Dennis Eckhardt, Nelli Feist, Alexandros Gazos, Tilo Grenz, Daniel Guagnin, Laura Kocksch, Sezgin Sönmez, Basil Wiesse*

Für eine multitemporale Bestimmung von Cybersicherheit: Spannungsverhältnisse digitaler Gesellschaften

Towards a Multitemporal Definition of Cybersecurity: Tensions of Digital Societies

https://doi.org/10.1515/zfsoz-2026-3010

Zusammenfassung: In diesem Beitrag adressieren wir vernachlässigte Aspekte der Digitalisierung. Cybersicherheit erweist sich als interdisziplinäres Feld, das zu seiner Untersuchung Multiperspektivität einfordert, und welches insbesondere durch die Produktion und Bearbeitung multipler Zeitlichkeiten gekennzeichnet ist. Zeitlichkeit, so unser Argument, erlaubt es, wesentliche Spannungsverhältnisse soziotechnischer Ordnung überhaupt erst zu erfassen und dabei über technikzentrierte Ereignislogiken hinauszugehen. Kernthese dieses Aufsatzes ist, dass sich Cybersicherheit in konkreten organisationalen Kontexten sowie in einem übergreifenden globalen Cybersicherheitsregime als Kooperation unter den Bedingungen zeitlicher Spannungsverhältnisse erweist. Jeweils bearbeitete und hervorgebrachte Grenzobjekte wie z. B. materielle Taktiken, IT-Sicherheitsstandards und Resilienzkonzepte vermitteln dabei Wissen; Akteure und Materialität bringen allerdings nicht nur interpretative Flexibilität zum Ausdruck. Eine infrastrukturelle Tiefenschicht, die durch multiple technische Zeitlichkeiten gekennzeichnet ist, verbirgt sich hinter der Arbeit an und mit Grenzobjekten der Cybersecurity. Anhand von drei empirischen Forschungsprojekten (mundane Praxis, Standardisierung und Resilienz) präsentiert der Beitrag temporale Logiken digitalisierter Gesellschaften und mit diesen korrelierende Spannungsverhältnisse: a) Ereigniszeitlichkeit, b) infrastrukturelle Zeitlichkeit sowie c) reflexive Zeitlichkeit.

Schlagworte: Zeitlichkeit; Cybersicherheit; Multiperspektivität; Grenzobjekte; Digitale Infrastruktur; Resilienz.

Abstract: This contribution addresses neglected aspects of digitalization. We found cybersecurity, an interdisciplinary field calling for multiperspectival investigation, to be suffused with the production and processing of multiple temporalities. A focus on temporality allows us to grasp essential tensions of socio-technical orders and move beyond technocentric logics of events. The primary thesis of our article posits that cybersecurity displays a form of cooperation under fraught temporal conditions. We show this to be the case both in concrete organizational contexts and in an overarching global cybersecurity regime. Boundary objects, such as material tactics, IT security standards, and concepts of resilience, play an important role here. They mediate knowledge as they are continually shaped and

Anmerkung: Alle Autor*innen haben gleichermaßen zum Artikel beigetragen.

***Korrespondenzautor: Basil Wiesse**, Soziologie III, KU Eichstätt-Ingolstadt, Kapuzinergasse 2, 85072 Eichstätt,
E-Mail: basil.wiesse@ku.de, https://orcid.org/0000-0002-3606-7798
Dennis Eckhardt, Institut für Kulturanthropologie und Europäische Ethnologie, Goethe-Universität, Norbert-Wollheim-Platz 1, 60629 Frankfurt am Main, E-Mail: dennis.eckhardt@fau.de,
https://orcid.org/0000-0002-5935-9144
Nelli Feist, FAU Erlangen-Nürnberg, Lehrstuhl für Soziologie (Technik – Arbeit – Gesellschaft), Fürther Str. 246c, 90429 Nürnberg,
E-Mail: nelli.feist@fau.de, https://orcid.org/0009-0008-9712-1218
Alexandros Gazos, Institut für Technikfolgenabschätzung und Systemanalyse, Karlsruher Institut für Technologie, Karlstraße 11, 76133 Karlsruhe, E-Mail: alexandros.gazos@kit.edu,
https://orcid.org/0000-0002-4779-6179
Tilo Grenz, Pädagogische Hochschule Thurgau, Unterer Schulweg 3, Postfach, CH-8280 Kreuzlingen 1, E-Mail: Tilo.Grenz@phtg.ch,
https://orcid.org/0000-0002-6255-3060
Daniel Guagnin, Freier Mitarbeiter, nexus Institut für Kooperationsmanagement und interdisziplinäre Forschung GmbH, EUREF-Campus 15a, D-10829 Berlin, E-Mail: soziologe@guagnin.de,
https://orcid.org/0009-0009-7715-0270
Laura Kocksch, The Techno-Anthropology Lab, Department of Culture and Communication, Aalborg University Copenhagen, A C Meyers Vænge 15, 2450 København SV, Denmark, E-Mail: laurak@ikk.aau.dk,
https://orcid.org/0000-0003-4661-2638
Sezgin Sönmez, Institut für Soziologie, Technische Universität Berlin, Fraunhoferstraße 33–36, 10587 Berlin,
E-Mail: sezgin.soenmez@tu-berlin.de,
https://orcid.org/0009-0003-7583-3779

reconfigured in practice, exhibiting interpretive flexibility embodied across actors and materialities. An underlying infrastructural layer, marked by multiple technical temporalities, operates beneath the practices surrounding boundary objects of cybersecurity. Based on three empirical projects (mundane practices, standardization and resilience) the contribution presents the temporal logics of digitized societies and their associated tensions: a) event temporality, b) infrastructural temporality, and c) reflexive temporality.

Keywords: Temporality; Cybersecurity; