bestandsaufnahme und Handlungsfelder 2021, Berlin, S. 24, https://www.bundesregierung.de/breg-de/service/publikationen/schwerpunktstudie-digitale-souveraenitaet-1981176.

| 24 Krupka, D. (2020): Dimensionen digitaler Souveränität – Ein Überblick, in: Gesellschaft für Informatik: Schlüsselaspekte Digitaler Souveränität, Arbeitspapier, S. 4–7, https://gi.de/meldung/gi-veroeffentlicht-arbeitspapier-zu-schluesselaspekten-digitaler-souveraenitaet.

| 25 Pohle, J.; Thiel, Th. (2019): Digitale Vernetzung und Souveränität: Genealogie eines Spannungsverhältnisses, S. 70, in: Borucki, I.; Schünemann, W. (Hrsg.): Internet und Staat. Perspektiven auf eine komplizierte Beziehung, Baden-Baden, S. 57–80.

| 26 So etwa in der Cybersicherheitsstrategie für Deutschland des Bundesministeriums des Innern, für Bau und Heimat, in der die Stärkung digitaler Souveränität eine eigene Leitlinie bildet, Bundesministerium des Innern für Bau und Heimat (2021): Cybersicherheitsstrategie für Deutschland 2021, Berlin, S. 22–24, https://www.bmi.bund.de/SharedDocs/downlads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf.

| 27 Vor allem die COVID-19-Pandemie hat hier einen erheblichen Schub verursacht, siehe bspw. HRK - Hochschulrektorenkonferenz (2021): Momentum der Digitalisierung nutzen: Forderungen an Bund und Länder zur Weiterentwicklung der digitalen Lehrinfrastruktur. Entschließung des 148. Senats der HRK am 8. Juni 2021, Videokonferenz, https://www.hrk.de/positionen/beschluss/detail/forderungen-an-bund-und-laender-zur-weiterentwicklung-der-digitalen-lehrinfrastrukturen/. Zum Wandel der Lehre durch die digitale Transformation insgesamt: Wissenschaftsrat (2022): Empfehlungen zur Digitalisierung in Lehre und Studium, Köln, https://doi.org/10.57674/sg3e-wm53.

sche Methoden, einschließlich lernender Systeme, steigende Rechenkapazitäten sowie die Verfügbarkeit großer Datenmengen in digitaler Form die Bearbeitung neuer Fragestellungen, die innovative und gesellschaftlich bedeutende Erkenntnisse versprechen. |[28]

Diese Erweiterungen der Erkenntnis- und Vermittlungsmöglichkeiten bergen Chancen und Potenziale, erzeugen zugleich aber auch neue Herausforderungen und Probleme, die sich sowohl auf die wissenschaftliche Praxis als auch auf die Gestaltungsfreiheit von Wissenschaft insgesamt auswirken. Vier Zieldimensionen sind dabei besonders hervorzuheben, die je nach Funktionsbereich – Lehre, Forschung, Administration oder Transfer – unterschiedlich ausgeprägt sein können.

II.1 Zugänglichkeit, Portabilität und Interoperabilität

Die extremen Skaleneffekte, die es im digitalen Raum gibt, haben zu Abhängigkeiten von wenigen privatwirtschaftlichen Anbietern (so genannte „Hyperscaler“ |[29]) geführt, die nicht nur auf der Kostenseite, sondern auch hinsichtlich der Durchsetzbarkeit von Qualitätsstandards sowie der Portabilität und Interoperabilität |[30] von digitalen Objekten aller Art (Daten, Codes, Workflows) Fragen aufwerfen. Dies gilt etwa für Geschäftsmodelle, die auf einer zwingenden Verbindung von Hard- und Software basieren. Sie führen zu Herstellerabhängigkeiten, die die Auswahl einschränken, Schnittstellenprobleme verursachen und aufgrund eines Quasi-Monopols oft hohe Kosten für wissenschaftliche Einrichtungen nach sich ziehen.

Angesichts solcher **Pfad- und Systemabhängigkeiten, so genannte Lock-in-Effekte**, drohen beschaffungs- und vergaberechtliche Vorschriften ausgehebelt zu werden. Damit einher geht ein zunehmendes Machtgefälle bezüglich der Vertrags- und Lizenzkonditionen sowie hohe Folgekosten, die wissenschaftliche Einrichtungen vor erhebliche finanzielle Probleme stellen können. |[31] Besonders pro-

| 28 Siehe dazu ausführlich Deutsche Forschungsgemeinschaft (2020): Digitaler Wandel in den Wissenschaften. Impulspapier, Bonn, https://doi.org/10.5281/zenodo.4191345.

| 29 Mit dem Begriff werden gemeinhin die global agierenden Internetkonzerne beschrieben, die mit ihren breit skalierenden Produkten und Geschäftsmodellen (Stichwort: Plattformökonomie) eine solche Reichweite und Dominanz erreicht haben, dass sich oligopolartige Marktstrukturen herausgebildet haben. Aufgrund dieser Marktstellung verfügen sie über so große finanzielle Möglichkeiten und vor allem eine solche Menge an Daten, dass sie auch bei der Weiter- und Neuentwicklung digitaler Angebote (bspw. durch KI) erhebliche Wettbewerbsvorteile haben. Vgl. für eine kritische Einordnung bspw. Zuboff, Sh. (2019): The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power, New York.

| 30 Dies meint die Fähigkeit unterschiedlicher Systeme, Geräte, Anwendungen oder Produkte, sich miteinander zu verbinden und auf koordinierte Weise zu kommunizieren. Im Unterschied zur Kompatibilität ist hierfür in der Regel kein Zutun der Nutzerinnen und Nutzer erforderlich. Vgl. https://www.ias.uni-stuttgart.de/service/begriffslexikon/bedeutung-der-interoperabilitaet-fuer-das-internet-der-dinge/.

| 31 Krupka, D. (2020): Dimensionen digitaler Souveränität – Ein Überblick, S. 5 f., in: Gesellschaft für Informatik: Schlüsselaspekte Digitaler Souveränität, Arbeitspapier, S. 4–7, https://gi.de/meldung/gi-veroeffentlicht-arbeitspapier-zu-schluesselaspekten-digitaler-souveraenitaet. In diesem Zusammenhang hat die Europäische Organisation für Kernforschung (CERN) öffentlich gemacht, dass Preiserhöhungen und der Wegfall von

blematisch ist dies im administrativen Bereich, wo oft eine hohe Anzahl an Lizenzen für Standardanwendungen erforderlich ist, während wissenschaftliche Einrichtungen im Vergleich zu anderen Akteuren über keine große Markt- und Verhandlungsmacht verfügen.

Bei cloudbasierten digitalen Infrastrukturen und Diensten treten diese Herausforderungen in besonderem Maße zutage. Diese reichen von domänen- und fachspezifischen Services über die Bereitstellung externer Speicher- und Rechenkapazitäten bis hin zu Kollaborations- und Kommunikationsplattformen sowie Datenräumen und -infrastrukturen. |[32] Sie spielen mittlerweile eine entscheidende Rolle, um verteilte Ressourcen und Kompetenzen für die Wissenschaft zu organisieren, zu strukturieren und zu bündeln. Verschiedene Forschungsprozesse und -perspektiven sowie virtuelle Interaktionen in Lehre und Forschung werden dadurch erst ermöglicht.

Solche Dienste und Infrastrukturen werden vielfach von kommerziellen Anbietern zur Verfügung gestellt, wodurch sich Souveränitätsbeschränkungen ergeben. Denn es gibt nur sehr wenige privatwirtschaftliche Unternehmen, die Clouddienste oder digitale Werkzeuge zur Online-Kommunikation und zum kollaborativen Arbeiten in der erforderlichen Qualität und Funktionalität für eine Vielzahl unterschiedlicher Nutzerinnen und Nutzer bereitstellen können. Dadurch können diese Hyperscaler eine große Marktmacht entfalten und die Bedingungen für die Nutzung ihrer Produkte weitgehend frei diktieren. Sie fungieren dadurch als „De-facto-Regulierer“ |[33] – eine Marktsituation, die das Risiko **enormer finanzieller und struktureller Folgekosten für die Wissenschaft birgt**. Einzelne Bestrebungen, wie die vom Verein zur Förderung eines Deutschen Forschungsnetzes (DFN-Verein) bereitgestellten Rahmenverträge für Cloud- und Videokonferenzdienste, |[34] versprechen zwar leichte Verbesserungen, ändern aber wenig an den grundlegenden Markt- und Machtasymmetrien.

Zudem werden extern bereitgestellte Speicher- und Rechenkapazitäten zunehmend mit anbieterspezifischen Diensten zu einer gemeinsamen, hoch integrierten digitalen Infrastruktur verzahnt. Nutzerinnen und Nutzer – seien es einzelne Studierende und Forschende, wissenschaftliche Einrichtungen oder deutschlandweit agierende wissenschaftliche Organisationen – können die Gestaltung dieser anbieterbezogenen Ökosysteme kaum noch beeinflussen. Bereits bestehende Ab-

Sonderkonditionen sie dazu bewogen haben, alternative Lösungen zu suchen. Vgl. https://www.zdnet.de/88362307/preiserhoehung-cern-steigt-von-microsoft-anwendungen-auf-open-source-um/.

| 32 Hierzu ausführlich Konrad, U. et al. (2018): Digitale Dienste für die Wissenschaft – wohin geht die Reise? Positionspapier, hrsg. v. der Arbeitsgruppe Forschungssoftware im Rahmen der Schwerpunktinitiative Digitale Information der Allianz der deutschen Wissenschaftsorganisationen, http://doi.org/10.5281/zenodo.4301924.

| 33 Kagermann, H.; Streibich, K.-H.; Suder, K. (2021): Digitale Souveränität. Status quo und Handlungsfelder. acatech Impuls, München, S. 7.

| 34 Vgl. https://www.conf.dfn.de/.

hängigkeiten werden zur Alternativlosigkeit gesteigert, da Schnittstellenkompatibilität in der Regel nur innerhalb konzerneigener Produkte gewährleistet ist. |[35] Hierdurch können die Unternehmen mitbestimmen, mit welchen Mitteln Wissenschaft im digitalen Zeitalter betrieben wird.

Insbesondere die Forschung stellt dies vor erhebliche Herausforderungen. Denn hier wächst der Bedarf an höchst leistungsfähigen Speicher- und Rechenkapazitäten beständig. Dies betrifft sowohl einzelne Forschungsfelder und -methoden, wie etwa Anwendungen zur Künstlichen Intelligenz oder komplexe Simulationen, als auch die über alle Disziplinen hinweg bedeutsame Praxis, Forschungsdaten und -objekte digital zu teilen bzw. kollaborativ zu bearbeiten. Um dieser Nachfrage zu begegnen, werden bereits seit einigen Jahren die Kapazitäten im Bereich des Hoch- und Höchstleistungsrechnens ausgebaut. |[36] Und auch Speicherkapazitäten finden Forschende grundsätzlich bei wissenschaftlichen Rechenzentren. Gleichwohl nimmt die Nutzung von cloudbasierten Datenräumen und -infrastrukturen der großen kommerziellen Anbieter zu. Ein Grund ist ihr hoher Verbreitungsgrad, der neben dem internationalen Austausch auch Transferaktivitäten sowie andere Interaktionen mit Akteuren außerhalb der Wissenschaft erleichtert. Dadurch werden Forschungsdaten und -objekte in die Cloud-Ökosysteme der Hyperscaler verlagert, was Abhängigkeiten schafft und die Verfügungsmöglichkeiten über wesentliche Grundlagen der Forschung einschränkt. |[37] Nicht selten gelingt es den Anbietern, durch die Verknüpfung von Daten oder das Trainieren lernender Systeme einen zusätzlichen Mehrwert abzuschöpfen, woran die einzelnen Nutzenden sie angesichts der Markt- und Machtasymmetrien kaum hindern können.

| 35 Bundesministerium für Wirtschaft und Energie – BMWi (2021): Schwerpunktstudie Digitale Souveränität. Bestandsaufnahme und Handlungsfelder 2021, Berlin, S. 17, https://www.bundesregierung.de/breg-de/service/publikationen/schwerpunktstudie-digitale-souveraenitaet-1981176; hier wird u. a. auch auf die neuen Problemstellungen durch die Umstellung auf das Office-365-Cloud-Servicemodell von Microsoft verwiesen.

| 36 Hervorzuheben sind hier v. a. die drei nationalen Höchstleistungsrechenzentren in Deutschland sowie das Nationale Hochleistungsrechnen (NHR): das Jülich Supercomputing Center (JSC), das Leibniz-Rechenzentrum (LRZ) in Garching bei München, das Höchstleistungsrechenzentrum Stuttgart (HLRS) sowie die neun NHR-Zentren. Im Rahmen der Europäischen Partnerschaft zum High Performance Computing (EuroHPC) wird voraussichtlich im Jahr 2024 der erste europäische Exascale-Rechner in Jülich aufgebaut und der Aufbau eines Ökosystems für Quantencomputing vorangetrieben, so bspw. die Initiative „Munich Quantum Valley“, die mit fast 400 Mio. Euro gefördert wird. Dazu ausführlich Bundesministerium für Bildung und Forschung – BMBF (2021): Technologisch souverän die Zukunft gestalten. Impulspapier zur technologischen Souveränität, Bonn/Berlin. Einen Überblick zur Lage im Bereich Quantencomputer bietet Gumz, J. D. et al. (2022): Quanten-IKT – Quantencomputing und Quantenkommunikation. ÖFIT-Whitepaper, Januar, https://www.oeffentliche-it.de/publikationen?doc=232465&title=Quanten-IKT - Quantencomputing und Quantenkommunikation.

| 37 Zum gesamten Absatz siehe Vorstand der Zentren für Kommunikation und Informationsverarbeitung in Lehre und Forschung e. V. – ZKI (Hrsg.) (2022): Sicherstellung der digitalen Souveränität und Bildungsgerechtigkeit. Empfehlungen zur Ausgestaltung von Rahmenbedingungen für die Nutzung von Cloud-basierten Angeboten im Bildungsbereich, Berlin, S. 8, https://doi.org/10.5281/zenodo.7104141.

Bei Infrastrukturen und Diensten, die von Wissenschaftseinrichtungen |[38] und den dazugehörigen Rechenzentren selbst betrieben oder bereitgestellt werden, ergeben sich Souveränitätsbeschneidungen weniger durch Herstellerabhängigkeiten als durch eine **Begrenzung der Zugriffs- und Nutzungsmöglichkeiten**. Denn die Angebote sind vielfach stark fragmentiert, mitunter an bestimmte Konfigurationen oder die jeweilige Domain der Hochschule oder Forschungseinrichtung gebunden, oder sogar nur lokal verfügbar. |[39] Schnelles Hochskalieren ist im Rahmen öffentlicher Finanzierungsmodelle in der Regel nicht vorgesehen. Hinzu kommen Fragen der Qualität und Nutzerfreundlichkeit, die bei Infrastrukturen und Diensten, die vom akademischen Betrieb entwickelt, getragen und bereitgestellt werden, aufgrund begrenzter Ressourcen tendenziell weniger Aufmerksamkeit erfahren. |[40]

II.2 Nachvollziehbarkeit und Überprüfbarkeit

In dem Maße, in dem **wissenschaftliche Praxis** auf digitale Werkzeuge, Dienste und Infrastrukturen zurückgreift, wird sie mehr und mehr **durch digitale Rahmenbedingungen und Handlungslogiken geprägt**. Dadurch kann es zu Zielkonflikten mit bestimmten wissenschaftlichen Grundsätzen kommen. Dies gilt allen voran für die Leitprinzipien der Nachvollziehbarkeit und Überprüfbarkeit.

Besonders davon betroffen ist die Forschungspraxis. So kann es in bestimmten Forschungskontexten beispielsweise zum Problem werden, wenn der Quellcode eingesetzter Software nicht öffentlich zugänglich ist. Denn der Quellcode ermöglicht es, die verwendeten Algorithmen zu verifizieren. Sind diese Informationen für Forschende nicht zugänglich, sind Forschungsergebnisse nicht oder nur begrenzt nachzuvollziehen und einzuordnen. |[41]

Auch die digitale Ausgestaltung von Rechercheprozessen hat Folgen für den Erkenntnisprozess. Im Rahmen der hierbei eingesetzten Hilfsmittel bleibt vielfach unklar, wie Suchergebnisse zustande kommen bzw. durch welche Parameter sie beeinflusst werden. Damit ist nur schwer nachzuvollziehen, welchen Kriterien die notwendigerweise selektive Präsentation des Forschungsstandes folgt, bis hin zu einer möglichen Beeinflussung im Sinne von Anbieterinteressen. Hinzu kommt, dass Forschende eine Vielzahl von Nutzungsspuren hinterlassen, die

| 38 Der Begriff steht abkürzend für die Gesamtheit der Hochschulen und außerhochschulischen Forschungseinrichtungen im öffentlichen Sektor.

| 39 Vorstand der Zentren für Kommunikation und Informationsverarbeitung in Lehre und Forschung e. V. – ZKI (Hrsg.) (2022), a. a. O., S. 8.

| 40 Konrad, U. et al. (2018): Digitale Dienste für die Wissenschaft – wohin geht die Reise? Positionspapier, hrsg. v. der Arbeitsgruppe Forschungssoftware im Rahmen der Schwerpunktinitiative Digitale Information der Allianz der deutschen Wissenschaftsorganisationen, S. 16, http://doi.org/10.5281/zenodo.4301924.

| 41 Deutsche Forschungsgemeinschaft (2020): Digitaler Wandel in den Wissenschaften. Impulspapier, Bonn, S. 9 f., https://doi.org/10.5281/zenodo.4191345.

Rückschlüsse über ihr Verhalten im digitalen Raum zulassen. Dies eröffnet Digitalkonzernen grundsätzlich die Möglichkeit, durch das Sammeln und Auswerten dieser Daten zu steuern, welche Inhalte wem angezeigt werden, und insofern mittelbar den weiteren Forschungsprozess zu beeinflussen. Ebenso problematisch ist es, wenn Rechercheergebnisse durch vorherige Suchanfragen, den aktuellen Standort oder auch durch den Impact Factor bedingt werden, ohne dass dies unmittelbar ersichtlich ist. |[42]

Doch auch über den Forschungskontext hinaus wirken sich digitale Werkzeuge auf die Transparenz und die Möglichkeiten zur Überprüfbarkeit wissenschaftlichen Handelns aus. Hervorzuheben ist hier insbesondere der Einsatz von Large Language Models und anderen KI-gestützten Anwendungen. Befeuert durch die mediale Aufmerksamkeit um Chatbots wie „ChatGPT“ |[43] oder das Proteinstrukturvorhersageprogramm „AlphaFold“ |[44] hat bereits eine erste Auseinandersetzung damit eingesetzt, was diese Instrumente für Lehr-, Prüfungs- und Forschungspraktiken oder die Grundsätze guter wissenschaftlicher Praxis bedeuten. |[45] Doch stehen diese Anstrengungen erst am Anfang und viele Fragen, die den wissenschaftlichen Alltag unmittelbar betreffen, sind noch ungeklärt.

