Cybersecurity in Higher Education:
From Global Dynamics to Institutional Action

Masterarbeit

Im Virtuellen Weiterbildungsstudiengang Wirtschaftsinformatik

Verfasser: **Alexander Fehr, M.A.**

Prüfer: Prof. Dr. Günther Pernul
Universität Regensburg

Eingereicht: 09. Mai 2025

Dieses Werk ist als freie Onlineversion über das Forschungsinformationssystem (FIS; https://fis.uni-bamberg.de) der Universität Bamberg erreichbar.
Das Werk steht unter der CC-Lizenz CC BY-SA.

Lizenzvertrag: Creative Commons Namensnennung-Share Alike 4.0 International
https://creativecommons.org/licenses/by-sa/4.0/

URN: urn:nbn:de:bvb:473-irb-1083685
DOI: https://doi.org/10.20378/irb-108368

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

Abkürzung	Bedeutung
AI	Artificial Intelligence
ATHENE	Nationales Forschungszentrum für angewandte Cybersicherheit
AWS	Amazon Web Services
BMBF	Bundesministerium für Bildung und Forschung
BSI	Bundesamt für Sicherheit in der Informationstechnik
BWL	Betriebswirtschaftslehre
CDO	Chief Digital Officer
CERT	Computer Emergency Response Team
CISO	Chief Information Security Officer
CIO	Chief Information Officer
CSIRT	Computer Security Incident Response Team

Abkürzung	Bedeutung
CTO	Chief Technology Officer
CTO/CIO	Chief Technology Officer / Chief Information Officer
DFN-CERT	Deutsches Forschungsnetz – Computer Emergency Response Team
DFG	Deutsche Forschungsgemeinschaft
DNS	Domain Name System
DSA	Digital Services Act
DSGVO	Datenschutz-Grundverordnung
ENISA	European Union Agency for Cybersecurity
ERC	European Research Council
EU	Europäische Union
FAU	Friedrich-Alexander-Universität Erlangen-Nürnberg
GCP	Google Cloud Platform
HAW	Hochschule für Angewandte Wissenschaften
HISP	Hochschulinformationssicherheitsprogramm
HITIS	Hochschul-Informations- und Technologiesicherheits-Audit
HRK	Hochschulrektorenkonferenz
IAM	Identity and Access Management
IETF	Internet Engineering Task Force
IHE	Inside Higher Ed
IP	Internet Protocol
ISMS	Information Security Management System
ISO 27001	Information Security Management Standard (Zertifizierung)
ISO 27002	Information Security Management Controls (Leitfaden)
IT	Informationstechnologie
ITIL	IT Infrastructure Library
KI	Künstliche Intelligenz
KMK	Kultusministerkonferenz
KRITIS	Kritische Infrastrukturen
LMU	Ludwig-Maximilians-Universität München
MaRisk	Mindestanforderungen an das Risikomanagement
MFA	Multi-Faktor-Authentifizierung

Abkürzung	Bedeutung
MSC	Münchner Sicherheitskonferenz
NCSC	National Cyber Security Centre (UK)
NIS2	Network and Information Security Directive 2.0
NIST	National Institute of Standards and Technology
OpenAI	KI-Entwicklungsfirma
OZG	Onlinezugangsgesetz
PDF	Portable Document Format
PKI	Public Key Infrastructure
RZ	Rechenzentrum
SAP	SAP SE (Softwareunternehmen)
SIEM	Security Information and Event Management
SOC	Security Operations Center
SOP	Standard Operating Procedure
SOPHOS	IT-Sicherheitsunternehmen
StMWK	Bayerisches Staatsministerium für Wissenschaft und Kunst
TLS	Transport Layer Security
TUM	Technische Universität München
TUM.ai	KI-Initiative an der Technischen Universität München
UK	Vereinigtes Königreich
USA	Vereinigte Staaten von Amerika
VPN	Virtual Private Network
VP	Vizepräsident:in
ZKI	Zentren für Kommunikationsverarbeitung in Forschung und Lehre e.V.

Abstract (Deutsch)

Diese Arbeit untersucht, wie globale geopolitische Dynamiken die Rahmenbedingungen für Wissenschaft und Hochschulen im Cyberraum verändern – ein bislang wenig beleuchtetes Spannungsfeld zwischen Politik und Wissenschaft.

Aufbauend auf einem interdisziplinären theoretischen Fundament wird ein heuristischer Analyserahmen zentraler Spannungsverhältnisse – etwa zwischen Offenheit und Sicherheit oder Kooperation und Fragmentierung – entwickelt und erstmals systematisch auf nationalen sowie internationalen Cybersicherheitsstrategien empirisch validiert. Die Analyse zeigt eine deutliche Lücke zwischen strategischen Anforderungen und institutioneller Umsetzung und offenbart neue Risiken für Hochschulen. Ergänzt durch eine Fallstudie aus Bayern zeigt die Analyse signifikante Umsetzungsdefizite, strategische Leerstellen und institutionelle Risiken im Wissenschaftsbereich auf. Als Ergebnis werden sieben evidenzbasierte Handlungsempfehlungen formuliert, um Cybersicherheit in Hochschulen nachhaltig zu verankern – ohne die Grundprinzipien wissenschaftlicher Freiheit, Transparenz und digitaler Souveränität zu gefährden.

1. Einleitung

Das Ende des Ost-West-Konflikts weckte Hoffnungen auf eine Ära globaler Stabilität, Frieden und Zusammenarbeit. Konzepte wie das „Ende der Geschichte“ (Fukuyama 1992) prägten das Narrativ einer neuen Blütezeit von Globalisierung, Demokratie, Marktwirtschaft und regelbasierter internationaler Ordnung – und auch einer grenzüberschreitenden, frei zugänglichen Wissenschaft.

Parallel dazu führte der technologische Fortschritt zu einer neuen globalen Vernetzung der Universitäten. Sie wurden zu Pionieren des entstehenden Cyberraums: Bereits 1988 waren weltweit über 60.000 Rechner miteinander verbunden. 1990 nahm das zivile Internet als World Wide Web seinen Anfang. Seine Ursprünge liegen in strategischen Überlegungen des Kalten Krieges – als ARPANET konzipiert, sollte es auch unter atomaren Bedingungen kommunikationsfähig bleiben.

Nach dem Kalten Krieg übernahmen wissenschaftliche Einrichtungen dieses dezentrale Netzwerkkonzept, entwickelten es weiter und adaptierten es für Forschung und Lehre. Ziel war es nicht mehr, einen Krieg zu überstehen, sondern Wissen dezentral, offen und global zugänglich zu machen.

Diese Entwicklung entsprach der Systemlogik der Wissenschaft, wie sie etwa Niklas Luhmann beschreibt: Wissenschaft operiert im Medium der Wahrheit, indem sie Erkenntnisse kommuniziert, überprüft und weiterentwickelt (Luhmann 1992). Das Internet wirkte als idealer Katalysator – durch beschleunigten Austausch, breite Partizipation und globale Verfügbarkeit von Wissen.

Getragen von der Hoffnung auf internationalen Austausch und Erkenntnisgewinn wurde der Cyberraum zur Projektionsfläche eines digitalen Humanismus. Die Universität – in ihrer Selbstdefinition als korporative Gemeinschaft von Lernenden und Lehrenden mit übernationalem Charakter (Jaspers 2016) – schien diesem Ideal zeitweise sehr nahe zu kommen.

David Clark brachte den frühen Geist des Internets 1992 mit den Worten auf den Punkt: „We reject: kings, presidents and voting.“ John Perry Barlow ergänzte in seiner berühmten

Declaration of the Independence of Cyberspace (1996): „Ihr [Staaten] seid nicht willkommen unter uns. Ihr habt keine Souveränität, wo wir uns versammeln.“ Diese Perspektiven standen sinnbildlich für ein Internet, das sich als Gegenmodell zu staatlicher Macht verstand. Diese Utopie fügte ich gut ins Narrativ der 1990er-Jahre – doch sie sollte nicht lange Bestand haben. Der Cyberraum, gedacht als Friedensraum, erwies sich bald als umkämpfter Schauplatz.

Zunächst dominierte der Glaube an die selbstregulierende Kraft des Marktes. Globale Plattformen wie Google, Amazon und Facebook wuchsen rasant – die Wissenschaft profitierte enorm vom freien Informationsfluss. Doch bald zeigte sich: Der Cyberraum ist nicht neutral. Spätestens mit den Ereignissen des Arabischen Frühlings und den Wahlmanipulationen 2016 in den USA trat eine neue Phase ein, in der soziale Medien zu geopolitischen Akteuren wurden.

Heute wird der Cyberraum zunehmend fragmentiert. Nationale Initiativen wie Stargate (USA), Gaia-X (EU) oder das Social Credit System (China) verdeutlichen das Ringen um digitale Souveränität und strategische Kontrolle. Der technologische Wettbewerb ist längst sicherheitspolitisch aufgeladen. Es formen sich neue Allianzen u.a. zwischen Politik und Wirtschaft. Sam Altman, CEO von OpenAI, brachte diese Verflechtung in Bezug auf das KI-Megaprojekt Stargate auf den Punkt: „I think this will be the most important project of this era […] We wouldn’t be able to do this without you, Mr. President“ (Allyn 2025).

Diese Dynamik betrifft zunehmend auch die Wissenschaft. Wie Schmitt & Spiewak (2025) warnen: „Die deutsche Wissenschaft ist eng mit der amerikanischen vernetzt. Jahrzehntelang war das ein Vorteil. Nun wird es zur Bedrohung.“ Ein möglicher Rückzug der USA aus wissenschaftlichen Kooperationen, das Streben nach strategischer Autonomie und wachsender regulatorischer Druck verändern die Rahmenbedingungen für globale Wissenschaft tiefgreifend. Die politische Aufmerksamkeit richtet sich zunehmend auf Wissenschaft als sicherheitsrelevanten Sektor.

Auch Deutschland reagiert: Der Koalitionsvertrag der kommenden Bundesregierung definiert Cybersicherheit als Schlüsseltechnologie (Koalitionsvertrag 2025, S. 68) und kündigt Investitionen in Dual-Use-Forschung, IT-Sicherheitsprodukte und staatliche Schutzmaßnahmen an (ebd., S. 79).

Damit geraten Hochschulen in ein strukturelles Spannungsverhältnis: Sie müssen sich gegen neue Cyberbedrohungen wappnen, dabei jedoch das Ziel, „Deutschland in Zeiten globaler Polarisierung als attraktives Zielland und sicheren Hafen der Wissenschaftsfreiheit für Forschende aus aller Welt“ (Koalitionsvertrag 2025, S. 75) zu erhalten, nicht aus dem Blick verlieren.

Diese Spannungsfelder zeigen, wie Wissenschaft zum Objekt im Cyberraum wird – als Nutzerin, Gestalterin und Zielscheibe. Die Frage, wie sich unterschiedliche, zum Teil widersprüchliche Anforderungen austarieren lassen, bildet eine zentrale Problemstellung dieser Arbeit.

Obwohl in der Cybersicherheitsforschung zahlreiche Studien zu kritischen Infrastrukturen, staatlichen Strategien und industriellen Akteuren vorliegen, fehlt bislang eine systematische Analyse der Rolle von Hochschulen im geopolitisch fragmentierten Cyberraum. Die besonderen Spannungsverhältnisse wissenschaftlicher Institutionen – etwa zwischen Offenheit und Schutzbedarf – bleiben wissenschaftlich unterbeleuchtet.

1.1. Zielsetzung und Forschungsfrage

Diese Arbeit untersucht die Auswirkungen globaler geopolitischer Dynamiken auf den Cyberraum sowie die Rolle von Wissenschaft und Hochschulen innerhalb dieses Spannungsfeldes. Im Mittelpunkt steht die Frage, wie daraus institutionelle Handlungsoptionen im Bereich der Cybersicherheit entwickelt werden können.

Die Analyse folgt einem dreistufigen Untersuchungsrahmen:

- **Makroebene – Global Dynamics**: Analyse internationaler und nationaler politischer Entwicklungen im Cyberraum, insbesondere geopolitischer Spannungen, Sicherheitsstrategien und digitaler Souveränitätsbestrebungen, die die Rahmenbedingungen für Wissenschaft grundlegend verändern.
- **Mesoebene – Science Policy & Institutional Strategy**: Untersuchung wissenschaftspolitischer Programme, strategischer Leitlinien und institutioneller Wahrnehmungen, die Cybersicherheit auf der Ebene von Wissenschaftsorganisationen und Governance-Strukturen adressieren.
- **Mikroebene – Institutional Actions**: Analyse konkreter Strategien und Handlungsansätze von Hochschulräumen, mit denen sie auf die Spannungsverhältnisse reagieren.

Die zentrale Forschungsfrage lautet:

Wie beeinflussen globale geopolitische Dynamiken den Cyberraum für Wissenschaft und Hochschulen, und wie können Spannungsverhältnisse systematisch kategorisiert werden, um daraus institutionelle Handlungsempfehlungen im Bereich Cybersicherheit zu entwickeln?

Die Relevanz dieser Fragestellung ergibt sich aus den aktuellen Umbrüchen im Cyberraum[1] und den daraus resultierenden Ambivalenzen für wissenschaftliche Institutionen. Hochschulen müssen Offenheit und internationale Kooperation sichern und zugleich ihre digitale Widerstandsfähigkeit ausbauen.

Zur Beantwortung dieser Frage entwickelt die Arbeit ein deduktives Analyseraster aus fünf zentralen Spannungsverhältnissen, die als heuristische Strukturkategorie dienen. Dieses Modell wird systematisch auf politisch-strategische Texte, wissenschaftspolitische Steuerungslogiken und die Hochschulpraxis angewendet.

Ziel der Arbeit ist es, einen wissenschaftlich fundierten Orientierungsrahmen bereitzustellen, der es Wissenschaft, Hochschulen und politischen Entscheidungsträgern ermöglicht, Cybersicherheit in der Wissenschaft strategisch zu verankern – ohne wissenschaftliche Grundprinzipien und institutionelle Autonomie zu kompromittieren.

[1] Cyberraum und digitaler Raum werden in dieser Arbeit an einigen Stellen synonym verwendet um die sprachliche Varianz zu erhöhen.

1.2. Aufbau der Arbeit

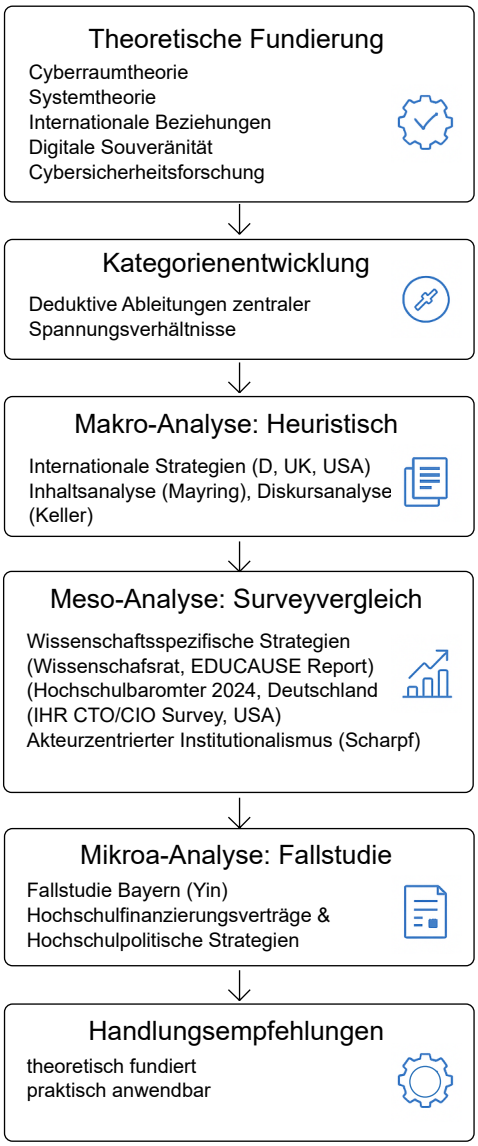

Abbildung 1: Ablaufstruktur und methodisches Vorgehen der Arbeit (eigene Darstellung).

Die Arbeit gliedert sich in sechs logisch aufeinander aufbauende Schritte, die theoriegeleitet entlang eines deduktiven Spannungsverhältnismodells strukturiert sind.

Zunächst erfolgt eine theoretische Fundierung des Begriffs „Cyberraum“, eingebettet in Perspektiven der Systemtheorie, Cybersicherheitsforschung, internationalen Beziehungen, der Souveränitätsforschung sowie diskurstheoretischer Ansätze. Aufbauend darauf werden zentrale Macht- und Wissensstrukturen im Cyberraum analysiert, aus denen deduktiv Spannungsverhältnisse abgeleitet werden, die als analytische Heuristik der gesamten empirischen Untersuchung dienen.

Im nächsten Schritt erfolgt eine **Makroanalyse internationaler und nationaler Strategiedokumente** (Deutschland, Großbritannien, USA). Ziel ist es, die Relevanz und Anwendbarkeit der Spannungsverhältnisse im Rahmen strukturierender Inhaltsanalyse und diskurstheoretischer Perspektiven zu prüfen.

Darauf folgt eine **Mesoanalyse wissenschaftspolitischer Strategien** sowie die Einbeziehung quantitativer Survey-Daten (u. a. EDUCAUSE Horizon Report 2024, Hochschulbarometer, IHE CTO/CIO Survey 2024). Diese Phase zielt auf die institutionellen Steuerungslogiken und Zielkonflikte in der Governance von Wissenschaft und Cybersicherheit.

Ergänzend wird in einer **Mikroanalyse die konkrete Umsetzung an bayerischen Hochschulen** untersucht. Diese Fallstudie analysiert sowohl die hochschulischen Sicherheitsstrukturen als auch die politischen und technischen Rahmenbedingungen auf Landesebene, orientiert an der Methodik von Yin (2018).

Abschließend werden aus den empirischen Befunden **Handlungsempfehlungen für Hochschulen und politische Akteure** abgeleitet. Diese Empfehlungen zielen auf eine balancierte Gestaltung zwischen Offenheit, Sicherheit und digitaler Souveränität im Wissenschaftssystem.

1.3. Methodisches Vorgehen

Diese Arbeit folgt einem qualitativ-analytischen Forschungsdesign, das theoriegeleitet entlang dreier Analyseebenen – Makro, Meso und Mikro – strukturiert ist. Im Zentrum steht ein deduktiv entwickeltes Spannungsverhältnismodell, das zentrale Zielkonflikte der Wissenschaft im Cyberraum, wie etwa zwischen Offenheit und Sicherheit, systematisch erfasst. Dieses Modell dient als analytische Heuristik, um strategische Texte, politische Steuerungslogiken und institutionelle Umsetzungspraktiken vergleichend zu untersuchen.

Die Methodenkombination ist theoriegeleitet und pragmatisch: Sie verbindet qualitative Inhaltsanalyse (Mayring, Kuckartz) mit diskurstheoretischen Perspektiven (Keller), Policy-Analyse (Scharpf) sowie einer vertiefenden Fallstudienanalyse (Yin). Die Spannungsverhältnisse fungieren dabei als durchgängige analytische Achse. Die Inhaltsanalyse wurde primär zur Strukturierung und Kategorisierung des Textmaterials eingesetzt, während die Diskursanalyse dazu diente, Deutungsmuster, narrative Verschiebungen und Auslassungen in den Strategietexten sichtbar zu machen. Eine funktionale Differenzierung der Methoden erfolgte entlang der jeweiligen Analyseebene.

- **Makroebene:** Nationale und internationale Cybersicherheitsstrategien werden mittels strukturierender Inhaltsanalyse und wissenssoziologischer Diskursanalyse ausgewertet. Die Auswahl der Länder basiert auf ihrem strategischen Einfluss, ihren Sicherheitskulturen und der politischen Relevanz der Wissenschaft.
- **Mesoebene:** Wissenschaftspolitische und organisationale Strategien werden durch Policy-Analyse, ergänzt durch internationale Survey-Daten, untersucht. Das Datenmaterial wurde aufgrund seiner Aktualität (2023–2025), institutionellen Relevanz und der Bezugnahme auf Cybersicherheit an Hochschulen ausgewählt.
- **Mikroebene:** Die Umsetzung von Cybersicherheitsmaßnahmen an bayerischen Hochschulen wird im Rahmen einer Fallstudie analysiert. Die Wahl fiel auf Bayern aufgrund des umfassenden Zugriffs auf unveröffentlichtes Archivmaterial, Berichte und Briefe. Eine geplante empirische Erhebung konnte aufgrund von Ressourcen- und Zugangsbarrieren nicht realisiert werden. Stattdessen wurde ein interner Audit-

Bericht der IT-Services für Informationssicherheit (HITS IS) verwendet, der aggregierte qualitative und quantitative Daten zur Cybersicherheit an Hochschulen enthält.

Die methodische Vorbereitung und detaillierte Ausführung dieses Forschungsansatzes erfolgt ausführlich in Kapitel 8. Der Forschungsansatz kombiniert interdisziplinär qualitative Inhaltsanalyse, Diskursanalyse, Policy-Analyse und Fallstudienforschung. Die zentrale methodische Grundlage bildet ein deduktiv entwickeltes Kategoriensystem, das aus den theoretischen Spannungsverhältnissen zwischen Offenheit und Sicherheit, Kooperation und Fragmentierung sowie digitaler Souveränität und technologischer Abhängigkeit abgeleitet wird.

2. Theoretischer Fundierung der globalen Dynamiken im Cyberraum

Im folgenden Kapitel wird zunächst der theoretische Rahmen entwickelt, in den der Begriff des Cyberraums sowie zentrale Konzepte aus Systemtheorie, Cybersicherheits- und Souveränitätsforschung sowie der Internationalen Beziehungen eingebettet werden.

2.1. Theorien des Cyberraums

Bevor Cybersicherheit als Untersuchungsgegenstand betrachtet werden kann, muss der zugrunde liegende Raum theoretisch verortet werden. Der Cyberraum stellt diese analytische Grundlage dar und bildet ein zentrales Fundament der vorliegenden Untersuchung. Ursprünglich aus der Science-Fiction-Literatur stammend, hat sich der Begriff in den letzten Jahrzehnten zu einem vielschichtigen Konzept mit technologischen, politischen und sozialen Dimensionen entwickelt. Dieses Kapitel beleuchtet den Cyberraum aus unterschiedlichen Perspektiven und entwickelt auf dieser Basis eine Arbeitsdefinition, die als theoretischer Ausganspunkt für die weitere Analyse dient.

2.2. Kuehls technologisch-informationsverarbeitender Cyberraum

Bereits 2009 legte Kuehl einen umfassenden Überblick zur Begriffs- und Definitionsgeschichte des Cyberraums vor. Er zeichnet die Entwicklung des Konzepts nach – von der Science-Fiction der 1980er-Jahre über die Ausweitung durch das entstehende Internet bis

hin zur sicherheitspolitischen Relevanz in geopolitischen und militärischen Kontexten. Dabei zeigt er, wie unterschiedliche Akteure und Disziplinen den Begriff geprägt haben: von Gibsons metaphorischer „konsensueller Halluzination“ (1984) über infrastrukturelle Perspektiven bei Waltz (1998) bis hin zur Definition als Domäne in der National Military Strategy for Cyberspace der USA (2006). Diese Vielfalt verdeutlicht, dass der Cyberraum sowohl technische als auch soziopolitische Dimensionen umfasst. Kuehl schlägt folgende Definition vor: „Cyberspace is a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies.” (Kuehl 2009, S. 4)

Diese Definition betont **die technische Grundlage des Cyberraums**: globale, durch das elektromagnetische Spektrum verbundene Systeme wie Internet, Telekommunikationsnetze und eingebettete Technologien. Als infrastrukturelles Rückgrat digitaler Kommunikation ermöglicht der Cyberraum jede Form von drauf basierender Informationsverarbeitung. Bis heute werden angelehnte Definitionen verwendet. Die Cybersicherheitsstrategie für Deutschland 2021 definiert ihn ähnlich: „Der Cyberraum ist der virtuelle Raum aller weltweit auf Datenebene vernetzten bzw. vernetzbaren informationstechnischen Systeme. Dem Cyberraum liegt als öffentlich zugängliches Verbindungsnetz das Internet zugrunde, das durch beliebige andere Datennetze erweitert werden kann“ (Deutschland 2021, S. 133).

Kuehls technologische Perspektive bildet somit die infrastrukturelle Basis für das Verständnis des Cyberraums – hebt aber gleichzeitig dessen funktionale Begrenztheit hervor.

2.3. Rattrays Environment-Konzept des Cyberraums

Aufbauend auf Kuehl kann das Konzept des Cyberraums mit Rattray um eine politische Dimension erweitert werden. Er versteht ihn nicht nur als technisches Netzwerk, sondern als **operativen Raum politischer Handlungen**. Der Cyberraum wird zur „environmental domain“, geformt durch die Interaktion physischer Systeme, Softwareprotokolle und Informationsflüsse. „Cyberspace is actually a physical environment: it is created by the connection of physical systems and networks, managed by rules set in software and communications protocols. [...] Cyberspace is a new theater of operations” (Rattray 2009, S. 2).

Diese Perspektive hebt die **Operabilität** des Cyberraums hervor. Analog zu anderen Domänen wie Land oder Luft eröffnet der Cyberraum Möglichkeiten zur Ausübung von Kontrolle, Macht und Einfluss. „Cyberspace is a manmade environment [...]. States, corporations and other actors [...] make choices about ownership, control, and operation of these key cyberspace features" (ebd., S. 13).

Ein entscheidender Unterschied zu klassischen Domänen liegt in der extremen Veränderlichkeit des Cyberraums: „A second unique characteristic of cyberspace is its rapid changeability" (ebd.). Technologische Entwicklungen können Hauptmerkmale und Betriebsmodi des Cyberraums rasch verändern. Dies erfordert **kontinuierliche Anpassungsstrategien**, auch seitens wissenschaftlicher Institutionen. Rattray betont, dass verteidigungsrelevante und wirtschaftliche Strukturen auf den Erhalt eines stabilen Cyberumfelds angewiesen sind: „We must strive to preserve the benefits of innovation and connectivity that have made the cyberspace environment so valuable" (ebd., S. 18).

Auch die Wissenschaft, als stark vom Cyberraum abhängiges System, muss eigene Resilienzmechanismen entwickeln – nicht nur gegen technische Angriffe, sondern auch gegen strategische Einflussnahme. Es müssen offene, kooperative Prinzipien verteidigt werden, die den Cyberraum ursprünglich prägten.

Rattrays Betonung der **Operabilität im Cyberraum** bildet eine Brücke zu soziologischen Perspektiven, etwa bei Thiedeke.

2.4. Thiedekes soziologische Perspektiven auf den Cyberraum

Über seine technologische Grundlage hinaus wird der Cyberraum von Thiedeke in seinem Buch „Soziologie des Cyberspace" weitergedacht als ein „**Sinnhorizont virtualisierten Handelns und Erlebens**", der durch computergestützte Kommunikation ermöglicht wird (Thiedeke 2009, S. 20 ff.). Diese Perspektive umfasst mehrere wesentliche Aspekte, die weit über die eher technischen Definitionen oder reine Operabilität hinausgehen, setzt diese jedoch voraus.

Koevolution mit dem Internet: Der Cyberraum ist nicht identisch mit dem Internet, sondern entwickelt sich in Wechselwirkung mit der Kommunikationsinfrastruktur. Während

das Internet die physische Grundlage bildet, repräsentiert der Cyberraum die virtuelle Dimension menschlichen Handelns.

Eigenständige Realität: Im Cyberraum entfalten sich Realitäten, die von der physischen Welt unterscheidbar, jedoch nicht als Ersatz für diese zu verstehen sind. Virtuelle Welten schaffen neue Erfahrungsräume, die bestehende Realitäten ergänzen.

Erweiterung bestehender Medien: Der Cyberraum erweitert bestehende Medien[2] und gesellschaftliche Sinnhorizonte, ohne diese zu ersetzen. Diese Erweiterung eröffnet neue Möglichkeiten der Interaktion und Wissensgenerierung.

Hybridisierung sozialer Strukturen: Durch die Digitalisierung von Personen, Objekten und Systemen verschmelzen soziale Verhaltensmuster und technische Funktionalitäten, was die Entstehung neuer soziotechnischer Strukturen begünstigt.

Validierung und Konditionierung: Handeln und Erleben im Cyberraum sind an die Bestätigung oder Enttäuschung der virtuellen Interaktion gebunden, wodurch der Verlauf der Kommunikation beeinflusst wird (Thiedeke 2023, S. 27).

Auch wenn Thiedeke in vielen Punkten soziologisch präzise darstellt, was der Cyberraum nicht ist, sieht er darin einen fruchtbaren Versuch, soziale **Systeme im Cyberspace als hybride sozio-technische Systeme** zu rekonstruieren und in entsprechenden Selbstbeschreibungen sinnhaft zu reflektieren. Handeln, Erleben, Realität und Sinn sind soziologisch vielfach behandelte Konzepte und erlauben Anschlussfähigkeit in der Wirklichkeitskonstruktion und führen über den Medienbegriff zur funktionalen Systemtheorie.

2.5. Luhmanns Konzept der symbolisch generalisierbaren Kommunikationsmedien im Cyberraum

Hier knüpft Luhmanns Konzept der **symbolisch generalisierten Kommunikationsmedien** und der **sozialen Systeme** an, das zeigt, wie Medien wie Macht, Geld, Wissen oder Liebe wirken – auch im Cyberraum. Diese Medien tragen zur sozialen Ordnungsbildung bei und passen sich, obwohl Luhmann (1998 verstorben) dies nicht mehr beobachten konnte, den Bedingungen des Cyberraums an.

Luhmann beschreibt: „Diese Medien lösen die Selektionsprobleme der Kommunikation durch eine symbolische Generalisierung des Kommunikationscodes“ (Luhmann 1997, S.

[2] Das Konzept der symbolisch generalisierten Kommunikationsmedian wird an späterer Stelle mit der funktionalen Systemtheorie nach Nicklas Luhmann vertieft eingeführt.

247). Sie schaffen damit stabile Erwartungen und reduzieren Komplexität – auch unter den veränderten Bedingungen digitaler Kommunikation.

In Luhmanns Terminologie wird die **Autopoiesis** der Gesellschaft und ihrer Teilsysteme dadurch ermöglicht, dass sie – ohne ihre jeweilige Funktion zu verlieren – neue Formen der Kommunikation und Erwartungsbildung etablieren. Sie wirken sowohl in der physischen Realität der Weltgesellschaft als auch im Cyberraum und ermöglichen differenzierte Erwartungsstrukturen und symbolische Formen.

Ein prägnantes Beispiel zeigt sich im Bereich der Finanzmärkte: Im Cyberraum wird heute über digitale Börsen und Broker mehr Geld bewegt – also das generalisierte Kommunikationsmedium der Wirtschaft im Code „Zahlung/Nicht-Zahlung“ – als jemals zuvor in der physischen Welt. Und das, ohne eine einzige Münze tatsächlich zu berühren. Hier zeigt sich besonders anschaulich, wie sich das Medium Geld im Cyberraum angepasst und weiterentwickelt hat.

Die Auswirkungen sind unmittelbar spürbar: Ein schlechter Börsentag im Cyberraum kann Existenzen vernichten, lange bevor in der realen Welt ein Unternehmen seine Produktion drosselt. Genauso kann eine durch die Decke schießende Kryptowährung aus einem bislang unbekannten Entwickler über Nacht einen Millionär machen. Virtuelle Finanzströme erzeugen neue ökonomische Wirklichkeiten, die unser reales Leben beeinflussen, obwohl sie sich vollständig im Cyberraum abspielen.

Diese Medien ermöglichen es, dass wir auch in sehr komplexen Situationen kommunizieren und handeln können, weil sie Erwartungen strukturieren: Wenn ich mit Geld bezahle, erwarte ich eine Leistung. Wenn jemand Macht hat, erwarte ich eine Entscheidung. Wenn jemand Wissenschaftler ist, erwarte ich faktisches Wissen. Zum Problem wird das, wenn diese Erwartungen nicht mehr erfüllt werden – oder wenn Erwartungen gestellt werden, die gar nicht erfüllbar sind.

„Wissen ist Macht“ gilt im systemtheoretischen Sinne nicht. Nach Luhmann sind **Macht** und **Wissen** zwei eigenständige, symbolisch generalisierte Kommunikationsmedien, die unterschiedlichen gesellschaftlichen Funktionen dienen. Während Macht auf die Durchsetzung von Entscheidungen zielt (Luhmann 1975, S. 21), ist Wissen auf Erkenntnisgewinn, Nachvollziehbarkeit und Anschlussfähigkeit in der Kommunikation ausgerichtet (Luhmann 1990, S. 143).

Problematisch wird es, wenn von Wissenschaft nicht mehr primär die Produktion von Wissen, sondern die Generierung faktischer Macht erwartet wird – etwa durch exklusive technologische Innovationen. Eine solche **Instrumentalisierung eines gesellschaftlichen Teilsystems** (z. B. Wissenschaft) durch ein anderes (z. B. Politik oder Wirtschaft) bezeichnet Luhmann als Irritation. Diese sei, so Luhmann sinngemäß, **kein direkter Steuerungsmechanismus**, sondern eine Irritation, die ein System intern verarbeiten muss (Luhmann 2004, S. 103).

Wenn jedoch diese Irritation dauerhaft besteht, kann es zur Zweicodierung kommen: Der eigene Systemcode wird durch den Fremdcode überlagert. In extremen Fällen kann dies die Autopoiesis gefährden – also die Fähigkeit eines Systems, sich selbst auf Basis seiner eigenen Operationen zu erhalten. Das lässt sich gut mit einem System Override aus der Informatik vergleichen: Schadsoftware überschreibt nicht den Originalcode, sondern zwingt ein System durch externe Eingriffe, anders zu funktionieren, als es ursprünglich gedacht war. Es läuft weiter – aber nicht mehr nach seiner eigenen Logik.

Im Verlauf der Untersuchung wird dieser Zusammenhang weiter präzisiert: Wenn Macht in den Cyberraum einzieht, wirkt sich dies nicht nur auf einzelne Organisationen, sondern auch auf das Wissen selbst aus. Die soziologischen Perspektiven auf den Cyberraum bieten umfangreiche Möglichkeiten, diese komplexen sozio-technischen Prozesse zu reflektieren und zu beschreiben – ein Weg, den diese Untersuchung bewusst einschlägt, um nicht bei rein technischen Schutzmaßnahmen zu verharren.

Auf der Ebene der Hochschulen zeigt sich, dass Cybersicherheit weit mehr erfordert als technische Infrastruktur: Die von Thiedeke hervorgehobenen sozialen und kulturellen Dimensionen machen deutlich, dass insbesondere die Sensibilisierung der Nutze**r** für Risiken und die Einbindung aller Akteure in eine gelebte Sicherheitskultur essenziell sind.

Auf der Ebene der Wissenschaft insgesamt stellt sich die Herausforderung noch grundlegender: Die Prinzipien von Offenheit und Wissenschaftsfreiheit geraten durch die neuen Machtverschiebungen im Cyberraum unter Druck und müssen neu reflektiert und geschützt werden.

Symbolisch generalisierte Kommunikationsmedien wie Macht, Geld und Wissen sorgen laut Luhmann dafür, dass Kommunikation auch in komplexen und unsicheren Systemen funktional bleibt. Diese Medien prägen maßgeblich, wie Wissenschaft als gesell-

schaftliches Teilsystem und Hochschulen als Organisationen ihre Rolle im Cyberraum definieren und Sicherheitsstrategien entwickeln. Luhmanns Ansatz wirkt damit verbindend zwischen den technischen und soziopolitischen Perspektiven von Kuehl, Rattray und Thiedeke, indem er aufzeigt, wie soziale Ordnung durch Kommunikation entsteht – und sich im Cyberraum neu entfaltet. Auch auf der Ebene internationaler Beziehungen lassen sich diese Mechanismen erkennen.

2.6. Fragmentierung des Cyberraums

Der Cyberraum hat sich in den vergangenen Jahren zunehmend zu einem **zentralen Schauplatz geopolitischer Interessen** und strategischer Konflikte entwickelt. Bereits 2012 beschrieb Myriam Dunn Cavelty ihn als fragmentiertes Feld, in dem verschiedenste Akteure – Staaten, Militär, Unternehmen – um Kontrolle und Einfluss ringen. Sie betont zugleich die strukturellen Grenzen staatlicher Steuerung: „Cyberspace is only in parts controlled or controllable by state actors […]. Considering cyberspace as an occupation zone is an illusion" (Dunn Cavelty 2012, S. 151).

Diese Einschätzung macht deutlich: Entscheidende Infrastrukturen des Cyberraums liegen außerhalb der unmittelbaren Reichweite nationaler Institutionen. Schutz und Steuerung können nicht ausschließlich staatlich erfolgen – sie erfordern die Einbindung privatwirtschaftlicher Akteure und transnationaler Kooperation. Cavelty spricht in späteren Arbeiten vom „wicked problem" der Cybersicherheit: „Cyber security is a so-called 'wicked problem': it is transboundary in nature, occurs at multiple levels across sectors, between institutions, and impacts all actors [...] in complex, politicized ways." (Dunn Cavelty 2022, S. 1)

Trotz dieser Vielschichtigkeit und Begrenztheit zeigt sich ein klarer Trend: Staaten und supranationale Organisationen reagieren zunehmend mit Strategien zur digitalen Souveränität. Projekte wie Gaia-X, IRIS2 oder das chinesische „Social-Credit-System" zielen darauf ab, technologische Abhängigkeiten zu verringern oder zu schaffen und infrastrukturelle Kontrolle oder gar Kontrolle über das Volk im Cyberraum zu gewinnen.

Diese Bestrebungen führen jedoch nicht zu einer einheitlicheren Ordnung, sondern verstärken die **Fragmentierung** des Cyberraums: Es entstehen parallel existierende, teils inkompatible Infrastrukturen mit eigenen Regulierungslogiken – ein Prozess, den Eriksson

& Giacomello (2022) mit Blick auf Satellitennetzwerke eindrucksvoll beschreiben: „Cyberspace infrastructure is increasingly reliant on space infrastructure, especially satellites, yet the consequences for politics and security remain uninvestigated" (S. 95).

Ein aktuelles Beispiel liefert das europäische Projekt IRIS2, eine Satellitenprojekt der EU[3], das als Gegengewicht zu Elon Musks Starlink-System positioniert wird. Während Starlink bis 2030 über 40.000 Satelliten betreiben will, plant Europa ein eigenes, kontrolliertes „Non-Terrestrial Network". Auch China, Amazon (Project Kuiper) und Kanada (Telesat) verfolgen ähnliche Vorhaben. „The wide array of entrepreneurs involved, dispersed across the globe, suggest that fragmentation rather than hegemony will characterize this domain" (Eriksson & Giacomello 2022, S. 97).

Diese Entwicklung verändert den Charakter des Cyberraums: **weg von einer offenen, globalen Infrastruktur hin zu einem Raum konkurrierender Machtzentren, technopolitischer Blockbildung und divergierender Standards**.

Für Hochschulen und wissenschaftliche Institutionen stellt dies eine doppelte Herausforderung dar: Sie müssen weiterhin global kooperieren, Wissen austauschen und offen agieren. Gleichzeitig wachsen die Anforderungen an Sicherheit, Souveränität und politische Anpassungsfähigkeit.

Diese Spannungen verschärfen sich insbesondere dann, wenn digitale Infrastruktur nicht mehr neutral gedacht wird, sondern zum Austragungsort strategischer Konflikte wird. Damit wird der Cyberraum für Wissenschaftsinstitutionen gleichzeitig Medium, Bedingung und Risiko ihrer Tätigkeit.

2.7. Synthese und Arbeitsdefinition

Vor dem Hintergrund der dargestellten theoretischen Perspektiven wird deutlich: Der Cyberraum ist ein **mehrdimensionales Phänomen**, das sich nur durch die Verbindung technologischer Grundlagen, politischer Steuerungsmechanismen und sozialer Kommunikationsprozesse angemessen erfassen lässt. Die Konzepte von Kuehl, Rattray, Thiedeke und Luhmann beleuchten dabei jeweils unterschiedliche, sich ergänzende Facetten – von der

[3] Mehr Informationen unter: https://defence-industry-space.ec.europa.eu/eu-space/iris2-secure-connectivity_en

technischen Infrastruktur über geopolitische Machtkonstellationen bis hin zu symbolischen Ordnungen und soziokulturellen Sinnwelten.

Um diesen Perspektiven gerecht zu werden und gleichzeitig eine tragfähige Grundlage für die weitere Analyse zu schaffen, ist eine präzise Arbeitsdefinition erforderlich. Sie dient als heuristischer Ankerpunkt, um den heuristischen Rahmen daran aufzuhängen, Spannungsverhältnisse im Cyberraum systematisch zu identifizieren, zu strukturieren und vergleichend auszuwerten.

Der Cyberraum ist eine dynamische, globale, soziotechnische Domäne, die digitale Infrastrukturen, Informations- und Kommunikationsströme sowie symbolisch generalisierte Kommunikationsmedien integriert.
Er basiert auf der technischen Grundlage des Internets und verwandter Netzwerke, ist zugleich aber ein Raum sozialer Ordnungsbildung und ein Schauplatz geopolitischer Auseinandersetzungen. Geprägt durch Machtkonflikte, Fragmentierung und diskursive Deutungskämpfe, bildet er ein Umfeld, in dem universelle Medien wie Wissen, Macht und Geld unter neuen Bedingungen verhandelt und operationalisiert werden.

Diese Definition verknüpft die zentralen Elemente der vorangegangenen Kapitel:

- die technische **Infrastruktur** (Kuehl),
- die politisch-strategische **Operabilität** (Rattray),
- die **sozialen Sinnhorizonte** und Handlungslogiken (Thiedeke),
- sowie die **systemische Strukturierung durch Medien** (Luhmann).

Sie bildet die **theoretische Grundlage** für das in Kapitel 9 entwickelte Modell zentraler **Spannungsverhältnisse**, das als analytisches Raster zur Bewertung politischer Strategien, institutioneller Praktiken und organisationaler Handlungsspielräume dient.

3. Cyberraum als globales Machtfeld

Der Cyberraum wurde lange Zeit als eine grenzenlose Sphäre der Freiheit und des Austauschs verstanden. John Perry Barlow beschrieb ihn in seiner Declaration of the Independence of Cyberspace (Barlow 1996) als „neue Heimat des Geistes“, die sich den Zwängen physischer Staaten entzöge. Diese idealistische Vision wurde jedoch von einer

Realität eingeholt, in der der Cyberraum zunehmend von Nationalstaaten als strategisches Machtfeld beansprucht wird. Der Cyberraum ist nicht länger ein autonomes und neutrales Territorium, sondern wird von geopolitischen Zielen, wirtschaftlichen Interessen und sicherheitspolitischen Erwägungen geprägt. Staaten können es nicht hinnehmen, diese Sphäre außerhalb ihrer Kontrolle zu belassen.

Wie Hobbes Leviathan ist die staatliche Macht in den Cyberraum vorgedrungen und hat begonnen, ihn nach ihren Vorstellungen umzugestalten. Thomas Hobbes' Konzept des Leviathans (Hobbes 1651) findet im Cyberraum eine neue Relevanz. Der Leviathan als Staat ist sprichwörtlich in den Cyberraum gekrochen und hat sich mit Cyberbehemoth, einer Art unreguliertem Naturzustand des Cyberraums, angelegt. Dort fällt es ihm jedoch schwer, seine Allmacht zu entfalten, denn er teilt sich diese mit weiteren mächtigen Akteuren, darunter transnationalen Konzernen. Noch ist nicht entschieden, welche Akteure sich durchsetzen werden und welche Machtstrukturen dominieren werden.

Belege für die wachsende staatliche Einflussnahme finden sich beispielsweise im Verhalten von Tech-Milliardären des Cyberraums: Der demonstrative Auftritt von Mark Zuckerberg vor Präsident Trump oder Elon Musks Versuche, ökonomische Macht in politische Einflussnahme zu verwandeln, zeigen, dass sich auch große Konzerne dem politischen Druck beugen müssen oder gar wollen, oder es auch nur eine temporäre Strategie ist, um eigene Logiken weiterzuverfolgen.

Wie Zettl (2022, S. 67) beschreibt, verwandelt sich der Cyberraum zunehmend in eine Arena, die von staatlicher Einflussnahme, Überwachung, Zensur und Fragmentierung geprägt ist. Auch andere Autoren (z. B. Gartzke 2013; Valeriano/Maness 2015; Blank 2017; Nye 2010) beobachten eine ähnliche Entwicklung. Ein Blick in den aktuellen Koalitionsvertrag Deutschlands bestätigt dies: Cybersicherheitsforschung wird künftig explizit als Teil der Sicherheits- und Verteidigungsforschung behandelt (Koalitionsvertrag 2025, S. 79). Die Macht tritt ans Ruder im Cyberraum.

3.1. Macht im Cyberraum

Eine Möglichkeit, diese Transformation zu beschreiben webt das Konzept der Macht in den Cyberraum ein. Max Weber definiert Macht als die "Chance, innerhalb einer sozialen Beziehung den eigenen Willen auch gegen Widerstreben durchzusetzen, gleichviel worauf diese Chance beruht" (Weber 1972, S. 28). Fähigkeit und Wille sind in den meisten

Machtdefinitionen nach Max Weber übernommen und weiterentwickelt worden. Der letzte Teil der Definition – die Chance, worauf diese beruht – wird weniger und auch kontroverser diskutiert. Dabei zeigt sich spätestens seit den Enthüllungen von Edward Snowden zur globalen Überwachungspraxis der USA im Cyberraum oder der Wahlmanipulation durch Russland im Zuge der US-Wahl 2016, dass gerade im Cyberraum unklar ist, worauf solche Chancen beruhen, da diese schlicht nicht bekannt sind.

Nye (2010) differenziert diese Perspektive durch die Unterscheidung von **Hard- und Softpower**. Hardpower zeigt sich in militärischen Cyberstrategien, Kontrolle über Basistechnologien und Überwachungspraktiken, während Softpower in der Gestaltung von Normen und der Kontrolle von Informationen, Datenflüssen und Technologien sichtbar wird. In Bezug auf Macht liefern u.a. Rattray (2009) Kuehn (2009) plausible Annahmen, dass der Cyberraum nicht anders ist als die vier physischen Domänen Land, Wasser, Luft und Weltraum.

"First, cyberspace is an operational space where humans and their organizations use the necessary technologies to act and create effects, whether solely in cyberspace or in and across the other operational domains and elements of power. In this sense, it is like any of the other four physical domains – land, sea, air, and outer space – in which we operate, and one of the explicit objectives of this definition is to place cyberspace firmly within the bounds of the operational domains and elements of power within which the national security community operates" (Kuehl 2009, S. 5).

Während Hardpower in der physischen Welt durch Kriegsschiffe, Panzer, Flugzeuge und Raketen manifest und quantifizierbar erscheint, erweist sich die Differenzierung zwischen Hard- und Softpower im Cyberraum als weitaus komplexer und bleibt vielfach epistemisch verborgen. Auch wenn die technologischen Voraussetzungen zur Nutzung des Cyberraums grundsätzlich denen physischer Domänen – wie Fahrzeuge, Schiffe oder Raumfahrzeuge – vergleichbar sind, bleibt ein konstitutiver Unterschied.

Der Cyberraum entzieht sich unmittelbarer sinnlicher Erfahrung. Diese anthropozentrische, sinnesorientierte Perspektive kann dazu führen, die Bedrohung durch Machtmittel im Cyberraum zu unterschätzen, da sie – anders als ein Flugzeug, ein Panzer oder eine Rakete – weder sichtbar noch hörbar ist. Es wäre aber falsch dies so zu sehen, denn Milliarden Menschen bewegen sich täglich im Cyberraum, während sich nie mehr als 19 Menschen zeitgleich im Weltraum (Space) befanden (Stand: 12.09.2024). Dies verdeutlicht,

dass der Cyberraum klare soziale Realitäten konstruiert. Eine Möglichkeit dies sichtbar zu machen wird im folgenden Kapitel beschrieben.

Das konstruktivistische Konzept symbolisch generalisierten Kommunikationsmedien von Niklas Luhmann wurde bereits eingeführt und liefert wichtige Ergänzung zu klassischen Machtdefinitionen. Diese Medien – wie Geld, Recht, Wissenschaft oder Macht selbst – dienen dazu, Erwartungen in komplexen sozialen Systemen zu stabilisieren und Kommunikation trotz Unsicherheit anschlussfähig zu machen. Im Cyberraum entfalten sie eine neue Dynamik: Macht wird durch digitale Technologien operationalisiert, etwa durch Algorithmen, Plattformen oder die Regulierung von Datenflüssen. Diese Mechanismen schaffen die Möglichkeit, soziale Ordnungen im Cyberraum zu gestalten und spezifische Erwartungen durchzusetzen, wie es auch klassische Machtkonzepte beschreiben. Nach Niklas Luhmann ist Macht ein symbolisch generalisiertes Medium der Kommunikation, das die Wahrscheinlichkeit erhöht, dass bestimmte Entscheidungen akzeptiert werden; seine Funktion liegt dementsprechend in der Herstellung allgemein gültiger Entscheidungen (Luhmann 1988, S. 118). Damit wird deutlich, dass Macht im Cyberraum nicht nur als physische oder militärische Kontrolle sichtbar wird, sondern vor allem als strukturierende Kraft in einem Netzwerk digitaler Interaktionen.

Diese Diskussion führte uns aber tiefer in die politische Philosophie der Macht im Cyberraum. Dies wäre ein spannendes Unterfangen, kann hier jedoch nicht weiter vertieft werden. Im Ergebnis bleibt, dass Macht auch in der neuen Domäne Cyberraum als Konzept greift, relevant ist und für Deutungs- und Erklärungsmuster und Wirklichkeitskonstruktionen gut herangezogen werden kann. In der Cyber Strategie des Vereinigten Königreichs heißt es dann dazu doch wieder sehr einfach: „Cyber power is the ability to protect and promote national interests in and through cyberspace. Countries that are best able to navigate the opportunities and challenges of the digital age will be more secure, more resilient and more prosperous in future“ (UK 2022, S. 11).

Besonders bleibt, dass der Cyberraum menschengemacht ist und einer weitaus höheren Dynamik ausgesetzt ist als die anderen Domänen. Dies wurde in der für diese Arbeit verwendeten Definition bereits reflektiert. Wenn die Topografie und Dynamik im Cyberraum andere sind, wie lässt sich Macht im Cyberraum dann fassen und messen?

3.2. Cyberpower messen

Weiterführend könnte ein Blick darauf sein, wie sich Macht im Cyberraum konkret darstellt – wer also über die übliche anekdotische Zuweisung von Macht im Cyberraum, u. a. an die USA, Russland oder China, in unterschiedlichen Cyberkontexten tatsächlich Machtmittel aufbaut und einsetzt. Einen seltenen und spannenden Ansatz zur Operationalisierung von Machtmitteln im Cyberraum unternimmt der National Cyber Power Index (NCPI) des Cyber Projects am Belfer Center for Science and International Affairs der Harvard Kennedy School. Danach ist "Cyber power […] the effective deployment of cyber capabilities by a state to achieve its national objectives." (Voo, Hemani, Cassidy 2022, S. 7). Ganz nach Weber ist der Cyberpower Index ein Produkt aus "Capability" x "Intent" also das Produkt aus Fähigkeit und Willen (ebd., S. 18). Beide Dimensionen werden aktuell in einem "Conceptual Framework" in folgenden acht Kategorien erhoben und bewertet.

