Büro für Technikfolgen-Abschätzung
beim Deutschen Bundestag

TAB

Cybersicherheit im Forschungsprozess

Ergebnisse aus dem Resilienz-Check

Michaela Evers-Wölk
Nona Bledow
Carolin Kahlisch

September 2026
Resilienz-Dossier Nr. 2

Inhalt

Zusammenfassung

Der jährlich im Rahmen der Foresight-Aktivitäten des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB) durchgeführte Resilienz-Check untersucht relevante Fragen zur Stärkung der Resilienz kritischer Infrastruktursysteme. Er baut auf dem Resilienz-Radar und dem Foresight-Report zum Infrastruktursystem Bildung und Forschung auf und vertieft eines der darin identifizierten Fokusthemen. Der Resilienz-Check 2025/2026 widmet sich der Cybersicherheit im Forschungsprozess, die im Resilienz-Radar zum Infrastruktursystem Bildung und Forschung als Fokusthema identifiziert wurde. Untersucht wird das Thema entlang der drei Handlungsdimensionen Schutz und Integrität von Forschungsdaten, Sicherheit, Kompetenzen und Governance in Forschungseinrichtungen sowie digitale Souveränität und vertrauenswürdige internationale Kooperationen. Ziel ist es, mögliche zukünftige Entwicklungen und daraus resultierende Vulnerabilitäten des Forschungssystems frühzeitig zu erkennen, politisch einzuordnen und robuste Handlungsoptionen zur Stärkung der Cybersicherheit im Forschungsprozess und damit der Resilienz des Forschungssystems insgesamt abzuleiten.

Der Resilienz-Check verbindet methodisch drei aufeinander aufbauende Arbeitsschritte: die Entwicklung eines Systembildes und die Identifikation themenrelevanter Einfluss- und Schlüsselfaktoren, die Entwicklung alternativer Zukunftsszenarien 2030+ sowie die Ableitung von Handlungsoptionen. Grundlage bilden Quellenanalysen, ein strukturierter Partizipationsprozess mit inter- und transdisziplinären Expert/innen sowie software- und KI-gestützte Analysen. Drei moderierte Round Tables und eine Onlinekonsultation dienen dazu, ausgewählte Zwischenergebnisse im Projektverlauf fachlich einzuordnen, zu ergänzen und zu validieren. Die Szenariobildung wird durch die Software ScenarioWizard des Zentrums für interdisziplinäre Risiko- und Innovationsforschung unterstützt. Generative KI kommt entsprechend den TAB-Leitlinien als Instrument zur Erweiterung und Strukturierung des Analyseraums zum Einsatz; Prüfung, Bewertung und Interpretation bleiben dem Projektteam überlassen. Das vorliegende Resilienz-Dossier bündelt die Ergebnisse des Resilienz-Checks 2025/2026 in einem Systembild, drei Zukunftsszenarien und daraus abgeleiteten kurz-, mittel- und langfristigen Handlungsoptionen. Es bildet zugleich die Grundlage für die gemeinsame Veranstaltung „TA im Dialog: Cybersicherheit im Forschungsprozess. Datenintegrität, Kompetenzen und sichere Kooperationen“ von TAB und dem Ausschuss für Forschung, Technologie, Raumfahrt und Technikfolgenabschätzung am 22. September 2026 im Deutschen Bundestag.

Der Resilienz-Check 2025/2026 zeigt, dass Cybersicherheit im Forschungsprozess durch ein komplexes Zusammenspiel gesellschaftlicher, technologischer, wirtschaftlicher und politisch-rechtlicher Faktoren geprägt wird. Über 60 Einflussfaktoren wurden identifiziert und 19 besonders relevante Schlüsselfaktoren priorisiert. Sie wirken als zentrale Hebel für die Resilienz des Forschungssystems und adressieren unter anderem das Spannungsfeld zwischen Offenheit und Sicherheit sowie zentrale Themen wie Cyberkompetenzen, komplexe IT-Infrastrukturen, Fachkräfte und Abhängigkeiten sowie digitale Souveränität, Regulierung und internationale Kooperation.

Auf Basis der Schlüsselfaktoren wurden drei konsistente alternative Zukunftsszenarien zur Cybersicherheit im Forschungsprozess 2030+ entwickelt. Sie sind keine Prognosen, sondern zeigen unterschiedliche Entwicklungspfade und Gestaltungsspielräume. Die Szenarien unterscheiden

sich nach politischem Handlungsdruck, institutioneller Handlungsfähigkeit und sozial-kultureller Verankerung von Cybersicherheit im Forschungssystem. Szenario 1 „Hoher Handlungsdruck bei strukturellen Defiziten“ beschreibt eine verschärfte Bedrohungslage, der aufgrund von Fragmentierung, Kompetenzdefiziten und unzureichender Governance keine hinreichend wirksamen Maßnahmen gegenüberstehen. Szenario 2 „Politischer Sicherheitsfokus mit deutlichen Defiziten in der Umsetzung“ geht von einer stärkeren politischen Priorisierung der Cybersicherheit aus, die jedoch nur unzureichend in die Forschungspraxis übersetzt wird. Szenario 3 „Resilientes System mit punktuellem Nachbesserungsbedarf“ beschreibt eine Zukunft, in der Cybersicherheit politisch und kulturell weitgehend verankert ist und sich der Handlungsbedarf auf punktuelle Nachbesserungen und die Anpassung an neue Herausforderungen konzentriert.

Aus den Zukunftsszenarien ergeben sich Handlungsoptionen, die von der Behebung grundlegender Sicherheitsdefizite bis zur Stärkung eines digital souveränen Forschungssystems reichen. Kurzfristig (0 bis 2 Jahre) adressieren sie vor allem den Bedarf an Transparenz über IT-Systeme sowie an koordinierten Informations-, Austausch- und Unterstützungsstrukturen einschließlich eines einrichtungsübergreifenden Lagebildes. Mittelfristig (3 bis 5 Jahre) zielen sie auf die institutionelle Verankerung von Cybersicherheit durch den Aufbau von Fachpersonal und klaren Zuständigkeiten, die Integration von Cybersicherheitskompetenzen in Forschung, Lehre und Weiterbildung sowie ein nach Schutzbedarfen differenziertes Forschungsdatenmanagement. Langfristig (5 bis 10 Jahre) betreffen sie lernfähige und souveräne Sicherheitsstrukturen sowie die strategische Gestaltung internationaler Forschungskooperationen. Risikobasierte, transparente Verfahren bringen wissenschaftliche Offenheit und Sicherheitsanforderungen in ein tragfähiges Verhältnis; souveräne digitale Infrastrukturen reduzieren Abhängigkeiten von externen Anbietern. Insgesamt verbinden die Handlungsoptionen kurzfristige Schutz- und Reaktionsfähigkeit mit und längerfristigem Kompetenzaufbau, institutioneller Lernfähigkeit und digitaler Souveränität und stärken so die Resilienz des Forschungssystems.

1 Einleitung

Der Resilienz-Check wird im Rahmen der Foresight-Aktivitäten des TAB jährlich durchgeführt und richtet den Blick auf Aspekte kritischer Infrastruktursysteme, die im wissenschaftlichen Diskurs als besonders relevant für die Stärkung von Resilienz gelten. Ziel ist es, mögliche und konsistente Zukunftsszenarien zu entwickeln und daraus tragfähige Handlungsoptionen abzuleiten. Die Auswahl des jeweiligen Schwerpunktthemas erfolgt durch die Berichterstattergruppe Technikfolgenabschätzung des Deutschen Bundestages auf Grundlage der im Resilienz-Radar und den zugehörigen Foresight-Reports identifizierten Fokusthemen. Dies stellt sicher, dass sowohl wissenschaftlich als auch politisch besonders relevante Fragestellungen adressiert werden.

Im Zentrum des Resilienz-Checks 2025/2026 steht die Cybersicherheit im Forschungsprozess, die im Foresight-Report zum Infrastruktursystem Bildung und Forschung – vor dem Hintergrund der zunehmenden Digitalisierung und Vernetzung von Forschungseinrichtungen – als relevantes Fokusthema identifiziert wurde.[1] Analysiert wurden dabei drei zentrale Handlungsdimensionen:

- der Schutz und die Integrität von Forschungsdaten,
- Cybersicherheit, Kompetenzen und Governance in Forschungseinrichtungen sowie
- digitale Souveränität und vertrauenswürdige internationale Kooperationen.

Ziel war es, plausible alternative Zukunftsszenarien zur Cybersicherheit im Forschungsprozess zu erarbeiten, damit verbundene Herausforderungen politisch einzuordnen und daraus Handlungsoptionen zur Stärkung von Cybersicherheit und Resilienz im Forschungssystem abzuleiten.

Das vorliegende Resilienz-Dossier fasst die Ergebnisse abschließend zusammen und richtet sich an Parlament, Wissenschaft, Forschungspolitik und Fachöffentlichkeit. Es dient zugleich als Grundlage für die gemeinsame öffentliche Diskussionsveranstaltung „TA im Dialog: Cybersicherheit im Forschungsprozess. Datenintegrität, Kompetenzen und sichere Kooperationen“ von TAB und dem Ausschuss für Forschung, Technologie, Raumfahrt und Technikfolgenabschätzung am 22. September 2026 im Deutschen Bundestag.

Das Resilienz-Dossier gliedert sich in drei Teile: Zunächst wird das Systembild mit den zentralen Einfluss- und Schlüsselfaktoren skizziert. Darauf aufbauend werden drei konsistente Zukunftsszenarien bis 2030+ entwickelt. Abschließend werden aus diesen Szenarien politische Handlungsoptionen zur kurz-, mittel- und langfristigen Stärkung der Resilienz abgeleitet.

Für ihre wertvollen fachlichen Beiträge im Rahmen von Interviews und Workshops danken wir den im Anhang (Kapitel 7) genannten Expert/innen. Die Verantwortung für die Auswahl, Strukturierung und Verdichtung des Materials sowie dessen Zusammenführung mit eigenen Recherchen und Analysen tragen die Verfasserinnen des Berichts.

1 https://foresight.tab-beim-bundestag.de/reports/bildung-und-forschung/ (28.8.2026)

2 Arbeitsschritte und methodische Herangehensweise

Der Resilienz-Check umfasst insgesamt drei Hauptschritte, in die je nach Themenstellung externe Expertise aus Wissenschaft, Wirtschaft, Politik und Administration sowie gegebenenfalls der Zivilgesellschaft einbezogen wird:

- *Erstellung eines Systembildes und Identifikation relevanter Einfluss- und Schlüsselfaktoren*: Im ersten Schritt wird ein Systembild des Resilienz-Check-Vertiefungsthemas entwickelt, das Einflussbereiche thematisch strukturiert und zentrale Handlungsdimensionen einbezieht, die besonders großes Resilienzpotenzial vermuten lassen. Darauf aufbauend werden relevante Einflussfaktoren identifiziert und zentrale Schlüsselfaktoren priorisiert, die sich durch eine besonders hohe Wirkungstiefe, strategische und systemische Relevanz, Hebelwirkung sowie Gestaltbarkeit auszeichnen und die künftige Entwicklung des Vertiefungsthemas maßgeblich prägen.
- *Entwicklung alternativer Zukunftsszenarien*: Im zweiten Schritt werden die identifizierten Schlüsselfaktoren in eine Wechselwirkungsmatrix überführt, mit deren Hilfe die gegenseitigen Einflussbeziehungen zwischen den Ausprägungen der Faktoren systematisch erfasst und bewertet werden. Auf dieser Grundlage werden alternative Ausprägungen der Schlüsselfaktoren zu in sich konsistenten Zukunftsszenarien verdichtet. Dieses Vorgehen ermöglicht es, unterschiedliche, jeweils plausible Entwicklungspfade sichtbar zu machen und so die Bandbreite möglicher Zukünfte systematisch zu erschließen. Aus den Szenarien lassen sich Vulnerabilitäten des Vertiefungsthemas, in diesem Fall der Cybersicherheit im Forschungsprozess, ableiten, aus denen sich Ansatzpunkte für Handlungsoptionen ergeben.
- *Ableitung von Handlungsoptionen*: Im dritten Arbeitsschritt werden auf Basis der vorangegangenen Arbeitsschritte konkrete Handlungsoptionen zur Stärkung der Resilienz mit Bezug zum Vertiefungsthema identifiziert. Die Handlungsoptionen zielen darauf ab, in den Zukunftsszenarien sichtbar gewordene Schwachstellen gezielt zu adressieren und zudem erkennbare Stärken und Entwicklungspotenziale strategisch zu nutzen, um tragfähige Strategien für die Stärkung von Resilienz zu eröffnen.

Die drei Arbeitsschritte werden durch das Zusammenspiel von Quellenanalysen, partizipativen Verfahren und ergänzender KI-Unterstützung methodisch unterstützt. Die Quellenanalysen dienen dazu, den jeweiligen Untersuchungsgegenstand systematisch zu erschließen, relevante Entwicklungen und Einflussfaktoren zu identifizieren sowie die Entwicklung von Zukunftspfaden und Handlungsoptionen fachlich zu fundieren.

Ein Partizipationsprozess bindet themenspezifisch ausgewählte Expert/innen aus Wissenschaft, Wirtschaft, Politik, Administration und gegebenenfalls Zivilgesellschaft in die drei Arbeitsschritte ein und dient vor allem der fachlichen Einordnung, Ergänzung und Validierung der Zwischenergebnisse. Hierzu werden drei aufeinander aufbauende moderierte digitale Round Tables durchgeführt: Der erste dient der gemeinsamen Kartierung des Systembildes, der Identifikation zentraler Einflussfaktoren und ihrer Wechselwirkungen sowie der Priorisierung von etwa 15 bis

20 Schlüsselfaktoren. Im zweiten Round Table werden plausible Entwicklungspfade der Schlüsselfaktoren vor dem Hintergrund aktuell diskutierter Handlungsmöglichkeiten erörtert. Der dritte Round Table dient schließlich der Prüfung der abgeleiteten Thesen und ihrer Verknüpfung mit Handlungsfeldern. Ergänzend ermöglicht die Onlineplattform discuto ausgewählten Expert/in–nen, Zukunftsentwürfe und Handlungsoptionen leitfragengestützt zu kommentieren, zu ergänzen und zu priorisieren. Diese Kombination aus direktem Austausch und strukturierter schriftlicher Rückmeldung ermöglicht die systematische Berücksichtigung differenzierter Einschätzungen und vielfältiger fachlicher Perspektiven auf das jeweilige Resilienz-Check-Vertiefungsthema.

Für die systematische Wechselwirkungsanalyse und Szenariobildung wird die Software Scenario Wizard[2] des Zentrums für interdisziplinäre Risiko- und Innovationsforschung (ZIRIUS) der Universität Stuttgart eingesetzt Stuttgart. Sie unterstützt dabei, die bewerteten Wechselwirkungen zwischen den möglichen Ausprägungen der Schlüsselfaktoren auszuwerten und zu in sich konsistenten Kombinationen möglicher zukünftiger Entwicklungen zu verdichten.

Ergänzend kommen auf Grundlage der „Leitlinien für den Einsatz generativer KI im TAB“ (TAB 2025b) KI-gestützte Werkzeuge wie Claude, ChatGPT, Mistral und Perplexity als Ideen- und Impulsgeber sowie als exploratives Analyseinstrument zum Einsatz. Sie unterstützen insbesondere die Identifikation und Strukturierung möglicher Trends und Einflussfaktoren sowie die Entwicklung und Reflexion von Zukunftspfaden. KI-generierte Ergebnisse werden dabei nicht als eigenständige wissenschaftliche Befunde behandelt, sondern durch das Projektteam kritisch geprüft, fachlich eingeordnet und mit den Ergebnissen der Quellenanalysen und des Partizipationsprozesses abgeglichen. Die abschließende Bewertung, Auswahl und Interpretation der Ergebnisse im Zuge der Erstellung des Resilienz-Dossiers erfolgt durch das Projektteam. KI dient damit der Exploration, Strukturierung und Erweiterung des Analyseraums, aber nicht der Substitution wissenschaftlicher Analyse und Bewertung.

2 https://www.scenariowizard.org/ (28.8.2026)

3 Systembild, Einfluss- und Schlüsselfaktoren

Cybersicherheit im Forschungsprozess bezeichnet die Gesamtheit politischer, organisatorischer und technischer Rahmenbedingungen, Kompetenzen und Maßnahmen, die darauf ausgerichtet sind, Forschungsdaten in ihrer Vertraulichkeit und Integrität zu schützen, IT-Infrastrukturen und digitale Arbeitsprozesse wirksam gegen digitale Angriffe, Manipulation und unbefugte Nutzung abzusichern, dadurch verursachte Störungen des Forschungsbetriebs zu vermeiden und zu bewältigen sowie die Funktionsfähigkeit, Belastbarkeit und Wiederherstellungsfähigkeit von Forschung langfristig sicherzustellen. Sie umfasst darüber hinaus die Stärkung digitaler Souveränität sowie die Schaffung sicherer und vertrauenswürdiger Rahmenbedingungen für internationale Forschungskooperationen. Diese Aufgabe betrifft die gesamte Forschungslandschaft gleichermaßen, angefangen von der universitären Forschung an Universitäten, Fachhochschulen und Universitätskliniken über die außeruniversitäre Forschung an öffentlich finanzierten Forschungseinrichtungen bis hin zur Ressort- und Drittmittelforschung (Abbildung 3.1).

Im Resilienz-Check 2025/2026 wurden auf Grundlage der Quellenanalyse und des partizipativen Austauschs mit inter- und transdisziplinären Expert/innen (Kapitel 7.1), ergänzt durch KI-gestützte Exploration, über 60 Einflussfaktoren identifiziert und daraus 19 Schlüsselfaktoren priorisiert (Abbildung 3.1).

Abbildung 3.1 Systembild und Schlüsselfaktoren

Eigene Darstellung

Als Schlüsselfaktoren werden zentrale Einflussgrößen verstanden, die die Cybersicherheit und Resilienz im Forschungsprozess maßgeblich und längerfristig prägen. Sie zeichnen sich durch

eine strategische und systemische Relevanz aus, wirken über verschiedene Phasen und Bereiche des Forschungsprozesses hinweg und können aufgrund ihrer Hebelwirkung weitere Einflussfaktoren wesentlich beeinflussen. Zugleich sind sie grundsätzlich organisatorisch, technisch oder kulturell gestaltbar. Ihre Resilienzrelevanz ergibt sich dabei nicht allein aus ihrer präventiven Wirkung gegen Cybervorfälle, sondern auch aus ihrem Beitrag zur Reaktions-, Anpassungs- und Lernfähigkeit des Forschungssystems.

Wie Abbildung 3.1. veranschaulicht, lassen sich die priorisierten Schlüsselfaktoren den drei zentralen Handlungsdimensionen von Cybersicherheit im Forschungsprozess zuordnen: dem Schutz und der Integrität von Forschungsdaten, dem Aufbau von Kompetenzen und Governance in Forschungseinrichtungen sowie der Stärkung digitaler Souveränität und vertrauenswürdiger internationaler Kooperationen. Zugleich zeigt die Grafik, dass diese Dimensionen von übergreifenden Entwicklungsdynamiken wie KI-basierter Cyberkriminalität und Cybersicherheitsregulierung geprägt sind. In das Analysespektrum der Einflussfaktoren sind dabei gesellschaftliche, wissenschaftlich-technologische, umweltbezogene, wirtschaftliche sowie politisch-rechtliche Faktoren eingeflossen (STEEPL-Kategorien), die zugleich die untere Zeile von Abbildung 3.1 bilden und als durchgängige Strukturierungslogik für die Analysen im Resilienz-Radar bzw. -Check dienen. Die Ergebnisse verdeutlichen, dass Cybersicherheit im Forschungsprozess durch ein komplexes und eng verflochtenes Zusammenspiel dieser Faktoren geprägt ist: gesellschaftlich vor allem durch das Spannungsfeld von Offenheit und Sicherheit sowie durch Kompetenzfragen, technologisch durch historisch gewachsene und komplexe IT-Systeme bei gleichzeitig hoher Innovationsdynamik, wirtschaftlich durch Fachkräftemangel und wachsende Abhängigkeiten sowie politisch bzw. rechtlich durch Fragen der digitalen Souveränität und Koordination sowie durch Regulierungsmaßnahmen. Im Folgenden werden die Einflussfaktoren skizziert und die priorisierten Schlüsselfaktoren entlang der übergeordneten thematischen Kategorien erläutert.

3.1 Gesellschaftliche Faktoren

Aus gesellschaftlicher Perspektive wird die Cybersicherheit im Forschungsprozess insbesondere durch das Spannungsverhältnis von Offenheit und Sicherheit sowie durch Kompetenz und Veränderungsfähigkeit geprägt. Zu den in dieser Perspektive identifizierten Einflussfaktoren zählen unter anderem die Arbeits- und Beschäftigungsformen, demografische Entwicklungen, Internationalisierung, die öffentliche Wahrnehmung von Cyberbedrohungen, Technikakzeptanz, Veränderungsbereitschaft sowie das Verhältnis von Wissenschaft und Gesellschaft. Aus diesem Spektrum wurden drei Faktoren aufgrund ihrer besonderen Bedeutung für die Cybersicherheit und Resilienz im Forschungsprozess als Schlüsselfaktoren priorisiert.

Die *akademische Freiheit* im Umgang mit IT-Systemen und Daten beschreibt das Spannungsverhältnis zwischen der für Forschung konstitutiven Offenheit und den Anforderungen der IT-Sicherheit. Sie wurde als Schlüsselfaktor eingestuft, weil sie strukturell und phasenübergreifend auf den gesamten Forschungsprozess wirkt und gleichzeitig durch institutionelle Regelwerke, Governancestrukturen und Sicherheitskonzepte organisatorisch gestaltbar ist. Der freie Austausch von Informationen, Daten und Erkenntnissen bildet eine wesentliche Grundlage wissenschaftlicher Zusammenarbeit und des Erkenntnisgewinns. Vor dem Hintergrund geopolitischer Spannungen, staatlicher Einflussnahme und gezielter Ausspähung gewinnt jedoch der Schutz des Forschungs-

prozesses vor unberechtigten Zugriffen und Eingriffen an Bedeutung (Allianz der Wissenschaftsorganisationen/BMBF 2025; Freyberg-Inan 2025). Akademische Freiheit steht dabei in enger Wechselwirkung mit der auch als Schlüsselfaktor eingestuften digitalen Souveränität (Kapitel 3.5), welche die eigenständige Kontrolle über Datenflüsse und Infrastrukturen zur Abwendung technologischer Fremdbestimmtheit fordert (Wittpahl 2016). Für die Cybersicherheit im Forschungsprozess ergibt sich daraus ein zentraler Zielkonflikt: Sicherheitsmaßnahmen müssen Offenheit, Autonomie und internationale Zusammenarbeit ermöglichen und zugleich Forschungsdaten, Infrastrukturen und wissenschaftliche Integrität wirksam schützen.

Die *digitale und KI-Kompetenz* von Forschenden und Beschäftigten umfasst das Verständnis für Funktionsweise, Chancen und Risiken digitaler Werkzeuge und KI-Anwendungen ebenso wie das Verständnis ihrer rechtlichen, ethischen und sicherheitsrelevanten Implikationen. Ihre Bedeutung als Schlüsselfaktor ergibt sich daraus, dass sie weit über rein technisches Bedienwissen hinausgeht und die Fähigkeit umfasst, digitale Technologien zur Wissensschöpfung und Problemlösung sicher, verantwortungsvoll und reflektiert einzusetzen und dabei Datenschutz, Informationssicherheit, wissenschaftliche Integrität und ethische Standards zu berücksichtigen (Fan/Li 2025). In der Wissenschaft gewinnt in diesem Zusammenhang das Konzept der Digital Fluency an Bedeutung, das auf das synergetische Zusammenspiel von Wissen, Fertigkeiten und Einstellungen zur Erzielung verlässlicher Forschungsergebnisse in einer digital transformierten Umgebung abstellt (Ochôa et al. 2026). Als Schlüsselfaktor weist die digitale und KI-Kompetenz eine sehr hohe Hebelwirkung auf, da sie mehrere Dimensionen der Cybersicherheit unmittelbar beeinflusst. Erstens trägt der Kompetenzaufbau zur Risikominimierung und Prävention bei (Adamu/Chaudhry 2026). Zweitens bildet der Kompetenzaufbau zunehmend eine Voraussetzung für wissenschaftliche Integrität und einen verantwortungsvollen KI-Einsatz. Dazu gehört, algorithmische Verzerrungen (Bias), Datenqualität und Grenzen KI-generierter Ergebnisse kritisch zu beurteilen sowie Verantwortung und Interpretationshoheit beim Menschen zu belassen (Human-in-the-Loop-Ansatz) (Nöhmke et al. 2026). Drittens stärkt digitale Kompetenz die Handlungsfähigkeit und digitale Souveränität von Forschenden und Beschäftigten, indem sie einen sicheren und selbstbestimmten Umgang mit digitalen Werkzeugen, Daten und KI-Systemen ermöglicht. Zugleich ist der Schlüsselfaktor gezielt beeinflussbar: Kontinuierliche, adaptive, verhaltensbasierte Lernumgebungen und projektbezogene Trainings können Kompetenzen wirksamer und nachhaltiger aufbauen als punktuelle, statische Formate und so dazu beitragen, die Resilienzlücke in der Cybersicherheit wirksam zu schließen (Adamu/Chaudhry 2026). Wenn Forschende und Beschäftigte digitale Werkzeuge nicht als Blackbox, sondern als gestaltbare Instrumente begreifen, kann dies zu einer resilienten Forschungskultur beitragen, die wissenschaftliche Exzellenz schützt und die technologische Autonomie der Wissenschaft gegenüber externer Einflussnahme und Cyberbedrohungen stärkt (Fan/Li 2025; Nöhmke et al. 2026).