In einem wesentlich allgemeineren Sinne werden Nachvollziehbarkeit und Überprüfbarkeit ferner dadurch beeinträchtigt, dass beim Nutzen digitaler Dienste und Infrastrukturen vielfach nur schwer zu ergründen ist, welche und wie viele Daten mit oder ohne Personenbezug gespeichert, verarbeitet und genutzt werden. Diese **datenschutzrechtlichen Fragen** stellen sich in besonderer Weise, wenn es sich um Anbieter handelt, die ihren Hauptsitz außerhalb der Europäischen Union haben, was bei Clouddiensten sowie bei den in der Online-Lehre

| 42 Siems, R. (2022): Das Lesen der Anderen. Die Auswirkungen von User Tracking auf Bibliotheken, in: Das offene Bibliotheksjournal 9 (2022), Nr. 1, S. 1–25, https://doi.org/10.5282/o-bib/5797; Konrad, U. et al. (2018): Digitale Dienste für die Wissenschaft – wohin geht die Reise? Positionspapier, hrsg. v. der Arbeitsgruppe Forschungssoftware im Rahmen der Schwerpunktinitiative Digitale Information der Allianz der deutschen Wissenschaftsorganisationen, S. 17 f., http://doi.org/10.5281/zenodo.4301924.

| 43 Aus der Fülle an Beiträgen zu diesem Thema vgl. bspw. Himmelrath, A.; Quecke, F.: „Eine Renaissance des Mündlichen“, in: Der Spiegel vom 04.02.2023, S. 42–43; Schulz, W.; Fecher, B.: ChatGPT. Sind Maschinen die besseren Forscher?, in: Tagesspiegel vom 15.02.2023, S. 12; Thiel, Th.: Der neue Kollege. Künstliche Intelligenz und Autorenschaft, in: FAZ vom 01.02.2023, S. N4; Weßels, D. (2023): Meilenstein der KI-Entwicklung? Der Chatbot ChatGPT, in Forschung & Lehre 30, Nr. 1, S. 26–27.

| 44 Siehe etwa Callaway, E.: Das Proteinuniversum in einer Datenbank, in: Spektrum der Wissenschaft Nr. 31 vom 04.08.2022, https://www.spektrum.de/news/kuenstliche-intelligenz-das-proteinuniversum-in-einer-datenbank/2045533; Grolle, J. (2022): KI-System AlphaFold. Sollte diese Maschine den Nobelpreis bekommen?, in: Der Spiegel vom 04.10.2022; Meier, Ch.: Turbo für die Biologie. Eine Protein-Software gilt als Durchbruch des Jahres, in: Süddeutsche Zeitung vom 27.12.2021, S. 12.

| 45 Das Zentrum für Wissenschaftsdidaktik der Ruhr-Universität Bochum hat hierzu im Auftrag des Ministeriums für Kultur und Wissenschaft des Landes Nordrhein-Westfalen jüngst eine ausführliche Würdigung vorgelegt: Salden, P.; Leschke, J. (Hrsg.) (2023): Didaktische und rechtliche Perspektiven auf KI-gestütztes Schreiben in der Hochschulbildung (Zentrum für Wissenschaftsdidaktik der Ruhr-Universität Bochum), März 2023, https://doi.org/10.13154/294-9734. Hierzu außerdem: Fecher, B. et al. (2023): Delphi Study: Exploring the Implications of Large Language Models on the Science System, 6. Juni 2023, https://doi.org/10.5281/zenodo.8009429.

breit eingesetzten Kollaborations- und Kommunikationsplattformen die Regel ist. Alternativen, die ihre Server innerhalb der Europäischen Union betreiben, werden mittlerweile zwar von einigen Wissenschaftseinrichtungen gezielt gefördert. Ihre Verbreitung hält sich aber (noch) in Grenzen. |[46]

II.3 Dauerhaftigkeit und Verlässlichkeit

Mit den Leitprinzipien der Nachvollziehbarkeit und Überprüfbarkeit ist im wissenschaftlichen Kontext eine langfristige zeitliche Perspektive verbunden, um den Zugriff auf die Grundlagen und die Ergebnisse wissenschaftlichen Handelns möglichst dauerhaft abzusichern. Dieser Anspruch steht allerdings vielfach im Konflikt mit den vorherrschenden Funktionsmechanismen des digitalen Raumes, die sich – zumindest im kommerziellen Bereich – primär an Marktlogiken, der Konkurrenz innovativer Lösungen und damit einhergehenden Anpassungsnotwendigkeiten orientieren. Es muss auch immer damit gerechnet werden, dass Dienste oder ganze Unternehmen eingestellt werden, wenn sie nicht kostendeckend betrieben werden können. Dadurch ergeben sich für eine digitalisierte Wissenschaft diverse Herausforderungen, etwa mit Blick auf die dauerhafte Speicherung und Zugänglichkeit von Forschungsdaten und -ergebnissen oder auch beim Einsatz von wissenschaftsstützender Software. |[47]

Auch bei Infrastrukturen und Diensten, die vom akademischen Betrieb selbst entwickelt, getragen und bereitgestellt werden, sind Dauerhaftigkeit und Verlässlichkeit nicht garantiert – wenngleich aus anderen Gründen. Denn die überwiegende Zahl der wissenschaftseigenen Angebote wird in befristet finanzierten Projekten entwickelt, deren (dauerhafte) Fortführung vielfach nicht gesichert ist. Zudem besteht hier eine starke Abhängigkeit vom Engagement und institutionellen Verbleib einzelner Personen. Dadurch wird es erschwert, diese Eigenlösungen längerfristig in Betrieb zu halten, zu warten und fortwährend zu aktualisieren. |[48]

In abgeschwächter Form können diese Probleme auch bei digitalen Infrastrukturen und Diensten zum Tragen kommen, die Wissenschaftseinrichtungen über wissenschaftsbezogene Dienstleister, wie den DFN-Verein, die Hochschul-Informations-System eG (HIS eG) oder auch entsprechende Landesinitiativen, bereitgestellt werden. Zu nennen sind etwa Campus- und Learningmanagementsysteme, die als institutionenübergreifende Angebote grundsätzlich auf eine möglichst langfristige Verfügbarkeit ausgerichtet und mit entsprechenden Support-Struk-

| 46 Um Lehrenden und Studierenden eine Nutzung zu vereinfachen, setzten manche Hochschulen auf eine unmittelbare Anbindung an das Lehr- und Veranstaltungsmanagement.

| 47 Konrad, U. et al. (2018), a. a. O., S. 16.

| 48 Deutsche Forschungsgemeinschaft (2020): Digitaler Wandel in den Wissenschaften. Impulspapier, Bonn, S. 9, https://doi.org/10.5281/zenodo.4191345.

turen versehen sind. Angesichts begrenzter personeller und finanzieller Ressourcen vor Ort können sich aber auch hier Einschränkungen hinsichtlich Verlässlichkeit und dauerhaft abgesicherter Nutzbarkeit ergeben. |[49]

II.4 Sicherheit trotz Heterogenität und Offenheit

Hochschulen und Forschungseinrichtungen sind in der Regel offene und hoch durchlässige Organisationen. Zugleich verfügen sie über sensible, nicht selten personenbezogene Daten und wertvolles intellektuelles Eigentum. Deshalb bieten **Wissenschaftseinrichtungen eine besonders große Angriffsfläche für Cyberangriffe** unterschiedlichster Natur – sei es aus kriminellen Motiven oder aus Gründen der wirtschaftlichen oder politischen Spionage. |[50] In letzter Zeit wurden viele Cyberattacken auf Wissenschaftseinrichtungen bekannt, was die hohe Verwundbarkeit eindrücklich zeigt. |[51]

Außerdem erschwert es die für das wissenschaftliche Umfeld kennzeichnende Offenheit, Heterogenität und Freiheit, einrichtungsweit einheitliche Sicherheitsvorschriften zu erlassen und durchzusetzen. Sicherheit im digitalen Raum lässt sich für den wissenschaftlichen Sektor daher nicht primär als technische Herausforderung betrachten, sondern bedarf umfassender Gestaltung. Neben Cybersicherheitsvorkehrungen im engeren Sinne spielen Fragen der Compliance sowie adäquate Governancestrukturen und -prozesse eine noch gewichtigere Rolle als in anderen Wirtschafts- und Gesellschaftsbereichen. |[52]

Vor allem Hochschulen sind **dezentral geprägte Organisationen**. Neben der Zentralverwaltung sowie hochschulweiten digitalen Infrastrukturen und Diensten

| 49 Dies gilt besonders mit Blick auf mögliche Cyberattacken: So beklagen Studierende vielfach, dass sie in der Folge nicht mehr auf Lernmaterialien zugreifen können und auch die zuständigen Verwaltungen sehen sich teils nicht in der Lage, sich einen Überblick über erbrachte Studienleistungen zu verschaffen. Vgl. Fokken, S. (2023): Wenn ein Cyberangriff eine Hochschule ausknockt, in: Spiegel Online, 12.01.2023, https://www.spiegel.de/panorama/bildung/digitalisierung-wenn-ein-cyberangriff-eine-hochschule-ausknockt-a-0a81da2b-3e7f-465c-8066-7e53b8b40c08.

| 50 Dies hat auch die Europäische Kommission erkannt und Empfehlungen zum Umgang mit möglichen Sicherheitsrisiken durch ausländische Akteure aufgestellt, European Commission (ed.) (2022): Tackling R&I Foreign Interference. Staff Working Document, Januar 2022, https://data.europa.eu/doi/10.2777/513746.

| 51 Brandel, B.; Porombka, S.; Oevel, G. (2020): IT-Schutz ist kein Projekt, sondern ein Prozess. Cybersicherheit ist für Forschungseinrichtungen essenziell. Ein Überblick über die besonderen Herausforderungen für Hochschulen, S. 657, in: Forschung & Lehre 27 (2020) 8, S. 656–657, https://www.forschung-und-lehre.de/management/it-schutz-ist-kein-projekt-sondern-ein-prozess-3005. Zu den Wissenschaftseinrichtungen, die seit 2020 Angriffen ausgesetzt waren, zählen u. a. die Universitäten in Gießen, Bochum, Göttingen, Berlin (TU), Wuppertal und Duisburg-Essen als auch Hochschulen in Leipzig, Ansbach, Hamburg, Berlin sowie im westlichen Ruhrgebiet und im Harz, ebenso außerhochschulische Forschungseinrichtungen wie das Wissenschaftszentrum Berlin für Sozialforschung gGmbH (WZB), das Fraunhofer-Institut für Mikrostruktur von Werkstoffen und Systemen (IMWS) oder das Leibniz-Informationszentrum Wirtschaft (ZBW).

| 52 HRK – Hochschulrektorenkonferenz (2018): Informationssicherheit als strategische Aufgabe der Hochschulleitung. Empfehlung der 25. Mitgliederversammlung der HRK am 6. November 2018 in Lüneburg, https://www.hrk.de/positionen/beschluss/detail/informationssicherheit-als-strategische-aufgabe-der-hochschulleitung/; vgl. hierzu auch den Themenschwerpunkt Cybersicherheit in der Printausgabe von Forschung & Lehre vom August 2023, https://www.forschung-und-lehre.de/heftarchiv/ausgabe-8/23.

gibt es dort vielfältige ergänzende IT-Angebote, die primär in der Verantwortung von Fakultäten, Fachbereichen, Instituten oder einzelnen Professuren und Forschungsgruppen liegen. Auf dieser Ebene fehlt es jedoch vielfach an den Ressourcen und auch am Wissen, ausreichende Sicherheitsvorkehrungen zu ergreifen. So eröffnen sich Cyberkriminellen Möglichkeiten, in verhältnismäßig wenig geschützte Umgebungen einzudringen und ihre Angriffe anschließend über die Anbindung an das zentrale Hochschulnetz auf die gesamte Einrichtung auszuweiten. |[53]

Hinzu kommt, dass an Wissenschaftseinrichtungen der **Kreis der Nutzenden groß, heterogen und durch hohe Fluktuation geprägt** ist. Er reicht von Professorinnen und Professoren, Lehrbeauftragten und Postdocs, über Promovierende und Studierende unterschiedlichster Disziplinen bis hin zu Verwaltungsangehörigen. Das bedeutet eine große Bandbreite an Digitalkompetenzen und ein ebenso uneinheitliches Bewusstsein für Sicherheitsrisiken. In Forschung und Transfer spielen zudem Kooperationen eine große Rolle – sowohl mit Forschenden anderer Wissenschaftseinrichtungen aus dem In- und Ausland als auch mit Akteuren außerhalb der Wissenschaft. Mit diesen Partnern werden nicht nur Nachrichten ausgetauscht, sondern digitale Dienste und Daten gemeinsam genutzt. Dadurch eröffnen sich potenzielle Einfallstore und Sicherheitsvorkehrungen gestalten sich insgesamt schwieriger; zugleich haben diese Partner – seien es Unternehmen oder staatliche Einrichtungen – vielfach eigene (Sicherheits-)Standards, die im Rahmen von Kooperationen zu beachten und mit den eigenen Regeln in Einklang zu bringen sind. Die IT-Sicherheitsarchitekturen und -konzepte von Hochschulen und Forschungseinrichtungen müssen dieser Offenheit nach außen Rechnung tragen.

Im Bereich der Forschung ergeben sich weitere Sicherheitsrisiken dadurch, dass manche Forschungsprozesse auf sehr kostspielige Großgeräte angewiesen sind, deren Laufzeiten den immer schneller werdenden Rhythmus des digitalen Fortschritts (weit) überschreiten. In dieser Konstellation kommt es vor, dass Forschungsgeräte aufgrund ihres Alters nur mit veralteten Computern, Betriebssystemen und Software betrieben werden können. Spätestens wenn hierfür durch die Hersteller keine Updates mehr zur Verfügung gestellt werden, bergen diese Systeme erhebliche Risiken, die im Falle einer Anbindung an die internen Netz- und Serverstrukturen für die gesamte Wissenschaftseinrichtung zur Bedrohung werden können.

Trotz dieser besonderen Bedrohungslage **sind viele Hochschulen und teilweise auch Forschungseinrichtungen in Deutschland nicht ausreichend gegen Cyber-**

| [53] Shulman, H.; Waidner, M. (2023): Forschung muss besser geschützt werden. IT-Sicherheit an Hochschulen und Forschungseinrichtungen, S. 186, in: Forschung & Lehre 30 , Nr. 3, S. 184–186, https://www.forschung-und-lehre.de/management/forschung-muss-besser-geschuetzt-werden-5449.

angriffe sowie Sabotage- oder Spionageversuche geschützt. |[54] Vor allem im hochschulischen Bereich sind die Sicherheitsniveaus sehr unterschiedlich ausgeprägt und variieren nicht zuletzt in Abhängigkeit von der Größe der Einrichtung. Ursächlich hierfür scheinen weniger fehlende Empfehlungen zur Ausgestaltung von Cybersicherheitsvorkehrungen im Wissenschaftsbereich zu sein als ein Mangel an Fachpersonal, finanzieller Ausstattung und Bedeutung des Themas in der Governance. |[55] Viele Hochschulen und bisweilen auch Forschungseinrichtungen haben im Rahmen ihrer Haushalte keine eigenen Budgets für Cyber- bzw. Informationssicherheit eingestellt. Die allgemeinen IT-Mittel reichen häufig nicht aus, um den finanziellen Aufwand für Vorkehrungen zu decken, die neuesten technischen Anforderungen entsprechen, oder Mitarbeiterinnen und Mitarbeiter fortlaufend für Gefahrenquellen zu sensibilisieren und zu schulen. |[56]

| 54 Siehe für die Lage an Hochschulen ausführlich das Themenheft „Cybersicherheit an Hochschulen“ von Forschung & Lehre 27 (2020) 8, https://www.forschung-und-lehre.de/heftarchiv/ausgabe-8/20.

| 55 Kebschull, U.; Pordesch, U. (2020): Wie IT-Sicherheit an Hochschulen gelingt, 30.11.2020, https://www.forschung-und-lehre.de/management/wie-it-sicherheit-an-hochschulen-gelingt-3292/; Schmermund, K. (2019): „Uns fehlen Geräte und Personal“. Wie gut sind Hochschulen gegen Cyberangriffe gerüstet? Ein Gespräch mit Professor Manfred Paul vom Arbeitskreis Informationssicherheit des ZKI, 20.12.2019, https://www.forschung-und-lehre.de/management/uns-fehlen-geraete-und-personal-2389/.

| 56 Brandel, B.; Porombka, S.; Oevel, G. (2020): IT-Schutz ist kein Projekt, sondern ein Prozess. Cybersicherheit ist für Forschungseinrichtungen essenziell. Ein Überblick über die besonderen Herausforderungen für Hochschulen, S. 657, in: Forschung & Lehre 27 (2020) 8, S. 656–657, https://www.forschung-und-lehre.de/management/it-schutz-ist-kein-projekt-sondern-ein-prozess-3005.

B. Handlungsdimensionen

In Teil A wurde dargelegt, weshalb die zunehmende Bedeutung digitaler Werkzeuge die digitale Souveränität und Sicherheit der Wissenschaft in den Fokus rückt. Es muss sichergestellt werden, dass **Forschende, Lehrende und Wissenschaftseinrichtungen im digitalen Raum** über **genügend Kontrolle, Selbstbestimmung und Handlungsfreiheit** verfügen. Andernfalls drohen wesentliche Rahmenbedingungen und Grundprinzipien wissenschaftlichen und wissenschaftsnahen Arbeitens in Gefahr zu geraten. Bereits in seinem Positionspapier „Impulse aus der COVID-19-Krise für die Weiterentwicklung des Wissenschaftssystems in Deutschland“ hat der Wissenschaftsrat betont, wie wichtig Souveränität und Sicherheit im digitalen Raum sind, wenn ein resilientes Wissenschaftssystem sichergestellt werden soll. Hier seien „erhebliche Kraftanstrengungen und ein ausdauernd hoher Einsatz an personellen und finanziellen Ressourcen erforderlich“, die über die genuine Sphäre der Wissenschaft und die nationale Ebene hinausreichen müssen. | [57]

Im selben Positionspapier hat der Wissenschaftsrat mit digitaler Souveränität nicht nur eine negative, auf Abwehr und Unabhängigkeit ausgerichtete Funktion verbunden, sondern auch einen positiven Anspruch: „Souveränität umfasst nicht allein die Unabhängigkeit von etablierten Akteuren auf dem Markt, sondern zielt auch auf eine an den eigenen Zielen orientierte, autonome Gestaltung des digitalen Raums.“ Die Akteure des Wissenschaftssystems forderte er auf, den digitalen Raum aktiv mitzugestalten und die sich eröffnenden Potenziale gewinnbringend zu nutzen. Davon könnten auch andere gesellschaftliche Bereiche profitieren und Innovationen ermöglicht werden. | [58]

Daran anknüpfend werden im Folgenden Handlungsdimensionen identifiziert, die es aus Sicht des Wissenschaftsrats zu adressieren gilt, um diese Ziele erreichen und somit die Souveränität und Sicherheit der Wissenschaft im digitalen Raum insgesamt steigern zu können.

| 57 Wissenschaftsrat (2021): Impulse aus der COVID-19-Krise für die Weiterentwicklung des Wissenschaftssystems in Deutschland | Positionspapier, Köln, S. 43 f., https://www.wissenschaftsrat.de/download/2021/8834-21.html.

| 58 Ebd., S. 47 f.

Einschränkungen und Risiken für die digitale Souveränität und Sicherheit von Wissenschaft kann nur dann wirksam begegnet werden, wenn diese Ziele in der **strategischen Ausrichtung und Steuerung von Wissenschaftseinrichtungen** eine größere Rolle spielen. Die digitale Transformation von Lehre, Forschung, Administration und Transfer muss konsequenter und umfassender, als dies bisher der Fall ist, als wichtiges Handlungs- und Aufgabenfeld in Strategieprozessen verankert |[59] und in Governancestrukturen abgebildet werden.