Ziel	Kurze Beschreibung
Amassing & Protecting Wealth	Cyber-Operationen zur Anhäufung und Sicherung von Vermögen, z.B. durch Diebstahl, Erpressung und Angriffe auf Finanzinfrastrukturen.
Controlling & Manipulating the Information Environment	Elektronische Kontrolle und Beeinflussung von Informationen im In- und Ausland, inkl. Propaganda, Desinformation und Bekämpfung extremistischer Inhalte.
Defining International Cyber Norms and Technical Standards	Aktive Mitgestaltung internationaler Cyber-Normen, z.B. durch Verträge, Arbeitsgruppen und Partnerschaften.
Destroying or Disabling an Adversary's Infrastructure and Capabilities	Zerstörung oder Störung gegnerischer Infrastruktur durch Cyberangriffe, etwa auf kritische Systeme oder Kommunikationsnetzwerke.
Foreign Intelligence Collection for National Security	Cyberspionage zur Gewinnung sicherheitsrelevanter Informationen, wie militärische Pläne oder Regierungskommunikation.
Growing National Cyber and Commercial Technology Competence	Förderung der heimischen Technologiebranche, legal durch Forschung oder illegal durch Industriespionage.
Strengthening and Enhancing Cyber Defenses	Verbesserung der nationalen Cyberabwehr, Förderung von Cybersicherheit und Aufklärung der Bevölkerung.
Surveilling and Monitoring Domestic Groups	Überwachung und Beobachtung inländischer Gruppen mittels gesetzlicher und technischer Cyberüberwachung.

Abbildung 2: Conceptual Framework gemäß NCPI 2022, S. 17f.

Auch wenn nicht auf die Kategorien im Einzelnen eingegangen werden kann, spannt die 2022 Edition des NCPI im Ergebnis Netzdiagramme von Staaten nach „Objektives“ auf.

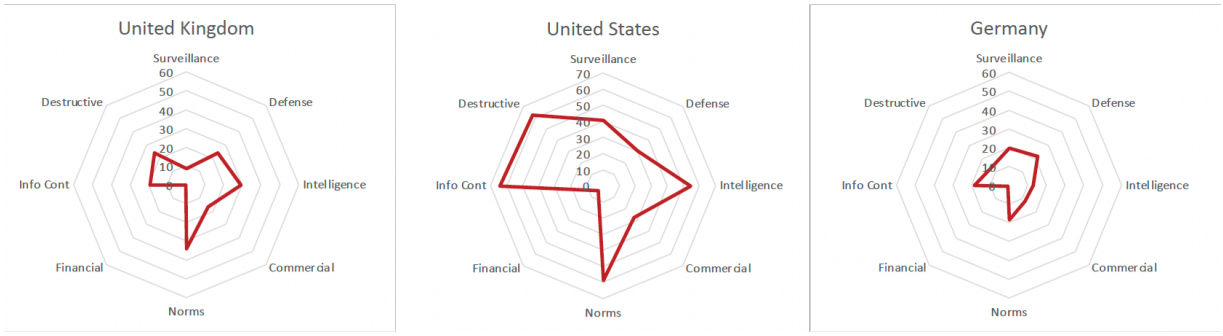

Abbildung 3: National Cyber Power Radar Charts by Objective, gemäß NCPI 2022, S. 25f.

In der Gegenüberstellung von „Capability“ x „Intend“ ergibt sich ein Verteilungsdiagramm der Cybermacht. Auch wenn Staaten wie USA und China hier weiterhin auf den vorderen Plätzen insgesamt landen, entstehen auch spannende Einsichten und eine weitaus differenziertere und objektivere Übersicht der Verteilung von Cyberpower insgesamt und Cyber- Capability und Cyber-Intend im Besonderen.

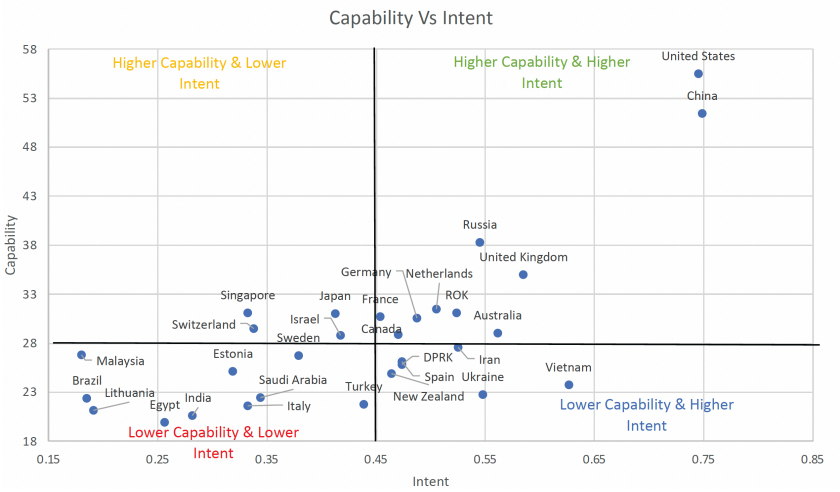

Abbildung 4: Capability vs Intend Scatter chart, gemäß NPCI 2022, S. 26.

Deutschland findet sich insgesamt hierbei im Mittelfeld auf Platz 11 von 30 betrachteten Staaten ein, wird aber im Feld der Fähigen und Willigen aufgeführt und damit der Gruppe zugeordnet, die aktiv Cybermacht zu formen und einzusetzen bereit ist.

Der Ansatz des NCPI-Index ist unbedingt weiterzuverfolgen, stößt jedoch an Grenzen angesichts der enormen Dynamik des Cyberraums und der mangelnden Verfügbarkeit von Daten: "NCPI’s objective oriented analysis of national cyber power suffers from some limitations, which are mostly connected with the evolving and contested nature of “Cyber Power” and the limited data available in the public domain about state cyber capabilities and intentions." (ebd. S. 13). Der Ansatz kann jedoch prototypisch dazu dienen, ein ausdifferenziertes Messinstrumentarium für Cyberpower und Machtmittel im Cyberraum zu

entwickeln. Bedenkt man die Vielfalt von methodischen Ansätzen zur Messung von klassischen Machtmitteln oder gar die fein ziselierten Methoden und Instrumente von BWL und VWL zur Messung von wirtschaftlichen Leistungsdimensionen ergibt sich für den Bereich Cyberpower ein sehr großes Zukunftspotenzial.

3.3. Globale Machtdynamiken im Cyberraum

Der NCPI stellt jedenfalls fest, dass Macht im Cyberraum durchaus divergent verteilt ist. Die neuen Asymmetrien führen zu neuen geopolitischen Spannungen im Cyberraum. Der allgemeine Weltzustand wird von manchen Autoren gar als „Weltunordnung“ (Masala 2023; Neumann 2022) beschrieben.

Die Anpassungsstrategien im Cyberraum sind vielfältig. Für die EU werden diese mit der strategischen Ausdifferenzierung des Konzepts der „Digitalen Souveränität“ und Ideen wie „De-Risking“ – einem Konzept, das von EU-Kommissionspräsidentin Ursula von der Leyen geprägt wurde – kontextualisiert. Damit sind europäische Bestrebungen verbunden, digitale Souveränität (zurück)zu erlangen und die Abhängigkeit von außereuropäischen Technologieanbietern zu verringern. Gleichzeitig erfordert die globale Verflechtung des Cyberraums Kooperation über nationale Grenzen hinweg – nun jedoch vermehrt in geopolitischen Blöcken, deren Zuschnitt neu verhandelt wird.

Zettl (2022, S. 81) beschreibt diese Dynamik als einen **diskursiven Machtkampf**, in dem Begriffe wie "Cyber Strategie", "Digitale Souveränität" und „Cybersecurity“ strategisch eingesetzt werden. Diese Entwicklung wird durch die spezifischen Machtstrukturen des Cyberraums vorangetrieben. Staaten nutzen ihre "Cyberpower" nicht nur, um ihre Interessen zu verteidigen, sondern auch, um den Cyberraum nach ihren eigenen Normen und Standards zu fragmentieren.

Die Fragmentierung entsteht dabei aus konkurrierenden Konzepten digitaler Souveränität und der gezielten Regulierung von Datenflüssen und Technologien, die zunehmend nationale Interessen über globale Kooperationen stellen. Dadurch wird der Cyberraum nicht mehr als universeller Raum wahrgenommen, sondern in überregionale und nationale "Inseln" zersplittert, die eigenen Regeln und Standards folgen.

Die Unterbindung von Anschlussfähigkeit im Cyberraum durch Fragmentierung ist damit ein Machtmittel eigener Art, da die cyber-physische Abgängigkeit offenbart und zur Wahrnehmung von Machtlosigkeit führt.

Dass Fragmentierung auch die Wissenschaft trifft, zeigt sich daran, dass Staaten auch im Bereich der Forschung die Schilde hochfahren, wenn es heißt:

„Wir stärken die Forschungssicherheit, entwickeln gemeinsam mit der Allianz der Wissenschaftsorganisationen Leitlinien für den Umgang in sensiblen internationalen Kontexten und verbessern die Beratungsinfrastruktur.“ (Koalitionsvertrag 2025, S. 81).

Dies wird Auswirkungen auf die Wissenschaft haben, denn klar ist: Es wird nicht mehr selbstverständlich bleiben, Wissen global und frei zu teilen.

3.4. Weaponized Interdependencies

Neben Nationalstaaten, die bisher vorrangig betrachtet werden, prägen auch transnationale Akteure den Cyberraum. Internationale militärische Organisationen wie die NATO, global agierende Unternehmen wie Google, Microsoft, Meta, X, ByteDance (Tiktok) oder Huawei neu auch OpenAI oder NGOs wie die Internet Society setzen mandatiert oder de-facto Normen und Standards, die weitreichende Konsequenzen haben.

Drezner et al. (2021) führen das Konzept der „Weaponized Interdependencies“ ein, das beschreibt, wie globale Netzwerke strategisch genutzt werden, um Abhängigkeiten zu schaffen und Macht auszuüben. Die Macht privater Unternehmen kann sogar so weit reichen, dass sie politische Amtsinhaber von ihren Plattformen und damit einem bedeutenden, öffentlichen Diskursraum ausschließen können, was somit ihre in den letzten Jahren gestiegene Diskursmacht begründet. "Social media companies now have more power over public speech than any government, yet they are largely unaccountable to the public they serve" (Singer & Brooking 2018, S. 27).

Der Ausschluss von Präsident Donald Trump von Twitter (jetzt X) ist ein prominentes Beispiel – der jüngste Bußgang von Mark Zuckerberg und Co. gegenüber nun wieder Präsident Donald Trump ebenfalls. "In a world where a handful of tech companies control the major platforms for political discourse, the line between private power and public responsibility is dangerously thin" (Roose 2021, S. 213). Das prägnanteste aktuelle Beispiel für

„Weaponized Interdepence“ im Cyberraum ist derzeit die Abhängigkeit der Ukraine als Staat von Space X und Starlink und damit von Elon Musk als Einzelperson. An diesem Beispiel wird die cyber-physische Dependenz greifbar. Ohne Starlink und damit Zugang zum Cyberraum ist die Ukraine kaum in der Lage, den Krieg gegen Russland fortzusetzen, da die meisten moderneren (Waffen)Systeme nur wirksam eingesetzt werden können, wenn sie eine Anbindung an den Cyberraum haben. Der Fall Starlink zeigt, wie einzelne Akteure – in dem Fall eine Einzelperson - im Cyberraum geopolitische Macht entfalten können. Die Drohung eines einzigen Unternehmens reicht aus, um staatliches Handeln substanziell zu beeinflussen.

In den Bereich der Wissenschaft übertragen, stellt sich aktuell die Frage, wo diese überall in kritische Abhängigkeit bei Daten, Infrastrukturen, Geld und Personal geraten ist. Einige Beispiele, wie Überseemessbojen für die Meeres- und Klimaforschung, die Genomdatenbank des „National Institutes of Health (NIH)“ sind identifiziert und im Koalitionsvertrag gar mit dem Ziel versehen: „Wir schaffen eine Nationale Biobank […]“ (Koalitionsvertrag zwischen 2025, S. 80). Eine Übersicht kritischer Abhängigkeiten in der Wissenschaft wird derzeit eilig von den Wissenschaftsorganisationen zusammengetragen. Dies bestätigt das Konzept der „Weaponized Interdependencies“ im Cyberraum und zeigen das der Leviathan in der Tat mit anderen "Monstern" darin um Macht ringt.

3.5. Cyberraum als militärische Domäne

Eine eindeutige Manifestation von staatlicher Macht im Cyberraum ist die Anerkennung des Cyberraums als eigenständige militärische Domäne. Neben den klassischen Domänen Land, Wasser, Luft und Weltraum ist der Cyberraum heute integraler Bestandteil der globalen Sicherheitsarchitektur. Begriffe wie „Cyberkrieg“ (Cyberwar) und „Hybrider Krieg“ (Hybrid War) unterstreichen die fortschreitende Militarisierung dieses digitalen Raumes. Die Gründung spezialisierter Cyberkommandos spiegelt den strategischen Anspruch wider, den Cyberraum nicht nur zu schützen, sondern ihn auch gezielt zur Machtprojektion einzusetzen.

Der Cyberraum eröffnet dabei neuartige Machtoptionen. Angriffs- und Verteidigungsoperationen können hier mit verhältnismäßig geringem Ressourceneinsatz durchgeführt werden und stellen traditionelle Hierarchien und Abschreckungsmechanismen in Frage. Bits und Bytes lassen sich schneller und billiger bewegen als Truppen oder Schiffe. Dadurch

wird der Cyberraum zu einem besonders dynamischen Machtfeld, in dem neue Akteure asymmetrische Vorteile gegenüber etablierten Mächten suchen und finden.

„Once available only to a small number of well-resourced countries, offensive hacking tools and services, including foreign commercial spyware, are now widely accessible. These tools and services empower countries that previously lacked the ability to harm U.S. interests in cyberspace and enable a growing threat from organized criminal syndicates“ (US 2023, S. 7).

Da klassische Machtmittel im Cyberraum nur begrenzt abschreckend wirken, entwickeln Staaten zunehmend spezifische Cyberabschreckungskonzepte (Krüger 2018, S. 126). Sowohl demokratische als auch autokratische Regime nutzen den Cyberraum gezielt, um externe Gegner und interne Kritiker zu beeinflussen und klassische Machtverteilungen herauszufordern (Zettl-Schabath 2021, S. 65). Ein zentraler historischer Wendepunkt war der Stuxnet-Angriff im Jahr 2010. Der Angriff auf iranische Nuklearanlagen demonstrierte erstmals, dass Cyberwaffen physische Schäden in kritischen Infrastrukturen verursachen können. Stuxnet erfüllte mehrere Schlüsselkriterien (Dunn-Cavelty 2012, S. 148):

- Zielgerichtete digitale Sabotage ohne physische Präsenz,
- reale physische Konsequenzen (Zerstörung von Urananreicherungszentrifugen),
- hohe technologische Komplexität und Ressourcenaufwand, was auf staatliche Akteure hinweist,
- erhebliche Signalwirkung bezüglich der strategischen Bedeutung des Cyberraums.

Die internationale Reaktion auf diese neue Qualität der Bedrohung war eindeutig. Zahlreiche Staaten begannen, spezialisierte Cyberkommandos aufzubauen oder bestehende militärische Strukturen entsprechend zu erweitern. Dunn-Cavelty (2012, S. 148) betont, dass die Schaffung solcher Einheiten direkt aus der Erkenntnis resultierte, dass der Einsatz von Cyberwaffen kaum kontrollierbar sei und neue Formen verdeckter oder offener militärischer Aggression ermögliche: „The reaction is that more and more states are opening up or enhancing ‘cyber commands’, which are military units for cyber war activities, because just the possibility that one or several state actors are behind the computer worm means that this could mark the beginning of the unchecked use of cyber weapons in open or more clandestine military aggressions.“

Zu den führenden Beispielen zählen das United States Cyber Command (USCYBERCOM), das Kommando Cyber- und Informationsraum (KdoCIR) der Bundeswehr sowie die Strategic Support Force (SSF) in China. Während Länder wie Russland die Existenz entsprechender Strukturen nicht offiziell bestätigen, deuten zahlreiche Indizien auf aktive Cybermilitärkapazitäten hin. Dies verweist auf die schwer fassbare, oftmals hybride Natur von Machtprojektionen im Cyberraum.

Die Etablierung dieser Strukturen zeigt, dass der Cyberraum nicht länger als ausschließlich zivile Infrastruktur betrachtet wird. Vielmehr wird er zunehmend als militärisch-strategischer Raum verstanden, in dem klassische Prinzipien der territorialen Souveränität neu interpretiert und operationalisiert werden.

Die fortschreitende Militarisierung des Cyberraums verändert die Bedingungen für alle Akteure im digitalen Raum grundlegend. Staaten erkennen Cyberoperationen als gleichwertige Instrumente der Machtprojektion und investieren systematisch in offensive und defensive Kapazitäten.

Für die Wissenschaft bedeutet diese Entwicklung eine massive strukturelle Herausforderung. Wissenschaftliche Einrichtungen geraten zunehmend in den Fokus staatlicher und nichtstaatlicher Akteure. Die epistemischen Prinzipien der Offenheit, Kooperation und kritischen Reflexivität stehen unter Druck, da sie im neuen Machtfeld des Cyberraums als strategische Verwundbarkeiten erscheinen.

Damit wird deutlich: Der Wandel des Cyberraums zur militärischen Domäne hat nicht nur Auswirkungen auf die globale Sicherheitsarchitektur, sondern stellt auch grundlegende Fragen an die Autonomie, Offenheit und internationale Handlungsfähigkeit der Wissenschaft.

3.6. Grauzonen im Cyberraum

Die globale Vernetzung des Cyberraums bietet Nationalstaaten neue Möglichkeiten der Einflussnahme. Insbesondere der Einsatz von Troll- und Hackerfabriken ermöglicht schwer nachvollziehbare Operationen, die dennoch klaren strategischen Zielen dienen. ”Non-state actors active in cyberspace having the potential to employ digital force or, to various degrees, to be involved in cyber military operations may substantially differ according to size, internal structure, motivational grounds, and relation with the state. Their

size may vary […]. Their organizational structure may be informal, lacking a chain of command, or complex, formal, and stable hierarchical. They may be driven by economic, political, ideological, or religious motivations. Usually, such organisms do not pursue purely military goals, such as power-outcome, typical of state actors or traditional non-state groups that engage in kinetic warfare. Further, they may be directed or stimulated by states or be ercely opposed to any connection with state political entities" (Bussolati 2015, S. 107). Diese Definition veranschaulicht die enorme Bandbreite nichtstaatlicher Akteure im Cyberraum und zeigt, wie schwer eine klare Zurechnung oder Regulierung dieser Aktivitäten fällt.

Diese Aktivitäten verdeutlichen die Herausforderungen, die aus der Anonymität und Grenzlosigkeit des Cyberraums resultieren. Akteure agieren in Grauzonen zwischen Krieg und Frieden, zwischen Eigenmotivation und staatlicher Instrumentalisierung, was nicht nur eine rechtliche Einordnung, sondern Zurechenbarkeit und Verantwortlichkeit zunehmend erschwert.

3.7. Zwischenfazit Macht im Cyberraum

Die Analyse zeigt deutlich: Der Cyberraum hat sich zu einem zentralen Schauplatz geopolitischer Konflikte entwickelt. Für die Wissenschaft ist er eine ambivalente Umwelt – voller neuer Möglichkeiten für Kooperation, aber ebenso voller Risiken: Datenverlust, Manipulation, Spionage (Shaping Europe's Digital Future 2020, S. 19).

Diese geopolitischen Dynamiken im Cyberraum betrifft die Wissenschaft in ihrer Grundstruktur. Als global vernetztes System muss sie sich neuen Bedrohungen und verschiebenden Machtverhältnissen stellen – ohne dabei ihre Prinzipien von Offenheit, Transparenz und Unabhängigkeit zu verlieren. Hochschulen bewegen sich dabei in einem fragmentierten Umfeld, in dem Macht über Infrastruktur, Standards und Informationsflüsse ausgeübt wird. Wissenschaftliche Autonomie gerät unter Druck – durch nationale Sicherheitsinteressen, regulatorische Eingriffe und transnationale Einflussnahme.

Entscheidend wird sein, Macht nicht einfach abzuwehren, sondern sie zu verstehen: Wer kontrolliert Wissen im digitalen Raum? Wer entscheidet, was sichtbar, nutzbar oder schützbar ist? Die Antwort auf diese Fragen bestimmt, wie frei Wissenschaft im Cyberraum agieren kann.

Im folgenden Kapitel wird daher untersucht, wie sich die strukturellen Kopplungen zwischen Wissenschaft und Cyberraum konkret auswirken – auf Prinzipien wie Offenheit, Nachvollziehbarkeit und die Fähigkeit zur kritischen Selbstkorrektur. Der Fokus liegt darauf, wie Wissen selbst zum Objekt strategischer Auseinandersetzung wird – und wie das Wissenschaftssystem darauf reagieren kann.

4. Wissenschaft im Cyberraum

Wie im vorherigen Kapitel gezeigt, ist der Cyberraum längst kein neutrales, grenzenloses Territorium mehr, sondern ein geopolitisch aufgeladener Handlungsraum. Seine Struktur wird maßgeblich von Staaten, transnationalen Akteuren und digitalen Plattformen geprägt. Diese Entwicklung betrifft nicht nur wirtschaftliche und sicherheitspolitische Bereiche, sondern hat auch direkte Auswirkungen auf die Wissenschaft. Diese sieht sich im digitalen Raum neuen Abhängigkeiten und Steuerungsmechanismen ausgesetzt – etwa durch den kontrollierten Zugang zu Daten, algorithmische Sichtbarkeitslogiken oder geopolitisch motivierte Einschränkungen des Wissenstransfers.

Wissenschaft agiert in diesem Kontext nicht isoliert, sondern steht in Wechselwirkung mit den politischen und technologischen Dynamiken des Cyberraums. Dabei geraten zentrale wissenschaftliche Prinzipien wie Offenheit, Kooperation und Wahrheitssuche zunehmend unter Druck.

Das folgende Kapitel untersucht, wie sich diese Machtverschiebungen konkret auf Wissenschaft und Wissensproduktion auswirken – und in welchem Spannungsverhältnis sich wissenschaftliche Autonomie und digitale Souveränität heute befinden.

4.1. Transformation von Wissen im Cyberraum

Die im vorherigen Kapitel beschriebenen Machtstrukturen wirken auf die Wissenschaft, indem sie den Zugang zu Wissen, dessen Verfügbarkeit und Verwertung kontrollieren. Im Cyberraum wird Wissen zunehmend als strategische Ressource betrachtet, die Macht generiert und Machtverhältnisse stabilisiert. Gleichzeitig unterliegt die Wissenschaft selbst den Zwängen dieser Machtdynamiken, da Staaten, Plattformen und Unternehmen entscheiden, welche Forschungsinhalte gefördert, geschützt oder geteilt werden.

Diese Doppelrolle der Wissenschaft als Akteur und Betroffener im Machtgefüge des Cyberraums stellt eine zentrale Herausforderung dar, die sich in der Transformation des wissenschaftlichen Codes widerspiegelt. Während die Wissenschaft traditionell danach strebt, jede Form von wissenschaftlich gewonnener Wahrheit zu kommunizieren, um sie zugänglich zu machen, dem kritischen Widerspruch zu übergeben und auf ihre Wahrheit zu prüfen, stellt sich durch die Machtdurchdringung des Cyberraums immer häufiger die Frage, ob und welches Wissen überhaupt geteilt werden darf – welches Wissen zurückgehalten und geschützt werden muss, um als Machtmittel zu fungieren. Luhmann betont, dass jede Beobachtung Unsicherheit erzeugt, da Beobachten selbst neue Differenzen und Unordnung hervorbringt (Luhmann 1992, S. 521). Im digitalen Raum verschärft sich dieses Problem durch die globale Verflechtung von Kommunikation und Technologien erheblich. Dies führt zu einer Verschiebung von der ursprünglichen Frage: Wie teile ich Wissen am effektivsten? Hin zu: Darf ich Wissen überhaupt teilen, und wenn ja, mit wem? Dies bildet eine epistemische Verschiebung, die die traditionelle Universalitätsnorm der Wissenschaft zunehmend in Frage stellt.

4.2. Der epistemische Wandel: Vom Wahrheits- zum Verwertungswissen

Diese Verschiebung kann anhand der von Scheler differenzierten Wissensformen beschrieben werden (Knoblauch 2014). Die Neugewichtung von Wissen im Cyberraum verdeutlicht eine Re-Kodierung der Wissenschaft entlang von Nützlichkeits- und Machtkriterien. Das in Anlehnung an Scheler als "Leistungs- und Herrschaftswissen" bezeichnete, auf technologischen Innovationen und gesellschaftlicher Nützlichkeit basierende Wissen wird präferiert. Dieses gerät in den politischen Fokus und wird zunehmend unter den Vorbehalt der Verwertbarkeit auch zu Zwecken der technologischen Souveränität, der nationalen Sicherheit und der militärischen Anwendbarkeit gestellt. Gleichzeitig wird das von Scheler sogenannte "Bildungswissen" und "Erlösungswissen" (Henckmann 1998; S. 188), letzteres der freien Neugier und Kontemplation dienend und um seiner selbst willen angestrebt, immer stärker unter Rechtfertigungsdruck gesetzt. Hier verlaufen zunehmend auch die Trennlinien von digitalen Souveränitätszielsetzungen für die Wissenschaft. „Leistungswissen“ soll zukünftig vor allem dazu dienen, Machtmittel exklusiv zu erzeugen. Es soll dadurch nicht mehr frei geteilt werden, während die anderen Wissensformen weiterhin der „reinen Lehre“ der Wissenschaft und ihres Codes global verfügbar sein dürfen, da diese eben nicht geeignet scheinen, Macht zu formen.

4.3. Politische Steuerung und sicherheitspolitische Forschungsprioritäten

Empirisch könnte dies dadurch gefasst werden, indem betrachtet wird, wie politische Zielsetzungen für die Wissenschaft aktuell formuliert werden. Ein Beispiel dafür ist die „Hightech Agenda Bayern“, die explizit einen technologischen Fokus hat und auf Transfer und Verwertung – und damit auf die ökonomische Nutzbarkeit oder Generierung von Machtmitteln – ausgelegt ist. In der Regierungserklärung von Ministerpräsident Söder vom 10. Oktober 2019 heißt es:

„Wir zünden damit den Forschungsturbo, damit Bayern auch noch in 10 Jahren in der Champions League mitspielen kann. Früher gab es ein militärisches Wettrüsten, heute findet ein Wettbewerb um die klügsten Köpfe und um technologische Dominanz statt. Noch sind wir in Deutschland und Bayern spitze. Aber gilt das auch für morgen? Der Wettbewerb um Künstliche Intelligenz hat längst begonnen und wird die Zukunft prägen. Den dürfen wir nicht verlieren. Allein China steckt bis 2030 rund 150 Milliarden Euro in KI. Deutschland will dagegen bis 2025 nur drei Milliarden Euro investieren.“ (Regierungserklärung Markus Söder 2019)

Im geleakten Verhandlungspapier der Arbeitsgruppe 8 der Koalitionsverhandlungen von CDU/CSU und SPD mit Stand 23.03.2025, die mittlerweile weitestgehend vom Koalitionsvertrag bestätigt wurden, finden sich dazu folgende Aussagen:

„Wir starten eine Hightech Agenda für Deutschland unter Einbindung der Länder. Wir wollen dazu in definierten Missionen technologieoffene Innovationsökosysteme und Forschungsfelder organisieren und fördern mit klaren Zielen und Meilensteinen und unter Einbeziehung von universitären, außeruniversitären Akteuren, Industrie und Startups. Neben Förderprogrammen wird der Staat auch als Ankerkunde tätig. Wir priorisieren in einem ersten Schritt die Forschungs- und Innovationsförderung des Bundes auf folgende Schlüsseltechnologien.“ (AG 8, S. 5, Koalitionsvertrag 2025, S.77)

Zu diesen Schlüsseltechnologien werden Künstliche Intelligenz, Quantentechnologien, Mikroelektronik, Biotechnologien, Fusionsforschung sowie Luft- und Raumfahrttechnik genannt – alles zweifelsfrei Forschungsfelder, die sich dem „Leistungswissen“ zuschreiben lassen und deren Begründung sich direkt mit Zielsetzungen technologischer und digitaler

Souveränität verknüpfen lassen. Neu – und deshalb bemerkenswert – ist, dass die „Sicherheits- und Verteidigungsforschung, sowie Dual-Use“ erstmals explizit aufgeführt werden:

„Wir bauen die Friedens- und Konfliktforschung sowie Regionalforschung (z.B. Osteuropa, China, USA) aus und schaffen eine Förderkulisse für Sicherheits- und Verteidigungsforschung einschl. Cybersicherheit und sicherer Infrastrukturen, um Kooperation von Hochschulen und AuF mit Bundeswehr und Unternehmen gezielter zu ermöglichen.“ (ebd. S. 6)

Damit wird konkret auch die Zielsetzung verbunden, die „Resilienz des Wissenschaftssystems“ zu stärken:

„Wir stärken die Forschungssicherheit, entwickeln gemeinsam mit der Allianz der Wissenschaftsorganisationen Leitlinien für den Umgang in sensiblen internationalen Kontexten und verbessern die Beratungsinfrastruktur. Wir bauen die Forschung zu Desinformationsaktivitäten aus und entwickeln ein Kompetenznetzwerk für unabhängige Chinawissenschaften.“ (ebd. S. 8)

An den Zielsetzungen und an der Sprache ist ein Beleg dafür erbracht, wie Wissenschaft und Macht strukturell gekoppelt werden. Gleichzeitig gerät stärker theoriebasierte oder grundlagenorientierte Forschung – insbesondere in den Geistes- und Sozialwissenschaften – unter Legitimationsdruck, auch weil diese nicht im gleichen Umfang durch politische Förderung ausgestattet wird. Sie wird in dem Verhandlungspapier zwar ebenfalls genannt, aber dort mit Themen wie „Erinnerungskultur, politische Bildung und Demokratieforschung, […] jüdischer Gegenwartsforschung und Antisemitismusforschung“ (ebd.) verbunden – zweifellos ebenfalls relevante Themen, die sich jedoch stark an geopolitische oder machtzentrierte Fragestellungen anlehnen oder entsprechenden Legitimierungsdiskursen unterliegen.

4.4. Fragmentierung des digitalen Wissenschaftsraums

Daraus ergibt sich eine Verschiebung des Wahrheitsbegriffs der Wissenschaft hin zu einer stärkeren Ausrichtung auf die gesellschaftliche Verwertbarkeit und den Nutzen ihres Wissens – eine Entwicklung, die bereits Scheler (1924) einer umfangreichen Kritik unterzogen hätte.

Diese neuen Zielsetzungen zeigen deutlich, wie Wissen und Wissenschaft mit nationalen Sicherheitsinteressen verknüpft und damit zunehmend mit dem Code der Macht zweicodiert werden.

Diese Verschiebungen tragen insgesamt zur Veränderung des wissenschaftlichen Codes bei, sodass statt der reinen Suche nach Wahrheit zunehmend die gesellschaftliche und wirtschaftliche Nützlichkeit von Wissen in den Vordergrund rückt. Diese Entwicklungen können als Ausdruck einer wachsenden Instrumentalisierung von Wissen und Wissenschaft im Cyberraum verstanden werden – einer Verschiebung weg von den traditionellen Prinzipien der Wissenschaft hin zu einer stärkeren Ausrichtung auf Geld, Macht und Herrschaft.

Diese Entwicklungen werden durch die Beobachtungen gestützt, dass der Cyberraum von verschiedenen Akteuren und Organisationen wie Unternehmen, Regierungen, Militär und Geheimdiensten vereinnahmt wird, um ihre jeweiligen Macht- und Kontrollinteressen durchzusetzen. So können Fragen der Forschungsagenda, des Datenzugangs, der Datenhoheit, des Datenschutzes, der Cybersicherheit und der digitalen Souveränität insgesamt zum Gegenstand von Diskursen auch für die Wissenschaft werden (Pohle und Thiel, 2020).

Die Dynamik und Fragmentierung des Cyberraums haben tiefgreifende Auswirkungen auf die Prinzipien und Strukturen der Wissenschaft. Der zunehmende Einfluss nationaler Interessen und die Fragmentierung in digitale „Inseln“ führen dazu, dass der globale Austausch von Wissen eingeschränkt wird. Wissenschaft, die traditionell auf Offenheit und Kooperation angewiesen ist, steht in einem Spannungsfeld zwischen internationaler Zusammenarbeit und nationaler Abschottung. Dies ist eine Entwicklung, die nicht ohne Gegenbewegung aus der Wissenschaft vonstatten gehen wird.

4.5. Regulierungsdruck und institutionelle Reaktionen

Einer dieser Diskurse manifestiert sich am „Gesetz zur Förderung der Bundeswehr in Bayern“. Darin geht es u.a. um ein Verbot von Zivilklauseln, die Universitäten sich selbst geben könnten, um sich der rein zivilen Forschung zu verpflichten, sowie um eine Kooperationspflicht von Universitäten mit der Bundeswehr in Fragen der nationalen Sicherheit. Konkret heißt es:

„Die Hochschulen sollen mit Einrichtungen der Bundeswehr zusammenarbeiten. […] Erzielte Forschungsergebnisse dürfen auch für militärische Zwecke der Bundesrepublik Deutschland oder der NATO-Bündnispartner genutzt werden. Eine Beschränkung der Forschung auf zivile Nutzungen (Zivilklausel) ist unzulässig.“ (Auszug Gesetz über die Förderung der Bundeswehr in Bayern)

Der Verband der Bayerischen Universitäten – Universität Bayern e.V. hat sich dazu differenziert positioniert:

„Die bayerischen Universitäten teilen grundsätzlich die Analyse der Staatsregierung in Bezug auf die veränderte globale sicherheitspolitische Bedrohungslage und einen daraus erwachsenen Bedarf zur Steigerung der Verteidigungsfähigkeit auch durch eine kooperative Haltung der Hochschulen zur Bundeswehr. Sie unterstützen das verfassungsmäßige Ziel einer wehrhaften und verteidigungsfähigen Demokratie gegen Bedrohungen von innen und außen.“ (Universität Bayern 2024)

Gleichwohl wird in der Stellungnahme darauf hingewiesen, dass „die Universitäten darauf beharren, dass jegliche Kooperation mit der Bundeswehr die grundgesetzlich verankerte Wissenschaftsfreiheit nicht untergraben darf.“ (ebd.)

Die GEW Bayern hat gegen dieses Gesetz eine Popularklage eingereicht. Sie sieht darin „einen populistischen Akt der Staatsregierung, der die pädagogische Freiheit der Lehrkräfte an den Schulen sowie die Wissenschaftsfreiheit an den Universitäten im bedenklichen Maße einschränkt“, so die GEW-Landesvorsitzende Martina Bergendale.

Besonders deutlich wird diese Problematik in der Frage des Datenzugangs. Nationale Regulierungen und geopolitische Spannungen bestimmen, wer Zugang zu relevanten Daten hat und wie diese genutzt werden dürfen. Dadurch entstehen wissenschaftliche Abhängigkeiten, die nicht nur die Produktion von Wissen, sondern auch die globale Verteilung und Legitimation wissenschaftlicher Erkenntnisse beeinflussen.

Gleichzeitig beschleunigt die hohe Dynamik des Cyberraums den Wettbewerb um wissenschaftliche Innovationen, was zu einer verstärkten Priorisierung von "Leistungswissen" führt, während Bildungs- und Erlösungswissen zunehmend an den Rand gedrängt werden. Diese Entwicklung birgt die Gefahr, dass wissenschaftliche Diskurse stärker fragmentiert werden und globale Herausforderungen, deren Bewältigung einer gemeinsamen Wissensbasis bedarf, weniger effektiv adressiert werden können – siehe Klimawandel.

4.6. Prinzipien der Wissenschaft im Cyberraum

Dies führt uns zu einer tieferen Betrachtung der Kernprinzipien der Wissenschaft, die in diesen Diskursen und Prozessen neu verhandelt werden.

4.7. Offenheit und Zugänglichkeit

Digitale Plattformen und Algorithmen legen fest, welche wissenschaftlichen Inhalte Sichtbarkeit erlangen und welche marginalisiert werden. Was eigentlich dem wissenschaftlichen Diskurs, also der Selbstreferenz der Wissenschaft, obliegt – da nach Luhmanns Beschreibung die Wissenschaft als ein selbstreferentielles System operiert, das durch Kommunikation agiert (Luhmann 1992, S. 122) – wird dadurch teilweise der Selbstreferenz entzogen. Ein Beispiel hierfür sind Algorithmen in allgemeinen, ggf. auch in wissenschaftlichen Suchmaschinen, die bevorzugt hochrangige Journals oder häufig zitierte Artikel anzeigen, wodurch weniger bekannte, aber innovative Arbeiten oft nicht in den Fokus geraten. Algorithmen, egal ob aus Macht- oder Ökonomielogiken entstammend, fungieren als zusätzliche Filter, die nicht nur wissenschaftliche Kommunikation, sondern auch deren gesellschaftliche Relevanz beeinflussen. Open Science-Initiativen versuchen dem entgegenzuwirken, stoßen jedoch auf strukturelle Widerstände, da wissenschaftliche Sichtbarkeit zunehmend von Plattformlogiken geprägt ist.

4.8. Nachvollziehbarkeit – Überprüfbarkeit – Kritikfähigkeit

Dabei ist es nicht mehr der Kritik wissenschaftlicher Rationalität überlassen, was für eine Betrachtung herangezogen wird und was nicht. Dies erzeugt Herausforderungen für Grundprinzipien wie Nachvollziehbarkeit und Überprüfbarkeit von Forschungsarbeiten, da machtbasierte und ökonomische Verwertungslogiken sowie Aufmerksamkeitsökonomien überblenden, was in den Fokus der Wissenschaft gerät. So kann es vorkommen, dass Forschungsarbeiten, die Themen mit hoher öffentlicher oder politischer Aufmerksamkeit behandeln, überproportional Beachtung finden, während beispielsweise Grundlagenforschung, mag sie noch so innovativ und kreativ sein, ins Abseits gerät (Pohle, 2019). „Damit ist nur schwer nachzuvollziehen, welchen Kriterien die notwendigerweise selektive Präsentation des Forschungsstandes folgt, bis hin zu einer möglichen Beeinflussung im Sinne von Anbieterinteressen. Hinzu kommt, dass Forschende eine Vielzahl von Nut-

zungsspuren hinterlassen, die Rückschlüsse über ihr Verhalten im digitalen Raum zulassen (WR 2023, S. 17). Damit wird die Selbststeuerung der Wissenschaft durch rationale Kritikmechanismen sukzessive ausgehöhlt.

4.9. Objektivität und Intersubjektivität

Diese Spuren im Cyberraum erzeugen zunehmend eine individuelle Repräsentanz, die intersubjektiv nicht rekonstruierbar ist, und damit auch nicht mehr objektiv ist. Durch die zunehmende Digitalisierung betrifft dies nicht mehr nur die Recherchearbeit in Form von individualisierten Trefferlisten in Suchmaschinen, sondern auch die eigentliche wissenschaftliche Produktionsarbeit. Wenn z. B. generative KI-Systeme, die ohnehin auf Wahrscheinlichkeiten beruhen, bei gleichartigen Prompts an Nutzer angepasste und individuell zugeschnittene Ergebnisse liefern, weil diese von ihnen „lernen“, wird dies zu einer weiteren Herausforderung. Beispielsweise könnten generative KI-Systeme einem Forscher, der sich auf sozialwissenschaftliche Aspekte konzentriert, andere Ergebnisse liefern als einem Ingenieur, obwohl beide dieselbe Fragestellung eingeben. Dabei ist es aktuell nicht ausgeschlossen, dass in wissenschaftlichen Prozessen ggf. auch „Lerneffekte“ von Prompts, die mit der Forschungsarbeit nichts zu tun haben ebenfalls mit einbezogen werden. So kann ein KI-System gestern dabei geholfen haben ein Kuchenbackrezept zu erstellen und wird morgen ggf. Lerneffekte aus diesen Prompts dazu nutzen eine wissenschaftliche Arbeit zu schreiben. Dann sieht diese ggf. auch so aus wie ein Backrezept. Die individualisierte Wissensproduktion durch KI-Systeme verschärft die Tendenz zur epistemischen Fragmentierung und tangiert reihenweise wissenschaftliche Prinzipien wie Originalität, Validität, Integrität, Reliabilität.

Diese Arbeit selbst ist ein hochtechnisiertes Unterfangen, das mit dem Einsatz digitaler Technologien beginnt, etwa der Internetsuche in einschlägigen wissenschaftlichen Katalogen, und bei der Unterstützung von KI-Anwendungen wie ChatGPT oder Jenni.ai als sokratischer Diskussionspartner, Datenanalyst, Feedbackgeber, Schreibassistent usw. mündet. Diese Sachverhalte erzeugen große Herausforderungen an eine intersubjektive Überprüfbarkeit aber auch die Validität und Reliabilität von wissenschaftlicher Arbeit an sich. Diese Herausforderungen gilt es auszuhalten und zu reflektieren, solange diese von der Haltung getragen werden, dass Wissenschaft immer kritischer Widerspruch ist – und dass dieser Widerspruch unweigerlich bei sich selbst beginnen muss.

4.10. Unabhängigkeit und Freiheit

Im Ergebnis werden sowohl Wissensrezeption und Wissensproduktion durch die globalen Dynamiken des Cyberraums stark beeinflusst. Es reicht nicht mehr aus, einen guten wissenschaftlichen Artikel zu verfassen und zu publizieren, um diesen der wissenschaftlichen Kritik zu stellen. Zunehmend kommt es darauf an, wo dieser publiziert wird, um gleich von Beginn an den optimalen Aufmerksamkeitsvektor zu finden. Vielleicht kommt es bereits zu sehr darauf an, denn die Wissenschaft trägt interessanterweise selbst durch umfassende Rankingsysteme von „Journals“ dazu bei, diese Entwicklung zu intensivieren. So könnten „Scientifc Journal Rankings (SJRs)“ unter diesem Aspekt auch kritisch betrachtet werden. Eigentlich als Qualitätssicherungsinstrumente beschrieben sind diese in vollem Umfang reputationswirksam. Eine Gegenentwicklung der Wissenschaft im Cyberraum, die an ihre ursprünglichen Logiken heranführt, wie die „Open Science“-Bewegung kommt bisher nur langsam voran. Diese hat derzeit noch Akzeptanzprobleme, die daraus resultieren, dass es an einer Incentivierung für Wissenschaftlerinnen und Wissenschaftler fehlt, ihre Daten und Methoden offen zu teilen, sowie aus der Sorge um den Verlust von Reputation. So ist die Wissenschaft selbst nicht davor geschützt, in eigens induzierte „Lock-In“-Effekte zu geraten und damit Unabhängigkeit und Freiheit einzubüßen.

Diese und andere Phänomene des Cyberraums wirken sich auf die Prinzipien der Wissenschaft grundlegend aus und führen dazu, dass institutionelle Machtstrukturen statt wissenschaftlicher Kriterien darüber entscheiden, welche Erkenntnisse dominant werden und damit zur Wirklichkeitskonstruktion herangezogen werden. Nur eine bewusste Förderung offener Wissenschaftspraktiken könnte langfristig eine epistemische Resilienz gegenüber den neuen Machtstrukturen gewährleisten.

4.11. Ethik und Verantwortung

Die Dynamiken des Cyberraums haben tiefgreifende Auswirkungen auf die ethischen Grundlagen der Wissenschaft. Die Verbreitung von Fake News, Desinformation, Propaganda und die Bildung sogenannter "Bubbles" – segregierter Echokammern – zeigen, wie algorithmisch gesteuerte Wissensvermittlung die sozialen Dynamiken im digitalen Raum verändert. Diese Entwicklungen verdeutlichen, dass Wissenschaft nicht mehr isoliert von den Kommunikationsprozessen des Cyberraums betrachtet werden kann.

Wie Bechthold-Hengelhaupt (2024) ausführt, fungieren Desinformation und Fake News als systematische Kommunikationsstörungen, die die Anschlussfähigkeit von Diskursen untergraben und die Fähigkeit zur rationalen Auseinandersetzung in öffentlichen Räumen schwächen. Übertragen auf den Cyberraum bedeutet dies: Wissenschaft ist zunehmend von Mechanismen betroffen, die nicht mehr auf Wahrheitssuche und Diskursausgleich, sondern auf Aufmerksamkeitserzeugung, Polarisierung und strategische Einflussnahme abzielen. Der Cyberraum wird dadurch selbst zum Akteur in der Transformation von Wissenschaftskommunikation und Wissensverbreitung.

Besonders brisant ist, dass die Techniken algorithmischer Verstärkung durch künstliche Intelligenz diese Prozesse weiter beschleunigen könnten. Welche Wirkung die zunehmende Verschmelzung von Cyberraum und KI auf die Wissenschaft entfalten wird, ist derzeit noch nicht absehbar und bleibt ein drängendes Forschungsdesiderat.

Für die Wissenschaft erwächst daraus eine neue ethische Verantwortung: Sie muss sich nicht nur mit der Generierung und Verbreitung von Wissen auseinandersetzen, sondern auch aktiv die Bedingungen der eigenen Kommunikation im Cyberraum reflektieren und gestalten. Dies betrifft sowohl die Art und Weise, wie wissenschaftliche Erkenntnisse verbreitet werden, als auch die ethische Pflicht, auf Verzerrungen, Manipulation und Desinformation aufmerksam zu machen und diesen aktiv entgegenzuwirken.

Die strukturellen Veränderungen im Cyberraum fordern damit eine Neubestimmung der wissenschaftlichen Ethik, die über klassische Konzepte wie Plagiarismus oder Datenmanipulation hinausgeht und die gesamte soziale Infrastruktur der Wissenschaftskommunikation in den Blick nimmt. Wissenschaftliche Ethik im Cyberraum muss sich also von einer normativen auf eine proaktiv-strukturelle Dimension erweitern.

4.12. Grauzonen der Wissenschaft

Die Dynamik des Cyberraums erzeugt nicht nur neue sicherheitspolitische Risiken, sondern schafft auch neue Grauzonen für die Wissenschaft. Dual-Use-Forschung, die sowohl für zivile als auch für militärische Zwecke nutzbar ist, wird zunehmend zum Gegenstand sicherheitspolitischer Aufmerksamkeit. Politische Zielsetzungen, wie sie sich im Koalitionsvertrag 2025 abzeichnen, fokussieren verstärkt auf die sicherheitsrelevante Forschung und fördern gezielt Kooperationen zwischen Hochschulen, außeruniversitären Forschungseinrichtungen und der Bundeswehr.

Diese Entwicklungen werfen fundamentale Fragen nach der Offenheit und Autonomie der Wissenschaft auf. Es stellt sich die grundsätzliche Frage, inwieweit militärische oder sicherheitsstaatliche Akteure – gestützt durch politische Regelwerke – Zugang zu sensiblen Forschungsprojekten erhalten und ob dies dazu führen könnte, dass wissenschaftliche Erkenntnisse zunehmend der zivilen Öffentlichkeit entzogen und ausschließlich in militärischen Kontexten verwertet werden.

Dies birgt die Gefahr einer schleichenden Versicherheitlichung oder Militarisierung der Wissenschaft, bei der bestimmte Forschungsfelder unter Verschluss geraten, während gleichzeitig die Transparenz, Nachvollziehbarkeit und kritische Anschlussfähigkeit wissenschaftlicher Arbeit massiv eingeschränkt werden. Besonders im Bereich der Cybersicherheit, der Künstlichen Intelligenz und der Biotechnologie allgemein der Technologieforschung entstehen neue Risiken, die bisherige Prinzipien wie Offenheit, Nachvollziehbarkeit und Intersubjektivität zunehmend unter Spannung setzen.

Die Deutsche Forschungsgemeinschaft (DFG) und die Nationale Akademie der Wissenschaften Leopoldina (2022) betonen in diesem Zusammenhang, dass „der Schutz sicherheitsrelevanter Forschung nicht zu einer Einschränkung der Wissenschaftsfreiheit führen darf“ und fordern „transparente Entscheidungsprozesse und die Sicherstellung wissenschaftlicher Diskurse auch bei sicherheitsrelevanten Themen“ (DFG/Leopoldina 2022).

Die Wissenschaft sieht sich damit einem Spannungsfeld gegenübergestellt, in dem sie ihre Prinzipien der Offenheit, der freien Kommunikation von Erkenntnissen und der internationalen Kooperation aktiv verteidigen muss, ohne dabei berechtigte Sicherheitsinteressen vollständig auszublenden. Es bedarf eines reflektierten Umgangs mit der Dualität von Chancen und Risiken, um die wissenschaftliche Integrität und die gesellschaftliche Anschlussfähigkeit von Forschung auch in sicherheitsrelevanten Kontexten zu gewährleisten.

4.13. Synthese: Macht und Wissen im Cyberraum

Der Cyberraum wirkt nicht nur als geopolitisches Spannungsfeld, sondern transformiert die epistemischen Grundlagen der Wissensproduktion. Die im Cyberraum wirkenden Machtstrukturen beeinflussen, welche Forschung priorisiert wird, wer Zugang zu Wissen erhält und wie Wissensproduktion und -kommunikation gestaltet werden. Gleichzeitig schafft die Wissenschaft selbst durch ihre Erkenntnisse neue Machtpotenziale, die von Staaten, transnationalen Akteuren und digitalen Plattformen strategisch genutzt werden.

In diesem Spannungsfeld zeigt sich die doppelte Dynamik des Cyberraums: Einerseits beschleunigt er die Wissensproduktion und bietet neue Möglichkeiten für globale Kooperation, andererseits führt seine Fragmentierung zu einer zunehmenden Abschottung und Instrumentalisierung wissenschaftlicher Inhalte. Besonders die Priorisierung von "Leistungswissen" gegenüber Bildungs- und Erlösungswissen verstärkt diese Tendenz. Wissenschaftliche Systeme stehen vor der Herausforderung, ihre Autonomie und universellen Prinzipien in einem digitalen Umfeld zu bewahren, das von Machtinteressen geprägt ist.

Ein zentraler Begriff, der diese Dynamik bündelt, ist die digitale Souveränität. Sie dient als diskursiver Container, der die Schnittstellen zwischen Macht und Wissen, zwischen Offenheit und Kontrolle sowie zwischen Universalität und Partikularität umfasst. Digitale Souveränität reflektiert die Bestrebungen, nicht nur politische und wirtschaftliche Kontrolle über den Cyberraum zu gewinnen, sondern auch dessen soziale und epistemologische Dimension zu gestalten.

Im nächsten Kapitel wird untersucht, wie der Diskurs um digitale Souveränität die Schnittstelle von Macht und Wissen prägt und welche Auswirkungen dies auf die Wissenschaft als gesellschaftliches Teilsystem hat. Besondere Aufmerksamkeit gilt dabei der Frage, wie wissenschaftliche Systeme ihre digitale Resilienz stärken können, um sich an neue Bedrohungen und technologische Entwicklungen anzupassen, ohne ihre Autonomie zu verlieren.

Digitale Souveränität beschreibt dabei nicht nur den Versuch, technologische Abhängigkeiten zu reduzieren, sondern auch die Aushandlungsprozesse zwischen politischer Kontrolle und wissenschaftlicher Autonomie. Sie dient als theoretischer Rahmen, um die Herausforderungen der Machtstrukturen im Cyberraum für die Wissenschaft zu analysieren und Lösungsansätze für eine souveräne Gestaltung des Cyberraums zu entwickeln. Digitale Souveränität bedeutet somit nicht nur technologische Kontrolle, sondern ebenso epistemische Selbstbestimmung im digitalen Zeitalter.

5. Digitale Souveränität

Wissenschaftliche Systeme operieren zunehmend in einem digitalen Raum, dessen Struktur nicht allein durch technologische Infrastrukturen bestimmt wird, sondern in wachsendem Maße durch geopolitische Machtinteressen, ökonomische Abhängigkeiten und normative Auseinandersetzungen um Kontrolle und Offenheit. In diesem komplexen Umfeld wird die Autonomie wissenschaftlicher Institutionen zu einer Verhandlungsgröße: Digitale Souveränität beschreibt die Fähigkeit, in einer hochvernetzten Welt handlungsfähig zu bleiben – durch Zugriff auf und Kontrolle über Daten, Infrastrukturen und Kommunikationsprozesse – ohne dabei die Prinzipien wissenschaftlicher Offenheit und internationaler Kooperation zu gefährden.