Das *Sicherheitsbewusstsein* (Security Awareness) (Goliath et al. 2026) und die Risikowahrnehmung von Forschenden und Beschäftigten wurden als Schlüsselfaktor identifiziert, da der Faktor Mensch nach wie vor als das kritischste Glied in der Cybersicherheitskette gilt (Adamu/Chaudhry 2026). In einer digitalen Landschaft, in der schätzungsweise 82 % aller Sicherheitsverletzungen auf menschliches Fehlerverhalten oder Social Engineering, also der gezielten Manipulation von Personen, um sie zur Preisgabe sensibler Informationen oder zu sicherheitskritischen Handlungen zu bewegen, zurückzuführen sind, ist die Stärkung der individuellen Urteilskraft eine strategische Notwendigkeit für die individuelle, institutionelle und nationale Sicherheit (Adeshola/Oluwajana 2025). Ein ausgeprägtes Risikobewusstsein stärkt dabei insbesondere auch die Präven-

tion, indem es über rein theoretisches Wissen hinausgeht und die Entwicklung von Sicherheitsgewohnheiten und -reflexen betrifft.

3.2 Technologische Faktoren

Aus technologischer Perspektive wird die Cybersicherheit im Forschungsprozess insbesondere durch das Spannungsverhältnis zwischen historisch gewachsenen, heterogenen und komplexen IT-Infrastrukturen des Forschungssystems und einer hohen Innovationsdynamik geprägt. Zu den in diesem Zusammenhang identifizierten Einflussfaktoren zählen unter anderem Datenverschlüsselung und Kryptografie sowie der Vernetzungsgrad von Geräten und Systemen (IoT/Edge Computing). Aus dem Spektrum der technologischen Einflussfaktoren wurden acht Faktoren aufgrund ihrer besonderen Bedeutung für die Cybersicherheit im Forschungsprozess als Schlüsselfaktoren priorisiert. Die vergleichsweise hohe Anzahl an Schlüsselfaktoren unterstreicht die zentrale Bedeutung technologischer Entwicklungen und Infrastrukturen für die Resilienz des Forschungssystems.

Die *Fähigkeit zur Angriffserkennung* wurde ausgewählt, da sie die Detektions- und Lernfähigkeit von Forschungseinrichtungen stärkt und durch geeignete Monitoringsysteme, eine verlässliche Datenbasis sowie entsprechende Analyse- und forensische Kompetenzen gezielt aufgebaut werden kann. Die frühzeitige Detektion von Cyberangriffen und eine sofortige Reaktion darauf gewinnen im Kontext von sich verändernden Cyberkriminalitätslandschaften und der zunehmenden Nutzung von KI durch Cyberkriminelle an Bedeutung (BSI 2026d). Nach Einschätzung des Bundesamtes für Sicherheit in der Informationstechnik (BSI 2026c) besteht in vielen KRITIS-Sektoren und Branchen insbesondere bei Systemen zur Angriffserkennung weiterhin größerer Nachholbedarf, der auch für Forschungseinrichtungen relevant ist. Institutionenübergreifende Auswertungs- und Austauschstrukturen können zudem dazu beitragen, Erkenntnisse aus Sicherheitsvorfällen systematisch zu teilen, ein gemeinsames Lagebild zu entwickeln und Präventions- und Resilienzmaßnahmen kontinuierlich zu verbessern.

Die *Komplexität und Heterogenität* der IT-Infrastrukturen zählt zu den Schlüsselfaktoren, weil sie die Absicherbarkeit der gesamten IT-Landschaft strukturell und bereichsübergreifend beeinflusst und damit eine hohe systemische Relevanz und Hebelwirkung besitzt. Forschungseinrichtungen verfügen meist über heterogene, komplexe und verzweigte IT-Infrastrukturen, was sie besonders verwundbar macht (Becker/Aghaye 2022; Plattner 2025). Forschungseinrichtungen verfügen meist über heterogene, komplexe und verzweigte IT-Infrastrukturen, was sie besonders verwundbar macht (Becker/Aghaye 2022; Plattner 2025). Teilweise werden IT-Systeme dezentral, beispielsweise auf Lehrstuhlebene, verwaltet und durch zusätzliche Systeme für einzelne Förderprogramme oder Projekte ergänzt (Becker/Aghaye 2022). So können im Rahmen spezifischer Projekte z.B. vernetzte Forschungsgeräte für Labore angeschafft worden sein, die ein potenzielles Einfallstor für Cyberangriffe darstellen, weil sie nicht in die übergreifenden Sicherheitsstrukturen der Universität eingebunden und entsprechend unzureichend gesichert sind (Becker/Aghaye 2022). Verbesserungen in der Systemarchitektur wirken sich positiv auf zahlreiche nachgelagerte Sicherheitsaspekte aus.

Die *Nutzung von externen IT-Infrastrukturen, Geräten und Diensten* wurde als Schlüsselfaktor eingestuft, weil sie die Angriffsfläche, externe Abhängigkeiten und zugleich die Möglichkeiten zur

Kontrolle und Gestaltung der IT-Sicherheit im Forschungsprozess wesentlich beeinflusst. Mit der zunehmenden Nutzung von Cloudinfrastrukturen sowie extern bezogener Software einschließlich Open-Source-Komponenten gewinnen insbesondere Risiken durch Drittanbieter und Softwarelieferketten an Bedeutung. Diese sind meist schwer zu überblicken, zudem sind die Kontrollmöglichkeiten über Cybersicherheitsmaßnahmen bei Drittanbietern häufig gering (WEF 2026). Risiken durch Drittanbieter können Forschungseinrichtungen sowohl direkt als Ziel gezielter Angriffe als auch indirekt betreffen, wenn beispielsweise weit verbreitete Software oder zentrale Dienste angegriffen werden. Auch wenn in Deutschland viele Forschungseinrichtungen, vor allem Hochschulen, nach wie vor On-Premise-Systeme betreiben, hat die Nutzung externer Dienste in den letzten Jahren zugenommen (ATHENE 2025). Für ein wirksames Risikomanagement und eine stärkere digitale Souveränität (Kapitel 3.4) ist es daher entscheidend, bestehende Abhängigkeiten, eingesetzte Komponenten und deren Lieferketten zu kennen und die Cybersicherheitsvorkehrungen der genutzten Drittanbieter angemessen bewerten zu können. Dabei spielt auch eine hinreichende Trennung zwischen privat genutzten Systemen und Diensten und solchen der Forschungseinrichtung eine Rolle (Plattner 2025).

Der technische *Zustand und Lebenszyklus von IT-Systemen* gilt als Schlüsselfaktor mit hoher Wirkungstiefe, da veraltete Systeme und unzureichendes Patchmanagement im Sinne einer zeitnahen Aktualisierung von Software zur Behebung von Sicherheitslücken die strukturelle Vulnerabilität der gesamten Forschungsinfrastruktur unmittelbar bestimmen, zugleich aber durch konsequentes IT-Lebenszyklusmanagement gestaltbar sind. Forschungseinrichtungen sind häufig durch historisch gewachsene IT-Systeme geprägt, die zahlreiche veraltete Hard- und Softwareelemente, sogenannte Legacysysteme, umfassen, für die teilweise keine Sicherheitsupdates mehr bereitgestellt werden (ATHENE 2025). Durch den Wegfall von regelmäßigen Updates für ältere Systeme werden Schwachstellen nicht mehr behoben, wodurch Legacysysteme zu einem besonders attraktiven Ziel für Cyberangriffe werden. Veraltete Systeme sind zudem häufig nicht kompatibel mit neuen IT-Sicherheitssystemen, sodass Lücken im Sicherheitsmanagement entstehen (Becker/Aghaye 2022). Dennoch bleiben veraltete IT-Systeme häufig im Einsatz, da die Anschaffung neuer Systeme erhebliche Kosten verursacht und neben Anschaffungskosten teilweise auch Kosten für Integration, Schulungen und Ähnliches anfallen. Zudem können spezialisierte Anwendungen teilweise nur auf spezifischen Legacyplattformen ausgeführt werden (Geißler 2025). Fehlt eine ausreichende Übersicht über die eingesetzte Hard- und Software, erschwert dies ein effektives Lebenszyklusmanagement. Begünstigt wird dies durch die – auch als Schlüsselfaktor eingestuften – komplexen und heterogenen IT-Strukturen von Forschungseinrichtungen. Forschungsspezifische Beispiele sind unter anderem Laborgeräte sowie andere spezialisierte Geräte (ATHENE 2025). Auch die zeitnahe Deaktivierung von Benutzerkonten nach dem Weggang von Mitarbeitenden ist von Bedeutung, da nicht mehr benötigte oder unzureichend verwaltete Zugänge ein Sicherheitsrisiko darstellen und für unbefugte Zugriffe auf IT-Systeme und Forschungsdaten genutzt werden können (Becker/Aghaye 2022).

Die *Schutzbedarfe von Forschungsdaten* sind aufgrund der stetig wachsenden Menge und Bedeutung von Forschungsdaten sowie der besonderen Anforderungen an ihre Speicherung, Verarbeitung und langfristige Verfügbarkeit ein zentraler Schlüsselfaktor. Forschungseinrichtungen verfügen dabei neben einer große Menge an personenbezogenen Daten zu Studierenden, Forschenden und Verwaltungspersonal insbesondere über große Bestände an Forschungsdaten (Plattner 2025), die teils hohe Schutzbedarfe aufweisen und gleichzeitig für die wissenschaftliche Nutzung verfügbar und zugänglich sein müssen. Diese Schutzbedarfe sind in hohem Maße kontextsensitiv und spiegeln

jeweils spezifische Bedarfe des Forschungsprozesses wider, wie den Umgang mit großen und heterogenen Datensätzen sowie deren langfristige Archivierung und wissenschaftliche Nutzbarkeit. Verschärft wird diese Herausforderung durch zwei parallele Entwicklungen: Zum einen wachsen im Zuge der Digitalisierung die im Forschungssystem produzierten und genutzten Datenmengen immer schneller an (Forschungsdaten.info o.J.), wodurch auch die Herausforderungen für den Langzeitdatenerhalt steigen. Zum anderen verändern sich mit der zunehmenden Nutzung von KI die Anforderungen an die Bereitstellung und Nutzung von Daten: Über ihre langfristige Archivierung und Analyse hinaus dienen Forschungsdaten zunehmend auch als Trainings- und Grundlagendaten für die Entwicklung und Anwendung von KI- Modellen. Dies stellt erhöhte Anforderungen an Datenaufbereitung und ist mit Fragen nach rechtlichen Rahmenbedingungen und Schutzbedarfen verbunden (WR 2025a). Die Komplexität der Schutzbedarfe unterschiedlicher Forschungsdaten dürfte durch einen möglicherweise verstärkten Sicherheitsfokus in der Forschung weiter an Relevanz gewinnen (Plattner 2025). Dies stellt erhöhte Anforderungen an Datenaufbereitung und ist mit Fragen nach rechtlichen Rahmenbedingungen und Schutzbedarfen verbunden (WR 2025a). Die Komplexität der Schutzbedarfe unterschiedlicher Forschungsdaten dürfte durch einen möglicherweise verstärkten Sicherheitsfokus in der Forschung weiter an Relevanz gewinnen (Plattner 2025).

Die *Innovationsgeschwindigkeit*, mit der neue Technologien, Anwendungen und IT-Architekturen entwickelt und in Forschungseinrichtungen eingeführt werden, wurde als Schlüsselfaktor bewertet, da sie eine hohe Wirkungstiefe und strategische Relevanz besitzt: Schnelle Innovationszyklen können Sicherheitskonzepte, Prüfprozesse und den Kompetenzaufbau von Forschenden und Beschäftigten überholen und temporäre Sicherheitslücken erzeugen. Umso wichtiger ist es, Sicherheit von Beginn an (Security by Design) in Entwicklungs- und Einführungsprozesse zu integrieren und kontinuierlich mit der Technologie weiterzuentwickeln. Neue Technologien und Anwendungen müssen daher kontinuierlich erfasst und in die Gesamtarchitektur eingebettet werden, was angesichts der Innovationsgeschwindigkeit eine kontinuierliche Herausforderung darstellt. Sie weisen gleichzeitig häufig höhere standardmäßig implementierte Sicherheitsstandards auf, die zu einer Verbesserung der Sicherheit insgesamt beitragen können (ATHENE 2025). Voraussetzung dafür ist, dass geeignete Sicherheitskonzepte vorliegen und sicherheitsrelevante Aspekte bei der Einführung innovativer Lösungen systematisch geprüft und berücksichtigt werden. Erschwert werden die Erfassung und Sicherheitsprüfung neuer Anwendungen und Technologien jedoch unter anderem durch deren eigenständige, nicht abgestimmte Nutzung durch Mitarbeitende, wodurch Schatten-IT entstehen kann. Wenn offiziell verfügbare Systeme spezifische Anforderungen nicht erfüllen oder als unpraktisch erlebt werden, wird häufig zu anderen, auf dem Markt verfügbaren Lösungen gegriffen (Schuller 2026). Die Innovationsgeschwindigkeit wirkt damit als ambivalenter Faktor: Sie treibt einerseits Sicherheitsverbesserungen durch neue Konzepte voran, erhöht andererseits aber das Risiko, unkontrollierter Parallelstrukturen, wenn Einführungs- und Prüfprozesse mit der Innovationsgeschwindigkeit nicht Schritt halten können.

Sowohl der Verbreitungsgrad von *KI in der Cyberkriminalität* als auch der Verbreitungsgrad von *KI in der Cybersicherheit* im IT-Betrieb wurden als Schlüsselfaktoren priorisiert, da sie eine hohe Hebelwirkung auf das künftige Kräfteverhältnis zwischen offensiven und defensiven Fähigkeiten besitzen und zugleich strategisch hochrelevant für die langfristige Sicherheitslage von Forschungseinrichtungen sind. Der Einsatz von KI in der Cyberkriminalität nimmt zu und spielt in allen Bereichen der Cyberkriminalität eine Rolle. KI ermöglicht einerseits technisch weniger versierten Akteuren Cyberangriffe zu begehen, stärkt aber auch hoch versierte Akteure, vor allem hinsichtlich Effizienz und Schnelligkeit. Beispielsweise kann der Versand von authentisch wirkenden

Phishingmails durch die Nutzung von KI weitaus schneller und in größerem Ausmaß erfolgen (BKA 2026). Auch die Detektion von Schwachstellen kann KI maßgeblich vereinfachen, wie Claude Mythos, ein auf Cybersicherheitsaufgaben spezialisiertes KI-Modell des US-Unternehmens Anthropic, gezeigt hat. Das Modell kann zum einen bislang unbekannte Schwachstellen in Software identifizieren, und damit sowohl zur Stärkung der Cybersicherheit beitragen als auch neue Missbrauchsrisiken eröffnen (BSI 2026b). Darüber hinaus schafft die Nutzung von KI selbst neue Angriffsflächen für Cyberkriminalität, beispielsweise durch direkte oder indirekte Prompt Injections, bei denen versteckte Befehle in Prompts die KI anweisen maliziöse Aktivitäten auszuführen (BKA 2026; Check Point 2026). Auch die zunehmende Verbreitung von KI-Agenten stellt die Cybersicherheit vor neue Herausforderungen (WEF 2026). Dies verdeutlichen Vorfälle, bei denen KI-Agenten vorgesehene technische Begrenzungen überwinden und auf nicht für sie bestimmte Systeme oder Ressourcen zugreifen können. Ein Vorfall vom Juli 2026, bei dem ein KI-System von OpenAI eine eigentlich abgeschottete Testumgebung (Sandbox) verließ und Zugriff auf Systeme eines anderen Unternehmens erlangte, verdeutlicht das potenzielle Risiko zunehmend autonom agierender KI-Systeme und die damit verbundenen neuen Anforderungen an deren sichere Einbettung und Kontrolle (BSI 2026d). Auf der anderen Seite eröffnet KI erhebliche Innovationspotenziale für die Verbesserung der Cybersicherheit. Gerade ihre Fähigkeit, komplexe Muster zu erkennen und Schwachstellen zu identifizieren, kann gezielt genutzt werden, um Software automatisiert zu prüfen und Sicherheitslücken schneller zu erkennen und zu schließen (BSI 2026b). KI-gestützte Systeme können zudem die Angriffserkennung, Analyse und Bewältigung von Sicherheitsvorfällen (Incident Response) verbessern und zeitaufwändige Aufgaben wie Protokollanalysen oder die Erstellung von Complianceberichten erheblich beschleunigen. In der Cyberabwehr ist KI bereits verbreitet und wird vor allem zur Phishingerkennung sowie zur Erkennung von und Reaktion auf Angriffsversuche und Anomalien genutzt (WEF 2026). Für Forschungseinrichtungen liegt das Potenzial darin, Cybersicherheit schneller, skalierbarer und adaptiver zu gestalten und begrenzte personelle Ressourcen gezielter einzusetzen.

3.3 Umweltbezogene Faktoren

Aus umweltbezogener Perspektive wird die Cybersicherheit im Forschungsprozess wesentlich durch die wachsende Ressourcenabhängigkeit digitaler IT-Systeme und Infrastrukturen geprägt. Zu den relevanten Einflussfaktoren zählen insbesondere der steigende Energiebedarf, wachsende Nachhaltigkeitsanforderungen sowie physische Umwelt- und Versorgungsrisiken. Besonders deutlich wird dies am massiven Energiebedarf von KI-Systemen, der sich bis 2030 verdoppeln könnte und Energie zu einer strategischen Steuerungsvariablen für den IT-Betrieb macht (Kracke 2026; Kranzlmüller/Grimshaw 2026). Wachsende Anforderungen bezüglich des digitalen CO_2-Fußabdrucks und des E-Waste-Managements zwingen dabei zu einer ökologischen Transformation der Infrastruktur, während geopolitische Spannungen, Rohstoffverknappung und Umweltereignisse die Stabilität globaler Lieferketten für Hardware gefährden (Lemke 2026). In Bezug auf die Cybersicherheit im Forschungsprozess bildet diese ökologische und energetische Stabilität die physische Basis der Resilienz: Nur wenn die zugrunde liegende Infrastruktur gegenüber Umwelt und Versorgungsrisiken abgesichert ist, können die kontinuierliche Verfügbarkeit von Rechenkapazitäten sowie die Integrität und Sicherheit von Forschungsdaten dauerhaft gegen systemische Unterbrechungen geschützt werden (TAB 2024).

Keiner der identifizierten umweltbezogenen Einflussfaktoren wurde als Schlüsselfaktor eingestuft. Dies lässt sich damit erklären, dass sie zwar relevante Rahmenbedingungen für den Betrieb und die Aufrechterhaltung digitaler Infrastrukturen darstellen, ihre Wirkung auf die Cybersicherheit im Forschungsprozess im engeren Sinne jedoch eher indirekt bleibt. Anders als die im Zusammenhang mit gesellschaftlichen, technologischen, wirtschaftlich sowie politisch-rechtlichen Perspektiven ausgewählten Schlüsselfaktoren sind die umweltbezogenen Faktoren kaum durch Forschungseinrichtungen selbst gestaltbar, sondern hängen primär von externen, gesamtgesellschaftlichen Entwicklungen ab.

3.4 Wirtschaftliche Faktoren

Aus wirtschaftlicher Perspektive wird die Cybersicherheit im Forschungsprozess vor allem durch Einflussfaktoren geprägt, die mit dem Fachkräftemangel, den verfügbaren finanziellen Ressourcen und wachsenden wirtschaftlichen Abhängigkeiten zusammenhängen. Zu den identifizierten Einflussfaktoren zählen unter anderem die Abhängigkeit von Drittmittel- und Industriekooperationen, die Attraktivität des Forschungsstandortes Deutschland, Finanzierungsbedingungen, Folgekosten von Cybervorfällen, die Professionalisierung der Cyberkriminalität sowie die Versicherbarkeit von Cyberrisiken. Aus diesem Spektrum wurden drei Faktoren aufgrund ihrer besonderen Bedeutung für die Cybersicherheit im Forschungsprozess als Schlüsselfaktoren priorisiert.

Die Abhängigkeit von *monopolistischen IT- und Clouddienstleistern* wurde als Schlüsselfaktor bewertet, da sie über Lock-in-Effekte und potenziell systemische Auswirkungen bei Sicherheitsvorfällen eine hohe strategische Relevanz für die digitale Souveränität (Kapitel 3.5) besitzt und gleichzeitig zum Beispiel über Beschaffungsentscheidungen grundsätzlich gestaltbar bleibt. In digitalen Märkten führen selbstverstärkende Netzwerkeffekte sowie massive Skalen- und Verbundvorteile zur Herausbildung monopolähnlicher Anbieterstrukturen und globaler Quasistandards, die derzeit primär von außereuropäischen Hyperscalern dominiert werden (Christ 2025). Diese Marktmacht führt zu erheblichen Pfadabhängigkeiten und hohen Wechselkosten (TAB 2025a), die durch eine tiefe Integration in proprietäre Plattformdienste sowie eine oft fehlende Portabilität von Daten und Workloads strategisch verstärkt werden (Czachowski 2026). Vor dem Hintergrund geopolitischer Instabilitäten resultiert daraus ein existenzielles Risiko, da der Zugriff auf essenzielle Infrastrukturen und Dienste durch externe politische Entscheidungen oder Sanktionen kurzfristig unterbunden werden kann (Christ 2025). Die Gestaltbarkeit dieses Schlüsselfaktors liegt in einer risikobasierten Cloud Governance. Durch die gezielte Nutzung offener Standards, die Etablierung von Multicloudstrategien sowie die Definition von verbindlichen Beschaffungsstandards kann die technische Alternativfähigkeit und operative Resilienz institutionell gestärkt werden (Czachowski 2026). Die Reduktion einseitiger Providerabhängigkeiten bietet letztlich eine wichtige Säule für die Cybersicherheit im Forschungsprozess, da nur durch technologische Alternativfähigkeit die dauerhafte Integrität und Verfügbarkeit wissenschaftlicher Datenbestände gesichert werden kann.

Die *Fachkräftesituation im Bereich Cybersicherheit* gilt als Schlüsselfaktor mit besonders hoher Hebelwirkung, da der Mangel an spezialisiertem Personal den Aufbau interner Sicherheitskompetenzen in nahezu allen anderen Handlungsfeldern begrenzt und damit querschnittlich auf die gesamte Sicherheitsarchitektur einer Forschungseinrichtung wirkt. Der globale Mangel an

Cybersicherheitsfachkräften wird auf rund 4,8 Millionen geschätzt (Schneider et al. 2025); auch in Deutschland bleibt der IT-Fachkräftemangel mit zuletzt rund 109.000 unbesetzten Stellen hoch, wobei der Bereich Cybersicherheit besonders betroffen ist (Bitkom 2026). Diese Knappheit führt zu einer dauerhaften Überlastung des vorhandenen Personals, was die operative Resilienz und die Fähigkeit zur zeitnahen Reaktion auf Cybersicherheitsvorfälle deutlich beeinträchtigt. Die besondere Kritikalität dieses Faktors ergibt sich aus der rasanten Entwicklungsdynamik des Cybersicherheitswissens, dessen Halbwertszeit insbesondere im taktischen Bereich oft nur wenige Monate beträgt (Bitkom 2026). In der Praxis erweist sich der Ressourcenmangel häufig als zentrales Umsetzungshindernis für notwendige Sicherheitsmaßnahmen und regulatorische Anforderungen wie die Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie)[3] zur Netzwerk- und Informationssicherheit (Döttl 2025). In spezialisierten Bereichen wie dem Betrieb von Rechenzentren ist zudem der Aufbau von Hybridkompetenzen erforderlich, die tiefes technisches Fachwissen mit digitaler Souveränität als Schlüsselfaktor (im Sinne von Handlungsfähigkeit und Unabhängigkeit von einzelnen außereuropäischen Anbietern; Kapitel 3.5) verknüpfen (Kanagalingam/Loncar 2026). Eine tragfähige Fachkräftebasis bildet daher das personelle Fundament der Cybersicherheit im Forschungsprozess, da technologische Schutzmaßnahmen ohne die notwendige Expertise für deren Konfiguration, Überwachung und kontinuierliche Weiterentwicklung ihre Wirksamkeit verlieren.

Der wirtschaftliche *Wert von Forschungsdaten* und geistigem Eigentum wurde als Schlüsselfaktor identifiziert, weil er unmittelbar mit den strategischen Zielen und Wissensbeständen von Forschungseinrichtungen verbunden ist: Forschungsdaten stellen zunehmend eine zentrale Ressource des Forschungssystems dar, deren wissenschaftlicher und wirtschaftlicher Wert sich teilweise erst langfristig durch Zitationen, Metaanalysen oder die Nachnutzung in der datengetriebenen Forschung realisiert (Schiffner/Kiesler o. J.). Da die Erhebung hochwertiger Daten, insbesondere in den Natur- und Lebenswissenschaften, enorme öffentliche Fördermittel und zeitliche Ressourcen bindet, stellt deren Integrität und Verfügbarkeit ein besonders schützenswertes Gut dar. Dabei bilden Forschungsdaten eine wichtige Grundlage zukünftiger Innovationen sowie des Trainings von KI- und Deep-Learning-Modellen (Herres-Pawlis et al. 2022). Mit diesem wachsenden wissenschaftlichen und wirtschaftlichen Wert steigt zugleich die Attraktivität von Forschungseinrichtungen als Angriffsziel für Akteure der Cyberkriminalität: Angriffe wie Spionage oder Ransomwareattacken gefährden nicht nur den wissenschaftlichen Vorsprung, sondern bedrohen auch die globale Wettbewerbsfähigkeit und materielle Existenz von Forschungseinrichtungen (Schneider et al. 2025). Damit bildet der wirksame Schutz dieses ökonomischen und intellektuellen Kapitals den Kern der Cybersicherheit im Forschungsprozess, um die technologische Souveränität und die Validität wissenschaftlicher Erkenntnisse gegen externe Einflussnahme abzusichern.