In den letzten Jahren sind bereits wichtige Schritte in diese Richtung unternommen worden, wie etwa die zunehmende Verbreitung des Modells eines Chief Information Officer (CIO) zeigt. Gleichwohl ist das Bild insgesamt sehr heterogen und für den Bereich der Cybersicherheit sind vergleichbare Strukturen weit weniger verbreitet. |[60] Handlungsfähige Steuerungsmechanismen für IT-Prozesse im Allgemeinen wie auch für Fragen der Cybersicherheit im Speziellen sind jedoch unverzichtbar, damit Wissenschaftseinrichtungen den digitalen Raum für sich möglichst sicher und souverän ausgestalten können. Aus Sicht des Wissenschaftsrats wäre es kurzsichtig und fahrlässig, an dieser Stelle die eigene Handlungsfähigkeit zu kompromittieren, weil der Einsatz der notwendigen Ressourcen gescheut wird.

Digitalstrategien und die damit verbundenen Governancestrukturen stärken Wissenschaftseinrichtungen darin, die Chancen und Herausforderungen der digitalen Transformation ihres Aufgaben- und Leistungsspektrums planvoll und zielgerichtet zu adressieren. |[61] Wie sehr Sicherheit und Souveränität dadurch gestärkt werden, hängt jedoch davon ab, inwieweit sich diese Regelungs- und Lenkungsbestrebungen auch im operativen Geschäft von Hochschulen und Forschungseinrichtungen bewähren können. Dies wird durch die individuellen Bedingungen vor Ort beeinflusst. Dennoch lassen sich allgemeine Faktoren benennen, die sich in dieser Hinsicht positiv auswirken können. Hierzu zählt, relevante Akteure und Funktionsgruppen in Strategiebildungs- und Entscheidungsprozesse einzubeziehen, um sachgerechte IT-bezogene Vorgaben und Richtlinien auf allen Organisations- und Funktionsebenen zu entwickeln sowie zu ihrer Akzeptanz und damit zur Durchsetzbarkeit beizutragen. Dies gilt besonders für Regelungen zur

| 59 Mit Blick auf Lehre und Studium hat der Wissenschaftsrat dies bereits ähnlich für die Hochschulen gefordert: Wissenschaftsrat (2022): Empfehlungen zur Digitalisierung in Lehre und Studium, Köln, https://doi.org/10.57674/sg3e-wm53.

| 60 Einen Überblick über die verschiedenen Modelle, die an Hochschulen und Forschungseinrichtungen zur IT-Governance zum Einsatz kommen, bietet eine aktuelle Umfrage des ZKI-Arbeitskreises Strategie und Organisation, vgl. Dreyer, M. (2023): Ergebnisse der ZKI Top Trends-Umfrage des ZKI-Arbeitskreises Strategie und Organisation für das Jahr 2023, S. 10–13, https://doi.org/10.5281/zenodo.7599852.

| 61 Darin ist sich die Vielzahl der Empfehlungen zu den Herausforderungen, vor die Wissenschaftseinrichtungen durch die zunehmende Digitalisierung von Forschung, Lehre und Administration gestellt werden, weitgehend einig. Siehe die Papiere vom Centrum für Hochschulentwicklung (CHE), vom Stifterverband für die deutsche Wissenschaft oder auch vom Hochschulforum Digitalisierung.

Cybersicherheit, deren Ziele nur erreicht werden können, wenn alle Angehörige einer Hochschule oder Forschungseinrichtung mitwirken.

Vor allem in der IT-Governance von Hochschulen sollte es zudem Raum für mögliche Sonderregelungen geben, um neben den übergeordneten Zielsetzungen für die Gesamtinstitution auch die Besonderheiten einzelner Fachkulturen und ihrer Netzwerke berücksichtigen zu können. Allgemeiner gesprochen bedeutet das: die IT-Strategien und -Richtlinien von Wissenschaftseinrichtungen flexibel zu gestalten, ohne dabei die übergeordnete Zielsetzung aus den Augen zu verlieren, durch mehr Kohärenz und Kontrolle den digitalen Wissenschaftsbetrieb aktiver und damit auch souveräner und sicherer gestalten zu können.

Ein weiteres Hemmnis für (mehr) Souveränität und Sicherheit im Wissenschaftsbereich ist der **ungenügende Einsatz von Ressourcen für den Betrieb und die Absicherung leistungsstarker und zeitgemäßer IT-Infrastrukturen**. Vielfach ist eine personelle und finanzielle Unterversorgung der zuständigen Organisationseinheiten festzustellen, die durch die im Wissenschaftsbetrieb vorherrschende hohe Personalfluktuation und die in den Finanzierungsmechanismen wurzelnde Dominanz von Projektstrukturen verschärft wird. |[62] Mittel- bis längerfristige Planungshorizonte, die essenziell sind, um den digitalen Wissenschaftsbetrieb aufrechtzuerhalten und zukunftsgerichtet weiterzuentwickeln, lassen sich dadurch kaum gewährleisten. Angesichts der zunehmenden Bedeutung des Digitalen für die wissenschaftliche Arbeit droht der Wissenschaftsstandort Deutschland damit insgesamt an Innovations- und Wettbewerbsfähigkeit einzubüßen.

Neben einer auskömmlichen und dauerhaften Finanzierung sowie einer angemessenen Priorisierung innerhalb der Einrichtungen ist es erforderlich, dass Hochschulen und Forschungseinrichtungen im IT-Bereich auf eine breite Kompetenzbasis zurückgreifen können – sowohl auf Entscheidungs- als auch auf Handlungsebene. Dies ist vielfach nicht oder nur eingeschränkt der Fall, da Stellen fehlen oder qualifizierte IT-Fachkräfte nicht im notwendigen Umfang gewonnen und längerfristig gehalten werden können. Ein wesentlicher Grund für die Schwierigkeiten, Personen mit entsprechender Expertise zu rekrutieren, besteht in der mangelnden Konkurrenzfähigkeit des wissenschaftlichen Sektors gegenüber den Verdienstmöglichkeiten in der freien Wirtschaft. Zudem senken die vielfach hohe Befristungsquote, mangelnde Personalentwicklungskonzepte und das Fehlen längerfristiger Perspektiven die Attraktivität einer Beschäftigung in wissenschaftlichen Einrichtungen. |[63]

| 62 Für eine breitere Einordnung siehe: Wissenschaftsrat (2023): Strukturen der Forschungsfinanzierung an deutschen Hochschulen | Positionspapier, Köln, DOI: https://doi.org/10.57674/pms3-pr05.

| 63 Hierzu ausführlich HIS-Institut für Hochschulentwicklung – HIS-HE (2019): Digitalisierung der Hochschulen. Ergebnisse einer Schwerpunktstudie für die Expertenkommission Forschung und Innovation (Studien zum deutschen Innovationssystem, Nr. 14-2019), Februar 2019, S. 106–120, https://medien.his-he.de/publikationen/detail/digitalisierung-der-hochschulen.

Weil nahezu alle Arbeitsabläufe innerhalb der Wissenschaft heute digitale Komponenten nutzen, ist es zudem unumgänglich, dass auch jenseits des genuinen IT-Personals Digitalkompetenzen vorhanden sind. Dies betrifft Wissenschaftlerinnen und Wissenschaftler ebenso wie Management und Administration. Dabei kann Art und Ausmaß der erforderlichen digitalen Expertise zwar je nach Tätigkeit und Fachdisziplin variieren, sodass einheitliche Aussagen kaum möglich sind. |[64] Dennoch gilt: Je ausgeprägter und aktueller die digitalen Handlungs- und Entscheidungskompetenzen |[65] in Lehre, Forschung, Administration und Transfer, desto größer sind die Chancen, die digitale Souveränität und Sicherheit der Wissenschaft insgesamt zu steigern.

B.II KOOPERATION IM MEHREBENENSYSTEM

Kooperation und Vernetzung können dazu beitragen, die Handlungsfähigkeit, Selbstbestimmtheit und Sicherheit von Wissenschaft im digitalen Raum zu steigern. **Synergie- und Skaleneffekte** führen zu einem effizienteren Einsatz personeller, finanzieller wie auch materieller Ressourcen und **wirken sich positiv auf den digitalen Wissenschaftsbetrieb aus**. Solche Effekte lassen sich innerhalb der einzelnen Einrichtungen, in begrenzten Partnerschaften oder auch im gesamten Wissenschaftssystem erzielen. Daher sind Netzwerk- und Verbundstrukturen ein probates Mittel, um auch unter finanziell und personell limitierten Bedingungen sicherzustellen, dass den partizipierenden Einrichtungen – unabhängig von ihrer Größe, finanziellen Ausstattung oder fachlichen Schwerpunktsetzung – qualitativ hochwertige und ausreichend abgesicherte digitale Dienste und Infrastrukturen zur Verfügung stehen.

Vor allem im Bereich **genuiner Wissenschaftsdienste sowie bei besonders kosten- und pflegeintensiven digitalen Infrastrukturen** werden diese Positiveffekte bereits genutzt. Zu nennen sind allen voran die Aktivitäten des DFN-Vereins, der mit dem deutschen Forschungs- bzw. Wissenschaftsnetz nicht nur eine zentrale Kommunikationsinfrastruktur für die Wissenschaft betreibt, sondern auch eine stetig wachsende Zahl an digitalen Diensten zur Verfügung stellt. Infolge der Erfahrungen aus der COVID-19-Krise wurde das Angebotsportfolio noch-

| 64 Deutsche Forschungsgemeinschaft (2020): Digitaler Wandel in den Wissenschaften. Impulspapier, Bonn, S. 5, https://doi.org/10.5281/zenodo.4191345; KMK – Kultusministerkonferenz (2019): Empfehlungen zur Digitalisierung in der Hochschullehre (Beschluss der Kultusministerkonferenz vom 14.03.2019), Bonn/Berlin, https://www.kmk.org/aktuelles/artikelansicht/digitalisierung-empfehlungen-fuer-hochschulen-entwickelt.html.

| 65 Dies meint u. a. den verantwortungsvollen, sicheren und reflektierten Einsatz digitaler Technologien, die Fähigkeit, Potenzial und Vertrauenswürdigkeit von digitalen Komponenten verstehen, beurteilen und prüfen zu können, sowie das Vermögen, technologische Abhängigkeiten erkennen und reduzieren zu können. Vgl. Bundesministerium für Wirtschaft und Energie – BMWi (2021): Schwerpunktstudie Digitale Souveränität. Bestandsaufnahme und Handlungsfelder 2021, Berlin, S. 31, https://www.bundesregierung.de/breg-de/service/publikationen/schwerpunktstudie-digitale-souveraenitaet-1981176.

mals deutlich ausgeweitet, sodass wissenschaftliche Akteure über den DFN-Verein mittlerweile neben einer Authentifizierungs- und Autorisierungsinfrastruktur unter anderem auch Sicherheits- und Kollaborationsdienste nutzen können. |[66]

Mit der HIS eG existiert ein zentraler Dienstleister für Softwarelösungen, die speziell auf die Bedürfnisse von Hochschuladministrationen zugeschnitten sind. Anwendungsfelder sind beispielsweise das Management von Prüfungen und Lehrveranstaltungen oder die digitale Abwicklung der Studienplatzvergabe und Studierendenverwaltung. |[67] Auch im Bereich des High Performance Computing haben sich Bund und Länder dazu entschieden, über den Verbund für Nationales Hochleistungsrechnen |[68] sowie das Gauss Centre for Supercomputing (GCS) |[69] national koordinierte Infrastrukturangebote inklusive entsprechender Beratungs- und Schulungsmöglichkeiten einzurichten. Hinzu kommen diverse Kooperationsmodelle, die für Forschung und Lehre regional oder auf Ebene der Bundesländer digitale Dienstleistungen und Infrastrukturen bündeln. |[70]

Während somit bei wissenschaftsspezifischen Angeboten bereits umfassend kooperiert wird, ist dies im Bereich **generischer Soft- und Hardware sowie entsprechender Dienst- und Cloudangebote** weit weniger der Fall. |[71] Im Bereich der außerhochschulischen Forschungseinrichtungen gibt es zwar, insbesondere bei den Trägerorganisationen, bereits Bestrebungen, auch hier eine stärkere Bündelung vorzunehmen bzw. vermehrt gemeinsam zu agieren. |[72] Darüber hinaus existieren aber kaum übergreifende Strukturen, obwohl die Abhängigkeiten gegenüber den wenigen Hyperscalern, die diese für den digitalen Wissenschafts-

| 66 Hervorzuheben ist neben den Angeboten der DFN-Cloud u. a. der Identity and Access Management Dienst (IAM), der im Rahmen der NFDI-Basisdienste entwickelt und über den DFN-Verein zugänglich gemacht wird. Einen aktuellen Überblick bietet die Internetpräsenz des DFN-Vereins: https://www.dfn.de/dienste/.

| 67 Zu den Dienstleistungen der HIS eG siehe: https://www.his.de/loesungen.

| 68 Zu Auftrag, Struktur und Zielen des NHR-Verbunds ausführlich: https://www.nhr-verein.de/unser-auftrag.

| 69 Das GCS dient dem Zusammenschluss der drei nationalen Höchstleistungsrechenzentren in Deutschland (JSC, LRZ, HLRS) und soll sowohl die Bereitstellung von Supercomputing-Ressourcen als auch die Weiterentwicklung des wissenschaftlichen Höchstleistungsrechnens fördern, https://www.gauss-centre.eu/about-us.

| 70 So bspw. die Gesellschaft für wissenschaftliche Datenverarbeitung (GWDG) in Göttingen, die zugleich Hochschulrechenzentrum für die Georg-August-Universität Göttingen sowie Rechen- und IT-Kompetenzzentrum für die Max-Planck-Gesellschaft ist, das Leibniz-Rechenzentrum in Garching, das seine Dienste sowohl den Münchner Universitäten als auch der Bayerischen Akademie der Wissenschaften zur Verfügung stellt, oder die diversen Landesinitiativen, die darauf zielen, Kompetenzen und Ressourcen für die Digitalisierung der Hochschulen zu bündeln und besser zu koordinieren.

| 71 Für die Hochschulen des Bundeslandes Hamburg hat dies auch der dortige Rechnungshof bemängelt und zu einem Ausbau der Kooperation im IT-Bereich aufgerufen. Vgl. Rechnungshof Freie und Hansestadt Hamburg (Hrsg.) (2023): Jahresbericht 2023 über die Prüfung der Haushalts- und Wirtschaftsführung der Freien und Hansestadt Hamburg einschließlich der Haushalts- und Konzernrechnung 2021, Hamburg, S. 224.

| 72 Beispielsweise werden bei der Fraunhofer-Gesellschaft die IT für die Verwaltung und gewisse Infrastrukturservices gemeinsam beschafft und gemanagt. Ähnliche Strukturen finden sich auch bei der Max-Planck-Gesellschaft und der Helmholtz-Gemeinschaft. Bei der Leibniz-Gemeinschaft existiert ein Kompetenzcenter, über das u. a. gemeinsame Rahmenverträge genutzt werden können.

betrieb essenziellen Dienstleistungen und Produkte bereitstellen, besonders stark ausgeprägt sind.

Dass es auch hier möglich ist, durch gemeinsames Handeln Vorteile zu erzielen, zeigt ein Blick ins europäische Ausland. So ist etwa das Joint Information Systems Committee (Jisc) als gemeinsame Einrichtung des britischen Hochschulsektors neben dem Betrieb gemeinsamer digitaler Infrastrukturen und Dienste unter anderem damit betraut, Rahmenverträge mit externen IT-Anbietern auszuhandeln, sodass alle angeschlossenen Einrichtungen von den gleichen Lizenzbedingungen profitieren können. |[73] Ein ähnliches Modell existiert in den Niederlanden. Dort haben sich mehr als 100 Wissenschaftseinrichtungen im kooperativen Interessenverband SURF zusammengeschlossen. Dieser Verband tritt als zentraler IT-Dienstleister für alle beteiligten Institutionen auf und übernimmt in diesem Rahmen unter anderem die Beschaffung und Bereitstellung diverser Standardanwendungen und breit einsetzbarer IT-Services von Privatanbietern. |[74]

Neben Vorteilen durch einen verbesserten Ressourceneinsatz innerhalb des Wissenschaftssystems selbst versprechen Vernetzungs- und Kollaborationsmodelle eine gestärkte Position im Umgang mit Souveränitäts- und Sicherheitsherausforderungen von außen. Wie neben den Aktivitäten von SURF und Jisc auch die Bestrebungen der Bundesressorts zur Etablierung einer gemeinsamen IT-Beschaffungs- und Lizenzmanagementstrategie |[75] zeigen, kann der Zusammenschluss zahlreicher Einzelakteure zu einem größeren und einheitlich agierenden Konglomerat die Verhandlungsposition gegenüber den marktbeherrschenden Digitaldienstleistern verbessern. Wegen des verhältnismäßig kleinen Marktanteils der Wissenschaft ist zwar nicht davon auszugehen, dass durch ein solches Vorgehen die Machtasymmetrien bezüglich Kostengestaltung und Nutzungsbedingungen gänzlich abgebaut werden können. Dennoch lässt sich eine Stärkung der eigenen Akteursqualität und somit zumindest eine Verringerung der bestehenden Abhängigkeiten erwarten.

Im deutschen Wissenschaftssystem müssen Kooperation und Vernetzung unter **Berücksichtigung der föderalen Ordnung** geplant und umgesetzt werden, die sowohl in organisatorischer als auch in finanzieller Hinsicht wesentliche Rahmenbedingungen für Aufbau, Betrieb und Pflege digitaler Infrastrukturen und Dienste vorgibt. Länderübergreifende Kooperationen bleiben jedoch ebenso sinnvoll wie (gesamt-)europäische Lösungen, um von größeren Skaleneffekten profitieren zu können. Sicherheits- und Souveränitätsziele stehen insofern in einem Spannungsverhältnis zum Prinzip der Subsidiarität, das es abzuwägen gilt.

| 73 Als Betreiber des „National research and education network“ (NREN) stellt Jisc zugleich das britische Äquivalent zum DFN-Verein dar, https://www.jisc.ac.uk/about.

| 74 Zum Aufbau und Leistungsspektrum des niederländischen Modells: https://www.surf.nl/en/about-surf.

| 75 Neben den Einrichtungen des Bundes können auch Landeseinrichtungen von den ausgehandelten Sonderkonditionen profitieren, vgl.: https://www.cio.bund.de/Webs/CIO/DE/digitale-loesungen/it-beschaffung/lizenzmanagement-bund/lizenzmanagement-bund-node.html.

Zugleich verlangt auch der wissenschaftliche Wettbewerb eine Abwägung von Kooperation und Konkurrenz. So können beispielsweise besonders elaborierte digitale Angebote und Technologien sowie die damit einhergehende Expertise als Mittel der Distinktion und inhaltlichen Profilbildung dienen, um die besten Köpfe an einen Wissenschaftsstandort zu locken oder Fördermittel einzuwerben. Sind gemeinsame Angebote zu anspruchslos oder unflexibel, besteht daher die Gefahr, dass diese berechtigten Eigeninteressen und damit auch die Akzeptanz für kooperative Praktiken untergraben werden. Als weiteres Hemmnis für den gemeinsamen Aufbau und Betrieb digitaler Dienstleistungen benennen Vertreter wissenschaftlicher Einrichtungen zudem das Auslaufen der Sonderregelungen zum Umsatzsteuerrecht, da dadurch der Leistungsaustausch zwischen Wissenschaftseinrichtungen steuerpflichtig zu werden droht. |[76]

B.III AUSWAHL- UND GESTALTUNGSMÖGLICHKEITEN

Die im Teil A beschriebenen Asymmetrien und Abhängigkeiten im Verhältnis zu den marktbeherrschenden Digitaldienstleistern ergeben sich unter anderem dadurch, dass diese von Skaleneffekten massiv profitieren, weshalb für Alternativen, die hinsichtlich Leistungsspektrum, Qualität und Sicherheit konkurrenzfähig wären, nahezu unüberwindbare Markteintrittsschwellen bestehen. Die Folgen dieser Marktdominanz betreffen nicht nur den wissenschaftlichen Sektor, sondern stellen grundsätzlich alle Wirtschafts-, Gesellschafts- und Politikbereiche vor ähnliche Herausforderungen.