Diese Entwicklung konfrontiert das Wissenschaftssystem mit einer doppelten Herausforderung: Einerseits gilt es, die Resilienz gegenüber technologischen und politischen Fremdeinflüssen zu stärken. Andererseits darf dabei die Anschlussfähigkeit an globale wissenschaftliche Diskurse nicht gefährdet werden. Digitale Souveränität erweist sich in diesem Spannungsfeld als analytischer Schlüsselbegriff. Sie benennt nicht nur neue Abhängigkeiten, sondern erlaubt es auch, die strukturellen Voraussetzungen wissenschaftlicher Selbstbestimmung im digitalen Zeitalter kritisch zu reflektieren.

Ziel dieses Kapitels ist es daher, digitale Souveränität nicht nur als technische oder sicherheitspolitische Maßnahme zu behandeln, sondern als komplexen, normativ aufgeladenen Diskurs zu analysieren. Dieser Diskurs ordnet Fragen nach Kontrolle, Autonomie, Vertrauen und globaler Vernetzung neu – und eröffnet wissenschaftlichen Institutionen Handlungsoptionen, um ihre epistemische und infrastrukturelle Unabhängigkeit strategisch zu gestalten.

5.1. Digitale Souveränität als Konzept

Digitale Souveränität ist in den letzten Jahren zu einem Schlüsselbegriff politischer und wissenschaftlicher Diskurse avanciert. Sie beschreibt die Fähigkeit von Staaten, Organisationen und Individuen, digitale Technologien im Einklang mit eigenen Zielen, Werten und Interessen zu gestalten und zu nutzen – bei gleichzeitiger Kontrolle über digitale Infrastrukturen, Datenflüsse und Kommunikationsräume. Anders als klassische Vorstellungen staatlicher Souveränität, die auf territoriale Herrschaft und rechtliche Letztverantwor-

tung fokussieren, verweist digitale Souveränität auf eine komplexe Mischung aus technologischer Steuerungsfähigkeit, normativer Autonomie und gesellschaftlicher Selbstbestimmung im digitalen Raum.

Der Erfolg des Begriffs liegt – wie Thiel (2024) herausstellt – gerade in seiner semantischen Offenheit, die es erlaubt, unterschiedliche politische, ökonomische und zivilgesellschaftliche Anliegen unter einem diskursiven Dach zu bündeln. Diese Ambivalenz wird nicht als Schwäche, sondern als analytische Produktivität verstanden: Der Begriff fungiert als Resonanzfläche für normative Erwartungen, politische Zielsetzungen und infrastrukturelle Strategien, die sich zwischen Kontrollanspruch und Offenheitsgebot bewegen.

Im Wissenschaftskontext erhält digitale Souveränität eine zusätzliche epistemische Dimension: Sie verweist auf die Fähigkeit wissenschaftlicher Institutionen, ihre Autonomie in einer zunehmend digital verfassten Welt zu behaupten – gegen technologische Fremdbestimmung, aber auch gegen neue Formen asymmetrischer Wissensordnung, wie sie etwa durch Plattformdominanz oder algorithmische Steuerung entstehen.

Wie Greef (2023) formuliert, fungiert digitale Souveränität dabei nicht als einheitliches Konzept, sondern als „Mantel“, unter dem unterschiedlichste Diskurse – von Datensouveränität über Cybersicherheit bis hin zu demokratischer Teilhabe – verhandelt werden. Entscheidend ist, dass dieser Mantel nicht zur homogenen Strategie wird, sondern Differenz, Konflikt und Kontextualisierung zulässt.

Diese Perspektive macht deutlich, dass digitale Souveränität nicht als technokratische Zielmarke, sondern als **diskursives Spannungsfeld** zu verstehen ist: Es ordnet zentrale Fragen neu – nach Autonomie, Abhängigkeit, Vertrauen und Steuerung im digitalen Zeitalter – und eröffnet damit neue Möglichkeitsräume für wissenschaftspolitische Selbstvergewisserung und strategische Orientierung.

5.2. Definitionen und Abgrenzungen

Die Diskussion um digitale Souveränität ist von einer bemerkenswerten konzeptuellen Heterogenität geprägt. In der wissenschaftlichen Literatur existiert kein einheitliches Begriffsverständnis, sondern ein Spektrum von Deutungen, die je nach disziplinärem Zugang, politischer Stoßrichtung und normativem Fokus stark variieren. Dieses Kapitel ordnet zent-

rale Positionen ein und arbeitet heraus, wie unterschiedliche Autorinnen und Autoren digitale Souveränität interpretieren – und inwiefern sich diese Perspektiven ergänzen oder widersprechen.

Goldacker (2017) versteht digitale Souveränität vor allem als **Fähigkeit zur sicheren, selbstbestimmten Teilhabe** an digitalen Prozessen – durch Individuen, Organisationen und Institutionen. Sie betont die technische, infrastrukturelle und gestalterische Handlungskompetenz von Akteuren im digitalen Raum. Im Zentrum steht die praktische Umsetzbarkeit: Digitale Souveränität umfasst sowohl Datenschutz und Datennutzung als auch Kompetenzen zur Auswahl, Gestaltung und Kontrolle digitaler Technologien. Damit vertritt Goldacker eine operationalisierbare, anwendungsnahe Sichtweise, die sich deutlich von makropolitischen oder diskurstheoretischen Zugängen unterscheidet.

Pohle und Thiel (2020) rücken den Begriff in ein gänzlich anderes Licht. Für sie ist digitale Souveränität keine normative Zielvorstellung, sondern eine **diskursive Praxis**: ein politischer Kampfbegriff, mit dem Staaten und politische Akteure versuchen, Autorität im digitalen Raum symbolisch und institutionell zurückzugewinnen. Sie kritisieren technokratische Verkürzungen des Begriffs und weisen darauf hin, dass der Souveränitätsbegriff zunehmend dazu verwendet wird, staatliche Eingriffe im Namen der Selbstbestimmung zu legitimieren – ohne demokratische Rechenschaftspflicht systematisch mitzudenken.

Bendiek und Stürzer (2022) entwickeln dagegen ein strategisch-europapolitisches Verständnis. Für sie ist digitale Souveränität ein **Handlungsprinzip europäischer Re-Souveränisierung**, das darauf zielt, geopolitische Abhängigkeiten zu reduzieren und regulatorische Handlungsfähigkeit zu sichern. Im Zentrum stehen Maßnahmen wie der Aufbau eigener Infrastrukturen (z. B. Gaia-X) und die Externalisierung europäischer Normen über den sogenannten „Brüssel-Effekt“. Damit rahmen sie digitale Souveränität als instrumentelle Ressource in einem globalen Technologie- und Ordnungswettbewerb.

Celeste (2021) hingegen betont die **ambivalente Semantik** des Begriffs. Er sieht digitale Souveränität als normativ aufgeladenes Konzept, das einerseits notwendig sei, um europäische Werte und Grundrechte im digitalen Raum zu schützen, andererseits aber schnell in **„digitalen Souveränismus“** umschlagen könne. Gemeint ist die Gefahr, dass unter dem Vorwand der Selbstbestimmung nationalistische Abgrenzungsstrategien oder technologische Protektionismen vorangetrieben werden, die die Offenheit des Internets untergraben. Celeste plädiert daher für eine balanceorientierte, kooperative Interpretation, die zwischen technischer Selbstbehauptung und globaler Interdependenz vermittelt.

Thiel (2024) alleine verfolgt eine **diskurstheoretische Metareflexion**: Er beschreibt digitale Souveränität als ein semantisch offenes und gerade deshalb wirkmächtiges Konzept. Die produktive Ambiguität erlaubt es, sehr unterschiedliche politische, wirtschaftliche und gesellschaftliche Anliegen unter einem gemeinsamen Begriff zu versammeln. Diese Perspektive unterscheidet sich von funktionalen oder normativen Zugängen insofern, als Thiel weniger fragt, was digitale Souveränität ist, als wozu sie im politischen Diskurs dient. Er zeigt, wie sich der Begriff als symbolische Projektionsfläche im Spannungsfeld von Autonomie, Kontrolle und Innovation etabliert hat.

Die Gegenüberstellung dieser Positionen zeigt: Digitale Souveränität ist ein polyvalenter Schlüsselbegriff, dessen Bedeutung je nach disziplinärem Zugriff stark variiert. Während Goldacker den Begriff an individueller und organisatorischer Handlungskompetenz festmacht, verhandeln Pohle & Thiel ihn als politisch aufgeladene Deutungspraxis. Bendiek & Stürzer nutzen ihn strategisch im geopolitischen Kontext, während Celeste auf seine normative Ambivalenz hinweist. Thiel wiederum analysiert seine diskursive Anschlussfähigkeit quer zu diesen Positionen. Das wiederum ist hat eine hohe Anschlussfähigkeit an die Methodik wieder Arbeit, die sich an ebendiese Spannungsverhältnisse als heuristischer Rahmen heranwagt.

Für die wissenschaftliche Systemperspektive ergibt sich daraus eine doppelte Herausforderung: Sie muss digitale Souveränität einerseits als strategisches Gestaltungsprinzip ernst nehmen, das infrastrukturelle und regulatorische Resilienz stärkt. Andererseits darf sie die normativen Risiken und diskursiven Vereinnahmungen des Begriffs nicht übersehen. Gerade die Widersprüchlichkeit und Kontextabhängigkeit digitaler Souveränität macht sie zu einem zentralen Analyseinstrument für die Neuverhandlung wissenschaftlicher Autonomie im digitalen Zeitalter.

5.3. Dimensionen der digitalen Souveränität

Die vorangegangenen Abschnitte haben gezeigt, dass digitale Souveränität ein vielschichtiger und normativ umkämpfter Begriff ist. Um diese Komplexität analytisch handhabbar zu machen, bietet sich eine strukturierende Gliederung entlang zentraler Wirkungsbereiche an. Die folgenden Dimensionen fassen die in der Forschungsliteratur prominent diskutierten Handlungsfelder zusammen und bilden zugleich ein Raster, um die

spezifischen Herausforderungen und Gestaltungsaufgaben im Wissenschaftssystem systematisch zu analysieren. Diese Differenzierung ergänzt das in Kapitel 9 entwickelte Spannungsmodell, das zentrale Konfliktlinien sichtbar macht.

5.4. Politische Dimension

Diese Dimension umfasst die Fähigkeit politischer Institutionen, digitale Räume normativ zu gestalten, strategisch zu sichern und regulatorisch zu kontrollieren. Für das Wissenschaftssystem ist sie insofern relevant, als Hochschulen und Forschungseinrichtungen zunehmend in politische Strategien wie Cybersicherheitsgesetze oder europäische Digitalprogramme eingebunden sind. Sie verlangt, politische Rahmung nicht nur zu akzeptieren, sondern aktiv mitzugestalten – ohne wissenschaftliche Autonomie aufzugeben.

5.5. Ökonomische Dimension

Digitale Souveränität umfasst auch die Frage, inwieweit Forschungsinstitutionen in ihrer digitalen Infrastruktur von marktbeherrschenden Plattformanbietern abhängig sind – etwa bei Cloud-Diensten, KI-Infrastrukturen oder Publikationssystemen. Eine ökonomische Perspektive betont hier die strategische Notwendigkeit, europäisch getragene Alternativen zu stärken, um Wertschöpfung, Datenschutz und wissenschaftliche Innovationsfähigkeit nachhaltig zu sichern. Dabei ist Souveränität nicht allein als technische oder organisatorische Kontrolle zu verstehen, sondern auch als Fähigkeit zur informierten und freien Entscheidung – unabhängig von einseitigem ökonomischem oder funktionalem Druck. Erst wenn wissenschaftliche Einrichtungen zwischen realen Optionen wählen können, ohne in Abhängigkeit von proprietären Standards, Lizenzmodellen oder Förderlogiken zu geraten, lässt sich von echter digitaler Souveränität sprechen.

5.6. Technologische Dimension

Technologische Souveränität bezeichnet die Fähigkeit, zentrale digitale Technologien – etwa im Bereich Datenanalyse, KI oder Sicherheitssysteme – zu verstehen, selbst zu betreiben oder mitzugestalten. Hochschulen müssen hier nicht nur als Nutzer auftreten, sondern aktiv an der Entwicklung souveräner technologischer Lösungen mitwirken. Besonders die Kontrolle über Forschungsdaten, Datenflüsse und IT-Systeme ist für die funktionale Resilienz zentral.

5.7. Wissenschaftliche Dimension

Die wissenschaftliche Dimension digitaler Souveränität beschreibt die Fähigkeit des Wissenschaftssystems, seine epistemische Autonomie im digitalen Raum gegenüber externen technologischen, politischen und ökonomischen Einflussfaktoren zu wahren. Sie verknüpft die Interaktionen der Wissenschaft mit anderen gesellschaftlichen Systemlogiken und zielt auf die Sicherung unabhängiger Forschung und Lehre. Dies umfasst die souveräne Auswahl und Gestaltung digitaler Werkzeuge, die Wahrung von Publikationsfreiheit sowie die Absicherung grundlegender wissenschaftlicher Prinzipien – wie Transparenz, Nachvollziehbarkeit und Replizierbarkeit, wie sie in Kapitel 4 herausgearbeitet wurden. Digitale Souveränität wird damit zur konstitutiven Voraussetzung für wissenschaftliche Selbstbestimmung, Innovationsfähigkeit und internationale Anschlussfähigkeit.

5.8. Fazit: Digital Souveränität

Die Analyse der digitalen Souveränität zeigt, dass es sich nicht um ein einheitlich definierbares oder abschließend operationalisierbares Konzept handelt, sondern um einen vielschichtigen Orientierungsrahmen, der politische, technologische, gesellschaftliche und epistemische Aspekte miteinander verknüpft. In dieser begrifflichen Offenheit liegt zugleich analytische Stärke: Der Begriff erlaubt es, die Verflechtung von Macht, Infrastruktur und Autonomie im digitalen Raum sichtbar zu machen – insbesondere dort, wo wissenschaftliche Institutionen zugleich als Akteure, Objekte und Vermittler auftreten.

Im Zentrum steht dabei kein statischer Zustand souveräner Kontrolle, sondern ein dynamischer Aushandlungsprozess entlang unterschiedlicher Felder: von der Regulierung internationaler Infrastrukturen über die Entwicklung sicherer Technologien bis zur ethischen Normierung digitaler Praktiken. Die in Kapitel 5.3 eingeführten fünf Dimensionen markieren zentrale Handlungs- und Beobachtungsfelder, in denen diese Prozesse konkret sichtbar werden.

Für das Wissenschaftssystem ergibt sich daraus eine doppelte Herausforderung: Einerseits gilt es, Autonomie und Offenheit gegenüber wachsenden externen Einflüssen zu bewahren; andererseits besteht die Aufgabe darin, aktiv zur Gestaltung jener Technologien und Infrastrukturen beizutragen, die genau diese Autonomie absichern sollen.

Digitale Souveränität erscheint in diesem Kontext nicht als feststehender Zustand, sondern als konflikthaftes Aushandlungsfeld, in dem politische, ökonomische und technologische Dynamiken ineinandergreifen. Die Analyse der folgenden Kapitel nimmt diese Konfliktlagen genauer in den Blick – insbesondere das Spannungsverhältnis zwischen Souveränität und struktureller Abhängigkeit, das sich in strategischen Texten und institutionellen Praktiken des Wissenschaftssystems verdichtet.

6. Cybersicherheit

Cybersicherheit ist untrennbar mit der Ambivalenz des Cyberraums verbunden: Jede technologische Innovation bringt nicht nur neue Möglichkeiten, sondern auch potenzielle Risiken mit sich. Diese doppelte Natur erfordert einen integrativen Sicherheitsansatz, der technologische, gesellschaftliche und politische Dimensionen gleichermaßen berücksichtigt. Der Cyberraum als dynamische, soziotechnische Domäne ist geprägt von globalen Macht- und Wissensstrukturen – Cybersicherheit agiert in diesem Kontext als dynamisches Regulierungsprinzip, das nicht nur technische Bedrohungen adressiert, sondern auch institutionelle Autonomie schützt und asymmetrische Machtverhältnisse reflektiert.

Diese doppelte Funktion wird insbesondere auf institutioneller Ebene sichtbar: Cybersicherheit adressiert technische Angriffsvektoren und sichert gleichzeitig epistemische Infrastrukturen, die für die wissenschaftliche Wissensproduktion essenziell sind. Zugleich schützt sie die Autonomie von Institutionen vor geopolitischen Einflussnahmen (Schünemann 2020). Wie Lange und Bötticher (2015) hervorheben, sind Nutzen und Schaden technischer Innovationen oft zwei Seiten derselben Medaille – ein Befund, der die Notwendigkeit eines ganzheitlichen Sicherheitsansatzes unterstreicht. Die ambivalente Natur der künstlichen Intelligenz ist derzeit Gegenstand zahlreicher Forschungsarbeiten, die hier nicht vertieft behandelt werden können. Dennoch stützen sie die These, dass technologische Innovationen nicht nur Risiken bergen, sondern potenziell die grundlegenden Operationsmuster des Cyberraums verändern.

Die Anfänge der Cybersicherheit – auch bezeichnet als IT-Sicherheit, Netz- oder Informationssicherheit – waren vorrangig informationstechnischer Natur. In dieser Tradition wurde Cybersicherheit primär als infrastrukturelle Aufgabe verstanden. Nur unter dieser technischen Vorbedingung lässt sich Cybersicherheit als Abwesenheit oder Vermeidung von Gefahr im Sinne eines Schutzes von Hardware, Software und Daten definieren, bezogen

auf „vereinbarte Verfügbarkeit, Integrität, Vertraulichkeit, Zurechenbarkeit und Rechtsverbindlichkeit“ (Witt 2006, S. 65). Diese Definition orientiert sich stark an der Vorstellung zuverlässiger technischer Systeme und entspricht eher dem Konzept der „Cyber-Safety“, analog zu den Sicherheitskonzeptionen von Bonß (2015, S. 35).

Der konstruktivistischen Sichtweise des Cyberraums als diskursiv geprägtem Kommunikationsraum wird diese rein technische Lesart jedoch nicht gerecht. Cybersicherheit ist weit mehr als technischer Schutz: Sie muss als sozio-technisches Konzept verstanden werden, das die Interdependenz technologischer, sozialer und politischer Dimensionen umfasst. Lange und Bötticher (2015) definieren Cybersicherheit entsprechend als „die Gesamtheit aller strategischen, organisatorischen und technischen Maßnahmen, die darauf abzielen, Informations- und Kommunikationssysteme sowie die darüber verarbeiteten Informationen zu schützen“ (S. 12).

Diese Entwicklung spiegelt sich auch im Verständnis des Cyberraums wider. Schünemann (2020) zeigt, dass Cybersicherheit sich zu einem eigenständigen Politikfeld entwickelt hat, das zunehmend von geopolitischen Spannungen durchzogen ist. Hochschulen stehen dabei in einer doppelten Rolle: Sie sind einerseits Ziel von Angriffen, andererseits zentrale Akteure bei der Entwicklung innovativer Sicherheitsstrategien.

Möller (2023) betont die integrative Natur der Cybersicherheit, die technische, organisatorische und soziale Dimensionen miteinander verknüpft. Er fasst zusammen: „Effective cybersecurity management requires an integrated approach, balancing technical, organizational, and human factors“ (Möller 2023, S. 50). Damit wird deutlich: Cybersicherheit ist ein systemisch eingebettetes Konzept, das die Dynamik des Cyberraums aufgreift und auf die spezifischen Anforderungen von Institutionen wie Hochschulen reagieren muss.

6.1. Dimensionen der Cybersicherheit

Um die Komplexität der Cybersicherheit zu erfassen, lassen sich verschiedene Dimensionen identifizieren, die spezifische Aspekte der Sicherheitsanforderungen beleuchten. Diese Dimensionen reflektieren die systemische Einbettung von Cybersicherheit in technologische, regulatorische, organisatorische und soziale Kontexte.

- **Technologische Dimension:** „Der Schutz von IT-Infrastrukturen bildet die Grundlage jeder Cybersicherheitsstrategie. Maßnahmen wie Firewalls, Verschlüsselung und sichere Softwareentwicklung minimieren technische Angriffsflächen.“ (Beispiel: Sicherheitsprotokolle wie TLS oder Intrusion-Detection-Systeme.)
- **Regulatorische Dimension:** „Datenschutzrichtlinien wie die DSGVO schaffen rechtliche Rahmenbedingungen, die den Schutz individueller Rechte und die Sicherheit digitaler Prozesse gewährleisten.“ (Beispiel: Bußgelder bei Verstößen gegen die DSGVO.)
- **Organisatorische Dimension:** „Institutionen müssen Sicherheitsrichtlinien entwickeln, die durch Schulungen und eine etablierte Sicherheitskultur getragen werden.“ (Beispiel: Einführung von Notfallplänen bei Datenlecks.)
- **Soziale Dimension:** Die Sensibilisierung der Gesellschaft für Cybergefahren ist ein zentraler Bestandteil der Cybersicherheitsstrategie. Nur durch ein Bewusstsein für Risiken können technologische Maßnahmen effektiv umgesetzt werden. (Beispiel: Kampagnen zur Aufklärung über Phishing.)

Zudem wird von Lange & Bötticher (2015) hervorgehoben, dass Cybersicherheit als kontinuierlicher Prozess verstanden werden muss, der flexibel auf neue Bedrohungen und technologische Entwicklungen reagiert.

6.2. Herausforderungen und Spannungsfelder

Die vielschichtigen Herausforderungen der Cybersicherheit spiegeln die Dynamik des Cyberraums wider. Sie betreffen sowohl die technologische als auch die institutionelle Ebene und erfordern interdisziplinäre Ansätze, um flexibel auf neue Bedrohungen zu reagieren.

- **Zunehmende Komplexität:** Mit der wachsenden Zahl vernetzter Systeme steigt auch die Anzahl potenzieller Angriffspunkte. Phishing-Angriffe nutzen etwa soziale Schwachstellen aus, während Zero-Day-Exploits technische Lücken ausnutzen.
- **Technologische Abhängigkeiten:** Die Abhängigkeit von proprietären Technologien globaler Anbieter schränkt die strategische Autonomie ein. Beispiele hierfür sind Cloud-Dienste von Amazon oder Microsoft.
- **Geopolitische Spannungen:** Internationale Machtkämpfe um Basistechnologien wie Halbleiter oder KI erschweren die Zusammenarbeit und beeinträchtigen die Cybersicherheitsstrategien von Institutionen.

- **Knappe Ressourcen:** Öffentlich finanzierte Institutionen stehen vor der Herausforderung, mit begrenzten Mitteln wirksame Sicherheitsstrategien zu entwickeln.

Wie bereits im Kontext der digitalen Souveränität gezeigt, verschärfen Fragmentierungsprozesse diese Spannungsfelder. Schünemann (2020) argumentiert, dass diese Herausforderungen nur durch einen interdisziplinären Ansatz bewältigt werden können, der technologische Innovation mit regulatorischer und gesellschaftlicher Reflexion verbindet. Für Hochschulen ist dies besonders relevant, da sie als Zentren des Wissensaustauschs und der Innovation sowohl Ziel von Angriffen als auch Akteure in der Entwicklung von Sicherheitsstrategien sind.

6.3. Relevanz für Hochschulen

Angriffe auf sensible Forschungsdaten, wie etwa der Angriff auf die Universität Maastricht im Jahr 2019, verdeutlichen die Gefahren für Hochschulen. Neben finanziellen Schäden bedrohen solche Angriffe auch die Integrität und Vertraulichkeit von Forschungsprojekten.

- **Angriffe auf sensible Forschungsdaten:** Forschungsergebnisse stellen einen hohen Wert dar und sind daher ein attraktives Ziel.
- **Balance zwischen Offenheit und Sicherheit:** Hochschulen müssen den freien Wissensaustausch gewährleisten, ohne dabei die Sicherheit zu vernachlässigen.
- **Kompetenzentwicklung:** Als Ausbildungsstätten tragen Hochschulen Verantwortung für die Entwicklung von Fachkräften im Bereich Cybersicherheit.

6.4. Fazit: Cybersicherheit

Cybersicherheit ist weit mehr als technischer Schutz – sie bildet das Fundament digitaler Souveränität. Für Hochschulen heißt das: Sie müssen nicht nur ihre Systeme absichern, sondern auch aktiv an der Gestaltung resilienter digitaler Infrastrukturen mitwirken. Die Balance zwischen Offenheit und Sicherheit bildet dabei ein zentrales Spannungsfeld.

Im Verständnis dieser Arbeit ist Cybersicherheit dabei nicht isoliert zu betrachten, sondern als funktionale Gegenebene zum zuvor beschriebenen Cyberraum: Beide Begriffe folgen einem soziotechnischen Verständnis. Während der Cyberraum als diskursiv strukturierte,

globale Domäne konzipiert wurde, erscheint Cybersicherheit als dynamisches Regulierungsfeld innerhalb dieses Raums – geprägt von technischen, politischen und epistemischen Aushandlungen.

Damit wird deutlich: Cybersicherheit ist nicht bloß Reaktion auf Gefahren, sondern Teil der strukturellen Formierung des digitalen Raums selbst. Sie konstituiert nicht nur Schutzmechanismen, sondern rahmt auch, welche Formen von Offenheit im digitalen Raum überhaupt möglich, legitim und sicher gelten. Besonders für Hochschulen ergibt sich eine doppelte Verantwortung: Einerseits müssen sie sich gegen gezielte Angriffe schützen, andererseits spielen sie eine zentrale Rolle in der Entwicklung innovativer Sicherheitsstrategien und der Ausbildung zukünftiger Fachkräfte. Nur durch einen integrativen Ansatz, der die Ambivalenz technologischer Innovationen berücksichtigt, kann Cybersicherheit nachhaltig gewährleistet werden.

7. Bedrohungslage der Wissenschaft im Cyberraum

Damit die Arbeit nicht nur die theoretische, sondern auch praktische Relevanz aufspannt, soll aufgezeigt werden, dass Cyberangriffe auf wissenschaftliche Einrichtungen längst kein theoretisches Szenario mehr, sondern dokumentierte Realität – quer durch alle Hochschulsysteme global. Aktuelle Studien aus Deutschland, dem DACH-Raum, dem Vereinigten Königreich und den USA zeigen eindeutig, dass Hochschulen zu den am stärksten betroffenen Sektoren im digitalen Raum gehören. Sie werden nicht nur aus kriminellen Motiven angegriffen, sondern zunehmend auch gezielt von staatlich unterstützten Akteuren ausspioniert.

Laut dem **Hochschulbarometer 2024** halten 97,3 % der deutschen Hochschulleitungen Cyberangriffe für eine große oder eher große Bedrohung (S. 35). Die **ZKI Top-Trends-Umfrage 2024** für den DACH-Raum bestätigt diese Einschätzung aus operativer Sicht: IT-Leitungen bewerten die Bedrohungslage mit einem durchschnittlichen Risiko-Score von 7,9 von 10, in Österreich sogar mit 8,4 (ZKI 2024, S. 15). Auch international ist das Bild eindeutig. Im der **Cyber Security Breaches Survey 2024 aus UK** wird aufgezeigt, dass 97 % der britischen Hochschulen von mindestens einem Sicherheitsvorfall im letzten Jahr betroffen zu sein; 59 % erlebten dadurch konkrete betriebliche Beeinträchtigungen (DSIT 2024, S. 9).

In den USA zeigt sich ein ähnliches Bild: Nur 17 % der CTOs amerikanischer Hochschulen sind laut **IHE CTO/CIO Survey 2024** „zuversichtlich“, ihre Institution gegen Cyberangriffe wirksam schützen zu können (IHE 2024, S. 25), niemand ist „sehr zuversichtlich“. Die große Mehrheit berichtet von nur moderatem Sicherheitsgefühl bzw. Schutzfähigkeit.

Hochschulen sind zu strategischen Zielen im globalen Wettbewerb um Wissen, Daten und technologische Souveränität geworden – nicht nur für Kriminelle, sondern zunehmend auch für staatlich gesteuerte Akteure.

7.1. Systematische Analyse aktueller Cyberangriffe (2024/2025)

Die unabhängige Plattform Kon Briefing dokumentiert Angriffe auf Hochschulen weltweit systematisch und kontinuierlich. Aufgrund der offenen Kommunikation der betroffenen Einrichtungen ist gemäß der Plattform die Dunkelziffer bei Großangriffen vermutlich geringer als in anderen gesellschaftlichen Teilsystem wie der Wirtschaft. Die Stärken der Plattform liegen in ihrer einfachen Bedienbarkeit, Übersichtlichkeit und Aktualität. Bereits im Zeitraum Januar bis März 2025 wurden neun größere und damit erfolgreiche Angriffe auf wissenschaftliche Einrichtungen registriert.

Eine Auswahl aktueller Vorfälle verdeutlicht die Breite und Schwere der Bedrohungslage:

Monat /Jahr	Einrichtung	Land	Auswirkungen	Quelle
März 2025	Université de Rennes	Frankreich	Einstellung des Lehrbetriebs nach Ransomware-Angriff	ouest-france.fr
Januar 2025	Universität der Bundeswehr München	Deutschland	Lahmlegung zentraler IT-Systeme, Sicherheitsrelevanz	heise.de
Januar 2025	Fachhochschule Nordwestschweiz (FHNW)	Schweiz	Unautorisierte Zugriffe, Gefahr von Datenabfluss	fhnw.ch
Januar 2025	Eindhoven University of Technology	Niederlande	Schließung des Netzwerks, Ausfall von Lehrveranstaltungen	tue.nl
Dezember 2024	Valdosta State University	USA	Ausfälle bei Unterricht und Computerlaboren	wtxl.com
Juli 2024	Frankfurt University of Applied Sciences	Deutschland	Lahmlegung von Verwaltung und Kommunikation	heise.de
März 2024	Universität Potsdam	Deutschland	Langfristige Folgeschäden historisch gewachsener IT-Strukturen	forschung-und-lehre.de
Februar 2024	Hochschule Kempten	Deutschland	Angriff auf zentrale Server, Beeinträchtigung des Lehrbetriebs	hs-kempten.de

Abbildung 5: Auszug aktueller Cyberangriffe 2024/2025 auf Hochschulen, Darstellung aus Daten von Kon Briefing, https://konbriefing.com/de-topics/cyber-angriffe-universitaeten.html

Diese Tabelle zeigt deutlich, dass Cyberangriffe auf Hochschulen längst keine Ausnahmeerscheinung mehr sind, sondern sich als regelmäßige Bedrohungslage etabliert haben.

7.2. Gründe für die Attraktivität wissenschaftlicher Einrichtungen als Ziel

Hochschulen und Forschungseinrichtungen gelten im digitalen Raum als besonders attraktive Angriffsziele. Diese Attraktivität ergibt sich aus einer Kombination struktureller, technischer und strategischer Faktoren, die in internationalen Studien wiederholt hervorgehoben werden.

Zum einen verfügen Hochschulen über eine Vielzahl hochwertiger und sensibler Daten – von personenbezogenen Informationen über wissenschaftliche Rohdaten bis hin zu geistigem Eigentum mit technologischem oder wirtschaftlichem Potenzial. In der britischen Lageeinschätzung von Universities UK, Jisc, UCISA und dem National Cyber Security Centre (NCSC) heißt es wörtlich: „Because of the work we do and the data we hold, our sector remains an attractive target for all kinds of cyber criminals, [Universities] operate large, complex and diverse digital infrastructures, with significant storage and processing capabilities.“ (Universities UK et al. 2023, S. 2).

Hinzu kommt die institutionelle Offenheit wissenschaftlicher Einrichtungen. Die notwendige internationale Vernetzung und die Dezentralität vieler IT-Entscheidungen erhöhen die Angriffsflächen. Das Hochschulbarometer 2024 hebt hervor, dass diese Offenheit zwar zur DNA der Wissenschaft gehört, zugleich aber „die Angriffsexponiertheit erhöht“ (Hochschulbarometer 2024, S. 36).

Neben klassischen Cyberkriminellen werden Hochschulen zunehmend auch Ziel **staatlich unterstützter Gruppen**, die sich gezielt für Forschungsdaten aus sicherheitsrelevanten Bereichen wie Biotechnologie oder KI interessieren (Universities UK et al. 2023, S. 5; ZKI 2024, S. 22). Die Motivation reicht dabei von finanzieller Erpressung über Wissensdiebstahl und Wissenschaftsspionage bis hin zur geopolitischen Einflussnahme.

Hochschulen sind damit keine zufälligen Opfer – sie sind **systematisch verwundbare, gleichzeitig strategisch wertvolle Einrichtungen**, die sowohl aus krimineller als auch aus politischer Motivation heraus angegriffen werden.

7.3. Typische Angriffsvektoren

Für die Analyse typischer Angriffsvektoren auf Hochschulen bildet die britische "Cyber Security Breaches Survey 2024 – Education Institutions Annex" die empirische Hauptquelle. Sie bietet die aktuell umfassendste quantifizierte Darstellung realer Vorfallsmuster im Hochschulbereich. Zur Kontextualisierung und Validierung werden ergänzend Daten aus der ZKI Top-Trends-Umfrage 2024 (DACH-Raum), der IHE CTO/CIO Survey 2024 (USA), dem strategischen Lagebericht von Universities UK et al. (2023) sowie dem BSI-Lagebericht 2024 herangezogen. Die sechs häufigsten und länderübergreifend als besonders kritisch identifizierten Angriffsvektoren sind: Phishing, Ransomware, Credential Theft, unautorisierter Zugriff, Angriffe über Drittanbieter und Advanced Persistent Threats (APT).

1. Phishing

Phishing ist der mit Abstand häufigste Einstiegsvektor für Cyberangriffe. Laut der britischen Umfrage berichten 100 % der Hochschulen von entsprechenden Vorfällen (DSIT 2024, S. 11). Auch in der IHE CTO/CIO Survey 2024 wird Phishing als permanent präsente Gefahr thematisiert, was in 88 % der US-Hochschulen zur verpflichtenden Einführung von MFA führte (IHE 2024, S. 25). In der ZKI-Umfrage 2024 wird Phishing mehrfach in Freitextfeldern als gängiger Angriffsweg genannt (ZKI 2024, S. 17).

2. Ransomware

77 % der britischen Hochschulen berichten von Schadsoftware-Vorfällen (DSIT 2024, S. 11). Ransomware wird im Bericht von Universities UK et al. (2023, S. 6) anhand konkreter Auswirkungen beschrieben: "Some universities hit by ransomware over the last few years have lost control of their entire digital estates, with systems broken and data lost." In den USA wird sie in der IHE-Umfrage als eines der schwerwiegendsten Bedrohungsszenarien bewertet (IHE 2024, S. 25), in Deutschland besteht laut ZKI-Report ein strukturelles Risiko durch mangelhafte Backup-Infrastrukturen (ZKI 2024, S. 20–21). Der BSI-Lagebericht 2024 hebt hervor, dass auch Hochschulen verstärkt von Ransomware-Angriffen betroffen sind, da Angreifer gezielt den "Weg des geringsten Widerstands" wählen (BSI 2024, S. 10).

3. Credential Theft

Der Diebstahl von Zugangsdaten, häufig durch Phishing oder Brute-Force-Angriffe, wird international als Schlüsselproblem wahrgenommen. Die britische DSIT-Studie meldet regelmäßige Vorfälle kompromittierter Accounts (DSIT 2024, S. 12). In der IHE-Umfrage

wird das Identitätsmanagement als besonders verwundbar eingeschätzt, insbesondere durch Phishing-basierte Credential Harvesting-Angriffe (IHE 2024, S. 13). Die ZKI-Umfrage nennt fehlende MFA und intransparente Rollenzuweisungen als typische Schwachstellen im DACH-Raum (ZKI 2024, S. 18). Der BSI-Lagebericht verweist auf die wachsende Rolle sogenannter "Access Broker", die Zugangsdaten gezielt verkaufen (BSI 2024, S. 19).

4. Unautorisierter Zugriff

Laut der britischen Umfrage kam es in **27 % der Hochschulen** zu Zugriffen durch Mitarbeitende und in **20 %** zu externen Zugriffen auf Systeme ohne Berechtigung (DSIT 2024, S. 12). Die ZKI nennt als Ursache überalterte Nutzerkonten und unzureichende Protokollierung (ZKI 2024, S. 19). Die US-Ergebnisse betonen die Notwendigkeit verbesserter Identity-Governance (IHE 2024, S. 13).

5. Angriffe über Drittanbieter / Supply Chain

Universities UK et al. warnen vor simultanen Angriffen auf Institutionen, die identische Plattformen oder Dienstleister verwenden (2023, S. 6). Die britische Studie nennt explizit **Cloud-Plattformen und IT-Dienstleister** als Risikozonen. Die IHE CTO/CIO Survey 2024 meldet fehlende Richtlinien für die Absicherung externer Tools in **mehr als 50 % der US-Hochschulen** (IHE 2024, S. 20). Die ZKI-Umfrage verweist auf Migrationsstrategien in Richtung Open Source aus Sicherheitsgründen (ZKI 2024, S. 20). Auch der BSI-Bericht 2024 dokumentiert konkrete Vorfälle staatlicher Angreifer über kompromittierte Cloud-Signaturen (z. B. Microsoft) (BSI 2024, S. 10).

6. Advanced Persistent Threats (APT)

Zunehmend geraten Hochschulen in das Visier staatlich unterstützter, hochspezialisierter Angreifergruppen, sogenannter Advanced Persistent Threats (APT). Laut Universities UK et al. (2023, S. 5) richten sich diese Angriffe gezielt gegen Forschungseinrichtungen, insbesondere in den Bereichen Verteidigung, Biotechnologie und Künstliche Intelligenz. In der ZKI-Umfrage wird auf entsprechende Gefährdungen durch forschungsnahe Spionage hingewiesen (ZKI 2024, S. 22). Auch in der IHE CTO/CIO Survey 2024 zeigen CTOs erhebliche Unsicherheiten im Umgang mit systemweiten Datenabflüssen im Kontext generativer KI und Cloud-Nutzung (IHE 2024, S. 20–21). Der BSI-Lagebericht 2024 bestätigt die Aktivität von **22 APT-Gruppen allein in Deutschland** und verweist auf Forschungseinrichtungen als indirekt betroffene Ziele (BSI 2024, S. 22).

Diese sechs Angriffsformen zeichnen sich nicht nur durch ihre Häufigkeit aus, sondern durch ihre internationale Relevanz, Schadenswirkung und geopolitische Dimension. Sie betreffen Kernelemente der digitalen Hochschulinfrastruktur und unterstreichen die Notwendigkeit strategischer Sicherheitskonzepte im Wissenschaftsmanagement.

7.4. Fazit: Wissenschaft als strategisches Angriffsziel

Die Angriffe auf Hochschulen und Forschungseinrichtungen sind Ausdruck einer tieferliegenden Dynamik: Wissenschaft ist längst nicht mehr nur Träger von Erkenntnis, sondern wird zunehmend als geopolitischer Faktor wahrgenommen. Wissen ist Macht – und diese Macht wird im Cyberraum umkämpft.

Die dargestellte Bedrohungslage macht unmissverständlich deutlich: Hochschulen benötigen nicht nur moderne technische Schutzvorkehrungen, sondern eine strategische Neuausrichtung im Umgang mit Cybersicherheit. Nur so kann Wissenschaft auch in einer digitalisierten Welt frei, offen und souverän agieren. Daraus ergibt sich die Notwendigkeit, resiliente Strukturen und umfassende Schutzstrategien zu entwickeln, um die wissenschaftliche Handlungsfähigkeit im Cyberraum nachhaltig zu sichern.

7.5. Theoretisches Gesamtfazit: Wissenschaft im Cyberraum – Macht, Wissen, digitale Souveränität und Cybersicherheit

Die vorangegangene Analyse hat gezeigt, dass der Cyberraum längst nicht mehr als neutrales Medium der Kommunikation begriffen werden kann, sondern als ein von Machtstrukturen durchzogener, dynamischer Raum, der tief in die Prinzipien, Praktiken und Selbstverständnisse der Wissenschaft eingreift. Die Wechselwirkungen zwischen geopolitischen Interessen, technologischen Dynamiken und wissenschaftlichen Strukturen haben eine neue Konstellation entstehen lassen, in der Wissen selbst zunehmend zur Ressource und Waffe in globalen Machtkämpfen wird.

Zentrale Spannungsfelder prägen diese Entwicklung: Offenheit, traditionell ein Grundprinzip der Wissenschaft, gerät unter Druck, während nationale Interessen und sicherheitspolitische Erwägungen zu einer stärkeren Fragmentierung und strategischen Kontrolle von Wissen führen. Autonomie und Unabhängigkeit der Wissenschaft stehen in einem ständi-

gen Spannungsverhältnis zur Notwendigkeit von Cybersicherheit und Resilienz gegenüber externen Bedrohungen. Die Wissenschaft sieht sich gezwungen, ihre Position zwischen systemischer Geschlossenheit und globaler Kopplung neu zu definieren.

Im Zentrum dieser Neuverhandlung steht der Begriff der digitalen Souveränität. Er bündelt die Bestrebungen, technologische, politische und epistemische Selbstbestimmung im digitalen Raum zu sichern. Für wissenschaftliche Institutionen bedeutet digitale Souveränität nicht nur den Schutz vor Bedrohungen, sondern auch die aktive Gestaltung der Bedingungen, unter denen Wissen produziert, verbreitet und geschützt wird. Dabei ist digitale Souveränität kein statischer Zustand, sondern ein dynamischer Prozess, der kontinuierlich im Wechselspiel von technologischem Fortschritt, politischem Handeln und gesellschaftlicher Reflexion ausgehandelt werden muss.

Die Wissenschaft ist damit nicht nur Objekt der Transformation, sondern zugleich Subjekt ihrer eigenen Verteidigung und Neugestaltung. Sie muss neue Formen epistemischer Resilienz entwickeln, die eine Balance zwischen Offenheit und Schutz, zwischen internationaler Kooperation und strategischer Autonomie ermöglichen. Wissenschaftliche Ethik muss sich erweitern, indem sie die strukturellen Bedingungen wissenschaftlicher Kommunikation im Cyberraum kritisch reflektiert und neue normative Grundlagen für wissenschaftliches Handeln unter Bedingungen digitaler Fragmentierung schafft.

Die theoretische Analyse hat schließlich verdeutlicht, dass die grundlegende Funktionslogik der Wissenschaft im digitalen Zeitalter selbst einem tiefgreifenden Wandel unterliegt: Wahrheitssuche bleibt ein zentrales Ziel, wird aber zunehmend ergänzt (und teilweise überlagert) durch die Notwendigkeit, wissenschaftliche Ergebnisse als strategische Ressourcen im Kontext globaler Machtkämpfe zu positionieren. Offenheit, Intersubjektivität und Kritikfähigkeit müssen unter veränderten Bedingungen verteidigt und weiterentwickelt werden.

Diese Erkenntnisse bilden den theoretischen Ausgangspunkt für die anschließende empirische Untersuchung: Wie gestalten wissenschaftliche Institutionen angesichts dieser neuen Konstellationen konkret ihre digitale Resilienz? Welche Strategien, Strukturen und Kulturen entwickeln sie, um die Balance zwischen Autonomie, Sicherheit und Offenheit zu wahren? Das folgende empirische Kapitel knüpft an diese Fragen an und untersucht, wie die in der Theorie beschriebenen Dynamiken praktisch adressiert werden.

8. Methodischer Teil

8.1. Forschungsdesign

Diese Arbeit verfolgt einen mehrstufigen, qualitativ fundierten Forschungsansatz, der auf einer deduktiven Entwicklung von Kategorien basiert, die aus einem interdisziplinär aufgebauten Theorierahmen abgeleitet werden. Zentrale Spannungsverhältnisse der Wissenschaft im Cyberraum, wie beispielsweise das Spannungsverhältnis zwischen Offenheit und Sicherheit, werden aus Theorien der Systemtheorie, Cybersicherheitsforschung, internationalen Beziehungen, Diskurstheorie und Souveränitätsforschung extrahiert. Diese Spannungen dienen als analytisches Raster, das auf drei Untersuchungsebenen angewendet wird: Makro (Strategien und Diskurse), Meso (Governance- und Institutionenebene) und Mikro (konkrete Umsetzung).

Das Ziel ist eine theoriegeleitete, mehrdimensionale Analyse, die qualitative Inhaltsanalyse mit diskurstheoretischer Perspektive, Policy-Analyse und Fallstudienforschung kombiniert. Diese Methodenkombination zielt darauf ab, empirische Ergebnisse auf die theoretisch abgeleiteten Spannungsdimensionen zurückzuführen und dabei die relevanten Dynamiken zu identifizieren, die auf verschiedenen Ebenen des politischen und institutionellen Kontextes operieren.

8.2. Analytisches Rahmenmodell: Spannungsverhältnisse als Heuristik

Das deduktiv entwickelte Spannungsverhältnismodell fungiert als zentrale Heuristik, die theoriegeleitet Kategorien bereitstellt, anhand derer empirische Materialien strukturiert analysiert werden. Die Spannungsverhältnisse, die in Kapitel 9 systematisch entwickelt wurden, bilden sowohl Strukturierungs- als auch Interpretationsrahmen. Methodisch wird das Raster flexibel angewendet: Es bietet klare Analyseachsen und lässt dennoch Raum für emergente Phänomene. Die Kategorien fungieren somit als ein strukturierendes Werkzeug, das gleichzeitig als heuristische Hilfe dient.

Ein methodisches Spannungsfeld besteht in der potenziellen Zirkularität des deduktiven Vorgehens, da die Spannungsverhältnisse sowohl theoretisch abgeleitet als auch als Strukturkategorie der Analyse verwendet werden. Um diesem Risiko zu begegnen, wurde

die Offenheit für emergente Kategorien im Analyseprozess gewahrt. Narrative Verschiebungen, die außerhalb des vorgegebenen Rahmens liegen, werden diskurstheoretisch erfasst und insbesondere auf der Mikroebene dokumentiert.

8.3. Methoden je Analyseebene

Makroebene: Diskursive Rahmung von Wissenschaft und Sicherheit

Fokus: Internationale und nationale Strategiepapiere (Deutschland, UK, USA)
Methode: Qualitative Inhaltsanalyse (Mayring, Kuckartz) kombiniert mit diskurstheoretischen Perspektiven (Wissenssoziologische Diskursanalyse, Keller)
Ziel: Identifikation dominanter Deutungsmuster und diskursiver Rahmungen
Begründung: Mayring (2019) liefert eine fundierte Strukturierung qualitativer Kategorien, die der systematischen Analyse von Textmaterial dient. Keller (2011) erweitert diese Strukturierung durch eine machtanalytische Perspektive: Diskurse werden als regelgeleitete symbolische Ordnungspraktiken verstanden, die nicht nur Wirklichkeit abbilden, sondern diese auch konstituieren. Die Wissenssoziologische Diskursanalyse ergänzt die strukturierende Codierung um eine interpretative Analyseebene, die insbesondere für Fragen epistemischer Macht und strategischer Wissenspolitik im Kontext digitaler Souveränität zentral ist.

Mesoebene: Wissenschaftspolitische und organisatorische Strategien

Fokus: Wissenschaftsspezifische Strategieempfehlungen und institutionelle Rahmenbedingungen (z. B. EDUCAUSE Report, Wissenschaftsrat)
Methode: Policy-Analyse nach dem akteurzentrierten Institutionalismus (Scharpf)
Ziel: Analyse von Steuerungslogiken, Rollenkonflikten und institutioneller Zielambivalenz im Spannungsfeld von Offenheit und Sicherheit
Begründung: Scharpfs (1997) Ansatz erlaubt es, Akteurskonstellationen und institutionelle Interessen systematisch zu erfassen und im Kontext strategischer Steuerung zu interpretieren.

Mikroebene: Institutionelle Praxis und Umsetzungslogiken

Fokus: Fallstudie Bayern (Cybersicherheitsstrukturen an Hochschulen, HISP-Programm)
Methode: Fallstudienanalyse nach Yin (2018), analytische Generalisierung
Ziel: Untersuchung der praktischen Ausgestaltung und Umsetzung institutioneller Cybersicherheitsmaßnahmen auf Hochschulebene

Begründung: Yin ermöglicht eine theoriegesteuerte Vertiefung eines spezifischen Falls, ohne eine statistische Verallgemeinerung anzustreben. Dies stellt sicher, dass tiefgehende Einblicke in die spezifische Umsetzung der Cybersicherheitsstrategien in einem realen institutionellen Kontext gewonnen werden.

8.4. Rolle der KI im Analyseprozess

KI-gestützte Tools wurden als strukturierende Unterstützung im Vorfeld der Analyse eingesetzt, etwa zur Quellensichtung, Texterfassung und Begriffssegmentierung. Die qualitative Codierung selbst erfolgte manuell und theoriegeleitet. Große Sprachmodelle wie Chat-GPT wurden auf ihre methodische Tragfähigkeit geprüft, jedoch nicht zur interpretativen Kategorienbildung verwendet.

ChatGPT wurde als sokratischer Dialogpartner eingesetzt, um Annahmen, Thesen und Schlussfolgerungen in einem iterativen Prozess kritisch zu hinterfragen. Darüber hinaus wurde es verwendet, um wissenschaftliche Gütekriterien zu evaluieren und Feedback zur Weiterentwicklung der Arbeit zu generieren. Für Fleißarbeiten wie Rechtschreibkorrektur, Grammatikkorrektur, Formulierungshilfen sowie die Sortierung und Standardisierung von Verzeichnissen war der Einsatz ebenfalls von Nutzen.

8.5. Validität und Reflexivität

Die Validität der Analyse wird durch mehrere Ebenen gesichert:

- **Transparenz:** Alle Kategorienentwicklungen, Codierentscheidungen und Materialauswahlen sind dokumentiert und reflektiert.
- **Intersubjektivität:** Theoretisch fundierte Kategorien wurden pilotcodiert. Aufgrund des Rahmens einer Einzelarbeit war jedoch keine Intercoder-Reliabilitätsprüfung möglich. Stattdessen wurde auf Intracoder-Reliabilitätsprüfung zurückgegriffen.
- **Triangulation:** Kombination von Strategiedokumenten, Survey-Daten und Fallstudienquellen zur Validierung der Ergebnisse.
- **Analytische Generalisierung:** Die Fallstudie Bayern zielt nicht auf Repräsentativität ab, sondern auf eine theoriekonforme Vertiefung der Untersuchung.

8.6. Methodische Grenzen

Die parallele Anwendung von Inhalts- und Diskursanalyse birgt potenzielle Spannungen, die methodisch durch die funktionale Trennung von strukturierender Analyse und kontextueller Rahmung abgefedert wurden. Eine wesentliche methodische Limitation ergibt sich aus dem Fehlen empirischer Primärdatenerhebungen auf der Mikroebene, insbesondere Interviews und quantitative Erhebungen. Diese Lücke schränkt die Tiefe der Analyse von hochschulinternen Entscheidungsprozessen und individuellen Wahrnehmungen der Cybersicherheitsstrategien ein. Eine ergänzende qualitative Erhebung durch Experteninterviews wäre in zukünftiger Forschung wünschenswert, um die Perspektiven der beteiligten Akteure stärker zu integrieren.

Die Fallstudie ist exemplarisch gewählt und erlaubt keine statistische Verallgemeinerung. Die Surveys ergänzen die qualitative Perspektive um punktuelle quantitative Indikatoren. Die methodische Offenheit des Heuristikmodells erfordert eine bewusste Reflexion über mögliche kategoriale Unschärfen und die Tiefe der Interpretation.