3.5 Politische und rechtliche Faktoren

Aus politischer und rechtlicher Perspektive wird die Cybersicherheit im Forschungsprozess vor allem durch Fragen der digitalen Souveränität, der institutionellen Koordination sowie durch regulatorische Rahmenbedingungen geprägt. Zu den identifizierten politischen Einflussfaktoren zählen unter anderem nationale Cybersicherheitsstrategien, öffentliche Förder- und Subventions-

3 Richtlinie (EU) 2022/2555 vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)

politik sowie die politische Priorisierung von Cybersicherheit. Das Spektrum rechtlich relevanter Einflussfaktoren umfasst vor allem datenschutzrechtliche Vorgaben, Haftungsregelungen, internationale Rechtskonflikte sowie die Regulierung von Cloud-, Dritt- und KI-Anbietern. Aus dem Spektrum der politischen Einflussfaktoren wurden drei Faktoren und aus dem der rechtlichen Einflussfaktoren ein weiterer Faktor aufgrund ihrer besonderen Bedeutung für die Cybersicherheit und Resilienz im Forschungsprozess als Schlüsselfaktoren priorisiert.

Die *digitale Souveränität* bezeichnet die Fähigkeit von Institutionen und Individuen, in der digitalen Welt selbstbestimmt und sicher zu handeln sowie die Kontrolle über Daten, digitale Vermögenswerte, IT-Infrastrukturen und Schlüsseltechnologien zu behalten (Kranich 2026). Als Schlüsselfaktor besitzt sie angesichts wachsender externer Abhängigkeiten und geopolitischer Risiken eine hohe strategische Relevanz und Hebelwirkung. Einer ihrer zentralen Treiber ist die auch als Schlüsselfaktor bewertete Abhängigkeit von monopolistischen, überwiegend außereuropäischen IT- und Clouddienstleistern (Kapitel 3.4) kann durch proprietäre Strukturen und Lock-in-Effekte die informationelle Selbstbestimmung und operative Handlungsfähigkeit einschränken sowie bei Sicherheitsvorfällen systemische Auswirkungen entfalten (Sitarska et al. 2026). Zugleich ist digitale Souveränität etwa durch Beschaffungsentscheidungen und die strategische Gestaltung technologischer Abhängigkeiten politisch beeinflussbar. Für die Forschungssicherheit ist sie insbesondere deshalb relevant, weil die Verfügbarkeit, Integrität und Vertraulichkeit von Forschungsdaten zunehmend von digitalen Infrastrukturen und technologischen Diensten abhängen, die außerhalb der unmittelbaren Kontrolle von Forschungseinrichtungen liegen. Mit der zunehmenden Nutzung von KI-Systemen erweitert sich die Souveränitätsfrage zudem auf den Zugang zu und die Kontrolle über KI-Modelle, Trainingsdaten und Recheninfrastrukturen (WR 2026). Die damit verbundenen technologischen Abhängigkeiten können nicht nur Cyber- und Ausfallrisiken erhöhen, sondern auch unerwünschten Daten- und Wissenstransfer sowie externe Einflussnahme begünstigen. Entsprechend verknüpft die Europäische Union in ihrer aktuellen Forschungs- und Infrastrukturpolitik digitale bzw. Datensouveränität ausdrücklich mit Forschungssicherheit und fordert eine vertrauenswürdige, sichere und souveräne Forschungsinfrastruktur. Digitale Souveränität ist damit weniger als vollständige technologische Unabhängigkeit denn als Fähigkeit zu verstehen, kritische digitale Ressourcen verlässlich zu kontrollieren und auch unter geopolitisch veränderten Bedingungen handlungsfähig zu bleiben (Ananda et al. 2026).

Die *internationale Wissenschaftspolitik* gilt als Schlüsselfaktor, weil sie kontextsensitiv die für Forschung typische internationale Zusammenarbeit abbildet und durch strategische Partnerschaften und Förderprogramme bestimmt, mit welchen Ländern und Akteuren unter welchen Sicherheitsanforderungen kooperiert wird; ein Umstand mit unmittelbarer systemischer Bedeutung für die Absicherung internationaler Forschungskooperationen. Vor dem Hintergrund zunehmender geopolitischer Spannungen und des globalen Wettbewerbs um strategische Technologien gewinnt die sicherheitspolitische Dimension internationaler Forschungskooperationen an Bedeutung (OECD 2025). Für die Cybersicherheit von Forschungsprozessen ist dies insbesondere relevant, weil internationale Kooperationen den grenzüberschreitenden Austausch von Forschungsdaten, digitalen Diensten, Software, Zugangsberechtigungen und wissenschaftlichem Know-how voraussetzen und dadurch potenzielle Angriffs- und Einflussvektoren über institutionelle und nationale Grenzen hinweg entstehen. Die Europäische Union berücksichtigt diese Risiken im Rahmen ihrer Forschungssicherheitspolitik und verweist insbesondere auf unerwünschten Wissenstransfer, ausländische Einflussnahme und Cyberbedrohungen (Rat der Europäischen Union 2024). Damit beeinflusst die internationale Wissenschaftspolitik unmittelbar die sicherheitsre-

levanten Rahmenbedingungen für die digitale und grenzüberschreitende Organisation von Forschungsprozessen.

Die *politische Koordination zwischen Bund, Ländern und EU* wurde als Schlüsselfaktor identifiziert, weil sie in besonderem Maße systemische Bedeutung besitzt: Fragmentierte Zuständigkeiten zwischen Bund, Ländern, Hochschulleitungen, Rechenzentren und Drittmittelgebern wirken bereichs- und ebenenübergreifend auf die Umsetzung einheitlicher Cybersicherheitsmaßnahmen und begrenzen so deren Wirksamkeit (HRK 2025; Naß et al. 2026). Zugleich ist der Grad der Abstimmung zwischen den beteiligten Akteuren institutionell gestaltbar und entfaltet dadurch eine erhebliche Hebelwirkung auf nachgelagerte Wirkungszusammenhänge. Aktuelle Untersuchungen weisen auf unterschiedliche Umsetzungsstände und Unterstützungsstrukturen in den Bundesländern sowie auf die hohe Komplexität der ineinandergreifenden europäischen, bundes- und landesrechtlichen Vorgaben hin (Bretschneider et al. 2020; Kreutzer et al. 2026; Naß et al. 2026). Damit kann eine unterschiedliche Ausgestaltung und Umsetzung von Cybersicherheitsanforderungen zwischen Ländern und Hochschulen entstehen, was die Herstellung eines konsistenten Sicherheitsniveaus im Wissenschaftssystem erschwert. Politische Koordination und klare Zuständigkeiten stellen damit eine zentrale Voraussetzung für die übergreifende Wirksamkeit von Cybersicherheitsmaßnahmen im Wissenschaftssystem dar.

Die *Cybersicherheitsregulierung* (zum Beispiel NIS-2-Richtlinie und nationale Umsetzungsvorschriften wie das BSI-Gesetz[4]) wurde als Schlüsselfaktor eingestuft, da sie durch verbindliche Mindestanforderungen an IT-Sicherheit, Risikomanagement und Resilienz eine hohe Wirkungstiefe und strategische Relevanz für das gesamte Sicherheitsniveau von Forschungseinrichtungen entfaltet. Zugleich ist ihre Umsetzung in hohem Maße durch die Ausgestaltung entsprechender Compliance-, Governance- und Sicherheitsstrukturen innerhalb der Einrichtungen beeinflussbar (Christen 2020). Dies betrifft die Beschaffung, IT-Infrastrukturen, die Cloud- und Softwarenutzung, Forschungskooperationen, Meldewege und die Organisation von Sicherheitsverantwortung. Für das Forschungssystem ist dabei besonders relevant, dass regulatorische Anforderungen die unterschiedlichen Risikoprofile, institutionellen Strukturen und Ressourcen von Hochschulen und Forschungseinrichtungen berücksichtigen, ohne dabei ein angemessenes Sicherheitsniveau zu unterschreiten. Auf europäischer Ebene ist die NIS-2-Richtlinie von besonderer Bedeutung für ein hohes Cybersicherheitsniveau in der EU und regelt die Netzwerk- und Informationssicherheit sowie Berichtspflichten. Sie gilt nicht direkt und muss deshalb in nationales Recht umgesetzt werden (Stein et al. 2025). Mit der Umsetzung der Richtlinie durch das nationale BSI-Gesetz sind Forschungseinrichtungen, die angewandte Forschung oder experimentelle Entwicklung primär für kommerzielle Zwecke betreiben, seit 2025 von einer Meldepflicht für Sicherheitsvorfälle betroffen. Damit beeinflusst die regulatorische Einordnung unmittelbar, welche Cybervorfälle im Forschungssystem erfasst, gemeldet und in übergreifende Lagebilder einbezogen werden.

4 BSI-Gesetz vom 2. Dezember 2025, zuletzt am 23. Juli 2026 geändert

4 Zukunftsszenarien zur Cybersicherheit im Forschungsprozess 2030+

Auf Grundlage der identifizierten Schlüsselfaktoren wurden im Resilienz-Check drei konsistente Zukunftsszenarien entwickelt, die unterschiedliche, jeweils in sich stimmige Entwicklungspfade bis zum Zeithorizont 2030+ beschreiben. Hierzu wurden für jeden Schlüsselfaktor zunächst drei mögliche zukünftige Ausprägungen definiert, die unterschiedliche Entwicklungspfade des jeweiligen Faktors abbilden. Anschließend wurden die Wechselwirkungen zwischen diesen Ausprägungen systematisch analysiert und zu konsistenten Kombinationen verdichtet. Konsistenz bedeutet dabei, dass die in einem Szenario zusammengeführten Ausprägungen der Schlüsselfaktoren in ihren wechselseitigen Beziehungen möglichst widerspruchsfrei und plausibel zusammenwirken.

Die Szenarien stellen keine Prognosen dar, sondern alternative, plausible Zukunftsbilder. Ihr Nutzen für die vorausschauende Technikfolgenabschätzung besteht darin, unterschiedliche Entwicklungsmöglichkeiten und mögliche Handlungsbedarfe frühzeitig sichtbar zu machen sowie politische und institutionelle Gestaltungsoptionen unter verschiedenen zukünftigen Rahmenbedingungen zu reflektieren. Damit bilden die Zukunftsszenarien die Grundlage für die Ableitung konkreter Handlungsoptionen (Kapitel 5), mit denen die Cybersicherheit und Resilienz des Forschungssystems unter unterschiedlichen zukünftigen Bedingungen gestärkt werden können.

Die drei Szenarien unterscheiden sich insbesondere grundlegend hinsichtlich des politischen Handlungsdrucks, der institutionellen Handlungsfähigkeit sowie des Grades der strukturellen und kulturellen Verankerung von Cybersicherheit im Forschungssystem:

Szenario 1: Hoher Handlungsdruck bei strukturellen Defiziten beschreibt eine Zukunft 2030+, in der sich die Bedrohungslage verschärft und die öffentliche Aufmerksamkeit für Cybersicherheit erhöht hat, strukturelle Schwächen des Forschungssystems, wie Fragmentierung der IT-Systeme, Kompetenzdefizite und unzureichende Governance, jedoch weitgehend fortbestehen. Es besteht folglich ein hoher Handlungsdruck, dem keine entsprechend effektiven Maßnahmen gegenüberstehen.

Szenario 2: Politischer Sicherheitsfokus mit deutlichen Defiziten in der Umsetzung zeichnet demgegenüber eine Zukunft, in der Cybersicherheit politisch und strategisch deutlich stärker priorisiert wird, zum Beispiel durch nationale Strategien, Regulierung und gezielte Förderprogramme. Diese politische Schwerpunktsetzung übersetzt sich jedoch nur unvollständig in die operative Praxis der Forschungseinrichtungen, sodass zwischen politischem Anspruch und tatsächlicher Umsetzung eine spürbare Lücke bestehen bleibt.

Szenario 3: Resilientes System mit punktuellem Nachbesserungsbedarf entwirft schließlich eine Zukunft, in der es gelungen ist, Cybersicherheit sowohl politisch-strategisch zu verankern als auch strukturell und kulturell in den Forschungseinrichtungen zu etablieren. Zentrale Schwachstellen früherer Entwicklungsphasen wurden weitgehend adressiert, der verbleibende Handlungsbedarf konzentriert sich auf punktuelle Nachbesserungen und die kontinuierliche Anpassung an neue Herausforderungen.

Aus Gründen der Übersichtlichkeit und um Redundanzen zu vermeiden, wird im Folgenden nur Szenario 1 als vollständige narrative Darstellung ausgeführt. Die Szenarien 2 und 3 werden demgegen-

über nicht erneut vollständig, sondern jeweils mit Bezug auf die grundlegenden Unterschiede in den Ausprägungen der Schlüsselfaktoren gegenüber Szenario 1 dargestellt. Dieses Vorgehen macht die zentralen Weichenstellungen zwischen den drei Zukunftsbildern unmittelbar sichtbar, ohne gemeinsame oder inhaltlich ähnliche Elemente der Szenarien wiederholt auszuformulieren.

4.1 Szenario 1: Hoher Handlungsdruck bei strukturellen Defiziten

Aus *gesellschaftlicher Perspektive* ist das Szenario zur Cybersicherheit im Forschungsprozess 2030+ durch die spezifischen Ausprägungen der drei Schlüsselfaktoren akademische Freiheit, digitale und KI-bezogene Kompetenzen sowie Sicherheitsbewusstsein geprägt. Die akademische Freiheit bleibt in diesem Szenario ein zentrales Leitprinzip und ermöglicht offene, kollaborative und international anschlussfähige Forschung. Wissenschaftliche Freiheit wird vielfach auch auf den individuellen Umgang mit IT-Systemen und Forschungsdaten bezogen, sodass verbindliche Sicherheitsvorgaben teilweise als Einschränkung der wissenschaftlichen Freiheit wahrgenommen und nicht konsequent umgesetzt werden. Gleichzeitig zeigt sich bei den digitalen und KI-bezogene Kompetenzen, dass die Anforderungen mit der fortschreitenden Digitalisierung und KI-Nutzung schneller steigen, als in den Forschungseinrichtungen entsprechende Qualifizierungsmaßnahmen aufgebaut werden können. Hinzu kommt ein defizitäres Sicherheitsbewusstsein: Cyberrisiken werden teilweise unterschätzt, Verantwortlichkeiten bleiben unklar und Schutzmaßnahmen werden oft nur unzureichend umgesetzt. Im Zusammenspiel erzeugen diese Ausprägungen eine Situation, in der hohe individuelle Freiheitsgrade mit unzureichenden Kompetenzen und einem schwach verankerten Sicherheitsbewusstsein einhergehen und dadurch die nachhaltige Verankerung sicherer digitaler Praktiken im Forschungsalltag erschwert wird.

Aus *technologischer Perspektive* ist die Forschungslandschaft in diesem Szenario 2030+ durch eine hohe Innovations- und Leistungsdynamik, gleichzeitig aber auch durch strukturelle Fragmentierung und ein uneinheitliches Sicherheitsniveau geprägt. Umfang, Komplexität sowie Vernetzungsgrad der IT-Infrastrukturen sind stark gewachsen, unter anderem getrieben durch Ausbauprogramme für KI-Hochleistungsrechner und die Nationale Forschungsdateninfrastruktur (NFDI). Sicherheitsarchitekturen, Lifecyclemanagement, Datengovernance sowie Detektions- und Abwehrfähigkeiten haben mit dieser Dynamik nur teilweise Schritt gehalten. Besonders sichtbar wird dieses Spannungsverhältnis im dauerhaften Parallelbetrieb hochmoderner und veralteter Systeme sowie in dezentralen, teilweise unklaren Verantwortlichkeiten auf Ebene von Instituten, Lehrstühlen und Projekten. Defizite bei Inventarisierung, Wartung und Updates führen dazu, dass verwundbare Legacysysteme sowie Alt- und Spezialgeräte weiterhin betrieben werden. Parallel dazu entsteht eine wachsende, zunehmend regulierte und abgesicherte neue Infrastruktur. Neue IT-Systeme werden teils systematisch und mit klarem Sicherheitsfokus, teils projekt- oder nutzergetrieben und ohne übergreifende Gesamtarchitektur eingeführt. Dadurch können erhebliche Innovationspotenziale für die datengetriebene Forschung erschlossen werden, ohne dass neue Systeme durchgängig in konsistente Sicherheitsarchitekturen eingebettet sind. In den durch die NIS-2-Richtlinie erfassten Forschungseinrichtungen für angewandte Forschung verbessert sich bis 2030+ die Inventarisierung deutlich. Auch die in der Verordnung (EU) 2024/2847 (Cyberresilienz-Verordnung)[5] verankerte Pflicht zur Bereitstellung von Sicherheitsupdates in digitalen Pro-

5 Verordnung (EU) 2024/2847 vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung)

dukten führt bei neu beschafften Systemen ab 2027 zu Verbesserungen bei Updates und Patches. Das erreichte Sicherheitsniveau hängt jedoch weiterhin stark von der finanziellen und personellen Ausstattung der einzelnen Einrichtungen ab.

Auch hinsichtlich der Segmentierung der IT-Infrastrukturen existieren in diesem Szenario erhebliche Unterschiede zwischen neuen und bestehenden Systemen: Neue, insbesondere KI- und cloudbezogene Infrastrukturen werden zunehmend nach den Prinzipien der granularen Segmentierung und des Zero-Trusts aufgebaut. Sie sind also in kleine, einzeln kontrollierbare Bereiche aufgeteilt, für die nur absolut notwendige Berechtigungen vergeben werden und jeder Zugriff überprüft wird. Bestehende Campusnetze sind dagegen häufig gering segmentiert und werden nur langsam nachgerüstet. Insgesamt ist die Nutzung externer IT- und Clouddienste hoch, was Effizienz- und Skalenvorteile bietet. Die Sicherung von Qualitätsstandards, die sicherheitsbezogene Vertragsgestaltung und die Überwachung der externen Abhängigkeiten halten jedoch mit dem Tempo der zunehmenden Auslagerung nicht Schritt, die zudem oft wenig koordiniert und vielfach eher projekt- oder personengetrieben erfolgt. In vielen Forschungseinrichtungen besteht nur begrenzte Transparenz darüber, welche Softwarekomponenten eingesetzt werden und welche Abhängigkeiten innerhalb der zugehörigen Lieferketten bestehen. Entscheidungen über interne oder externe Bereitstellung von IT-Leistungen erfolgen zudem nicht immer strategisch, sodass Leistungen teilweise intern erbracht werden, obwohl externe Dienste mit hohen Sicherheitsstandards effizienter oder sicherer wären. Eine forschungssystemweite Koordination der Auslagerung von IT- und Clouddiensten besteht nicht; eine zentrale Instanz zur einrichtungsübergreifenden Steuerung von Sourcingentscheidungen und Sicherheitsanforderungen existiert nur eingeschränkt. Fortschritte zeigen sich beim Ausbau föderativer Infrastrukturen, über die Teilbereiche koordiniert bereitgestellt werden. Dazu zählen die Authentifizierungs- und Autorisierungsinfrastruktur des Deutschen Forschungsnetzes (DFN-AAI), landesweite Identitätsmanagementinitiativen (Landes-IAM) sowie die Konsolidierung der Nationalen Forschungsdateninfrastruktur als One NFDI.

Die Bedrohungslage hat sich in diesem Szenario erheblich verschärft, da KI-gestützte Cyberangriffe zunehmend hochautomatisiert, adaptiv und skalierbar erfolgen und auch von staatlich unterstützten Akteuren eingesetzt werden. Durch umfangreichen KI-Einsatz im Kontext von Cybercrime-as-a-Service (CaaS), also dem Verkauf von Cyberangriffen und Angriffsschritten als Dienstleistungen, haben sich die Einstiegsschwellen für Akteure deutlich verringert. Darüber hinaus hat es in der Art und Weise der KI-Nutzung für cyberkriminelle Aktivitäten einen großen qualitativen Sprung gegeben – von KI als Werkzeug zu KI als autonomem Akteur in der Cyberkriminalität. Dies bedeutet den Übergang von KI-gestützten Angriffen zu vollständig autonomen Agentic-AI-Angriffen. Dieser Ausführungsmodus für Cyberangriffe bildet – vor allem in Bezug auf Ransomware und Identitätsdiebstahl – 2030+ den größten Angriffsvektor. Dem stehen nur begrenzt entwickelte defensive Fähigkeiten gegenüber. Zwar existieren punktuell fortgeschrittene Sicherheitslösungen, auch durch die Nutzung automatisierter Verfahren insgesamt bleiben die Fähigkeiten zur Angriffserkennung und forensischen Analyse jedoch hinter den Angriffsfähigkeiten zurück und sind vielfach unzureichend, sodass Angriffe oft erst spät erkannt und kaum systematisch ausgewertet werden. Die Erkennungs- und Meldeinfrastruktur wird durch die von der NIS-2-Richtlinie getriebene Standardisierung sowie den Ausbau gemeinsam genutzter Dienste – sowohl zwischen übergeordneten Behörden und Cybersicherheitsakteuren für die Wissenschaft (DFN/BSI) als auch zwischen Forschungseinrichtungen selbst – systematischer und schneller; allerdings profitiert davon nur ein Teil des Forschungssystems. Die meisten Hochschulen und viele

außeruniversitäre Forschungseinrichtungen werden nicht durch die NIS-2-Richtlinie reguliert. Ein flächendeckendes Monitoring, eine konsistente und umfassende Protokollierung und systematische forensische Analysen fehlen. Die Schere zwischen gut ausgestatteten Einrichtungen und kleineren, ressourcenschwachen Einrichtungen ist größer geworden. Zwar nimmt die Nutzung KI-gestützter Methoden zur Erkennung und Abwehr von Cyberangriffen zu und eine breite Palette vorkonfigurierter KI-basierter Sicherheitsprodukte und Dienstleistungen steht zur Verfügung. Nur wenige Forschungseinrichtungen verfügen jedoch über die KI-Kompetenzen, die für einen eigenständigen, professionellen Einsatz von KI-basierten Cybersecurityanwendungen nötig wären. Viele Forschungseinrichtungen haben keine eigenen KI-Kompetenz aufgebaut.

In dem Szenario bis 2030+ sind sowohl die Datenmenge als auch deren Komplexität unter anderem durch KI-getriebene Forschung stark gewachsen. Höhere technische Standards in von der NIS-2-Richtlinie betroffenen Forschungseinrichtungen und die Bestrebungen in Richtung einer umfassenden Nationalen Forschungsdateninfrastruktur (One NFDI) – haben den Umgang mit sensiblen Forschungsdaten teilweise professionalisiert. Dennoch sind viele Forschungsdaten weiterhin unzureichend nach Schutzbedarfen klassifiziert. Aufbewahrung, Archivierung und Verantwortlichkeiten bleiben oft implizit oder projektspezifisch geregelt, Sicherheitsmaßnahmen damit lückenhaft. Der Aufbau einer systematischen Datengovernance hält mit dem Datenwachstum nicht Schritt. Gleichzeitig macht der hohe strategische Wert von Forschungsdaten in ausgewählten Forschungsbereichen diese zu einem attraktiven Ziel für Cyberangriffe.

Wirtschaftlich ist das Szenario in den Jahren 2030+ durch einen anhaltenden Fachkräftemangel im Bereich Cybersicherheit geprägt. Im IT- und Infrastrukturbereich von Forschungseinrichtungen herrschen personelle Engpässe und Abhängigkeiten von externen Dienstleistern vor. Der Mangel an verfügbaren Cybersicherheitsfachkräften bleibt ein Kernproblem. Aufgrund seiner schwächeren Position im Wettbewerb um knappe Fachkräfte sowie seiner geringeren Budgets verfügt das Forschungssystem über schlechtere Voraussetzungen als die Industrie. Dies erschwert den Aufbau stabiler, institutionell verankerter Sicherheitskompetenzen; sicherheitsrelevantes Wissen bleibt häufig personengebunden und geht mit Personalwechseln verloren. Darüber hinaus prägen verstärkte Abhängigkeiten von marktbeherrschenden IT- und Cloudanbietern das Szenario. Diese Anbieter ermöglichen einerseits leistungsfähige und skalierbare Infrastrukturen, die für datenintensive Forschung essenziell sind. Forschungseinrichtungen profitieren somit von technologischen Fortschritten, verlieren jedoch gleichzeitig an Steuerungsfähigkeit. Große Anbieter von Cloud- und On-Premise-Systemen koppeln ihre Multifaktorauthentifizierungslösungen teilweise an die Cloudnutzung. Dies führt bei vielen Forschungseinrichtungen, unter anderem aufgrund von Fachkräfte- und Kapazitätsmangel, dazu, dass sie die Cloudoption nutzen. Mit dem steigenden Anteil datenintensiver und anwendungsnaher Forschung wächst zudem das Schadenspotenzial einzelner Sicherheitsvorfälle.

Auf politischer Ebene bestehen in diesem Szenario 2030+ moderat verbesserte regulatorische Rahmenbedingungen, die insbesondere auf die Umsetzung von europäischen Richtlinien – vor allem der NIS-2-Richtlinie – zurückzuführen sind. Deren Anwendungsbereich erfasst jedoch nicht alle Forschungseinrichtungen, und die Umsetzung erfolgt in fragmentierter Form zwischen Institutionen unterschiedlicher Größe und Ressourcenausstattung. Daraus resultiert eine Diskrepanz zwischen unterschiedlichen Forschungseinrichtungen, die von unzureichenden personellen und finanziellen Ressourcen vergrößert wird. Hinzu kommen anhaltende Koordinationsdefizite zwischen Bund, Ländern und Institutionen, die eine kohärente Cybersicherheitsstrategie verhindern.