Vor diesem Hintergrund gibt es bereits seit einiger Zeit Bestrebungen, diese Vormachtstellungen zu reduzieren bzw. auf eine angepasste Ausgestaltung des Angebotsportfolios der dominanten Dienstleister hinzuwirken. Dazu zählen allen voran **regulatorische Maßnahmen, die darauf zielen,** Standards bezüglich Offenheit, Portabilität und Interoperabilität einzufordern und bestehende Marktverzerrungen zu entschärfen. |[77]

Derartige Regulierungsbemühungen werden auch auf nationaler Ebene vorangetrieben, den entscheidenden Bezugsrahmen bildet jedoch die Europäische Uni-

|[76] Hierzu ausführlich HIS-Institut für Hochschulentwicklung – HIS-HE (2019): Digitalisierung der Hochschulen. Ergebnisse einer Schwerpunktstudie für die Expertenkommission Forschung und Innovation (Studien zum deutschen Innovationssystem, Nr. 14-2019), Februar 2019, S. 134–138, https://medien.his-he.de/publikationen/detail/digitalisierung-der-hochschulen. Die bis Ende des Jahres 2024 geltende Sonderregelung sollte dringend genutzt werden, um eine dauerhafte Lösung zu finden, die Kooperationen im Wissenschaftssystem nicht zusätzlich erschwert; vgl. Wissenschaftsrat (2023): Strukturen der Forschungsfinanzierung an deutschen Hochschulen | Positionspapier, Köln, S. 38, DOI: https://doi.org/10.57674/pms3-pr05.

|[77] Wie etwa ein Recht zum Wechsel von Cloudanbietern, das die Durchsetzung interoperabler Standards voraussetzen würde. Entsprechende Überlegungen finden sich in der Datenstrategie der Bundesregierung von 2021: Bundeskanzleramt (Hrsg.) (2021): Datenstrategie der Bundesregierung. Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum, Kabinettfassung, 27. Januar 2021, Berlin, S. 26, https://www.bundesregierung.de/breg-de/service/publikationen/datenstrategie-der-bundesregierung-1845632.

on. Die Bedeutung, die dieser Aspekt in der digitalpolitischen Agenda der EU mittlerweile eingenommen hat, lässt sich daran erkennen, dass die Schlagzahl entsprechender Vorstöße in den letzten Jahren deutlich zugenommen hat. Zu nennen sind etwa der Data Act und der Data Governance Act, die Rahmenbedingungen für die Nutzung, Weitergabe und den Zugang von Daten festlegen, oder auch der Digital Markets Act und der Digital Services Act, mit denen große Online-Dienste und -Plattformen stärker reguliert werden sollen. |[78] Wesentliche Zielsetzungen sind, Marktmachtmissbrauch und Datenmonopole zu verhindern und das Entstehen alternativer Lösungen in der EU und unter Berücksichtigung europäischer Sicherheits- und Wertvorstellungen zu fördern. |[79] Solche Regulierungsbemühungen überschreiten zwar den genuinen Bereich der Wissenschaftspolitik, entfalten aber wissenschaftspolitische Wirkungen, da sie Einfluss darauf haben, unter welchen Bedingungen Wissenschaft im digitalen Zeitalter agiert.

Eine weitere Möglichkeit, um die Handlungs- und Wahlmöglichkeiten für wissenschaftliche Akteure zu erhöhen, besteht darin, die Voraussetzungen für eine wettbewerbsfördernde **Angebotsvielfalt** insgesamt zu verbessern. Ergänzend zu ordnungspolitischen Instrumenten, die beispielsweise auf eine Senkung von Markteintrittsschwellen zielen, ist hier insbesondere an eine gezielte Förderung kleiner, wissenschaftsnaher Unternehmen zu denken, die mit ihren Angeboten zu einem offeneren Markt und bei entsprechender Ausgestaltung auch zu weiteren Souveränitätsgewinnen für ihre Nutzerinnen und Nutzer beitragen können.

Neben Maßnahmen zur Förderung kommerzieller Alternativangebote hat in den letzten Jahren ferner der Auf- und Ausbau **öffentlich finanzierter Infrastruktur- und Plattformprojekte** an Bedeutung gewonnen. Entsprechende Bestrebungen werden auf nationaler und europäischer Ebene vor allem für die Vernetzung sowie die ortsunabhängige Zugänglichkeit und Verfügbarkeit von digitalen Objekten vorangetrieben. Auf Basis von Open Source und gemeinsam definierten Standards streben diese Projekte danach, den Anforderungen an Datensicherheit und -hoheit, Interoperabilität, Transparenz sowie Dauerhaftigkeit und Verlässlichkeit der Zugriffsmöglichkeiten gerecht zu werden.

Für den wissenschaftlichen Bereich sind derzeit einige Initiativen besonders relevant: die Nationale Forschungsdateninfrastruktur (NFDI), die wissenschaftliche Datenbestände für das gesamte deutsche Wissenschaftssystem systematisch erschließen, vernetzen und nutzbar machen soll; die European Open Science Cloud (EOSC), mit der die Europäische Kommission europäischen Wissenschaftle-

| 78 Vgl. hierzu u. a. https://www.heise.de/news/Digital-Paket-EU-Staaten-wollen-Amazon-Google-Co-an-die-Leine-legen-6276706.html sowie https://www.euractiv.com/section/digital/news/data-governance-new-eu-law-for-data-sharing-adopted/.

| 79 Krupka, D. (2020): Dimensionen digitaler Souveränität – Ein Überblick, in: Gesellschaft für Informatik: Schlüsselaspekte Digitaler Souveränität, Arbeitspapier, S. 4–7, hier: S. 7, https://gi.de/meldung/gi-veroeffentlicht-arbeitspapier-zu-schluesselaspekten-digitaler-souveraenitaet.

rinnen und Wissenschaftlern den Zugang zu wissenschaftlichen Daten, Datenverarbeitungsplattformen sowie Dienstleistungen für die Datenverarbeitung erleichtern möchte; und Gaia-X, welches das Ziel verfolgt, eine Open-Source-basierte Referenzarchitektur für die verteilten Infrastrukturen wirtschaftlicher und anderer Akteure bereitzustellen. | [80]

Trotz der diskutierten Optionen und Bemühungen zur Förderung einer größeren Angebotsvielfalt werden die digitalen Infrastrukturen und Dienste der Hyperscaler jedoch auch in Zukunft von großer Bedeutung für den Wissenschaftsbetrieb bleiben. Denn ihre Angebote werden – gerade im Cloud-Bereich und bei kollaborativen Kommunikationsinstrumenten – häufig Vorteile bezüglich Qualität, Funktionalität, Usability und Sicherheitsstandards haben. Die enormen Skaleneffekte, die hohe Zahl der Nutzenden sowie die zur Verfügung stehenden Ressourcen eröffnen ganz andere Möglichkeiten als sie bei Angeboten bestehen, die primär einen wissenschaftlichen Nutzerkreis adressieren oder gerade erst auf den Markt drängen. Der hohe Verbreitungsgrad wirkt sich zudem positiv auf die Anschlussfähigkeit aus, die im wissenschaftlichen Kontext für Transferprozesse sowie für Kooperationen mit externen Partnern aus dem In- und Ausland sehr relevant ist.

Vor diesem Hintergrund sind für die Wissenschaft Marktverhältnisse anzustreben, die im Rahmen des geltenden Wettbewerbsrechts ein **Nebeneinander** verschiedener **kommerzieller und öffentlich finanzierter digitaler Infrastrukturen und Dienste** ermöglichen. Auf diese Weise können die jeweiligen Vor- und Nachteile gegeneinander aufgewogen und zugleich die Chancen erhöht werden, die Abhängigkeiten von wenigen marktbeherrschenden Anbietern zu reduzieren. | [81]

Ein weiterer Grund für die Abhängigkeiten, die sich im Hinblick auf kommerzielle Angebote der dominierenden Digitaldienstleister ergeben, besteht darin, dass Einfluss-, Kontroll- und Gestaltungsmöglichkeiten auf Anwenderseite stark limitiert sind. Auch Open-Source-Anwendungen werden teilweise kommerziell betrieben. Der wesentliche Unterschied besteht jedoch darin, dass der gesamte

| 80 Einen fundierten Überblick über die verschiedenen Projekte bietet RfII – Rat für Informationsinfrastrukturen (2023): Föderierte Dateninfrastrukturen für die wissenschaftliche Nutzung. NFDI, EOSC und Gaia-X: Vergleich und Anregungen für eine engagierte Mitgestaltung des Ausbaus und der Weiterentwicklung (RfII-Berichte, Nr. 4), Göttingen, https://rfii.de/?p=8533.

| 81 Wissenschaftsrat (2021): Impulse aus der COVID-19-Krise für die Weiterentwicklung des Wissenschaftssystems in Deutschland | Positionspapier, Köln, S. 45 f., https://www.wissenschaftsrat.de/download/2021/8834-21.html; bezogen auf Sicherheitsfragen empfiehlt auch das BSI eine Kombination verschiedener Anbieter(typen), um Risiken zu streuen und dadurch besser kalkulieren zu können, vgl. Bundesamt für Sicherheit in der Informationstechnik – BSI (2022): Die Lage der IT-Sicherheit in Deutschland 2022, Bonn, S. 78, https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/Archiv-Lageberichte/archiv-lagebericht_node.html.

Quellcode öffentlich zugänglich sowie grundsätzlich für jeden nutz- und gestaltbar ist. Eine Monopolisierung ist daher nicht gegeben. |[82]

Angesichts dieser Gestaltungsprinzipien gelten **Open-Source-Lösungen** als besonders geeignet, um die Souveränität der Nutzenden zu unterstützen. Quelloffene Ansätze bilden deshalb einen festen Bestandteil der Digitalstrategie der Bundesregierung und sollen gezielt von ihr gefördert werden, um Gegengewichte zu „monolithischen" Hard- und Softwareökosystemen großer Hersteller zu etablieren. |[83] In Kombination mit offenen Standards soll Open Source perspektivisch gar zum Standard in der öffentlichen Verwaltung und bei öffentlichen Entwicklungsaufträgen werden. |[84] Ähnliche Überlegungen für digitale Projekte in öffentlicher Trägerschaft finden sich auf EU-Ebene. |[85]

Für die Wissenschaft bieten Open-Source-Anwendungen weitere Vorteile, die über eine Reduktion von Abhängigkeiten hinausgehen. So trägt die Transparenz, die durch die Möglichkeit geschaffen wird, den Quellcode einzusehen, dazu bei, die Nachvollziehbarkeit und Reproduzierbarkeit von Forschungsergebnissen, die unter Einsatz digitaler Werkzeuge erzeugt wurden, zu gewährleisten. Da Open-Source-Anwendungen grundsätzlich für eine Weiterentwicklung und Anpassung offenstehen, bieten sie zudem den Vorteil, auf dieser Grundlage wissenschaftseigene Lösungen leichter und angesichts fehlender oder allenfalls geringer Lizenzkosten kostengünstiger entwickeln zu können. Mit Blick auf die Vielzahl hochspezialisierter Anwendungsfelder, für die Angebote auf dem freien Markt vielfach gar nicht existieren, ist dies vor allem für den Forschungskontext ein nicht zu unterschätzender Faktor. |[86]

Gleichwohl bringt der Rückgriff auf Open-Source-Lösungen im Vergleich zu konventionellen Angeboten, deren Codes nicht offen zugänglich sind, auch Nachtei-

| 82 Gleichwohl können auch auf Grundlage von Open Source geschlossene „Silos" einzelner Hersteller entstehen, die Nutzerinnen und Nutzer wiederum an die jeweiligen Ökosysteme binden. Vgl. O'Neil, M. et al. (2022): Open Source! Der Kampf um freie Software, in: Le Monde Diplomatique 01/2022.

| 83 Bundesministerium für Digitales und Verkehr: https://digitalstrategie-deutschland.de/; so auch Bundesministerium für Bildung und Forschung – BMBF (2021): Technologisch souverän die Zukunft gestalten. BMBF-Impulspapier zur technologischen Souveränität, Bonn/Berlin, S. 13, https://www.bmbf.de/SharedDocs/Publikationen/de/bmbf/5/24032_Impulspapier_zur_technologischen_Souveraenitaet.html.

| 84 Sozialdemokratische Partei Deutschlands (SPD), Bündnis 90/Die Grünen, Freie Demokratische Partei (FDP) (Hrsg.) (2021): Mehr Fortschritt wagen. Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit. Koalitionsvertrag 2021–2025 zwischen der Sozialdemokratischen Partei Deutschlands (SPD), Bündnis 90/Die Grünen und den Freien Demokraten, Berlin, https://www.bundesregierung.de/breg-de/service/gesetzesvorhaben/koalitionsvertrag-2021-1990800, S. 15.

| 85 Berlin Declaration on Digital Society and Value-Based Digital Government, 2020, https://digital-strategy.ec.europa.eu/en/news/berlin-declaration-digital-society-and-value-based-digital-government.

| 86 In diesem Sinne hat sich der Wissenschaftsrat bereits mehrfach geäußert: Wissenschaftsrat (2021): Impulse aus der COVID-19-Krise für die Weiterentwicklung des Wissenschaftssystems in Deutschland | Positionspapier, Köln, S. 46, https://www.wissenschaftsrat.de/download/2021/8834-21.html; Wissenschaftsrat (2020): Perspektiven der Informatik in Deutschland, Köln, S. 60, https://www.wissenschaftsrat.de/download/2020/8675-20.html.

le mit sich, die die Einsatzmöglichkeiten in der Wissenschaft begrenzen. Dazu zählt, dass der Betreuungsaufwand höher ist, da notwendige Wartungsarbeiten und Sicherheitsüberprüfungen in größerem Umfang selbst übernommen werden müssen. Mit Blick auf die angespannte Ressourcensituation und die Schwierigkeiten, ausreichend qualifiziertes Fachpersonal zu gewinnen, bedeutet dies zusätzliche Belastungen, die nicht nur bei kleineren Wissenschaftseinrichtungen zu Einbußen bezüglich Funktionalität und Sicherheit führen können. Damit eng verbunden sind Fragen bezüglich der dauerhaften Verfügbarkeit und der Regelung von Verantwortlichkeiten, die sich aufgrund der verbreiteten Projektstrukturen und der hohen Personalfluktuation im wissenschaftlichen Kontext auf besondere Weise stellen. |[87]

B.IV SENSIBILISIERUNG UND REFLEXIONSFÄHIGKEIT

Wer digitale Werkzeuge souverän und sicher nutzen will, muss eine Vielzahl an technischen, sozialen und ökonomischen Faktoren kennen und beachten, die die Handlungsspielräume einschränken können. Wie in den vorherigen Abschnitten ausgeführt, ist ein solches Problembewusstsein in Teilen der Wissenschaft noch schwach ausgeprägt. Dies hängt mit der Offenheit und Vielfalt des wissenschaftlichen Umfeldes zusammen, ist aber auch dadurch bedingt, dass die Auswirkungen der digitalen Transformation auf den Wissenschaftsbetrieb in ihrer Vielschichtigkeit und Komplexität erst allmählich sichtbar werden.

Abhilfe kann hier eine breiter angelegte **Sensibilisierung für die spezifischen Voraussetzungen und Herausforderungen einer digitalisierten Wissenschaft** schaffen. Neben der Vermittlung grundlegender Handlungs- und Entscheidungskompetenzen für das wissenschaftliche Arbeiten im digitalen Raum ist deshalb die Förderung kritischer Reflexionsfähigkeiten im Umgang mit digitalen Technologien von zentraler Bedeutung. Dies beinhaltet, dass sich wissenschaftliche Akteure – von Studierenden über Forschende und Lehrende bis hin zu Verwaltungsangehörigen und Einrichtungsleitungen – stärker damit auseinandersetzen, in welchem Ausmaß ihr Handeln, einschließlich ihrer Erkenntnisprozesse, durch technische Erfordernisse und Standards sowie Abhängigkeiten von bestimmten Digitaldienstleistern und den von ihnen bereitgestellten Infrastrukturen und Services geprägt ist. Auch die unterschiedlichen Handlungslogiken wissenschaftlicher, unternehmerischer und staatlicher Akteure, die zu widerstreitenden Interessen führen können, müssen im Zuge dessen reflektiert werden.

Größerer Aufmerksamkeit bedürfen auch die spezifischen Risiken, die mit einer digitalisierten Wissenschaft einhergehen. Neben dem akuten Bedrohungspotenzial durch Cyberattacken und einer erhöhten Vulnerabilität gegenüber techni-

| 87 Maurer, W.; Scherzinger, St. (2021): Digitale Forschungswerkzeuge. Nachhaltigkeit für Software und Daten, in: Forschung & Lehre, H. 10, S. 816–817.

schen Ausfallrisiken umfasst dies etwa unerwünschte Nebeneffekte beim Einsatz digitaler Werkzeuge – Stichwort: Tracking – oder auch Unwägbarkeiten bei der Kooperation mit externen Partnern. Vor allem beim Teilen und gemeinsamen Nutzen von digitalen Objekten ergeben sich verschiedene Herausforderungen, die bisher oft noch zu wenig bedacht werden. Zu denken ist unter anderem an eine mögliche Preisgabe von Forschungsdaten in nicht kontrollierbaren digitalen Umgebungen, an die Nutzung von Soft- und Hardware, die unter Sicherheits- und Datenschutzgesichtspunkten zu beanstanden ist, oder auch an etwaige Einfallstore für Wissenschaftsspionage, gerade wenn es sich um Kooperationspartner aus autoritären Staaten handelt. Die zunehmenden geopolitischen Spannungen, die sich auch auf die internationale Wissenschaftskooperation auswirken, verstärken dieses Gefahrenpotenzial zusätzlich und rücken Fragen bezüglich wirtschaftlicher und technologischer Abhängigkeiten weiter in den Fokus.

Die Förderung kritischer Reflexionsfähigkeiten bedeutet nicht nur, derartigen Risiken und Problembereichen Aufmerksamkeit zu schenken, sondern auch die **Chancen und Möglichkeiten in den Blick zu nehmen, die für die Wissenschaft bestehen**, um einen größeren Beitrag zur Stärkung von digitaler Souveränität und Sicherheit (auch in anderen Wirtschafts- und Gesellschaftsbereichen) leisten zu können. Dies gilt sowohl mit Blick auf Schlüsseltechnologien als auch hinsichtlich der (Weiter-)Entwicklungen von digitalen Infrastrukturen, Anwendungen und Diensten im Allgemeinen. In politischen Strategiepapieren spielt diese Funktion der Wissenschaft als technologischer Vorreiter und Innovationstreiber eine bedeutende Rolle; |[88] doch können die damit in Aussicht gestellten Zielsetzungen nur erreicht werden, wenn diese Zusammenhänge auch innerhalb der wissenschaftlichen Einrichtungen und Disziplinen selbst ausreichend Beachtung erfahren.

| 88 So bspw. Open Source Business Alliance – Bundesverband für digitale Souveränität e. V. (Hrsg.) (2021): Manifest für digitale Souveränität, 09. Dezember 2021, S. 4 f., https://osb-alliance.de/publikationen/veroeffentlichungen/manifest-fuer-digitale-souveraenitaet; Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen (2019): Strategie für das digitale Nordrhein-Westfalen 2019, Düsseldorf, insb. S. 45–49, https://broschuerenservice.wirtschaft.nrw/mwike/shop/Strategie_für_das_digitale_Nordrhein-Westfalen_Fortschrittsbericht/5#image-0; Bundesministerium für Bildung und Forschung – BMBF (2019): Digitale Zukunft: Lernen. Forschen. Wissen. Digitalstrategie des BMBF, Berlin, S. 31–35, https://www.bildung-forschung.digital/digitalezukunft/de/unsere-ueberzeugungen/digitalstrategie-des-bmbf/die-digitalstrategie-des-bmbf/die-digitalstrategie-des-bmbf.html.