Zusammenfassung der Methodik: Der methodische Ansatz dieser Arbeit basiert auf der analytischen Generalisierung: Das Ziel ist nicht, repräsentative Aussagen zu treffen, sondern theoriegeleitet zentrale Spannungsdynamiken sichtbar zu machen. Der methodische Rahmen bleibt flexibel genug, um neue empirische Phänomene zu integrieren, ohne die theoretische Kohärenz zu gefährden. Die Kombination von qualitativer Inhaltsanalyse, diskurstheoretischer Perspektive und Fallstudienforschung ermöglicht eine tiefgehende und mehrdimensionale Analyse, die sich der Komplexität der Forschungsfrage annähert und emergente Themen aufgreift.

9. Heuristischer Rahmen

Die empirische Analyse dieser Arbeit folgt einer deduktiven, theoriegeleiteten Struktur, die auf der Entwicklung zentraler Spannungsverhältnisse beruht. Diese Spannungsverhältnisse repräsentieren keine festen Kategorien, sondern dienen als heuristische Beobachtungsachsen, entlang derer zentrale Konfliktlinien und Handlungsspannungen im Schnittfeld von Wissenschaft, Politik und Technik im Cyberraum sichtbar gemacht werden.

Anstelle durchgehend mit klassischen Codierschemata wird in dieser Arbeit mit Spannungsverhältnissen als dynamischen Analyseeinheiten gearbeitet. Diese bilden nicht statische Zustände ab, sondern erfassen strukturelle Dilemmata, Erwartungsparadoxien und normative Zielkonflikte, die sich in strategischen Dokumenten, politischen Steuerungsversuchen und organisationalen Umsetzungskontexten materialisieren.

Jedes Spannungsverhältnis wird durch zwei gegensätzliche analytische Pole charakterisiert, etwa Offenheit vs. Sicherheit oder Kooperation vs. Fragmentierung. Diese Pole machen systematische Spannungen beobachtbar, ohne sie vorzeitig aufzulösen. Die Spannungsverhältnisse ermöglichen damit eine differenzierte, theoriegestützte Analyse von Diskursen, Strategien, Praktiken und Deutungsmustern, ohne einer mechanischen Codierlogik zu folgen.

Theoretisch verankert sich dieser Ansatz in einem interdisziplinären Fundament: Die funktionale Differenzierung nach Luhmann (1992, 1997), diskurstheoretische Rahmungen im Sinne der Wissenssoziologischen Diskursanalyse (Keller 2011), Konzepte aus den internationalen Beziehungen (Nye, Drezner), Souveränitäts- und Cybersicherheitsforschung (Dunn Cavelty, Rattray) bieten gemeinsam die Basis für die Ableitung und Anwendung dieser Heuristik.

In den folgenden Abschnitten werden fünf zentrale Spannungsverhältnisse vorgestellt, jeweils mit theoretischer Verortung, Relevanz für die empirische Analyse sowie beispielhaften Ausprägungen in nationalen Strategiedokumenten. Sie bilden das Raster, entlang dessen die anschließenden Kapitel strukturiert sind.

9.1. Spannungsverhältnisse als analytische Kategorien

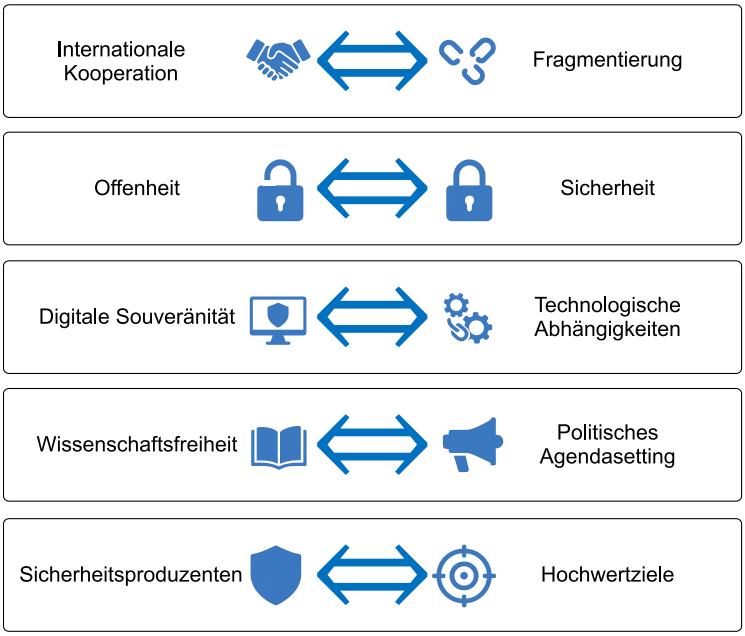

Abbildung 6: Darstellung der Spannungsverhältnisse als heuristischer Rahmen, eigene Darstellung

Die in dieser Arbeit entwickelten fünf Spannungsverhältnisse bilden die zentrale heuristische Struktur für die qualitative Analyse. Sie sind nicht als abstrakte Gegensatzpaare zu verstehen, sondern als analytisch produktive Spannungsachsen, entlang derer sich die widersprüchlichen Anforderungen an Hochschulen im digitalen Raum beobachten und deuten lassen.

Die Spannungsverhältnisse wurden aus dem interdisziplinären Theoriegerüst der Arbeit deduktiv hergeleitet und bilden zentrale Konfliktlinien in der Wechselwirkung von globaler Wissenschaft, politischer Steuerung, technologischer Abhängigkeit und sicherheitspolitischer Transformation ab.

Diese Spannungsverhältnisse werden in den folgenden Abschnitten jeweils einzeln entfaltet: mit theoretischer Fundierung, empirisch relevanten Kontexten und exemplarischen Bezügen aus nationalen Strategiedokumenten. In Kapitel 10 ff. wird das Spannungsraster dann systematisch auf die verschiedenen Analyseebenen (Makro, Meso, Mikro) angewendet.

Internationale Kooperation vs. Fragmentierung

Problemformulierung:

Internationale Zusammenarbeit ist ein grundlegendes Prinzip wissenschaftlicher Entwicklung. Mobilität, grenzüberschreitende Forschung und offene Wissensinfrastrukturen bilden die Basis globaler Wissensproduktion. Doch angesichts geopolitischer Spannungen, wachsender Sicherheitsbedenken und digitaler Kontrollpolitiken gerät dieses Kooperationsmodell zunehmend unter Druck. Die globale Wissenschaftslandschaft wird durch neue

Exportkontrollen, politische Blockbildungen und technologiepolitische Entkopplungstendenzen fragmentiert. Für Hochschulen entsteht dadurch ein struktureller Zielkonflikt: Sie sollen internationale Partnerschaften pflegen, zugleich aber regulatorische und sicherheitspolitische Anforderungen einhalten, die diese Kooperationen erschweren oder delegitimieren.

Theoretische Fundierung:

- **Systemtheorie (Luhmann 1992):**
  Wissenschaft operiert als funktional differenziertes System mit globaler Reichweite. Internationale Kooperation ist für seine Anschlussfähigkeit zentral. Politische und sicherheitsbezogene Regulierungen können als Störung dieser funktionalen Logik gelesen werden, da sie systemfremde Selektionskriterien in wissenschaftliche Kommunikationsprozesse einspeisen.
- **Diskurstheorie (Keller 2011):**
  Kooperation und Fragmentierung sind nicht nur institutionelle Prozesse, sondern auch diskursive Konstruktionen. Strategiepapiere rahmen Wissenschaft zunehmend entlang geopolitischer Risikologiken. Begriffe wie „gefährdete Kooperation“, „kritische Partnerschaft“ oder „Wissensexport“ markieren diskursive Verschiebungen, die Kooperation delegitimieren.
- **Internationale Beziehungen (Nye, Drezner):**
  Der Gegensatz zwischen Kooperation und Fragmentierung spiegelt den Konflikt zwischen liberalen Ordnungsvorstellungen (Interdependenz, Soft Power) und strategischer Steuerung (Abschottung, Sanktion, „Weaponized Interdependence“). Wissenschaft wird damit zum geopolitischen Handlungsfeld.
- **Cybersicherheitsforschung (Dunn Cavelty):**
  Der digitale Raum wird als sicherheitsrelevanter Infrastrukturraum definiert. Kooperation erscheint hier nicht mehr nur als epistemische Notwendigkeit, sondern als Risiko. Sicherheitspolitisch motivierte Steuerung von Datenflüssen, Partnerschaften und Plattformnutzung ist Teil dieser Neubewertung.

Beobachtungslogik:

In nationalen Strategiepapiere tritt das Spannungsverhältnis häufig doppelt auf: Einerseits wird internationale Kooperation als innovationsfördernd, resilienzstärkend und normativ erwünscht dargestellt. Andererseits finden sich in denselben Dokumenten Mechanismen, die Kooperation kontrollieren, beschränken oder sicherheitspolitisch relativieren. Diese Ambivalenz ist zentral für die diskursive Konstruktion von Wissenschaft im Cyberraum.

Fazit:

Das Spannungsverhältnis zwischen internationaler Kooperation und Fragmentierung zeigt, wie wissenschaftliche Offenheit zunehmend unter politischen und sicherheitstechnologischen Vorbehalten verhandelt wird. In nationalen Strategien treten beide Pole nicht als Widerspruch, sondern als simultane Erwartungen auf – ein Ausdruck funktionaler Ambivalenz, die Hochschulen zunehmend in strategische Dilemmata zwingt.

Offenheit vs. Sicherheit

Problemformulierung:
Wissenschaft ist auf Offenheit angewiesen – auf freien Zugang zu Wissen, internationale Zusammenarbeit, Transparenz von Daten und Reproduzierbarkeit von Ergebnissen.
Diese Offenheit gerät jedoch zunehmend in Konflikt mit wachsenden Anforderungen an Cybersicherheit, Kontrollmechanismen und Zugriffsbeschränkungen. Der strukturelle Zielkonflikt zwischen einem systemischen Offenheitsprinzip und sicherheitspolitischen Schutzinteressen wird insbesondere im Cyberraum sichtbar. Für Hochschulen und Forschungseinrichtungen ergibt sich daraus ein Spannungsfeld, das sowohl ihre Infrastrukturpraxis als auch ihre epistemische Kultur betrifft.

Theoretische Fundierung:

- **Systemtheorie (Luhmann 1997):**
  Offenheit ist ein funktionaler Imperativ des Wissenschaftssystems. Kommunikation erfolgt unter Unsicherheit, Zugang ist notwendig für Autopoesis (Anschlussfähigkeit) der Wissenschaft. Sicherheit hingegen operiert nach Inklusions-/Exklusionslogik: Sie selektiert, begrenzt, schützt. In ihrer Kopplung erzeugen beide Systeme strukturelle Irritationen – z. B. wenn Sicherheitsmaßnahmen wissenschaftliche Offenheit einschränken.
- **Diskurstheorie (Keller 2011):**
  Offenheit und Sicherheit sind diskursiv gerahmte Ordnungsbegriffe. In politischen und institutionellen Strategien werden sie mit normativer Bedeutung aufgeladen: „Offenheit“ als Fortschrittsbegriff, „Sicherheit“ als Legitimation von Eingriffen. Die Rahmung bestimmt, welcher Pol Vorrang erhält – z. B. in der Darstellung von Risiken, Verantwortlichkeiten oder Compliance.
- **Cyberraumforschung (Dunn Cavelty, Zettl):**
  Cybersicherheit ist nicht neutral, sondern eine Form der Machtausübung und der

symbolischen Kontrolle über Infrastrukturen. In sicherheitsorientierten Kontexten werden offene Forschungspraktiken zunehmend als Bedrohung geframet – besonders in technologischen Forschungsfeldern wie Quantenforschung, KI oder Biotechnologie.

- **Souveränitätsdiskurse:**
  Die Forderung nach Forschungssicherheit wird Teil nationalstaatlicher Souveränitätsansprüche – z. B. durch die Kontrolle über Datenklassifikationen, Zugriffsbeschränkungen oder Compliance-Vorgaben in Drittmittelvergabe und internationalen Projekten.

Beobachtungslogik:

Strategiedokumente rahmen Offenheit oft als Innovationsbedingung und demokratisches Prinzip – gleichzeitig aber als Risiko, das Schutzmaßnahmen erfordert. Die Spannung entsteht nicht aus einer Gegenüberstellung, sondern aus der gleichzeitigen Geltung beider Prinzipien. In der Makroperspektive zeigt sich dieser Zielkonflikt als zentrales Steuerungsdilemma.

Fazit:

Das Spannungsverhältnis zwischen Offenheit und Sicherheit ist nicht einfach als Gegensatzpaar zu verstehen, sondern als strukturelle Überlagerung zweier widersprüchlicher Systemlogiken. Die untersuchten Strategien rahmen Offenheit zunehmend unter Vorbehalt – als etwas, das geschützt, begrenzt oder überprüft werden muss. Die damit verbundene Verschiebung epistemischer Leitwerte wird nicht offen thematisiert, ist aber analytisch zentral für das Verständnis wissenschaftlicher Praxis im digitalen Zeitalter.

Digitale Souveränität vs. Technologische Abhängigkeit

Problemformulierung:
Mit dem digitalen Wandel wird die Frage nach technologischer Autonomie zu einer strategischen Herausforderung für Wissenschaft und Hochschulen. Der Ruf nach „digitaler Souveränität“ gewinnt an Bedeutung – als Ziel selbstbestimmter Kontrolle über Daten, Systeme und Infrastrukturen. In der Praxis geraten Hochschulen jedoch zunehmend in Abhängigkeit von wenigen globalen Plattformanbietern, proprietären Softwarelösungen und externen Dienstleistern. Das Spannungsverhältnis zwischen dem Anspruch auf Unabhängigkeit und faktischer Abhängigkeit beschreibt eine strukturelle Ambivalenz, die tief in die technische, organisatorische und politische Realität der digitalen Wissenschaft eingebettet ist.

Theoretische Fundierung:

- **Systemtheorie (Luhmann 1997):**
  Die Kopplung von Wissenschaft und Technik erfolgt funktional, nicht politisch: Hochschulen übernehmen Technologien, die Kommunikation ermöglichen. Dabei entsteht eine strukturelle Abhängigkeit von externen Systemen, deren Selektionslogik nicht steuerbar ist. Diese Abhängigkeit ist weder intentional noch kontrollierbar – sie ist systemisch.
- **Digitale Souveränitätsforschung:**
  „Digitale Souveränität" ist ein diskursives Machtinstrument: Der Containerbegriff markiert nicht nur eine strategische Zielsetzung, sondern erzeugt auch normative Erwartungen. In politischen und institutionellen Texten fungiert er als Legitimationsformel – selbst dort, wo faktische Abhängigkeiten fortbestehen.
- **Cyberraumforschung (Dunn Cavelty, Zettl):**
  Technologische Abhängigkeit wird zunehmend als Sicherheitsrisiko gerahmt. Insbesondere bei sensibler Forschungsinfrastruktur – etwa Künstlicher Intelligenz, Quantenrechnen, Cloud Computing, Identitätsmanagement, Kollaborationsplattformen – entsteht ein Spannungsfeld zwischen Innovationsfähigkeit und Kontrollverlust.
- **Techniksoziologie / Digitale Governance:**
  Entscheidungen über IT-Infrastruktur werden häufig unter wirtschaftlichem oder pragmatischem Druck getroffen. Open Source, föderale Systeme oder europäische Alternativen stehen in vielen Fällen nur symbolisch zur Verfügung. Der Souveränitätsdiskurs kann dadurch zur Rhetorik ohne Rückbindung an die technische Realität werden.

Beobachtungslogik:

Strategien thematisieren digitale Souveränität zunehmend explizit – etwa durch Verweise auf Open-Source-Technologien, europäische Alternativen oder „Resilienz durch Unabhängigkeit". Gleichzeitig bleibt unklar, wie diese Autonomie konkret erreicht werden soll. Der Souveränitätsbegriff wird so selbst Teil eines politisch-technischen Zielkonflikts.

Fazit:

Digitale Souveränität wird als strategisches Ziel formuliert, steht jedoch in einem Spannungsverhältnis zu strukturellen und ökonomischen Abhängigkeiten. Diese Ambivalenz zeigt sich nicht nur in der Umsetzung technischer Lösungen, sondern bereits in der politischen Sprache. Der Begriff wird häufig als symbolischer Marker verwendet, ohne dass die

Bedingungen seiner Einlösung geklärt wären. Für Hochschulen entsteht daraus ein systemisches Dilemma zwischen normativem Anspruch und operativer Realität.

Wissenschaftsfreiheit vs. Politisches Agendasetting

Problemformulierung:
Wissenschaftsfreiheit ist ein zentrales Strukturprinzip des modernen Wissenschaftssystems. Sie sichert die Autonomie wissenschaftlicher Fragestellungen, Methoden und Ergebnisse und institutionelle Selbstbestimmung gegenüber politischer oder ökonomischer Einflussnahme. Gleichzeitig wachsen die Erwartungen an Hochschulen, Beiträge zu sicherheitspolitischen, technologischen oder gesellschaftlichen Zielen zu leisten. Strategien und Förderlinien formulieren zunehmend explizite Agenden, denen sich Wissenschaft unterzuordnen hat. Daraus ergibt sich ein Spannungsverhältnis zwischen selbstreferentieller Erkenntnisproduktion und funktionaler Instrumentalisierung wissenschaftlicher Praxis.

Theoretische Fundierung:

- **Systemtheorie (Luhmann 1992):**
  Wissenschaft und Politik sind autopoietische Teilsysteme mit jeweils eigener Selektionslogik. Während Wissenschaft sich am Kriterium der Wahrheit orientiert, folgt Politik dem Prinzip von Macht und Konsens. Wird Wissenschaft systematisch politisch funktionalisiert, droht eine Entdifferenzierung – das heißt eine Verwischung systemischer Grenzen.
- **Diskurstheorie (Keller 2011):**
  Wissenschaftliche Themenfelder werden diskursiv gerahmt und politisch aufgeladen. Wenn politische Akteure Forschung nicht nur fördern, sondern auch definitorisch beeinflussen (z. B. durch Sicherheitsetikettierung oder thematische Vorgaben), verändert sich die Deutungshoheit über Erkenntnisinteressen. In der Folge wird die Grenze zwischen Erkenntnis und Zwecksetzung diskursiv verschoben.
- **Cyberraumforschung (Dunn Cavelty):**
  Forschungssicherheit wird zunehmend als Teil nationaler Sicherheitsarchitekturen verstanden. Dadurch verändern sich nicht nur institutionelle Zuständigkeiten, sondern auch die Logik von Drittmittelvergabe, Projektarchitektur und Public-Private-Partnerships – mit Folgen für die wissenschaftliche Selbststeuerung.
- **Governance-/Policy-Ansätze:**
  Die strategische Steuerung von Forschung kann direkt über Finanzmittelsteuerung oft

aber auch indirekt erfolgen – etwa über Zielvorgaben, Förderlogiken oder Kooperationspflichten. Agendasetting muss daher nicht in autoritativer Form erfolgen, sondern kann auch über subtile Steuerungsinstrumente wie Ausschreibungsbedingungen, Gremienbesetzungen oder Narrative wirken.

Beobachtungslogik:

In Strategiedokumenten wird die Wissenschaftsfreiheit meist affirmativ erwähnt – häufig als Schutzformel. Gleichzeitig werden konkrete sicherheitspolitische Agenden, strategische Forschungsfelder oder nationale Prioritäten eingeführt, an denen sich Forschung messen lassen soll. Diese Koexistenz normativer Bekenntnisse und instrumenteller Anforderungen ist analytisch zentral für dieses Spannungsverhältnis.

Fazit:

Das Spannungsverhältnis zwischen Wissenschaftsfreiheit und politischem Agendasetting wird in nationalen Strategien selten explizit thematisiert – wohl aber strukturell erzeugt. Politische Zielsetzungen werden zunehmend in wissenschaftliche Steuerungsinstrumente eingeschrieben, während die Autonomie rhetorisch abgesichert bleibt. Hochschulen bewegen sich dadurch in einem Raum doppelter Erwartung: Sie sollen unabhängig sein – und zugleich gesellschaftlich nützlich, sicherheitsrelevant und anschlussfähig an politische Programme. Dieses Spannungsverhältnis ist nicht auflösbar, aber analysierbar – insbesondere mit Blick auf die diskursive Rahmung von Forschung und die institutionelle Reaktion darauf.

Sicherheitsproduzenten vs. Hochwertziele

Problemformulierung:
Hochschulen nehmen im digitalen Zeitalter eine doppelte Rolle ein: Einerseits werden sie zunehmend als aktive Gestalter von Cybersicherheitskompetenz, Technologieentwicklung und digitaler Resilienz adressiert. Andererseits gelten sie selbst als besonders gefährdete Angriffsziele – etwa wegen ihrer offenen Infrastrukturen, sensiblen Forschungsdaten und begrenzten Schutzressourcen. Aus dieser Gleichzeitigkeit entsteht ein strukturelles Spannungsverhältnis: Hochschulen sollen Sicherheitsakteure sein – bleiben aber gleichzeitig Hochwertziele in sicherheitskritischen Feldern.

Theoretische Fundierung:

- **Systemtheorie (Luhmann 1991):**
  Organisationen operieren in Erwartungskontexten, die strukturell widersprüchlich sein können. Wird eine Hochschule gleichzeitig als Produzent sicherer Strukturen und als verwundbares Objekt beschrieben, entsteht ein Erwartungsparadox: Die Organisation soll sich selbst gegen Bedingungen wappnen, deren Teil sie strukturell ist.
- **Cyberraumforschung (Zettl, Dunn Cavelty):**
  Hochschulen werden zunehmend in nationale Sicherheitslogiken integriert – etwa durch Forschungsförderung, Awareness-Programme oder Mitgliedschaft in Sicherheitsnetzwerken. Gleichzeitig bleibt ihre Verwundbarkeit hoch, etwa durch föderale Zuständigkeiten, begrenzte Investitionen oder heterogene IT-Landschaften.
- **Diskurstheorie (Keller 2011):**
  Die Rahmung von Hochschulen als Sicherheitsakteure erfolgt nicht neutral: Sie erzeugt normative Erwartungen und Verantwortlichkeitszuschreibungen. Gleichzeitig bleiben diese Diskurse oft blind gegenüber realen Ressourcenlagen oder strukturellen Begrenzungen – was die Differenz zwischen Anspruch und Wirklichkeit weiter vertieft.

Beobachtungslogik:

Strategiepapiere markieren Hochschulen als Teil nationaler Sicherheitsarchitekturen – etwa durch deren Beiträge zu Cybersicherheitsforschung, Ausbildung oder Netzwerksicherheit. Gleichzeitig werden dieselben Hochschulen als potenzielle Angriffsziele dargestellt. Der doppelte Diskurs erzeugt Ambivalenzen, die sich in politischen Erwartungen, Förderstrukturen und institutionellen Zielkonflikten niederschlagen.

Fazit:

Hochschulen werden in nationalen Sicherheitsdiskursen doppelt adressiert: als Orte der Lösung – und als Teil des Problems. Dieses Spannungsverhältnis erzeugt strategische Zielambivalenzen, organisationale Überforderungspotenziale und politische Erwartungsspannung. Theoretisch lässt es sich als systemisches Paradox verstehen, diskursiv als ambivalente Rahmung und praktisch als Herausforderung für die Governance wissenschaftlicher Institutionen im digitalen Raum. Die Analyse macht sichtbar, wie Sicherheit nicht nur implementiert, sondern auch produziert und performativ zugewiesen wird.

10. Makroanalyse internationaler und nationaler Strategiedokumente

Die in Kapitel 9 entwickelten Spannungsverhältnisse bilden den heuristischen Analyserahmen für die nachfolgenden empirischen Untersuchungsschritte. In Kapitel 10 wird dieser Rahmen auf die Makroebene angewendet, konkret auf die jeweils aktuellsten und damit politisch gültigen nationalen strategischen Cybersicherheitsdokumente ausgewählter Staaten (Deutschland, USA, Großbritannien). Ziel ist es, zu analysieren, wie die Spannungsverhältnisse diskursiv adressiert, gewichtet oder aufgelöst werden – etwa durch politische Rahmungen, normative Zielsetzungen oder technologische Leitbilder. Dabei wird geprüft, inwieweit nationale Strategien Ambivalenzen sichtbar machen, rhetorisch überdecken oder funktional in Governance-Strukturen überführen.

Die Auswahl der betrachteten Länder (Deutschland, Großbritannien, USA) basiert auf ihrem dokumentierten strategischen Einfluss im Bereich geopolitische Relevanz, der Relevanz ihrer Wissenschaftssysteme sowie deren Fähigkeiten in der Cybersicherheit. Die Auswahl inkludiert 3 von 5 der bedeutendsten globalen Wissenschaftssysteme (Nature Index 2024). Diese Staaten spiegeln unterschiedliche Sicherheitskulturen wider, bleiben aber dem globalen Norden bzw. dem Westen zugeordnet. Es ist anzumerken, dass eine Erweiterung um insb. China und Japan, die TOP 5 komplettieren würde. Die Gewinnung entsprechender Daten und Dokumente insb. für China hier aber aus politischen und auch sprachlichen Gründen schwierig ist. Perspektiven des globalen Südens (z. B. China, Indien, Brasilien, Südafrika) würden die Generalisierbarkeit der Ergebnisse erweitern können.

Die Codierung erfolgte strukturiert entlang der Spannungsverhältnisse des heuristischen Rahmens mit dem Programm MAXQDA 2024 und folgt den Prinzipien der strukturierenden Inhaltsanalyse nach Mayring (2019), jedoch im Verständnis eines Mixed-Method-Ansatzes zur Ausarbeitung der Triangulation auf den Untersuchungsgegenstand. Die Analysemethode folgte dabei einem sequentiellen Vorgehen: Zunächst wurden zentrale Begrifflichkeiten auf Englisch (Research/University/Academia/Science/Education) identifiziert. Die lexikalische Suche führte zu 27 Fundstellen in der Cybersicherheitsstrategie der USA und 125 Fundstellen in der des UK. Eine äquivalente Suche nach den Begriffen (Forschung/Universität/Hochschule/Wissenschaft/Academia/Bildung) führte zu 165 Fundstellen. Dies erfolgte, um die Sichtbarkeit wissenschaftsbezogener Inhalte zu maximieren.

Anschließend erfolgte eine kontextualisierte Codierung entlang der Spannungsverhältnisse des heuristischen Rahmens, die schließlich in eine analytische Reflexion der Anschlussfähigkeit der Kategorien mündete.

Tabelle 1: Übersicht Nationaler Sicherheitsstrategien

Land	Dokument	Jahr	Umfang (Wörter)	Besondere Hinweise
Deutschland	Cybersicherheitsstrategie für Deutschland	2021	22.546	Sehr umfassendes Dokument, stark europäisch und innovationspolitisch orientiert.
Vereinigtes Königreich	National Cyber Strategy	2022	23.781	Geopolitisch akzentuiert, starke Verknüpfung von Wissenschaft, Technologie und nationaler Sicherheit.
USA	National Cybersecurity Strategy	2023	12.144	Kompakter Aufbau, Fokus auf nationale Resilienz, Innovationsfähigkeit und strategische Rivalitäten.

Zwei der drei analysierten Dokumente (Vereinigtes Königreich 2022, USA 2023) liegen im Original auf Englisch vor, während die Cybersicherheitsstrategie Deutschlands (2021) in deutscher Sprache verfasst ist. Ziel war es, die Spannungsverhältnisse unabhängig von sprachlichen Differenzen theoriegeleitet und methodisch kohärent zu erfassen.

10.1. Internationale Kooperation vs. Fragmentierung

Die Analyse des Spannungsverhältnisses zwischen internationaler Kooperation und geopolitisch bedingter Fragmentierung zeigt über alle drei untersuchten Strategiedokumente hinweg ein diskursiv ambivalentes Bild. Kooperation wird auf Ebene der politischen Zielsetzungen einhellig affirmiert. Deutschland betont explizit, dass „Bedrohungen im Cyberraum nicht an Ländergrenzen halt machen“ und Cybersicherheit daher „nur in Kooperation mit unseren europäischen und internationalen Partnern gewährleistet werden kann“ (Deutschland 2021, S. 23). Dabei wird Cybersicherheit als „gemeinsame Aufgabe von Staat, Wirtschaft, Wissenschaft und Gesellschaft“ verstanden, die ein „kooperatives Vorgehen sowie eine vertrauensvolle Zusammenarbeit“ voraussetzt (Deutschland 2021, S. 23). Besonders hervorgehoben wird hierbei die wirtschaftliche und sicherheitspolitische Vernetzung mit strategisch wichtigen Partnern zur Wahrung europäischer digitaler Souveränität (Deutschland 2021, S. 24).

Zugleich formuliert Deutschland die Relevanz internationaler Forschungskooperationen ausdrücklich: „Deutschland unterstützt internationale Forschungskooperationen zur Entwicklung sicherer IT-Systeme“ (Deutschland 2021, S. 85). Diese Kooperationen dienen sowohl technologischer Exzellenz als auch der nationalen Resilienz: „Die internationale

Vernetzung der Cybersicherheitsforschung wird gestärkt“ (Deutschland 2021, S. 105). Allerdings gibt es deutliche regulatorische Einschränkungen: „Exportkontrollregelungen betreffen zunehmend auch wissenschaftliche Kooperationen“ (Deutschland 2021, S. 88), was eine sicherheitspolitische Relativierung der wissenschaftlichen Offenheit darstellt.

Die US-amerikanische Strategie hebt internationale Kooperation ebenfalls hervor, jedoch mit klarer geopolitischer Zielsetzung: „Forge International Partnerships to Pursue Shared Goals“ (US 2023, S. 8). Explizit benennt sie geopolitische Konkurrenten wie China, Russland, Iran und Nordkorea, die „fortschrittliche Cyber-Fähigkeiten aggressiv einsetzen, um Ziele zu verfolgen, die unseren Interessen und allgemein akzeptierten internationalen Normen zuwiderlaufen“ (US 2023, S. 7). Wissenschaftliche Kooperation wird hier stark entlang politischer Loyalitäten strukturiert, wodurch der wissenschaftliche Modus des offenen Austauschs geopolitisch instrumentalisiert wird.

Großbritannien verfolgt einen vergleichbaren, aber normativ stärker ausgeprägten Ansatz. Es formuliert explizit: „We will work to uphold an open and interoperable internet as the best model to support global prosperity and wellbeing, resisting the pressure of authoritarian states towards fragmentation and their idea of internet sovereignty“ (UK 2022, S. 34). Wissenschaftliche Kooperation wird ebenfalls strategisch gerahmt als Mittel, globale Herausforderungen im Bereich der Cybersicherheit zu adressieren: „Strengthening international research collaborations to address global cyber challenges“ (UK 2022, S. 14). Der transnationale Charakter des Cyberraums wird anerkannt, zugleich als „arena of systemic competition and clash of competing interests, values and visions“ beschrieben (UK 2022, S. 10).

Übergreifend zeigt sich eine deutliche funktional-instrumentelle Orientierung internationaler Kooperation. Während staatliche und wirtschaftliche Partnerschaften intensiv betont werden, bleibt die Bedeutung grenzüberschreitender wissenschaftlicher Netzwerke – als genuin offene, nicht-souveräne Formen der Kooperation – systematisch unterreflektiert.

Fragmentierung wird sicherheitspolitisch externalisiert und primär autoritären Staaten zugeschrieben, während die eigene Rolle bei der Beschränkung wissenschaftlicher Offenheit kaum kritisch reflektiert wird.

Die **diskursive Gleichzeitigkeit von Offenheit und Kontrolle**, Kooperation und Regulierung, Globalität und nationaler Resilienz ist dabei kein bloßer Widerspruch, sondern Ausdruck einer funktionalen Ambivalenz. Wissenschaft gerät so zunehmend in strategische

Dilemmata, da sie einerseits offen und international anschlussfähig, andererseits national kontrollierbar und sicherheitspolitisch konform sein soll. Dies illustriert ein klassisches Erwartungsparadoxon und zeigt, dass die funktionale Differenzierung von Wissenschaft diskursiv suspendiert wird. Kooperation erscheint somit nicht mehr primär als epistemische Notwendigkeit, sondern als strategisch steuerbares Risikoobjekt.

10.2. Offenheit vs. Sicherheit

Das Spannungsverhältnis zwischen wissenschaftlicher Offenheit und IT-Sicherheitsanforderungen wird in den Strategiedokumenten nicht als explizites Dilemma, sondern als funktional überlagerte Rahmung verhandelt. Die Offenheit – als konstitutives Prinzip wissenschaftlicher Kommunikation – wird nicht grundsätzlich in Frage gestellt, erscheint jedoch zunehmend relativiert durch sicherheitspolitische Imperative. Aus Sicht der funktionalen Differenzierung erzeugt die Kopplung zweier inkompatibler Systemlogiken – Autopoiesis und Schutzlogik – strukturelle Irritationen, die in den untersuchten Texten diskursiv sichtbar werden.

Das Vereinigte Königreich rahmt Offenheit in affirmativer Sprache und stellt sie zugleich unter sicherheitspolitischen Vorbehalt: „open and democratic society“ (UK 2022, S. 33) ist das normativ gesetzte Ziel, doch bereits im selben Dokument findet sich die sicherheitslogische Einbettung: „Promoting secure research collaboration internationally“ (UK 2022, S. 40). Die Idee einer offenen, kooperativen Wissenschaft bleibt damit unter die Bedingung von Kontrollierbarkeit gestellt – Offenheit darf nur dort gelten, wo Sicherheit nicht gefährdet wird.

Noch deutlicher zeigt sich dieses Verhältnis in der US-amerikanischen Strategie. Dort heißt es: „The openness and connection enabled by access to the Internet are game-changers for communities everywhere“ (US 2023, S. 2). Offenheit erscheint hier als strukturprägendes Moment globaler Entwicklung. Doch bereits wenige Seiten später wird dieselbe Struktur als Risikoadressat beschrieben: „But this accelerating global interconnectivity also introduces risks“ (US 2023, S. 6). Die offene Vernetzung – Bedingung von Wissenschaftlichkeit – wird zur Angriffsfläche. Der offene Datenfluss, epistemisch notwendig, ist aus sicherheitspolitischer Sicht potenziell gefährlich.

Die deutsche Strategie schließlich verbindet explizit beide Pole in einer sicherheitsorientierten Semantik: „Deutschland setzt sich für ein freies, offenes und sicheres Internet ein“ (Deutschland 2021, S. 43). Die Trias von Freiheit, Offenheit und Sicherheit wird hier nicht

als Zielkonflikt, sondern als synthetisierbare Einheit dargestellt. Die eigentliche strukturelle Spannung bleibt dabei unterbelichtet.

Parallel zur diskursiven Rahmung der Offenheit zeigt sich in allen Dokumenten eine hohe Dichte an Passagen, die das Thema IT-Sicherheit in den Vordergrund rücken – besonders im Kontext von Hochschulen. So formuliert Deutschland: „Sicherheitsanforderungen für Hochschulnetzwerke werden verschärft“ (Deutschland 2021, S. 91). Hochschulen werden in den Status kritischer Infrastrukturen überführt – die epistemische Logik der Offenheit tritt hinter institutionelle Schutzanforderungen zurück.

Die Bedrohungsszenarien sind dabei konkret: „Russia’s 2017 'NotPetya' cyberattack on Ukraine […] causing billions of dollars in damage“ (US 2023, S. 6) oder „The cyber operations of criminal syndicates now represent a threat to the national security […]“ (US 2023, S. 8) verdeutlichen, wie umfassend und machtvoll der Sicherheitsdiskurs strukturiert ist. Die durch diese Rahmung erzeugte Risikosemantik macht aus Forschungspotenzialen potenzielle Gefahrenquellen.

Im Ergebnis werden zwei Tendenzen sichtbar:

1. **Offenheit wird nicht als eigenständiges Schutzgut verhandelt**, sondern als untergeordnetes Moment im Rahmen sicherheitspolitischer Zielhierarchien.
2. **Sicherheitsanforderungen werden präzise operationalisiert**, während Offenheit vage bleibt – ein asymmetrisches Steuerungsverhältnis, das die funktionale Autonomie der Wissenschaft unterläuft.

Diskurstheoretisch markiert diese Konstellation eine **semantische Verschiebung**: Offenheit wird nicht mehr primär als wissenschaftlicher Leitwert adressiert, sondern als regulierbares Risiko oder nachgeordnete Bedingung technologischer Resilienz. Damit verliert sie ihren epistemischen Eigenwert. Was sichtbar bleibt, ist eine strategisch konstruierte Erwartung an Wissenschaft, sich sicherheitskonform zu verhalten – ohne dabei ihren Offenheitsanspruch strukturell absichern zu können.

10.3. Digitale Souveränität vs. Technologische Abhängigkeit,

Frage nach digitaler Souveränität gehört zu den am prominentesten diskutierten strategischen Zielsetzungen in allen drei untersuchten Cyberstrategien. Dabei wird digitale Souveränität als Voraussetzung nationaler Resilienz und internationaler Wettbewerbsfähigkeit

beschrieben. Besonders im deutschen Dokument erscheint sie programmatisch verdichtet: „Digitale Souveränität ist daher eine zentrale Leitlinie der Cybersicherheitsstrategie 2021 und ein Handlungsmotiv in allen vier Handlungsfeldern“ (Deutschland 2021, S. 24). Zugleich wird sie operationalisiert – etwa über den Verweis auf eine gemeinsame europäische Strategie oder gezielte Forschungsförderung in sicherheitsrelevanten Technologiefeldern (ebd.).

Zahlreiche Passagen belegen diesen souveränitätsbezogenen Anspruch auf politischer, wirtschaftlicher und wissenschaftlicher Ebene. So heißt es etwa: „Digitale Souveränität von Staat, Wirtschaft, Wissenschaft und Gesellschaft stärken“ (Deutschland 2021, S. 7), ergänzt um die Zielstellung, „die Förderung von Schlüssel- und Zukunftstechnologien“ zu nutzen, um „die Digitale Souveränität und die Wettbewerbsfähigkeit der Unternehmen im Bereich Cybersicherheit auszubauen“ (ebd.). Gleichzeitig wird darauf verwiesen, dass digitale Souveränität nicht nur ein abstraktes Leitbild ist, sondern eine handlungsleitende Perspektive für konkrete Maßnahmen in der Forschung: „Schwerpunktbereiche sind unter anderem die anwendungsorientierte Forschung und Entwicklung sowie der Forschungstransfer“ (Deutschland 2021, S. 24).

Diese normative Setzung trifft jedoch auf eine empirische Realität tiefgreifender technologischer Abhängigkeiten. In zahlreichen Passagen adressiert das deutsche Dokument die systemische Verflechtung mit externen Akteuren – insbesondere mit Blick auf außereuropäische Anbieter: „Aktuell bestehen bei den eingesetzten und notwendigen technischen Lösungen häufig große Abhängigkeiten, insbesondere vom außereuropäischen Ausland“ (Deutschland 2021, S. 106). Auch die Behörden seien hiervon betroffen, wenngleich erste Fortschritte vermeldet werden: „Die Abhängigkeit der Sicherheitsbehörden von außereuropäischen Produkten und Lösungen ist gesunken“ (Deutschland 2021, S. 107). Diese Entwicklung wird jedoch primär als Risiko gerahmt, das politische Steuerung erfordert: „Insbesondere sollen zum Schutz der Sicherheitsinteressen Digitale Souveränität und Resilienz gegenüber hybriden Bedrohungen erlangt und die Abhängigkeit von ausländischen Informationstechnologien reduziert werden“ (Deutschland 2021, S. 24).

Die Logik dieses Spannungsverhältnisses – zwischen normativem Souveränitätsanspruch und faktischer technologischer Fremdbestimmung – zeigt sich auch im Vereinigten Königreich. Die britische Strategie spricht offen von strukturellen Grenzen souveräner Handlungsfähigkeit: „The UK will not be able to develop sovereign capability in all the technologies that matter“ (UK 2022, S. 30). Dennoch bleibt der Anspruch bestehen, zentrale Tech-

nologien selbst kontrollieren zu können: „Foster and sustain sovereign and allied advantage in the security of technologies critical to cyberspace“ (UK 2022, S. 14). Hier wird das Spannungsverhältnis nicht aufgelöst, sondern als strategische Balance formuliert: zwischen Eigenleistung, internationaler Kooperation und geopolitischer Einflussnahme auf Standardisierungsprozesse. Das Bekenntnis zur Souveränität ist dabei explizit technologiepolitisch aufgeladen: „There will be some areas where we need to maintain a truly sovereign capability, and others where we will collaborate with international partners or seek a leading position in one aspect of the market“ (UK 2022, S. 82).

Gerade in diesem Kontext rückt auch die Rolle der Wissenschaft in den Fokus. Während Deutschland auf Förderlinien und Technologieprogramme verweist, wird im britischen Dokument die Einbindung von Forschung systematischer adressiert: „Research and innovation will be central to maintaining UK cyber power“ (UK 2022, S. 15). Wissenschaftliche Einrichtungen erscheinen damit nicht nur als Stakeholder, sondern als strukturelle Träger technologischer Eigenständigkeit. Der Begriff „sovereign capability“ wird diskursiv eng mit innovationspolitischer Steuerung verbunden und über Forschung operationalisiert.

Die US-amerikanische Strategie ist in der Verwendung des Begriffs „digitale Souveränität“ zurückhaltender, formuliert jedoch vergleichbare Zielsetzungen in sicherheitspolitischem Duktus: „Reducing strategic reliance on untrusted foreign technology providers is essential“ (USA 2023, S. 8). Wissenschaft wird dabei als Teil staatlicher Resilienz adressiert, nicht jedoch als autonomer Akteur. Steuerungsmaßnahmen werden über zentrale Finanzierungsmechanismen institutionalisiert: „The Federal Government will fund cybersecurity research and promote innovation“ (USA 2023, S. 24). Die Verknüpfung zwischen wissenschaftlicher Innovationsfähigkeit und geopolitischer Positionierung ist dabei implizit, aber strukturell angelegt.

Der transatlantische Vergleich zeigt: Während alle drei Staaten digitale Souveränität als strategische Leitlinie formulieren, bleiben ihre Konzepte zur konkreten Umsetzung ambivalent. Wissenschaftliche Institutionen erscheinen dabei primär als funktionale Instrumente technologischer Selbstbehauptung – nicht jedoch als Akteure mit spezifischen Gestaltungsbedarfen oder epistemischen Schutzanforderungen. Diese funktionale Rahmung verstellt den Blick auf die strukturellen Implikationen der zunehmenden Plattformabhängigkeit, fragmentierten Forschungsinfrastrukturen und fehlenden Interoperabilität alternativer Systeme.

Gerade im deutschen Dokument tritt diese Spannung offen zutage. Einerseits heißt es: „Cybersicherheitsniveau trägt so zur Stärkung der Digitalen Souveränität von Bürgerinnen und Bürgern, Wirtschaft, Wissenschaft und Staat bei“ (Deutschland 2021, S. 23). Andererseits wird konstatiert, dass „die Abhängigkeit von Systemen, deren Vertrauenswürdigkeit nicht kontrolliert werden kann, potenzielle Einfallstore für Cyberakteure“ eröffne (Deutschland 2021, S. 14). Der Begriff der digitalen Souveränität wird so zur diskursiven Leitformel – er rahmt zugleich normative Erwartung und strukturelles Defizit.

Im Ergebnis werden zwei strukturelle Tendenzen sichtbar:

1. Digitale Souveränität wird zwar als **zentrale Leitlinie strategischer Orientierung** formuliert, doch ihre institutionelle Einlösung bleibt auf **symbolische Bekräftigungen und technologiepolitische Programme** beschränkt.
2. Technologische Abhängigkeiten werden klar benannt, jedoch primär als s**icherheitsrelevantes Risiko – nicht als strukturelles Hindernis wissenschaftlicher Autonomie**.

Diskurstheoretisch zeigt sich eine doppelte Rahmung: Digitale Souveränität fungiert einerseits als normativer Projektionsraum für Selbstbestimmung, andererseits als Legitimationsfigur für Sicherheits- und Infrastrukturpolitik. Die Wissenschaft erscheint darin nicht als souveräner Akteur, sondern als Mitvollzugsinstanz strategischer Technologiepolitik. Ihre Abhängigkeit von proprietären Lösungen, globalen Plattformen und geopolitisch geprägten Standards wird nicht als eigenes Steuerungsproblem adressiert, sondern als zu überwindendes Defizit innerhalb eines staatlich dominierten Souveränitätsdiskurses.

Was sichtbar bleibt, ist eine semantische Verschiebung: Autonomie wird nicht mehr als funktionale Selbststeuerung verstanden, sondern als politische Steuerungsleistung. Damit verliert digitale Souveränität ihren epistemischen Anker in der Wissenschaft und wird zu einem strategisch aufgeladenen Begriff – anschlussfähig an viele Interessen, aber wenig konkret in der operativen Umsetzung durch wissenschaftliche Akteure

10.4. Wissenschaftsfreiheit vs. politisches Agendasetting

Das Spannungsverhältnis zwischen Wissenschaftsfreiheit und politischem Agendasetting zeigt sich in den analysierten Strategiedokumenten weniger durch explizite Aussagen zur Autonomie der Wissenschaft, sondern vielmehr durch strategische Zielvorgaben, die Forschung funktional einbinden. Wissenschaft wird als Ressource für nationale Sicherheit

und technologische Wettbewerbsfähigkeit adressiert – ihre epistemische Eigenlogik hingegen bleibt strukturell unterbelichtet.

In der Cybersicherheitsstrategie der Vereinigten Staaten wird ein starker staatlicher Steuerungsanspruch sichtbar. Die US-Regierung kündigt an: "The Federal Government will also prioritize funding for cybersecurity research, development, and demonstration (RD&D) programs aimed at strengthening critical infrastructure cybersecurity and resilience." (USA 2023, S. 26). Diese Ausrichtung auf sicherheitspolitische Zielkorridore wird weiter konkretisiert: "Departments and agencies will direct RD&D projects to advance cybersecurity and resilience in areas such as artificial intelligence, operational technologies and industrial control systems, cloud infrastructure, telecommunications, encryption, system transparency, and data analytics used in critical infrastructure." (USA 2023, S. 28). Forschung wird hier nicht als offenes Erkenntnissystem, sondern als strategischer Hebel zur Stärkung nationaler Infrastrukturen definiert.

Auch Großbritannien bezieht wissenschaftliche Einrichtungen in sicherheitspolitische Steuerung ein. Die Regierung formuliert explizit: "As a government, we have committed to spend £22 billion on research and development, and to put technology at the heart of our plans for national security." (UK 2022, S. 9). Forschungsausgaben werden damit direkt an nationale Sicherheitsinteressen gekoppelt. Zugleich bleibt unklar, ob – und wie – dies mit bestehenden Freiräumen wissenschaftlicher Selbststeuerung vereinbar ist.

Die deutsche Cybersicherheitsstrategie bleibt in dieser Hinsicht vergleichsweise vage. Zwar wird betont, dass "rechtlich verbürgte Freiheiten geschützt werden" (Deutschland 2021, S. 13), doch dieser Hinweis bleibt programmatisch. Eine systematische Verankerung oder Operationalisierung wissenschaftlicher Autonomie findet nicht statt.

Auch die Diskussion zur globalen Konvergenz demokratischer Normen bleibt unkonkret. Zwar verweist das Vereinigte Königreich auf eine schwindende globale Offenheit: "Internet freedom is decreasing globally and the vision of the internet as a shared space that supports the exchange of knowledge and goods between open societies risks coming under threat." (UK 2022, S. 23). Die wissenschaftliche Freiheit wird jedoch nicht ausdrücklich in diesen Kontext integriert.

Im Ergebnis zeigt sich ein strategisches Ungleichgewicht: Während sicherheitspolitische Zielsetzungen präzise operationalisiert und institutionell verankert werden, bleibt die Wissenschaftsfreiheit entweder implizit oder rein deklarativ. Wissenschaft wird als Instrument

zur Erreichung politischer Zielsetzungen positioniert, ihre funktionale Eigenlogik jedoch nicht strukturell abgesichert. **Forschungsförderung folgt zunehmend sicherheitsstrategischen Rationalitäten** – etwa im Bereich kritischer Infrastrukturen oder neuer Schlüsseltechnologien. **Wissenschaftsfreiheit** wird formal referenziert, aber nicht praktisch in Schutzmechanismen übersetzt.

Diskurstheoretisch zeigt sich eine semantische Verlagerung: Wissenschaft erscheint nicht mehr als autonomes System, sondern als strukturierbares Feld sicherheitsbezogener Innovation – ein Narrativ, das epistemische Unabhängigkeit also Wissenschaftsfreiheit systematisch relativiert.

10.5. Sicherheitsproduzenten vs. Hochwertziele

Die Die Rolle von Hochschulen im sicherheitspolitischen Diskurs wird in allen drei analysierten Strategien zunehmend sichtbar. Dabei zeigt sich ein doppelter Zugriff: Einerseits erscheinen Hochschulen als potenzielle Hochwertziele im digitalen Raum – angreifbar, verletzlich, schützenswert. Andererseits werden sie als Akteure positioniert, die aktiv zur Cybersicherheitsarchitektur beitragen sollen – als Forschungsstandorte, Innovationsmotoren und Qualifizierungsinstanzen. Dieses Spannungsverhältnis markiert eine strategische Verschiebung im Rollenverständnis wissenschaftlicher Einrichtungen.

In der Strategie der Vereinigten Staaten wird die Gefährdungslage besonders deutlich adressiert: "Research institutions face increasing threats to their sensitive data and intellectual property" (USA 2023, S. 27). Gleichzeitig betont die US-Regierung, dass Hochschulen aktiv in die Entwicklung nationaler Resilienz eingebunden werden sollen: "Build a robust and diverse cyber workforce, embrace security and resilience by design, strategically coordinate research and development investments in cybersecurity" (USA 2023, S. 9). Dazu gehört auch eine institutionelle Verstärkung über Programme wie NICE oder CyberCorps: "The strategy will build on existing efforts to develop our national cybersecurity workforce including the National Initiative for Cybersecurity Education (NICE), the CyberCorps: Scholarship for Service program [...]" (USA 2023, S. 31). Wissenschaft wird damit nicht nur als vulnerabel, sondern auch als systemrelevant für die strategische Resilienz verstanden.

Auch in der deutschen Strategie wird die Relevanz der Wissenschaft für Cybersicherheit prominent hervorgehoben. Hochschulen werden dabei sowohl als Teil kritischer Infra-

strukturen adressiert, als auch als zentrale Innovationsakteure gefördert: "Die Wissenschaft leistet insbesondere durch ihre Forschungstätigkeit [...] einen zentralen Beitrag zur Erhöhung der Cybersicherheit in Deutschland" (Deutschland 2021, S. 19). Der Aufbau neuer Forschungszentren und Initiativen wie ATHENE oder die "Cyberagentur" wird explizit gefördert: "Mit dem Nationalen Forschungszentrum für angewandte Cybersicherheit ATHENE [...] sowie einer Vielzahl weiterer international sichtbarer Forschungsgruppen [...]" (Deutschland 2021, S. 69).

Gleichzeitig zeigt sich in Deutschland ein deutlicher Bezug zur Sicherheitsarchitektur des Staates: "Mit der Cyberagentur werden ressortübergreifend ambitionierte Forschungsvorhaben mit hohem Innovationspotenzial auf dem Gebiet der Cybersicherheit [...] finanziert" (Deutschland 2021, S. 69). Damit wird nicht nur auf Schutz, sondern auf aktive Mitgestaltung durch Wissenschaft gesetzt. Die strategische Rolle der Forschung in nationaler Sicherheitspolitik wird hier diskursiv befestigt.

Das Vereinigte Königreich verfolgt in besonderer Klarheit ein umfassendes Konzept, das Wissenschaft gleichzeitig als Schutzobjekt und Sicherheitsproduzent fasst: "UK science and technology will be the engine room of this change [...] ensuring that cyber continues to be a national economic and strategic asset" (UK 2022, S. 9). Die Forschung wird nicht nur als Reaktionsraum, sondern als strategischer Treiber adressiert. Besonders deutlich wird dies in der Aussage: "We must have a diverse and technically skilled workforce, a vibrant research community [...] all built on stronger partnerships between government, industry and academia" (UK 2022, S. 49).