Digitale Souveränität bleibt trotz ihrer strategischen Bedeutung begrenzt ausgeprägt, zugleich erodieren institutionsinterne Kompetenzen zur eigenständigen Wahrnehmung von Infrastrukturaufgaben zunehmend. Regulatorische Anforderungen führen dabei häufig zu formaler Compliance, ohne dass dies mit einer Steigerung der operativen Resilienz verbunden ist.

Schlussfolgerung: systemisches Gefährdungspotenzial und Ankerpunkte für Handlungsoptionen

Das Zusammenwirken hochautomatisierter, zunehmend autonomer KI-gestützter Angriffe, einer strukturell verzögerten Angriffserkennung, fortbestehender Legacysysteme und wachsender Abhängigkeit von wenigen marktbeherrschenden Cloud- und IT-Anbietern begründet in diesem Szenario ein erhebliches Kaskadenrisiko für das Forschungssystem. Erfolgreiche Cyberangriffe auf zentral genutzte Dienste, wie zum Beispiel auf Cloudinfrastrukturen oder Rechenzentren, können mehrere Forschungsbereiche und Forschungseinrichtungen gleichzeitig beeinträchtigen und so zu Versorgungsengpässen führen, sowohl bei Forschungsdienstleistungen selbst als auch bei gesellschaftlich relevanten Anwendungen, die auf kontinuierliche Datenverfügbarkeit und Datenintegrität angewiesen sind. Hierzu könnten beispielsweise die krankheitserregerbezogene Überwachung und Entwicklung von Impfstoffentwicklung im Pandemiefall zählen, sicherheitsrelevante Forschung zur Resilienz der Energie- und Wasserversorgung oder Frühwarnsysteme, die auf stets verfügbare und unverfälschte Forschungsdaten angewiesen sind. Verschärft wird dieses Risiko durch die ungleiche Resilienz zwischen gut und schlecht ausgestatteten Forschungseinrichtungen; insbesondere Einrichtungen, die strategisch oder wirtschaftlich wertvolle Daten verarbeiten, gleichzeitig jedoch über eine unterdurchschnittliche Detektions- und Reaktionsfähigkeit verfügen, stellen im vernetzten Forschungssystem bevorzugte Angriffsziel dar.

Aus diesem Befund lassen sich mehrere miteinander verzahnte Ansatzpunkte für eine wirksame Verbesserung der Cybersicherheit im Forschungsprozess ableiten (Kapitel 5). Grundlegend ist der Aufbau automatisierter Assettransparenz, also eines stets aktuellen Überblicks über vorhandene IT-Systeme, Geräte und Anwendungen. Ohne einen verlässlichen Überblick über die heterogenen, teils veralteten Systeme – im Szenario explizit als Defizit im Lifecyclemanagement benannt – bleiben alle weiteren Schutzmaßnahmen lückenhaft. Um der zentralen Bedrohung im Szenario in Form von autonomen, KI-gestützten Angriffen bei gleichzeitig fragmentierter und später Erkennung, wirksam zu begegnen, bedarf es zudem koordinierter Informations-, Austausch- und Unterstützungsstrukturen sowie eines gemeinsamen Lagebildes. Solche Strukturen können zugleich der im Szenario beschriebenen ungleichen Verteilung der Auswirkungen entgegentreten. Zwar existieren in vielen Bundesländern hochschulübergreifende Einrichtungen oder Kooperationen, die zentrale Sicherheitsdienste bündeln und vor allem kleineren Hochschulen zugutekommen. Diese Strukturen sind jedoch nicht flächendeckend etabliert. Außeruniversitäre Forschungseinrichtungen mit strategisch oder wirtschaftlich relevanten Datenbeständen bleiben dabei aufgrund oft begrenzter Detektions- und Reaktionsfähigkeit besonders exponiert.

Ebenso bedeutend sind die institutionelle Verankerung, zum Beispiel durch klare Zuständigkeiten, Prozesse und Governancestrukturen der Cybersicherheit sowie ein gezielter Personalaufbau. Beides ist vor dem Hintergrund des im Szenario beschriebenen Fachkräftemangels besonders voraussetzungsvoll. Ohne eine ausreichende personelle Basis bleiben auch technische und organisatorische Maßnahmen langfristig wirkungslos. Nicht zuletzt verdeutlicht das Szenario, dass

technische und personelle Maßnahmen allein nicht ausreichend sind. Erforderlich ist eine Cybersicherheitskultur im Sinne verantworteter Freiheit in Forschung und Lehre, die verhindert, dass Sicherheitsvorgaben als Einschränkung akademischer Freiheit wahrgenommen und in der Folge umgangen werden. Da das Forschungssystem in Deutschland durch eine Vielzahl eigenständiger, dezentral organisierter Forschungseinrichtungen mit hoher individueller Autonomie geprägt ist, lässt sich Cybersicherheit hier nicht von oben durchsetzen, sondern muss als gemeinsam getragene Verantwortung von Forschenden, Lehrstühlen und Institutionen verstanden werden. Nur wenn das Sicherheitsbewusstsein nicht als Gegensatz zu Freiheit und Kollaboration, sondern als integraler Bestandteil guter wissenschaftlicher Praxis verstanden wird, lässt sich die im Szenario beschriebene Umgehung von Sicherheitsvorgaben reduzieren.

4.2 Szenario 2: Politischer Sicherheitsfokus mit deutlichen Defiziten in der Umsetzung

Dieses Szenario unterscheidet sich von Szenario 1 vor allem durch eine deutlich stärkere politische Priorisierung der Cybersicherheit im Forschungssystem 2030+. In gesellschaftlicher Perspektive zeigen sich hingegen weitgehend vergleichbare Entwicklungen wie in Szenario 1 – insbesondere das Verständnis akademischer Freiheit, das Sicherheitsbewusstsein sowie die digitalen und KI-bezogenen Kompetenzen der Forschenden und Beschäftigten weisen ähnliche Ausprägungen auf. Auch im Hinblick auf die *technologischen Schlüsselfaktoren* sind viele Aspekte ähnlich. Jedoch gelingt hinsichtlich veralteter Systeme und Geräte immerhin eine selektive Erneuerung. Es gibt Fortschritte in der Inventarisierung von Altbeständen. Altgeräte und -systeme werden erfasst und abgeschaltet oder modernisiert, wenn auch selektiv. Das Patchmanagement (systematisches Einspielen von Sicherheitsupdates) offener Schwachstellen ist stellenweise etabliert. Das Lifecyclemanagement bleibt unvollständig, erfasst aber insgesamt einen größeren Teil der IT-Systeme und Geräte als in Szenario 1. Neue Systemelemente werden systematisch erfasst, die Verantwortung für eine Abschaltung nach Nutzungsende ist jedoch nicht immer klar zugewiesen. Auch mit Blick auf die Adoption neuer Technologien unterscheidet sich Szenario 2 von Szenario 1: Die Adoption erfolgt schnell, wird aber zumindest teilweise durch Sicherheits- und Architekturüberlegungen begleitet. Sicherheitsanforderungen von Innovationen werden bei zentralen Systemen berücksichtigt, bei dezentralen Innovationen jedoch weniger.

Zudem ist in diesem Szenario der professionelle KI-Einsatz in der Cyberabwehr in Forschungseinrichtungen weit verbreitet. Während strategische Entscheidungen und kritische Reaktionen unter menschlicher Kontrolle bleiben, verfügen die meisten Forschungseinrichtungen über KI-Kompetenzen in der Cyberabwehr, die eine umfassende Anwendung von KI-gestützten Werkzeugen in der Cybersicherheit ermöglichen. Vielfach werden jedoch proprietäre Dienste großer Anbieter genutzt. Die Verteidigung ist zwar leistungsfähig, aber stark abhängig von externen Plattformen. Die Transparenz über Trainingsdaten und Entscheidungslogiken ist in vielen Forschungseinrichtungen gering ausgeprägt. Updates, Anpassungen und Reaktionsmuster sind automatisiert und teilweise extern gesteuert.

Aus wirtschaftlicher Perspektive verschärft sich die bereits in Szenario 1 ausgeprägte Bedrohungslage zusätzlich. Dies ist auf den hohen ökonomischen und geopolitischen Wert von Forschungsdaten und geistigem Eigentum zurückzuführen, der sich aus ihrer wachsenden Bedeutung für KI-

Entwicklung, Dual-Use-Anwendungen und den internationalen Technologiewettbewerb ergibt. Ein großer Anteil der Forschung ist sicherheitsrelevant oder dem Dual-Use-Bereich zuzuordnen, sodass Forschungseinrichtungen nahezu flächendeckend zum Ziel von Cyberangriffen werden. Die Bedrohungslage ist 2030+ entsprechend durch systematische, langfristig angelegte Ausspähungs-, Infiltrations- und Manipulationskampagnen geprägt, die auf kritische Infrastrukturen, Schlüsselpersonen und sensible Datenbestände abzielen. In den übrigen Ausprägungen der wirtschaftlichen Schlüsselfaktoren entspricht das Szenario weitgehend dem Szenario 1.

Mit Blick auf die *politischen Schlüsselfaktoren* unterscheidet sich dieses Szenario deutlich. Zwar ist die digitale Souveränität auch in diesem Szenario unzureichend, die Cybersicherheit genießt jedoch strategische Priorität und auch die Koordination zwischen Bund und Ländern ist deutlich gestärkt. Regulierungen sind deutlich verschärft und ausgeweitet – Sicherheit genießt absolute Priorität, bis hin zu einer stark sicherheitsgetriebenen Überregulierung. Große Teile von Forschungs- und Dateninfrastrukturen gelten als kritisch oder sicherheitsrelevant und müssen umfassenden Melde-, Nachweis- und Kontrollpflichten nachkommen. Auch die Rahmenbedingungen internationaler Forschungskooperationen sind von hohen Sicherheitsanforderungen geprägt, Kooperationen werden systematisch an Risikoanalysen geknüpft und gemeinsame Forschungsprojekte unterliegen häufig Sicherheitsüberprüfungen oder abgestuften Zugriffsregelungen.

Schlussfolgerungen: systemisches Gefährdungspotenzial und Ankerpunkte für Handlungsoptionen

Die Kombination aus hochautomatisierten Angriffen und der nahezu flächendeckenden Attraktivität von Forschungseinrichtungen als Angriffsziel, auch bedingt durch den besonders hohen ökonomischen und geopolitischen Wert fast aller Forschungsdaten und geistigem Eigentum, begründet in diesem Szenario ein hohes systemisches Gefährdungspotenzial. Gezielte, langfristig angelegte Ausspähungs- und Manipulationskampagnen gegen kritische Infrastrukturen können dabei nicht nur einzelne Forschungseinrichtungen, sondern ganze Forschungsfelder, vor allem solche mit hoher Dual-Use-Relevanz, empfindlich treffen. Da die verschärfte Regulierung vor allem auf Melde-, Nachweis- und Kontrollpflichten ausgerichtet ist, ohne deren tatsächliche Umsetzbarkeit auf individueller und institutioneller Ebene sicherzustellen, besteht trotz politischer Priorisierung eine strukturelle Sicherheitslücke. Diese zeigt sich beispielsweise dort, wo verschlüsselte oder manipulierte Forschungsdaten sicherheitsrelevante Prozesse in der Gesundheits- oder Energieforschung verzögern oder verfälschen und dadurch Versorgungsengpässe begünstigen können.

Auch in diesem Szenario treten strukturelle Defizite hervor, an denen Handlungsoptionen zur Verbesserung der Cybersicherheit im Forschungsprozess ansetzen sollten. Im Unterschied zu Szenario 1 geht der politische Fokus auf Cybersicherheit in der Forschung hier mit unzureichend sicherheitsorientiertem Verhalten, mangelhaften digitalen Kompetenzen der Forschenden und Beschäftigten sowie zum Großteil ungenügenden technischen Sicherheitsmaßnahmen einher; ein Befund, der die Diskrepanz zwischen regulatorischem Anspruch und operativer Umsetzungsfähigkeit deutlich macht. Ansatzpunkte liegen daher vor allem darin, die tatsächliche Umsetzbarkeit für die einzelnen Forschungsinstitute stärker zu berücksichtigen und zu ermöglichen, anstatt den Fokus einseitig auf pauschale Nachweis- und Kontrollpflichten zu legen. Vor dem Hintergrund des hohen ökonomischen und geopolitischen Werts von Forschungsdaten und geistigem Eigentum sowie des hohen Anteils sicherheitsrelevanter und Dual-Use-Forschung zeigt sich zudem der

Bedarf an einer differenzierten Klassifizierung von Schutzbedarfen sowie der Sicherstellung von Integrität und Verfügbarkeit von Forschungsdaten besonders deutlich. Dies gilt umso mehr, da pauschale Melde- und Kontrollpflichten der fachlichen Heterogenität der betroffenen Forschungsbereiche nicht gerecht werden. Darüber hinaus gewinnen vertrauenswürdige internationale Forschungskooperationen an Bedeutung: Internationale Wissenschaftspolitik ist in diesem Szenario systematisch mit Risikoanalysen verbunden und kooperative Projekte unterliegen sehr strengen Sicherheitsprüfungen und Zugriffsregelungen. Es fehlen jedoch tragfähige Ansätze, um wissenschaftliche Offenheit, ausreichenden Austausch und Kooperationsfähigkeit trotz geopolitischer Konflikte und Sicherheitsmaßnahmen zu erhalten und Kooperationen nicht ausschließlich über Kontrollmechanismen zu regeln.

4.3 Szenario 3: Resilientes System mit punktuellem Nachbesserungsbedarf

In diesem Szenario wird eine Zukunft 2030+ entworfen, in der es gelungen ist, Cybersicherheit sowohl politisch-strategisch zu verankern als auch strukturell und kulturell in den Forschungseinrichtungen zu etablieren. Auf *gesellschaftlicher Ebene* wird akademische Freiheit mit Blick auf Cybersicherheit als verantwortete Freiheit innerhalb klar definierter Sicherheitsleitplanken verstanden. Forschende und Beschäftigte setzen sich mit Cyberbedrohungen auseinander und haben ein hohes Sicherheitsbewusstsein. Vor allem Führungskräfte verfügen über eine geschärfte Risikowahrnehmung, die sie als integralen Bestandteil ihrer Führungsverantwortung verstehen. Forschende und Beschäftigte haben darüber hinaus ausgeprägte digitale und KI-Kompetenzen.

In *technologischer Hinsicht* sind viele Aspekte der IT-Sicherheit recht fortgeschritten. Forschungseinrichtungen verfügen über etablierte, institutionenübergreifende Fähigkeiten zur kontinuierlichen Cyberüberwachung in Echtzeit sowie zur Analyse und Auswertung cybersicherheitsrelevanter Ereignisse. Dies gilt nicht nur für die durch die NIS-2-Richtlinie regulierten Forschungseinrichtungen, sondern für die Mehrheit der Hochschulen. Forensische Erkenntnisse werden über Institutions- und Ländergrenzen hinweg geteilt und fließen systematisch in Präventions-, Resilienz- und Schulungsmaßnahmen ein. Es besteht ein gemeinsames, regelmäßig aktualisiertes Lagebild, das aktuelle Bedrohungsindikatoren, anonymisierte Vorfallmeldungen, Schwachstelleninformationen und Trendanalysen institutionenübergreifend bündelt und über eine zentrale Plattform allen angeschlossenen Einrichtungen zugänglich macht. Der KI-Einsatz in der Cyberabwehr ist weit verbreitet, die menschliche Kontrolle bleibt jedoch ein zentrales Element der Gesamtstrategie. Strategische Entscheidungen und kritische Reaktionen werden weiterhin von Menschen getroffen, während KI-Ergebnisse durch menschliche Bewertung validiert werden. Es liegt ein starker Fokus auf Datenqualität, Modellvalidierung und Auditierbarkeit.

Die IT-Infrastrukturen an Forschungseinrichtungen wurden umfassend überarbeitet. Ihr Umfang, ihre Komplexität und ihr Vernetzungsgrad sind weitergewachsen, sie sind aber in Gesamtarchitekturen eingebettet und werden aktiv gesteuert. IT-Systeme sind weitgehend standardisiert, auch über Institutionen hinweg, sowie modular aufgebaut und segmentiert. Es existieren zudem definierte Verantwortlichkeiten für Cybersicherheitsaspekte von IT-Infrastrukturelementen. Ein systematisches Lifecyclemanagement hat sich durchgesetzt. IT-Systeme und Geräte werden konsequent entlang ihres gesamten Lebenszyklus geplant, betrieben und abgelöst. Auch be-

stehende Altgeräte und -systeme werden durch regelmäßige Inventuren vollständig erfasst und abgeschaltet oder aktualisiert, offene Schwachstellen werden schnell gepatcht. Dadurch hat sich die Anzahl der Schwachstellen in Altsystemen und -geräten signifikant verringert. Sicherheit ist integraler Bestandteil von Beschaffung, Betrieb und Aussonderung. Die Adoption von Innovationen wird aktiv gesteuert und in übergreifende Architektur-, Sicherheits- und Lebenszykluskonzepte eingebettet. Es existieren klare Prozesse zur Einführung neuer Technologien, Sicherheits- und Architekturprüfungen sind Teil des Adoptionsprozesses. Der Kompetenzaufbau und der Betrieb werden parallel mitgedacht. Die Adoptionsprozesse erfolgen etwas verlangsamt, da Prüfprozesse und Koordination Zeit brauchen. Auch das Datenmanagement ist lebenszyklusorientiert: Die unterschiedliche technische Komplexität und der unterschiedliche Schutzbedarf von Forschungsdaten werden für unterschiedliche Datentypen entlang des Datenlebenszyklus adressiert und systematisch in Governance- und Sicherheitsstrukturen eingebettet. Forschungsdaten sind klar nach Sensibilität, Integritäts- und Verfügbarkeitsanforderungen kategorisiert. Es existieren durchgängige Provenancekontrollen (Datenherkunft) und Integritätskontrollen sowie regelmäßige Sicherheitsprüfungen, auch für Langzeitarchive.

Mit Blick auf externe Anbieter wurde entschieden, einen großen Teil der IT-Leistungen auszulagern, sodass externe IT-Infrastrukturen und Dienste integrale Bestandteile der IT-Architektur sind. Ausgelagerte Systemelemente werden aktiv koordiniert und verwaltet. Die intensive Auslagerung führt zu einheitlichen Sicherheitsstandards, allerdings bestehen dadurch auch hohe Outsourcing- und Cloudabhängigkeiten, die konstant im Bewusstsein bleiben müssen. Abhängigkeiten, Lieferketten und Wechseloptionen sind größtenteils transparent. Da vor allem die Dienste von wenigen großen externen Anbietern genutzt werden bleibt jedoch eine Abhängigkeit von ebendiesen.

Aus wirtschaftlicher Perspektive wird das Szenario insbesondere durch die Ausprägungen der Schlüsselfaktoren zur Bedrohungslage und zum strategischen Wert von Forschungsdaten geprägt. Die Bedrohungslage ist durch eine zunehmende Nutzung von KI durch Cyberkriminelle gekennzeichnet, die allerdings vor allem zur Skalierung und Verbreiterung von Aktivitäten und weniger für tiefgreifende, hochautomatisierte Angriffe eingesetzt wird. KI wird routinemäßig genutzt, um Angriffe realistischer und effizienter zu gestalten. Personalisierte Phishing- und Spear-Phishingkampagnen nehmen zu. KI wird auch für die automatisierte Analyse von Zielorganisationen und öffentlich verfügbaren Daten genutzt und unterstützt bei der Schadsoftwareentwicklung. Die Eintrittshürden für komplexe Angriffe sinken, bestehende Bedrohungen werden deutlich verstärkt. Wie in Szenario 1 erhöht der hohe wirtschaftliche strategische Wert von Forschungsdaten in ausgewählten Forschungsbereichen deren Attraktivität als Angriffsziel, sodass entsprechende Einrichtungen gezielt angegriffen werden.

Was weitere *wirtschaftliche Zusammenhänge* angeht, ist die digitale Souveränität generell hoch, trotz der Nutzung weniger großer Anbieter. Forschungseinrichtungen koordinieren die Nutzung externer Dienste, insbesondere von monopolistischen Anbietern, und es wird Wert auf Dienstleister und Infrastruktur aus der EU gelegt. Der durch den Fachkräftemangel entstehende Handlungsdruck konnte durch einen mittleren Kompetenzaufbau teilweise reduziert werden, bleibt jedoch eine Herausforderung, denn Cybersicherheitskompetenzen hängen weiterhin stark von einzelnen Personen sowie teilweise von externen Dienstleistern ab. Die Umsetzung von Cybersicherheitsmaßnahmen erfordert weiterhin erhebliche personelle und finanzielle Ressourcen.

Auf *politischer und rechtlicher Ebene* hat die Priorisierung von Cybersicherheit in der Forschung deutlich zugenommen und ist als strategisches Querschnittsthema in Regierungsprogrammen,

Sicherheitsstrategien und Forschungsförderlinien fest verankert. Die politische Koordination zwischen Bund, Ländern und der EU im Bereich Cybersicherheit ist durch verbindliche Rahmenwerke und gemeinsame Gremien gestärkt und ermöglicht einheitliche Strategieumsetzungen. Regulierung ist wirkungsorientiert und kontextsensitiv, starre Vorgaben haben Platz gemacht für adaptive, abgestufte Anforderungen. Innerhalb der internationalen Wissenschaftspolitik verfolgt Deutschland eine Strategie freier Wissenschaft. Kooperationen mit verlässlichen Partnerländern werden gezielt vertieft und ausgeweitet, zugleich werden risikobehaftete Partnerschaften restriktiver gehandhabt.

Schlussfolgerungen: systemisches Gefährdungspotenzial und Ankerpunkte für Handlungsoptionen

In diesem Szenario wirken die gesellschaftlichen Faktoren, anders als in Szenario 1, überwiegend resilienzfördernd und verstärken sich gegenseitig. Über ein stärker sicherheitsorientiertes Verhalten tragen sie zudem maßgeblich dazu bei, dass technologische Sicherheitsmaßnahmen – wie Verschlüsselungstechnologien oder Systeme zur Angriffserkennung – ihre Schutzwirkung entfalten können. Auch die Ausprägungen der technologischen Schlüsselfaktoren begünstigen Sicherheit und Resilienz. Trotz dieser insgesamt hohen Resilienz verbleibt als wesentliches strukturelles Risiko die Abhängigkeit von wenigen großen, marktbeherrschenden Anbietern, die sich auch durch koordinierte Auslagerung und aktives Abhängigkeitsmanagement nur begrenzt reduzieren lässt. Der Ausfall eines solchen Anbieters, zum Beispiel aufgrund eines Cyberangriffs, geopolitischer Restriktionen oder unternehmerischen Entscheidungen außerhalb des Einflussbereichs des Forschungssystems, kann erhebliche Versorgungsengpässe in der Forschungsinfrastruktur verursachen. Darin zeigt sich ein grundlegender Zielkonflikt: Die im Szenario erreichte digitale Souveränität beruht im Wesentlichen darauf, dass sich wenige, dafür als aber als vertrauenswürdig geltende europäische Anbieter mit einheitlichen Lösungen durchsetzen. Diese Konzentration ermöglicht zwar hohe Sicherheitsstandards und Skaleneffekte, verlagert die Abhängigkeit von außereuropäischen Anbietern jedoch lediglich auf eine kleinere Zahl innereuropäischer Anbieter und erzeugt damit neue systemische Abhängigkeiten und potenzielle kritische Ausfallpunkte. Digitale Souveränität bedeutet in diesem Szenario also nicht Unabhängigkeit von Anbietern insgesamt, sondern Kontrolle über und Vertrauen in die verbleibenden, weiterhin wenigen Anbieter. Digitale Souveränität setzt zugleich die dauerhafte Verfügbarkeit vertrauenswürdiger und leistungsfähiger technologischer Alternativen voraus; eine Voraussetzung, die einzelne Forschungseinrichtungen nur begrenzt beeinflussen können, wirksamer lässt sich hier über Forschungsverbünde und durch politische Weichenstellungen ansetzen.

Der wichtigste Ankerpunkt für Handlungsoptionen liegt in diesem Szenario daher in der Stärkung der digitalen Forschungssouveränität. Auch bei einem bereits funktionierenden souveränitätsorientierten Anbietermanagements sollten Strategien zur technologischen Autonomie und wissenschaftlichen Unabhängigkeit langfristig weiterentwickelt werden, um Konzentrationsrisiken zu minimieren, Wechsel- und Ausweichmöglichkeiten zur fördern und die Abhängigkeit von einzelnen mächtigen Anbietern zu begrenzen. Dies erfordert neben Maßnahmen innerhalb des Forschungssystems auch gesamtgesellschaftliche und industriepolitische Weichenstellungen zur Entwicklung und Verfügbarkeit von souveränen Alternativen. Ergänzend verweist auch dieses Szenario auf die hohe Bedeutung eines gezielten Personalaufbaus sowie eine institutionelle

Verankerung der Cybersicherheit im Forschungssystem. Der trotz des bisherigen Kompetenzaufbaus fortbestehende Fachkräftemangel verdeutlicht, dass interne Kompetenzen und Kapazitäten kontinuierlich gestärkt werden müssen, um Abhängigkeiten von einzelnen Wissensträgern und externen Dienstleistern weiter zu reduzieren; eine Aufgabe, die angesichts des branchenübergreifenden Fachkräftemangels zu einem erheblichen Teil außerhalb des Forschungssystems selbst zu adressieren ist.