C. Empfehlungen

C.I DIGITALE SELBSTBEFÄHIGUNG VON WISSENSCHAFTSEINRICHTUNGEN

I.1 Strategien und Governancestrukturen für die digitale Wissenschaft

Strategie und Governance von Wissenschaftseinrichtungen sind zentral für ihre Fähigkeit, mit den beschriebenen Chancen und Herausforderungen im digitalen Raum umzugehen. Wesentliche Zielsetzung ist dabei, Strategieprozesse und Steuerungsmechanismen derart weiterzuentwickeln, dass sie Hochschulen, Forschungseinrichtungen und die darin tätigen Personen befähigen, den digitalen Raum selbstbestimmt, sicher und an den eigenen Zielen orientiert gestalten zu können.

Ein entscheidender Schritt in diese Richtung besteht darin, auf Einrichtungsebene Governancestrukturen zu etablieren, die die Verantwortung für die digitalen Voraussetzungen des Wissenschaftsbetriebs klar bestimmen. Die Einrichtungen gewinnen dadurch sowohl in der strategischen als auch in der operativen Steuerung IT-bezogener Prozesse an Handlungs- und Kontrollfähigkeit. Angesichts der Bedeutung für die Funktionsfähigkeit nahezu aller Abläufe in Forschung, Lehre und Administration spricht sich der Wissenschaftsrat dafür aus, diese **Steuerungsaufgaben auf Leitungsebene zu verankern und in speziellen Funktionseinheiten abzubilden**.

Das Modell des Chief Information Officer, das bereits in verschiedenen Einrichtungen zur Anwendung kommt, |[89] erscheint in dieser Hinsicht besonders geeignet und sollte daher möglichst flächendeckend etabliert werden. Dabei kommt es weniger darauf an, in welcher konkreten Form dies vor Ort ausgestaltet wird, als dass es sich tatsächlich um ein zentrales Leitungsorgan handelt, bei dem sämtliche IT-bezogenen Prozesse über alle Organisations- und Funktionsebenen hinweg zusammenlaufen. Der Bereich der Cybersicherheit sollte allerdings hiervon ausgenommen sein. Denn Sicherheitsinteressen können anderen Zielen, die bei der Ausgestaltung der IT-Architektur einer Einrichtung angestrebt werden, entgegenlaufen. Diese Zielkonflikte sollten in einer Einrichtung transparent ge-

| 89 Einen Überblick bietet Dreyer, M. (2023): ZKI Top Trends-Umfrage des ZKI-Arbeitskreises Strategie und Organisation für das Jahr 2023 (Version 1), S. 10–13, https://doi.org/10.5281/zenodo.7599852.

macht und offen ausgehandelt werden. Daher ist grundsätzlich zu empfehlen, diese inhaltliche Trennung auch durch Schaffung einer separaten Organisationseinheit zu vollziehen, die je nach Größe der Einrichtung mit eigenen Ressourcen und Kompetenzen auszustatten ist (vgl. C.II). |[90]

Angesichts der Heterogenität der Wissenschaftslandschaft können zur Ausgestaltung dieser Steuerungseinheiten nur einige Grundsätze aufgestellt werden: Hierzu zählt eine dem breiten Aufgabenspektrum entsprechende personelle und finanzielle Ausstattung, die es ermöglicht, den jeweiligen Anliegen sowohl innerhalb der Leitungsgremien als auch auf den darunterliegenden Organisationseinheiten ausreichend Gehör und Beachtung zu verschaffen. Damit geht einher, dass CIOs, IT-Sicherheitsbeauftragte oder ähnliche Organe von den Einrichtungsleitungen in relevante Entscheidungsprozesse eingebunden und mit den notwendigen Kompetenzen, Rechten und Entscheidungsbefugnissen ausgestattet werden, um die gewünschten, einrichtungsweiten Steuerungs- und Kontrolleffekte auch in der Praxis erreichen zu können. Mit Blick auf Akzeptanz und Compliance ist es zudem notwendig, Strukturen und Prozesse dafür zu schaffen, dass Akteure und Funktionsgruppen aller Ebenen ihre Anliegen und Bedarfe geltend machen können.

Darüber hinaus ermöglichen es solche Governancestrukturen, Fragen der **digitalen Souveränität und Sicherheit auch in Strategie- und Planungsprozessen von Wissenschaftseinrichtungen mehr Beachtung** zu verschaffen. Denn durch die Anbindung an die Leitungsebene können die Herausforderungen einer zunehmend digitalen Wissenschaft unmittelbar in Entscheidungen zur zukünftigen Ausrichtung der jeweiligen Hochschule oder Forschungseinrichtung einbezogen werden. Dies umfasst sowohl strategische Perspektiven für die Ausgestaltung und Weiterentwicklung der einrichtungsinternen IT-Architektur – wie etwa Entscheidungen zum Aufbau eigener Rechen- und Speicherkapazitäten, zur Lizensierung bestimmter Software und Cloudangebote oder zur Wahl eines Identitätsmanagementdienstes – als auch finanzielle und personelle Ressourcen, derer es bedarf, um einen handlungsfähigen, ausreichend abgesicherten und qualitativ hochwertigen IT-Betrieb realisieren zu können. |[91]

| 90 Für eine entsprechende Verantwortungsbündelung auf Leitungsebene hat sich auch die HRK ausgesprochen und neben der Etablierung von Governancestrukturen insbesondere zur strategischen Positionierung angemahnt, HRK – Hochschulrektorenkonferenz (2018): Informationssicherheit als strategische Aufgabe der Hochschulleitung. Empfehlung der 25. Mitgliederversammlung der HRK am 6. November 2018 in Lüneburg, https://www.hrk.de/positionen/beschluss/detail/informationssicherheit-als-strategische-aufgabe-der-hochschulleitung/.

| 91 Aufgrund der komplexen Organisationsstrukturen und Zuständigkeitsregelungen zeigt sich vor allem für Hochschulen, dass bereits die Bezifferung eines Gesamtbudgets für IT-Dienstleistungen und -Infrastrukturen erhebliche Schwierigkeiten mit sich bringt, vgl. HIS-Institut für Hochschulentwicklung – HIS-HE (2019): Digitalisierung der Hochschulen. Ergebnisse einer Schwerpunktstudie für die Expertenkommission Forschung und Innovation (Studien zum deutschen Innovationssystem, Nr. 14-2019), Februar 2019, S. 100, https://medien.his-he.de/publikationen/detail/digitalisierung-der-hochschulen.

Neben solchen strategischen Prozessen sind die IT-Verantwortlichen von Wissenschaftseinrichtungen zudem gefordert, Souveränitäts- und Sicherheitskriterien in ihren eigenen Entscheidungs- und Planungsprozessen zu beachten. Hierfür ist es unter anderem sinnvoll, einen Katalog mit Grundanforderungen zu formulieren, der zur Überprüfung und Weiterentwicklung der bestehenden IT-Infrastruktur herangezogen werden kann. Darin ließen sich beispielsweise Vorgaben zur Zugänglichkeit und zum Schutz von Daten, zu offenen Schnittstellen und Standards oder auch zu Identitätsmanagement und Authentifizierungsmethoden aufstellen. Orientierungspunkte bieten etwa der von SURF entwickelte „Values Compass“ oder das ebenfalls in den Niederlanden angesiedelte „Trust Framework“. | [92] Auch die von der Datenschutzkonferenz aufgestellten „Kriterien für Souveräne Clouds“ | [93] können hier herangezogen werden. Ergänzend gilt es, sowohl bei bereits genutzten als auch bei neuen Diensten und Infrastrukturen stets die Frage nach möglichen Alternativen zu stellen, um sich strategisch breiter aufstellen, Lock-in-Effekte vermeiden und etwaige Rückfalloptionen einbeziehen zu können.

Ein wertvolles Hilfsmittel stellt zudem die Erarbeitung und Pflege eines Datenkatalogs dar. Dieser dient insbesondere dazu, einen Überblick über die in einer Einrichtung vorhandenen Daten zu gewinnen, Zuständigkeits-, Zugriffs- und Nutzungsrechte festzuhalten sowie zu regeln, unter welchen Umständen Daten mit welchem Personenkreis geteilt werden dürfen. Dadurch lassen sich nicht nur die Handlungs- und Entscheidungsfähigkeiten von IT-Verantwortlichen (nach innen und außen) stärken, sondern auch eine rechtssichere Handhabung von Daten fördern. Mit Blick auf mögliche Sicherheitsvorfälle bietet der Rückgriff auf einen Datenkatalog außerdem den Vorteil, rasch einen Überblick gewinnen und dementsprechend steuernd eingreifen zu können.

Für die innerhalb von Fakultäten, Instituten oder Forschungseinrichtungen gelebte IT-Praxis ist darüber hinaus dazu zu raten, Souveränitäts- und Sicherheitsüberlegungen in interne Steuerungsinstrumente einzubeziehen. Dies umfasst vor allem Schulungen, Richtlinien, Handreichungen und Verhaltenskodizes, mit deren Hilfe auf dezentraler und individueller Ebene Einfluss auf die Auswahl und Nutzung digitaler Infrastrukturen und Dienste genommen werden kann. Dabei ist es erforderlich, nach den jeweiligen Adressaten und Anwendungsfeldern zu differenzieren, um unterschiedliche Anforderungen an Freiheitsgrade oder die Schutzbedürftigkeit und Sensibilität von Daten sowie disziplinäre Besonderheiten berücksichtigen zu können.

| 92 Vgl. https://www.surf.nl/en/about-surf/value-compass-supports-discussion-on-public-values-in-digital-transformation und https://trustframework.io/.

| 93 Datenschutzkonferenz – DSK: Kriterien für Souveräne Clouds. Positionspapier der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 11. Mai 2023, https://www.datenschutzkonferenz-online.de/weitere_dokumente.html.

Für die digitale Selbstbefähigung von Wissenschaftseinrichtungen ist es wichtig, die verfügbaren personellen Ressourcen und die damit einhergehende Kompetenzbasis zu stärken. Dafür müssen Personalstrukturen so gestaltet werden, dass sie es erlauben, den gegenwärtigen und absehbar weiter steigenden Bedarf für die Planung, Betreuung und Absicherung der eigenen IT-Infrastruktur abzudecken, und zugleich eine **weitere Professionalisierung der Aufgabenwahrnehmung im IT-Bereich** befördern. Dies gilt sowohl für die operative als auch die strategische Ebene. Lehr- und Forschungstätigkeiten auf der einen sowie IT-Zuständigkeiten auf der anderen Seite sollten möglichst klar getrennt werden. Dass IT-Aufgaben als Zusatzaufgabe neben einer primär wissenschaftlichen Tätigkeit übernommen werden, kann zwar je nach Disziplin und Kontext im Einzelfall zweckdienlich sein; vor allem für Leitungsfunktionen ist diese Praxis allerdings problematisch, steht einer Professionalisierung entgegen und kann Interessenkonflikte erzeugen. Dies wird weder der zunehmenden Bedrohungslage durch Cyberattacken noch der essenziellen Bedeutung gerecht, die hochwertige digitale Dienste und Infrastrukturen für den Wissenschaftsbetrieb haben.

Es stellt Wissenschaftseinrichtungen vor erhebliche Probleme, trotz der starken Konkurrenz die nötige Anzahl gut ausgebildeter Fachkräfte zu gewinnen und langfristig zu binden. Zu den Möglichkeiten, die ihnen offenstehen, zählt, das in der Wissenschaft vorhandene Potenzial an qualifizierten Personen besser für sich zu nutzen. Vor allem für Hochschulen ist es lohnend, Strategien zu entwickeln, um entsprechend qualifizierte Absolventinnen und Absolventen für eine Tätigkeit in den hochschuleigenen IT-Abteilungen zu gewinnen und sich auch jenseits der klassischen Wissenschaftsberufe als attraktiver Arbeitgeber zu präsentieren. Im Rahmen des Personalmanagements empfiehlt sich zudem, Fort- und Weiterbildungen einzusetzen, um das bereits vorhandene administrative und wissenschaftliche Personal entsprechend der Bedarfe im IT-Bereich weiterzuentwickeln und derart zusätzliche Karriereperspektiven zu eröffnen.

Für Bereiche wie IT-Administration und Support hat man in den Leitungsebenen von Wissenschaftseinrichtungen bereits erkannt, dass die Förderung der eigenen **(beruflichen) Ausbildungstätigkeit** ein probates Mittel darstellt, um den Personalbedarf besser abdecken zu können. |[94] Diese Entwicklung gilt es weiter zu forcieren und etwaige Hemmnisse gegenüber einer Berufsausbildung im wissenschaftlichen Umfeld abzubauen.

| 94 Vgl. HIS-Institut für Hochschulentwicklung – HIS-HE (2019): Digitalisierung der Hochschulen. Ergebnisse einer Schwerpunktstudie für die Expertenkommission Forschung und Innovation (Studien zum deutschen Innovationssystem, Nr. 14-2019), Februar 2019, S. 113, https://medien.his-he.de/publikationen/detail/digitalisierung-der-hochschulen.

Auch über die **Gestaltung der allgemeinen Rahmenbedingungen für eine Beschäftigung im IT-Bereich** können die Personalverantwortlichen und Einrichtungsleitungen Einfluss auf die Attraktivität der angebotenen Stellen nehmen. Hier spielt vor allem ein anderer Umgang mit der Befristung von Beschäftigungsverhältnissen eine Rolle. Personalkonzepte und Personalentwicklung sollten weiterentwickelt werden, |[95] um planbare Karriereperspektiven zu eröffnen und zugleich den Betrieb qualitativ hochwertiger und ausreichend abgesicherter IT-Infrastrukturen verlässlich sicherstellen zu können. In dieser Hinsicht sind die Hochschulen und Forschungseinrichtungen selbst, aber auch ihre Träger und Förderer gefordert, strukturell und finanziell die notwendigen Voraussetzungen dafür zu schaffen, den Anteil an Dauerstellen in der IT perspektivisch erhöhen zu können.

Weitere Verbesserungen lassen sich erreichen, wenn Einrichtungen ihre Personalbewirtschaftung zielgerichteter auf die Gegebenheiten des IT-Fachkräftemarktes ausrichten, um die Verdienstmöglichkeiten attraktiver gestalten zu können. Sinnvolle Optionen sind, auf höhere Stellenbewertungen hinzuwirken – wie es beispielsweise durch das Zusammenlegen vormals getrennter Tätigkeitsfelder möglich ist |[96] – sowie die Anzahl der IT-Stellen, die dem höheren Dienst zugeordnet sind, insgesamt zu steigern. In den Personalplanungen wissenschaftlicher Einrichtungen werden höher bewertete Stellen vielfach noch zu eng mit einer wissenschaftlichen Tätigkeit in Verbindung gebracht, wodurch gut ausgebildeten IT-Fachkräften potenzielle Karriereperspektiven verwehrt werden. |[97]

Bei der Schaffung und Eingruppierung von Stellen sind die Handlungsspielräume der wissenschaftlichen Einrichtungen nicht nur durch ihre Haushalte begrenzt, sondern auch durch die Vorgaben des jeweils anzuwendenden Tarifrechts. Diese stellen nicht nur Hochschulen und Forschungseinrichtungen, sondern den gesamten öffentlichen Sektor vor ähnliche Herausforderungen. Angesichts des vorherrschenden IT-Fachkräftemangels und der stetig zunehmenden Nachfrage ist davon auszugehen, dass sich diese Problemlage noch verschärfen und damit die angestrebte Stärkung der digitalen Souveränität und Sicherheit der Wissenschaft erschweren wird.

| 95 In diesem Sinne hat der Wissenschaftsrat Hochschulen bereits dazu ermutigt, freiwerdende Mittel durch eine anvisierte Erhöhung der Programmpauschalen für die Finanzierung von Dauerstellen bspw. im IT-Bereich zu nutzen. Vgl. Wissenschaftsrat (2023): Strukturen der Forschungsfinanzierung an deutschen Hochschulen | Positionspapier, Köln, https://doi.org/10.57674/pms3-pr05.

| 96 HIS-Institut für Hochschulentwicklung – HIS-HE (2019), a. a. O., S. 115.

| 97 Laut Rat für Informationsinfrastrukturen ist der Bedarf an spezialisierter Unterstützung in der „Betreuung von Anwendungen bzw. Geräten sowie in der Forschungsdokumentation […] in den letzten Jahren in dramatischem Umfang gewachsen. Nachhaltige personelle Lösungen fehlen jedoch: Die Aufgaben werden von Hilfskräften, Promovierenden oder ‚umfunktionierten' wissenschaftlichen Mitarbeiterinnen und Mitarbeitern wahrgenommen." RfII – Rat für Informationsinfrastrukturen (2019): Digitale Kompetenzen – dringend gesucht! Empfehlungen zu Berufs- und Ausbildungsperspektiven für den Arbeitsmarkt Wissenschaft, Göttingen, S. 23 f., https://rfii.de/?p=3883.

Vor diesem Hintergrund spricht sich der Wissenschaftsrat dafür aus, auf **Anpassungen der Eingruppierungs- und Vergütungssysteme von Bund und Ländern hinzuwirken**, und unterstützt diesbezüglich die Empfehlungen der Kultusministerkonferenz |[98] und des Rates für Informationsinfrastrukturen (RfII) |[99]. Die seit einigen Jahren bestehende Möglichkeit einer (übertariflichen) Fachkräftezulage, die insbesondere für IT-Personal gewährt werden kann, |[100] ist zwar grundsätzlich geeignet, um die Attraktivität einer IT-Tätigkeit in Wissenschaftseinrichtungen (und dem öffentlichen Sektor insgesamt) zu erhöhen. Allerdings ist ihr Erfolg angesichts des Konkurrenzdrucks aus der Wirtschaft fraglich, wenn nicht eine stärkere Orientierung an den marktüblichen Verdienstmöglichkeiten und eine auf Dauer angelegte Perspektive in Aussicht gestellt werden. |[101] Hinzu kommt, dass dieses Instrument in den Tarifgebieten von Bund und Ländern nicht einheitlich ausgestaltet ist und es insofern an Transparenz und Übersichtlichkeit für Hochschulen und Forschungseinrichtungen sowie die betroffenen Personen fehlt.