Institutionelle Initiativen wie die "Academic Centres of Excellence in Cyber Security Research" belegen diesen Anspruch: "We have consolidated the UK’s reputation as a global leader in cyber security research, with 19 academic centres of excellence and 4 research institutes tackling our most pressing cyber security challenges" (UK 2022, S. 21). Der Transfer wissenschaftlicher Expertise in staatliche Strukturen wird dabei als strategisches Ziel gefasst: "Taking the lead in the technologies vital to cyber power, building our industrial capability and developing frameworks to secure future technologies" (UK 2022, S. 13).

Im Ergebnis zeigen sich deutliche Unterschiede in der Zuschreibung wissenschaftlicher Rollen:

1. Die USA betonen die Vulnerabilität wissenschaftlicher Einrichtungen, koppeln diese aber klar an ihre Rolle in der Resilienz- und Ausbildungsarchitektur.

2. Deutschland sieht **Hochschulen als Forschungsakteure**, die durch staatlich geförderte Programme in die nationale Sicherheitsstrategie eingebunden sind.
3. Das Vereinigte Königreich geht am weitesten, indem es Forschung und Innovation explizit als integralen **Bestandteil nationaler Cybermacht** versteht.

Dabei entstehen neue Governanceformen, die Wissenschaft in sicherheitspolitische Steuerungsprozesse integrieren, ohne ihre epistemische Eigenlogik systematisch abzusichern. Hochschulen werden diskursiv zu Sicherheitsressourcen umcodiert, ohne dass die damit verbundenen Zielkonflikte – etwa zwischen Autonomie und Funktionalisierung – explizit reflektiert würden.

Pointiert formuliert, belegen die Strategien empirisch den doppelten Zugriff auf Hochschulen:

1. Sie sind **Hochwertziele** – verletzlich, schützenswert, sicherheitsrelevant.
2. Sie sind **Sicherheitsproduzenten** – innovationsstark, strategisch steuerbar, funktional instrumentalisierbar.

Diese doppelte Rolle erzeugt ein asymmetrisches Steuerungsverhältnis: Während Anforderungen, Programme und Förderlogiken präzise operationalisiert werden, bleibt die Frage nach der strukturellen Absicherung wissenschaftlicher Autonomie weitgehend unbeantwortet. Die Funktion von Wissenschaft wird strategisch neu codiert – nicht als Ort unabhängiger Erkenntnisproduktion, sondern als Ressource staatlicher Sicherheitsarchitekturen. Zusammengenommen mit den anderen empirisch aufgezeigten Spannungsverhältnissen könne diese diskursiven Dilemmata auf tieferen Eben zu Handfesten Handlungsdilemmata führe, die ggf. im weiteren Verlauf der Analyse beobachtbar werden.

10.6. Synthese: Wissenschaft als blinder Fleck der Cybersicherheitsstrategien

Die vergleichende Analyse der Cybersicherheitsstrategien Deutschlands, des Vereinigten Königreichs und der USA entlang der fünf Spannungsverhältnisse zeigt ein deutliches Muster: Wissenschaft ist für alle drei Staaten ein strategisches Element zur Förderung von Cybersicherheit, wird aber primär funktional gerahmt – als Ressource für Resilienz, Wettbewerbsfähigkeit und technologische Souveränität. Ihre systemischen Eigenlogiken, Schutzbedarfe und epistemischen Prinzipien hingegen bleiben unterbelichtet.

Tabelle 2: Makroanalyse Synthese Übersicht nach Spannungsfeldern und Staaten, eigene Darstellung

Spannungsfeld	Deutschland	Vereinigtes Königreich	USA
Kooperation ⇅ Fragmentierung	Betonung multilateraler Abstimmung (EU, ENISA), aber wenig geopolitische Differenzierung.	Eindeutige Allianzorientierung, geopolitisch selektiv.	Kooperation als Wert adressiert, in der Praxis jedoch durch Bedrohungsdominanz eingeschränkt
Offenheit ⇅ Sicherheit	Wissenschaftliche Offenheit kaum adressiert; Fokus auf Schutz kritischer Infrastrukturen.	Erkennt Rolle offener Forschung in Digitalstrategie an – wird jedoch durch NCSC reguliert.	Offene Forschung stark durch Sicherheit gerahmt (z. B. NSF, DoD-Kooperation).
Souveränität ⇅ Abhängigkeit	„Digitale Souveränität" als EU-Narrativ, aber hohe Cloud-Abhängigkeit (US-Anbieter).	Tech-Souveränität als Industriepolitik (u. a. Halbleiter), Forschung soll liefern.	Dominanz eigener Tech-Konzerne – Souveränität durch Kontrolle, nicht Unabhängigkeit.
Wissenschaftsfreiheit ⇅ Agendasetting	Forschung wird als Schutzgut betrachtet, aber nicht als politisch-autonome Stimme eingebunden.	Forschungsförderung durch Regierungsziele klar steuernd (z. B. DSIT, NCSC).	Sicherheitspolitik steuert über Fördermittel und Compliance (z. B. CMMC-Standards).
Sicherheitsproduzenten ⇅ Hochwertziele	Hochschulen als „kritische Infrastruktur" benannt, aber ohne finanzielle Umsetzungskraft.	Hochschulen zunehmend als Teil des nationalen Cyberökosystems gesehen.	Hochschulen sind Teil des „National Security Ecosystem" (inkl. Geheimhaltungspflichten).

Internationale Kooperation und Fragmentierung: Alle drei Staaten betonen internationale Zusammenarbeit. Deutschland verweist auf „die internationale Vernetzung der Cybersicherheitsforschung" (Deutschland 2021, S. 105), das Vereinigte Königreich unterstreicht: „Strengthening international research collaborations to address global cyber challenges" (UK 2022, S. 14), und die USA formulieren: „We will deepen international partnerships and alliances to counter cyber threats and support global resilience" (USA 2023, S. 8). Doch diese Kooperation bleibt sicherheitspolitisch gerahmt; Wissenschaft als transnationales System mit spezifischer Offenheitslogik wird kaum differenziert betrachtet. Fragmentierung wird primär geopolitisch verstanden („pressure of authoritarian states towards fragmentation", UK 2022, S. 34), nicht als Risiko für offene Wissenschaftskooperationen.

Offenheit und IT-Sicherheitsanforderungen: Offenheit erscheint in den Strategien unter dem Vorbehalt sicherheitsbezogener Kontrolllogiken. Deutschland etwa formuliert: Open Science-Initiativen sollen auch im Bereich Cybersicherheit gefördert werden (Deutschland

2021, S. 102), betont aber zugleich: Sicherheitsanforderungen für Hochschulnetzwerke werden verschärft (Deutschland 2021, S. 91). Die USA sprechen davon: „The openness and connection enabled by access to the Internet are game-changers for communities everywhere“ (USA 2023, S. 2) und „we must seize the opportunity to instill our most cherished values, as embodied by the Declaration for the Future of the Internet (DFI)“ (US 2023, S. 5) ohne diese konkret auszuformulieren. Offenheit bleibt eine normative Idee wird in der Praxis aber regulierbare Größe, nicht ein zu schützendes epistemisches Prinzip verstanden.

Digitale Souveränität und technologische Abhängigkeit: Digitale Souveränität ist in allen Strategien zentral verankert, etwa als „zentrale Leitlinie der Cybersicherheitsstrategie 2021“ (Deutschland 2021, S. 24) oder in der britischen Strategie als Ziel, „there will be some areas where we need to maintain a truly sovereign capability, and others where we will collaborate with international partners“ (UK 2022, S. 82). Gleichzeitig wird die faktische Abhängigkeit benannt: „Aktuell bestehen bei den eingesetzten und notwendigen technischen Lösungen häufig große Abhängigkeiten, insbesondere vom außereuropäischen Ausland“ (Deutschland 2021, S. 106). Die Ambivalenz zwischen aufgeladener Souveränitätsrethorik und real existierender globaler Abhängigkeit wird nicht produktiv aufgelöst.

Wissenschaftsfreiheit und politisches Agendasetting: Die strategische Steuerung von Forschung wird offen thematisiert, etwa in den USA: „The Federal Government will prioritize funding for cybersecurity research“ (USA 2023, S. 26) oder im Vereinigten Königreich: „We have committed to spend £22 billion on research and to put technology at the heart of our plans for national security“ (UK 2022, S. 9). Gleichzeitig bleibt die Wissenschaftsfreiheit schwach verankert. Deutschland spricht zwar allgemein davon, „sich für ein freies, offenes, sicheres und globales Internet ein[zusetzten], in dem grundrechtlich verbürgte Freiheiten geschützt werden“ (Deutschland 2021, S. 13), aber ohne konkrete Absicherung. Wissenschaft als selbstreferentielles System bleibt konzeptionell unterrepräsentiert.

In den nationalen Cyberstrategien der USA, Großbritanniens und Deutschlands wird die Wissenschaft in ihrer sicherheitspolitischen Relevanz zwar anerkannt, jedoch bleibt eine systematische Reflexion ihrer Doppelrolle als Schutzobjekt und Sicherheitsproduzentin weitgehend aus. Die deutsche Strategie betont. Die IT-Sicherheitsforschung zu Zukunftstechnologien sowie zu Cyberbedrohungen liefert wichtige und relevante Erkenntnisse. […] Hierfür werden Universitäten, Hochschulen und Forschungseinrichtungen […] gezielt ge-

fördert. (Deutschland 2021, S. 70). Die US-Strategie hebt hervor: We must […] strategically coordinate research and development investments in cybersecurity, and promote the collaborative stewardship of our digital ecosystem (USA 2023, S. 9). Die britische Strategie verbindet Innovationsfähigkeit mit nationaler Sicherheit: „Universities will contribute to national cyber-security innovation ecosystems“ (UK 2022, S. 26).

Fazit: Im Ergebnis zeigen sich über alle Strategien hinweg drei strukturelle Muster:

1. Wissenschaft wird sicherheitspolitisch funktionalisiert, nicht epistemisch differenziert.
2. Offenheit, Autonomie und internationale Kooperation erscheinen als regulierbare Momente, nicht als eigenständige Prinzipien.
3. Die strategischen Dokumente reproduzieren ein asymmetrisches Steuerungsverhältnis: Wissenschaft passt sich an, wird aber nicht geschützt.

Eine Vergleichsperspektive zwischen den Ländern zeigt, dass trotz übergreifender Steuerungslogiken und gemeinsamer Zielstrukturen (Sicherheit, Souveränität, Resilienz) deutliche Unterschiede in der strategischen Rahmung von Wissenschaft und Hochschulen bestehen. Diese Differenzen sind nicht nur semantischer Natur, sondern spiegeln tiefere Unterschiede in sicherheitspolitischer Kultur, Governanceverständnis und Wissenschaftseinbindung wider.

- **Deutschland** betont Forschung als Teil gesellschaftlicher Resilienz, bleibt in der konkreten Operationalisierung aber oft abstrakt. Die strategische Rahmung oszilliert zwischen innovationspolitischer Förderung und vorsichtiger Einbindung in staatliche Sicherheitsstrukturen. Wissenschaft erscheint als Partner, nicht als eigenständiger Akteur mit abgesicherten Rechten – institutionelle Autonomie wird selten explizit geschützt, sondern implizit vorausgesetzt.
- **Großbritannien** geht am weitesten in der funktionalen Integration von Wissenschaft in nationale Cybersicherheitsarchitekturen. Forschung wird systematisch als Motor strategischer Selbstbehauptung adressiert – als „engine room“ der Cybermacht. Diese klare Kopplung erzeugt einerseits Sichtbarkeit, andererseits eine starke Erwartungskonvergenz: Wissenschaft ist sichtbar, weil sie steuerbar sein soll. Wissenschaftsfreiheit wird affirmiert, aber primär als Teil demokratischer Außenwirkung verstanden – nicht als intern abzusicherndes Prinzip.

- **Die USA** formulieren den umfassendsten Steuerungsanspruch. Wissenschaft wird als strategischer Faktor nationaler Sicherheit adressiert – insbesondere in der Qualifikation von Fachkräften und Entwicklung sicherheitsrelevanter Technologien. Zugleich bleibt Wissenschaftsfreiheit fast ausschließlich implizit; der wissenschaftliche Eigenwert wird diskursiv nicht gesondert geschützt, sondern als Teil strategischer Ziele mitgeführt. Die Rolle der Wissenschaft ist damit weniger offen, aber klarer funktional definiert.

Diese Differenzen markieren keine völligen Gegensätze, aber sie strukturieren die institutionelle Anschlussfähigkeit von Cybersicherheitszielen an Hochschulrealitäten deutlich unterschiedlich – ein Befund, der für die folgende Mesoanalyse von besonderer Relevanz sein könnte.

Insgesamt markiert das Kapitel eine analytische Leerstelle: Der wissenschaftliche Eigenwert erscheint marginal, die strukturellen Anforderungen des Wissenschaftssystems werden semantisch überlagert von Sicherheitsnarrativen. Eine funktional differenzierte Politikberatung, die Wissenschaft nicht nur als Ressource, sondern als eigenständiges Subsystem ernst nimmt, bleibt bislang aus.

10.7. Kritische Rückbindung: Wissenschaft im sicherheitspolitischen Ordnungsrahmen

Die Makroanalyse der nationalen Cybersicherheitsstrategien hat ein konsistentes, zugleich problematisches Befundbild ergeben: Wissenschaftliche Institutionen erscheinen primär als Ressourcen und Zielstrukturen sicherheitspolitischer Steuerung – nicht jedoch als epistemisch autonome Systeme mit spezifischen Schutzbedarfen. Offenheit, Autonomie und internationale Kooperation werden zwar diskursiv anerkannt, jedoch strukturell untergeordnet.

Die entlang der fünf Spannungsverhältnisse entwickelten Kategorien haben sich dabei als analytisch tragfähig erwiesen. Sie machen sichtbar, wie sicherheitspolitische Anforderungen systematisch mit wissenschaftlicher Praxis verschränkt werden – etwa durch gezielte Förderarchitekturen, technologische Steuerung und die semantische Rahmung von Forschung als sicherheitsrelevante Dienstleistung. Auffällig ist eine durchgängige Asymmetrie: Sicherheitsinteressen werden präzise operationalisiert, während wissenschaftliche

Prinzipien weitgehend abstrakt bleiben. Diese semantische Verschiebung delegitimiert Offenheit und Selbststeuerung nicht explizit – sie entwertet sie stillschweigend als nicht-prioritäre Kategorien. Die Analyse legt nahe, dass sich bestehende Spannungsverhältnisse wie Offenheit vs. Schutz oder Sicherheitsproduzent vs. Hochwertziel in der strategischen Praxis funktional verschieben – hin zu neuen Erwartungsparadoxien Erwartung vs. Ausstattung, die in den folgenden Kapiteln vertieft analysiert werden.

Gleichzeitig gilt es, die methodische Herleitung kritisch einzuordnen. Die Spannungsverhältnisse wurden deduktiv aus einem interdisziplinären Theoriegerüst abgeleitet und anhand strategischer Dokumente textanalytisch überprüft. Die Befunde stützen sich auf wörtliche Zitate und dokumentierbare Strukturmuster. Gleichwohl bleibt der Zugriff diskursiv – er erfasst nicht die reale Handlungspraxis in Hochschulen, sondern deren semantische Rahmung durch nationale Strategien. Damit ist die Analyse kein Abbild institutioneller Wirklichkeit, sondern ein Zugriff auf ihre politisch-kommunikative Verhandlung.

Diese Begrenzung ist analytisch gewollt – zugleich aber erkenntnisleitend für den nächsten Untersuchungsschritt: der **Übergang von der Makro- zur Mesoebene**. Denn wenn sich Spannungsverhältnisse in nationalen Strategiediskursen als strukturelle Erwartungsparadoxien zeigen, stellt sich die Frage, wie diese in konkreten organisatorischen Konfigurationen aufgenommen, transformiert oder bearbeitet werden. Aus diskursiven Spannungsfeldern werden hier potenziell reale Dilemmata – etwa in der Infrastrukturentwicklung, der Drittmittelvergabe oder der Governance digitaler Forschung.

Die folgende Analyse widmet sich daher der Mesoebene wissenschaftlicher Organisationen – mit dem Ziel, die Anschlussfähigkeit der entwickelten Kategorien an institutionelle Praxis und strukturelle Steuerungskonflikte systematisch zu prüfen.

11. Mesoanalyse wissenschaftspolitischer Strategien

Die Makroanalyse der nationalen Cybersicherheitsstrategien (Kap. 10) hat gezeigt, dass Wissenschaft in sicherheitspolitischen Diskursen primär funktionalisiert wird – etwa als Ressource zur Stärkung nationaler Resilienz oder technologischem Wettbewerb. Ihre systemischen Eigenlogiken, wie Offenheit, Autonomie und internationale Kooperation, bleiben dabei unterbelichtet. Die diskursive Einbettung wissenschaftlicher Akteure erfolgt entlang sicherheitsstrategischer Zielvorgaben – nicht jedoch im Sinne epistemischer Eigenständigkeit.

An diesen Befund anschließend richtet sich der Blick nun auf die Mesoebene wissenschaftlicher Governance. Ziel der folgenden Analyse ist es, die strategischen Selbstverständnisse und institutionellen Steuerungslogiken wissenschaftlicher Organisationen im Cyberaum zu rekonstruieren. Im Zentrum steht dabei die Frage, wie wissenschaftspolitische Akteure – etwa Beratungsinstitutionen, Hochschulleitungen oder operative Technologieverantwortliche – zentrale Spannungsverhältnisse wie Offenheit vs. Sicherheit oder Souveränität vs. Abhängigkeit interpretieren, bearbeiten und institutionell operationalisieren.

Methodisch bedient sich dieser Abschnitt zusätzlich am akteurszentrierten Institutionalismus (Scharpf 2000), der es ermöglicht, Akteurskonstellationen, Steuerungsinteressen und institutionelle Zielambivalenzen systematisch zu analysieren. Die zuvor entwickelten Spannungsverhältnisse (Kap. 9) dienen weiterhin analytische Heuristik: Sie strukturieren die empirischen Materialien, ermöglichen aber zugleich Offenheit für emergente Muster und institutionelle Besonderheiten.

Zur systematischen Differenzierung der verwendeten Quellen wird im Folgenden deren methodische, thematische und regionale Ausrichtung in einer kompakten Übersicht dargestellt:

Tabelle 3: Übersicht der Charakteristika der Quellen, eigene Darstellung

Quelle	Typ	Fokus	Methodik	Charakteristika
Wissenschaftsrat (2023) Souveränität und Sicherheit der Wissenschaft im digitalen Raum	Nationale Strategieempfehlung für Deutschland	Autonome Handlungsfähigkeit, digitale Selbstbestimmung von Hochschulen	Expertenkommission, Beratungsprozess, Gutachten	Systematisch, normativ, gesellschaftstheoretisch
EDUCAUSE Horizon Report (2024) Cybersecurity and Privacy Edition	Internationale Trendauswertung, Fokus aber USA	Globale Bedrohungen, neue Technologien (z.B. AI Governance, Datenschutz), Szenarien basiert	Delphi-Methode, Expertenpanel	Trendbericht, zukunftsgerichtet, adaptiv
Hochschulbarometer (2024) Digitale Sicherheit und Infrastruktur an Hochschulen	Nationale Bestandsaufnahme Deutschland	Wahrnehmung der Cybersicherheitslage und institutionelle Umsetzung in deutschen Hochschulen	Quantitative Umfrage	Deskriptiv, empirisch, institutionenbezogen

Diese drei Quellen decken unterschiedliche methodische Zugänge, Perspektiven und institutionelle Ebenen ab. Ihre gemeinsame Analyse erlaubt eine triangulierte Sicht auf Cybersicherheit im Wissenschaftssystem – von normativen Leitbildern über strategische Trendentwicklungen bis hin zur praktischen Umsetzung bzw. deren Wahrnehmung im Wissenschaftsbetrieb.

Durch die gezielte Kombination des Überganges von der strategischen Mata- zur Meso-Ebene über die Empfehlungen des **Wissenschaftsrats**, die Betrachtungen des **technologiegetriebenem Zukunftsdiskurs (EDUCAUSE)** von Cybersicherheitsexpertinnen und -experten aus dem Hochschulbereich sowie der **institutionell empfundenen Umsetzung durch die Hochschulleitung (Hochschulbarometer)** entsteht ein komplexes und interskalierbares Bild institutioneller Verortung von Wissenschaft im Cyberraum.

Die qualitative Inhaltsanalyse, wie sie auf der Makroebene in Anlehnung an Mayring und Kuckartz zur strukturierenden Erfassung diskursiver Rahmungen diente, wird auf der Mesoebene in modifizierter Form fortgeführt: nicht mehr als systematische Codierung entlang formalisierter Kategorien, sondern als theoriegeleitete, interpretative Dokumentenanalyse. Relevante Textpassagen werden dabei entlang des heuristischen Spannungsverhältnismodells strukturiert zugeordnet – jedoch im Sinne eines analytischen Mappings, das ohne formale Codierregeln auskommt. Diese methodische Lockerung trägt der Materialdichte, der Unterschiedlichkeit der Quellen sowie der Zielstellung Rechnung, komplexe institutionelle Selbstbeschreibungen, Steuerungslogiken und Zielambivalenzen entlang der Spannungsachsen sichtbar zu machen.

Parallel dazu verschiebt sich die diskurstheoretische Perspektive zunehmend in Richtung einer policy-analytischen Logik: An die Stelle der Analyse diskursiver Tiefenstrukturen im Sinne der Wissenssoziologischen Diskursanalyse (WDA) tritt eine Untersuchung institutioneller Akteurskonstellationen, Handlungsrestriktionen und Steuerungsmodi. Methodisch wird dieser Zugriff durch den akteurzentrierten Institutionalismus (Scharpf) gerahmt, der es erlaubt, die institutionelle Bearbeitung der Spannungsverhältnisse sowie das Zusammenspiel von Akteuren, Interessen und Handlungslogiken systematisch zu rekonstruieren.

11.1. Empfehlungen des Wissenschaftsrats 2023

Die Empfehlungen „Souveränität und Sicherheit der Wissenschaft im Cyberraum“ (2023) des Wissenschaftsrats bilden einen zentralen Referenzpunkt für das strategische Selbstverständnis wissenschaftlicher Organisationen. Quellenkritisch ist der Wissenschaftsrat

als normativer Akteur der Wissenschaft an der Schnittstelle zur Politik zu sehen. „Er berät die Bundesregierung und die Regierungen der Länder in allen Fragen der inhaltlichen und strukturellen Entwicklung der Wissenschaft, der Forschung und des Hochschulbereichs“ (WR 2025, Homepage[4]).

Im Rahmen der theoriegeleiteten, heuristisch strukturierten Dokumentenanalyse zeigt sich, dass der Wissenschaftsrat in seinen Empfehlungen Wissenschaftseinrichtungen nicht allein funktional als Schutzobjekte staatlicher Sicherheitspolitik adressiert, sondern explizit als eigenständige gesellschaftliche Teilsysteme mit spezifischen Eigenlogiken begreift. Im Mapping zentraler Spannungsverhältnisse werden dabei insbesondere Offenheit, epistemische Freiheit und internationale Kooperation als grundlegende Prinzipien wissenschaftlicher Selbststeuerung hervorgehoben.

Die strukturierende Analyse des Dokuments anhand der heuristischen Spannungsverhältnisse verdeutlicht, dass der Wissenschaftsrat digitale Souveränität als dynamisches Steuerungsziel formuliert, das über klassische sicherheitspolitische Paradigmen hinausweist. Im Mapping der Selbstbeschreibungen wird digitale Souveränität als Fähigkeit beschrieben, „eigenständig und selbstbestimmt über die Nutzung und Gestaltung digitaler Technologien zu entscheiden“ (Wissenschaftsrat, 2023, S. 5) – eine Formulierung, die epistemische Autonomie gegenüber externen technologischen, politischen und wirtschaftlichen Einflussfaktoren betont und damit das Spannungsverhältnis zwischen Selbststeuerung und systemischer Abhängigkeit explizit adressiert.

Das Spannungsverhältnis zwischen Offenheit und Sicherheit tritt besonders deutlich hervor. Die Beschreibung wissenschaftlicher Praxis als gleichermaßen auf internationalen Austausch wie auf den Schutz kritischer Ressourcen angewiesen, markiert diesen Zielkonflikt nicht als lösbares Problem, sondern als strukturelle Daueraufgabe: „Die Wissenschaft ist auf Offenheit und internationalen Austausch angewiesen. Gleichzeitig muss sie schützen, was für ihre Arbeit essentiell ist“ (Wissenschaftsrat, 2023, S. 7). Anders als auf der Makroebene, wo „Sicherheit“ als übergeordnete Zielkategorie dominierte, formuliert der Wissenschaftsrat das Spannungsverhältnis zwischen Offenheit und Schutz nicht als Zielhierarchie, sondern als strukturell eingebettete Ambivalenz, die institutionelle Aushandlung erfordert.

[4] https://www.wissenschaftsrat.de/DE/Ueber-uns/Wissenschaftsrat, abgerufen am 17.04.2025.

Die Empfehlungen verweisen zudem auf die strukturelle Heterogenität wissenschaftlicher Organisationen: „Der Kreis der Nutzenden ist groß, heterogen und durch hohe Fluktuation geprägt. […] Das bedeutet eine große Bandbreite an Digitalkompetenzen und ein ebenso uneinheitliches Bewusstsein für Sicherheitsrisiken“ (Wissenschaftsrat, 2023, S. 21). Im Lichte der gewählten Heuristik lässt sich dies als organisationsinterne Ausprägung des Spannungsverhältnisses zwischen Offenheit und Schutz deuten. Anstelle technokratischer Standardisierung fordern die Empfehlungen differenzsensible und adaptive Konzepte ein – ein Hinweis auf institutionelle Zielambivalenzen, wie sie im heuristischen Rahmen als analytisches Strukturmuster gefasst wurden. Der Wissenschaftsrat leistet hier einen entscheidenden Beitrag, indem er einen auf der Makroebene aus der Balance geratenden Diskurs auf die systemische Eigenlogik wissenschaftlicher Organisationen rückbindet.

Auch die technologische Abhängigkeit von privatwirtschaftlichen Anbietern wird als strukturelles Risiko markiert. Proprietäre Plattformen, undurchsichtige Cloud-Dienste und geschlossene Softwarelösungen gefährden laut Wissenschaftsrat die wissenschaftliche Nachvollziehbarkeit und institutionelle Unabhängigkeit: „Die Nutzung von Software und Cloud-Diensten kommerzieller Anbieter birgt das Risiko der Monopolisierung wissenschaftlicher Arbeitsumgebungen und der Abhängigkeit von geschlossenen, nicht nachvollziehbaren Systemen“ (Wissenschaftsrat, 2023, S. 19). Diese Passagen lassen sich im Spannungsverhältnis zwischen digitaler Souveränität und technologischer Abhängigkeit verorten. Bemerkenswert ist dabei die explizite Betonung epistemischer Robustheit als Zielgröße – ein Perspektivwechsel, der Cybersicherheit nicht als technische Schutzmaßnahme, sondern als Voraussetzung wissenschaftlicher Integrität positioniert.

Besonders hervorzuheben ist die gesellschaftstheoretische Rahmung, mit der der Wissenschaftsrat Cybersicherheit als integralen Bestandteil epistemischer Validität begreift: „Wenn die Integrität der verwendeten digitalen Technologien nicht mehr nachvollzogen werden kann, wird die Validität wissenschaftlicher Erkenntnisse in Frage gestellt“ (Wissenschaftsrat, 2023, S. 20). Diese Perspektive verschiebt die Bedeutung von Cybersicherheit weg von operativer Gefahrenabwehr hin zur systemischen Absicherung von Wissenschaftsfreiheit und Erkenntnisproduktion – ein Spannungsverhältnis, das im heuristischen Modell als Balance zwischen Schutzbedürfnis und epistemischer Offenheit gefasst wurde. Die Analyse zeigt somit, dass sich hier ein Reflexionsniveau etabliert, das über rein funktionale Risikodiskurse hinausreicht und auf die institutionelle Verfasstheit der Wissenschaft zielt.

Die Empfehlungen des Wissenschaftsrats konkretisieren die zuvor entwickelten Leitlinien durch strategisch-normative Handlungsanweisungen: Hochschulen sollen digitale Souveränität aktiv in ihre Governance-Strukturen integrieren, den Aufbau nachvollziehbarer, souveräner Technologien fördern und Kompetenzen im Bereich Cybersicherheit strukturell verankern. Dabei wird nicht auf standardisierte Lösungen gesetzt, sondern auf institutionenspezifische Umsetzungen – ein Hinweis auf die Notwendigkeit adaptiver Steuerung im Spannungsverhältnis zwischen Schutzanspruch und Offenheit. Die Förderung internationaler Kooperationen im Bereich souveräner Infrastrukturen zeigt zudem, dass digitale Souveränität nicht als Abschottung, sondern als handlungsfähige Vernetzung gedacht wird – eine Deutung, die sich entlang der heuristischen Achse Souveränität vs. Abhängigkeit verorten lässt.

Insgesamt positioniert der Wissenschaftsrat Wissenschaft nicht nur als Schutzobjekt, sondern als aktiv handlungsfähiges System im Cyberraum – mit spezifischen Eigenlogiken und Ambivalenzen. Cybersicherheit wird explizit als Voraussetzung epistemischer Integrität und institutioneller Autonomie adressiert. Anstelle technokratischer Standardisierung fordert das Papier differenzsensible, adaptive Konzepte – ein Hinweis auf institutionelle Zielambivalenzen, wie sie im heuristischen Rahmen dieser Arbeit analytisch gefasst sind. Die Empfehlungen leisten damit einen wichtigen Beitrag zur Reartikulation sicherheitspolitischer Diskurse aus der Perspektive wissenschaftlicher Spannungsverhältnisse – ein Perspektivwechsel, der auf der Makroebene weitgehend ausgeblendet blieb.

Auch wenn die nachfolgende Analyse systematisch auf der Mesoebene verbleibt, eröffnet das kürzlich veröffentlichte CIO-Positionspapier der Universitäten aus Bayern und Baden-Württemberg (März 2025) eine analytisch besonders ergiebige Perspektive, um Ebeneninteraktionen exemplarisch sichtbar zu machen. Denn hier lässt sich nachzeichnen, wie ein auf der Makroebene wirkmächtig gewordenes Spannungsverhältnis – etwa zwischen Offenheit und Sicherheit – von Akteuren der Wissenschaft nicht nur rezipiert, sondern aktiv bearbeitet wird. Was im strategischen Diskurs noch als ambivalente Spannung verhandelt wird, erscheint aus Sicht der institutionellen Praxis zunehmend als handfestes Handlungsparadoxon. Die CIOs reagieren darauf nicht nur mit normativen Positionierungen, sondern mit konkreten Vorschlägen zur institutionellen Operationalisierung digitaler Souveränität. Damit eröffnet das Papier eine selten klare Sicht auf das Wechselspiel zwischen diskursiver Rahmung, strategischer Deutung und praktischer Umsetzung im Wissenschaftssystem.

Das Papier nimmt explizit Bezug auf die Empfehlungen des Wissenschaftsrats, adaptiert diese jedoch aus einer deutlich operativeren Perspektive der Hochschul-IT. Dabei formulieren die CIOs eine eigenständige institutionelle Lesart von digitaler Souveränität – nicht als theoretisches Leitbild, sondern als unmittelbar praxisrelevante Steuerungskategorie. Die Bezugnahme auf ein „Spannungsfeld zwischen verschiedenen übergeordneten Entscheidungsdimensionen“ (CIO-Positionspapier Baden-Württemberg und Bayern 2025, S. 3) verweist dabei auf ein strategisches Problembewusstsein, das mit den in dieser Arbeit theoretisch entwickelten Spannungsverhältnissen in enger inhaltlicher Korrespondenz steht.

Besonders scharf konturiert das Papier das Spannungsverhältnis zwischen technologischer Abhängigkeit und institutioneller Souveränität. Einerseits erkennen die CIOs an, dass kommerzielle Anbieter zentrale Dienste mit hoher Qualität bereitstellen; andererseits problematisieren sie die daraus resultierende Abhängigkeit – etwa durch proprietäre Schnittstellen, eingeschränkte Exportfunktionen oder sogenannte Lock-in-Effekte. Die Dringlichkeit dieser Problematik wird deutlich formuliert: „Eine zu starke Abhängigkeit von einzelnen Anbietern kann langfristig die Handlungsfähigkeit von Hochschulen gefährden“ (ebd., S. 4). Damit rückt das Papier ein zentrales Dilemma in den Fokus: Der kurzfristige Effizienzgewinn durch Fremdlösungen steht dem langfristigen Ziel nachhaltiger digitaler Selbstbestimmung diametral gegenüber – ein klassisches institutionelles Zielparadoxon.

Die CIOs fordern daher ein differenziertes, dynamisches Steuerungsverständnis, das mit Spannungen nicht nur reaktiv umgeht, sondern sie explizit anerkennt und bearbeitet. Governance im digitalen Raum wird in diesem Sinne nicht als technokratische Standardisierung, sondern als reflexive Aushandlungsleistung begriffen – etwa durch partizipative Gremienprozesse, dokumentierte Bewertungsmaßstäbe oder das bewusste Nebeneinander konkurrierender Ziele. Digitale Souveränität erscheint so als „balancierter Steuerungskorridor“, nicht als rigides Zielraster.

Der Abschnitt zeigt damit exemplarisch, wie abstrakte Spannungsverhältnisse auf der Mesoebene in konkrete Entscheidungssituationen und institutionelle Handlungsdilemmata übersetzt werden. Während auf der Makroebene wissenschaftliche Prinzipien durch sicherheitspolitische Zielsetzungen semantisch umakzentuiert wurden, gelingt es auf der Mesoebene – etwa durch dieses CIO-Papier –, das Spannungsverhältnis Offenheit und Schutz bewusst zu reflektieren und institutionell rückzubinden.

Die Analyse macht deutlich: Der Beitrag der CIOs liegt nicht nur Einhegung auf die Empfehlungen des Wissenschaftsrats, sondern in der performativen Leistung, Spannungsverhältnisse nicht aufzulösen, sondern institutionell bearbeitbar zu machen. Die Aussagen des Papiers bestätigen nicht nur die heuristische Struktur dieser Arbeit, sondern schärfen deren empirische Fundierung – als Beispiel dafür, wie Governance unter Bedingungen digitaler Ambivalenz auch institutionell reflexiv angelegt sein kann.

Die Analyse der Empfehlungen des Wissenschaftsrats sowie des CIO-Positionspapiers zeigt exemplarisch, wie die in dieser Arbeit entwickelten Spannungsverhältnisse auf der Mesoebene institutioneller Steuerung nicht nur diskursiv gerahmt, sondern operativ reflektiert und strategisch bearbeitet werden. Während der Wissenschaftsrat strukturelle Ambivalenzen normativ und systemisch adressiert, konkretisieren die CIOs diese Spannungen als institutionelle Handlungsdilemmata – etwa zwischen technologischer Abhängigkeit und digitaler Selbstbestimmung oder zwischen Offenheit und Schutz.

Aus heuristischer Perspektive wird damit deutlich: Die Spannungsverhältnisse fungieren nicht nur als analytisches Raster, sondern als reale Strukturbedingungen institutioneller Entscheidungsfindung. Die Gegenüberstellung beider Dokumente macht sichtbar, wie wissenschaftspolitische Leitbilder (Makro/Meso) durch operative Akteursperspektiven (Meso/Mikro) gerahmt, transformiert und weiterverhandelt werden – ohne dass die grundlegenden Spannungen dabei auflösbar wären. Genau darin liegt die analytische Leistung der heuristischen Struktur dieser Arbeit: Sie ermöglicht es, Spannungsverhältnisse nicht als Defizite, sondern als strukturierende Elemente digitaler Governance im Wissenschaftssystem zu fassen.

Im Lichte der heuristischen Spannungsverhältnisse lässt sich festhalten, dass der Wissenschaftsrat eine analytische Leerstelle füllt, die im Rahmen der Makroanalyse als problematische Umcodierung wissenschaftlicher Prinzipien durch sicherheitspolitische Zielrationalitäten identifiziert wurde. Indem er die Eigenlogik wissenschaftlicher Praxis explizit betont und vor einer einseitigen funktionalen Vereinnahmung warnt, formuliert er nicht nur ein strategisches Gegenbild, sondern unternimmt eine gezielte Re-Codierung des Wissenschaftssystems entlang seiner systemimmanenten Leitdifferenzen – insbesondere Autonomie, Offenheit und epistemische Integrität. Die Empfehlungen versuchen damit, wissenschaftliche Selbststeuerung aus sicherheitslogischen Semantiken zu lösen und als eigenständige gesellschaftliche Rationalität zu stabilisieren. Re-Codierung meint hier, im

Sinne Luhmanns, nicht bloße Rückbesinnung, sondern eine aktuelle Reartikulation systemeigener Semantiken unter veränderten Umweltbedingungen – im Cyberraum ebenso wie im geopolitischen Kontext.

11.2. Internationale Perspektiven: Der 2024 EDUCAUSE Horizon Report

Der 2024 EDUCAUSE Horizon Report: Cybersecurity and Privacy Edition erweitert die zuvor analysierten nationalen Perspektiven um eine internationale Dimension. Basierend auf einem Delphi-Verfahren mit Expertinnen und Experten aus Wissenschaft, Verwaltung und Praxis identifiziert der Bericht zentrale Trends, Herausforderungen und Zukunftsszenarien im Bereich Cybersicherheit und Datenschutz im Hochschulkontext.

Bereits das Executive Summary des Berichts setzt einen Ton, der weit über technische Detailfragen hinausgeht. In bemerkenswerter Deutlichkeit beschreibt EDUCAUSE den aktuellen Kontext als von geopolitischer Instabilität und technologischem Umbruch geprägt:

“These are, in many ways, tumultuous times. Global political movements and ideologies continue to erode social ties and disrupt state and national legislative processes. Wars in Eastern Europe and the Middle East threaten to destabilize the global order. And new AI-powered technologies are evolving at breakneck speed, offering the world both the promise of new utopian capabilities and the threat of dystopian collapse. Against this backdrop of seismic change, higher education cybersecurity and privacy professionals must navigate new questions around what needs to be done to keep our institutions and our students safe and secure.” (EDUCAUSE 2024, S. 4)

Damit rahmt der Bericht die digitale Transformation nicht als linearen Modernisierungsprozess, sondern als ambivalente Suchbewegung zwischen Hoffnung und Kontrollverlust. Diese Grundspannung durchzieht den gesamten Text – implizit anknüpfend an gesellschaftliche Bruchstellen, explizit aber zumeist technikbezogen entfaltet.

Im Zentrum der Analyse stehen wachsende Anforderungen an digitale Sicherheit, personelle Engpässe und die beschleunigte Entwicklung KI-gestützter Technologien. Die Hochschulen erscheinen nicht mehr nur als Objekte von Sicherheitsbedrohungen, sondern als reflexive Akteure, die auf neue Problemkonstellationen reagieren müssen: „Higher education cybersecurity and privacy professionals must navigate new questions around what

needs to be done […]" (ebd.). Diese Beschreibung bleibt jedoch im Rahmen einer funktionalen Rollenbeschreibung, ohne deren institutionelle Eigenlogiken weiter auszudifferenzieren.

Deutlich wird auch im EDUCAUSE-Bericht ein Spannungsverhältnis zwischen technologischer Beschleunigung und institutioneller Anpassungsfähigkeit. Der Einsatz von KI-Systemen wird dabei doppelt gelesen: als Chance zur Verbesserung digitaler Schutzmechanismen – aber auch als Ursache neuer Komplexität und Unsicherheit: „Cyberattacks are becoming more sophisticated through AI" (ebd., S. 15). Besonders innovativ ist die Thematisierung ökologischer Folgen KI-basierter Sicherheitstechnologien: „posing challenges due to their environmental impacts" (ebd., S. 12). Damit verweist der Report auf Spannungsverhältnisse, die jenseits der klassischen Dualität von Sicherheit und Freiheit liegen und neue Kategorien in die Debatte einbringen.

Gleichzeitig bleiben zentrale Prinzipien wissenschaftlicher Praxis – etwa internationale Kooperation, Offenheit oder epistemische Freiheit – weitgehend unterbelichtet. Im Unterschied zum Wissenschaftsrat, der Wissenschaft als eigenständiges gesellschaftliches Teilsystem mit spezifischer Logik adressiert, verbleibt EDUCAUSE primär in einem technologisch-funktionalen Diskurs. Offenheitspraktiken, Diskursautonomie oder institutionelle Reflexionsfähigkeit erscheinen nur am Rande oder in Form normativer Randbemerkungen. Auch die Beobachtung politischer Einflussnahme auf Hochschulcurricula – „Politics is influencing higher education programs and curricula" (ebd., S. 11) – bleibt oberflächlich und wird nicht systematisch mit Fragen wissenschaftlicher Autonomie verknüpft.

Im heuristischen Rahmen dieser Arbeit lässt sich der EDUCAUSE-Bericht als Versuch interpretieren, sich den zukünftigen Konfigurationen institutioneller Spannungsverhältnisse im digitalen Raum anzunähern. Die diagnostizierten Herausforderungen lassen sich insbesondere in zwei Dimensionen verorten: im neuen Spannungsfeld zwischen **technologischem Fortschritt und institutioneller Verwundbarkeit** sowie zwischen **kurzzyklischen Anpassungsimperativen und langfristiger Offenheit wissenschaftlicher Praxis**.

Der analytische Mehrwert dieser Perspektive liegt weniger in der tiefergehenden Ausdifferenzierung wissenschaftlicher Eigenlogiken als vielmehr in der Antizipation neuer Ambivalenzen. Der Bericht markiert – aus einer international-technischen Perspektive – mögliche zukünftige Konstellationen von Spannungslagen im Cyberraum, ohne diese jedoch epistemisch oder institutionentheoretisch weiter zu reflektieren. Seine Funktion liegt damit im

Aufspannen eines Möglichkeitsraums, nicht in dessen Durchdringung. Gerade dadurch eröffnet EDUCAUSE einen wichtigen Horizont für die Frage, wie sich heutige institutionelle Spannungsverhältnisse unter dem Eindruck technologischer Disruption weiterentwickeln könnten.

11.3. Institutionelle Wahrnehmung und Umsetzung: Hochschulbarometer 2024 und IHE CTO/CIO Survey 2024 im Vergleich

Das **Hochschulbarometer 2024** ermöglicht eine empirische Bestandsaufnahme der Bedrohungswahrnehmung und der praktischen Umsetzung von Cybersicherheitsmaßnahmen an deutschen Hochschulen. Für das Hochschulbarometer befragt der Stifterverband jährlich die Hochschulleitungen in Deutschland zu ihren Einschätzungen der aktuellen Lage der Hochschulen, seit neuestem auch für den Bereich „digitale Infrastruktur und digitale Sicherheit“. Es liefert damit wichtige Hinweise darauf, inwieweit die zuvor entwickelten strategischen Anforderungen auf institutioneller Ebene aufgegriffen und umgesetzt werden.

Parallel dazu bietet die **IHE CTO/CIO Survey 2024** eine komplementäre empirische Grundlage für US-amerikanische Hochschulen. In dieser Umfrage erheben Inside Higher Ed und Hanover Research die Einschätzungen der Chief Technology Officers (CTOs) und Chief Information Officers (CIOs) zur Cybersicherheit und Digitalisierung direkt aus operativer Sicht. Während das Hochschulbarometer primär die Governance-Perspektive der Hochschulleitungen dokumentiert, fokussiert die IHE CTO/CIO Survey auf die praktische Umsetzung und Herausforderungen in der IT-Infrastruktur. Beide Surveys sind damit nicht ebenengleich, ergänzen sich jedoch und bieten dort wo Ergebnisse doch vergleichbar sind Ansatzpunkte für einen internationalen Vergleich institutioneller und technischer Perspektiven auf Cybersicherheitsfragen.

Im Folgenden wird dies an folgenden Feldern durchgeführt, belegt und verglichen:

- Bedrohungswahrnehmung und Schutzfähigkeit
- Technische Prävention und Awareness
- Krisenresilienz und Notfallmanagement
- Strategische Verankerung von Cybersicherheit
- Ressourcen
- Weitere Befunde

11.4. Bedrohungswahrnehmung und Schutzfähigkeit

Ein zentrales Ergebnis des Hochschulbarometers ist die hohe Sensibilität gegenüber der allgemeinen Bedrohungslage: 97,3 % der Hochschulleitungen schätzen die Gefahr durch Cyberangriffe auf Hochschulen in Deutschland als groß oder eher groß ein (Hochschulbarometer 2024, S. 35). Gleichzeitig zeigt sich eine deutliche Diskrepanz zwischen dieser allgemeinen Bedrohungswahrnehmung und der Einschätzung der eigenen Verwundbarkeit. Lediglich rund 77 % der Hochschulen nehmen ein vergleichbares Risiko für die eigene Einrichtung wahr. Die eigene Sicherheitslage wird deutlich optimistischer beurteilt als die Lage im Hochschulsystem insgesamt: 62,5 % der Hochschulen bewerten ihre eigenen Sicherheitsvorkehrungen als gut oder eher gut, während nur 13,6 % dies für andere Hochschulen annehmen (ebd.). Diese Wahrnehmungsdifferenz deutet auf eine verzerrte Sicherheitswahrnehmung hin, die institutionelle Verwundbarkeiten unterschätzen könnte, und spiegelt typische Herausforderungen im Bereich der organisationalen Risikowahrnehmung wider.

Eine ähnliche Wahrnehmungsproblematik zeigt sich auch in der Inside Higher Ed CTO/CIO Survey 2024. Hier äußern nur 17 % der befragten CTOs in den USA, dass sie sehr zuversichtlich sind, die Sicherheit ihrer Hochschule gegen Cyberangriffe gewährleisten zu können, während keiner der Befragten extreme Zuversicht äußerte (Inside Higher Ed 2024, S. 25). Die Mehrheit der CTOs (63 %) gibt an, lediglich moderate Sicherheit zu empfinden.

Obwohl in beiden Erhebungen unterschiedliche Gruppen befragt wurden – in Deutschland Hochschulleitungen, in den USA Fachverantwortliche für IT – ergibt sich ein vergleichbares Muster: In beiden Fällen wird die Bedrohungslage als hoch eingeschätzt, während die eigene Schutzfähigkeit als unzureichend bewertet wird. Die Befunde deuten auf ein länderübergreifendes strukturelles Spannungsverhältnis zwischen Bedrohungswahrnehmung und praktischer Schutzfähigkeit hin. Die Unterschiede in den institutionellen Rollen der Befragten scheinen dabei kaum Einfluss auf die Grundtendenz der Einschätzung zu haben. Cybersicherheitsrisiken werden unabhängig von institutioneller Ebene und nationalem Kontext als zentrale Herausforderung erkannt.

11.5. Technische Maßnahmen und Awareness

In Bezug auf die technischen Cybersicherheitsmaßnahmen zeigt sich eine gemischte Bilanz. Für Deutschland geben 75,3 % der Hochschulen an, hochschulweite Back-up-Strategien zu implementieren, präventive Schutzmaßnahmen sind jedoch weit weniger verbreitet. So führen lediglich 29,7 % der Hochschulen hochschulweite Sicherheitsschulungen für Mitarbeitende durch, bei Studierenden sind es sogar nur 9,5 % (Hochschulbarometer 2024, S. 36). Der Mangel an Awareness-Maßnahmen bleibt somit ein strukturelles Defizit: "Die unzureichende Sensibilisierung für digitale Sicherheit unter den Hochschulmitgliedern sehen 58,5 Prozent als einen Schwachpunkt" (ebd.).

Auch in den USA zeigt sich ein ambivalentes Bild bezüglich der Umsetzung technischer Schutzmaßnahmen. Der Schwerpunkt liegt hier auf technologischen Präventionsmaßnahmen: 94 % der CTOs berichten, dass ihre Hochschule im letzten Jahr Software-Updates durchgeführt hat, und 88 % verlangen eine verpflichtende Multi-Faktor-Authentifizierung für Mitarbeiteraccounts (Inside Higher Ed 2024, S. 25). Zusätzlich geben 78 % der CTOs an, dass ihre Verwaltungspersonen an verpflichtenden Sicherheitsschulungen teilnehmen müssen. Sicherheitstrainings für Studierende hingegen sind ebenfalls eine Schwachstelle: Nur 18 % der Institutionen in den USA geben an Trainings von Studierenden anzubieten (ebd.). Während technische Schutzmaßnahmen in den USA breiter implementiert werden als in Deutschland, bleibt die Integration von Awareness-Programmen auf allen Ebenen insbesondere für Studierende auf beiden Seiten des Atlantiks unzureichend.

Diese Ergebnisse verdeutlichen, dass präventive technische Maßnahmen wie Updates und Authentifizierung in den USA stärker institutionalisiert sind, wohingegen kulturelle Maßnahmen zur Steigerung des Sicherheitsbewusstseins – insbesondere unter Studierenden – international weiterhin eine erhebliche Lücke darstellen.

11.6. Krisenresilienz und Notfallmanagement

Neben dem Mangel an Sensibilisierungsmaßnahmen zeigt sich auch eine unzureichende Krisenresilienz: Nur 31,8 % der Hochschulen in Deutschland verfügen über hochschulweite Notfallpläne für Cyberangriffe, obwohl die Bedrohungslage als hoch eingeschätzt wird (Hochschulbarometer 2024, S. 36). Diese Lücke verweist auf Schwächen in der institutionellen Vorbereitung auf akute Sicherheitsvorfälle. Notfallmanagement ist eine reaktive

Fähigkeit, die eigentlich mit einer nach vorne schauenden Risikoplanung oder -management verbunden sein müsste. Das Hochschulbarometer selbst erhebt die Existenz von Risikomanagementsystemen allerdings nicht systematisch. Ein Auditbericht des HITS IS aus Bayern verweist jedoch darauf: „Risikoplanung oder -management ist praktisch nicht vorhanden. Unter 10 % der Hochschulen haben begonnen, toolgestützt ein Risikomanagement aufzubauen und können so Vorbildwirkung erreichen“ (HITS IS 2025, S. 5).

Auch im US-amerikanischen Hochschulsystem zeigt sich eine Lücke zwischen Bedrohungslage und institutioneller Resilienz. Zwar berichten 85 % der CTOs, dass ihre Hochschule über eine Cyberversicherung verfügt, um finanzielle Schäden abzusichern (Inside Higher Ed 2024, S. 20), doch beziehen sich weitere Angaben vorrangig auf den Bereich künstliche Intelligenz: Nur 14 % der Hochschulen haben ein dediziertes Team für AI-Sicherheit, und lediglich 12 % verfügen über eine umfassende Policy für den Schutz vor Risiken durch generative KI. Notfallübungen oder die Beschäftigung von White-Hat-Hackern zur aktiven Prüfung der Sicherheit werden nur von 20 % der Hochschulen genutzt (ebd.). Hier liegt der Fokus auf finanziellen Absicherungsmechanismen, während präventive Risiko- und Resilienzstrategien spezifisch für KI-Anwendungen ebenfalls vergleichsweise schwach entwickelt sind.

Insgesamt deutet der Vergleich darauf hin, dass in beiden Hochschulsystemen reaktive Maßnahmen wie Versicherungen oder Backups deutlich weiter verbreitet sind als proaktive Strategien zur systematischen Erfassung und Steuerung von Sicherheitsrisiken. Allerdings muss berücksichtigt werden, dass sich die US-amerikanischen Befunde primär auf KI-spezifische Risiken beziehen, während die deutschen Daten allgemeine Cybervorfälle adressieren. Trotz dieser inhaltlichen Unterschiede offenbart sich auf beiden Seiten ein grundlegendes Defizit beim Aufbau einer umfassenden und vorausschauenden Krisenresilienz im Hochschulbereich.

11.7. Strategische Verankerung von Cybersicherheit

Die strukturelle Verankerung von Cybersicherheitsstrategien in den Governance-Strukturen der Hochschulen bleibt ebenfalls unzureichend. Zwar liegt in 76,5 % der Hochschulen die Verantwortung für digitale Sicherheit bei der IT-Abteilung, jedoch verfügen nur 32,7 % über eine explizite CIO-Rolle (Hochschulbarometer 2024, S. 36). Die Etablierung strategischer Leitungsfunktionen, wie sie etwa vom Wissenschaftsrat gefordert wird, bleibt damit

die Ausnahme und verweist auf eine Lücke bei der nachhaltigen institutionellen Absicherung von Cybersicherheitsfragen. Auf die Notwendigkeit einer hochschulweiten strategischen Verankerung von Cybersicherheit weisen auch von der Heyde und Gerl (2022) hin. Sie betonen, dass die Etablierung von CIO-Rollen im direkten Umfeld der Hochschulleitungen ein zentrales Qualitätsmerkmal für die institutionelle Weiterentwicklung der digitalen Sicherheit darstellt.

Im US-amerikanischen Kontext zeigt sich ein differenzierteres Bild: Laut der Inside Higher Ed CTO/CIO Survey 2024 sind 63 % der CTOs Mitglied des Executive Cabinets der Präsidenten oder Kanzler ihrer Hochschulen (Inside Higher Ed 2024, S. 9). Diese enge Anbindung der IT- und Sicherheitsverantwortlichen an die oberste Leitungsebene deutet auf eine vergleichsweise stärkere institutionelle Integration der Cybersicherheit in der Hoschul-Governance hin. Allerdings berichten gleichzeitig über die Hälfte der CTOs, dass ihre Arbeit trotz dieser Einbindung noch immer primär als "Utility Service" und nicht als strategischer Partner wahrgenommen wird (ebd., S. 33). Dies zeigt, dass die bloße formale Anbindung an das Leitungsgremium nicht zwangsläufig mit einer tatsächlichen strategischen Aufwertung der Cybersicherheit verbunden sein muss, zumindest in den USA.

Vergleicht man die Befunde, so wird deutlich: Während in Deutschland die Rolle des CIO häufig organisatorisch schwach ausgebildet ist, existiert in den USA zumindest eine stärkere strukturelle Verankerung auf Leitungsebene. Dennoch bleibt die Herausforderung bestehen, Cybersicherheit nicht nur als technische Dienstleistung, sondern als strategisches Handlungsfeld im Wissenschaftsmanagement zu etablieren.

11.8. Ressourcen

Besonders auffällig ist die Ressourcenproblematik, die eine zentrale Herausforderung für den Aufbau resilienter Cybersicherheitsstrukturen darstellt. 89,8 % der deutschen Hochschulen berichten von Schwierigkeiten, qualifiziertes IT-Personal zu gewinnen, und 82,2 % beklagen unzureichende finanzielle Mittel für Cybersicherheitsmaßnahmen (Hochschulbarometer 2024, S. 36). Diese strukturellen Engpässe stehen in enger Parallelität zu den internationalen Befunden des Horizon Reports: "Institutions continue to face financial constraints and workforce gaps″(EDUCAUSE 2024, S. 13) und deuten auf eine systemische Ressourcenproblematik im Hochschulsektor hin.

Auch im US-amerikanischen Hochschulsystem sind Ressourcenengpässe ein gravierendes Problem. 68 % der CTOs geben an, dass ihre Hochschule Schwierigkeiten hat, neue

IT-Mitarbeitende einzustellen, und 40 % berichten von Problemen bei der Bindung bereits vorhandener Fachkräfte (Inside Higher Ed 2024, S. 26). Als Hauptgrund nennen 86 % der CTOs die attraktiveren Gehalts- und Arbeitsbedingungen außerhalb der Hochschulen. Weitere Faktoren wie unzureichende Investitionen in die IT-Infrastruktur (40 %) und fehlende flexible Arbeitsmodelle (24 %) verschärfen die Situation zusätzlich (ebd.).

Der internationale Vergleich zeigt damit deutlich: Sowohl in Deutschland als auch in den USA leidet die Cybersicherheit an Hochschulen unter einem Mangel an qualifiziertem Personal und finanziellen Ressourcen. Während in Deutschland zudem der allgemeine politische Rahmen als unzureichend bewertet wird, ringen die US-Hochschulen trotz besserer struktureller Einbindung der CTOs mit ähnlichen personal- und ressourcenbezogenen Herausforderungen. Die Ressourcenproblematik stellt somit ein systemisches und länderübergreifendes Risiko für die nachhaltige Sicherung der digitalen Infrastruktur im Wissenschaftsbereich dar.

11.9. Weitere Befunde

Auch die politischen Rahmenbedingungen werden von den deutschen Hochschulen kritisch bewertet. Nur 3,8 % der Befragten zeigen sich zufrieden mit den Vorgaben und der Unterstützung aus der Politik, während 43,5 % explizit Unzufriedenheit äußern (Hochschulbarometer 2024, S. 36). Damit spiegeln sich Defizite in der politischen Steuerung und Förderung digitaler Sicherheit wider, die auch vom Wissenschaftsrat auf strategischer Ebene thematisiert wurden.

In der Inside Higher Ed CTO/CIO Survey 2024 wird die politische Steuerung hingegen nicht explizit adressiert. Indirekt lassen sich jedoch Hinweise auf strategische Defizite erkennen: Nur 12 % der befragten CTOs berichten, dass ihre Hochschule über eine umfassende Policy zur Sicherheit beim Einsatz von Künstlicher Intelligenz verfügt (Inside Higher Ed 2024, S. 20). Über die Hälfte der CTOs gibt an, dass es keine institutionellen Richtlinien zur Nutzung neuer Technologien gibt. Zudem beklagen viele CTOs einen fehlenden systemweiten strategischen Ansatz zur Risikosteuerung im Bereich generativer KI und Cloud-Technologien. Diese Befunde beziehen sich jedoch auf interne institutionelle Strategien und lassen keine direkten Rückschlüsse auf politische Rahmenbedingungen im weiteren Sinne zu.

Im Bereich der technologischen Abhängigkeiten und der digitalen Souveränität zeigt sich in beiden Ländern Handlungsbedarf. Während in Deutschland Datenschutzkonformität

(60,8 %) und Interoperabilität (48,3 %) bei der Beschaffung digitaler Technologien hohe Priorität genießen, spielt die Nutzung von Open-Source-Lösungen mit lediglich 12 % eine untergeordnete Rolle (Hochschulbarometer 2024, S. 36). In den USA wird Open Source in der IHE CTO/CIO Survey überhaupt nicht explizit thematisiert, was auf eine noch geringere strategische Priorisierung souveräner Technologien schließen lässt. Stattdessen setzen US-Hochschulen stark auf Kooperationen mit kommerziellen Technologieunternehmen: 20 % der CTOs berichten von aktiven Partnerschaften zur Implementierung von KI-Technologien, und weitere 32 % prüfen eine solche Zusammenarbeit (ebd.).

Insgesamt zeigt die vergleichende Analyse, dass in beiden Ländern ein Spannungsverhältnis zwischen kurzfristigem Effizienzgewinn durch den Rückgriff auf externe Technologien und langfristiger Sicherung digitaler Souveränität besteht. Der fehlende Fokus auf Open-Source-Alternativen und die starke Abhängigkeit von kommerziellen Anbietern könnten die technologische Selbstbestimmung der Hochschulen auf Dauer erheblich beeinträchtigen.

11.10. Zwischenfazit Institutionelle Wahrnehmung und Umsetzung

Die vergleichende Analyse des Hochschulbarometers 2024 und der Inside Higher Ed CTO/CIO Survey 2024 zeigt deutlich, dass Cybersicherheit an Hochschulen sowohl in Deutschland als auch in den USA als zentrale Herausforderung wahrgenommen wird.

Beide Surveys verdeutlichen eine hohe Bedrohungssensibilität und eine deutliche Diskrepanz zwischen Bedrohungswahrnehmung und tatsächlicher Schutzfähigkeit. Trotz unterschiedlicher Rollen der Befragten – strategische Leitungsebene in Deutschland, operative-strategische Fachverantwortliche in den USA – bestätigt sich diese Tendenz.

Technische Schutzmaßnahmen wie Updates und Multi-Faktor-Authentifizierung sind verbreitet, kulturelle Maßnahmen wie Awareness-Schulungen bleiben jedoch international schwach ausgeprägt. Auch im Bereich der Krisenresilienz zeigt sich, dass reaktive Maßnahmen dominieren, während präventive Strategien unterentwickelt sind.

Governance-Strukturen sind unterschiedlich ausgeprägt, bleiben aber in beiden Systemen hinter den Anforderungen an eine strategische Integration von Cybersicherheit zurück. Die Ressourcenproblematik erweist sich als internationales Phänomen, das unabhängig von nationalen Kontexten die Umsetzung erschwert.

Politische Steuerung und technologische Souveränität bleiben sowohl in Deutschland als auch in den USA Herausforderungen. Kooperationen mit externen Anbietern werden zwar intensiviert, könnten langfristig jedoch technologische Abhängigkeiten verstärken.

11.11. Synthese: Diskrepanz zwischen strategischem Anspruch und institutioneller Realität

Während die analysierten Quellen wertvolle Einblicke in die aktuellen Herausforderungen der Cybersicherheit im Wissenschaftssystem liefern, bleibt die Berücksichtigung jüngster politischer Umbrüche – etwa eine stärkere Fragmentierungstendenz internationaler Kooperationen, teils auch ausgehend von den USA – bislang weitgehend aus. Diese analytische Leerstelle muss in zukünftigen wissenschaftspolitischen Reflexionen stärker adressiert werden.

Die vergleichende Analyse der Empfehlungen des Wissenschaftsrats (2023), des EDUCAUSE Horizon Reports (2024), der empirischen Befunde des Hochschulbarometers (2024) sowie der Inside Higher Ed CTO/CIO Survey (2024) ermöglicht es, wissenschaftspolitische, technologische, institutionelle und operative Perspektiven auf die gewählten Spannungsverhältnisse systematisch gegenüberzustellen.

Unabhängig von methodischer Herangehensweise und regionalem Fokus identifizieren alle vier Quellen Cybersicherheit als strategische Daueraufgabe für Wissenschaftseinrichtungen. Sowohl auf nationaler als auch auf internationaler Ebene wird betont, dass Hochschulen eigenständige Cybersicherheitsstrategien entwickeln müssen, die über rein technische Schutzmaßnahmen hinausgehen. Die Themenfelder digitale Souveränität**,** IT-Sicherheitsanforderungen**,** technologische Abhängigkeiten**,** Ressourcenausstattung sowie das Spannungsverhältnis zwischen Offenheit und Sicherheit durchziehen die Analysen als zentrale Spannungsfelder.

Besonders auffällig ist die Übereinstimmung in der Diagnose struktureller Defizite: Der Mangel an qualifiziertem IT-Personal**,** unzureichende finanzielle Mittel und fehlende strategische Verankerung auf Leitungsebene werden in allen Quellen als wesentliche Herausforderungen benannt. Diese systemische Ressourcenproblematik erweist sich damit als globales Phänomen im Hochschulsektor – unabhängig davon, ob strategische Leitungen oder operative Fachverantwortliche befragt wurden.

Trotz unterschiedlicher Befragtengruppen – Hochschulleitungen in Deutschland, CTOs in den USA – bestätigen die Befunde eine hohe Bedrohungswahrnehmung und eine gleichzeitig als unzureichend empfundene Schutzfähigkeit. Die methodische Differenz der Erhebungen beeinflusst die grundsätzlichen Problemdiagnosen nur marginal.

Unterschiedliche Akzentsetzungen

Trotz dieser Übereinstimmungen setzen die Quellen unterschiedliche Schwerpunkte:

- Der **Wissenschaftsrat** als wissenschaftspolitisches Beratungsgremium verfolgt eine **strategisch-normative Perspektive** und betont die **digitale Souveränität** und die **epistemische Integrität der Wissenschaft** als zentrale Schutzgüter.
- Der **EDUCAUSE Horizon Report** fokussiert auf **technologische Trends**, insbesondere die Auswirkungen von **Künstlicher Intelligenz**, Datenschutzanforderungen und die zunehmende Komplexität der Bedrohungslage. Seine Szenarien sind innovativ, aber in Teilen spekulativ und methodisch weniger belastbar.
- Das **Hochschulbarometer** dokumentiert die **institutionelle Umsetzungsrealität** deutscher Hochschulen anhand der Wahrnehmung von Hochschulleitungen und zeigt Diskrepanzen zwischen Problemwahrnehmung und konkreter Maßnahmenumsetzung auf.
- Die **Inside Higher Ed CTO/CIO Survey** erweitert das Bild um eine **operative Perspektive**: Trotz der Einbindung der CTOs auf Leitungsebene offenbaren sich gravierende Defizite bei Schulungsmaßnahmen, Krisenresilienz und AI-Sicherheitsrichtlinien.

Damit entsteht ein vielschichtiges Bild: **Strategische Leitbilder** (Wissenschaftsrat), **technologische Zukunftsszenarien** (Horizon), **institutionelle Governance-Daten** (Hochschulbarometer) und **operative Realisierungen** (IHE CTO/CIO Survey) ergänzen sich zu einer umfassenden Problemanalyse.

Reflektion der Spannungsverhältnisse auf der Mesoebene

Die Reflexion globaler Dynamiken und geopolitischer Veränderungen fällt unterschiedlich aus. Der **Wissenschaftsrat** verweist explizit auf die Bedrohung der wissenschaftlichen Kooperationen durch zunehmende geopolitische Spannungen, insbesondere im Kontext digitaler Technologien. Der **Horizon Report** betont technologische Innovationen als Chance, reflektiert politische Verschiebungen jedoch nur implizit in seinen Szenarien.

Das **Hochschulbarometer** bleibt stärker auf die nationale Bedrohungswahrnehmung fokussiert und berücksichtigt globale Dynamiken kaum. Die **IHE CTO/CIO Survey** dokumentiert eine wachsende technologische Abhängigkeit von externen Anbietern, deutet jedoch ebenfalls nicht explizit auf geopolitische Risiken hin.

Sollte sich der abzeichnende Wandel zu einer verstärkten Fragmentierung und Abschottung internationaler Wissenschaftskooperationen nicht nur ausgehend von klassischen Akteuren wie China oder Russland, sondern zunehmend auch von den Vereinigten Staaten realisieren, würde der Handlungsdruck auf das Wissenschaftssystem erheblich steigen. Künftige Strategien müssen daher stärker als bisher geopolitische Risiken systematisch in die Cybersicherheitsplanung integrieren.

Zusammenfassung

Die qualitative Synthese zeigt, dass technologische Umbrüche und politischer Anpassungsdruck zentrale Triebkräfte für die Re-Definition von Cybersicherheit und digitaler Souveränität im Wissenschaftssystem darstellen. Trotz unterschiedlicher Perspektiven weisen die analysierten Quellen eine hohe Kohärenz in der Diagnose struktureller Defizite auf.

Zugleich wird deutlich, dass bisherige wissenschaftspolitische Reflexionen globale makrostrukturelle Veränderungen nur unzureichend berücksichtigen. Eine umfassende Strategie für Cybersicherheit in der Wissenschaft muss künftig stärker:

- funktionale Differenzierungen des Wissenschaftssystems (Leitung vs. operative Ebene),
- technologische Innovationsdynamiken
- sowie geopolitische Verschiebungen

in Einklang bringen. Die Analyse zeigt, dass sich auf der Meso-Ebene präzisierte emergente Spannungsverhältnisse herausbilden, die die in Kapitel 9 entwickelten Pole funktional erweitern. So wird aus dem Steuerungsparadox auf Makroebene ein Koordinationsdefizit im System aus Mesoebene. Strukturelle Ambivalenzen werden erkannt und adressiert – sind aber nicht vollende produktiv bearbeitbar. Die Mesoebene bleibt zwischen Anspruch und Realität blockiert. Zentral werden auch die Überwindung struktureller Ressourcenengpässe und die konsequente strategische Verankerung von Cybersicherheitsfragen in den Governance-Strukturen der Hochschulen.

12. Mikroanalyse Cybersicherheit an Hochschulen

Kapitel 12 untersucht die institutionelle Umsetzung von Cybersicherheit an Hochschulen – also auf der Mikroebene des dreistufigen Analysemodells. Im Sinne der analytischen Generalisierung (Yin 2018) wird ein theoriebasierter Blick auf konkrete Umsetzungspraxen geworfen, um die Wirksamkeit strategischer Steuerungsansätze (Kapitel 11) im Hochschulkontext zu überprüfen. Dazu wird ein Mixed-Method-Ansatz verfolgt: normativ-strategische Dokumentenanalyse (NIS2, IT-Grundschutzprofil), qualitative Fallstudienauswertung (Bayern) sowie explorative Nutzung vertraulicher Auditdaten (HITS IS 2025). Die Analyse wird entlang der in Kapitel 9 entwickelten Spannungsverhältnisse gespiegelt, um institutionelle Handlungsmöglichkeiten und Blockaden zu identifizieren.

Die institutionelle Umsetzung von Cybersicherheit lässt sich nicht unabhängig von ihren übergeordneten Steuerungs- und Rahmenbedingungen analysieren. Während Kapitel 11 die politisch-strategischen Zielsetzungen auf Mesoebene im nationalen und internationalen Kontext beleuchtet hat, richtet sich der Blick nun auf die Mikroebene – konkret auf die Umsetzung an Hochschulen in Deutschland.

Um diese empirische Analyse fundiert einzuordnen, werden zunächst zentrale regulatorische und normative Vorgaben dargestellt, die den institutionellen Handlungsrahmen maßgeblich prägen. Dazu zählen insbesondere die europäische NIS2-Richtlinie, welche die nationale IT-Sicherheitsgesetzgebung deutlich erweitert hat, das bundesweit gültige IT-Grundschutzprofil für Hochschulen sowie ausgewählte föderale Steuerungsinstrumente – am Beispiel des Freistaats Bayern.

Diese Kontextualisierung schafft die notwendige analytische Brücke zwischen normativen Erwartungen, strategischer Steuerung und der institutionellen Praxis.

12.1. Analyse ausgewählter Strategiekonzepte

Zur systematischen Kontextualisierung der Mikroanalyse wurden drei unterschiedliche Konzepte ausgewählt, die exemplarisch verschiedene Ebenen der Cybersicherheitsanforderungen an Hochschulen abbilden. Die Auswahl folgt den Kriterien **Relevanz, Repräsentativität** und **Diversität der Perspektiven**, um sowohl die strategisch-normative Rahmung als auch die konkrete Umsetzung institutionell greifbar zu machen:

- **Erstens:** Die **NIS2-Richtlinie** der Europäischen Union (EU 2022) bildet den aktuellen europäischen Rahmen für Cybersicherheit. Sie adressiert Hochschulen potenzielle als Betreiber kritischer Einrichtungen und verankert sie damit strategisch im europäischen Sicherheitsdiskurs.
- **Zweitens:** Das **IT-Grundschutzprofil für Hochschulen** (ZKI 2022) fungiert als nationales Instrument zur Standardisierung operativer Cybersicherheitsstrukturen im Hochschulkontext. Es konkretisiert Anforderungen des BSI IT-Grundschutzes für den Hochschulkontext und operationalisiert Sicherheitsziele für Lehre, Forschung und Verwaltung.
- **Drittens:** Im Rahmen einer **Fallstudie** wird die Entwicklung hochschulübergreifender Sicherheitsstrukturen in Bayern untersucht. Der Fokus liegt auf Programmen wie dem Hochschulinformationssicherheitsprogramm (**HISP**), dem Dienstleisterverbund **HITS IS** sowie dem **Digitalverbund Bayern**. Diese bieten Einblicke in die praktische Umsetzung auf Landesebene.

Durch die Kombination dieser drei Perspektiven wird eine mehrdimensionale Analyse möglich: Die strategische Rahmensetzung (NIS2), die standardisierte operative Umsetzung (IT-Grundschutzprofil) und die konkrete institutionelle Praxis (Fallstudie Bayern) werden systematisch miteinander verknüpft und kritisch reflektiert. So entsteht ein konsistentes Bild der strukturellen Spannungsverhältnisse zwischen regulatorischem Anspruch und institutioneller Realität im Hochschulbereich.

12.2. NIS2-Richtlinie (EU 2022)

Die Richtlinie (EU) 2022/2555 (NIS2) bildet den neuen europäischen Rahmen für Mindestanforderungen an die Cybersicherheit. Forschungseinrichtungen werden darin ausdrücklich als potenziell kritische Akteure benannt, da sie zentrale Funktionen in sensiblen Wertschöpfungsketten übernehmen:

„Forschungstätigkeiten spielen eine Schlüsselrolle bei der Entwicklung neuer Produkte und Prozesse [...] Diese Einrichtungen können daher wichtige Akteure in Wertschöpfungsketten sein, was die Sicherheit ihrer Netz- und Informationssysteme zu einem entscheidenden Faktor für die Cybersicherheit des Binnenmarkts macht.“ (NIS2 2022, S. 8–9)

Darüber hinaus fordert die Richtlinie, dass Mitgliedstaaten Forschung und Entwicklung im Bereich innovativer Cybersicherheitstechnologien – insbesondere im Kontext automatisierter Systeme und künstlicher Intelligenz – gezielt fördern: „Die Mitgliedstaaten sollten Tätigkeiten im Bereich Forschung und Entwicklung fördern [...] insbesondere solcher, die sich auf automatisierte oder halbautomatisierte Instrumente beziehen“ (ebd., S. 11). NIS2 adressiert damit nicht nur die Absicherung bestehender Infrastrukturen, sondern begreift

Hochschulen als aktive Akteure eines europäischen Sicherheitsökosystems. Einrichtungen sollen Risiken aus Forschungskooperationen systematisch in ihre Cybersicherheitsstrategien integrieren: „Wesentliche und wichtige Einrichtungen sollten sicherstellen, dass ihre Zusammenarbeit mit Hochschul- und Forschungseinrichtungen ihrer Cybersicherheitsstrategie entspricht [...] insbesondere hinsichtlich des Schutzes von Geschäftsgeheimnissen und geistigem Eigentum“ (ebd., S. 17).

Die Mitgliedstaaten haben zudem die Möglichkeit, Hochschulen formal in den Geltungsbereich der Richtlinie einzubeziehen: „Die Mitgliedstaaten können vorsehen, dass diese Richtlinie Anwendung findet auf [...] Bildungseinrichtungen, insbesondere wenn sie kritische Forschungstätigkeiten durchführen“ (ebd., S. 30).

In Deutschland zeichnet sich jedoch ab, dass Hochschulen davon ausgenommen werden sollen. Die für das Bildungswesen zuständigen Bundesländer planen, sie nicht als wesentliche oder wichtige Einrichtungen einzustufen – vor allem aufgrund der erwarteten Ressourcenbelastung. Diese Entscheidung wird in der Fachöffentlichkeit kritisch bewertet:

„Durch die Länder wurden die kommunalen Verwaltungen und die Hochschulen aus der NIS2-Umsetzung ausgenommen [...] Zwei besonders wichtige, aber auch besonders angreifbare Sektoren werden komplett herausgenommen“ (Schulmann, ATHENE 2024).

Obwohl die Richtlinie die strategische Bedeutung von Hochschulen für die Cybersicherheit betont, bleibt ihre Umsetzung in vielen EU-Ländern offen – insbesondere dort, wo föderale Zuständigkeiten greifen.

Zugleich ignoriert NIS2 weitgehend die spezifischen Logiken wissenschaftlicher Einrichtungen – etwa ihre Offenheit, epistemische Autonomie und internationale Vernetzung. Hochschulen erscheinen primär als funktionale Teile wirtschaftlicher Wertschöpfung. Eine differenziertere Berücksichtigung wissenschaftsspezifischer Schutzbedarfe wäre jedoch erforderlich, um den Besonderheiten des Wissenschaftssystems gerecht zu werden.

Die Analyse der NIS2-Richtlinie macht eine strukturelle Diskrepanz sichtbar zwischen dem objektiven Schutzbedarf wissenschaftlicher Einrichtungen und ihrer tatsächlichen politischen Einstufung. Daraus ergibt sich ein Spannungsverhältnis zwischen geopolitischen Erwartungen, regulatorischen Anforderungen und der institutionellen Umsetzbarkeit – wie es auch im Hochschulbarometer und im EDUCAUSE Horizon Report dokumentiert wird.

Zugleich ist in Deutschland nicht eindeutig geregelt, welche gesetzlichen Anforderungen Hochschulen in Bezug auf Cybersicherheit konkret erfüllen müssen. Die juristische Antwort darauf lautet derzeit oft: „Es kommt darauf an."
Denn:

- Hochschulen fallen nicht generell unter das IT-Sicherheitsgesetz oder NIS2,
- aber in Ausnahmefällen – etwa bei KRITIS-Betrieb – könnten einzelne Einrichtungen wie Universitätsklinikabetroffen sein.
  Diese wiederum sind oft eigenständige Körperschaften öffentlichen Rechts und somit nicht automatisch Teil der Universität im rechtlichen Sinn.

Klarer ist die Lage bei der DSGVO: Nach Art. 32 sind Verantwortliche verpflichtet, angemessene technische und organisatorische Maßnahmen (TOMs) zum Schutz personenbezogener Daten zu treffen. Diese Verpflichtung trifft alle Hochschulen, unabhängig von ihrer Trägerschaft oder Größe.

Eine weitere juristische Orientierung bietet das jeweilige Landesrecht. Für den Freistaat Bayern – als Fallstudienkontext dieser Arbeit – heißt es in Art. 43 Abs. 1 des Bayerischen Digitalgesetzes (BayDiG):

„Die Sicherheit der informationstechnischen Systeme der Behörden ist im Rahmen der Verhältnismäßigkeit sicherzustellen. Die Behörden treffen zu diesem Zweck angemessene technische, operative und organisatorische Maßnahmen und erstellen die hierzu erforderlichen Informationssicherheitskonzepte."

Da staatliche Hochschulen in der Regel als Behörden gelten, sind sie damit adressiert – allerdings ohne klare Definition, was „angemessen" konkret bedeutet. Ob dabei dieselben Maßstäbe wie für Ministerien, Polizeidienststellen oder Schulen gelten, bleibt offen.

Angesichts dieser Regelungslücken und Unschärfen kommt branchenspezifischen Standards eine zentrale Rolle zu – insbesondere dem IT-Grundschutzprofil für Hochschulen, das im folgenden Abschnitt behandelt wird. Es handelt sich dabei um eine vom ZKI-

Verbund entwickelte und vom Bundesamt für Sicherheit in der Informationstechnik (BSI) unterstützte Handreichung, die Hochschulen bei der Entwicklung standardisierter und praxistauglicher Sicherheitskonzepte unterstützt.

12.3. IT-Grundschutz-Profil für Hochschulen (ZKI 2022)

Der IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI) gilt in Deutschland als zentraler Standard für Informationssicherheit. Um Hochschulen eine praxisgerechte Umsetzung zu ermöglichen, wird direkt abgeleitet aus der IT-Grundschutz-Methodik des BSI durch den Verein Zentren für Kommunikationsverarbeitung in Forschung und Lehre (ZKI) ein spezifisches IT-Grundschutzprofil entwickelt – das in mehreren Weiterentwicklungsstufen seit 2005 in der 2022 veröffentlichten Version ausgewertet wurde.

Das Profil trägt der besonderen Struktur von Hochschulen Rechnung: dezentrale Organisation, heterogene IT-Landschaften und vielfältige Aufgaben in Forschung, Lehre und Verwaltung. Ziel ist es, die Erstellung eines Informationssicherheitskonzepts auf Basis des BSI-Grundschutzes handhabbar zu machen. „Das IT-Grundschutz-Profil soll Hochschulen wirkungsvoll dabei helfen, die Erstellung eines Informationssicherheitskonzepts auf Basis des IT-Grundschutzes handhabbar zu machen“ (ZKI 2022, S. 9).

Im Zentrum stehen typische hochschulische Kernprozesse wie Bewerbungsmanagement, Prüfungsverfahren und Studierendenverwaltung. Für diese Prozesse benennt das Profil konkrete Bausteine aus dem IT-Grundschutz-Kompendium und gibt Umsetzungshinweise. „Das IT-Grundschutz-Profil konzentriert sich auf ausgewählte, in allen Hochschulen ähnliche Kernprozesse“ (ZKI 2022, S. 9).

Die Methodik beginnt mit einer Schutzbedarfsfeststellung, gefolgt von der Modellierung eines Informationsverbunds. Nach einer Basisabsicherung erfolgt – falls nötig – eine vertiefende Risikoanalyse für besonders kritische Bereiche. Durch die Anbindung an ISO/IEC 27001 können Hochschulen zudem eine Zertifizierung auf Basis des IT-Grundschutzes anstreben.

Trotz seiner Praxisnähe bleibt das Profil nicht ohne Kritik. In der aktuellen Diskussion um NIS2 wird etwa angemerkt, dass zentrale Prinzipien wie „Zero Trust“ bislang nicht berücksichtigt werden. „Der IT-Grundschutz deckt allerdings nicht alle notwendigen Bereiche der Cybersicherheit ab. Sinnvoll wäre beispielsweise ebenso die verbindliche Umsetzung von

Zero-Trust-Prinzipien […]“ (Schulmann, ATHENE 2024). Während etwa die US-Regierung Zero-Trust-Architekturen bereits 2021 per Executive Order für ihre Behörden eingeführt hat, basiert der IT-Grundschutz weiterhin auf traditionellen Sicherheitsmodellen, die eine klare Trennung interner und externer Netzwerke voraussetzen.

Auch zentrale Zukunftsthemen wie die Rolle künstlicher Intelligenz in der Cybersicherheit bleiben im Profil unberücksichtigt. Internationale Berichte wie der EDUCAUSE Horizon Report 2024 verweisen jedoch auf die wachsende Bedeutung KI-basierter Bedrohungen, automatisierter Abwehrsysteme und deren ökologische Implikationen. Diese Dynamiken spiegeln sich im aktuellen IT-Grundschutzprofil nicht wider.

Diese fehlende Einbindung neuer Technologien birgt das Risiko, dass Hochschulen, die sich ausschließlich auf den IT-Grundschutz stützen, künftige Bedrohungen nur unzureichend antizipieren können. Angesichts der wachsenden Dynamik im Cyberraum wäre es notwendig, etablierte Modelle um adaptive, zukunftsorientierte Ansätze zu erweitern.

Zudem bleibt der IT-Grundschutz stark in einem nationalen, technisch geprägten Sicherheitsverständnis verankert. Auch wenn dies seinem Zweck entspricht, wäre es hilfreich, globale Trends wie Cyberraum-Fragmentierung, KI-basierte Angriffe oder den Bedeutungszuwachs digitaler Souveränität stärker einzubeziehen. Andernfalls besteht die Gefahr, dass Hochschulen internationale Entwicklungen verzögert wahrnehmen – und reaktiv statt strategisch handeln. BSI IT-Grundschutz, die ISO 2070X Normen, sowie die Diskussionen um neue Standards wie NIS2 bilden Basis von Frameworks, die auch den bayerischen Hochschulen vorliegen. Ausgehend davon folgt eine Fallstudie zu Umsetzung im bayerischen Hochschulsystem.

12.4. Mikroanalyse Fallbeispiel Bayern

Dieses Kapitel liefert ein Fallbeispiel zur Untersuchung institutioneller Handlungsoptionen im Spannungsfeld von Wissenschaft und Cybersicherheit. Am Beispiel des Freistaats Bayern wird aufgezeigt, wie Hochschulen kooperative Strukturen aufbauen, um ihre Resilienz im Cyberraum zu stärken – und zugleich mit den Grenzen struktureller Unterfinanzierung bei gleichzeitig ambitionierten Zielen kämpfen. Die Fallstudie veranschaulicht somit exemplarisch, dass Kooperation allein reicht nicht ausreicht, um neue geopolitische Spannungen in die Cybersicherheit zu integrieren, wenn es nicht gelingt hinreichende Ressourcen und politische Rückendeckung dafür zu gewinnen.

Bayern wurde als Untersuchungsgegenstand gewählt, weil hier eine vergleichsweise umfassende Datenlage vorliegt: Interne CIO-Dokumente, Stellungnahmen des Bayerischen Obersten Rechnungshofs (ORH), Schriftverkehr der Bayerischen Universitätenkonferenz, Präsentationsunteralgen der CIO-Runde, vertrauliche Auditberichte sowie die gesetzlich verankerten Strukturen des Digitalverbunds Bayern ermöglichen eine fundierte Analyse. Diese Quellen erlauben nicht nur einen Einblick in strategische Zielsetzungen, sondern auch eine Bewertung der tatsächlichen Umsetzung – ein zentraler Aspekt der Analyseebene „Institutional Actions“.

Ziel der Analyse ist es, aufzuzeigen, wie sich die in Kapitel 9 entwickelten Spannungsverhältnisse – etwa zwischen wissenschaftlicher Offenheit und Sicherheitsanforderungen, oder zwischen Autonomie und staatlicher Steuerung – in der Praxis konkret manifestieren. Die Fallstudie Bayern zeigt zugleich, dass diese Spannungsverhältnisse nicht nur konzeptionell, sondern insbesondere durch Ressourcenmangel operativ blockiert werden: Hochschulen können auf Bedrohungen reagieren, doch es fehlt an Mitteln, Maßnahmen wirksam umzusetzen. Die Folge ist eine strategische Lücke zwischen Anspruch und Realität.

12.5. Entwicklungslinien und strukturelle Voraussetzungen: Von der CIO-Runde zur ersten strategischen Verortung von Cybersicherheit

Die institutionelle Auseinandersetzung mit Cybersicherheit im bayerischen Hochschulsystem begann bereits im Jahr 2010 mit der Aufwertung eines losen Arbeitskreises der Rechenzentrumsleiter zur offiziellen CIO-Runde der bayerischen Universitäten. Dieses Gremium erhielt von der Universität Bayern e.V., der bayerischen Universitätenkonferenz, in der sich die Präsidentinnen und Präsidenten strategisch austauschen, sowie dem für Wissenschaft zuständigen Ministerium den Auftrag, ein strategisches IT-Konzept für die Universitäten zu erarbeiten.

In der 5. Sitzung der CIO-Runde vom 24.06.2010 tauchte erstmals das Thema IT-Sicherheit auf – allerdings noch in Form externer Hinweise: In einem Informationsschreiben regte der damalige IT-Sicherheitsbeauftragte des Freistaats Bayern, Dr. Mück, die Durchführung von Web-TÜV-Prüfungen für Internetauftritte und Penetrationstests an. Aufgrund hoher Aufwände seien diese im Hochschulbereich jedoch kaum umsetzbar, hieß es damals.

Zeitgleich wurde im selben Protokoll deutlich, dass viele Hochschulen Mühe hatten, den laufenden IT-Betrieb aufrechtzuerhalten: „Die bestehenden Mittel reichen vielerorts nicht mehr aus, um den laufenden IT-Service aufrechtzuerhalten“, so die CIOs. Die Antwort des Ministeriums verwies auf die Autonomie der Hochschulen: Jede Einrichtung müsse selbst entscheiden, welchen Stellenwert sie der IT einräume. Dieser frühe Zielkonflikt zwischen zentraler Verantwortung und dezentraler Autonomie zieht sich seither wie ein roter Faden durch die Governance-Fragen der Cybersicherheit. Im Folgenden zeichnen wir den Weg vom Web-TÜV zum aktuellen Cybersicherheitslage, ordnen diesen unserem heuristischen Rahmen zu und betten die Ergebnisse in die Gesamtanalyse ein.

Die erste gemeinsame IT-Strategie der Universitäten erschien Ende 2010. Zwar war Cybersicherheit noch nicht als eigenes Handlungsfeld benannt, doch Themen wie Identity- und Access-Management, Netzsicherheit oder Datenschutz wurden integriert. Explizit hieß es etwa: „Datentransfers im (offenen) Wissenschaftsnetz müssen vor unberechtigten Manipulationen geschützt sein“ (IT-Strategie 2010, S. 5). Die Strategie erkannte bereits damals die Heterogenität, Interdisziplinarität und Serviceorientierung der Hochschul-IT als strategische Herausforderung – Aspekte, die heute die strukturellen Rahmenbedingungen der Spannungsverhältnisse im Umgang mit Cybersicherheit wesentlich prägen.

Einen konzeptionellen Durchbruch markierte das Grundsatzpapier „Informationssicherheit an Bayerns Hochschulen“ vom Juli 2017. Darin wurde Cybersicherheit erstmals explizit als kritisches Handlungsfeld benannt. Die CIOs hielten fest: „IT-Sicherheit ist eine wichtige Grundlage für hochwertige Lehre und Forschung“ (Grundsatzpapier 2017, S. 1). Zugleich wurde die Differenzierung zwischen IT-Sicherheit und umfassender Informationssicherheit betont. Besonders prägnant war der Hinweis, dass Ressourcen für den Aufbau angemessener Sicherheitsniveaus zwar erforderlich, aber nicht vorhanden seien: „Zur Schaffung und Aufrechterhaltung eines angemessenen Informationssicherheitsniveaus sind initial und fortlaufend Ressourcen erforderlich. Diese sind aktuell nicht ausreichend vorhanden“ (Grundsatzpapier CIO 2017, S. 3).

Bereits in diesem frühen Dokument wurden Spannungsverhältnisse explizit benannt. Die Rolle der IT-Sicherheitsbeauftragten sei von einem strukturellen Interessenkonflikt geprägt: zwischen dem Anspruch auf Servicequalität und der Notwendigkeit sicherheitsorientierter Kontrolle. Auch Datenschutzbeauftragte befänden sich im Zielkonflikt: „zwischen datensparsamer Verarbeitung und der aus sicherheitsbedingten Gründen notwendigen Analyse technischer Informationen“ (ebd.).

Der politische Kontext blieb jedoch weitgehend unverändert: Eine im Jahr 2017 erstellte Ressourcenabschätzung auf Basis des BSI-Modells (Solbrig & Ennen 2014) zeigte für die elf bayerischen Universitäten einen Bedarf von über 50 Vollzeitstellen im Bereich Cybersicherheit. Eine von den Präsidentinnen und Präsidenten als politisch undurchsetzbar hohe Forderung wurde strategisch an die Staatsregierung angepasst auf zwei Stellen pro Hochschule sowie eine koordinierende Stelle auf Landesebene. Die Umsetzung dieser Forderung blieb weitgehend aus. Stattdessen wurde 2019 lediglich eine verstetigte zentrale, beratende Stabsstelle an der Hochschule Augsburg für das heute HITS IS bereitgestellt– ohne operative Zuständigkeiten und mit begrenztem Wirkungskreis.

In ihrer Stellungnahme zum Antwortschreiben des Bayerischen Staatsministeriums für Wissenschaft (damals BayStMBW) bekräftigte die CIO-Runde der Universität Bayern e.V. ihre grundsätzliche Zustimmung zu landesweiten Kooperationsansätzen, betonte jedoch mit Nachdruck die Notwendigkeit lokaler Strukturen und personeller Ressourcen:

„Insofern begrüßt die CIO-Runde ausdrücklich die Bereitschaft des BayStMBW zur Verstetigung der landesweiten Kompetenzstelle für IT-Sicherheit an Hochschulen sowie die im Antwortschreiben angedachte Etablierung zusätzlicher hochschul(art)übergreifender IT-Sicherheitsdienste durch ausgewählte zusätzliche Personalstellen. „Mit Blick auf die bereits erbrachten Eigenleistungen sind die ins Feld geführten primär universitätsinternen Stellenbewirtschaftungsmaßnahmen zur Deckung des zusätzlichen Personalbedarfs deshalb als sehr kritisch zu bewerten. Eine nachhaltige Informationssicherheit, wie gesetzlich gefordert, kann nach Meinung der CIO-Runde nur durch die Bereitstellung von zusätzlichen Personalressourcen erfolgen“ (Stellungnahme der CIO-Runde 2017).

Diese Passage zeigt deutlich: Auch aus Sicht der Universitäten selbst ist eine wirksame Cybersicherheitsstrategie ohne politische Unterstützung und gezielte Ressourcenausstattung kaum realisierbar. Die Spannungsverhältnisse zwischen Steuerung und Autonomie, zwischen Sicherheitsanspruch und struktureller Umsetzung, wurden hier bereits klar benannt – blieben jedoch in ihrer politischen Wirkung weitgehend folgenlos.

12.6. Strukturelle Verankerung: Parallelprozesse und institutionelle Verdichtung

Die bisherige Entwicklung zeigt, dass zentrale Herausforderungen im Bereich der Cybersicherheit im bayerischen Hochschulsystem bereits früh erkannt wurden. Es gelang jedoch zunächst nicht, diese dauerhaft politisch und strukturell zu verankern. Zwischen Problembewusstsein und tatsächlicher Umsetzung klaffte eine strategische Lücke. Erst das Zusammenspiel mehrerer gleichzeitig ablaufender Entwicklungsstränge führte zu einer neuen Stufe der Steuerung und institutionellen Koordination.

Vier Dimensionen waren dabei maßgeblich:

1. **Die neue IT-Strategie 2022**, die Informationssicherheit erstmals systematisch adressierte,
2. **Die ORH-Prüfung 2021** als strukturpolitischer Impuls,
3. **Die gesetzliche und institutionelle Verankerung** über das BayHIG und den Digitalverbund Bayern,
4. **Die pandemiebedingte Turbodigitalisierung**, die in kürzester Zeit neue Komplexität und Verwundbarkeiten erzeugte.

Diese Entwicklungen führten – teilweise unabhängig voneinander, teilweise gegenseitig verstärkend – zu einer strategischen Verdichtung, die den Weg für die Einführung des Hochschulinformationssicherheitsprogramms (HISP) und den Aufbau kooperativer Sicherheitsstrukturen bereitete.

1. Neue IT-Strategie als inhaltlicher Rahmen

Ende 2021 verabschiedeten die bayerischen Universitäten und Hochschulen eine neue gemeinsame IT-Strategie, die Informationssicherheit erstmals als eigenständiges strategisches Handlungsfeld adressierte. Ziel war es, die Digitalisierung der Hochschulen systematisch weiterzuentwickeln – auf Basis gemeinsamer Standards, koordinierter IT-Governance und kooperativer Serviceeinheiten. Im Kapitel „Stärkung der Informationssicherheit“ wird formuliert: „Die zunehmenden Bedrohungen der Cybersicherheit, gesetzliche Compliance-Anforderungen […] und die zunehmende Digitalisierung der Hochschullandschaft erfordern ein angemessenes Informationssicherheitsniveau an bayerischen Hochschulen“ (IT-Strategie 2022, S. 8). Dabei wird auch die strukturelle Unterfinanzierung

deutlich angesprochen: „Ein konsequenter Betrieb eines ISMS nach anerkannten Standards kann mit den in den Hochschulen vorhandenen Ressourcen zurzeit nicht erreicht werden“ (ebd.). Als strategisches Instrument wird das von der Stabsstelle IT-Sicherheit entwickelte **Hochschulinformationssicherheitsprogramm (HISP)** benannt, das innerhalb des entstehenden Digitalverbunds weitergeführt werden soll. Das Ziel lautet: „[HISP] schafft die Grundlage, an den Hochschulen […] ein für sie angemessenes Sicherheitsniveau anzustreben, gemeinsame IT-Services zur Informationsversorgung abzusichern und hinsichtlich der Informationssicherheit kontinuierlich zu beurteilen“ (ebd.). Zudem wird der Aufbau eines ganzheitlichen Notfallmanagements gefordert, unter Einbindung bestehender nationaler und bayerischer SOC-Strukturen (DFN-SOC, SOC am LRZ).

2. ORH-Prüfung als strategischer Impulsgeber

Der Bayerische Oberste Rechnungshof (ORH) veröffentlichte im Jahr 2021 eine beratende Äußerung zur Informationssicherheit an staatlichen Universitäten. Anders als viele vorangegangene Prüfungen wurde dieser Bericht von den Hochschulen nicht nur als Kritik, sondern auch als konstruktiver Impuls aufgenommen. Der Bericht stellte fest: „Die IT-Sicherheit war sehr unterschiedlich organisiert. Sieben der neun [geprüften] Universitäten hatten keinen Informationssicherheitsbeauftragten benannt. Die vom ORH festgestellten Mängel […] zeigen „Defizite bei der Informationssicherheit auf“ (ORH 2021, S. 22). Und weiter: „Der ORH hält einheitliche Vorgaben und Vorgehensweisen für erforderlich, um ein angemessenes und einheitliches Sicherheitsniveau in wirtschaftlicher Weise zu erreichen“ (ebd.). Diese Einschätzung wurde innerhalb der CIO-Runde als Bestätigung zentraler Forderungen gewertet, insbesondere hinsichtlich der Notwendigkeit verbindlicher Vorgaben, klarer Verantwortlichkeiten und zusätzlicher Ressourcen auf Landesebene.

3. Gesetzliche und institutionelle Verankerung

Die strategischen Elemente der IT-Strategie wurden 2023 institutionell abgesichert durch die Gründung des Digitalverbunds Bayern, der als hochschulübergreifendes Koordinationsnetzwerk operiert. Grundlage hierfür war das Bayerische Hochschulinnovationsgesetz (BayHIG)**,** das in Art. 5 Abs. 5 die verbindliche Zusammenarbeit der staatlichen Hochschulen im Rahmen eines Digitalverbunds vorsieht – mit besonderem Fokus auf IT-Governance, Digitalisierung und Informationssicherheit.

Die operative Ausgestaltung dieser Vorgaben erfolgt durch die Rahmenvereinbarung Hochschule 2023–2027, in der konkrete Verpflichtungen verankert sind: Die Hochschulen

müssen ISB benennen, ein ISMS gemäß HISP aufbauen, sich an Audits beteiligen. Der schrittweise weitere Aufbau von Personalressourcen nach CIO-Berechnung soll zumindest geprüft werden. Damit werden strategische Zielsetzungen mit operativen Aufgaben verknüpft – für die die zentrale Governance des Digitalverbunds auch mit Stellen verstärkt wurden. Eine dezentrale Ressourcenausstattung an den Hochschulen wurde im Unklaren gelassen, was das Spannungsverhältnis zwischen Sicherheitsanspruch und Umsetzungskapazität weiterhin erhält.

4. Turbodigitalisierung als externer Beschleuniger

Unabhängig von den oben genannten strukturellen Entwicklungen wirkte die COVID-Pandemie als externer Beschleuniger. In kürzester Zeit wurden cloudbasierte Dienste, Fernzugriffe, Homeoffice-Infrastrukturen und neue Kommunikationsplattformen flächendeckend eingeführt – häufig ohne finale und ausreichende Prüfung sicherheitsrelevanter Auswirkungen. Die funktionierenden Lösungen mussten schnell beschafft werden. Die Moderation der Spannungsverhältnisse wurde in die Zukunft verlagert. Dies führte zu einem raschen Anstieg der technologischen Komplexität, die den aktuellen Ist-Zustand bildet.

Gleichzeitig erhöhte die Pandemie den Veränderungsdruck auf politischer und administrativer Ebene. Die langfristig angelegte Digitalisierungsstrategie musste unter akuter Krisendynamik kurzfristig operative Lösungen liefern – was das Bewusstsein für Cybersicherheitsfragen deutlich schärfte. Das Thema Informationssicherheit wurde damit nicht nur inhaltlich, sondern auch kommunikativ-politisch aufgewertet. Dies hat sich in einem Aufwuchs auf 14 Haushaltsstellen für Cybersicherheit für alle staatlichen Hochschulen darunter zehn Universitäten, 17 Hochschulen für angewandte Wissenschaften (HAW) / Technische Hochschulen (TH) sowie fünf Kunsthochschulen umgemünzt. Ein Fortschritt jedoch nicht hinreichend um die Zielsetzungen zu erreichen.

Die strukturelle Steuerung der Cybersicherheit an bayerischen Hochschulen resultiert nicht aus einem singulären Impuls, sondern aus einem Mehr-Ebenen-Prozess, in dem Prüfimpulse, strategische Selbstverpflichtungen, gesetzliche Rahmensetzungen und externer Veränderungsdruck parallel wirken. Das Hochschulinformationssicherheitsprogramm (HISP) bildet in diesem Kontext die erste kohärente Operationalisierung dieser Steuerungsambitionen und soll im Folgenden kurz vorgestellt werden.

12.7. Hochschulinformationssicherheitsprogramm (HISP 2020), Konzeption und strategische Zielsetzung

Das Hochschulinformationssicherheitsprogramm (HISP) wurde im Jahr 2020 von der Stabsstelle Informationssicherheit der bayerischen Hochschulen und Universitäten entwickelt, um den strukturierten Aufbau eines Informationssicherheitsmanagementsystems (ISMS) im Hochschulkontext zu unterstützen. Ziel ist es, ein angemessenes Cybersicherheitsniveau mit vertretbarem organisatorischem Aufwand herzustellen und Hochschulen durch einen praxisnahen Ansatz handlungsfähig zu machen.

Anders als umfassende Standardwerke wie der IT-Grundschutz verfolgt das HISP einen pragmatisch-schrittweisen Ansatz. Der Aufbau eines ISMS wird in mehrere klar definierte Phasen gegliedert:

- Bestandsaufnahme (Audits),
- Erstellung einer hochschulweiten Informationssicherheitsleitlinie,
- Aufbau organisatorischer Strukturen (z.B. Informationssicherheitsbeauftragte, Gremien),
- Etablierung von Schulungs- und Kommunikationsstrukturen,
- Einführung eines systematischen Risikomanagements,
- Kontinuierliche Fortschrittskontrolle über ein Reifegradmodell.

Zentrales Steuerungsinstrument ist das HISP-Reifegradmodell, das Hochschulen entlang sechs Entwicklungsstufen (0–5) bewertet:

Reifegrad	Beschreibung
0	Fehlen von erkennbaren Richtlinien, Verfahren und Maßnahmen
1	Entwicklung gestartet, aber erheblicher Nachholbedarf
2	Arbeiten sind in Umsetzung, aber noch nicht abgeschlossen
3	Aufbau im Wesentlichen abgeschlossen, erste Implementierung erfolgt
4	Prozess vollständig etabliert und in Betrieb genommen
5	Prozess vollständig etabliert, aktiv überwacht und kontinuierlich verbessert

Abbildung 7: HISP-Reifegradmodell, gemäß HISP

Das Ziel besteht darin, bis 2027 einen Zielreifegrad von mindestens 3 an allen staatlichen Hochschulen zu erreichen. Die Umsetzung wird durch strukturierte Audits unterstützt, die vom Hochschulübergreifenden IT-Service für IT-Sicherheit (HITS IS) organisiert und auf Basis der ISO 27001 sowie ISO 27002 durchgeführt werden.

Wie weit die Umsetzung des HISP in der Praxis tatsächlich getragen und wirksam umgesetzt wurde, zeigt der aktuelle Auditbericht 2025, der im folgenden Abschnitt analysiert wird.

12.8. Empirische Bestandsaufnahme: Entwicklung der Informationssicherheit an bayerischen Hochschulen 2017–2025

Für die vorliegende Arbeit stehen neben dem offiziellen HISP-Dokument auch die internen Auditberichte des HITS IS aus den Jahren 2017 und 2025 zur Verfügung. Diese vertraulichen Erhebungen ermöglichen eine belastbare Einschätzung des Umsetzungsstandes informationssicherheitsrelevanter Maßnahmen an bayerischen Hochschulen. Alle dargestellten Ergebnisse beruhen auf aggregierten Daten, um Rückschlüsse auf einzelne Institutionen auszuschließen.

Beide Auditberichte basieren methodisch auf standardisierten Interviews, Dokumentenanalysen und Vor-Ort-Begehungen gemäß den Normen ISO 27001 und ISO 27002.

- **Auditbericht 2017**: ISMS-Bestandsaufnahme an 12 Hochschulen (9 HAWs, 3 Universitäten), März – Dezember 2017
- **Auditbericht 2025**: interne Audits an 16 Hochschulen (10 HAWs, 6 Universitäten) im Rahmen des Hochschulinformationssicherheitsprogramms (HISP), Dezember 2022 – November 2024.

Während der Bericht von 2017 primär eine initiale Bestandsaufnahme darstellt, dokumentiert der Bericht von 2025 gezielt die Wirkungen strukturierter Maßnahmenprogramme und politischer Steuerungsimpulse (z.B. Förderlinien, zentrale IT-Dienstleistungen). Die methodische Validität ergibt sich aus dieser standardisierten Vorgehensweise sowie aus der Vergleichbarkeit über die Zeit hinweg. Dies gewährleistet, dass die beobachteten Veränderungen im Bereich der Informationssicherheit auf tatsächliche Entwicklungen und nicht auf methodische Verzerrungen zurückzuführen sind.

Die Analyse der Auditergebnisse zeigt eine deutliche Heterogenität in der Entwicklung von Informationssicherheitsstrukturen. Hochschulen, die frühzeitig personelle Ressourcen für die Rolle eines Informationssicherheitsbeauftragten (ISB) bereitgestellt haben, erreichen signifikant höhere Reifegrade. Hochschulen ohne ausreichende organisatorische Strukturen verbleiben dagegen häufig auf Reifegradstufen 1 oder 2 und zeigen erhebliche Defizite insbesondere im Bereich Risikomanagement und Notfallvorsorge.

Im Bereich der organisatorischen Maßnahmen bleibt die systematische Umsetzung weitgehend unzureichend, was im Auditbericht 2025 ausdrücklich betont wird: „Die Entwicklung von organisatorischen Maßnahmen geht schleppend voran. Es wurden organisatorische Strukturen geschaffen, diese sind aber mit ungenügenden Ressourcen ausgestattet“ (HITS IS 2025, S. 4).

Hingegen konnten bei technischen Schutzmaßnahmen deutliche Fortschritte erzielt werden, insbesondere bei der Zugangskontrolle durch die Implementierung von Zwei-Faktor-Authentifizierung (MFA): „Die Zugangskontrolle hat sich, vor allem durch die Implementierung des 2. Faktors, verbessert, geht aber mit unterschiedlicher Geschwindigkeit voran“ (ebd.). Dennoch bestehen gravierende Schwächen weiterhin im Notfallmanagement sowie im Informationsfluss zur Leitungsebene: „Nur 10 % der Rechenzentren/IT-Abteilungen verfügen über dokumentierte Notfallpläne“ (HITS IS 2025, S. 5). Zudem wird kritisiert: „Wegen fehlender Berichte an die Leitungsebene ist diese über den Stand und die Entwicklung von Risiken oder der Informationssicherheit kaum informiert“ (ebd.).

Weiterhin wurde festgestellt, dass aktuelle Technologietrends wie die Einführung von Microsoft 365 und erste KI-Projekte zu einer Umlenkung von Ressourcen führen, die ursprünglich für den Ausbau der Cybersicherheitsmaßnahmen vorgesehen waren: „Anstatt die begonnene Stärkung der IT-Sicherheit fortzusetzen, werden Ressourcen abgezogen oder in anderen Bereichen (Tagesgeschäft) eingesetzt“ (ebd.).

Im Folgenden werden zunächst die Ergebnisse zur Entwicklung der Managementsysteme nach ISO 27001 dargestellt. Anschließend erfolgt eine Betrachtung konkreter Maßnahmen gemäß ISO 27002, welche die operative Umsetzung dieser Anforderungen unterstützt.

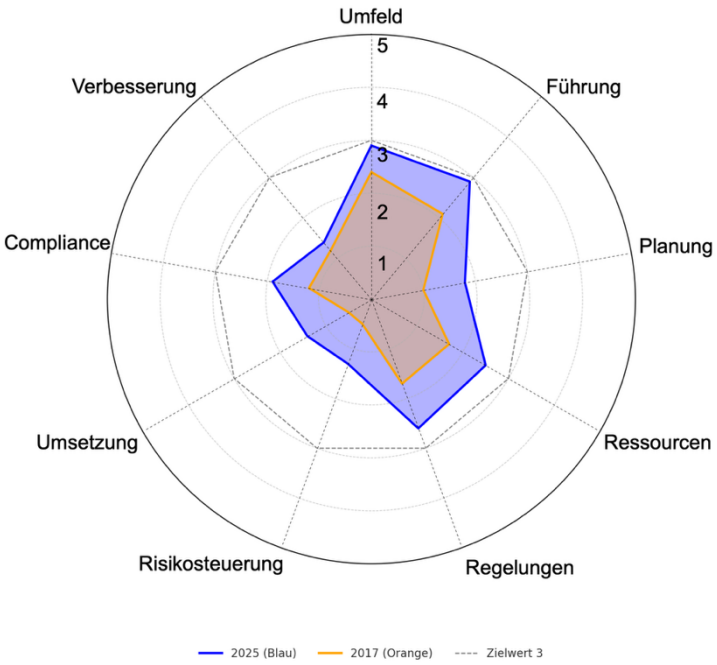

Abbildung 8: Reifegradmodell im Managementbereich (ISO 27001), 2017 und 2025

ISO 27001 definiert die Anforderungen an ein Informationssicherheitsmanagementsystem (ISMS). Im Vergleich der beiden Erhebungsjahre zeigt sich eine insgesamt positive Entwicklung der Managementsysteme. Dennoch bleiben zentrale Bereiche wie Risikomanagement und Verbesserungssysteme unterhalb des für etablierte Prozesse erforderlichen Zielwerts von Reifegrad 3.

ISO 27002 spezifiziert die konkreten Sicherheitsmaßnahmen, die zur praktischen Umsetzung der Managementsystemziele erforderlich sind. Im Audit 2025 zeigten sich besonders bei technischen Maßnahmen Fortschritte:

- **Zugangskontrollen (technisch)**: Der Einsatz von Zwei-Faktor-Authentifizierung hat zu einer signifikanten Verbesserung der technischen Zugangskontrollen geführt, häufig wurden Reifegrade über 3 erreicht.
- **Netzwerksicherheit und Schwachstellenscans**: Auch diese Maßnahmen konnten erfolgreich verbessert werden und tragen zur erhöhten technischen Resilienz bei.

Demgegenüber bleiben organisatorische Maßnahmen wie Risikomanagementprozesse und Notfallplanung stark unterentwickelt, was sich in niedrigen Reifegraden von 1,5 bis 2,5 niederschlägt:

- **Risikomanagement**: Trotz erster Ansätze bleiben diese Prozesse oft fragmentarisch und nicht vollständig integriert.
- **Notfallmanagement**: Formalisierte und dokumentierte Notfallpläne sind weiterhin selten vorhanden, was angesichts der Bedeutung für die Cybersicherheit kritisch zu bewerten ist.

Diese Diskrepanz zwischen technischer und organisatorischer Umsetzung verdeutlicht, dass technologische Maßnahmen kurzfristig durch gezielte Förderprogramme realisierbar

sind, organisatorische Veränderungen hingegen auf institutionelle Barrieren und Ressourcenengpässe stoßen und langfristige strukturelle sowie kulturelle Anpassungen erfordern.

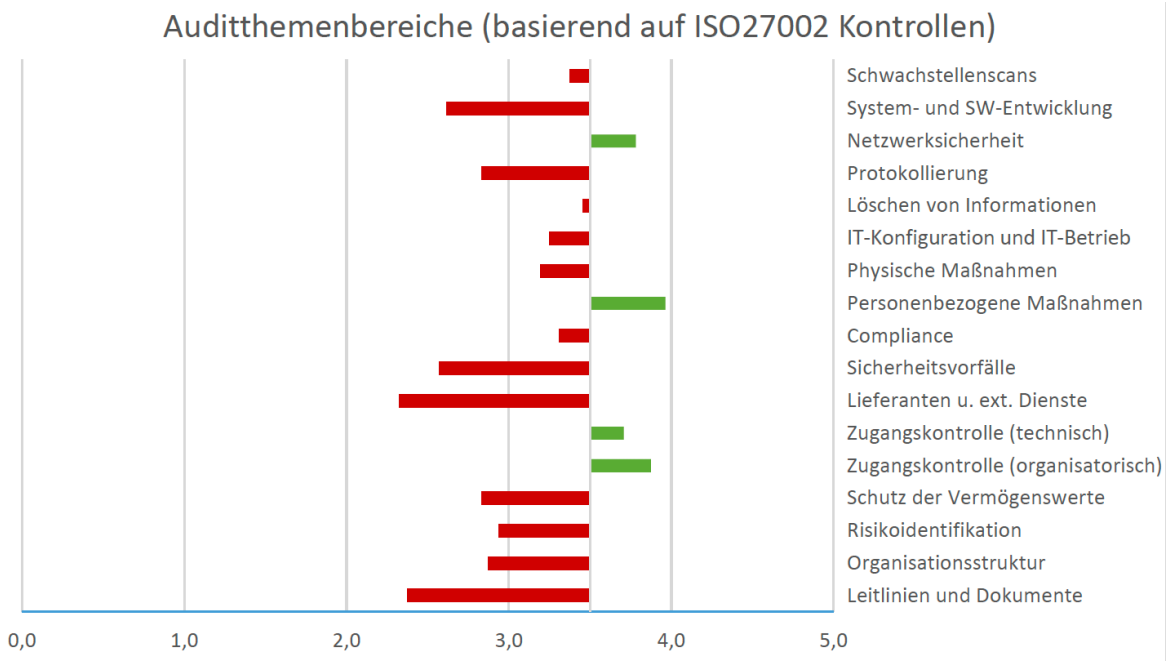

Abbildung 9: Übersicht des durchschnittlichen Reifegrads einzelner Sicherheitsmaßnahmen nach ISO27002, aus Audit Bericht 2025.

Zusammenfassend bestätigt die Analyse der Auditberichte die zentrale These dieser Arbeit: Während technische Maßnahmen noch relativ schnell implementiert werden können, verzögern institutionelle Hindernisse die organisatorische Verankerung von Sicherheitsprozessen erheblich. Dies trägt maßgeblich dazu bei, dass der durchschnittliche Reifegrad in entscheidenden Bereichen auch im Jahr 2025 unter der für ein vollständig etabliertes ISMS notwendigen Schwelle verbleibt.

12.9. Fazit: Anspruch, Umsetzung und Spannungsverhältnisse: Cybersicherheit an bayerischen Hochschulen

Die Cybersicherheit an bayerischen Hochschulen verdeutlicht ein zentrales Steuerungsdilemma: Zwischen politischen Zielsetzungen und operativer Umsetzung klafft eine strukturelle Lücke. Programme wie das Hochschulinformationssicherheitsprogramm (HISP), der Digitalverbund Bayern und die Rahmenvereinbarung 2023–2027 markieren zwar einen politischen Aufbruch – doch die Auditergebnisse von 2025 zeigen, dass viele Hochschulen hinter den formulierten Ansprüchen zurückbleiben.

Diese Diskrepanz ist nicht allein auf mangelndes Engagement der Hochschulen zurückzuführen. Sie verweist auf ein Geflecht aus unklaren Verantwortlichkeiten, institutionellen Logiken und Ressourcenengpässen – also auf Spannungen zwischen Governance, Autonomie und struktureller Befähigung. Die Fallstudie Bayern macht deutlich, an welchen systemischen Grenzen Cybersicherheitsgovernance im Hochschulbereich scheitert.

Strategische Zielsetzungen – politische Ambitionen, institutionelle Realität

Die Einführung von HISP, die IT-Strategie 2021 und der Ausbau des Digitalverbunds Bayern setzen wichtige Impulse: Cybersicherheit soll strukturell verankert werden. Die Rahmenvereinbarung 2023–2027 konkretisiert dies u. a. durch ISMS-Pflicht, Auditteilnahmen und Kooperationen. Doch die Umsetzung bleibt begrenzt. Die Audits zeigen, dass viele Hochschulen lediglich Reifegrad 1 oder 2 erreichen. Fortschritte bleiben punktuell und stark von lokaler Initiative abhängig. Politische Programme entfalten erst dann Wirkung, wenn sie mit Ressourcen, Zuständigkeiten und institutioneller Verbindlichkeit hinterlegt sind. Genau hier offenbart sich das zentrale Defizit: Die strategische Steuerung bleibt auf der Zielebene stehen.

Governance-Spannungen: Steuerung, Autonomie und Verantwortung

Das Verhältnis zwischen staatlicher Steuerung und hochschulischer Selbstverwaltung zeigt sich widersprüchlich: Zwar existieren gesetzliche Vorgaben, doch operative Verantwortung liegt bei den Hochschulen. Zusätzliche Mittel werden nur begrenzt bereitgestellt – vorrangig für zentrale Unterstützungsstrukturen, nicht für eine flächendeckende Ausstattung.
Hochschulen verfügen formal über Autonomie, stoßen aber im Bereich Cybersicherheit an klare Grenzen. Wo keine Zuständigkeiten definiert und keine ISB-Stellen geschaffen wurden, bleiben Fortschritte aus. Daraus ergibt sich das Konzept der **negativen Autonomie**: Autonomie wird nicht als Gestaltungsrahmen genutzt, sondern als politische Rückzugsstrategie. Verantwortung wird delegiert – ohne Befähigung.

Ressourcen als struktureller Engpass

Die größte Schwachstelle bleibt die unzureichende Ressourcenausstattung. Schon 2017 warnte die CIO-Runde, dass Informationssicherheit ohne zusätzliches Personal nicht zu

leisten sei. Prüfberichte wie die des ORH stützen diese Einschätzung. Bis heute beschränken sich Maßnahmen auf zentrale Stabsstellen, Einzelförderungen und einige hochschulübergreifende Dienste.

Die Audits von 2025 zeigen: Fortschritte gelingen nur dort, wo ISB-Stellen institutionell verankert sind, wo klare örtliche Zuständigkeiten und Kompetenzen aufgebaut sind. Ansonsten bleibt Cybersicherheit eine Zusatzaufgabe – getragen von überlastetem Personal. Es handelt sich nicht um ein punktuelles Problem, sondern um einen strukturellen Mangel, der die Umsetzung systematisch hemmt.

Reaktives Handeln und strategische Lücke

Die Pandemie hat gezeigt, wie schnell Hochschulen Innovationen in der Digitalisierung adaptieren können – mit virtueller Lehre, hybriden Formaten, Cloudlösungen und KI. Doch diese Dynamik wurde nicht mit entsprechender Sicherheitsarchitektur begleitet. Statt strategischer Planung dominieren reaktive Maßnahmen, oft ausgelöst durch Vorfälle oder externe Prüfungen. Diese Reaktivität führt zu dauerhaft niedrigen Sicherheitsniveaus. Gleichzeitig wächst die Bedrohungslage durch neue Technologien und globale Angriffsvektoren. Hochschulen sollen Innovationstreiber sein, operieren aber vielfach mit basalen Sicherheitskonzepten. Diese Kluft ist nicht nur organisatorisch, sondern strategisch gefährlich.

Spannungsverhältnisse als Blockadepotenzial

Die Fallstudie Bayern zeigt, wie sich strukturelle Spannungsverhältnisse praktisch auswirken. Theoretisch rekonstruierte Gegensätze – zwischen Anspruch und Realität, zwischen Steuerung und Autonomie, zwischen Innovation und Risiko – werden operativ sichtbar. Besonders prägnant wird dies im Konzept der **negativen Autonomie**: Hochschulen sind formal verantwortlich, jedoch strukturell unterversorgt.

Auch die auf Kooperation setzende Governance-Architektur stößt an Grenzen, wenn Verbindlichkeit und Ressourcen fehlen. Cybersicherheitsgovernance ist kein technisches Detail, sondern ein Ausdruck systemischer Spannungen im Verhältnis von Staat und Wissenschaft. Solange diese nicht strategisch bearbeitet und strukturell unterfüttert werden, bleibt die digitale Resilienz der Hochschulen prekär.

12.10. Politische Strategien im föderalen Vergleich, Anschlussfähigkeit über Bayern hinaus, Verbundlogiken und föderale Strategien

Obwohl die vorliegende Mikroanalyse am Beispiel des Freistaats Bayern bewusst auf einen datenreichen Einzelkontext fokussiert, ist sie nicht isoliert zu verstehen. Vielmehr erlaubt sie – unter methodischer Vorsicht – eine analytische Öffnung: Denn zentrale Spannungsverhältnisse, wie sie in Kapitel 9 theoretisch entwickelt und in Kapitel 12 empirisch aufgezeigt wurden, zeigen sich auch in anderen Bundesländern – wenn auch unter unterschiedlichen institutionellen und politischen Bedingungen.

Der Aufbau hochschulübergreifender Kooperationsstrukturen zur Cybersicherheit lässt sich mittlerweile in mehreren Ländern beobachten – mit teils beachtlicher institutioneller Tiefe. Dabei kristallisiert sich ein wiederkehrendes Grundmuster heraus: Netzwerke wie der **Digitalverbund Bayern** (IT-Strategie 2022), die **Digitale Hochschule NRW** (DH.NRW 2025), die **Cybersicherheitsagentur Baden-Württemberg** (Cybersicherheit-BW 2025) oder **Hochschule.digital Niedersachsen** (Landeshochschulkonferenz Niedersachsen 2024) übernehmen koordinierende Funktionen.

Sie dienen dazu, Fragmentierung zu überwinden, Sicherheitsstandards hochschulübergreifend zu operationalisieren und Wissenstransfer zu erleichtern. Ihre Aufgaben reichen dabei von Sensibilisierung und Schulung über technische Audits und Beratung bis hin zur Entwicklung gemeinsamer Sicherheitsstrategien und Standards.
Trotz dieser funktionalen Ähnlichkeit unterscheiden sich die Strukturen in rechtlicher, finanzieller und politischer Hinsicht deutlich.

Während in **Nordrhein-Westfalen** mit der *Vereinbarung zur Cybersicherheit (VzC)* erstmals rechtlich verbindliche Anforderungen zur Einführung von ISMS formuliert wurden (DH.NRW 2025), verfolgt **Bayern** eher einen kooperativen Pfad mit einer IT-Strategie, Rahmenvereinbarungen und Hochschulverträgen – ohne verbindliche Vorgaben oder garantierte Ressourcenzuweisung. **Baden-Württemberg** geht einen intermediären Weg: Dort wird die Koordination über die **CSBW (Cybersicherheitsagentur BW)** sowie das Netzwerk Informationssicherheit abgesichert, verbunden mit Elementen strategischer Steuerung durch den Hochschulfinanzierungsvertrag (Land BW 2025). In **Niedersachsen**

zeigt sich ein stärker projektbasierter Ansatz – Hochschulsicherheit wird primär über befristete Programme wie *Hochschule.digital Niedersachsen* und Sonderbudgets gefördert (LHK Niedersachsen 2024), ohne fest etablierte Koordinationsstrukturen.

Diese föderalen Unterschiede zeigen deutlich, dass die in Bayern untersuchten Spannungsverhältnisse nicht spezifisch oder exklusiv, sondern strukturell angelegt sind – und sich auch in anderen Landesstrategien widerspiegeln. Der föderale Vergleich dient daher nicht der Generalisierung im engeren Sinne, sondern der **Validierung analytischer Muster**: Er zeigt, dass viele institutionelle Reibungslinien, wie sie in Bayern exemplarisch sichtbar wurden – etwa zwischen Anspruch und Umsetzung, zwischen Autonomie und Steuerung, zwischen Ressourcenzuschnitt und Governance-Architektur – bundesweit von Relevanz sind.

12.11. Bayerns Cybersicherheit in der Wissenschaft im föderalen Vergleich

Die identifizierte strukturelle Lücke in Bayern – das Fehlen verbindlich unterlegter personeller Ressourcen für dezentrale Umsetzung – stellt sich im föderalen Vergleich als entscheidende Differenzlinie dar.

In Nordrhein-Westfalen sind mit der VzC neben den strategischen Zielsetzungen auch 66 feste Stellen sowie 30 Millionen Euro für befristete Maßnahmen und externe Beratung bereitgestellt worden (Digitale Hochschule NRW 2025). Die Hochschulen verpflichten sich im Gegenzug zur Einführung von ISMS nach internationalen Standards. In Baden-Württemberg wurden bereits im Haushalt 2020/2021 58 Stellen für Informationssicherheit eingeplant und über den Hochschulfinanzierungsvertrag III fortgeführt – mit der Option, diese später in die Hochschulhaushalte zu überführen und damit zu verstetigen (Land Baden-Württemberg 2025). Niedersachsen stellt über ein Sonderprogramm einmalig 10 Millionen Euro für Cybersicherheitsmaßnahmen zur Verfügung (Landeshochschulkonferenz Niedersachsen 2024), ohne auf Personalstellen einzugehen.

Bayern bleibt dagegen auf zentral koordinierte Maßnahmen und die freiwillige Ausstattung der Hochschulen angewiesen. Die ursprünglich von den CIOs vorgeschlagenen 50,5 Stellen, die im Vergleich mit den anderen zwei großen Flächenländern auch in einem ähnlichen Umfang dort zu Verfügung gestellt sind, wurden politisch nie durchgesetzt (Universi-

tät Bayern e.V. 2017a). Aktuell sind 14 Stellen unterschiedlicher Wertigkeit in Bayern bereitgestellt.[5] Die vorhandenen Stellen beim HITS IS sind verstetigt, reichen – belegt durch den Auditbericht – aber nicht aus, um eine flächendeckende Umsetzung und damit Erreichung der Ziele mit einem Gesamtreifegraf von mindestens 3 nach HISP zu gewährleisten. Damit wird deutlich: Bayern hat das strukturelle Problem früh sichtbar gemacht – andere Länder haben daraus politisch-operative bessere Konsequenzen gezogen.

12.12. Fazit Mikroanalyse: Zwischen Erwartungsdruck und struktureller Ohnmacht

Die Analyse der Mikroebene leistet einen zentralen Beitrag zur Beantwortung der Forschungsfrage: Sie zeigt, wie sich die in Kapitel 9 entwickelten Spannungsverhältnisse auf der operativen Ebene der Hochschulen konkret materialisieren. Die strukturellen Defizite in der Cybersicherheitsgovernance lassen sich nicht als rein technische oder organisatorische Probleme verstehen, sondern sind Ausdruck systemischer Zielkonflikte im Verhältnis von politischer Steuerung, wissenschaftlicher Autonomie und institutioneller Befähigung.

Im Spannungsfeld **Offenheit vs. Sicherheit** zeigt sich exemplarisch, wie stark wissenschaftliche Innovationsfähigkeit – etwa während der pandemiebedingten Digitalisierung – mit strukturellen Sicherheitsdefiziten kollidiert. Hochschulen agieren als hochdynamische Innovationsökosysteme, in denen neue Technologien oft schneller eingeführt werden, als flankierende Schutzmaßnahmen etabliert werden können. Genau diese zeitliche Entkopplung verstärkt auf der Makroebene den Eindruck, Offenheit sei ein Risiko, nicht – wie im Wissenschaftssystem eigentlich erforderlich – eine Ermöglichungsbedingung. Der politische Diskurs neigt damit dazu, Offenheit sicherheitspolitisch zu problematisieren, anstatt sie als strukturelle Grundlage wissenschaftlicher Entwicklung zu verstehen.

Das Spannungsverhältnis **digitale Souveränität vs. technologische Abhängigkeit** verdeutlicht, dass strategische Begriffe wie Souveränität in vielen Hochschulstrategien zwar präsent sind, institutionell jedoch noch kaum operationalisiert werden. Dies ändert sich aber zunehmend nicht nur aus politischen, sondern auch aus organisatorischen Gründen. Der Umgang mit Plattformen wie Microsoft 365 wird zu einer Gretchenfrage, die nur durch wirksames Risikomanagement aufgelöst werden könnte. Dieses ist vielerorts aber nicht

[5] Gemäß Auskunft des Digitalverbunds.

etabliert, wodurch die Souveränität zur normativen Rhetorik ohne reale Handlungsfähigkeit verkommt. Im schlechten Fall werden Systementscheidungen aus reiner Pragmatik getroffen, „weil´s funktioniert“ und nicht als balancierte Entscheidung unterschiedlicher Faktoren.

Im Zentrum steht das Spannungsverhältnis **Autonomie vs. politische Steuerung**. Auf der Makroebene erfährt die Wissenschaft eine zunehmend machtpolitische Aufladung: Sie soll technologische Souveränität sichern, digitale Schlüsseltechnologien bereitstellen und globale Wettbewerbsfähigkeit stützen. Es vollzieht sich eine **Hochrüstung der Erwartungen** an die Wissenschaft – oft ohne politische Rückkopplung mit ihren institutionellen Möglichkeiten. Auf der Mikroebene begegnet die Politik dieser Erwartungslogik mit Verweis auf Autonomie und Eigenverantwortung – und damit mit einer **Fahnenflucht der Verantwortung**. Hochschulen bleiben Adressaten strategischer Programme, ohne dass ihre Umsetzungsfähigkeit gesichert wäre. Vor diesem Hintergrund wird **negative Autonomie** als analytischer Begriff greifbar: Sie bezeichnet eine Konstellation, in der Autonomie nicht zur Gestaltung, sondern zur Verantwortungsabwälzung genutzt wird. Was nach Freiheit klingt, ist faktisch Überforderung.

Kooperation vs. Fragmentierung zeigt sich auf Mikro- und Makroebene in grundverschiedener Gestalt – und das ist für die Gesamtanalyse zentral. Während auf der Makroebene Kooperation als Prinzip internationaler Wissenschaft unter geopolitischen und sicherheitspolitischen Vorbehalten verhandelt wird, tritt Fragmentierung dort als strategische Entkopplung, Exportkontrolle und diskursive Delegitimierung globaler Partnerschaften auf. Nationale Strategien produzieren damit eine funktionale Ambivalenz: Sie erwarten internationale Offenheit, implementieren aber gleichzeitig Kontrollregime, die Kooperation erschweren.

Demgegenüber bedeutet Fragmentierung auf der Mikroebene: fehlende institutionelle Verbindlichkeit, projektbasierte Strukturen, personelle Unterausstattung – also ein Zustand, in dem Kooperation zwar organisatorisch initiiert, aber strukturell nicht getragen wird. Der Digitalverbund Bayern oder CIO-Runden zeigen exemplarisch, dass Zusammenarbeit zwar angestrebt wird, aber ohne Governance, Ressourcen und Verbindlichkeit nicht bis in die Umsetzungsebne trägt. So entsteht eine paradoxe Konstellation: Kooperation wird erwartet, aber nicht ermöglicht – weder geopolitisch noch institutionell.

Zugleich zeigt sich ein unausgesprochenes Spannungsfeld zwischen der Rolle der Hochschulen als Hochwertziele im globalen Cyberraum – etwa im Kontext von NIS2, Forschungsangriffen oder Plattformnutzung – und ihrer realen Positionierung als nicht befähigte Sicherheitsproduzenten. Es fehlen institutionelle Rollen, klare Zuständigkeiten und eine verlässliche Ausstattung.

Die Mikroanalyse bestätigt damit die zentrale These dieser Arbeit: Cybersicherheit in der Wissenschaft ist kein technisches Problem, sondern Ausdruck eines Governance-Dilemmas. Die Fallstudie Bayern zeigt paradigmatisch, wie Spannungsverhältnisse auf der operativen Ebene zur strukturellen Blockade werden. Programme wie HISP und Strukturen wie der Digitalverbund sind vorhanden, aber unterfinanziert und in ihrer Wirkung zu unverbindlich. Das Spannungsverhältnis Sicherheitsproduzenten vs. Hochwertziele transformiert sich auf institutioneller Ebene zu Verantwortungszuschreibung vs. Ausstattungslücke.

Solange diese Spannungen nicht aktiv moderiert und durch verlässliche Ressourcen, klare Verantwortungsstrukturen und nachhaltige Governance-Modelle hinterlegt werden, bleibt die digitale Resilienz der Hochschulen in Bayern prekär. Hochschulen agieren dann zwischen Erwartungsdruck und struktureller Ohnmacht – und die Politik riskiert, an dieser Asymmetrie ihrer eigenen Steuerung zu scheitern.

13. Übergreifende Befunde und Handlungsempfehlungen

Die vorliegende Analyse hat Cybersicherheit im Wissenschaftssystem nicht als isoliertes Technikfeld, sondern als Ausdruck tiefgreifender Spannungsverhältnisse im Verhältnis von Wissenschaft, Politik und Gesellschaft untersucht. Der Mehrebenenvergleich zwischen Makro-, Meso- und Mikroebene verdeutlicht, dass sich die in Kapitel 9 entwickelten Spannungsverhältnisse nicht nur als analytisches Raster bewähren, sondern als reale Strukturbedingungen institutioneller Entscheidungsfindung wirksam sind. Dabei offenbaren sich nicht nur systemische Ambivalenzen und Zielkonflikte, sondern auch systematische Steuerungsprobleme, die Cybersicherheit zu einer politischen Dauerherausforderung machen.

Makroebene: Sicherheitspolitische Reframing-Prozesse

Auf der Makroebene zeigt sich eine strategische Umdeutung wissenschaftlicher Prinzipien: Offenheit, Kooperation und Autonomie werden sicherheitspolitisch umcodiert. Internationale Kooperation wird rhetorisch gestützt, aber durch Exportkontrollen und Technologiebeschränkungen real eingeschränkt. Digitale Souveränität erscheint als politischer Imperativ, bleibt jedoch konzeptionell vage und praktisch oft wirkungsschwach. Sicherheitsnarrative dominieren die politische Semantik – Wissenschaft wird nicht als autonomes System adressiert, sondern als funktionale Ressource für Resilienz und Wettbewerbsfähigkeit. Dabei bleibt der systemische Eigenwert wissenschaftlicher Prinzipien unterbelichtet. Die Makroebene zeichnet sich somit durch ein Spannungsverhältnis zwischen politischer Steuerung und epistemischer Eigenlogik aus, das zugunsten geopolitischer Zielsetzungen verschoben ist.

Mesoebene: Strategien, Ambivalenzen und institutionelle Differenz

Auf Mesoebene treten unterschiedliche Strategietypen und Reflexionsniveaus hervor: Der Wissenschaftsrat bemüht sich um eine systemisch-normative Reartikulation wissenschaftlicher Selbststeuerung. Er adressiert Souveränität, Offenheit und Integrität als Leitprinzipien und warnt vor funktionaler Vereinnahmung durch Sicherheitsrationalitäten. Dem gegenüber steht etwa der EDUCAUSE Horizon Report, der zwar technologische Trends innovativ antizipiert (z. B. KI-Sicherheit, Datenschutz), dabei aber stärker technikzentriert und weniger epistemisch argumentiert.

Empirische Surveys wie das Hochschulbarometer und die IHE CTO/CIO Survey zeigen auf, dass eine grundsätzlich hohe Problemsensibilität auf institutioneller Leitungsebene besteht – aber auch Diskrepanzen – die häufig von mangelnden Umsetzungskapazitäten begleitet werden. Die strukturelle Einbindung von Cybersicherheit in Governance-Prozesse bleibt begrenzt, ebenso wie personelle und finanzielle Ressourcen. Besonders deutlich wird auf der Mesoebene das Spannungsverhältnis zwischen strategischer Programmatik und operativer Umsetzungsrealität. Diese liegt emergent quer zu den anderen Spannungsverhältnissen.

Mikroebene: Umsetzungslücken und institutionelle Blockaden

Auf der Mikroebene konkretisieren sich die Spannungsverhältnisse in Form institutioneller Blockaden. Die Fallstudie für das Wissenschaftssystem in Bayern zeigt exemplarisch, wie politische Erwartungen, regulatorische Programme und föderale Koordinationsstrukturen

auf eine unterausgestattete Realität treffen. Hochschulen werden adressiert als sicherheitsrelevante Akteure – ohne dass ihnen die strukturelle Befähigung zur Umsetzung entsprechender Strategien bereitgestellt wird.

Programme wie das HISP oder die neue IT-Strategie zeigen zwar konzeptionelle Klarheit und adressieren zentrale Managementfragen – etwa ISMS-Aufbau, Auditverpflichtungen, Notfallmanagement. Die Audits von 2025 zeigen jedoch: Fortschritte sind punktuell, abhängig von lokalem Engagement und Ressourcen. Besonders deutlich ist die Diskrepanz zwischen technischer und organisatorischer Umsetzung: Während technisch MFA und Zugangsschutz verbessert wurden, bleiben Risikomanagement, Schulung und Notfallkonzepte fragmentarisch.

Das Spannungsverhältnis zwischen wissenschaftlicher Autonomie und politischer Steuerung wird dabei zu einer strukturellen Falle: Hochschulen werden mit Verweis auf Selbstverantwortung adressiert, gleichzeitig aber nicht mit den notwendigen Mitteln ausgestattet. Negative Autonomie – als Rückzug des Staates bei gleichzeitiger Erwartung – wird so zur zentralen Blockadebedingung. Kooperation wird auf Mikroebene zwar organisatorisch angestrebt (z. B. Digitalverbund), aber strukturell nicht mit ausreichend Verbindlichkeit und Ressourcen unterlegt.

Spannungsverhältnisse als systemische Konstante

Der Mehrebenenvergleich zeigt: Die in Kapitel 9 entwickelten Spannungsachsen strukturieren nicht nur analytisch, sondern prägen realpolitische Entscheidungsräume. Dabei nehmen sie auf den verschiedenen Ebenen unterschiedliche Ausdrucksformen an:

Kooperation ↔ Fragmentierung: Geopolitisch durch Restriktionen und Inselbildung, institutionell durch fehlende Verbindlichkeit. Kooperation bleibt normativ erwarteter Wert, wird aber durch in der Umsetzung fragmentiert.

Offenheit ↔ Sicherheit: Offenheit wird strategisch entwertet, operativ unterausgestattet. Wissenschaftliche Innovationsprozesse stoßen auf sicherheitspolitische Risikologiken. Es droht eine Versicherheitlichung der Wissenschaft.

Souveränität ↔ Abhängigkeit: Der Ruf nach Souveränität bleibt oft ein symbolischer Akt, ein diskursiver Mantel – proprietäre Systeme prägen weiterhin die Praxis.

Wissenschaftsfreiheit ↔ Agendasetting: Steuerungsinteressen dringen tief in wissenschaftliche Prozesse ein. Freiheit bleibt eine implizite Voraussetzung, keine explizit geschützte Struktur.

Sicherheitsproduzenten ↔ Hochwertziele: Hochschulen sollen schützen, werden aber selbst nicht geschützt. Die Diskrepanz zwischen Anspruch und Ausstattung ist besonders eklatant.

Governance-Spannung als politische Herausforderung

Cybersicherheit in der Wissenschaft ist damit nicht primär ein Problem fehlender Technik oder mangelnder Grundawareness der Verantwortlichen, sondern Ausdruck systemischer Ambivalenzen. Steuerungslogiken, Autonomierhetorik, Ressourcendefizite und technologische Disruptionen treffen aufeinander – ohne systemische und institutionelle Moderation. Die Herausforderung liegt darin, Cybersicherheit als politisch-institutionelle Daueraufgabe zu begreifen, die nur durch verlässliche Governance, klare Zuständigkeiten und strukturelle Befähigung bewältigt werden kann.

Die übergreifende Diagnose lautet daher: Die digitale Resilienz des Wissenschaftssystems hängt nicht allein von technologischen Schutzmaßnahmen ab, sondern von der Fähigkeit, mit strukturellen Spannungsverhältnissen produktiv umzugehen – und diese nicht nur zu erkennen, sondern systemisch und institutionell zu moderieren.

Die folgenden sieben Handlungsempfehlungen leiten sich direkt aus diesen Analysen ab. Sie fokussieren auf systemische Hebelpunkte, an denen sich strukturelle, organisatorische und politische Bedingungen so verändern lassen, dass Cybersicherheit im Wissenschaftssystem nicht nur effizienter, sondern auch legitimer, anschlussfähiger und epistemisch integrierter gestaltet werden kann.

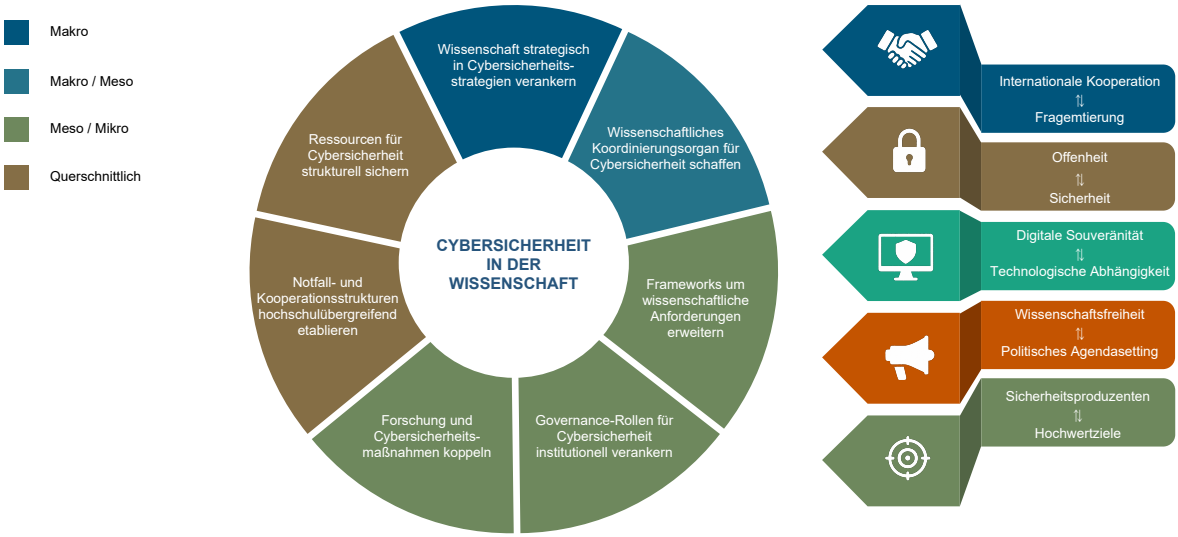

Abbildung 10: Handlungsempfehlungen Übersicht, eigene Darstellung

13.1. Wissenschaft als strategische Akteurin in nationalen und europäischen Cybersicherheitsstrategien stärken

Ebene: Makro

Zentrale Spannungsverhältnisse:

- Internationale Kooperation vs. Fragmentierung
- Offenheit vs. Schutz
- Digitale Souveränität vs. Technologischer Abhängigkeit
- Wissenschaftsfreiheit vs. Politischem Agendasetting
- Sicherheitsproduzenten vs. Hochwertziele

Die Analyse auf Makroebene (Kapitel 10) zeigt, dass Wissenschaft in nationalen und europäischen Cybersicherheitsstrategien bislang nicht als eigenständiger Akteur mit spezifischer Systemlogik, sondern primär als verwundbares Zielobjekt oder funktionale Ressource politischer Zielsetzungen dargestellt wird. In den untersuchten Strategiedokumenten (Deutschland, UK, USA) aber auch EU wird die Rolle der Hochschulen häufig auf technische Schutzaspekte oder funktionale Leistungen reduziert, während ihre epistemische Eigenlogik, ihr Beitrag zur Resilienzbildung sowie ihre systemische Vulnerabilität kaum differenziert thematisiert werden.

Diese Form der Rahmung erzeugt ein doppeltes Spannungsverhältnis. Einerseits entsteht ein Kooperationsanspruch, etwa durch den Verweis auf internationale Vernetzung und globale Forschungszusammenarbeit. Andererseits vollziehen dieselben Strategien eine regulatorische Entkopplung – z. B. durch Exportkontrollen, Sicherheitsauflagen oder Technologievorgaben, die genau diese Offenheit faktisch einschränken. Wissenschaftliche Kooperation wird damit gleichzeitig erwartet und erschwert – ein strukturelles Dilemma.

Zugleich wirkt das Verhältnis zwischen Wissenschaftsfreiheit und strategischem Agendasetting zunehmend asymmetrisch. Politische Zielsetzungen – etwa technologische Selbstbehauptung oder Resilienzaufbau – werden in nationale Forschungsprogramme, Drittmittelvergabe und Governancevorgaben eingeschrieben. Der wissenschaftliche Selbststeuerungsanspruch bleibt bestehen, verliert aber an Handlungsspielraum. So entsteht ein Erwartungsparadox: Hochschulen sollen politisch anschlussfähig, aber epistemisch unabhängig bleiben – ohne dass diese Balance institutionell abgesichert wäre.

Aus diesem Befund ergibt sich die folgende Handlungsempfehlung:

Wissenschaft sollte in nationalen und europäischen Cybersicherheitsstrategien als eigenständige, epistemisch verankerte und strategisch eingebundene Akteurin konzipiert und benannt werden.

Dazu zählen:

- Die explizite Ausweisung von Wissenschaft als eigenem Sektor (analog zu Wirtschaft, Gesundheit, Energie, Finanzwesen) in strategischen Papieren;
- Die Mitwirkung von Wissenschaftsorganisationen (z. B. Wissenschaftsrat, HRK, DFG, Leopoldina, Acatech, EU-Institutionen) an der Formulierung strategischer Ziele in nationalen oder supranational Strategien;
- Die Entwicklung eigener Leitlinien zur wissenschaftlichen Resilienz, die die aufgespannten Spanungsfelder balancieren;
- Die systematische Integration von Wissenschaft in nationale Reaktionsarchitekturen.

Nur wenn die Wissenschaft nicht nur als Betroffene oder Leistende, sondern als aktiv Mitgestaltende anerkannt und strukturell eingebunden wird, kann sie ihre doppelte Rolle im Cyberraum konstruktiv ausfüllen: als Trägerin demokratischer Wissensordnung und als Schutz-und Reflektionsraum gegen ggf. technokratische oder gar autoritaristische Kontrolllogiken. Diese Doppelrolle – als Sicherheitsakteur und Schutzgut – muss sich auch

strategisch abbilden. Andernfalls bleiben Cyberraum- oder spezifischer Cybersicherheitsstrategien technisch-administrative Projekte – ohne Rückbindung an demokratische Wissensproduktion.

13.2. Etablierung eines eigenständigen wissenschaftlichen Organs für Cybersicherheit und digitale Souveränität

Ebene: Makro / Meso
Zentrale Spannungsverhältnisse:

- Fragmentierung vs. internationale Kooperation
- digitale Souveränität vs. technologische Abhängigkeit
- Offenheit vs. Schutz
- Wissenschaftsfreiheit vs. Politischem Agendasetting
- Sicherheitsproduzenten vs. Hochwertziele

Die Mesoanalyse (Kap. 11) zeigt deutlich, dass der wissenschaftliche Sektor aktuell nicht über eine kohärente institutionelle Vertretung in Fragen der Cybersicherheit verfügt**.** Obwohl zahlreiche Institutionen – etwa das BSI, ZITiS, das Hochschulforum Digitalisierung, acatech oder auch die Nationale Kompaktstelle Cybersicherheit – einzelne Schnittstellen zur Wissenschaft aufweisen, fehlt ein strukturell legitimiertes Organ, das die spezifische Eigenlogik wissenschaftlicher Akteure strategisch bündeln, koordinieren und politisch vertreten kann.

Diese Lücke erzeugt ein institutionelles Spannungsfeld: Die Sicherheitserwartungen an Hochschulen steigen stetig (z. B. durch die EU, die geopolitische Lage, den Innovationserwartungsruck), während ihre strukturelle Handlungsfähigkeit nur fragmentarisch ausgeprägt ist und sich nicht ausreichend weiterentwickelt. Der Wissenschaftsrat (2023) benennt dies explizit als „Governance-Problem“, das sich im Fehlen systematischer Zuständigkeiten und Verantwortlichkeiten niederschlägt. Hochschulen driften somit in eine **negative Autonomie** ab: adressiert aber nicht mitgenommen, formal frei, faktisch jedoch überfordert.

Zudem zeigt die CIO-Analyse (Kap. 11.3.1–11.3.4), dass operative Verantwortliche in Hochschulen zwar Awareness für strategische Zielkonflikte entwickeln, jedoch keine Möglichkeit haben, diese auf einer übergeordneten Steuerungsebene zu adressieren. Koope-

ration zwischen Hochschulen erfolgt punktuell und freiwillig, nicht jedoch ausreichend gestützt durch verpflichtende oder unterstützende politische Strukturen und/oder Ressourcen.

Aus diesen Befunden ergibt sich folgende Handlungsempfehlung:

Ein wissenschaftliches Organ für Cybersicherheit und digitale Souveränität sollte als nationale, strategische Sprecher- und Koordinierungsstruktur etabliert werden – nicht als neue Behörde, sondern als konsolidierende Schnittstelle auf höchster Ebene bestehender Institutionen.

Die Etablierung eines eigenen wissenschaftlichen Organs für Cybersicherheit und digitale Souveränität zielt daher auf eine dreifache Funktion:

1. **Koordination:** Bündelung bestehender Maßnahmen, Standards und Initiativen aus dem Hochschulbereich in einem gemeinsamen Steuerungsgremium oder Netzwerk – voll integriert in das zentrale Nationale Cybersicherheitsorgan.
2. **Repräsentation:** Institutionalisierte Mitwirkung an politischen Entscheidungs- und Krisengremien, etwa durch feste Sitze in nationalen Cybersicherheitsräten;
3. **Reflexion:** Entwicklung wissenschaftseigener Leitlinien, Modelle und Strategien, die technische, organisatorische und epistemische Dimensionen der Sicherheit im Cyberraum aus der Wissenschaftsperspektive verbinden.

Best-Practice-Modelle wie das britische **National Cyber Security Centre** zeigen, dass eine eigenständige wissenschaftliche Stimme Cybersicherheitsarchitekturen nicht fragmentiert, sondern strukturell stärkt. Für Deutschland wäre dies ein zentraler Schritt, um aus der **doppelten Erwartung (leisten & schützen)** eine gestaltbare Institution zu machen.

13.3. Weiterentwicklung bestehender Cybersicherheitsframeworks mit Fokus auf wissenschaftliche Anforderungen

Ebene: Meso, Micro
Zentrale Spannungsverhältnisse:

- Offenheit vs. Sicherheit
- Wissenschaftsfreiheit vs. Politisches Agendasetting

- Digitale Souveränität vs. Technologischer Abhängigkeit
- Sicherheitsproduzenten vs. Hochwertziele

Die Analyse in Kapitel 12 zeigt, dass branchenspezifische Cybersicherheitsframeworks wie das IT-Grundschutz-Profil für Hochschulen (ZKI 2022) und das Hochschulinformationssicherheitsprogramm (HISP) in Bayern mittlerweile weit verbreitete Orientierungsrahmen darstellen. Sie bieten technisch und organisatorisch wertvolle Grundstrukturen für die Einführung von Informationssicherheitsmanagementsystemen (ISMS), insbesondere durch ihren modularen Aufbau, konkrete Umsetzungshilfen und Reifegradmodelle.

Gleichzeitig weisen diese Modelle eine gewisse Begrenzung in Bezug auf wissenschaftsspezifische Anforderungen auf, da sie vorwiegend allgemeine Anforderungen der Cybersicherheit auf die Wissenschaft bezogen übersetzten. Insbesondere fehlt es diesen dann wie den allgemeinen Frameworks an Vorschaut und Spezifik, da Konzepte – wie Zero-Trust-Architekturen, die Rolle von KI, adaptive Schutzkonzepte oder dynamische Risikoklassen – bislang nicht systematisch integriert sind. Der Fokus liegt weiterhin auf klassischen Schutzparadigmen, die oft von Behördenlogik und einer Trennung interner/externer Netzwerke geprägt sind. Diese Logik ist mit dem Prinzip nach zwar auf die Wissenschaft anwendbar und bringt diese ebenfalls in Cybersicherheitsfragen voran, vollzieht aber auf operativer Ebene ebenjene Fehlstellen, die auf Makro-Ebene ebenfalls erkennbar sind.

Zusätzlich zeigt die Empirie, dass trotz vorhandener Frameworks eine große Heterogenität in der Umsetzung besteht: Hochschulen mit proaktiv geschaffenen Rollen und Ressourcen erreichen deutlich höhere Reifegrade als solche, die die dazu - aus welchen Gründen auch immer - nicht willens meist wohl nicht fähig sind, diese bereitzustellen. Damit werden oft nicht einmal Mindeststandards erreicht. Nur eine Universität in Bayern hat nach Audit Bericht 2025 die Zertifizierung nach ISO 27001 bereits erreicht. Dies legt nahe, dass bestehende Frameworks zwar Orientierung bieten, aber nicht ausreichend Transformationspotenzial entfalten, solange sie sich nicht stärker auf die funktionalen Eigenlogiken von Wissenschaft beziehen und vor allem nicht ausreichend personell und finanziell ausgestattet sind.

Daher ergibt sich folgende Handlungsempfehlung:

Bestehende Cybersicherheitsframeworks sollten systematisch um wissenschaftsspezifische Anforderungen erweitert werden – sowohl inhaltlich als auch in ihrer institutionellen Verankerung.

Die Handlungsempfehlung zielt daher auf eine doppelte Erweiterung bestehender Rahmenwerke:

1. **Inhaltlich-konzeptionelle Weiterentwicklung:**
   Integration wissenschaftsspezifischer Anforderungen in bestehende Profile, z. B. durch:
   - risikoadaptive Schutzschichtenmodelle,
   - flexible Bausteine für sensible Forschungsbereiche,
   - Szenarien für internationale Projektarbeit,
   - Maßnahmen zur Balance zwischen regulatorischem Druck und wissenschaftlicher Freiheit.

2. **Governance-Integration und Umsetzungsunterstützung:**
   Entwicklung von strategischen Leitfäden, Schulungsmodulen und institutionellen Steuerungsinstrumenten, die über die IT hinaus auch Leitungsebene, Forschungskommunikation und Kooperationspolitik adressieren.

Die Frameworks müssen dadurch nicht ersetzt, sondern organisationssensibel erweitert werden – im Sinne eines „Modularen Schutzkonzepts Wissenschaft“, das die spezifische Balance von Offenheit, Sicherheit und Souveränität ermöglicht. Nur wenn Cybersicherheit nicht nur technisch, sondern epistemisch eingebettet ist, kann sie im Wissenschaftssystem wirksam, legitim und tragfähig verankert werden.

13.4. Institutionalisierung strategischer Governance-Rollen für Cybersicherheit auf Leitungsebene

Ebene: Meso / Mikro
Zentrale Spannungsverhältnisse:

- Verantwortung vs. Autonomie der Hochschule (abgeleitet)
- Sicherheitsanspruch vs. Steuerungsfähigkeit (abgeleitet)
- Strategisches Handlungsfeld vs. technische Dienstleistung (abgeleitet)

Die Meso- und Mikroanalyse offenbart ein strukturelles Steuerungsdefizit im Bereich der Cybersicherheit auf der Leitungsebene deutscher Hochschulen. Während operative Verantwortlichkeiten – etwa durch Informationssicherheitsbeauftragte, CIOs oder IT-Leitungen – formal bestehen, fehlt es vielfach an **institutionalisierten, strategisch legitimierten Governance-Rollen**, die Cybersicherheit als gesamthafte, querschnittliche Aufgabe der Hochschule begreifen.

Der Bayerische Oberste Rechnungshof konstatierte bereits 2021, dass in sieben von neun geprüften Hochschulen keine benannten ISB-Strukturen existierten. Die Organisation der IT-Sicherheit sei „sehr unterschiedlich" und es herrschten „erhebliche Umsetzungsdefizite". Auch die CIO-Runde bestätigt: Strategische Steuerung fehlt häufig, selbst wenn das Problembewusstsein vorhanden ist. Nur eine Minderheit deutscher Hochschulen verfügt über eine explizite, institutionell verankerte Cybersicherheitsstrategie.

Gleichzeitig ist der Erwartungsdruck von außen hoch: Hochschulen sollen sich gegen hybride Bedrohungen wappnen, kritische Infrastrukturen schützen, digitale Souveränität sicherstellen und zugleich als Innovationsmotoren agieren. Damit wird ihnen Sicherheitsverantwortung zugewiesen, ohne dass diese systematisch durch Steuerungsmandate, Ressourcen oder institutionelle Autorität abgesichert wäre.

Diese Konstellation konkretisiert das übergeordnete Spannungsverhältnis zwischen der Rolle der Hochschulen als Sicherheitsakteure und ihrer realen Positionierung als Hochwertziele. In der Praxis entsteht daraus ein strukturelles Ungleichgewicht – eine Verantwortungszuschreibung ohne Befähigung. Kapitel 12.3 beschreibt diesen Zustand als „negative Autonomie": Hochschulen gelten als eigenverantwortlich – faktisch aber fehlt es an den Voraussetzungen, um diese Verantwortung wirksam wahrzunehmen.

Aus diesen Beobachtungen ergibt sich folgende Handlungsempfehlung:

Hochschulen sollten deshalb strategische Governance-Rollen im Bereich Cybersicherheit auf Leitungsebene institutionalisieren und mit klaren Mandaten, Entscheidungsbefugnissen und Ressourcen ausstatten.

Wichtige Kriterien dabei sind:

- Direkte Anbindung an die Hochschulleitung,
- Eigenständige Budget- und Eskalationsrechte,
- Interdisziplinäre Verankerung über Lehre, Forschung und Verwaltung hinweg,

- Strategische Legitimation in Hochschulentwicklungsplanung und Risikomanagement.

Internationale Vergleichsstudien (CTO/CIO Survey, Inside Higher Ed) zeigen: Selbst in Hochschulsystemen mit formal etablierten Rollen bleibt Cybersicherheit oft operativ. Die Herausforderung liegt daher nicht nur in der Benennung, sondern in der **strategischen Verankerung** dieser Rollen – mit Mandat, Relevanz und institutioneller Sichtbarkeit. Nur wenn Cybersicherheit als Führungsaufgabe verstanden wird, kann sie im Wissenschaftssystem nachhaltig wirksam werden.

13.5. Systematische Rückkopplung von Cybersicherheitsforschung in operative Hochschulpraxis

Ebenen: Makro / Meso / Mikro
Zentrale Spannungsverhältnisse:

- Sicherheitsakteure vs. Hochwertziele
- Wissen (Anspruch) vs. Umsetzung (Wirklichkeit) (abgeleitet)
- Wissenschaftsproduktion vs. institutionelle Nutzung (abgeleitet)
- Innovationsfähigkeit vs. Transferfähigkeit (abgeleitet)

Die Arbeit belegt eindrücklich, dass im deutschen Hochschulbereich eine strukturelle Kluft zwischen Forschung und Praxis im Bereich Cybersicherheit besteht. Einerseits verfügen Hochschulen über exzellente Forschungskapazitäten und Kompetenzen in der Sicherheitsforschung, andererseits gelingt es ihnen kaum, diese Expertise in ihre eigene IT-Sicherheitsarchitektur zu überführen.

Kapitel 11.3.6 zeigt, dass Forschungsergebnisse – auch wenn sie konkrete Relevanz für institutionelle Resilienzstrategien haben – selten zurückfließen in operative Entscheidungsprozesse oder die Gestaltung interner Sicherheitsmaßnahmen. Die Gründe dafür sind vielfältig: fehlende organisatorische Schnittstellen, unklare Zuständigkeiten, mangelnde Ressourcen oder fehlende Kommunikationsformate zwischen Forschungs- und Verwaltungseinheiten durch Überlagerung von Behördenlogik.

Dabei erwartet der sicherheitspolitische Diskurs zunehmend, dass Hochschulen nicht nur als Schutzobjekte, sondern als aktive Sicherheitsproduzenten agieren. Diese Erwartung kann nur erfüllt werden, wenn Hochschulen resilient und transferfähig sind – also wenn sie eigene Forschung in ihre Sicherheitsarchitekturen rückkoppeln können.

Aus diesen Befunden ergibt sich folgende Handlungsempfehlung:

Hochschulen sollten institutionalisierte Mechanismen schaffen, um Forschungsergebnisse aus der Cybersicherheitsforschung systematisch in operative Sicherheitsstrukturen zu überführen.

Zentrale Maßnahmen könnten sein:

- Einrichtung hochschulinterner Transferstellen für Cybersicherheitsforschung, die Forschung und Rechenzentrum/Verwaltung verbinden;
- Aufrichtung von SOC und CERT-Formaten auf Transfer, damit nicht nur auf Vorfälle reagiert, sondern daraus auch Innovationstransfer betrieben werden kann; Die Wissenschaft eignet sich als System hier besser als die Wirtschaft.
- Integration von Forschungsergebnissen in strategische Steuerungsprozesse (z. B. Risikoanalysen, Policy-Entwicklung, IT-Beschaffungsentscheidungen);
- Förderung operativer Anwendungsszenarien in Drittmittelprojekten, z. B. verpflichtender „Praxis-Output“ bei BMBF-Förderung, wird oft schon angewendet;
- Aufbau regionaler Transfernetzwerke zwischen Hochschulen, Wirtschaft und Behörden. Auch diese sind bereits erkennbar.

Diese Maßnahmen adressieren das in der Arbeit klar identifizierte emergente Spannungsverhältnis zwischen Wissen und Umsetzung: Cybersicherheitsrelevantes Wissen wird an Hochschulen zwar erzeugt – etwa durch Forschungsprojekte, Kompetenzzentren oder Lehrstühle – doch es fehlt an strukturellen Schnittstellen, um dieses Wissen institutionell rückzukoppeln und praktisch wirksam zu machen.

Kapitel 11.3.6 zeigt, dass diese Rückkopplung nicht durch fehlende Einsicht, sondern durch organisatorische Fragmentierung und fehlende strategische Steuerung ausbleibt. Die Arbeit bezeichnet dies als Ausdruck einer „asymmetrischen Systemintegration“: Forschung wird funktional erwartet, institutionell aber nicht eingebettet.

Indem Hochschulen gezielte Transferformate, CERTs mit Forschungseinbindung oder operative Anwendungspfade für Projekte schaffen, übersetzen sie Wissen in Widerstandsfähigkeit – und sichern zugleich ihre eigene Rolle im sicherheitspolitischen Ordnungsrahmen. Die Maßnahmen operationalisieren damit nicht nur Transfer, sondern auch den in der Arbeit formulierten Anspruch, Cybersicherheit als institutionelle Selbstbeobachtung der Wissenschaft zu verstehen – mit konkreten infrastrukturellen Konsequenzen.

13.6. Aufbau resilienter, hochschulübergreifender Notfall- und Kooperationsarchitekturen

Ebene: Meso / Makro
Zentrale Spannungsverhältnisse:

- Sicherheitsproduzenten vs. Hochwertziele
- Offenheit vs. Sicherheit
- Fragmentierung vs. kollektive Sicherheitsarchitektur (abgeleitet)

Die Analyse der Mikro- und Mesoebene zeigt: Derzeit bestehen im deutschen Hochschulraum kaum institutionalisierte Mechanismen zur hochschulübergreifenden Krisenreaktion oder Ressourcenbündelung im Ernstfall. Erste CERTS wie das DFN-Cert bestehen sehr lange, haben aber sehr spezifische Aufgaben, die wenig skalierbar sind.

Angesichts der wachsenden Häufigkeit und Intensität von Cyberangriffen – insbesondere Ransomware-Attacken – ist dies ein strukturelles Risiko. Die Arbeit zeigt: Hochschulen agieren im Krisenfall überwiegend isoliert**,** häufig ohne dokumentierte Notfallpläne oder abgestimmte Kommunikationsprotokolle.

Kapitel 11.3.3 und 12.3.2 analysieren detailliert, wie mangelnde Governance-Strukturen, begrenzte Ressourcen und föderale Fragmentierung die Reaktionsfähigkeit im Schadensfall einschränken. So verfügen laut Auditbericht HITS IS 2025 nur 10 % der Hochschulen über dokumentierte Notfallpläne, und selbst dort sind Leitungsebene und strategische Steuerung häufig nicht eingebunden.

Gleichzeitig verdeutlicht die theoretische Perspektive (insb. Luhmann, Dunn Cavelty, Keller), dass Hochschulen im Spannungsverhältnis Hochwertziel vs. Sicherheitsproduzent institutionell überfordert sind, wenn sie individuell für systemische Risiken Verantwortung tragen, ohne kollektive Absicherungsmechanismen nutzen zu können.

Diese Befunde führen zu folgender Handlungsempfehlung:

Hochschulen sollten resilientere, hochschulübergreifende Notfall- und Kooperationsarchitekturen aufbauen – mit dem Ziel, auf schwerwiegende Cybervorfälle koordiniert, ressourcenteilend und kollektiv reagieren zu können.

Kernbausteine wären:

- **Abgestimmte Krisenreaktionspläne und Eskalationsprotokolle**, eingebunden in Landes- und Bundestrukturen,
- **Gemeinsame Recovery-Architekturen**, etwa über rollierende Backup-Systeme oder Ersatzinfrastrukturen,
- **Regionale CERT-Cluster**, die Vorfälle koordinieren, Frühwarnung leisten und mit BSI/LandesCERTs verzahnt sind,
- **Sektorale SOC-Strukturen** (Security Operations Center), das wissenschaftsspezifische Lagebilder erfassen, überwachen und kommunizieren,
- **Regelmäßige Planspiele und Simulationen** zur institutionellen Stresstestung und zur Erhöhung der operativen Resilienz.

CERTs und SOCs sollten dabei nicht nur als technische Einheiten verstanden werden, sondern als strategische Schnittstellen: zwischen Hochschulen und Staat, Forschung und Verwaltung, Autonomie und Sicherheit. Ihr hochschulübergreifender Ausbau ist der logische Schritt aus der Erkenntnis, dass Resilienz im Wissenschaftssystem keine Eigenschaft einzelner Organisationen ist – sondern ein kollektives Resultat geteilter Verantwortung.

13.7. Strukturelle Sicherung personeller und finanzieller Ressourcen für wissenschaftliche Cybersicherheit

Ebene: Meso / Makro
Zentrale Spannungsverhältnisse:

- Alle Spannungsverhältnisse sowie
- Fähigkeit vs. Erwartung (emergent)
- Steuerungsanspruch vs. Ressourcenrealität (abgeleitet)
- Innovationsdruck vs. institutionelle Unterausstattung (emergent)

Die Analyse zeigt klar: Der strukturelle Mangel an qualifiziertem Personal und verlässlicher Finanzierung stellt das größte Hindernis für die nachhaltige Etablierung von Cybersicherheitsstrukturen an Hochschulen dar. Laut Hochschulbarometer 2024 geben **89,8 % der deutschen Hochschulen** an, Schwierigkeiten bei der Rekrutierung von IT-Personal zu haben; **82,2 % beklagen** unzureichende Mittel für Sicherheitsmaßnahmen. Besonders betroffen sind kleinere und mittlere Hochschulen, denen strategische Hebel zur Ressourcenumlenkung fehlen.

Diese Problemlage ist nicht temporär oder punktuell, sondern systemisch:

- Die Grundfinanzierung der Hochschulen wurde nie im Hinblick auf wachsende Cybersicherheitsanforderungen dimensioniert.
- Maßnahmen beschränken sich häufig auf projektbezogene Drittmittel oder zentrale Stabsstellen ohne flächendeckende Wirkung.
- Der Auditbericht (2025) zeigt, dass Reifegrade über Level 2 (nach HISP) nur dort erreicht werden, wo institutionelle Stellen mit klaren Mandaten verankert sind.

Die Arbeit diagnostiziert dies als strategische Blockade durch strukturelle Unterausstattung – ein Spannungsverhältnis zwischen politischem Anspruch und institutioneller Fähigkeit, das als *emergentes* „Ermöglichungsspannungsverhältnis“ identifiziert wird.

Daraus ergibt sich folgende Handlungsempfehlung:

Es müssen verbindliche, strukturell verankerte Ressourcenformate für die personelle und finanzielle Ausstattung von Cybersicherheit an Hochschulen geschaffen werden.

Zentrale Elemente sind:

- **Anpassung der Grundfinanzierung** an digitale Bedrohungslagen (z. B. über Hochschulfinanzierungsverträge mit Cybersicherheitskomponenten);
- **Dauerhafte Stellen für Cybersicherheitsmanagement**, insbesondere ISB-, CISO-, Datenschutz- und CERT-Personal;
- **Spezifische Zulagenmodelle** und **Karrierepfade**, um im Wettbewerb mit der Privatwirtschaft bestehen zu können;
- **Erweiterung projektunabhängiger Förderlinien**, um strategische Planungssicherheit zu ermöglichen;
- **Verknüpfung von Mittelvergabe mit Zielvereinbarungen**, z. B. ISMS-Einführung, Reifegradentwicklung oder Beteiligung an CERT-Strukturen.

Die Arbeit zeigt zudem, dass Hochschulen eine doppelte Verantwortung tragen: Sie müssen ihre eigene digitale Souveränität sichern und zugleich die nächste Generation von Cybersicherheitsexpert:innen ausbilden. Ihre strukturelle Unterversorgung gefährdet daher nicht nur die interne Funktionsfähigkeit, sondern auch die Innovations- und Sicherheitsinfrastruktur der gesamten Gesellschaft.

Diese Empfehlung fungiert somit als Querschnittsbedingung für alle anderen Handlungsempfehlungen: Ohne strukturell unterlegte Ressourcen bleiben Governance, Kooperation und Strategie ambivalent – ein Zustand, den die Arbeit als „negative Autonomie“ bezeichnet.

14. Schluss und Ausblick

14.1. Zusammenfassung der Arbeit

Diese Arbeit untersuchte, wie sich globale geopolitische Dynamiken auf die Handlungsbedingungen von Wissenschaft und Hochschulen im Cyberraum auswirken – und wie sich daraus systematisch Spannungsverhältnisse ableiten lassen, die als Grundlage für strategische Institutionalisierung und Cybersicherheitsmaßnahmen dienen können.

Ausgangspunkt war ein theoriegeleiteter Zugang: Aufbauend auf systemtheoretischen, diskurstheoretischen und cybersicherheitsbezogenen Ansätzen wurde ein analytisches Modell zentraler Spannungsverhältnisse zwischen Wissen, Macht und Sicherheit entwickelt. Diese wurden in Kapitel 9 als fünf heuristische Grundkonflikte formuliert – darunter Offenheit vs. Sicherheit, internationale Kooperation vs. Fragmentierung und technologische Abhängigkeit vs. digitale Souveränität.

Im Rahmen einer dreistufigen Mehrebenenanalyse wurde das Modell auf unterschiedliche Kontexte angewendet:

- **Makroebene**: Diskursanalytische Auswertung nationaler und internationaler Cybersicherheitsstrategien (Deutschland, UK, USA, EU) zur semantischen Rahmung von Wissenschaft;
- **Mesoebene**: Sekundäranalyse wissenschaftspolitischer Quellen (Wissenschaftsrat, Hochschulbarometer, EDUCAUSE, CIO-Survey) zur Governance und Steuerungsrealität;
- **Mikroebene**: Fallstudie inkl. Analyse eines vertraulichen Auditberichts zu Informationssicherheit bayerischer Hochschulen zur empirischen Erfassung operativer Praxis, Risikowahrnehmung und institutioneller Steuerung.

Die Analyse zeigte, dass die in Kapitel 9 entwickelten Spannungsverhältnisse auf allen Ebenen erkennbar sind – jedoch in funktional angepassten, institutionell gerahmten oder

emergent verschärften Formen auftreten. Diese Vielschichtigkeit ermöglichte eine evidenzbasierte Herleitung von sieben Handlungsempfehlungen, die Cybersicherheit im Wissenschaftssystem nicht nur als Schutzaufgabe, sondern als strategische Führungs-, Steuerungs- und Reflexionsdimension verankern.

14.2. Beantwortung der Forschungsfrage

Die Forschungsfrage lautete:

Wie beeinflussen globale geopolitische Dynamiken den Cyberraum der Wissenschaft und Hochschulen, und wie können Spannungsverhältnisse systematisch kategorisiert werden, um daraus institutionelle Handlungsempfehlungen im Bereich Cybersicherheit zu entwickeln?

Die Arbeit zeigt, dass Wissenschaft und Hochschulen zunehmend in geopolitische Machtfelder und sicherheitspolitische Steuerungslogiken des Cyberraums eingebunden werden – etwa durch Technologiekontrollen, sicherheitspolitische Agenden oder die Fragmentierung internationaler Kooperationen. Diese Dynamiken erzeugen strukturelle Zielkonflikte, die wissenschaftliche Offenheit, Selbststeuerung und institutionelle Handlungsfähigkeit erheblich unter Druck setzen.

Zur Analyse dieser Konfliktlagen wurde ein Spannungsverhältnismodell entwickelt, das fünf zentrale Kategorien systematisiert:

- Offenheit vs. Sicherheit,
- Digitale Souveränität vs. technologische Abhängigkeit,
- Internationale Kooperation vs. Fragmentierung,
- Wissenschaftsfreiheit vs. politisches Agendasetting,
- Sicherheitsproduzenten vs. Hochwertziele.

Dieses Modell wurde deduktiv aus Theorie gewonnen, empirisch fundiert und in einer Mehrebenenanalyse angewendet. Die Ergebnisse:

- Auf **Makroebene** bleibt Wissenschaft in Cybersicherheitsstrategien vielfach auf eine Ressource reduziert. Ihre spezifischen Schutzbedarfe, epistemische Prinzipien und institutionellen Eigenlogiken werden selten berücksichtigt.

- Auf **Mesoebene** bestehen deutliche Diskrepanzen zwischen politischen Erwartungen und institutionellen Ressourcen – etwa in Form fehlender Governance-Strukturen, schwacher strategischer Steuerung oder fehlender Finanzierungsmodelle.
- Auf **Mikroebene** zeigt die Fallstudie, dass Hochschulen operativ häufig überfordert sind. Selbst dort, wo Sicherheitsstrategien vorhanden sind, fehlt es oft an nachhaltiger Ressourcenunterlegung und institutioneller Verbindlichkeit.

Das Spannungsmodell erwies sich dabei als tragfähige Heuristik: Es erlaubt nicht nur eine strukturierte Analyse diskursiver Steuerungsmuster, sondern auch die Identifikation konkreter Handlungsbedarfe.

Auf dieser Basis wurden sieben Handlungsempfehlungen entwickelt – von strategischer Repräsentation im politischen Raum bis hin zum Aufbau operativer Resilienzarchitekturen. Sie adressieren zentrale Steuerungslücken und schlagen Maßnahmen vor, die Cybersicherheit epistemisch integrieren und systemisch verankern – als Voraussetzung für wissenschaftliche Resilienz im geopolitisch fragmentierten Cyberraum.

14.3. Kritische Reflexion

Diese Arbeit versteht sich als theoriegeleiteter Beitrag zur strategischen Verortung von Hochschulen im geopolitisch fragmentierten Cyberraum. Sie verbindet systematische Kategorienbildung mit einer Mehrebenenanalyse, um Cybersicherheit nicht als rein technische Herausforderung, sondern als strukturelles und steuerungspolitisches Spannungsfeld sichtbar zu machen. Gleichwohl ist sie mit methodischen und analytischen Begrenzungen verbunden, die im Folgenden reflektiert werden.

1. Methodischer Zuschnitt:
Der Forschungsansatz stützt sich auf qualitativ-interpretative Verfahren – insbesondere die deduktive Entwicklung eines Spannungsmodells und dessen Anwendung auf politische, institutionelle und organisationale Texte. Diese Methodik erlaubt differenzierte Tiefenanalyse, ist jedoch anfällig für *confirmation bias*, insbesondere bei der Interpretation strategischer Diskurse. Um dem zu begegnen, wurden Theoriegeleitetheit, Triangulation und Texttransparenz besonders beachtet – auf systematische Intercoder-Validierung musste jedoch verzichtet werden.

2. Datenbasis:
Die Analyse basiert auf öffentlich zugänglichen strategischen Dokumenten, wissenschaftspolitischen Studien und einem vertraulichen Auditbericht. Diese Kombination ermöglicht eine hohe Nähe zur Praxis, bleibt aber punktuell: Primärdatenerhebungen (z. B. Interviews oder standardisierte Erhebungen) konnten aus Datenschutz- und Zugangsbeschränkungen nicht durchgeführt werden. Die Tiefe einzelner Einsichten geht damit zulasten der empirischen Breite.

3. Regionaler Fokus:
Die mikroanalytische Fallstudie konzentriert sich auf Hochschulen im Freistaat Bayern. Die hier gewonnenen Erkenntnisse lassen sich nicht ohne Weiteres auf andere Bundesländer oder internationale Hochschulsysteme übertragen. Gleichwohl deuten viele strukturelle Spannungsverhältnisse – etwa im Bereich Governance, Ressourcen oder strategische Steuerung – auf bundesweite oder sogar internationale Muster hin.

4. Theoretische Weiterentwicklung des Modells:
Das in Kapitel 9 entwickelte Spannungsverhältnismodell wurde in dieser Arbeit erstmals systematisch eingesetzt. Es hat sich als heuristisch tragfähig erwiesen, insbesondere zur Strukturierung diskursiver Steuerungsprozesse und institutioneller Zielkonflikte. Eine breitere Anwendung in anderen Disziplinen, Institutionstypen oder Ländern steht jedoch noch aus – ebenso wie eine umfassende Theoriekritik oder Anschlussfähigkeit an alternative Governance-Modelle.

5. Begriffsverwendung des Cyberraums:
Der in dieser Arbeit verwendete Begriff des Cyberraums geht bewusst über eine technische oder infrastrukturelle Definition hinaus. Aufbauend auf systemtheoretischen, diskurstheoretischen und cybersicherheitsbezogenen Ansätzen wurde der Cyberraum als **gesellschaftlich strukturierte Konfliktzone** konzipiert – ein Raum, in dem staatliche, wirtschaftliche, militärische und wissenschaftliche Logiken aufeinandertreffen.

In dieser Lesart ist der Cyberraum nicht bloß Träger digitaler Prozesse, sondern ein Ort von **Machtkonflikten, epistemischer Aushandlung und semantischer Steuerung**. Besonders durch die Kombination von Systemtheorie (Luhmann), Diskurstheorie (Keller) und Sicherheitsforschung (Dunn Cavelty, Zettl) wurde er als Raum der **strukturellen Spannung** verstanden.

Die Begrenzung liegt daher nicht in einer Engführung des Begriffs, sondern in seiner selektiven Anwendung auf den Hochschulbereich. Militärische, wirtschaftliche oder zivilgesellschaftliche Kontexte wurden nur randständig einbezogen. Diese bewusste Eingrenzung ermöglichte eine analytische Fokussierung auf wissenschaftliche Institutionen – zugleich wäre eine breitere intersektorale Perspektive ein fruchtbarer Gegenstand zukünftiger Forschung.

Trotz dieser Einschränkungen bietet die Arbeit neue Impulse für die wissenschaftspolitische Diskussion zur Cybersicherheit. Sie schließt eine doppelte Forschungslücke: Sie thematisiert erstmals systematisch die Rolle von Wissenschaft im strategischen Diskurs über den Cyberraum – und stellt ein fundiertes Instrument zur Verfügung, um Spannungsverhältnisse nicht nur zu benennen, sondern systematisch zu analysieren und strategisch zu bearbeiten.

14.4. Der kritische Widerspruch der Wissenschaft als Grundlage strategischer Resilienz im Cyberraum

In einer Zeit zunehmender geopolitischer Fragmentierung und sicherheitspolitischer Überformung des Cyberraums gerät das Wissenschaftssystem in Spannungsverhältnisse, die weit über technische Schutzmaßnahmen hinausreicht. Der Cyberraum ist nicht nur ein infrastrukturelles Medium wissenschaftlicher Arbeit, sondern ein politisch umkämpftes Machtfeld, in dem die Logiken von Staat, Markt und Militär zunehmend Einfluss auf wissenschaftliches Handeln nehmen. In dieser Situation liegt die größte Gefahr nicht allein in der Verletzbarkeit wissenschaftlicher Infrastrukturen, sondern in der möglichen Selbstaufgabe der Wissenschaft durch eine Übernahme fremder Funktionslogiken.

Die Wissenschaft ist, systemtheoretisch gesprochen, ein eigenlogisch operierendes gesellschaftliches Teilsystem. Ihr Operationscode ist die Unterscheidung zwischen "wahr" und "unwahr". Sie generiert Wissen nicht primär zur strategischen Verwertung, sondern zur Erzeugung von Verstehbarkeit, Kritikfähigkeit und Erkenntnis. Wird dieser Code durch die Funktionslogik anderer Systeme – etwa Politik (Code: Macht), Wirtschaft (Code: Geld) oder Sicherheit (Code: Schutz/Nicht-Schutz) – überlagert, droht die Wissenschaft ihre Autopoiesis zu verlieren. Sie wird dann nicht mehr zur reflexiven Instanz, sondern zum Instrument.

Diese Gefahr stellt sich im Cyberraum in besonderer Weise. Hier verdichtet sich die Forderung an die Wissenschaft, technologisch verwertbares, sicherheitsrelevantes Wissen hervorzubringen. Das Sicherheitsnarrativ, das die staatliche Steuerung in strategischen Dokumenten dominiert, sieht in der Wissenschaft eine Ressource im geopolitischen Wettbewerb. Die Freiheit der Forschung wird dabei nicht explizit negiert, aber implizit funktionalisiert. Die offene, kritische, nicht-zweckgebundene Dimension wissenschaftlicher Arbeit erscheint zunehmend als Störfaktor.

Vor diesem Hintergrund ergibt sich eine doppelte Verantwortung der Hochschulen: Zum einen müssen sie Sicherheitsstrategien entwickeln, um ihre digitalen Infrastrukturen und die Integrität von Forschung und Lehre zu schützen. Zum anderen müssen sie die Eigenlogik der Wissenschaft gegen Übergriffe verteidigen und sichtbar machen. Diese Verteidigung geschieht nicht durch Isolation, sondern durch **kritischen Widerspruch** – das heißt: durch die fortgesetzte Artikulation wissenschaftlicher Perspektiven auf sicherheitspolitische Erwartungen.

Der kritische Widerspruch ist dabei kein destruktives Element, sondern konstitutiv für eine balancierte Ordnung im Cyberraum. Er zwingt zur Selbstreflexion, verhindert Monoperspektiven und überführt technische und politische Schutzrhetorik in einen Dialog über Ziele, Werte und Nebenfolgen. Wissenschaftliche Institutionen, die sich dieser Rolle stellen, agieren nicht gegen den Staat, sondern als **dialogische Gegenüber**. Sie schaffen strategische Resilienz, indem sie nicht nur auf Bedrohungen reagieren, sondern epistemische Vielfalt, institutionelle Reflexivität und kulturelle Differenzfähigkeit bewahren.

Ein solches Verständnis erfordert neue Governance-Modelle. Die Hochschule muss nicht nur Schutzschichten aufbauen, sondern auch Bewusstsein fördern: für die eigene Position, für die Spannungsverhältnisse, in denen sie agiert, und für die Räume, in denen Offenheit unabdingbar bleibt. Awareness ist damit nicht nur ein technisches Schulungsthema, sondern eine epistemologische Grundhaltung. Nur wer weiß, in welcher "Schicht" er sich bewegt, kann verantwortlich handeln – und entscheiden, wann Anpassung notwendig ist und wann Widerspruch geboten.

Am Ende läuft alles auf eine einfache, aber folgenreiche Frage hinaus: **Was darf Wissenschaft nicht tun, selbst wenn es politisch gefordert wird?**

Die Antwort darauf markiert die rote Linie: **Sie darf nicht aufhören, Wissenschaft zu sein.**

Nicht aus Arroganz. Sondern aus Verantwortung für eine Gesellschaft, die ohne kritischen Widerspruch blind für ihre eigenen Machtmechanismen würde.

In einer Welt, in der der Cyberraum zunehmend Fragmentierung, Kontrolle und Nutzenorientierung unterworfen wird, bleibt die freie Wissenschaft ein Ort der Differenz. Und nach Luhmann steht am Anfang immer eine Differenz und zwar „die Einheit der Differenz von Aktualität und Potentialität“, vom dem was ist, und dem was möglich ist. Die Wissenschaft muss ein Ort sein, an dem auch das Unbequeme, das Unverwertbare und das Unzeitgemäße gedacht werden darf. Gerade deshalb ist sie so schützenswert.

14.5. Ausblick

Die Arbeit hat gezeigt: Cybersicherheit im Wissenschaftssystem ist keine rein technische Herausforderung, sondern eine strategische Gestaltungsfrage. Sie berührt zentrale Prinzipien akademischer Selbststeuerung, betrifft institutionelle Handlungsfähigkeit unter geopolitischem Druck – und verlangt nach neuen Formen der Governance, Kooperation und Reflexion. Daraus ergeben sich mehrere Anschlussfelder für zukünftige Forschung und Entwicklung.

1. Pilotprojekte zur Umsetzung und Evaluation der Empfehlungen
Ein nächster logischer Schritt wäre die gezielte Erprobung einzelner Handlungsempfehlungen in realen Hochschulkontexten. Pilotprojekte könnten etwa strategische Governance-Rollen, sektorale CERT-Cluster oder institutionelle Transferformate praktisch implementieren und hinsichtlich Wirkung, Anschlussfähigkeit und Skalierbarkeit evaluiert werden. Dadurch ließe sich die normative Fundierung dieser Arbeit mit evidenzbasierter Praxisentwicklung verbinden. Eine Beachtung Ergebnisse der Arbeit in die Neuauflage der im Koalitionsvertrag angekündigten nationalen Cybersicherheitsstrategie wäre anzustreben.

2. Erweiterung internationaler Vergleichsstudien
Die Arbeit hat auf Makroebene drei der fünf weltweit führenden Wissenschaftssysteme – Deutschland, das Vereinigte Königreich und die USA – analysiert. Der Vergleich offenbarte grundlegende Gemeinsamkeiten, aber auch kulturelle Unterschiede in der sicherheitspolitischen Rahmung von Wissenschaft. Eine Erweiterung um China und Japan, die diese globale Spitzengruppe komplettieren, wäre forschungsstrategisch hochrelevant. Allerdings erschwerten sprachliche Barrieren, differente Steuerungslogiken und einge-

schränkte Dokumentenzugänge eine adäquate Analyse im Rahmen dieser Arbeit. Zukünftige Studien oder Ergänzungen könnten diese Lücke schließen und so die weltweite Spannbreite sicherheitsbezogener Wissenschaftspolitik kartieren.

3. Analyse hybrider Bedrohungen und konzeptuelle Erweiterung durch "Knowledge Security"

Zunehmend ist erkennbar, dass Cybersicherheit und physische Sicherheit nicht mehr getrennt gedacht werden können. Hybride Bedrohungen – etwa durch gekoppelte Angriffe auf IT-Infrastruktur, physische Einrichtungen und institutionelle Vertrauensressourcen – betreffen Hochschulen in besonderer Weise. Die Verschränkung von Cyberraum und physischem Raum erzeugt neue Angriffsflächen, aber auch neue Verantwortlichkeiten.

Dies erfordert eine konzeptionelle Weiterentwicklung über klassische Cybersicherheit hinaus. Der Begriff **"Knowledge Security"** bietet hierfür eine vielversprechende Erweiterung gerade auf geopolitische Kontexte bezogen. „Knowledge security means preventing the unauthorised transfer of knowledge and technology. It also includes preventing covert influence by state actors on higher education and research, which can impair the freedom of scientific research either directly or via self-censorship“ (OECD 2022, S. 18).

4. Theoretische Weiterentwicklung des Spannungsmodells

Das in dieser Arbeit entwickelte Modell der Spannungsverhältnisse hat sich als tragfähige analytische Heuristik erwiesen, um komplexe Zielkonflikte im Zusammenspiel von Wissenschaft, Politik und Sicherheit systematisch zu erfassen. Seine konzeptionelle Weiterentwicklung – etwa im Dialog mit Resilienzforschung, Multi-Level-Governance oder Theorien kritischer Infrastrukturen – könnte neue theoretische Fundierungen liefern und seine Anwendung auf andere Felder erweitern: etwa auf medizinische Forschung, Open Science oder globale Dateninfrastrukturen.

5. Wissenschaftspolitische Reflexion und institutionelle Positionsbildung

Nicht zuletzt eröffnet die Arbeit Impulse für eine aktive, wissenschaftsseitige Positionierung in sicherheitspolitischen Diskursen. Der aufgezeigte blinde Fleck in strategischen Steuerungsarchitekturen – die fehlende explizite Benennung und Beteiligung der Wissenschaft – kann nur durch Sichtbarkeit, Koordination und strukturelle Mitsprache behoben werden. Hierfür braucht es nicht nur politische Reformen, sondern auch eine stärkere Selbstpositionierung wissenschaftlicher Akteure – etwa durch strategische Leitlinien, forschungsbasierte Politikberatung und interinstitutionelle Allianzen für resilientere Wissenssysteme.

15. Literaturverzeichnis

Allyn B (2025, March 7) OpenAI's Sam Altman warned America about Trump. Now he's partnering with him. ABC News. https://abcnews.go.com/US/openais-sam-altman-warned-america-trump-now-partnering/story?id=118145337

Alterman JB, McElwee L (2025) Pursuing Global Order in the Twenty-First Century. Online verfügbar, Abruf am 2025-04-05

Barlow JP (1996) A Declaration of the Independence of Cyberspace. Electronic Frontier Foundation, San Francisco

Bechthold-Hengelhaupt T (2020) Fake News und Desinformation aus der Sicht der Theorie sozialer Systeme. In: Pörksen B (Hg) Schlüsselwerke des Konstruktivismus. Wiesbaden, VS Verlag, S. 135–151.

Beck U (1986) Risikogesellschaft. Auf dem Weg in eine andere Moderne. Frankfurt am Main, Suhrkamp

Blank S (2017) Cyber War and Cyberterrorism. Routledge, New York

Bongiovanni I (2019) The least secure places in the universe? Cybersecurity threats to space systems. In: European Space Policy Institute (ESPI) Perspectives 98

Bonß W et al. (2015) Gesellschaftstheorie: Eine Einführung, UTB GmbH

Bussolati N (2015) The Rise of Non-State Actors in Cyberwarfare. In: Ohlin JD et. al. Cyber War: Law and Ethics for Virtual Conflicts, Oxford University Press, Oxford, S. 102 – 126

Clark D (1992) We reject: kings, presidents and voting

DFG; Leopoldina (2022) Wissenschaftsfreiheit und Wissenschaftsverantwortung – Empfehlungen zum Umgang mit sicherheitsrelevanter Forschung. Deutsche Forschungsgemeinschaft und Nationale Akademie der Wissenschaften Leopoldina, Bonn/Halle.

Drezner DW, Farrell H, Newman AL (2021) The Uses and Abuses of Weaponized Interdependence. In: Annual Meeting of the American Political Science Association (APSA), Seattle, S. 1–18

Dunn-Cavelty M (2012) Cyber-Security and Threat Politics. Routledge, New York

Dunn-Cavelty M (2012) The Militarisation of Cyberspace: Why Less May Be Better. In: Czosseck C, Ottis R, Ziolkowski K (Hrsg) Proceedings of the 4th International Conference on Cyber Conflict (CyCon 2012). NATO CCD COE Publications, Tallinn, S. 141–153

Eisenhardt, K M (1989) Building Theories from Case Study Research. Academy of Management Review, 14(4), 532–550

Eriksson J, Giacomello G (2022) Cyberspace in Space: Fragmentation, Vulnerability, and Uncertainty. In: Dunn Cavelty, M., Wenger, A. (Hrsg.): Cyber Security Politics. Socio-Technological Transformations and Political Fragmentation

Fukuyama F (1992) The End of History and the Last Man. New York: Free Press

Gartzke E (2013) The Myth of Cyberwar: Bringing War in Cyberspace Back Down to E-arth. International Security 38(2): 41–73

Henckmann W (1998) Einführung in die Philosophie Max Schelers. C.H. Beck, München

Hobbes T (1651) Leviathan. Andrew Crooke, London

Keller, R (2011) Wissenssoziologische Diskursanalyse. VS Verlag für Sozialwissenschaften

Knoblauch H (2014) Wissenssoziologie. De Gruyter, Berlin

Krüger P S (2018) „Agile Abschreckung“ gegen Bedrohungen aus dem Cyber Raum – Optionen für deutsche Politik. SIRIUS – Zeitschrift für Strategische Analysen, 2(2), 126–136

Kuehl DT (2009) From Cyberspace to Cyberpower. In: Kramer FD, Starr S, Wentz L (Hrsg.): Cyberpower and National Security. National Defense University Press, Washington, S. 24–42

Lange, B, Bötticher, A (2015) Cybersicherheit. In: Lange, B., Bötticher, A. (Hrsg.): Cybersicherheit – Grundlagen, Strategien, Maßnahmen. Springer VS, Wiesbaden, S. 1–22

Luhmann, N (1988) Macht. Stuttgart: Enke

Luhmann N (1992) Die Wissenschaft der Gesellschaft. Suhrkamp, Frankfurt am Main

Luhmann N (1997) Die Gesellschaft der Gesellschaft. Suhrkamp, Frankfurt am Main

Luhmann, N (2004) Einführung in die Systemtheorie. Carl-Auer, Heidelberg

Masala C (2023) Weltunordnung: Die globalen Krisen und das Versagen des Westens. C.H. Beck, München

Mayring P (2025) Qualitative Inhaltsanalyse mit ChatGPT: Fallstricke, grobe Annäherungen und grobe Fehler. Ein Erfahrungsbericht. Forum Qualitative Sozialforschung / Forum: Qualitative Social Research, 26(1), Art. 4. DOI

Mayring P, Fenzl T (2019) Qualitative Inhaltsanalyse. In: Baur N, Blasius J (Hrsg.): Handbuch Methoden der empirischen Sozialforschung. Springer Fachmedien Wiesbaden GmbH. DOI

Möller D P. F. (2023) Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices. Springer, Cham

Möller TA (2023) Cybersicherheit für Staat, Wirtschaft und Gesellschaft. In: Zeitschrift für Außen- und Sicherheitspolitik, 16, 1–12

Muckel P (2011) Die Entwicklung von Kategorien mit der Methode der Grounded Theory. In: Mey K, Mruck K (Hrsg.): Grounded Theory Reader. Springer Fachmedien Wiesbaden GmbH

Neumann PR (2022) Die neue Weltunordnung: Wie sich der Westen selbst zerstört. Rowohlt, Hamburg

Nye JS (2010) Cyber Power. Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge

Pohle J. & Thiel T. (2020) Digital sovereignty. Internet Policy Review, 9(4). https://doi.org/10.14763/2020.4.1532

Rattray GJ (2003) Strategic Warfare in Cyberspace. MIT Press, Cambridge

Rattray GJ (2009) An Environmental Approach to Understanding Cyberpower.In: Kramer, Starr, Wentz (Hrsg.): Cyberpower and National Security, Kapitel 10. National Defense University Press, Washington D.C

Roose K (2021) Futureproof: 9 Rules for Humans in the Age of Automation. Random House, New York

Schmitt S & Spiewak M. (2025, April 2) Die deutsche Wissenschaft und der drohende Rückzug der USA. Die Zeit. https://www.zeit.de/2025/15/wissenschaft-usa-zusammenarbeit-deutschland-donald-trump

Schulmann H (2024) Stellungnahme zur Umsetzung der NIS2-Richtlinie im Hochschulbereich. ATHENE, Darmstadt, Online verfügbar unter: https://www.bundestag.de/resource/blob/1027446/1e333b31c1f017dfc95bb9b84362b6a2/20-4-523-H.pdf, Abruf 12.04.2025

Singer PW, Brooking ET (2018) LikeWar: The Weaponization of Social Media. Houghton Mifflin Harcourt, Boston

Solbrig K, Ennen G (2014) Personelle Ausstattung von ITSicherheitsteams. InnovVerwalt 36: 26–30. DOI

Thiedeke U (2009) Soziologie des Cyberspace. UVK, Konstanz

Tolkiehn J, Rodrigues A, Dengler S, Kacprowski T (2025) Advancing AI-driven thematic analysis in qualitative research. *BMC Medical Informatics and Decision Making*. https://doi.org/10.1186/s12911-025-02961-5

Tran B-L, Grue K, Kwan LK et al. (2024) ChatGPT for Automated Qualitative Research: Content Analysis of Online Forums. *JMIR Formative Research*. https://www.jmir.org/2024/1/e59050/

Valeriano B, Maness RC (2015) Cyber War versus Cyber Realities. International Studies Quarterly 59(2): 302–315

Vance JD (2025) Rede auf der Münchner Sicherheitskonferenz 2025

von der Heyde M, Gerl A (2022) Entwicklungsstand der CIO-Funktion und hochschulübergreifenden IT-Governance im Kontext der Digitalen Transformation an Hochschulen in Bayern. HMD 59: 881–895. DOI

Voo J, Hemani J, Cassidy P (2022) National Cyber Power Index 2022. Harvard Kennedy School, Belfer Center

Weber M (1972) Wirtschaft und Gesellschaft. Mohr Siebeck, Tübingen.

Yin, R K (2018) Case Study Research and Applications: Design and Methods (6th ed.). Thousand Oaks, CA: SAGE Publications

Zettl-Schabath A (2021) Cyber Security and International Relations. Nomos, Baden-Baden

Zettl, K. (2022) Macht im Cyberspace: Eine Übersicht der bisherigen Forschung und künftiger Perspektiven anhand des Proxy-Konzepts. Zeitschrift für Außen- und Sicherheitspolitik 11, 65–90 (2022). https://doi.org/10.1007/s42597-021-00064-2

Zhang Y, Yang J, Lin K, Lee D (2024) When Qualitative Research Meets Large Language Model: Exploring the Potential of QualiGPT as a Tool for Qualitative Coding. *arXiv preprint*. https://arxiv.org/abs/2407.14925

16. Quellenverzeichnis

Bayerischer Oberster Rechnungshof (2021) Beratende Äußerung zum IT-Einsatz bei den Universitäten. München. Online verfügbar, Abruf am 2025-04-14

Bundesministerium des Innern, für Bau und Heimat (BMI) (2021) Cybersicherheitsstrategie für Deutschland 2021. PDF, Abruf am 2025-04-05

Burk M, Hetze P (2024) Hochschulbarometer 2024. Stifterverband für die Deutsche Wissenschaft, Essen

CDU, CSU und SPD (2025) Koalitionsvertrag 2025. Verantwortung für Deutschland. 21. Legislaturperiode. Berlin

CDU, CSU und SPD (2025) Verhandlungspapier Koalitionsvertrag AG 8: Bildung, Forschung und Innovation. Online verfügbar, Abruf am 2025-04-05

CIO Baden-Württemberg und Bayern (2025) Digitale Souveränität an Universitäten und Hochschulen. Positionspapier. 28. März 2025. Online verfügbar, Abruf am 2025-04-14

Department for Science, Innovation and Technology (DSIT) (2024) Cyber Security Breaches Survey 2024 – Education Institutions Annex. Online verfügbar, Abruf am 2025-04-17

DH.NRW (2025) Konzept „Netzwerk Informationssicherheit.nrw“. Online verfügbar, Abruf am 2025-04-14

Digitale Hochschule NRW (2025) Vereinbarung zur Cybersicherheit (VzC). Online verfügbar, Abruf am 2025-04-14

Digitalverbund Bayern (2020) Hochschulinformationssicherheitsprogramm – HISP. Online verfügbar, Abruf am 2025-04-05

Digitalverbund Bayern (2025) Strategie und Maßnahmen für digitale Sicherheit an Hochschulen. Online verfügbar, Abruf am 2025-04-05

EDUCAUSE (2024) Horizon Report: 2024 Cybersecurity and Privacy Edition. Online verfügbar, Abruf am 2025-04-05

Europäische Kommission (2020) Shaping Europe's Digital Future. PDF, Abruf am 2025-04-05

Europäische Union (2022) Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS2-Richtlinie). Amtsblatt der Europäischen Union, L 333/80. Online verfügbar, Abruf am 2025-04-05

HITS IS (2025), Fötinger C S, Schneider U, Auditbericht Informationssicherheit 2022–2024. Hochschulübergreifender IT-Service für Informationssicherheit (HITS IS), unveröffentlichtes internes Dokument, Stand: 31. März 2025

HITS IS (2025), Fötinger C S, Schneider U, Auditbericht Informationssicherheit 2022–2024. Hochschulübergreifender IT-Service für Informationssicherheit (HITS IS), unveröffentlichtes internes Dokument, Stand: 31. März 2025

Freistaat Bayern (2023) Rahmenvereinbarung Hochschulen 2023–2027. Online verfügbar, Abruf am 2025-04-14

Hochschulrektorenkonferenz (2025) Empfehlungen an den Bund zur Stärkung der Cybersicherheit. Online verfügbar, Abruf am 2025-04-14

Inside Higher Ed; Hanover Research (2024) IHE 2024 Survey of Campus Chief Technology/Information Officers (CTO/CIO Survey). Washington, D.C., Online verfügbar, Abruf am 2025-04-14

IT-Strategie 2022: Universität Bayern e.V. & Hochschule Bayern e.V. (Hrsg.) (2022) IT-Strategie der bayerischen Hochschulen. Strategische Handlungsfelder, Governance und Kooperationsstrukturen. Version vom 20. Januar 2022. Online verfügbar, Abruf am 2025-04-14

Kon Briefing Research. (n.d.) Cyberangriffe auf Hochschulen. aufgerufen am 13.04.2025, https://konbriefing.com/de-topics/cyber-angriffe-universitaeten.html

Land Baden-Württemberg (2025) Hochschulfinanzierungsvereinbarung III (HoFV III) 2026–2030. Online verfügbar, Abruf am 2025-04-14

Landeshochschulkonferenz Niedersachsen (2024) Gemeinsam digital – Gesamtstrategie 2030 der Hochschule.digital Niedersachsen. Online verfügbar, Abruf am 2025-04-14

OECD (2022) Integrity and Security in the Global Research Ecosystem. Policies and Practices to Prevent Misuse and Foreign Interference, Paris: OECD Publishing. DOI: https://doi.org/10.1787/c2766d66-en

Universities UK (2023) Cyber Security and Universities – Managing the Risk 2023 Update. Online verfügbar, Abruf am 2025-04-17

UK Government (2022) National Cyber Strategy 2022. PDF, Abruf am 2025-04-05

Waterfall Security Solutions (2024) 2024 Threat Report – OT Cyberattacks with Physical Consequences. Online verfügbar, Abruf am 2025-04-05

Wissenschaftsrat (2023) Souveränität und Sicherheit der Wissenschaft im digitalen Raum. Online verfügbar, Abruf am 2025-04-05

ZKI e.V. (2022) IT-Grundschutz-Profil für Hochschulen. Online verfügbar, Abruf am 2025-04-05

ZKI-Arbeitskreis Strategie & Organisation (2024) Ergebnisse der ZKI Top-Trends-Umfrage 2024. Online verfügbar, Abruf am 2025-04-17

17. Anlagenverzeichnis

Anlage 1: Kodierleitfaden

Anlage 1: Kodierleitfaden

Kategorie	Definition	Ankerbeispiele	Kodierregeln
K1: Internationale Kooperation	Positive Bezugnahme auf internationale wissenschaftliche Kooperation, Mobilität und grenzüberschreitende Forschung.	„Wissenschaft lebt vom internationalen Austausch.“ / „Unsere Universität pflegt zahlreiche Partnerschaften weltweit.“	Aussagen müssen explizit internationale Kooperation oder Mobilität als positiv hervorheben oder verteidigen.
K2: Fragmentierung nationaler Systeme	Betonung von Abschottung, Exportkontrollen, Sanktionsregimen oder politischer Trennung der Wissenschaftsräume.	„Neue Exportkontrollen erschweren die Zusammenarbeit mit Partnern.“ / „Sanktionspolitik betrifft nun auch akademische Kooperationen.“	Aussagen müssen Fragmentierung nationaler Systeme thematisieren oder negative Auswirkungen politischer Maßnahmen auf Kooperationen betonen.
K3: Offenheit	Positive Bezugnahme auf Open Science, offene Daten und internationale Transparenz in Forschung.	„Wir setzen auf offene Datenplattformen.“ / „Open Science ist Grundlage unserer Forschungsstrategie.“	Aussagen müssen die Förderung oder Verteidigung von Offenheit im wissenschaftlichen Kontext thematisieren.
K4: IT-Sicherheitsanforderungen	Betonung des Schutzes wissenschaftlicher Daten, IT-Sicherheitsvorgaben oder Zugangsbeschränkungen.	„Sensible Forschungsdaten müssen besonders geschützt werden.“ / „Zugriffsrechte wurden restriktiver gestaltet.“	Aussagen müssen explizit den Schutzbedarf oder IT-Sicherheitsvorgaben im Wissenschaftskontext thematisieren.
K5: Technologische Abhängigkeit	Hinweise auf Abhängigkeit von Drittanbietern, proprietären Cloud-Diensten oder Softwaremonopolen.	„Unsere Infrastruktur basiert auf wenigen großen Anbietern.“ / „Es bestehen Abhängigkeiten von internationalen Cloud-Diensten.“	Aussagen müssen technologische Abhängigkeiten oder strukturelle Abhängigkeiten im IT-Bereich thematisieren.
K6: Digitale Souveränität	Hinweise auf Strategien zur Eigenständigkeit, Nutzung von Open-Source-Technologien oder Aufbau eigener IT-Infrastrukturen.	„Wir streben digitale Unabhängigkeit an.“ / „Der Einsatz von Open-Source-Lösungen wird priorisiert.“	Aussagen müssen Strategien oder Bestrebungen zu mehr digitaler Souveränität oder technologischer Eigenständigkeit adressieren.
K7: Politisches Agendasetting	Hinweise auf politische Einflussnahme, Agenda-Setting durch Fördergeber oder sicherheitspolitische Zielvorgaben.	„Neue Förderlinien setzen sicherheitspolitische Schwerpunkte.“ / „Politische Erwartungen prägen zunehmend die Forschungsprioritäten.“	Aussagen müssen politische Einflussnahmen oder Steuerungsversuche thematisieren.
K8: Wissenschaftsfreiheit	Verteidigung wissenschaftlicher Autonomie, Kritik an politischer Steuerung oder Einschränkungen.	„Forschung muss frei von politischer Einflussnahme bleiben.“ / „Unsere Autonomie ist nicht verhandelbar.“	Aussagen müssen explizit auf die Verteidigung der Wissenschaftsfreiheit oder Kritik an deren Einschränkung abzielen.
K9: Hochwertziele	Hinweise auf Hochschulen als Ziel von Cyberangriffen, Bedrohung sensibler Forschung oder besondere Gefährdung.	„Universitäten sind zunehmend Ziel von Cyberattacken.“ / „Unsere sensiblen Forschungsdaten sind hochgradig gefährdet.“	Aussagen müssen Hochschulen explizit als verwundbare Ziele oder Objekte von Bedrohungen darstellen.
K10: Hochschulen als Sicherheitsakteure	Hochschulen als aktive Akteure im Bereich Cybersicherheit, z.B. durch For-	„Unsere Universität forscht aktiv an neuen Cybersicherheitslösungen.“ / „Wir engagieren	Aussagen müssen Hochschulen explizit als aktive Gestalter oder produzierende

	schungsbeiträge, Technologieentwicklung, Technologieerwartungen, Awareness-Programme oder Sicherheitstrainings.	uns in nationalen Sicherheitsnetzwerken.“ / „Studierende erhalten verpflichtende Awareness-Schulungen zu IT-Sicherheit.“ / „Die Hochschule wird als Partner in der nationalen Cybersicherheitsstrategie genannt.“	Akteure im Bereich Cybersicherheit darstellen (z.B. durch Forschung, Sicherheitsprojekte, Trainingsangebote oder Mitwirkung an Sicherheitsnetzwerken). Passive Darstellungen von Bedrohungen oder reiner Betroffenheit sind nicht zu codieren.