5 Handlungsoptionen

Aus den dargestellten Szenarien lassen sich Handlungsoptionen ableiten, die zentrale Schwachstellen wie Fragmentierung, Kompetenzdefizite, prekäre Beschäftigungsstrukturen und Governancelücken adressieren und zugleich die in den Szenarien angelegten Stärken und Entwicklungspotenziale nutzen, zu denen die Skalierung von Maßnahmen und Strukturen sowie die Vernetzung zählen. Für die Darstellung der abgeleiteten Handlungsoptionen bietet sich eine strukturierte Darstellung an, die sowohl unterschiedliche Zeithorizonte als auch die jeweiligen Verantwortlichkeiten zentraler Akteure berücksichtigt und damit realistische Umsetzungsperspektiven eröffnet.

Entsprechend gliedert sich die folgende Darstellung der Handlungsoptionen in drei aufeinander aufbauende Phasen: Kurzfristig (0 bis 2 Jahre) können Maßnahmen ansetzen, die bestehende Systeme stabilisieren, akute Risiken reduzieren, Transparenz schaffen und grundlegende Sicherheitsstrukturen etablieren (stabilisieren und sichtbar machen). Mittelfristig (3 bis 5 Jahre) eröffnet sich das Potenzial, Cybersicherheit strukturell in Governance- und Personalstrukturen zu verankern sowie Schutzbedarfe und Kompetenzen differenziert und kontextsensitiv auszugestalten (differenzieren und institutionell verankern). Langfristig (5 bis 10 Jahre) besteht die Möglichkeit in einer grundlegenden Transformation hin zu mehr digitaler Souveränität, resilienten Infrastrukturen und lernfähigen Systemen (transformieren und resilient machen).

Die Zuordnung einzelner Handlungsoptionen zu diesen drei Phasen folgt dabei einer pragmatischen Logik und ist nicht als trennscharfe Kategorisierung zu verstehen. Nahezu jede Option entfaltet Wirkungen auf mehreren Zeithorizonten zugleich: Eine kurzfristig eingeführte Sicherheitsmaßnahme kann erst mittelfristig ihre volle Wirkung entfalten, während der Aufbau langfristig angelegter Strukturen häufig kurzfristige Vorarbeiten erfordert. Die Zuordnung orientiert sich daher primär daran, wann eine Option realistischerweise initiiert werden kann und nicht daran, wann ihre Wirkung einsetzt oder sie vollständig abgeschlossen ist. Diese Systematisierung ist damit weniger als starres Ablaufschema und vielmehr als Orientierungsrahmen zu verstehen, der hilft, Prioritäten zu setzen und Verantwortlichkeiten sinnvoll zuzuordnen, auch wenn im Einzelfall andere Einordnungen vertretbar wären.

Entsprechend wird auch deutlich, dass die Umsetzung dieses Orientierungsrahmens eine abgestufte Verantwortung nahelegt, die sich an denselben zeitlichen Schwerpunkten ausrichten kann: Kurzfristig sind vor allem die Forschungseinrichtungen selbst gefragt, bestehende Defizite zu adressieren und Mindeststandards umzusetzen. Mittelfristig kommt den Ländern eine zentrale Rolle beim Aufbau tragfähiger Strukturen und Finanzierungsmodelle zu. Langfristig bedarf es einer strategischen Neuausrichtung auf Bundes- und europäischer Ebene, um digitale Souveränität zu stärken und ein kohärentes, resilient ausgerichtetes Gesamtsystem zu etablieren.

5.1 Kurzfristige Optionen: stabilisieren und sichtbar machen

Der kurzfristige Möglichkeitsraum (0 bis 2 Jahre) adressiert insbesondere die in Szenario 1 dargestellten strukturellen Defizite wie mangelnde Assettransparenz, fragmentierte Koordination

und unzureichendes Sicherheitsbewusstsein. Ähnliche Defizite zeigen sich abgeschwächt auch in Szenario 2, während Szenario 3 den langfristigen Nutzen eines systematischen Lifecyclemanagements und eines gemeinsamen Lagebildes verdeutlicht.

Im Fokus stehen die Reduktion kritischer Schwachstellen und der Aufbau grundlegender Sicherheitsstrukturen. Dazu gehören die Herstellung von Mindestschutz und Transparenz, der Aufbau von Sicherheitsbewusstsein auf allen Ebenen der Forschungseinrichtungen, sowie eine bessere Koordination zwischen Forschungseinrichtungen, insbesondere beim Austausch über Sicherheitsvorfälle und bei der Entwicklung gemeinsamer Lagebilder.

Vor diesem Hintergrund werden zwei besonders zentrale und kurzfristig wirksame Handlungsoptionen konkretisiert:

- *Automatisierte Assettransparenz* (Kapitel 5.1.1) schafft auf Einrichtungsebene Transparenz über IT-Systeme und deren Schwachstellen und ist damit eine wesentliche Grundlage resilienter Cybersicherheit.
- *Koordinierte Informations-, Austausch- und Unterstützungsstrukturen sowie ein gemeinsames Lagebild* (Kapitel 5.1.2) bündeln auf institutionenübergreifender Ebene Erkenntnisse aus Sicherheitsvorfällen und machen sie für gemeinsame Lernprozesse nutzbar.

Beide Optionen ergänzen sich: Verlässliche Transparenz innerhalb der Einrichtungen bildet eine wesentliche Grundlage für koordinierte Unterstützungsmaßnahmen und ein aussagekräftiges, einrichtungsübergreifendes Lagebild.

5.1.1 Automatisierte Assettransparenz: Fundament einer resilienten Cybersicherheit im Forschungsprozess

Die heterogenen und dezentral organisierten IT-Landschaften vieler Hochschulen und Forschungseinrichtungen erschweren eine vollständige Übersicht über die im Forschungsprozess eingesetzten digitalen Ressourcen. Forschungsgruppen betreiben häufig eigene Hard- und Software, Clouddienste oder Laborinfrastrukturen, die vielfach durch lokale Administrator/innen oder wissenschaftliche Beschäftigte ohne formale IT-Sicherheitsausbildung verwaltet werden (Hoffmann/Buchmann 2026). Dies begünstigt Schatten-IT, also nicht zentral erfasste Geräte, Dienste oder KI-Anwendungen (Annino 2026). Gleichzeitig verändern sich Forschungsumgebungen kontinuierlich, sodass statische Inventarlisten schnell veralten. Fehlende Transparenz über IT-, OT(Operational Technology)-, IoT(Internet of Things)- und Datenressourcen stellt daher eine grundlegende Schwachstelle der Cyberresilienz dar. Entscheidend ist dabei nicht eine einheitliche zentrale Steuerung, sondern ein kontinuierliches, gegebenenfalls auch KI-gestütztes Monitoring, das auch in heterogenen föderal organisierten Strukturen Veränderungen und Sicherheitslücken zeitnah erfasst, ohne die dezentrale, heterogene Struktur und methodische Vielfalt der Forschungslandschaft einzuschränken.

Ziel dieser Handlungsoption ist eine kontinuierliche, automatisierte Assettransparenz als Grundlage einer risikoorientierten Cybersicherheitsstrategie. Hierfür sollten Hochschulen und Forschungseinrichtungen automatisierte IT-Assetmanagementsysteme (ITAM) einführen bzw. bestehende Ansätze ausbauen, die über Programmierschnittstellen mit Clouddiensten, Virtualisie-

rungsplattformen sowie Netzwerk- und Sicherheitssystemen verbunden sind und Veränderungen der IT-Landschaft kontinuierlich erfassen. Das Inventar sollte sämtliche digitalen Ressourcen des Forschungsprozesses umfassen, darunter Hard- und Software, Clouddienste, Container, APIs, Labor- und Messsysteme (OT/IoT), KI-Modelle einschließlich Trainingsdatensätzen, Forschungsdaten und digitale Zwillinge. Gerade Laborgeräte und IoT-Komponenten weisen häufig Sicherheitsdefizite auf und sind bislang unzureichend in Sicherheitskonzepte integriert (Hoffmann/Buchmann 2026). Automatisierte Inventarisierung schafft dabei die notwendige Datengrundlage, ersetzt jedoch nicht die personellen und organisatorischen Ressourcen für Absicherung, Pflege und Lifecyclemanagement der erfassten Assets.

Die gewonnene Assettransparenz bildet die Grundlage für eine priorisierte, risikobasierte Bereinigung und Absicherung bestehender IT-Strukturen. Hierzu gehören die Abschaltung veralteter oder ungenutzter Systeme, die Konsolidierung redundanter Dienste, ein strukturiertes Patchmanagement sowie die Bereinigung historisch gewachsener Datenbestände. Ergänzend sollten schutzbedürftige Forschungsdaten und Datenflüsse identifiziert sowie Abhängigkeiten zwischen IT-Systemen und kritischen Forschungsprozessen dokumentiert werden. Auf dieser Grundlage können Netzwerke segmentiert, sensible Forschungsbereiche isoliert und sicherheitsorientierte IT-Architekturen schrittweise aufgebaut werden, ohne zentrale Forschungs- und Verwaltungsdienste zu beeinträchtigen[6] (BSI 2017, 2026a).

Kurzfristig sollten alle im Forschungsprozess eingesetzten Geräte und Dienste registriert, automatisierte Verfahren zur Identifikation unbekannter Assets eingeführt, privilegierte Benutzerkonten konsolidiert und durch verpflichtende Mehrfaktorauthentifizierung abgesichert, besonders schutzbedürftige Forschungsdaten identifiziert sowie ein strukturiertes Patchmanagement eingeführt werden. Bei OT-Umgebungen und Labortechnik, die aufgrund notwendiger Betriebsunterbrechungen nicht regelmäßig gescannt oder gepatcht werden können, sind insbesondere Segmentierung und Abschottung erforderlich, zum Beispiel durch Datendioden, die Daten physikalisch nur in eine Richtung übertragen und so einen Informationsabfluss erlauben, ohne einen Zugriff von außen zuzulassen. Die Umsetzung setzt personelle und finanzielle Ressourcen voraus. Zur Erhöhung der Akzeptanz sollte zugleich der Nutzen für Sicherheit, Reproduzierbarkeit und Nachvollziehbarkeit von Forschung gegenüber den Fachcommunities kommuniziert werden.

Die Umsetzung sollte nach Forschungseinrichtungstyp und Risikoprofil differenziert erfolgen, dabei aber einem einheitlichen Mindeststandard folgen. Hochschulen sollten insbesondere dezentrale IT-Strukturen besser integrieren, Schatten-IT reduzieren und einrichtungsübergreifende Mindeststandards etablieren. Bei außeruniversitären Forschungseinrichtungen stehen organisationsweite Standardisierung, Assetgovernance und standortübergreifende Transparenz im Vordergrund. KRITIS-relevante Forschungsinfrastrukturen wie Hochsicherheitslabore mit Erreger- und Toxinforschung (BSL-4-Labore) sollten kritische Assets risikobasiert priorisieren, konsequent segmentieren und kontinuierlich überwachen. Grundlegende Sicherheitsanforderungen müssen dabei mit der für Forschung und wissenschaftlichen Wettbewerb erforderlichen Flexibilität in Einklang gebracht werden.

Bund und Länder sind hier für die übergeordneten Rahmenbedingungen zuständig. Dem Bund bieten sich dabei mehrere Ansatzmöglichkeiten: die Entwicklung eines bundesweit einheitlichen Mindeststandards (Baseline Security), gegebenenfalls in Abstimmung mit den Ländern, die

6 BSI-Standard 200-2, perspektivisch ergänzt durch Grundschutz ++, die seit 2026 laufende, stärker automatisierbare und prozessorientierte Weiterentwicklung des IT-Grundschutzes

Förderung einrichtungsübergreifend nutzbarer Dienste zur systematischen Erfassung und Verwaltung von IT-Ressourcen (IT Asset Management, ITAM) und Sicherheitsdienste sowie – insbesondere für Medizin und Labortechnik – die Etablierung zeitlich befristeter Zertifizierungs- und Zulassungsverfahren, damit Haftungsfragen nicht länger regelmäßigen Aktualisierungen von Geräten entgegenstehen. Ergänzend sind gezielte Finanzierungsprogramme für die Modernisierung und Ablösung veralteter technischer Infrastrukturen erforderlich. Die Länder sollten öffentliche Hochschulen zu regelmäßigen IT-Bestandsaufnahmen verpflichten und Investitionsmittel für grundlegende Sicherheitsmaßnahmen bereitstellen.

Auf Einrichtungsebene tragen Hochschul- und Institutsleitungen die strategische Verantwortung für Assetmanagement und Ressourcenausstattung (Annino 2026; Hofer 2026; Sommerhäuser 2026). Chief Information Officer und IT-Sicherheitsbeauftragte können die Inventarisierungsstrategie entwickeln und sie in das Informationssicherheitsmanagement integrieren (Annino 2026), zentrale IT-Abteilungen können Auswahl, Betrieb und Pflege der ITAM-Systeme verantworten (Hoffmann/Buchmann 2026; Richter 2025). Forschungsgruppen und lokale Administrator/innen können die Erfassung spezialisierter Forschungsinfrastrukturen und Aktualität der Inventardaten gezielt unterstützen (Hoffmann/Buchmann 2026). Personalabteilungen können dies durch strukturierte On- und Offboardingprozesse begleiten; externe IT-Dienstleister könnten zur transparenten Dokumentation eingesetzter Systeme und Dienste verpflichtet werden (Richter 2025; Sommerhäuser 2026).

5.1.2 Koordinierte Informations-, Austausch- und Unterstützungsstrukturen sowie ein gemeinsames Lagebild

Die Gewährleistung von Cybersicherheit in Forschungsumgebungen wird neben heterogenen IT-Landschaften durch unklare Verantwortlichkeiten und unzureichende Austauschstrukturen erschwert. Cyberangriffe erfolgen zunehmend professionalisiert, automatisiert und KI-gestützt, Sicherheitsinformationen bleiben jedoch häufig auf einzelne Einrichtungen oder Forschungsgruppen beschränkt (Schneider et al. 2025; VDI Research 2023). Mit dem Arbeitskreis Sicherheit und Wissenschaft (AK SuWi) und dem Arbeitskreis Informationssicherheit der deutschen Forschungseinrichtungen (AKIF) bestehen bereits Austauschstrukturen zwischen Sicherheitsbehörden und Wissenschaftsorganisationen, die jedoch nicht alle Einrichtungen und Vorfälle systematisch erfassen. Erkenntnisse aus Sicherheitsvorfällen werden dadurch nur unzureichend geteilt und Bedrohungen wie Ransomware, gezielter Datendiebstahl oder Datenmanipulation teilweise verspätet erkannt. Zudem fehlt ein übergreifendes Lagebild, das operative Sicherheitsinformationen mit einer vorausschauenden Bewertung neuer Bedrohungen verbindet. Der Aufbau entsprechender Strukturen erfordert dauerhaft verfügbare personelle und finanzielle Ressourcen, da Cybersicherheit als kontinuierliche Aufgabe angelegt werden muss.

Ziel der Handlungsoption ist der Aufbau koordinierter Informations-, Austausch- und Unterstützungsstrukturen, die ein gemeinsames Lagebild ermöglichen und Erkenntnisse aus Sicherheitsvorfällen für die Cyberresilienz des gesamten Forschungssystems nutzbar machen. Im Sinne einer gestuften Verantwortung nach dem Prinzip der Subsidiarität tragen hierbei alle Akteure auf individueller, institutioneller sowie auf Landes- und Bundesebene zur systematischen Stärkung der Forschungs- und Wissenssicherheit bei, um Risiken wie den unerwünschten Wissens- und

Technologieabfluss oder unzulässige Einflussnahme proaktiv zu managen (Allianz der Wissenschaftsorganisationen 2019; Gärtner 2026). Die Länder sollten hierfür bestehende Verbundstrukturen und hochschulübergreifende Kooperationen stärken – etwa im Rahmen von Landesdigitalverbünden –, um resiliente institutionelle Sicherheitsstrukturen vorzuhalten. Der Bund sollte einen ganzheitlichen Ansatz entwickeln und die dafür notwendigen Ressourcen bereitstellen. Einen Ansatzpunkt bietet die für 2027 geplante Nationale Plattform für Forschungssicherheit, deren Anspruch weit über ein reines Lagebild hinausgeht, da sie in Kooperation mit den zuständigen Stellen eine fortlaufende nationale Risikoanalyse zur Erkennung zukünftiger Bedrohungen und Vulnerabilitäten durchführt. Sie soll Hochschulen und außeruniversitäre Forschungseinrichtungen aktiv bei der Einschätzung von Kooperationen, Forschungsthemen und beteiligten Personen oder Institutionen unterstützen, Risiken und Chancen international ausgerichteter Zusammenarbeit bewerten helfen und dazu koordinierend, informierend und beratend tätig werden, ohne jedoch eigen Entscheidungsbefugnisse zu haben (BMFTR 2025). Größere Einrichtungen sollten zentrale Cyberkoordinationsstellen etablieren, die Meldungen dezentraler IT-Verantwortlicher bündeln, Sicherheitsvorfälle bewerten und externe Bedrohungsinformationen, etwa des BSI, zielgruppengerecht aufbereiten (Drews/Łabuz 2026; Hoffmann/Buchmann 2026; HRK 2025). Darauf aufbauend sollten kontinuierlich aktualisierte Cyberlagebilder Informationen aus automatisierten Assetmanagementsystemen (welche Systeme und Daten sind wo vorhanden) mit Threat Intelligence (aufbereitete Informationen zu aktuellen Bedrohungs- und Angriffsmustern) und Strategic Foresight (systematische Vorausschau auf zukünftige Risikoentwicklungen) verknüpfen. Neben dem aktuellen Sicherheitsstatus sollten durch Horizon-Scanning als ein zentrales Verfahren der Strategic Foresight auch zukünftige Bedrohungen, beispielsweise durch KI-gestützte Angriffe, systematisch berücksichtigt werden (Drechsler 2026; Sommerhäuser 2026). Perspektivisch könnte auf europäischer Ebene ein gemeinsames Lagebild für Cyberbedrohungen im Forschungsbereich entstehen (Drews/Łabuz 2026). Meldewege und Reaktionsprozesse sollten dabei möglichst schlank und automatisiert gestaltet werden, sodass sie mit der Geschwindigkeit KI-gestützter Angriffe Schritt halten können; langwierige, mehrstufige, bürokratische Prozesse würden die intendierte Resilienzwirkung des Lagebildes konterkarieren.

Die organisationsübergreifende Zusammenarbeit sollte zugleich durch standardisierte Unterstützungs- und Austauschformate gestärkt werden. Ein Ansatz sind Cybersecurity Clinics, in denen Hochschulen, Forschungseinrichtungen, Studierende und externe Expert/innen gemeinsam Risikoanalysen, Penetrationstests und Sicherheitsberatungen durchführen (Geppert et al. 2026). Ergänzend sollten niedrigschwellige Beratungsangebote, etwa in Kooperation mit gemeinnützigen Organisationen (zum Beispiel DFN – Deutsches Forschungsnetz, ZKI – Zentren für Kommunikation und Informationsverarbeitung als Zusammenschluss der Hochschulrechenzentren e.V.) über Rahmenverträge, verfügbar sein und auch die psychologische Begleitung Betroffener nach Cyberangriffen und Erpressungsversuchen umfassen (HRK 2025). Anonymisierte Vorfallberichte, Threat Intelligence und erprobte Incident-Response Playbooks als standardisierte Handlungsanleitungen zur Reaktion auf Sicherheitsvorfälle sollten systematisch zwischen Einrichtungen ausgetauscht werden. An bestehende Ansätze kann dabei angeknüpft werden, zum Beispiel an das vom Arbeitskreis Informationssicherheit des ZKI gemeinsam mit dem BSI entwickelte BCM(Business Continuity Management)-Profil[7], für Hochschulen. Ein weiterer Ansatz ist der Austausch von Indicators for Compromise (IoCs), also technischen Spuren wie auffälligen Dateien, IP-Adressen oder Netzwerkmustern, die auf einen laufenden oder bereits erfolgten Cyberangriff deuten,

7 Profil zur Aufrechterhaltung kritischer Prozesse im Notfall

zwischen BSI, Landessicherheitsbehörden, DFN-CERT und hochschuleigenen Einheiten zur Überwachung und Analyse von Sicherheitsvorfällen (SOCs – Security Operations Center). Eine stärkere Automatisierung und Vernetzung dieses Austauschs kann gemeinsame Lernprozesse und eine schnellere Reaktion auf neue Angriffsmuster unterstützen. Bund und Länder können dies über koordinierende Stellen, Sicherheitsbehörden und Forschungsverbünde fördern. Entscheidend ist der Rückfluss gewonnener Erkenntnisse in die Einrichtungen, damit Sicherheitsvorfälle zu organisationalem Lernen und zur kontinuierlichen Verbesserung technischer und organisatorischer Sicherheitsmaßnahmen beitragen.

Kurzfristig sollten zentrale Melde- und Eskalationsprozesse für Sicherheitsvorfälle sowie standardisierte Incident-Reporting-Formate etabliert, erste gemeinsame Lagebilder auf Verbund- oder Landesebene entwickelt, gemeinsame Cybersicherheitsübungen durchgeführt und sichere Plattformen für den Austausch anonymisierter Vorfallinformationen und Bedrohungsdaten sowie die Einrichtung sicherer Plattformen für den Austausch anonymisierter Vorfall- und Bedrohungsdaten eingerichtet werden. Diese Prozesse sollten von Beginn an möglichst automatisiert gestaltet werden, um mit der Dynamik aktueller Bedrohungslagen Schritt zu halten.

Die Umsetzung sollte nach Einrichtungstyp, Schutzbedarf und Risikoprofil differenziert erfolgen. Hochschulen sollten insbesondere den Austausch zwischen Fakultäten, Instituten und zentraler IT stärken; außeruniversitäre Forschungseinrichtungen können organisationsweite Lagebilder und standortübergreifende Sicherheitsnetzwerke etablieren. Für KRITIS-relevante Forschungsinfrastrukturen sind darüber hinaus ein kontinuierliches Sicherheitsmonitoring, Echtzeitlagebilder und mit nationalen Sicherheitsbehörden abgestimmte Krisenreaktionsprozesse erforderlich.

Klare Verantwortlichkeiten sind eine zentrale Voraussetzung für die Umsetzung. Hochschul- und Institutsleitungen können die strategische Verankerung der Cybersicherheit verantworten, Ressourcen bereitstellen und Kooperationsvereinbarungen mit Partnerinstitutionen schließen (Sommerhäuser 2026). Chief Information Security Officer (CISO) und IT-Sicherheitsbeauftragte können das institutionelle Lagebild koordinieren, Berichts- und Eskalationswege definieren und damit Regeln festlegen, wer bei einem Vorfall wann informiert wird und wer dann entscheidet. Darüber hinaus können sie Maßnahmen in das Informationssicherheitsmanagement integrieren und Notfallpläne zur Aufrechterhaltung eines eingeschränkten Forschungsbetriebs im Falle eines Sicherheitsvorfalles entwickeln (Naß et al. 2026). CISO-Strukturen sind an Hochschulen bereits verbreitet (Dreyer 2026); bei außeruniversitäre Forschungseinrichtungen, für die bislang kaum belastbare Daten vorliegen, könnten Informationssicherheitsbeauftragte benannt werden, bei kleineren Einrichtungen gegebenenfalls in überinstitutionellen regionalen oder fachlichen Strukturen. Zentrale IT- und Cybersecurityteams können Monitoringplattformen betreiben, Sicherheitsvorfälle analysieren und dezentrale Administrator/innen unterstützen (Hoffmann/Buchmann 2026; Naß et al. 2026). Landesweite SOC- und CERT-Strukturen können den Informationsaustausch und koordinierte Reaktionen auf Sicherheitsvorfälle zusätzlich stärken. Forschungsgruppen und lokale Administrator/innen können Sicherheitsvorfälle melden, lokale Schutzmaßnahmen umsetzen und sich an Awareness- und Schulungsmaßnahmen beteiligen (Hoffmann/Buchmann 2026). Externe Partner – insbesondere das BSI und kooperierende Forschungseinrichtungen – können bei Threat Intelligence, der Harmonisierung von Sicherheitsstandards und der Bewältigung größerer Sicherheitsvorfälle unterstützen (Drews/Łabuz 2026). Bestehende Strukturen und Rollen könnten damit flächendeckend etabliert und Verantwortlichkeiten klar kommuniziert werden, damit bestehende gute Praxis nicht auf Einzelfälle beschränkt bleibt.

Ein gemeinsames Cybersicherheitslagebild ist damit nicht allein eine technische Infrastruktur, sondern Bestandteil eines kontinuierlichen institutionenübergreifenden Lernprozesses. Die systematische Bündelung und Rückkopplung von Sicherheitsinformationen und Expertise stärkt die Reaktions- und Anpassungsfähigkeit des Forschungssystems gegenüber dynamischen Cyberbedrohungen (Heinbach/Pagel 2026). Voraussetzung sind ausreichend Zeit, qualifiziertes Personal und dauerhaft verfügbare Finanzmittel. Diese könnten durch die zuständigen Ministerien unbürokratisch bereitgestellt werden, gebunden an die Vorlage belastbarer Umsetzungspläne und eine regelmäßige Überprüfung hinsichtlich ihrer Wirksamkeit. Befristete Stellen sind möglichst zu vermeiden, da sie die notwendige Personalgewinnung strukturell erschweren. Ergänzend ist, wie in Handlungsoption 5.2.1. beschrieben – eine Fort- und Weiterbildungsstrategie erforderlich, um die notwendigen Kompetenzen aufzubauen.

5.2 Mittelfristige Optionen: differenzieren und institutionell verankern

Der mittelfristige Möglichkeitsraum (3 bis 5 Jahre) adressiert zentrale strukturelle Defizite der dargestellten Szenarien. In Szenario 1 betrifft dies insbesondere den Fachkräftemangel, fehlende Kompetenzen und ein schwach ausgeprägtes Sicherheitsbewusstsein. Szenario 2 verdeutlicht darüber hinaus Defizite in der Datengovernance, die angesichts des hohen ökonomischen und geopolitischen Werts vieler Forschungsdaten und der damit verbundenen Sicherheitsbedarfe besonders relevant sind. Szenario 3 zeigt demgegenüber wesentliche Elemente eines Zielbildes: Sicherheitsbewusstsein ist auf allen Ebenen und insbesondere bei Führungskräften verankert, Forschungsdaten werden lebenszyklusorientiert gemanagt und ihre Schutzbedarfe systematisch differenziert. Auch der langfristige Personal- und Kompetenzaufbau ist weit fortgeschritten. Verbleibende Abhängigkeiten von einzelnen Kompetenzträgern und externen Dienstleistern verdeutlichen jedoch, dass auch hier weiterer struktureller Handlungsbedarf besteht.

Im Zentrum des mittelfristigen Möglichkeitsraums stehen der Aufbau und die institutionelle Verankerung von Kompetenzen und Personal sowie die Etablierung nachhaltiger, langfristiger Strukturen für Datenmanagement und die differenzierte Berücksichtigung der Schutzbedarfe von Forschungsdaten.

Vor diesem Hintergrund werden drei Handlungsoptionen konkretisiert:

- Der gezielte Aufbau von Personal und die institutionelle Verankerung von Cybersicherheit im Forschungsprozess (Kapitel 5.2.1) schafft dedizierte Zuständigkeiten und stärkt durch klare Rollenprofile, Entwicklungsperspektiven und wettbewerbsfähige Vergütung die personelle Basis für Cybersicherheit.
- Die stärkere Integration von Cybersicherheit in Forschung und Lehre (Kapitel 5.2.2) stärkt durch die Verankerung im Studienverlauf sowie kontinuierliche Sensibilisierungs- und Weiterbildungsmaßnahmen Sicherheitsbewusstsein und Kompetenzen.
- Die Differenzierung von Forschungsdaten nach Schutzbedarfen (Kapitel 5.2.3) verbindet Schutz und Nutzbarkeit durch Orientierungshilfen, standardisierte Datenmanagementpläne und transparente, an Datentyp und Schutzbedarf angepasste Zugangsverfahren.

5.2.1 Personalaufbau und institutionelle Verankerung von Cybersicherheit im Forschungsprozess

In zwei der beschriebenen Szenarien bleiben Personalengpässe eine zentrale Hürde für die effektive Umsetzung von Cybersicherheitsmaßnahmen an Universitäten und außeruniversitären Forschungseinrichtungen. Hinzu kommen die häufig fragmentierten, unübersichtlichen Governancestrukturen in vielen Einrichtungen sowie unklare interne Verantwortlichkeiten hinsichtlich Cybersicherheit. Viele Lösungsansätze scheitern nicht an fehlender Technik oder fehlende Vorgaben, beispielsweise zu Informationssicherheitsmanagementsystemen (ISMS) und Business Continuity Management Systemen, sondern an mangelnder Umsetzung infolge von Schnittstellenproblemen und Missverständnissen sowie an der unzureichenden Integration von Sicherheit in den Forschungsalltag. Vor diesem Hintergrund kommt einer strukturellen Zuweisung und klaren Definition von Verantwortlichkeiten sowie dem Aufbau von Personal mit Cybersicherheitsexpertise eine zentrale Bedeutung zu.

Cybersicherheitsfachkräfte werden im Forschungsprozess auf allen Ebenen benötigt. Das Spektrum reicht von Chief Information Security Officers über operative Stellen in Rechenzentren bis hin zu Fachkräften für sicherheitsbezogene Beratung von Lehrstühlen und Forschungsgruppen. Auch für die Sicherung von Forschungsdaten sowie den Betrieb und die Nutzung von Dateninfrastrukturen sind dauerhaft beschäftigte IT-Fachkräfte mit Kompetenzen in Cybersicherheit und Datenkuratierung erforderlich (DFG 2026). Der Bedarf trifft auf einen bereits angespannten Arbeitsmarkt: Die Zahl der Stellenausschreibungen mit Cybersicherheitsbezug ist von 2019 bis 2022 von 117.000 auf über 250.000 pro Jahr gestiegen und lag 2024 nach einem konjunkturbedingten Rückgang bei 203.000 pro Jahr (Büchel et al. 2025), während laut der ISC2 Cybersecurity Workforce Study 2025 rund 92% der befragten Unternehmen in Deutschland bereits über negative Folgen durch fehlende Cybersecurityfachkräfte berichten. Besonders der öffentliche Sektor ist von Rekrutierungsproblemen betroffen, wozu auch Hochschulen und zum Teil außeruniversitäre Forschungseinrichtungen gehören (TAB 2025a, 2026). Die personellen Ressourcen für spezifische Cybersicherheitsaufgaben müssen zusätzlich aufgebaut werden und dürfen nicht überwiegend durch eine Umverteilung bestehender IT-Kapazitäten erfolgen: Werden zu viele personelle Ressourcen aus der bestehenden IT-Abteilung umgewidmet, können andere Aufgaben und Dienstleistungen beim Bereitstellen der IT- und Forschungsinfrastruktur wegfallen. Zudem sollten IT-Sicherheit und IT-Bereitstellung bzw. Betrieb ausreichend getrennt organisiert sein: Es braucht einen Chief Information Officer (CIO) sowie einen Chief Information Security Officer (CISO), da es Zielkonflikte zwischen Sicherheitsinteressen und anderen Zielsetzungen in der Gestaltung der IT-Architektur geben kann (WR 2023).

Um diese Fachkräfte gewinnen und langfristig binden zu können, könnten Stellen, die für die Cybersicherheit zentral sind, wettbewerbsfähig vergütet werden. Dies kann – insbesondere angesichts des allgemeinen Fachkräftemangels im Bereich der IT-Sicherheit – auch übertarifliche Vergütungsmodelle und flexiblere Eingruppierungsmöglichkeiten umfassen, z.B. durch die Schaffung von mehr Stellen im höheren Dienst (HRK 2025; WR 2023). Ergänzend zur Anpassung der Vergütungsstrukturen können klar definierte Rollenprofile sowie transparente Karriere- und Entwicklungspfade die Attraktivität entsprechender Positionen zusätzlich erhöhen. Der generelle IT- und Cybersicherheitsfachkräftemangel erschwert die Gewinnung von Fachkräften auch in der

Forschung – die Stärkung von Aus- und Weiterbildung sowie das Steigern der Attraktivität von Quereinstiegen in diesem Bereich sind daher ebenso entscheidend.

Hochschulen und Forschungseinrichtungen sollten neue Rollenprofile etablieren. Je nach Größe und Forschungsprofil könnten beispielsweise spezialisierte Research Security Officers, KI-Expert/innen und Data Scientists mit Sicherheitskompetenzen sinnvoll sein, sowie generell übergreifende Fachprofile an der Schnittstelle von Forschung, IT und Informations- bzw. Cybersicherheit. Solche Rollen können dazu beitragen, Sicherheitsanforderungen stärker in den Forschungsprozess selbst zu integrieren und gleichzeitig den spezifischen Anforderungen unterschiedlicher Disziplinen gerecht zu werden. Diese Rollen könnten in klar organisierte Cybersicherheitsstrukturen eingebunden sein, denen ein Informationssicherheitsbeauftragter vorsteht. Die CISO-Funktion muss über klare Befugnisse und Ressourcenhoheit verfügen und sollte als unbefristete Kernstelle zu wettbewerbsfähigen Konditionen ausgestaltet sein. Ziel der Schaffung zentral organisierter Strukturen, die sich aber auch in unterschiedliche Forschungsbereiche verzweigen, ist es, verbindliche Prozesse und klarere Verantwortlichkeiten zu schaffen. Gleichzeitig sollte das Bewusstsein für die individuelle Verantwortung aller in Forschungseinrichtungen tätigen Personen gestärkt und ein verantwortungsvolles sowie sicherheitsorientiertes Verhalten systematisch gefördert werden. Für kleine Einrichtungen kann es sinnvoll sein, regional übergreifend organisierte Strukturen zu etablieren. Bund und Länder können durch strukturelle Reformen zum Personalaufbau beitragen, etwa durch die Festlegung von Mindestanteilen unbefristeter Stellen in sicherheitskritischen Bereichen. Entfristete Stellen erhöhen nicht nur die Attraktivität entsprechender Tätigkeitsfelder im Wettbewerb mit der Privatwirtschaft, sondern tragen vor allem dazu bei, Cybersicherheits-Know-how, Verantwortlichkeiten und klare Ansprechpersonen dauerhaft in den Einrichtungen zu verankern (HRK 2025).

Der Einsatz sicher betriebener KI zur Angriffserkennung und gegebenenfalls auch zur Unterstützung der Angriffsabwehr wird aufgrund zunehmend komplexer Angriffe immer wichtiger. Solche Werkzeuge ermöglichen Effizienzgewinne und können Sicherheitsverantwortliche entlasten. Dies kann den bestehenden Fachkräftemangel jedoch nur teilweise abmildern und ersetzt den Bedarf an qualifiziertem Personal nicht.

5.2.2 Verantwortete Freiheit: Cybersicherheitskultur in Forschung und Lehre

Während die Erneuerung und Absicherung der technischen Infrastruktur eine wesentliche Voraussetzung für die Cybersicherheit in Wissenschaft und Forschung ist, kommt auch dem individuellen Handeln von Forschenden und Beschäftigten eine zentrale Bedeutung zu. Viele Angriffe wie Social Engineering oder Phishing setzen gezielt am menschlichen Verhalten an und können durch technische Schutzmaßnahmen allein nicht abgewehrt werden. Es bedarf daher unterschiedlicher Maßnahmen, um das Bewusstsein für Cyberrisiken zu stärken und Cybersicherheitskompetenzen auf allen Ebenen des Wissenschaftssystems systematisch auszubauen.

Das Ziel dieser Handlungsoption besteht darin, ein Verständnis von verantworteter Freiheit zu entwickeln, das den Grundwert der Wissenschaftsfreiheit wahrt und gleichzeitig das Bewusstsein für die mit Forschung verbundenen Sicherheitsrisiken stärkt. Wissenschaftliche Freiheit und Cybersicherheit sollten dabei nicht als Gegensätze verstanden werden, sondern als miteinander zu vereinbarende Ziele, die gemeinsam verantwortungsvoll ausgestaltet werden.

Hierfür sollte bereits im Studium angesetzt werden. Cybersicherheit und Forschungssicherheit sollten dauerhaft in den Curricula verankert werden (Gemeinsamer Ausschuss 2024; HRK 2025). Aspekte der Cybersicherheit und sicherheitsrelevante Fragestellungen können, ähnlich wie und gegebenenfalls gemeinsam mit den Grundlagen wissenschaftlichen Arbeitens, bereits in Bachelorstudiengänge integriert werden. In Kursen zu guter wissenschaftlicher Praxis sollte der Aspekt Cybersicherheit ausgebaut werden. Auch in die Vermittlung von KI-Kompetenzen sollte ein Umgang mit Cybersicherheit integriert werden. Im weiteren Studienverlauf sollten disziplinspezifische sowie interdisziplinäre Aspekte vertieft behandelt werden. Promovierende sollten sich intensiv mit den aktuellen Risiken ihres jeweiligen Forschungsfeldes sowie übergreifenden Entwicklungen auseinandersetzen. Hierfür bedarf es geeigneter Veranstaltungsformate, beispielsweise Seminare, Workshops oder Summer Schools. Um eine solche Verankerung in der Lehre zu ermöglichen, müssen Lehrende entsprechend qualifiziert werden (Gemeinsamer Ausschuss 2024).

Neben der akademischen Ausbildung sind kontinuierliche Sensibilisierungs- und Weiterbildungsmaßnahmen zur Cybersicherheit für alle Beschäftigten an Forschungseinrichtungen erforderlich. Hierzu gehören leicht zugängliche Informationsmaterialien, regelmäßige Schulungen, möglicherweise verpflichtend, sowie praxisnahe Übungen für Mitarbeitende aller Ebenen einschließlich der Leitungsebene, ähnlich wie Brandschutzübungen (HRK 2025; Plattner 2025). Ausgestaltet als Planspiele oder Simulationen von Cybervorfällen können sie dazu beitragen, Handlungsroutinen zu etablieren und das Sicherheitsbewusstsein nachhaltig zu stärken. Für kleinere außeruniversitäre Forschungseinrichtungen können solche Schulungs- und Übungsformate auch gemeinsam in Verbünden organisiert werden, um Ressourcen effizient zu bündeln. Neben der akademischen Ausbildung sind kontinuierliche Sensibilisierungs- und Weiterbildungsmaßnahmen zur Cybersicherheit für alle Beschäftigten an Forschungseinrichtungen erforderlich. Hierzu gehören leicht zugängliche Informationsmaterialien, regelmäßige Schulungen, möglicherweise verpflichtend, sowie praxisnahe Übungen für Mitarbeitende aller Ebenen einschließlich der Leitungsebene, ähnlich wie Brandschutzübungen (HRK 2025; Plattner 2025). Ausgestaltet als Planspiele, Simulationen oder Szenarien von Cybervorfällen können sie dazu beitragen, Handlungsroutinen zu etablieren und das Sicherheitsbewusstsein nachhaltig zu stärken. Für kleinere außeruniversitäre Forschungseinrichtungen können solche Schulungs- und Übungsformate auch gemeinsam in Verbünden organisiert werden, um Ressourcen effizient zu bündeln.

Darüber hinaus bedarf es eines kontinuierlichen Dialogs zwischen IT-Abteilungen, Cybersicherheitsverantwortlichen und Forschenden. Einerseits müssen die spezifischen Anforderungen und Arbeitsweisen der Forschung verstanden werden, andererseits müssen die Grenzen und Risiken aus Sicht der Cybersicherheit transparent vermittelt werden. Rollenspezifisch zugeschnittene Schulungen, die die Anforderungen beider Seiten vermitteln, können diesen Dialog unterstützen. Ziel sollte es sein, gemeinsam Lösungen zu entwickeln, die Forschenden die notwendigen Experimentierräume und die Ausübung wissenschaftlicher Freiheit ermöglichen und gleichzeitig ein angemessenes Sicherheitsniveau gewährleisten. Dieser Dialog muss als fortlaufender Prozess verstanden werden, da sich sowohl Bedrohungslagen als auch die Anforderungen der Forschung kontinuierlich verändern. Zudem unterscheiden sich die Bedürfnisse je nach Fachdisziplin sowie Art und Größe der Forschungseinrichtung teilweise erheblich, sodass einheitliche Lösungen nur begrenzt geeignet sind.

Die Länder können hier den Rahmen schaffen, in dem für die Integration von Cybersicherheit in die Lehre Studien- und Prüfungsordnungen gegebenenfalls angepasst werden; der Bund kann

diese Entwicklungen unterstützen. Bund, Länder, Wissenschaftsorganisationen sowie Forschungseinrichtungen sollten gemeinsam abgestimmte Grundlagen für Schulungs- und Übungsmaßnahmen entwickeln, um ein gemeinsames Sicherheitsverständnis zu fördern, gegenseitiges Lernen zu ermöglichen und organisationsübergreifend vergleichbare Kompetenzstandards aufzubauen. Hochschulen und Forschungseinrichtungen sollten diese einrichtungsspezifisch umsetzen, regelmäßig evaluieren und kontinuierlich verbessern. Besondere Aufmerksamkeit bei den Sensibilisierungs- und Weiterbildungsmaßnahmen verdient KI-gestütztes Social Engineering, das zunehmend forschungsspezifische Angriffsvektoren nutzt: Deepfakegestützte Anrufe oder Videoanfragen, die sich als Kolleg/innen, Gutachter/innen oder Fördermittelgeber ausgeben, um an unveröffentlichte Forschungsdaten, Gutachteninhalte oder Drittmittel zu gelangen, sowie gezielte, KI-personalisierte Angriffe auf Forschende in Bereichen mit hoher IP- oder Dual-Use-Relevanz. Multivektorielle Phishingkampagnen, die E-Mail, Sprache und Messenger-Dienste kombinieren, sowie ein Anstieg deepfakegestützter Social-Engineering-Angriffe um 40 % gegenüber dem Vorjahr (BSI 2025) verdeutlichen, wie sich generative KI zu einem ernstzunehmenden Bedrohungsvektor entwickelt hat – eine Entwicklung, die für den Bildungssektor (inklusive Hochschulen) als international überdurchschnittlich von Cyberattacken betroffener Sektor (Check Point 2026) hochgradig relevant ist. Aktuelle Entwicklungen in den Angriffsvektoren sollten deshalb regelmäßig in Weiterbildungsmaßnahmen vermittelt werden. Die im Wissenschaftssystem übliche Offenheit gegenüber neuen Kooperations- und Kontaktanfragen erhöht dabei die Anfälligkeit gegenüber täuschend echten Fakeanfragen zusätzlich. Awareness- und Schulungsformate sollten daher gezielt auf diese forschungsspezifischen Angriffsmuster ausgerichtet werden, etwa durch Verifikationsprozesse bei ungewöhnlichen Anfragen und eine grundsätzlich kritische Prüfhaltung auch gegenüber vermeintlich bekannten Kontakten.

5.2.3 Forschungsdaten: Differenzierung von Schutzbedarfen sowie Sicherstellen von Integrität und Verfügbarkeit

Infolge zunehmender Cyberbedrohungen und geopolitischer Fragmentierung gewinnt die strategische Sicherung von Forschungsdaten massiv an Bedeutung, wobei das Spannungsverhältnis zwischen dem Schutz der Forschungsdaten einerseits und ihrer wissenschaftlich essenziellen Verfügbarkeit andererseits eine systematische Differenzierung der Schutzbedarfe erfordert. Während sensible Datensätze hinsichtlich Vertraulichkeit und Integrität wirksam gegen verdeckte Manipulation und unbefugten Abfluss geschützt werden müssen, bildet die langfristige Zugänglichkeit die zwingende Voraussetzung für die Validität, Replikation und den weiteren globalen Erkenntnisgewinn. Um dieser Zielkollision wirksam zu begegnen, bedarf es risikobasierter Sicherheitskonzepte, die den spezifischen Forschungskontext berücksichtigen und Cybersicherheit als integralen Bestandteil der Regeln guter wissenschaftlicher Praxis verankern.

Ziel dieser Handlungsoption ist es, durch die Bereitstellung systematischer Orientierungshilfen und standardisierter Verfahren eine fundierte Einschätzung von Schutzbedarfen unterschiedlicher Forschungsdaten zu ermöglichen und so die Resilienz gegenüber hybriden Bedrohungen zu stärken. Dabei soll ein ausgewogener Umgang mit sensiblen Daten etabliert werden, der notwendige Schutzvorkehrungen mit dem Ziel einer größtmöglichen wissenschaftlichen Offenheit und effizienten Datennutzung in Einklang bringt (De-Risking) (Gärtner 2026).

Diese Differenzierung wird zunehmend anspruchsvoller, da heute potenziell alle Disziplinen inklusive der Rechts-, Geistes- und Sozialwissenschaften, aber auch die Grundlagenforschung sicherheitsrelevante Erkenntnisse hervorbringen können (WR 2025b). Forschungseinrichtungen und Forschende benötigen daher geeignete Orientierungshilfen, um Schutzbedarfe fundiert einschätzen und angemessene Maßnahmen ableiten zu können.

Gleichzeitig muss die wissenschaftliche Nutzbarkeit sensibler Forschungsdaten gewahrt bleiben. Gesundheitsdaten zeigen beispielhaft, dass dies möglich ist, wenngleich aktuelle Verfahren oft durch komplexe, langwierige und uneinheitliche Zugangsverfahren fragmentiert sind (TAB 2022). Für sensible Datenbestände sollten daher schnelle, transparente und einheitliche Zugangsverfahren geschaffen werden, die ein hohes Sicherheitsniveau garantieren, ohne die Forschungsagilität durch übermäßige Bürokratie einzuschränken. Klare, übergreifende Regelungen und Rahmenbedingungen zur Klassifizierung unterschiedlicher Datentypen nach ihrer Sensitivität helfen Forschungseinrichtungen dabei, diese Zugriffsprozess sicher zu organisieren und zu verwalten (Heo/Grable 2026; Sitarska et al. 2026).

Strukturelle, organisatorische und technische Maßnahmen sind nur dann wirksam, wenn sie durch ein verantwortungsvolles Verhalten der Forschenden ergänzt werden (Faktor Mensch). Neben dem Aufbau einer Sicherheitskultur ist die Erstellung strukturierter Datenmanagementpläne (DMP) bereits bei Projektbeginn essenziell, um Maßnahmen für Vertraulichkeit, Integrität und langfristige Verfügbarkeit festzulegen. Da vor allem kleinere Einrichtungen oft unter personellen Engpässen leiden, sind standardisierte Orientierungshilfen mit Leitfragen und Handlungsempfehlungen (zum Beispiel zu Zugriffsschutz, Datensicherung oder Langzeitspeicherung) unverzichtbar, um Schutzbedarfe systematisch einzuordnen und das Risiko einer systematischen Unterinvestition in die Datensicherheit zu vermeiden (Richter 2025). Zur Gewährleistung der wissenschaftlichen Nachnutzbarkeit sollten Forschende im Dialog mit den wissenschaftlichen Fachgesellschaften fachspezifische Metadatenstandards und Dokumentationsroutinen etablieren. Die Sicherung auf institutions- und regionsübergreifenden Infrastrukturen ist dabei essenziell, um die langfristige Datenverfügbarkeit über die Projektlaufzeit hinaus infrastrukturell abzusichern (DFG 2026).

Auf Ebene der Forschungseinrichtungen ist eine der zentralen Aufgaben, Forschenden durch klare Prozesse zur Prüfung von Sicherheitsbedarfen Orientierung zu bieten. Zudem kann die Erstellung eines regelmäßig zu aktualisierenden Datenkatalogs, der einen Überblick über die vorhandenen Daten einer Einrichtung gibt, die Abstimmung und Umsetzung von Verantwortlichkeiten und Zugriffsrechten erleichtern (WR 2023). Für Einrichtungen, die in besonders sicherheitsrelevanten Forschungsfeldern arbeiten oder mit hochsensiblen Daten umgehen, ist die Identifikation der Sicherheitsanforderungen und die Umsetzung hoher Sicherheitsstandards besonders akut. Um Ressourcenengpässe insbesondere in kleineren Einrichtungen zu kompensieren, sind der Aufbau von Kompetenznetzwerken und das Teilen bewährter Verfahren und gut funktionierender technischer Infrastrukturlösungen zwingend erforderlich. Besonders sensible Forschungsdaten bedürfen einer strikten Netzwerksegmentierung und Speicherung in geschützten, vom regulären Betrieb abgetrennten Sicherheitszonen. Gleichzeitig kommt der Sicherstellung der Verfügbarkeit eine zentrale Bedeutung zu. Hierfür sind redundante Datensicherungen notwendig, vorzugsweise nach dem 3-2-1-Backupkonzept oder nach erweiterten Konzepten wie dem 3-2-1-1-0-Prinzip. Dieses sieht vor, dass drei Kopien der Daten auf zwei verschiedenen Speichermedien gespeichert werden, von denen sich mindestens eine Kopie an einem externen Standort befindet. Außerdem

muss mindestens eine Kopie offline bzw. unveränderbar gespeichert und die Wiederherstellbarkeit regelmäßig fehlerfrei, also mit null Fehlern, überprüft werden. Darüber hinaus sind Konzepte zur sicheren Langzeitarchivierung sowie belastbare Wiederherstellungskonzepte für Verwaltungs- und Forschungsdaten erforderlich.

Auf Ebene von Bund, Ländern und Forschungsverbünden ist der dauerhafte Betrieb resilienter, einrichtungsübergreifender Forschungsdateninfrastrukturen zentral, da die langfristige Datenverfügbarkeit nicht allein einrichtungsintern gesichert werden kann. Länder sollten deshalb gemeinsam genutzte Basisdienste ausbauen, bei denen einzelne Forschungseinrichtungen gefördert durch Landesmittel Speicher- und Backupinfrastrukturen für ganze Verbünde bereitstellen, sodass Datenbestände auch bei schwerwiegenden Störungen oder Cyberangriffen erhalten bleiben (HRK 2025).

Auf nationaler und europäischer Ebene entstehen zunehmend sichere, kooperative Dateninfrastrukturen: Mit der Nationalen Forschungsdateninfrastruktur (NFDI) verfolgt Deutschland das Ziel eines föderierten Datennetzwerks, in dem Daten bei den jeweiligen Einrichtungen verbleiben und dennoch interoperabel nutzbar sind. Darüber hinaus kann das Netzwerk um die NFDI auch als koordinierende Instanz wirken, die beispielsweise Leitlinien bereitstellt. Auf EU-Ebene treibt die European Open Science Cloud (EOSC) den Aufbau eines Netzwerks aus Forschungsdaten, Rechenressourcen, Software und Diensten voran, wobei der EOSC Node Germany[8] daran arbeitet, die Anbindung der Infrastrukturen, Daten und Dienste der NFDI an den europäischen EOSC-Verbund zu ermöglichen. Ergänzend etabliert die Initiative GAIA-X[9] eine föderierte, europäische Dateninfrastruktur nach europäischen Souveränitäts- und Sicherheitsstandards; das Projekt „Fair-Data Spaces“ verknüpft GAIA-X gezielt mit der NFDI. Diese Entwicklungen sollten konsequent weitergeführt und stärker für Forschungsdaten genutzt werden. Angesichts geopolitischer Entwicklungen gewinnen zudem die langfristige Sicherung und Verfügbarkeit gefährdeter Datenbestände an Bedeutung. Die DFG-Förderinitiative für die Sicherung gefährdeter Datenbestände und zur Datenresilienz hat bereits wichtige Grundlagen geschaffen, die verstetigt und ausgebaut werden sollten.

Der Aufbau resilienter Forschungsdateninfrastrukturen sollte insgesamt als nationale Aufgabe wissenschaftlicher Daseinsvorsorge verstanden werden, die nicht allein privaten und wettbewerblichen Akteure überlassen werden kann; ihre Finanzierung muss langfristig gesichert, europäisch/international abgestimmt und länder- sowie förderorganisationsübergreifend gestaltet sein (DFG 2026). Die von der Gemeinsamen Wissenschaftskonferenz (GWK) beschlossene Bereitstellung weiterer Mittel für die NFDI zunächst bis 2038 ist ein Schritt in diese Richtung (GWK 2026). Wissenschaftliche Fachgesellschaften und Forschungsverbünde sollten schließlich den Austausch über Gefährdungen, Abhängigkeiten und Resilienzmaßnahmen intensivieren. Eine enge nationale und europäische Abstimmung kann gemeinsame Standards fördern und gefährdete Datenbestände langfristig sichern (DFG 2026).

8 https://www.nfdi.de/eosc-node-germany (28.8.2026)
9 https://gaia-x.eu/ (28.8.2026)

5.3 Langfristige Optionen: transformieren und resilient machen

Der langfristige Möglichkeitsraum (5 bis 10 Jahre) adressiert insbesondere strukturelle Herausforderungen, die in den Szenarien 2 und 3 sichtbar werden. Szenario 2 zeigt, dass hohe Sicherheitsanforderungen in der internationalen Wissenschaftspolitik bei unzureichender Wirksamkeit internationale Forschungskooperationen erheblich einschränken können. Angesichts des hohen ökonomischen und geopolitischen Werts vieler Forschungsdaten verschärft sich damit das Spannungsverhältnis zwischen wissenschaftlicher Offenheit und Sicherheit. Szenario 3 verdeutlicht dagegen, dass auch in einem weitgehend resilienten Forschungssystem die souveräne Nutzung externer IT-Anbieter und -Dienste eine Herausforderung bleibt.

Im Zentrum des langfristigen Möglichkeitsraums stehen daher die Weiterentwicklung resilienter, lernfähiger und souveräner Sicherheitsstrukturen sowie die strategische Ausgestaltung von internationalen Forschungskooperationen.

Zwei Handlungsoptionen werden vor diesem Hintergrund konkretisiert:

- Wissenschaftliche Offenheit versus (Cyber-)Sicherheit (Kapitel 5.3.1) zielt auf transparente, risikobasierte Prüfverfahren und abgestufte Kooperationsformate, die individuelle Verantwortung mit fachlicher Prüfung und langfristig etablierten nationalen Koordinationsstrukturen verbinden.
- Digitale Forschungssouveränität (Kapitel 5.3.2) zielt auf den Aufbau und die tatsächliche Nutzung souveräner Alternativen. Öffentlich geförderte Angebote sowie Wechsel- und Ausweichmöglichkeiten sollen Lock-in-Effekte und Abhängigkeiten von einzelnen marktmächtigen Anbietern begrenzen.

5.3.1 Wissenschaftliche Offenheit versus (Cyber-)Sicherheit: vertrauensvolle internationale Forschungskooperationen in Zeiten geopolitischer Fragmentierung

Internationale Kooperationen sind ein Kern wissenschaftlichen Arbeitens und eine wesentliche Voraussetzung für globalen wissenschaftlichen Fortschritt. Gleichzeitig gewinnt Forschungssicherheit im Zuge geopolitischer Veränderungen an Bedeutung und ist mit Fragen der Daten- und Cybersicherheit verbunden. Die Offenheit des Wissenschaftssystems ermöglicht exzellente Forschung, erhöht jedoch auch die Verwundbarkeit gegenüber Wissensabfluss, unerwünschtem Technologietransfer oder der Instrumentalisierung von Forschung durch staatliche oder andere Akteure. Internationale Forschungskooperationen sollten daher stärker risikobasiert ausgestaltet werden, zum Beispiel durch vorgelagerte Risikobewertungen von Partnereinrichtungen und Projekten sowie abgestufte Sicherheitsvorkehrungen, die sich nach der Sensibilität der Forschungsdaten richten, um sicherheitsrelevante Risiken frühzeitig zu erkennen und angemessen zu adressieren. Ziel ist keine Einschränkung internationaler Zusammenarbeit, sondern eine De-Risking-Strategie, die wissenschaftliche Offenheit und internationale Anschlussfähigkeit wahrt und zugleich bestehende Risiken systematisch minimiert (HRK 2025). Ebenso sollte eine Überreaktion (Overprotection) möglichst vermieden werden, bei der Kooperationen aus einem Gefühl der Unsicherheit gar nicht erst eingegangen werden.

Bund und Europäische Union sollten hierfür einen strategischen Rahmen für sichere internationale Forschungskooperationen schaffen. Hierzu zählen risikobasierte Kooperationsformate, gemeinsame Risikobewertungen, Risk-Sharing-Partnerschaften[10], differenzierte Zugriffsregelungen sowie gemeinsame Sicherheitsstandards. Die EOSC-Initiative zeigt beispielhaft, wie entsprechende Ansätze für Datenspeicherung und -zugriff umgesetzt werden können. Forschungseinrichtungen könnten diese Ansätze in die Praxis überführen, indem sie Sicherheitsanforderungen stärker an den jeweiligen Forschungskontext anpassen und differenzierte Sicherheitsniveaus etablieren.

Auf Ebene der Forschungseinrichtungen bedarf es transparenter, nachvollziehbarer und möglichst pragmatischer Prozesse, die Forschende dabei unterstützen, die Sicherheitsrelevanz ihrer Vorhaben einzuschätzen, potenzielle Risiken frühzeitig zu erkennen und bei erhöhtem Bedarf an zuständige Stellen weiterzugeben (OECD 2022; WR 2025b). Die Leitungsebenen der Einrichtungen sollten hierfür Standards festlegen, ausreichende Ressourcen bereitstellen und Sicherheitsprüfungen – auch mit Blick auf Cybersicherheit – als Bestandteil guter wissenschaftlicher Praxis institutionell verankern. Da sich Sicherheitsrisiken, Kooperationsstrukturen und Anwendungsmöglichkeiten wissenschaftlicher Erkenntnisse im Laufe eines Projekts verändern können, sollten Risikoprüfungen den gesamten Forschungslebenszyklus begleiten und nicht als einmalige Entscheidung angelegt sein (OECD 2022; WR 2025b).

Ein solches Prüfverfahren kann mehrstufig ausgestaltet werden. Im ersten Schritt kommt den Forschenden eine zentrale Rolle zu, da sie Forschungsinhalte und potenzielle Kooperationspartner am besten kennen. Leitlinien, Orientierungshilfen und Security-Awareness-Programme sollten sie befähigen, als dezentrale Sensoren auch schwache Signale für Bedrohungen wie Datenspionage oder die Instrumentalisierung von Forschungsergebnissen frühzeitig zu erkennen. In einem zweiten Schritt kann die Einschätzung in einem kollegialen Dialogverfahren reflektiert werden. Bei weitergehendem Prüfbedarf erfolgt im dritten Schritt die Übergabe an institutionelle Gremien oder Verantwortliche, beispielsweise Kommissionen für Ethik sicherheitsrelevanter Forschung (KEF) (WR 2025). Die Einbindung eines Chief Information Security Officers stellt dabei sicher, dass bei Sicherheitsprüfungen auch potenzielle Cybergefahren erkannt und Aspekte der Cyberresilienz mitgedacht werden.

Die konkrete Ausgestaltung der Verfahren sollte Größe, Forschungsprofil und Risikostruktur der jeweiligen Einrichtung berücksichtigen und so differenziert wie nötig, aber so unbürokratisch wie möglich erfolgen. Forschende sowie Verwaltungs- und Supportstrukturen sollten an ihrer Entwicklung beteiligt werden, um Praxistauglichkeit und Akzeptanz zu erhöhen. Vor allem kleinere Einrichtungen können Kompetenzen und Prüfstrukturen einrichtungsübergreifend bündeln und damit personelle Engpässe bei Sicherheitsverantwortlichen reduzieren (Naß et al. 2026; WR 2025b).

Ergänzend bedarf es einer dauerhaften Koordination auf nationaler Ebene. Die für 2027 geplante Nationale Plattform für Forschungssicherheit sollte hierfür langfristig als nationales Gremium etabliert werden, in dem Wissenschaft und staatliche Akteure, insbesondere Behörden und Organisationen mit Sicherheitsaufgaben, zusammenarbeiten (Hummert 2025; WR 2025). Eine solche Struktur kann Forschungseinrichtungen beraten, regelmäßig qualitativ hochwertige Informationen zur Sicherheitslage bereitstellen, besonders sicherheitsrelevante Forschungsfelder

10 im Sinne von Kooperationen, in denen die beteiligten Akteure Risiken, Verantwortlichkeiten und gegebenenfalls finanzielle Belastungen gemeinsam tragen

identifizieren und zu einer kohärenten Umsetzung von Forschungssicherheit in Deutschland beitragen. Essenziell ist dabei die systematische Bündelung von Informationen zu typischen Angriffsmustern, um den Akteuren Threat Intelligence in Echtzeit bereitzustellen. Die Einbindung staatlicher Akteure ermöglicht es, aktuelle sicherheitsrelevante Informationen und politische Lageeinschätzungen zur Verfügung zu stellen (Hummert 2025; WR 2025). Zugleich kann eine solche Struktur die Abstimmung mit europäischen und internationalen Partnern erleichtern (WR 2025), etwa im Rahmen des Digitalen Weimarer Dreiecks. Dabei handelt es sich um die Anwendung des seit 1991 bestehenden deutsch-französisch-polnischen Kooperationsforums auf digitale und cybersicherheitsbezogene Fragen.

Förderorganisationen sollten Fragen der Forschungssicherheit stärker in ihre Förderverfahren integrieren. Neben Anforderungen an Daten- und Cybersicherheit sollten Förderausschreibungen auch die Bewertung allgemeiner Wissensrisiken und wo möglich die Anwendung von Secure-by-Design-Prinzipien fordern, um Sicherheit von der ersten Planungsphase an fest in der Forschung zu verankern.

Obwohl jedes Forschungsvorhaben eine Sicherheitseinschätzung liefert, sollten für besonders sensible Forschungsfelder wie KI und Cloudcomputing (aufgrund ihrer weitreichenden Vernetzung) sowie der Biotechnologie oder den Materialwissenschaften, über die Prüfungsbedarfe hinausgehende Anforderungen gelten. Solche Forschungsbereiche sollten regelmäßig durch Methoden wie Strategic Foresight und Horizon-Scanning beobachtet und bewertet werden, um zukünftige Risiken frühzeitig zu antizipieren (Drechsler 2026). Hinweise auf einen erhöhten Prüfbedarf können zudem Kooperationen mit Partnern aus Staaten oder Unternehmen sein, bei denen ein erhöhtes Sicherheitsrisiko für Wirtschaftsspionage oder hybride Bedrohungen besteht. Auch diese Bewertungen sollten kontinuierlich aktualisiert und angepasst werden. Ebenso begründen Forschungsstandorte mit sensiblen Technologien, kritischen Geräten oder Versuchsaufbauten einen erhöhten Prüfungsbedarf, da sie als nicht substituierbare Infrastrukturen hochwertige Ziele für Sabotage und Spionage darstellen (AG KRITIS 2026).

5.3.2 Digitale Forschungssouveränität: strategische Ansätze für technologische Autonomie und wissenschaftliche Unabhängigkeit

Neben der Reduktion struktureller Abhängigkeiten von marktbeherrschenden IT-Anbietern zielt die Stärkung digitaler Souveränität innerhalb des Forschungssystems primär auf die Wiederherstellung der vollen Steuerungs- und Kontrollfähigkeit von IT-Infrastrukturen, Datenflüssen und Forschungsprozessen ab. Unter Federführung von Bund und Europäischer Union sollten, durch den Aufbau souveräner Forschungsclouds, sicherer Datenräume sowie eines bundesweiten Forschungsstacks – einer gemeinsamen technischen Basisinfrastruktur aus Rechenkapazitäten, Plattformen und Diensten für Forschungseinrichtungen – die technologische Basis für wissenschaftliche Unabhängigkeit geschaffen werden. Die gezielte Förderung von Open-Source-Lösungen und offenen Standards könnte dabei die notwendige Interoperabilität, Transparenz und Exitfähigkeit, also die Möglichkeit, technische Lösungen oder Dienstleister wechseln zu können, über institutionelle Grenzen hinweg schaffen. Auch im Hardwarebereich, beispielsweise bei Server- und Speichersystemen, Netzwerkkomponenten oder Cybersicherheitsprodukten, sollte digitale

Souveränität stärker berücksichtigt und gefördert werden. Hinzu kommen Rechenkapazitäten für KI bzw. die Schaffung von Alternativen zu den großen, kommerziellen Anbietern.

Die Stärkung der digitalen Souveränität im Forschungsprozess erfordert eine differenzierte Abwägung konkurrierender Ziele. Neben dem möglichen Spannungsfeld zwischen Souveränität einerseits sowie Nutzerfreundlichkeit und Funktionalität andererseits können auch digitale Souveränität und Cybersicherheit in Konflikt geraten: Große kommerzielle Anbieter bieten teils hohen Schutz vor cyberkriminellen Angriffen, schränken jedoch gleichzeitig die digitale Souveränität ein (WR 2023). Solch einen Trade-off gibt es teilweise auch bei den Diensten großer Anbieter, die Multifaktorauthentifizierung nur bei Cloudoptionen, nicht aber bei On-Premise-Lösungen unterstützen. Umgekehrt können geringe Souveränität und Abhängigkeit von außereuropäischen Anbietern angesichts der geopolitischen Lage Risiken durch staatliche Einflussnahme oder staatlich unterstützte Cyberangriffe erhöhen. Diese Komplexität unterstreicht den Bedarf an gestärkten Entscheidungskompetenzen sowie die Dringlichkeit, europäische Alternativen zu kritischen IT- und Infrastrukturdiensten aufzubauen.

Da kurz- bis mittelfristig für viele Anwendungen und Hardwarekomponenten noch keine praktikablen souveränen, europäischen Alternativen verfügbar sein werden, gilt es, bei Nutzung externer Anbieter bestehende Risiken durch Diversifizierung zu minimieren und die eigene Handlungsfähigkeit zu erhalten – beispielsweise hinsichtlich Datenspeicherung, Transparenz und Vermeidung von Lock-in-Effekten. Da diese Anforderungen häufig im Widerspruch zu kommerziellen Interessen proprietärer Anbieter stehen, könnte die Entwicklung ausreichender öffentlich geförderter Infrastrukturen und Plattformen als Alternative fokussiert werden (WR 2023). Mit Blick auf KI sollte der Zugang von Wissenschaftler/innen in Deutschland zu hochleistungsfähigen KI-Modellen gewährleistet sein. Gleichzeitig ist es essenziell, auch hier leistungsfähige, souveräne Benutzung befördernde Alternativen zu schaffen, beispielsweise Open-Source- oder europäische Lösungen, um den Zielkonflikt mit Souveränität abzumildern. Mit dem Beschluss der GWK im Juli 2026, den Ausbau des Nationalen Hochleistungsrechnens an Hochschulen (NHR) von 2027 bis 2030 zu fördern, ist hierfür ein wichtiger Baustein gelegt worden (GWK 2026).

Ein wichtiger Hebel zur Förderung der Nutzung von Produkten, die Souveränität ermöglichen, sind Beschaffungsprozesse. Digitale Souveränität sollte künftig ausdrücklich als Entscheidungskriterium berücksichtigt werden, etwa durch die Bevorzugung europäischer Lösungen, auch bei höheren Kosten, durch entsprechende Punktekriterien. Entsprechende Anforderungen sollten dabei klar und handhabbar gestaltet werden, um Beschaffungsprozesse nicht unnötig zu verkomplizieren.

Mit Fokus auf die Akteursebene können die Länder zur nachhaltigen Etablierung souveräner Infrastrukturen beitragen, indem sie Initiativen des Bundes in ihre Hochschullandschaften integrieren sowie geeignete organisatorische Schnittstellen schaffen. Hochschulen und Forschungseinrichtungen wiederum sollten innerhalb ihrer Organisationen die Rahmenbedingungen für die Nutzung souveräner Soft- und Hardwarealternativen schaffen. Hierfür sollte die Verantwortung für digitale Grundstrukturen innerhalb der Leitungsebene klar zugeordnet und gebündelt werden, beispielsweise bei einem Chief Information Officer (CIO), der sicherstellt, dass digitale Souveränität bei strategischen Entscheidungen der Einrichtung systematisch berücksichtigt wird (WR 2023). Darüber hinaus sollten die Kompetenzen und das Sicherheitsbewusstsein der Forschenden im Umgang mit Clouddiensten und digitalen Plattformen gestärkt werden, um souveränitätsorientierte Dienste und Plattformen zu fördern und gleichzeitig die Verbreitung nicht genehmigter IT außerhalb offizieller Strukturen (Schatten-IT) zu reduzieren. Dabei sollten die Bedeutung von

Souveränität und die Risiken durch Abhängigkeiten eindrücklich vermittelt werden, da diese häufig erst im Problemfall deutlich werden. Ein wesentlicher Baustein ist die Migration bestehender Systeme und Daten auf souveräne Plattformen, begleitet durch Qualifizierungsmaßnahmen und angepasste Arbeitsprozesse.

Hochschulübergreifende Zusammenarbeit, sowohl innerhalb von landesweiten als auch von länderübergreifenden Verbünden, kann die Verhandlungsposition gegenüber externen Anbietern stärken (WR 2023) und Möglichkeiten zur gemeinsamen Infrastrukturnutzung schaffen. Ein Beispiel ist der Arbeitskreis Softwarelizenzen des Vereins Zentren für Kommunikation und Informationsverarbeitung in Lehre und Forschung e. V. (ZKI), der Rahmenverträge für Hochschulen verhandelt; solche Kooperationen sollten vertieft und auf außeruniversitäre Institute ausgeweitet werden. Die während der COVID-19-Pandemie eingeführten DFN-Rahmenverträge für Videokonferenzsysteme sind ein weiteres Beispiel (Bei der Kellen 2025). Eine derartige Zusammenarbeit könnte auch auf KI-Nutzung angewandt werden.

Da sich Forschungseinrichtungen hinsichtlich Größe, vorhandener Expertise und verfügbarer Ressourcen teilweise erheblich unterscheiden (HRK 2025), sollten Souveränitätsstrategien an die jeweiligen institutionellen Voraussetzungen angepasst werden. Hierfür sind betroffene Akteursgruppen frühzeitig einzubeziehen, um unterschiedliche Anforderungen und Bedürfnisse zu berücksichtigen. Open-Source-Technologien können die Transparenz und Anpassungsfähigkeit erhöhen und Lock-in-Effekte gegenüber marktbeherrschenden, häufig außereuropäischen Anbietern reduzieren. Ihr Einsatz erfordert jedoch oft erhebliche Ressourcen für Betrieb und Betreuung, die nicht in allen Einrichtungen und Bereichen gleichermaßen verfügbar sind (WR 2023). Der einrichtungsübergreifende Austausch von Good-Practice-Beispielen zur Migration und zum Betrieb von Open-Source-Lösungen kann dazu beitragen, vorhandene Erfahrungen breiter nutzbar zu machen und Umsetzungshürden zu reduzieren.

6 Literatur

Adamu, Y. A.; Chaudhry, S. A. (2026): CyberSense AI: Enhancing Cybersecurity Awareness Through Adaptive, Behavior-Driven Education. In: Koucheryavy, Y. et al. (Hg.): Internet of Things, Smart Spaces, and Next Generation Networks and Systems. Lecture Notes in Computer Science, Cham, S. 36–54, https://doi.org/10.1007/978-3-032-19981-2_4

Adeshola, I.; Oluwajana, D. I. (2025): Assessing cybersecurity awareness among university students: implications for educational interventions. In: Journal of Computers in Education 12(4), S. 1283–1305, https://doi.org/10.1007/s40692-024-00346-7

AG KRITIS (2026): Stellungnahme zum Referentenentwurf des Bundesministeriums des Innern für eine Verordnung zur Bestimmung kritischer Anlagen nach dem KRITIS-Dachgesetz (Kritisverordnung – KritisV) mit Bearbeitungsstand vom 26.5.2026. https://ag.kritis.info/wp-content/uploads/2026/06/20260614-AG-KRITIS-Stellungnahme-Kritisverordnung.pdf (31.8.2026)

Allianz der Wissenschaftsorganisationen (2019): Zehn Thesen zur Wissenschaftsfreiheit. Forschungsorganisationen legen Selbstverpflichtung vor. https://www.allianz-der-wissenschaftsorganisationen.de/themen-stellungnahmen/zehn-thesen-zur-wissenschaftsfreiheit/ (31.8.2026)

Allianz der Wissenschaftsorganisationen; BMBF (2025): Gemeinsame Erklärung der Allianz der Wissenschaftsorganisationen und des Bundesministers für Bildung und Forschung. https://www.allianz-der-wissenschaftsorganisationen.de/wp-content/uploads/2025/03/20250326_Gemeinsame-Erklaerung_Allianz_BMBF-1.pdf (31.8.2026)

Ananda, A. et al. (2026): Cybersecurity Using Machine Learning: Implementing an Intrusion Detection System Using the NSL-KDD Dataset. In: Haldorai, A. et al. (Hg.): 7th EAI International Conference on Big Data Innovation for Sustainable Cognitive Computing. Cham, S. 195–212, https://doi.org/10.1007/978-3-032-02979-9_14

Annino, U. (2026): Die strategische Notwendigkeit der Cyber-Resilienz. In: HMD Praxis der Wirtschaftsinformatik 63(2), S. 270–287, https://doi.org/10.1365/s40702-026-01265-0

ATHENE (2025): ATHENE Cybernation Deutschland. Sicherheit der IT der Universitäten. ATHENE Nationales Forschungszentrum für angewandte Cybersicherheit, Goethe-Universität, Frankfurt a. M., https://scienceshield.athene-center.de/fileadmin/Studien/ATHENE-Lagebild-Bericht-Unis.pdf?_=1768469483 (31.8.2026)

Becker, L.; Aghaye, F. (2022): IT-Sicherheit an Hochschulen: Schwachstellen und Präventionsmaßnahmen. Hochschulforum Digitalisierung, https://hochschulforumdigitalisierung.de/it-sicherheit-an-hochschulen-schwachstellen-und-praeventionsmassnahmen/ (17.8.2026)

Bei der Kellen, D. (2025): Vielfalt gefragt – Videokommunikation im DFN. In: DFN-Mitteilungen 108, S. 22–23

Bitkom e. V. (2026): Der Arbeitsmarkt für IT-Fachkräfte. Berlin, https://doi.org/10.64022/2025-it-fachkraefte

BKA (2026): Bundeslagebild Cybercrime 2025. Bundeskriminalamt, Wiesbaden

BMFTR (2025): Eckpunkte zur Stärkung der Forschungssicherheit und zum Aufbau einer Nationalen Plattform für Forschungssicherheit. Bundesministerium für Forschung, Technologie und Raumfahrt, Berlin

Bretschneider, W. et al. (2020): Cybersicherheit als Katalysator für Innovation und Wachstum. Brandenburgisches Institut für Gesellschaft und Sicherheit, Berlin

BSI (2017): BSI-Standard 200-2. IT-Grundschutz-Methodik. Bundesamt für Sicherheit in der Informationstechnik, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.pdf?__blob=publicationFile&v=2 (31.8.2026)

BSI (2025): Die Lage der IT-Sicherheit in Deutschland 2025. Bundesamt für Sicherheit in der Informationstechnik, https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html (31.8.2026)

BSI (2026a): Grundschutz++. Neuentwicklung des Grundschutzes. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Grundschutz-in-der-Informationssicherheit/Grundschutz-Plus-Plus/grundschutz-plus-plus_node.html (31.8.2026)

BSI (2026b): KI-Modelle revolutionieren den Umgang mit Sicherheitslücken. Bundesamt für Sicherheit in der Informationstechnik, https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Blog/KI-Modelle_neue_Zeitrechnung_260508.html?nn=132646 (31.8.2026)

BSI (2026c): Resilienz. Lage der Cybernation in den Dimensionen der Cybersicherheit. Bundesamt für Sicherheit in der Informationstechnik, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Lageberichte/Monatsbericht_Lage-Cybernation/Lage_Resilienz/lage-Resilienz_node.html (31.8.2026)

BSI (2026d): Wenn eine KI aus ihrer Sandbox ausbricht. Bundesamt für Sicherheit in der Informationstechnik, https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Blog/KI_Ausbruch_Sandbox_260724.html?nn=520690 (31.8.2026)

Büchel, J. et al. (2025): Cybersicherheit: Kompetenzen gefragter denn je. IW-Kurzbericht 39, Köln

Check Point (2026): Cyber Security Report 2026. Check Point Software Technologies Ltd., Tel Aviv