Der Wissenschaftsrat appelliert deshalb an die Tarifparteien, die für die Eingruppierung von IT-Fachkräften maßgeblichen Tätigkeitsmerkmale und Qualifikationserfordernisse angemessen zu flexibilisieren. Hierüber lassen sich größere Spielräume bei der Stellenbewertung erreichen und die Anpassungsfähigkeit an die sich im IT-Bereich besonders rasch wandelnden Tätigkeitsfelder erhöhen. |[102] Dies kann gerade in den niedrigeren Entgeltgruppen die Ausgangsbasis bei der Personalgewinnung und -bindung zu verbessern helfen und würde auch den spezifischen Gegebenheiten des Arbeitsmarktes für IT-Kräfte, auf dem institutionelle Ausbildungen und Abschlüsse tendenziell von geringerer Bedeutung sind, Rechnung tragen. Für die Vergütung von IT-Führungskräften besteht im wissenschaftlichen Kontext zusätzlich die Herausforderung, diese in das personelle Gesamt-

| 98 KMK – Kultusministerkonferenz (2019): Empfehlungen zur Digitalisierung in der Hochschullehre (Beschluss der Kultusministerkonferenz vom 14.03.2019), Bonn/Berlin, S. 8, https://www.kmk.org/aktuelles/artikelansicht/digitalisierung-empfehlungen-fuer-hochschulen-entwickelt.html.

| 99 RfII – Rat für Informationsinfrastrukturen (2019): Digitale Kompetenzen – dringend gesucht! Empfehlungen zu Berufs- und Ausbildungsperspektiven für den Arbeitsmarkt Wissenschaft, Göttingen, S. 28–30, https://rfii.de/?p=3883.

| 100 Die Zulage beträgt aktuell monatlich bis zu 1 000 Euro und kann im Tarifgebiet des Bundes für maximal fünf Jahre gewährt werden. Mehrmalige Verlängerungen sind möglich. Vgl. Bundesministerium des Innern und für Heimat (2022): Rundschreiben „Maßnahmen zur Gewinnung und Bindung von Fachkräften“, 05.07.2022, https://www.bmi.bund.de/RundschreibenDB/DE/2022/RdSchr_20220705.html. Die Ausgestaltung in den Tarifgebieten der Länder erfolgt vielfach durch ähnliche Ministerialerlasse.

| 101 Diese Annahme wird etwa durch eine Studie des IT-Planungsrats von Bund und Ländern gestützt, der zufolge die zu erwartende Entlohnung die häufigste Begründung für den Rückzug einer Bewerbung auf IT-Stellen des öffentlichen Dienstes darstellt. Vgl. IT-Planungsrat (2016): Leitfaden. IT-Personal für die öffentliche Verwaltung gewinnen, binden und entwickeln. Beschluss des IT-Planungsrats vom 16.06.2016, https://www.it-planungsrat.de/beschluss/beschluss-2016-19.

| 102 Diese Forderung findet sich u. a. auch in einer Studie, die das HIS-Institut für Hochschulentwicklung im Auftrag der Expertenkommission Forschung und Innovation durchgeführt hat. Vgl. HIS-Institut für Hochschulentwicklung – HIS-HE (2019): Digitalisierung der Hochschulen. Ergebnisse einer Schwerpunktstudie für die Expertenkommission Forschung und Innovation (Studien zum deutschen Innovationssystem, Nr. 14-2019), Februar 2019, S. 120, https://medien.his-he.de/publikationen/detail/digitalisierung-der-hochschulen.

gefüge von Hochschulen und Forschungseinrichtungen einzuordnen, in denen in der Regel die Professur als Referenzgröße dient. Hier gilt es, außertarifliche Führungspositionen jenseits der Professur zu ermöglichen bzw. in dieser Hinsicht bereits bestehende Optionen auch konsequent zu nutzen.

I.3 Sensibilisierung für Abhängigkeiten und Risiken

Zur digitalen Selbstbefähigung von Wissenschaftseinrichtungen gehört es, sowohl auf institutioneller als auch auf individueller Ebene ein Bewusstsein für Abhängigkeiten und Risiken im digitalen Raum zu schaffen. Angehörige wissenschaftlicher Einrichtungen sind heute gefordert, sich mit Chancen und Risiken digitaler Werkzeuge für die Souveränität und Sicherheit wissenschaftlichen Handelns auseinanderzusetzen und ihre Eigenverantwortung kritisch auszuüben. Dieses **Problem- und Risikobewusstsein** gilt es, **auf Einrichtungsebene gezielt zu fördern**. Hier sind IT-Verantwortliche gefragt, Sicherheits- und Souveränitätsaspekte in IT-Praktiken und den sie leitenden Prinzipien zu verankern und durch unterstützende Maßnahmen zu vermitteln. Neben Richtlinien und Handreichungen sind regelmäßige Schulungen bzw. Fort- und Weiterbildungen erforderlich, um entsprechende Reflexionsfähigkeiten und die damit einhergehenden Kompetenzen in der Breite zu fördern. Die Erfolgsaussichten lassen sich noch steigern, wenn auch die Einrichtungsleitungen Anreize für die Angehörigen ihrer Einrichtung setzen, sich an diesen Sensibilisierungsmaßnahmen zu beteiligen, oder derartige Maßnahmen – je nach Zielgruppe – verpflichtend vorschreiben.

C.II CYBERSICHERHEIT IN OFFENEN ORGANISATIONEN

Angesichts der stetig wachsenden Bedrohungslage und der Häufigkeit, mit der Hochschulen und Forschungseinrichtungen bereits zum Ziel von Cyberangriffen wurden, sind Verbesserungen im Bereich der Cybersicherheit besonders wichtig und dringlich. **Cybersicherheit ist für die Betriebsfähigkeit von Wissenschaftseinrichtungen heute zentral** und muss deshalb auch in ihrer gesamten Tragweite in Planungs- und Strategieprozessen abgebildet werden. Dabei besteht die wesentliche Herausforderung darin, wissenschaftsadäquate Lösungen zu finden, die ein Mehr an Sicherheit schaffen, ohne die für den Wissenschaftsbereich kennzeichnenden Prinzipien der Offenheit und Freiheit unangemessen oder gar rechtswidrig einzuschränken. Wie in jeder Organisation kann auch in einer wissenschaftlichen Einrichtung nie hundertprozentige Sicherheit vor Cyberangriffen und -störfällen erreicht werden.

Um die Cybersicherheit von Wissenschaftseinrichtungen zu stärken, bedarf es möglichst **leistungsfähiger und professionell aufgestellter Organisations- und Governancestrukturen.** Hierfür spielt die Einrichtung einer oder eines IT-Sicherheitsverantwortlichen (CISO) eine zentrale Rolle. Wenngleich die tatsächlichen Möglichkeiten je nach Größe und Leistungsfähigkeit von Hochschulen und For-

schungseinrichtungen variieren werden, sollte es sich hierbei um eine hauptamtlich wahrgenommene Tätigkeit handeln, die getrennt vom Bereich des CIO mit eigenständigen Entscheidungs- und möglichst auch Vetokompetenzen einhergeht, um IT-Maßnahmen mit Blick auf Sicherheitserwägungen beeinflussen zu können (vgl. C.I.1). In der Regel sollte dies die Verfügungsgewalt über ein Cybersicherheitsbudget beinhalten, das es erlaubt, sich in technischer wie personeller Hinsicht hinreichend für die stetig wachsende Bedrohungslage aufzustellen. Als geeignete Richtgröße gelten hier mindestens zehn Prozent des gesamten IT-Budgets einer Einrichtung. | [103]

In die Zuständigkeit der oder des IT-Sicherheitsverantwortlichen fällt unter anderem die **Ausgestaltung und regelmäßige Fortschreibung eines Cybersicherheitskonzepts**, das der Bedrohungslage gerecht wird und zugleich spezifischen Gegebenheiten des wissenschaftlichen Kontextes sowie den individuellen Anforderungen und Besonderheiten vor Ort Rechnung trägt. Hierbei gilt es, mehrere miteinander verschränkte Bereiche zu berücksichtigen, die sich modellhaft in drei Kategorien einteilen lassen: (1) Vorsorge, (2) Schutz und Abwehr sowie (3) Schulung und Sensibilisierung. Eine unbedingt zu empfehlende Orientierungshilfe bietet hier das Grundschutzprofil für Hochschulen, das das BSI in Zusammenarbeit mit dem Verein der Zentren für Kommunikation und Informationsverarbeitung in Lehre und Forschung e. V. (ZKI) bereitstellt und laufend aktualisiert. | [104]

Zur Vorsorge zählt, **gut auf mögliche Cyberattacken und andere Ausfallrisiken vorbereitet zu sein, um rasch reagieren, Gegenmaßnahmen einleiten und zu einem handlungsfähigen Zustand zurückkehren zu können**. Dies erfordert neben klaren Zuständigkeitsregelungen und einer entsprechend dimensionierten Organisationseinheit auch ausreichend detaillierte Notfallpläne, die gerade angesichts der für die Wissenschaft kennzeichnenden Personalfluktuation und Projektstrukturen regelmäßig überprüft, eingeübt und aktualisiert werden müssen. | [105] Die in jüngster Zeit auffallende Häufung erfolgreicher Cyberattacken mit teils weit-

| [103] Zum gesamten Absatz siehe Shulman, H.; Waidner, M. (2023): Forschung muss besser geschützt werden. IT-Sicherheit an Hochschulen und Forschungseinrichtungen, S. 186, in: Forschung & Lehre 30 (2023), Nr. 3, S. 184–186, https://www.forschung-und-lehre.de/management/forschung-muss-besser-geschuetzt-werden-5449.

| [104] Vorstand der Zentren für Kommunikation und Informationsverarbeitung in Lehre und Forschung e. V. – ZKI (Hrsg.) (2022): IT-Grundschutz-Profil für Hochschulen, Version 2022.0.0, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Profil_Hochschulen.html. Orientierung bietet zudem der Standard ISO/IEC 27000ff., der als Grundlage für die Zertifizierung eines Information Security Management Systems dient.

| [105] Darauf weist u. a. der Beitrag von Eva Wolfangel und René Rehme hin, die im Rahmen einer umfangreichen Aktion die Cybersicherheitsvorkehrungen von Hochschulen geprüft haben, vgl. Wolfangel, E.; Rehme, R. (2023): Noten und Atteste frei zugänglich: Wir haben die IT-Sicherheit von Unis und Hochschulen getestet, in: RiffReporter, 10.02.2023, https://www.riffreporter.de/de/technik/hacking-datenschutz-ransomware-hochschulen-universitaeten-daten-im-netz-it-sicherheit.

reichenden und vor allem langanhaltenden Folgen | [106] hat eindrücklich offengelegt, dass in dieser Hinsicht erheblicher Nachholbedarf an Wissenschaftseinrichtungen besteht. Angriffe lassen sich nie gänzlich verhindern. Daher ist es umso wichtiger, adäquat auf etwaige Zwischenfälle reagieren und möglichst rasch wieder Handlungsfähigkeit erlangen zu können (so genannte Business Continuity | [107] oder Resilienzfähigkeit).

Die Besonderheiten des wissenschaftlichen Umfeldes wirken sich auch hinsichtlich der Schutz- und Abwehrvorkehrungen aus, die es im Rahmen eines wirkungsvollen Cybersicherheitskonzepts einzubeziehen gilt. Vor allem der große und offene Kreis der Nutzenden bringt ein erhöhtes Sicherheitsrisiko mit sich, das Wissenschaftseinrichtungen im Vergleich zu anderen öffentlichen Einrichtungen oder Unternehmen vor zusätzliche Herausforderungen stellt. Um dem entgegenzuwirken, empfiehlt es sich, die einrichtungsinternen Systeme nicht nur regelmäßig auf etwaige Schwachstellen zu überprüfen, sondern bereits beim Aufbau der Cybersicherheitsarchitektur auf **technische und organisatorische Segmentierungen zu setzen**. Derart können unterschiedliche Sicherheits- und Schutzniveaus realisiert werden, um einerseits den (Freiheits-)Bedürfnissen von Forschung und Lehre gerecht zu werden und andererseits die für den Betrieb der jeweiligen Einrichtung essenziellen Bereiche, wie etwa die Zentralverwaltung, möglichst umfangreich vor ungebetenen Eindringlingen zu schützen bzw. die Schadenswirkung erfolgreicher Angriffe zu begrenzen. Wo immer möglich, sollte das Sicherheitsniveau zudem durch eine konsequente Orientierung am Zero-Trust-Prinzip erhöht werden. | [108]

Als dritte und in ihrer Bedeutung kaum zu unterschätzende Komponente eines wissenschaftsadäquaten Cybersicherheitskonzepts kommen **regelmäßige und auf die unterschiedlichen Nutzerkreise zugeschnittene Sensibilisierungs- und Schulungsmaßnahmen** hinzu – etwa in Gestalt von Fort- und Weiterbildungen, Handreichungen für Studierende und Mitarbeitende oder auch durch die Nutzung offener, möglichst niedrigschwelliger Kommunikationskanäle, um auf aktuelle Risiken hinzuweisen oder an die Einhaltung gängiger Sicherheitsvorkehrungen

| [106] Hierzu eindrücklich: Technische Universität Berlin: Uni zieht nach Hacker-Angriff Bilanz, vom 18.05.2022, https://www.forschung-und-lehre.de/management/bilanz-des-hacker-angriffs-auf-die-tu-berlin-4721; Interview mit Susanne Kraus: Komplett offline. Rückblick auf den Cyberangriff an der Universität Gießen, in: Forschung & Lehre 30 (2023), Nr. 8, S. 568–570, https://www.forschung-und-lehre.de/management/wie-schuetzen-sich-universitaeten-vor-cyberangriffen-5813.

| [107] Das BSI hat hierzu einen eigenen Standard (200-4) entwickelt und bietet auf seiner Internetpräsenz eine Vielzahl an Informationen und Hilfsmitteln (inkl. entsprechender Dokumentenvorlagen), um diesen umzusetzen (https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-4-Business-Continuity-Management/bsi-standard-200-4_Business_Continuity_Management_node.html).

| [108] Shulman/Waidner (2023), a. a. O., S. 186.

zu erinnern. | [109] Wesentliche Zielsetzungen sollten dabei sein, das Bewusstsein für die besondere Vulnerabilität von Wissenschaftseinrichtungen zu schärfen und zielgruppengerechte Sicherheits- und Verhaltensregeln zu vermitteln, die an die jeweiligen Tätigkeits- und Aufgabenfelder angepasst sind. So unterscheiden sich die Sicherheitsanforderungen, die es in einer Forschungsgruppe im Hinblick auf die Möglichkeiten zum Datenaustausch oder bei der Kooperation mit Partnern außerhalb der Wissenschaft zu beachten gilt, von denen, die innerhalb des Verwaltungssektors, der für den Betrieb der Einrichtung essenziell ist, angebracht sind. Dem ist im Rahmen entsprechend ausgestalteter Sicherheitsrichtlinien Rechnung zu tragen. Angesichts der veränderten geopolitischen Lage müssen solche Richtlinien zudem mit denen abgestimmt sein, die der Sicherheit und Integrität von Lehr- und Forschungsprozessen dienen. Mit Blick auf Fragen der Compliance kann es im Rahmen derartiger Sensibilisierungsmaßnahmen ebenso sinnvoll sein, zu verdeutlichen, welche Auswirkungen ein erfolgreicher Cyberangriff für alle Angehörigen einer Wissenschaftseinrichtung nach sich ziehen kann.

Neben Maßnahmen zur Stärkung der Cybersicherheitskompetenzen auf Einrichtungsebene ist es zudem erforderlich, dass Wissenschaftseinrichtungen **schnell und effektiv auf externe Supportangebote hoher Qualität zurückgreifen** können. Dies betrifft allen voran Hilfestellungen für den Fall einer erfolgreichen Cyberattacke, da diese Ausnahmesituation die Kapazitäten und Fähigkeiten von einzelnen Hochschulen oder Forschungseinrichtungen in aller Regel übersteigt. Hervorzuheben ist in dieser Hinsicht neben der Unterstützung durch die jeweiligen Landeskriminalämter das Dienstleistungsangebot des DFN-CERT, über das unter anderem ein Notfallteam für akute Sicherheitsvorfälle zur Verfügung steht. Hinzu kommen Penetrationstests, Beratungsangebote sowie Warnungen vor Schwachstellen und aktuellen Angriffsmustern. | [110] Diese Services gilt es weiter zu popularisieren und fortwährend auszubauen, um Wissenschaftseinrichtungen darin zu unterstützen, die eigene Sicherheits- bzw. Gefährdungslage möglichst detailliert und umfassend einschätzen zu können.

Um trotz Ressourcenknappheit und Personalmangel auch den laufenden Cybersicherheitsbetrieb von Wissenschaftseinrichtungen in einer ausreichenden Qualität sicherstellen zu können, spricht sich der Wissenschaftsrat ferner dafür aus, IT-Sicherheitsverantwortliche gezielt durch Beratungsangebote oder die Bereitstellung anwendungsorientierter Handreichungen zur Ausgestaltung eines Cybersi-

| [109] Kebschull, U.; Pordesch, U. (2020): Wie IT-Sicherheit an Hochschulen gelingt, 30.11.2020, https://www.forschung-und-lehre.de/management/wie-it-sicherheit-an-hochschulen-gelingt-3292/; Expertenkommission Forschung und Innovation – EFI: Gutachten zu Forschung, Innovation und technologischer Leistungsfähigkeit Deutschlands 2020, https://www.e-fi.de/publikationen/gutachten.

| [110] Hierzu ausführlich DFN-CERT (Computer Emergency Response Team im DFN): https://www.dfn-cert.de/index.html.

cherheitskonzepts zu unterstützen. |[111] Da sich die Möglichkeiten und Werkzeuge zur Durchführung von Cyberangriffen absehbar wandeln werden, ist eine permanente Weiterentwicklung derartiger Angebote im Rahmen von verstetigten Strukturen notwendig (vgl. C.III.2).

C.III ÜBERGREIFENDE STRUKTUREN UND KOOPERATIONSMODI

III.1 Beschaffung und Betrieb

Angesichts von Synergie- und Skaleneffekten können erhebliche Souveränitätsgewinne für den digitalen Wissenschaftsbetrieb damit erzielt werden, **Ressourcen zu bündeln und koordiniert vorzugehen**. Die eigene Souveränität aufgrund eines falschen Verständnisses von wissenschaftlicher Autonomie zu beeinträchtigen, wäre aus Sicht des Wissenschaftsrats leichtfertig. Dies gilt insbesondere für die Beschaffung und den Betrieb digitaler Infrastrukturen und Dienste. Mit Blick auf die föderale Grundstruktur des deutschen Wissenschaftssystems bietet es sich vielfach an, hierbei auf Landesstrukturen zu setzen, die beispielsweise auf den bereits bestehenden Landesinitiativen zur Förderung von digitalen Infrastrukturen im Hochschulsektor aufbauen können. Der Wissenschaftsrat fordert die Länder auf, dieses Potenzial gezielt zu nutzen und davon ausgehend länderübergreifende Kooperationen zu prüfen. Eine Ebene darunter sind auch regionale Zusammenschlüsse zwischen einzelnen Wissenschaftseinrichtungen denkbar, um digitale Dienste und Infrastrukturen standort- und einrichtungsübergreifend als so genannte Shared Services zu betreiben. Als Vorbild können hier unter anderem wissenschaftliche Rechenzentren dienen, die – wie die GWDG oder das LRZ Garching – für mehrere Einrichtungen zuständig sind.

Angelehnt an die Digitaldienstleister aus Großbritannien (Jisc) und den Niederlanden (SURF) sollte aus Sicht des Wissenschaftsrats bei generischen Infrastrukturen und Diensten geprüft werden, ob bundesweite oder zumindest länderübergreifende Strukturen im Auftrag vieler Einrichtungen effektiver und effizienter agieren bzw. bessere Verhandlungsergebnisse erzielen können. Um dies möglichst kostenschonend realisieren zu können, empfiehlt es sich, an Vorhandenes anzuknüpfen. Besonders zielführend erscheint in dieser Hinsicht, das Aufgabenspektrum solcher Institutionen auszuweiten, die schon jetzt als Dienstleister für das gesamte Wissenschaftssystem in Erscheinung treten. Zu denken ist allen voran an den DFN-Verein und mit Blick auf die Hochschulen auch an die HIS eG. Ebenso können einzelne Einrichtungen oder Verbünde für einen Bereich, in dem sie federführend

| [111] Einen Vorstoß in diese Richtung unternimmt bspw. das vom BMBF geförderte und an der Goethe-Universität Frankfurt sowie dem Fraunhofer-Institut für Sichere Informationstechnologie (SIT) angesiedelte Projekt AIGIS. In diesem Rahmen soll noch im Jahr 2023 eine Referenzarchitektur bereitgestellt werden, die den spezifischen Anforderungen von Wissenschaftseinrichtungen Rechnung trägt und an der sich IT-Sicherheitsverantwortliche orientieren können. Vgl. https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/aigis-lab-1.

sind, übergreifende Zuständigkeiten übernehmen. Dabei gilt es stets zu prüfen, ob eine europäische Lösung möglich ist und parallel verfolgt werden kann. Als Finanzierungsmöglichkeit kommt ein Gebührenmodell in Betracht, das eine Abrechnung für einzelne Leistungen erlaubt, wie es etwa bei den Angeboten des DFN-Vereins bereits praktiziert wird.