Christ, J. (2025): Europas digitaler Niedergang? Zurückfallen und Abhängigkeiten bei Plattformdiensten, Cloud Computing und KI-Systemen in Zeiten geopolitischer Instabilität. In: Christ, J. P.; Giesen, K. (Hg.): Polykrisen, Strukturbrüche und Schwarze Schwäne. FOM-Edition, Wiesbaden, S. 149–169, https://doi.org/10.1007/978-3-658-49235-9_9

Christen, M. (2020): The Ethics of Cybersecurity. Cham

Czachowski, L. (2026): Cloud zwischen Souveränität, Resilienz und Wettbewerb. In: Datenschutz und Datensicherheit 50(4), S. 204–206, https://doi.org/10.1007/s11623-026-2233-5

DFG (2026): Zur Resilienz von Forschungsdateninfrastrukturen. Deutsche Forschungsgemeinschaft, https://news.dfg.de/a/a.aspx?AysDIsUxX3zXjxSjrH95pRnELg2 (13.4.2026)

Döttl, D. (2025): Umsetzung der NIS-2-Richtlinie im Abwassersektor. Fachhochschule der Wirtschaft, Graz

Drechsler, D. (2026): Risikofrüherkennung und Risikomanagement in digitalwirtschaftlichen Ökosystemen. In: Detscher, S.; Hepp, M. (Hg.): Praxishandbuch Digitales Management. Wiesbaden, S. 359–379, https://doi.org/10.1007/978-3-658-49581-7_27

Drews, L.-S.; Łabuz, M. (2026): Eine Typologie nationaler Cybersicherheitsarchitekturen: Cyberarchitekturmodelle von Deutschland, Frankreich und Polen im Vergleich. In: HMD Praxis der Wirtschaftsinformatik 63(2), S. 509–523, https://doi.org/10.1365/s40702-026-01258-z

Dreyer, M. (2026): ZKI Top-Trends-Umfrage 2026. Zenodo, https://doi.org/10.5281/ZENODO.18520230

EK (2025): Eine europäische Strategie für Forschungs- und Technologieinfrastrukturen. Europäische Kommission, COM(2025) 497 final/2, Brüssel

Fan, W.; Li, Y. (2025): Assessment of postgraduate digital research literacy: current competencies, desired skills, and enhancement strategies. In: Education and Information Technologies 30(15), S. 21551–21571, https://doi.org/10.1007/s10639-025-13622-5

Forschungsdaten.info (o.J.): Big Data in der Forschung. Die Arbeit mit großen Datenmengen. https://forschungsdaten.info/fdm-allgemein/speichern-und-rechnen/big-data-in-der-forschung (18.6.2026)

Freyberg-Inan, A. (2025): Academic Freedom in a Plural World: Global Critical Perspectives by Nandini Ramanujam and Frédéric Mégret, Eds. In: Human Rights Review 26(3), S. 249–252, https://doi.org/10.1007/s12142-025-00748-9

Gärtner, T. (2026): Globale Tendenzen in nationalen Cybersicherheitsstrategien: Ein Leitfaden für die Strategieentwicklung. In: Selzer, A. (Hg.): Aktuelle Entwicklungen des Rechtsrahmens der Cybersicherheit und Privatheit: Sammelband zur ATHENE-Konferenz 2025 in Darmstadt, Wiesbaden, S. 92–108, https://doi.org/10.1007/978-3-658-49640-1_7

Geißler, O. (2025): Legacy-Systeme: Risiken und Maßnahmen für IT-Sicherheit. Security-Insider, https://www.security-insider.de/legacy-systeme-risiken-massnahmen-fuer-it-sicherheit-a-443c546d400184e72dc8792302ac57c4/ (18.8.2026)

Gemeinsamer Ausschuss (2024): Wissenschaftsfreiheit und Sicherheitsinteressen in Zeiten geopolitischer Polarisierung. Tätigkeits- und Sachstandsbericht. Gemeinsamer Ausschuss zum Umgang mit sicherheitsrelevanter Forschung, Halle

Geppert, T. et al. (2026): CYREN^{zh} Cybersecurity Clinic: Konzept und Erkenntnisse. In: HMD Praxis der Wirtschaftsinformatik 63(2), S. 425–439, https://doi.org/10.1365/s40702-026-01250-7

Goliath, S. et al. (2026): Exploring the Cybersecurity-Resilience Gap: An Analysis of Student Attitudes and Behaviors in Higher Education. In: Venter, H. et al. (Hg.): Information and Cyber Security, Cham, S. 185–195, https://doi.org/10.1007/978-3-032-09660-9_19

GWK (2026): Wegweisende Schritte für zentrale Forschungsinfrastrukturen in Deutschland vereinbart: Stärkung des Forschungsdatenmanagements, des Hochleistungsrechnens mit KI an Hochschulen sowie der Digitalisierung in den Geisteswissenschaften. Gemeinsame Wissenschaftskonferenz, PM 09, Bonn

Heinbach, C.; Pagel, P. (2026): Cybersecurity und Resilienz – Schutzstrategien für Unternehmen. In: Wirtschaftsinformatik & Management 18(1–2), S. 1–2, https://doi.org/10.1365/s35764-026-00600-w

Heo, W.; Grable, J. E. (2026): Data Privacy and Cybersecurity. In: Heo, W.; Grable, J. E.: Ethics and Compliance in Financial Services. Cham, S. 197–224, https://doi.org/10.1007/978-3-032-14449-2_10

Herres-Pawlis, S. et al. (2022): Mindestinformationsstandards in der Chemie: Ein Appell zum besseren Umgang mit Forschungsdaten. In: Angewandte Chemie 134(51), Art. e202203038, https://doi.org/10.1002/ange.202203038

Hofer, D. (2026): Cybersicherheit und Compliance in der betrieblichen Praxis. In: Kälberer, D. R.; Sassmann, T. (Hg.): Digitale Transformation und Innovation in der betrieblichen Praxis. Wiesbaden, S. 179–202, https://doi.org/10.1007/978-3-658-51264-4_9

Hoffmann, M.; Buchmann, E. (2026): Cyber Resilience Through LLM-Enhanced Vulnerability Reports. In: Renaud, K. et al. (Hg.): Cybersecurity. Cham, S. 109–128, https://doi.org/10.1007/978-3-032-28957-5_7

HRK (2025): Handlungsdruck für Hochschulen, Länder und Bund Empfehlung der 40. Mitgliederversammlung der HRK am 13. Mai 2025 in Magdeburg. Hochschulrektorenkonferenz, Berlin

Hummert, C. (2025): Schriftliche Stellungnahme. Öffentliches Fachgespräch zum Thema „Forschungssicherheit“. Deutscher Bundestag, Ausschussdrucksache 21(18)24a, Berlin

Kanagalingam, N.; Loncar, M. (2026): Anforderungen an Ausbildung und Qualifikation für den Betrieb von Rechenzentren. In: Bieser, J.; Kurzrock, B.-M. (Hg.): Facility Management in Rechenzentren. Wiesbaden, S. 591–621, https://doi.org/10.1007/978-3-658-51314-6_19

Kracke, J. (2026): Künstliche Intelligenz zwingt Rechenzentren zum Wandel. In: IT-Director 4–5, S. 28–29, https://doi.org/10.1007/s44380-026-0432-4

Kranich, L. (2026): Cloudnutzung und digitale Souveränität. In: Datenschutz und Datensicherheit - DuD 4, S. 193, https://doi.org/10.1007/s11623-026-2229-1

Kranzlmüller, D.; Grimshaw, A. (2026): IT-Infrastrukturen und deren Stromverbrauch. In: Schmiedchen, F. et al. (Hg.): Künstliche Intelligenz und Wir. Berlin, S. 123–147, https://doi.org/10.1007/978-3-662-71567-3_7

Kreutzer, M. et al. (2026): Im Dickicht der Rechtsakte: Regulierung von Datenschutz, Datennutzung und Cybersicherheit: Ein Spannungsfeld zwischen Notwendigkeit für die Gesellschaft und Wettbewerbsnachteil für den Innovationsstandort Europa. In: Datenschutz und Datensicherheit - DuD 4, S. 234–236, https://doi.org/10.1007/s11623-026-2239-z

Lemke, C. (2026): Informationstechnologie für Nachhaltigkeit: Die versteckten Kosten des digitalen Zeitalters. In: Wollmann, P. et al. (Hg.): Die nachhaltige Organisation. Cham, S. 219–241, https://doi.org/10.1007/978-3-032-29607-8_9

Naß, M. et al. (2026): Security Awareness als institutionelles Anliegen: Voraussetzungen, Herausforderungen und Gestaltungsräume für NRW-Hochschulen. In: HMD Praxis der Wirtschaftsinformatik 63(2), S. 327–341, https://doi.org/10.1365/s40702-026-01261-4

Nöhmke, S. et al. (2026): Digitale Kompetenzentwicklung für die Entdeckung der Zukunft: Qualitative Forschung mit Künstlicher Intelligenz. In: Keller, K. et al. (Hg.): Bildungskonzepte für die digitale Gesellschaft der Zukunft. Wiesbaden, S. 41–56, https://doi.org/10.1007/978-3-658-50857-9_3

Ochôa, P. et al. (2026): Humanities, Humanism and Ethics in a Digital Context: Challenges for Digital Literacy Research and Learning. In: Kurbanoğlu, S. et al. (Hg.): Information Literacy in an AI-Driven World. Cham, S. 268–277, https://doi.org/10.1007/978-3-032-17272-3_22

OECD (2022): The contribution of RTOs to socio-economic recovery, resilience and transitions. Organisation for Economic Co-Operation and Development, Science, Technology and Industry Policy Papers 129, https://doi.org/10.1787/ae93dc1d-en

OECD (2025): OECD Science, Technology and Innovation Outlook 2025: Driving Change in a Shifting Landscape. Organisation for Economic Co-operation and Development, Paris, https://doi.org/10.1787/5fe57b90-en

Plattner, C. (2025): Schriftliche Stellungnahme. Öffentliches Fachgespräch zum Thema „Forschungssicherheit“. Deutscher Bundestag, Ausschussdrucksache 21(18)24c, Berlin

Rat der Europäischen Union (2024): Empfehlung des Rates zur Stärkung der Forschungssicherheit. Interinstitutionelles Dossier: 2024/0012(NLE) 9097/24, Brüssel

Richter, B. (2025): Cybersicherheit für KMU: Ein Leitfaden. In: Kohne, A.; Bauer, D. (Hg.): Die Mittelstandstransformation. Wiesbaden, S. 419–439, https://doi.org/10.1007/978-3-658-48184-1_16

Schiffner, D.; Kiesler, N. (o. J.): Open Science in den Bildungstechnologien: Zur Unterstützung bei der Veröffentlichung von Forschungsdaten. In: Kiesler, N.; Schulz, S. (Hg.): Workshopband der 22. Fachtagung Bildungstechnologien (DELFI). Gesellschaft für Informatik e. V., https://doi.org/10.18420/delfi2024-ws-00

Schneider, M. et al. (2025): Weiterbildung zur Cybersicherheit. In: Datenschutz und Datensicherheit - DuD 11, S. 737–741, https://doi.org/10.1007/s11623-025-2174-4

Schuller, T. (2026): IT-Sicherheit. Schatten-IT hat Innovations- und Zerstörungskraft. Springer Professional, https://www.springerprofessional.de/it-sicherheit/datenmanagement/schatten-it-hat-innovations--und-zerstoerungskraft/52170432 (18.8.2026)

Sitarska, A. et al. (2026): Innovation und Digitale Souveränität müssen kein Widerspruch sein. In: D'Onofrio, S.; Russ, C. (Hg.): Digital HealthTech. Edition HMD, Wiesbaden, S. 61–71, https://doi.org/10.1007/978-3-658-51795-3_5

Sommerhäuser, L. (2026): NIS 2 verankert Cybersicherheit als Management-Aufgabe. In: IT-Mittelstand 25(4–5), S. 32–33, https://doi.org/10.1007/s44381-026-0429-4

Stein, M. et al. (2025): Cybersicherheit an Hochschulen: Föderale Ansätze und (gemeinsame) Wege. HIS-Institut für Hochschulentwicklung e. V., Hannover

TAB (2022): Data-Mining – gesellschaftspolitische und rechtliche Herausforderungen. (Autorin: Gerlinger, K.) Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, TAB-Arbeitsbericht Nr. 203, Berlin, https://doi.org/10.5445/IR/1000156297

TAB (2024): Infrastruktursystem Energie (Autor/innen: Bledow, N. et al.). Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, Foresight-Report 1, Berlin, https://foresight.tab-beim-bundestag.de/wp-content/uploads/2025/09/Infrastruktursystem-Energie.pdf (31.8.2026)

TAB (2025a): Infrastruktursystem Bildung und Forschung (Autor/innen: Bledow, N. et al.). Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, Foresight-Report 4, Berlin, https://foresight.tab-beim-bundestag.de/wp-content/uploads/2025/09/Infrastruktursystem-Bildung-und-Forschung.pdf (31.8.2026)

TAB (2025b): Leitlinien für den Einsatz generativer KI im TAB. Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, Berlin, https://doi.org/10.5445/IR/1000188419

TAB (2026): Infrastruktursystem Staat und Verwaltung (Autor/innen: Bledow, N. et al.). Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, Foresight-Report Nr. 9, Berlin, https://doi.org/10.5445/IR/1000196376

VDI Research (2023): Deutsche Cybersicherheitsstrategie im Diskurs: Anforderungen und Impulse aus Europa. Düsseldorf

WEF (2026): Global Cybersecurity Outlook 2026. World Economic Forum, Genf

Wittpahl, V. (Hg.) (2016): Digitalisierung: Bildung, Technik, Innovation. Berlin, https://doi.org/10.1007/978-3-662-52854-9

WR (2023): Empfehlungen zur Souveränität und Sicherheit der Wissenschaft im digitalen Raum (Drs. 1580-23). Wissenschaftsrat, Köln, https://doi.org/10.57674/M6PK-DT95

WR (2025a): Strukturevaluation der Nationalen Forschungsdateninfrastruktur (NFDI) (Drs. 2627-25). Wissenschaftsrat, Köln, https://doi.org/10.57674/wcdc-6d36

WR (2025b): Wissenschaft und Sicherheit in Zeiten weltpolitischer Umbrüche (Drs. 2485-25). Wissenschaftsrat, Köln, https://doi.org/10.57674/9TR5-KN29

WR (2026): Wissenschaft in Deutschland – Perspektiven bis 2040 (Drs. 3014-26). Wissenschaftsrat, Köln, https://doi.org/10.57674/NPVJ-9804

7 Anhang

7.1 Expert/innen

Name	Organisation
Matthias Berg	Bundesamt für Sicherheit in der Informationstechnik, Referat Trendanalyse, Forschungsstrategie und Cybersicherheitsförderung
Bernhard Brandel	Katholische Universität Eichstädt-Ingolstadt, Sprecher Arbeitskreis Informationssicherheit
Dr. Lilli Bruckschen	Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE, Leiterin der Forschungsgruppe Attack Intelligence & Mitigation
Prof. Dr. Johannes Fähndrich	Prodekan an der Hochschule für Polizei Baden-Württemberg (HfPolBW, Fakultät IV: Sozialwissenschaften), Leiter der Fachgruppe Angewandte Informatik, Cybercrime und Digitale Spuren
Lukas Härter	Philipps-Universität Marburg, Informationssicherheitsbeauftragter
Manuel „HonkHase“ Atug	Gründer und Sprecher der AG KRITIS
Prof. Dr. Klaus-Peter Kossakowski	Hochschule für Angewandte Wissenschaften Hamburg, Professur für IT-Sicherheit
Dr. Rainer Lange	Wissenschaftsrat, Leiter der Abteilung Forschung
Prof. Dr. Wolfgang Lehner	Technische Universität Dresden, Professur für Datenbanken und Direktor des Instituts für Systemarchitektur/ Aalborg University, Professur für Data Engineering, Science and Systems/ Mitglied der Wissenschaftlichen Kommission des Wissenschaftsrats
Dr. Frank Lindemann	ZBW – Leibniz-Informationszentrum Wirtschaft, Leitung der Abteilung IT-Infrastruktur und Sprecher des Leibniz Arbeitskreises IT
Dr. Michael Littger	cyberintelligence.institute, Mitglied der Geschäftsleitung, Strategy Director, Jurist und Regulierungsexperte
Dr. Roland Nolte	IZT – Institut für Zukunftsstudien und Technologiebewertung gemeinnützige GmbH, Geschäftsführer
Prof. Dr. Haya Schulmann	Fachbereich Informatik an der Goethe-Universität Frankfurt a. M./ Mitglied im Direktorium des Nationalen Forschungszentrums für angewandte Cybersicherheit ATHENE
Vera Sikes	Bundesamt für Sicherheit in der Informationstechnik (BSI), Fachbereichsleitung IT-Systeme
Mirko Ross	asvin GmbH, Gründer und CEO
Prof. Dr. Ulrike Tippe	Hochschulrektorenkonferenz, HRK-Vizepräsidentin für Digitalisierung und wissenschaftliche Weiterbildung
Ariane Wolf	Agentur für Innovation in der Cybersicherheit, Abteilungsleiterin Sichere Gesellschaft

7.2 Einflussfaktoren

Im Folgenden werden die im Rahmen des ersten Untersuchungsschrittes identifizierten Einflussfaktoren und die priorisierten Schlüsselfaktoren strukturiert nach der STEEPL-Systematik (social, technological, economic, environmental, political und legal) dargestellt. Die Schlüsselfaktoren sind hervorgehoben und beinhalten die Benennung von jeweils drei möglichen Zukunftspfaden bis 2030+.

Gesellschaft

- *Akademische Freiheit im Umgang mit IT-Systemen und Daten* (Ausprägungen: Freiheit ohne Absicherung, verantwortete Freiheit, regulierte Forschung)
- Arbeits- und Beschäftigungsformen
- demografische Entwicklung der Beschäftigung
- *digitale und KI-Kompetenz* (Ausprägungen: überfordert im Fortschritt, souveräne Anwendung, Kompetenzverlust)
- fachliche Cybersicherheits- und Steuerungskompetenzen
- Gestaltung digitaler Arbeitsumgebungen
- Internationalisierung und Interkulturalität
- öffentliche Wahrnehmung von Cyberbedrohungen
- *Sicherheitsbewusstsein* (Ausprägungen: langsam steigendes Sicherheitsbewusstsein bei steigender Bedrohungslage, sicherheitsorientierte Führungskultur, defizitäres Sicherheitsbewusstsein)
- Technikakzeptanz und Akzeptanz von Sicherheitslösungen
- Veränderungs- und Lernbereitschaft
- Verhältnis von Wissenschaft und Gesellschaft

Technologie

- Datenverschlüsselung und Kryptografie
- *Fähigkeit zur Angriffserkennung* (Ausprägungen: mittlere Detektionsfähigkeit, geringe Detektionsfähigkeit, hohe Detektionsfähigkeit)
- *Komplexität und Heterogenität der IT-Infrastrukturen* (Ausprägungen: unkontrollierte Fragmentierung, teilweise Strukturierung, standardisierte IT-Landschaft)
- *Nutzung von externen IT-Infrastrukturen, Geräten und Diensten* (Ausprägungen: unkoordinierte Strukturen, pragmatische Auslagerung, weitreichende Auslagerung)

- *technische Komplexität und Schutzbedarfe von Forschungsdaten* (Ausprägungen: abgestufte Schutzbedarfe, diffuse Schutzbedarfe, integrierter Schutz)
- *technischer Zustand und Lebenszyklus von IT-Systemen* (Ausprägungen: selektive Erneuerung, technische Alterung, vollständiges Lifecycle-Management)
- *technologische Innovationsgeschwindigkeit und Adaption* (beschleunigte Adoption, asynchrone Adoption, gesteuerte Adoption)
- *Verbreitungsgrad von KI in Cyberkriminalität* (Ausprägungen: durchdringende KI-Angriffe, begrenzte Nutzung von KI, breite Nutzung zur Skalierung)
- *Verbreitungsgrad von KI in der Cybersecurity im IT-Betrieb* (Ausprägungen: geringe Nutzung, selektiver Einsatz, vollständig KI-gestützt)
- Verbreitungsgrad von KI in der Forschung
- Vernetzungsgrad von Geräten und Systemen (IoT und Edge Computing) in Laboren

Umwelt

- umweltbedingte Störungen globaler Lieferketten
- physische Klima- und Umweltbelastungen auf digitale Infrastruktur
- Nachhaltigkeitsanforderungen an digitale Infrastruktur
- Energieverfügbarkeit und -stabilität
- Abhängigkeit von ressourcenintensiver IT-Infrastruktur

Wirtschaft

- Abhängigkeit von Drittmittel- und Industriekooperationen
- *Abhängigkeit von monopolistischen IT- und Clouddienstleistern* (Ausprägungen: bewusst/begrenzt abhängig, unkoordiniert abhängig, souveränitätsorientiert)
- Abhängigkeit von Drittmittel- und Industriekooperationen
- *Abhängigkeit von monopolistischen IT- und Clouddienstleistern* (Ausprägungen: bewusst/begrenzt abhängig, unkoordiniert abhängig, souveränitätsorientiert)
- Abhängigkeit von proprietären Systemen
- Attraktivität und Wettbewerbsfähigkeit des Forschungsstandortes
- *Fachkräftesituation im Bereich Cybersicherheit* (Ausprägungen: struktureller Fachkräftemangel, mittlerer Kompetenzaufbau, gezielter Kompetenzaufbau)
- Finanzierungsbedingungen von Forschungseinrichtungen
- Folgekosten von Cybervorfällen

- Kostenstruktur und Investitionsprioritäten
- Professionalisierung der Cyberkriminalitätsbranche
- Versicherbarkeit von Cyberrisiken
- *Wert von Forschungsdaten und geistigem Eigentum* (Ausprägungen: z.T. hoher strategischer Wert, begrenzter ökonomischer Wert, hoher systemischer Wert)
- Wettbewerbsfähigkeit der Cybersicherheitsforschung in Deutschland
- Wirtschaftlicher Druck zur schnellen Digitalisierung und Adaption neuer Technologien

Politik

- *digitale Souveränität* (Ausprägungen: unzureichende digitale Souveränität durch geringe Priorisierung, vereinzelt hoch, umfassende Souveränität durch europäische Anbieter/Alternativen)
- Förderung von Kompetenzaufbau und Fachkräften im Bereich Cybersicherheit
- *internationale Wissenschaftspolitik* (Ausprägungen: offene Kooperation mit Partnerländern, restriktive Kooperation mit hohen Sicherheitsanforderungen, selektive Kooperation im Zuge globaler Blockbildung)
- nationale Cybersicherheitsstrategie
- politische Haltung zu Open Science und Offenheit
- *politische Koordination zwischen Bund, Ländern und EU* (Ausprägungen: Koordinierungsdefizite, gestärkte Koordination, mittlere Koordination)
- politische Reaktion auf Cybervorfälle
- politische Stabilität und Kontinuität in Deutschland
- *Priorisierung von Cybersicherheit und Maßnahmenumsetzung* (Ausprägungen: Cybersicherheit als strategische Priorität, hohe Priorität vs. Umsetzungsschwächen, keine Priorität)
- EU-Vorgaben und nationale Umsetzungsdefizite
- Regulierung und staatliche Steuerung der Forschung
- Sicherheits- und geopolitische Lage
- öffentliche Investitionspolitik

Recht

- *Cybersicherheitsregulierung* (zum Beispiel NIS-2-Richtlinie, BSI-Gesetz) (Ausprägungen: konsolidierte Mindestregulierung, wirkungsorientierte Regulierung, versicherheitlichte Hochregulierung)

- datenschutzrechtliche Vorgaben (Auslegung Datenschutz-Grundverordnung[11])
- Haftungsregelungen bei Cybervorfällen
- internationale Rechtskonflikte und Rechtsunterschiede
- Meldepflichten bei Sicherheitsvorfällen und sicherheitspolitische Einordnung der Forschung
- rechtliche Anforderungen an Forschungssicherheit
- Rechtsdurchsetzung und Sanktionspraxis
- Regulierung von Cloud- und Drittanbietern
- Regulierung von KI- und automatisierten Systemen
- Vergabe- und Beschaffungsrecht für IT-Sicherheit

11 Verordnung (EU) 2016/679 vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

Herausgeber
Büro für Technikfolgen-Abschätzung
beim Deutschen Bundestag
Neue Schönhauser Straße 10
10178 Berlin

Telefon: +49 30 28491-0
E-Mail: buero@tab-beim-bundestag.de
www.tab-beim-bundestag.de

2026

Bildnachweis
Andres Mejia/AdobeStock (S. 1)

DOI: 10.5445/IR/1000196771

Foresight

Die Resilienz-Dossiers fassen die Ergebnisse des Resilienz-Checks zusammen. Im Resilienz-Check wird untersucht, wie die Resilienz kritischer Infrastrukturen gegenüber systemischen Risiken gestärkt werden kann. Dazu werden ausgewählte Zukunftsthemen in einem strukturierten Analyse- und Szenarioprozess gemeinsam mit Akteuren aus Wissenschaft, Wirtschaft, Politik, Verwaltung und Zivilgesellschaft vertiefend untersucht.

Die Themen des Resilienz-Checks (https://foresight.tab-beim-bundestag.de/resilienz-check) werden im Resilienz-Radar (https://foresight.tab-beim-bundestag.de/resilienz-radar/) identifiziert. Die Berichterstattergruppe TA wählt daraus jeweils ein Fokusthema für die vertiefende Untersuchung aus.

Die Resilienz-Dossiers werden seit 2025 jährlich veröffentlicht. Alle Kernergebnisse sowie weitere Informationen zum TAB-Foresight-Prozess finden sich auf der Microsite https://foresight.tab-beim-bundestag.de.