Darüber hinaus bietet sich eine stärkere Anbindung an die IT-Beschaffung der Länder und des Bundes an. Eine Zusammenarbeit ist hier unter anderem im Bereich der digitalen Abwicklung von administrativen Tätigkeiten, für die Nutzung von Cloud-Services oder für die Beschaffung und Lizensierung generischer Software denkbar. Der Wissenschaftsrat bittet die Wissenschaftsministerien der Länder, eine entsprechende Öffnung für die Hochschulen und Forschungseinrichtungen, die in ihrer Zuständigkeit liegen, zu prüfen.

Nicht alle digitalen Dienste und Infrastrukturen eignen sich gleichermaßen dafür, auf einer übergreifenden Ebene betrieben oder bereitgestellt zu werden. Vielmehr ist **nach Einsatzgebiet, Funktion sowie der erforderlichen Fertigungstiefe zu differenzieren**. So sind etwa Identitätsmanagementanwendungen, generische Software zur Text- und Datenverarbeitung oder auch Server- und Rechenleistungen aufgrund ihres breiten Einsatzgebietes und der damit verbundenen Skalierbarkeit besonders gut für eine einrichtungsübergreife Beschaffung und Bereitstellung geeignet. Demgegenüber qualifizieren sich Soft- und Hardware, deren Nutzbarkeit sich weitgehend auf einzelne Forschungs- und Lehrgebiete beschränkt oder besonderen Ansprüchen hinsichtlich der individuellen Anpassbarkeit genügen muss, eher für einen lokalen Betrieb auf der Ebene einzelner Wissenschaftseinrichtungen. |[112] Eine solche Differenzierung bietet nicht zuletzt den Vorteil, den für die Wissenschaft spezifischen Anforderungen an Flexibilität und Autonomie Rechnung tragen zu können.

III.2 Beratungsangebote und Kompetenzzentren

Ein Auf- und Ausbau einrichtungsübergreifender Strukturen kann auch dabei helfen, die in der Wissenschaft vorhandene Kompetenzbasis zu stärken. Der Wissenschaftsrat ermuntert wissenschaftliche Einrichtungen und Zuwendungsgeber, gemeinsam das **Potenzial von zentral bereitgestellten Beratungsangeboten und Kompetenzzentren auf Landes- oder Bundesebene zu prüfen und bereits bestehende Angebote auszubauen**. Solche Angebote können Wissenschaftseinrichtungen bzw. ihren IT-Verantwortlichen als Unterstützung dienen und das Knowhow bereitstellen, das – gerade in kleineren Einrichtungen – vor Ort nicht oder nur eingeschränkt vorhanden ist. Dies kann etwa den Aufbau einer für die jeweilige Einrichtung passenden IT-Architektur, Schulungen für bestimmte

| 112 Innerhalb der Fraunhofer-Gesellschaft gibt es bereits Bestrebungen nach diesem Muster zwischen „core“ und „commodity“ zu differenzieren und auf diese Weise zu entscheiden, welche Infrastrukturen und Dienste zentral für alle Institute bereitgestellt und welche nach wie vor dezentral vor Ort betrieben werden sollten.

IT-Produkte oder auch die digitale Interaktion mit externen Kooperationspartnern betreffen. Vor allem über eigens entwickelte Handreichungen und Weiterbildungsangebote könnten solche Angebote dazu beitragen, fundierte Handlungs- und Entscheidungskompetenzen in der gesamten Breite des Wissenschaftssystem zu verankern. Zugleich können sie als Orte des Austauschs und des Lernens voneinander fungieren. Bereits bestehende Angebote des Hochschulforums Digitalisierung | [113] und der diversen Landesinitiativen zur Digitalisierung im Hochschulsektor, die diese Aspekte aufgreifen, sind daher zu begrüßen und können Anknüpfungspunkte bieten, um externe Unterstützungsmöglichkeiten weiter auszubauen.

Für den Bereich der Cybersicherheit existieren auf Landesebene teils schon Beratungsangebote | [114] bzw. diese befinden sich aktuell im Aufbau. | [115] Auch der DFN-Verein bietet entsprechende Dienstleistungen speziell für die Wissenschaft an (vgl. C.II). | [116] Dies ist ausdrücklich zu begrüßen und es gilt, derartige Bestrebungen weiter auszubauen, um eine möglichst flächendeckende Unterstützung von Wissenschaftseinrichtungen durch Beratungsangebote oder Kompetenzzentren für Cybersicherheit zu erreichen, die idealerweise sowohl präventiv als auch im Falle eines Angriffs Hilfe leisten können. In diesem Zusammenhang ist ebenfalls zu prüfen, inwiefern die nationalen Forschungszentren für Cybersicherheit (ATHENE, CISPA und KASTEL) für die Wissenschaft die Funktion zentraler Dienstleister übernehmen können. Derart könnte die umfassende und qualitativ hochwertige Forschung im Bereich Cybersicherheit stärker in die Anwendung gebracht werden und die Wissenschaft von den in der Forschung erzielten Fortschritten profitieren. Nicht zuletzt ließen sich über diese Strukturen übergreifende Austausch- und Informationsforen etablieren, über die beispielsweise Erkenntnisse aus bereits erfolgten Cybersicherheitsvorfällen an Wissenschaftseinrichtungen verbreitet werden können.

| 113 Beispielhaft sei hier auf das Programm zur Strategieberatung und -entwicklung verwiesen: https://hochschulforumdigitalisierung.de/news/ausschreibung-der-peer-to-peer-strategieberatung-2023-24-jetzt-bewerben/.

| 114 Hervorzuheben ist hier die Stabsstelle Informationssicherheit an den staatlichen bayerischen Hochschulen. Im Rahmen des Programms „Digitaler Campus Bayern“ wird diese zusätzlich ergänzt durch eine Stabsstelle für IT-Recht. Hierzu ausführlich: Universität Bayern e. V.; Hochschule Bayern e. V. (2021): IT-Strategie der bayerischen Hochschulen – Version 1.0, erstellt von den CIOs und IT-Leiter:innen der Universitäten und Hochschulen angewandter Wissenschaften in Bayern, Dezember 2021, https://www.unibayern.de/assets/Uploads/positionen/2022-01-20-Bayerische-IT-Strategie.pdf.

| 115 Bspw. hat die nordrhein-westfälische Landesregierung angekündigt, an der Universität Siegen ein landesweit agierendes Kompetenz- und Beratungszentrum aufzubauen, vgl. „Alle Hochschulen in NRW von Cyber-Angriffen betroffen“, in: Rheinische Post vom 01.04.2023. Ähnliche Bestrebungen existieren in Baden-Württemberg und in Schleswig-Holstein.

| 116 Einen ausführlichen Überblick bietet die Internetpräsenz des Vereins: https://www.dfn.de/dfn-security-ein-dach-fuer-it-sicherheit/.

IV.1 Diversifizierung und Regulierung

Wissenschaft und Wissenschaftspolitik haben nur bedingt Einfluss darauf, wie der Markt für digitale Dienste und Infrastrukturen ausgestaltet ist. Insofern kann es nicht Zielsetzung sein, auf eine gänzliche Umgestaltung der vorherrschenden Marktbedingungen hinzuwirken, die letztlich ursächlich für die beschriebenen Einschränkungen der digitalen Souveränität sind. Vielmehr muss es darum gehen, Abhängigkeiten zu reduzieren und die Handlungsfähigkeit von Wissenschaftseinrichtungen bzw. der in ihnen tätigen Personen insgesamt zu erhöhen.

Ein wesentlicher Anknüpfungspunkt sind dabei Beschaffungs- und Vergabeprozesse, da sich hierüber steuern lässt, welche digitalen Angebote innerhalb einer Einrichtung zur Verfügung stehen. Hier sind die jeweils zuständigen Stellen gefordert, diese Prozesse so auszugestalten, dass ein **Anbieterwechsel möglich** bleibt sowie **Pluralität und Offenheit gezielt** gefördert werden. Dies kann beispielsweise über die Definition souveränitätsfördernder Mindeststandards erfolgen, die von digitalen Diensten und Infrastrukturen erfüllt werden müssen und Bestandteil aller Leistungsbeschreibungen werden.

Bei jeder Entscheidung über konkrete IT-Infrastrukturen und -Dienste ist eine **Abwägung zwischen Souveränitäts- und Sicherheitsaspekten sowie Fragen der Qualität**, **Nutzerfreundlichkeit und Funktionalität** erforderlich. Hierbei kann es auch zu Spannungen zwischen den beiden Zielkategorien Souveränität und Sicherheit kommen. So sind die Angebote der großen kommerziellen Digitaldienstleister zwar unter Souveränitätsgesichtspunkten häufig zu beanstanden, doch schneiden sie mit Blick auf Sicherheitsfragen im Sinne eines bestmöglichen Schutzes von Daten vor cyberkriminellen Aktivitäten besonders gut ab. Um hierbei zu ausgewogenen Entscheidungen zu kommen, sollten insbesondere die Art und Sensibilität der jeweils betroffenen Daten berücksichtigt werden. Ebenso spielen das Einsatzgebiet und der potenzielle Nutzerkreis eine wesentliche Rolle. Ein mögliches Ergebnis kann dabei auch eine hybride Lösung sein, die – sofern realisierbar – Angebote verschiedener Dienstleister miteinander kombiniert, um von einem hohen Schutzniveau profitieren zu können, ohne sich in einseitige Abhängigkeiten zu begeben.

Derartige Abwägungen und Entscheidungen sind für Akteure, die an Wissenschaftseinrichtungen für die Auswahl und Beschaffung digitaler Dienste und Infrastrukturen verantwortlich sind, herausfordernd. Um diesen Anforderungen gerecht zu werden, sind Kompetenzen und Marktkenntnisse erforderlich, die nicht selbstverständlich vorausgesetzt werden können bzw. in Abhängigkeit von Größe und Art der jeweiligen Einrichtung variieren werden. Abhilfe können hier leicht zugängliche Informationsangebote mit praxisnahen Orientierungsbeispielen oder

auch institutionenübergreifende Austauschforen für IT-Verantwortliche schaffen (vgl. C.III.2).

Für eine schlüssige Gesamtstrategie zur Stärkung von Pluralität und Offenheit ist zugleich ein ausreichendes Angebot **öffentlich geförderter Infrastrukturen und Plattformen** sowie deren umfassende Nutzung durch die Wissenschaft unabdingbar. Eine wesentliche Herausforderung ist es hierbei allerdings, zu konkretisieren, in welchem Verhältnis die einzelnen Projekte – von KI-Kompetenzzentren über Hoch- und Höchstleistungsrechnen bis hin zu Dateninfrastrukturen – zueinanderstehen und wie sie sich in Zukunft besser miteinander verknüpfen lassen. Erste Schritte in diese Richtung sind bereits getan. So soll die NFDI laut Datenstrategie des Bundes der zentrale deutsche Beitrag zur EOSC sein |[117] und das vom BMBF finanzierte Projekt „FAIR Data Spaces" zielt darauf, Synergien zwischen Gaia-X und NFDI auszuloten. |[118] Hervorzuheben sind in dieser Hinsicht auch die verschiedenen Vorstöße des RfII, die Szenarien für eine (Weiter-)Entwicklung föderierter Dateninfrastrukturen für die Wissenschaft aufzeigen und dabei unter anderem dazu auffordern, Doppelstrukturen zu vermeiden sowie NFDI und EOSC stärker aufeinander abzustimmen und miteinander zu verbinden. |[119] Der Wissenschaftsrat wird sich dazu auch im Rahmen der Strukturevaluation der NFDI äußern, die im Jahr 2025 abgeschlossen werden soll.

Ergänzend zu diesen strukturellen Fragen bedarf es zudem mehr Klarheit darüber, wie die künftige Nutzung für wissenschaftliche Akteure ausgestaltet und wie die Abstimmungsprozesse dazu unter Beteiligung der einschlägigen Stakeholder organisiert werden (sollen). |[120] Wesentliche Zielsetzungen sollten dabei sein: (1) Strategien zu entwickeln, um sicherzustellen, dass die Angebote möglichst nahtlos an bestehende Strukturen anknüpfen, (2) Priorität auf eine nutzerfreundliche Ausgestaltung zu setzen und (3) die Bekanntheit der Angebote auf allen Ebenen des Wissenschaftssystems zu erhöhen.

| 117 Bundeskanzleramt (Hrsg.): Datenstrategie der Bundesregierung. Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum. Kabinettfassung, 27. Januar 2021, Berlin 2021, https://www.bundesregierung.de/breg-de/service/publikationen/datenstrategie-der-bundesregierung-1845632. Ebenso findet sich in der erneuerten Datenstrategie von 2023 ein klares Bekenntnis zur Förderung dieser Datenräume: Bundesministerium für Digitales und Verkehr; Bundesministerium für Wirtschaft und Klimaschutz; Bundesministerium des Innern und für Heimat (Hrsg.) (2023): Fortschritt durch Datennutzung. Strategie für mehr und bessere Daten für neue, effektive und zukunftsweisende Datennutzung, Berlin, S. 28, https://bmdv.bund.de/SharedDocs/DE/Anlage/K/nationale-datenstrategie.pdf.

| 118 FAIR - Findable, Accessible, Interoperable, Reusable, https://www.nfdi.de/fair-data-spaces/.

| 119 RfII – Rat für Informationsinfrastrukturen (2023): Föderierte Dateninfrastrukturen für die wissenschaftliche Nutzung. NFDI, EOSC und Gaia-X: Vergleich und Anregungen für eine engagiere Mitgestaltung des Ausbaus und der Weiterentwicklung (RfII-Berichte, Nr. 4), Göttingen, https://rfii.de/?p=8533; ders. (2022): Datenpolitik, Open Science und Dateninfrastrukturen: Aktuelle Entwicklungen im europäischen Raum. Bericht und Empfehlungen, Göttingen, https://rfii.de/?p=7743.

| 120 Wissenschaftsrat (2021): Impulse aus der COVID-19-Krise für die Weiterentwicklung des Wissenschaftssystems in Deutschland | Positionspapier, Köln, S. 52, https://www.wissenschaftsrat.de/download/2021/8834-21.html.

Neben diesen Maßnahmen innerhalb des Wissenschaftssystems selbst ist es aus Sicht des Wissenschaftsrats zudem ratsam, auch die breiteren politischen Bestrebungen für eine stärkere Regulierung des Digitalmarktes kritisch zu begleiten und hierbei gezielt wissenschaftsspezifische Anforderungen und Ziele zu artikulieren. Hierfür sollten Akteure aus Wissenschaftseinrichtungen und Wissenschaftspolitik möglichst eng zusammenarbeiten. Neben der Allianz der Wissenschaftsorganisationen sind hier auch die Stellungnahmen des RfII zu nennen, die wesentliche Interessen und Anliegen aus Sicht der Wissenschaft bündeln. | [121]

IV.2 Gestaltung des Softwareangebots

Auch über die Auswahl und Zusammensetzung des Softwareangebots können IT-Verantwortliche an Hochschulen und Forschungseinrichtungen zu einer offenen und selbstbestimmten Ausgestaltung des digitalen Raumes beitragen. Zu denken ist hierbei in erster Linie an einen verstärkten Rückgriff auf Open-Source-Lösungen, deren Einsatz und (Weiter-)Entwicklung weiter ausgebaut und gezielt gefördert werden sollten. Dies erfordert, die Anforderungen an digitale Dienste und Infrastrukturen im Rahmen von Beschaffungs- und Vergabeprozessen anzupassen und auch den Markt dahingehend zu sondieren, ob quelloffene Lösungen vorhanden sind, die sich hinsichtlich Funktionalität, Qualität und Nutzerfreundlichkeit als Alternativen zu den bisher eingesetzten IT-Produkten eignen.

Damit ist nicht gemeint, den IT-Betrieb einer Einrichtung pauschal auf Open Source umzustellen. Dies wäre wenig zielführend und mit den jeweils vorhandenen Ressourcen wohl kaum umsetzbar. Vielmehr empfiehlt sich auch hier eine **differenzierte Herangehensweise**. Neben Sicherheitsaspekten ist insbesondere der Betreuungs- und Ressourcenaufwand zu bedenken, den es gegenüber den zu erzielenden Souveränitätsgewinnen abzuwägen gilt. Hinzu kommt der potenzielle Nutzerkreis, da die Aufgeschlossenheit gegenüber digitalen Angeboten, die nicht aus dem gemeinhin bekannten Portfolio der großen Privatanbieter stammen, in Abhängigkeit von Funktionsbereich und Fachkultur variieren kann. Zwar ließe sich dem durch begleitende Schulungs- und Sensibilisierungsmaßnahmen begegnen, doch gilt es hier das Verhältnis von Kosten und Nutzen im Blick zu behalten.

Ein verstärkter Einsatz von Open-Source-Lösungen setzt voraus, dass es **nachhaltige Strukturen und eine Finanzierungsgrundlage für die Wartung und Weiterentwicklung** solcher Software gibt. Für Software im Bereich der Wissenschaftsadministration, wie etwa Campusmanagementsysteme, sowie für Anwendungen mit einem ähnlich breiten Nutzerkreis und einer potenziell langen Laufzeit bieten sich hier Kooperationen von Wissenschaftseinrichtungen besonders an. Wenn es sich hingegen um Software handelt, die als spezifisches Forschungsinstrument zum Einsatz kommt, erscheint ein Rückgriff auf wissenschaftsimmanente Förder- und

| [121] Die Stellungnahmen sind über die Homepage des RfII abrufbar: https://rfii.de/de/dokumente/.

Anreizlogiken zielführender, um den jeweiligen Kontexten und disziplinären Besonderheiten Rechnung tragen zu können.

Im Bereich der Standardanwendungen begrüßt der Wissenschaftsrat zudem die verstärkten Bemühungen von Bund und Ländern, gemeinsame Lösungen für den ganzen öffentlichen Sektor zu forcieren. |[122] Da sich hierdurch der Mehraufwand bezüglich Wartung und Betreuung vor Ort reduzieren lässt, ermuntert er die Wissenschaftseinrichtungen, sich aktiv an diesen Bestrebungen zu beteiligen. Zugleich bittet er den Bund und die Länder, bei der Förderung des Open-Source-Bereichs auch die Wissenschaft als Anwendungsbereich zu berücksichtigen. In diesem Zusammenhang kann es ebenso lohnend sein, die bereits bestehenden Aktivitäten des Sovereign Tech Fund (STF) im Bereich wissenschaftsspezifischer Anwendungen auch zukünftig weiter zu verfolgen. |[123]

Damit Open-Source-Anwendungen möglichst breit und vor allem verlässlich für alle Akteure innerhalb des Wissenschaftssystems zur Verfügung stehen, bedarf es zudem Vorkehrungen, um für eine allgemeine und auf Dauer angelegte Verfügbarkeit Sorge zu tragen (vgl. C.V). Damit geht die Zuweisung von Verantwortlichkeiten einher, die es innerhalb des Wissenschaftssystems zu regeln gilt. Zuständigkeiten und Prozessabläufe müssen eindeutig festgelegt, Support- und Beratungsmechanismen integriert werden. |[124]

Gesondert von einer Ausweitung des Einsatzes von Open-Source-Lösungen innerhalb der Wissenschaft selbst ist die Fragestellung zu betrachten, welche Rolle dem wissenschaftlichen Sektor bei der Weiterentwicklung und Förderung quelloffener Alternativlösungen insgesamt zukommen sollte. Hier besteht in der wissenschaftspolitischen Landschaft weitgehende Einigkeit, dass es das **in der Wissenschaft vorhandene Knowhow und Innovationspotenzial** zu nutzen und durch gezielte Fördermaßnahmen weiter auszubauen gilt. |[125] Die Vorstellungen darüber, in welcher Form dies am besten geschehen sollte, gehen hingegen auseinander. Dabei reicht die Bandbreite von (rein) öffentlichen Modellen der einrich-

| 122 Siehe hierzu insbesondere die Bestrebungen im Zusammenhang mit dem Souveränen Arbeitsplatz für die öffentliche Verwaltung: https://www.cio.bund.de/Webs/CIO/DE/digitale-loesungen/digitale-souveraenitaet/souveraener-arbeitsplatz/souverarner-arbeitsplatz-node.html.

| 123 So fördert der STF bspw. bereits die für die Wissenschaft relevanten Projekte „Open Blas“ und „Fortran“.

| 124 In Großbritannien hat man sich hierfür mit dem Software Sustainability Institute für einen zentralen Akteur entschieden, vgl. https://www.software.ac.uk/about; vgl. auch C.V.

| 125 So etwa Bundesministerium für Bildung und Forschung – BMBF (2021): Technologisch souverän die Zukunft gestalten. Impulspapier zur technologischen Souveränität, Bonn/Berlin; Wissenschaftsrat (2021): Impulse aus der COVID-19-Krise für die Weiterentwicklung des Wissenschaftssystems in Deutschland | Positionspapier, Köln, S. 46, https://www.wissenschaftsrat.de/download/2021/8834-21.html. Deutsche Forschungsgemeinschaft (2020): Digitaler Wandel in den Wissenschaften. Impulspapier, Bonn, S. 9, https://doi.org/10.5281/zenodo.4191345.

tungsübergreifenden Kooperation über Public-Private-Partnerships bis hin zu start-up-ähnlichen Strukturen. | [126]

Die Wissenschaft würde in jedem Fall profitieren – sowohl von der Möglichkeit, innovative Lösungen in der Praxis zu erproben als auch von den damit bezweckten Verbesserungen im Open-Source-Bereich. Dahingehende Bestrebungen sind daher ausdrücklich zu begrüßen und sollten durch gezielte Anreize flankiert werden, um Forschende und Einrichtungsleitungen dazu zu bewegen, sich aktiv in die Open-Source-Entwicklung einzubringen. Dies können beispielsweise Vorgaben im Rahmen der Forschungsförderung oder auch Anpassungen bei der Leistungsbewertung von Wissenschaftlerinnen und Wissenschaftlern sein.

IV.3 Innovationsbereitschaft der Wissenschaft

Mit Blick auf mehr Pluralität und Offenheit digitaler Angebote nimmt der wissenschaftliche Sektor eine Sonderrolle ein. Denn als wesentlicher Innovationstreiber ist Wissenschaft grundsätzlich dazu in der Lage, sich an der Ausgestaltung und Weiterentwicklung dieses Angebotsportfolios zu beteiligen und dadurch auch die Wirtschaft und andere Gesellschaftsbereiche zu beeinflussen. Um dieses Potenzial möglichst gewinnbringend zu nutzen, ist es wichtig, die Förderung von Transferleistungen, inklusive der hierfür nötigen Kompetenzen und Kapazitäten, weiter voranzutreiben und die Rahmenbedingungen für Start-ups bzw. Ausgründungen aus der Forschung insgesamt zu verbessern. Insofern sind neben wissenschaftspolitischen vor allem auch wirtschaftspolitische Akteure von Bund und Ländern gefordert.

Zudem können die Entscheidungs- und Steuerungsprozesse innerhalb von Wissenschaftseinrichtungen einen Beitrag dazu leisten, die Marktchancen für wissenschaftsnahe Unternehmen zu erhöhen – etwa indem deren Angebote bewusst in Beschaffungs- und Lizenzierungsentscheidungen einbezogen werden oder in Erwägung gezogen wird, ob der wissenschaftliche Akteurskreis für Multiplikator- und Skaleneffekte genutzt werden könnte. Wissenschaftliche Einrichtungen sind innovationsfreundlich und eignen sich deshalb besonders dafür, öffentliche Aufträge im Sinne der Start-up-Strategie der Bundesregierung für die Stärkung von Start-up-Ökosystemen zu nutzen. | [127] In diesem Zusammenhang ist auch zu prüfen, inwiefern vergaberechtliche Vorschriften kleineren Anbietern den Zugang

| [126] HRK - Hochschulrektorenkonferenz (2021): Momentum der Digitalisierung nutzen: Forderungen an Bund und Länder zur Weiterentwicklung der digitalen Lehrinfrastruktur. Entschließung des 148. Senats der HRK am 8. Juni 2021, Videokonferenz, https://www.hrk.de/positionen/beschluss/detail/forderungen-an-bund-und-laender-zur-weiterentwicklung-der-digitalen-lehrinfrastrukturen/, S. 8.

| [127] Bundesministerium für Wirtschaft und Klimaschutz – BMWK (2022): Die Start-up-Strategie der Bundesregierung, Berlin, S. 20 f., https://www.exist.de/EXIST/SUS/start-up-strategie-der-bundesregierung.html.

zum Wissenschaftsmarkt erschweren und daher für eine stärkere Diversifizierung digitaler Infrastrukturen und Dienste angepasst werden sollten. | [128]

C.V DIGITALITÄT (IN) DER WISSENSCHAFT ALS DAUERHAFTE AUFGABE

Um die Souveränität und Sicherheit der Wissenschaft im digitalen Raum langfristig zu sichern, genügt es nicht, die einzelnen Einrichtungen kurzfristig besser aufzustellen. Vielmehr müssen auch die strukturellen und finanziellen Rahmenbedingungen, in die der digitale Wissenschaftsbetrieb eingebettet ist, weiterentwickelt werden. Vielfach sind mittel- bis langfristige Planungshorizonte bedingt durch die gängigen Finanzierungsmechanismen und die damit verbundene Dominanz von Projektstrukturen kaum möglich. Dadurch werden souveränitäts- und sicherheitsfördernde Maßnahmen, wie sie weiter oben etwa im Bereich der Personal- und Governancestrukturen erläutert werden (vgl. C.I), deutlich erschwert. Insofern stoßen die Verantwortlichen von Wissenschaftseinrichtungen bisweilen an Grenzen, die in einer auffallenden Diskrepanz zu der herausragenden Bedeutung stehen, die das Digitale mittlerweile für nahezu alle Funktions- und Aufgabenbereiche innerhalb der Wissenschaft einnimmt.

Vor diesem Hintergrund bekräftigt der Wissenschaftsrat nachdrücklich seine Position, dass die **Gestaltung des digitalen Raumes als Daueraufgabe von Wissenschaftseinrichtungen zu verankern und dem auch in finanzieller Hinsicht Rechnung zu tragen** ist. | [129] Der Anteil der Budgets wissenschaftlicher Einrichtungen, der für die Planung, die Beschaffung und den sicheren Betrieb von digitalen Infrastrukturen und Diensten eingesetzt wird, muss deutlich steigen. Nur so kann es den Einrichtungen gelingen, einen digitalen Grundbetrieb zu bestreiten, der dem jeweils aktuellen Stand der Technik entspricht und neueste Sicherheitsstandards berücksichtigt, und dabei längerfristige Planungshorizonte zu eröffnen, um sowohl in personeller als auch in struktureller Hinsicht mehr Kontinuität, Verlässlichkeit und Qualität erreichen zu können. Dies sind zugleich Grundvoraussetzungen dafür, die Innovationsfähigkeit der Wissenschaft zu stärken. Im Umkehrschluss kann dies bedeuten, dass ein geringerer Anteil des Budgets der Einrichtungen für andere Aufgaben zur Verfügung steht. Hochschulen und Forschungseinrichtungen müssen intern sowie mit ihren jeweiligen Trägern und Zuwendungsgebern darüber verhandeln, wie dieser Zielkonflikt gelöst werden kann, um eine zukunftsgerichtete Weiterentwicklung und Stärkung des digitalen Wissenschaftsbetriebs sicherzustellen.

Eng verbunden mit mehr Planungssicherheit sind Fragen, die die längerfristige Zugänglichkeit und Nutzbarkeit von digitalen Infrastrukturen und Diensten ins-

| [128] Vor allem der hohe administrative Aufwand wirft Fragen nach der Chancengleichheit im Verhältnis zu den etablierten Hyperscalern auf, die hier auf eine wesentlich größere Ressourcenbasis zurückgreifen können.

| [129] Wissenschaftsrat (2022): Empfehlungen zur Digitalisierung in Lehre und Studium, Köln, https://doi.org/10.57674/sg3e-wm53.

gesamt betreffen. Hier bestehen im wissenschaftlichen Kontext aufgrund der Anforderungen an Transparenz und Nachvollziehbarkeit besondere Herausforderungen. Dies gilt insbesondere für die Verfügbarkeit von Daten und Software im Forschungskontext, ohne die Prozesse und Resultate nicht intersubjektiv überprüfbar wären. Entsprechende Vorhaben im Rahmen von NFDI und EOSC, die eine dauerhafte Verfügbarkeit, Zugänglichkeit und Nutzbarkeit von Daten – einschließlich der für ihre Erschließung erforderlichen Infrastrukturen und Dienste – anstreben und auf eine Stärkung der Interoperabilität zielen, sind deshalb zu begrüßen.

Mit Blick auf Software, die für und in der Forschung entwickelt wird, hat die Helmholtz-Gemeinschaft bereits Empfehlungen erarbeitet, um für mehr Nachhaltigkeit bei Ausgestaltung und Betrieb zu sorgen. | [130] Hier geht es unter anderem darum, die Abhängigkeiten von Projektstrukturen und dem institutionellen Verbleib einzelner Personen zu reduzieren.

Eine über den Helmholtz-Kontext hinausweisende Perspektive wird dadurch allerdings noch nicht eröffnet. Um eine nachhaltige Bereitstellung und Nutzung von Forschungssoftware unabhängig von der institutionellen Anbindung für alle wissenschaftlichen Akteure zu gewährleisten, sollte daher geprüft werden, inwiefern sich übergreifende Strukturen etablieren lassen, die Software konsequent als Teil der gesamten Forschungsinfrastruktur begreifen. Als Vorbild sowohl hinsichtlich Finanzierung als auch Organisationsstruktur kann hier das britische Software Sustainability Institute dienen. In diesem Modell tragen verschiedene Einrichtungen der Forschungsförderung gemeinsam eine Institution, die Software als zentrale Infrastruktur für die Forschung begreift und sie dementsprechend den dort tätigen Akteuren zur Verfügung stellt. | [131] Auch die NFDI wäre ein möglicher Anknüpfungspunkt. Dies böte nicht zuletzt den Vorteil, auf bereits vorhandenen Strukturen aufbauen zu können.

| [130] Arbeitskreis Open Science der Helmholtz-Gemeinschaft (2019): Empfehlungen zur Implementierung von Leit- und Richtlinien zum Umgang mit Forschungssoftware an den Helmholtz-Zentren, Positionspapier vom 21.11.2019, Potsdam, https://doi.org/10.2312/os.helmholtz.008; Arbeitskreis Open Science der Helmholtz-Gemeinschaft (2019): Muster-Richtlinie Nachhaltige Forschungssoftware an den Helmholtz-Zentren, Stand 21.11.2019, Potsdam https://doi.org/10.2312/os.helmholtz.007.

| [131] Vgl.: https://software.ac.uk/about/funders.

ATHENE	Nationales Forschungszentrum für angewandte Cybersicherheit
BMBF	Bundesministerium für Bildung und Forschung
BMI	Bundesministerium des Innern und für Heimat (davor Bundesministerium des Innern, für Bau und Heimat)
BMWi	Bundesministerium für Wirtschaft und Energie (nunmehr BMWK)
BMWK	Bundesministerium für Wirtschaft und Klimaschutz
BSI	Bundesamt für Sicherheit in der Informationstechnik
CHE	Centrum für Hochschulentwicklung
CIO	Chief Information Officer
CISO	Chief Information Security Officer (IT-Sicherheitsverantwortliche/r)
CISPA	Helmholtz Center for Information Security
DFN	Verein zur Förderung eines Deutschen Forschungsnetzes e. V.
DFN-CERT	Computer Emergency Response Team im DFN
DSK	Datenschutzkonferenz
EFI	Expertenkommission Forschung und Innovation
EOSC	European Open Science Cloud
EuroHPC	Europäische Partnerschaft zum High Performance Computing
FAIR	Findable, Accessible, Interoperable, Reusable (auffindbar, zugänglich, interoperabel, wiederverwendbar)
Gaia-X	Föderierte, sichere Dateninfrastruktur für Europa
GCS	Gauss Centre for Supercomputing e. V.
GWDG	Gesellschaft für wissenschaftliche Datenverarbeitung
HIS eG	Hochschul-Informations-System eG
HIS-HE	HIS-Institut für Hochschulentwicklung e. V.
HLRS	Höchstleistungsrechenzentrum Stuttgart
HPC	High Performance Computing
HRK	Hochschulrektorenkonferenz

IAM	Identity and Access Management
IKT	Informations- und Kommunikationstechnologie
IT	Informationstechnologie
Jisc	Joint Information Systems Committee
JSC	Jülich Supercomputing Center
KASTEL	Institut für Informationssicherheit und Verlässlichkeit am Karlsruher Institut für Technologie
KI	Künstliche Intelligenz
LRZ	Leibniz-Rechenzentrum
NFDI	Nationale Forschungsdateninfrastruktur
NHR	Nationales Hochleistungsrechnen
NREN	National research and education network
ÖFIT	Kompetenzzentrum Öffentliche IT
RfII	Rat für Informationsinfrastrukturen
SIT	Fraunhofer-Institut für Sichere Informationstechnologie
STF	Sovereign Tech Fund
SURF	Cooperative association of Dutch educational and research institutions
TU	Technische Universität
WR	Wissenschaftsrat
WZB	Wissenschaftszentrum Berlin für Sozialforschung gGmbH
ZenDiS	Zentrum für Digitale Souveränität der Öffentlichen Verwaltung
ZKI	Zentren für Kommunikation und Informationsverarbeitung in Lehre und Forschung e. V.

Mitwirkende

Im Folgenden werden die an den Beratungen im Wissenschaftsrat und in der Arbeitsgruppe „Souveränität und Sicherheit der Wissenschaft im digitalen Raum“ 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. Julia Arlinghaus
Otto-von-Guericke-Universität Magdeburg | Fraunhofer-Institut für Fabrikbetrieb und -automatisierung IFF, Magdeburg

Dr. Ulrich A. K. Betz
Merck KGaA

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

Dr. Cord Dohrmann
Evotec SE

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

Professorin Dr. Beate Escher
Universität Tübingen | Helmholtz-Zentrum für Umweltforschung – UFZ, Leipzig

Professor Dr. Christian Facchi
Technische Hochschule Ingolstadt

Professorin Dr. Christine Falk
Medizinische Hochschule Hannover

Marco R. Fuchs
OHB SE, Bremen

Professorin Dr. Uta Gaidys
Hochschule für Angewandte Wissenschaften Hamburg

Alexandra Gerlach
Journalistin

Professor Dr. Michael Hallek
Universität zu Köln

Dr.-Ing. Frank Heinricht
SCHOTT AG

Professor Dr. Jürgen Heinze
Universität Regensburg

Professorin Dr. Denise Hilfiker-Kleiner
Philipps-Universität Marburg

Dr. Stefan Kampmann
Voith Group

Professorin Dr. Gudrun Krämer
Freie Universität Berlin

Professor Dr. Wolfgang Lehner
Technische Universität Dresden

Dr. Claudia Lücking-Michel
AGIAMONDO e. V.

Professor Dr. Gerard J. M. Meijer
Fritz-Haber-Institut der Max-Planck-Gesellschaft, Berlin

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

Professorin Dr. Heike Solga
Freie Universität Berlin | Wissenschaftszentrum Berlin für Sozialforschung (WZB)
Vorsitzende der Wissenschaftlichen Kommission

Professor Dr. Thomas S. Spengler
Technische Universität Braunschweig

Professorin Dr. Birgit Spinath
Universität Heidelberg

Professor Dr.-Ing. Martin Sternberg
Hochschule Bochum | Promotionskolleg für angewandte Forschung in Nordrhein-Westfalen

Professorin i. R. Dr. Margit Szöllösi-Janze
Ludwig-Maximilians-Universität München

Professor Dr. Martin Visbeck
GEOMAR Helmholtz-Zentrum für Ozeanforschung Kiel

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

Verwaltungskommission (Stand: Oktober 2023)

Von der Bundesregierung entsandte Mitglieder

Professorin Dr. Sabine Döring
Staatssekretärin im Bundesministerium für Bildung und Forschung
Vorsitzende der Verwaltungskommission

Judith Pirscher
Staatssekretärin im Bundesministerium für Bildung und Forschung

Werner Gatzer
Staatssekretär im Bundesministerium der Finanzen

Juliane Seifert
Staatssekretärin im Bundesministerium des Innern und für Heimat

Silvia Bender
Staatssekretärin im Bundesministerium für Ernährung und Landwirtschaft

Udo Philipp
Staatssekretär im Bundesministerium für Wirtschaft und Klimaschutz

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, Pflege und Gleichstellung

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 Finanzbehörde

Hessen

Angela Dorn-Rancke
Staatsministerin für Wissenschaft und Kunst

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

Saarland

Jakob von Weizsäcker
Minister für Finanzen und Wissenschaft

Sachsen

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

Sachsen-Anhalt

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

Schleswig-Holstein

Karin Prien
Ministerin für Allgemeine und Berufliche Bildung, Wissenschaft, Forschung und Kultur

Thüringen

Wolfgang Tiefensee
Minister für Wirtschaft, Wissenschaft und Digitale Gesellschaft

Professorin Dr. Dorothea Wagner
Karlsruher Institut für Technologie (KIT)
Vorsitzende des Wissenschaftsrats bis Januar 2023 und Vorsitzende der Arbeitsgruppe

Ministerialrat Georg Antretter
Bayerisches Staatsministerium für Wissenschaft und Kunst

Dr. Ulrich A. K. Betz
Merck KGaA

Professor Dr. Christian Facchi
Technische Hochschule Ingolstadt

Regierungsdirektorin Andrea Herdegen
Bundesministerium für Bildung und Forschung

Leitender Senatsrat Bernd Lietzau
Senatsverwaltung für Wissenschaft, Gesundheit und Pflege

Professorin Dr. Sabine Maasen
Universität Hamburg

Professor Dr. Boris Otto
Fraunhofer-Institut für Software- und Systemtechnik (ISST) |
Technische Universität Dortmund

Professor Dr. Peter Parycek
Donau-Universität Krems, Österreich |
Kompetenzzentrum Öffentliche IT (ÖFIT) am Fraunhofer Fokus Institut Berlin

Professorin Dr. Louisa Specht-Riemenschneider
Rheinische Friedrich-Wilhelms-Universität Bonn

Professor Dr. Thomas S. Spengler
Technische Universität Braunschweig

Professor Dr. Michael Waidner
Fraunhofer-Institut für Sichere Informationstechnologie (SIT) |
Technische Universität Darmstadt

Professor Dr. Ramin Yahyapour
Gesellschaft für wissenschaftliche Datenverarbeitung Göttingen (GWDG) |
Georg-August-Universität Göttingen

Als Gast:

Dr. Pascal Hetze
Stifterverband

Helga Angermann (Teamassistentin)

Gudrun Hilles (Sachbearbeiterin)

Dr. Rainer Lange (Abteilungsleiter)

Pascal Pawlitta (Referent)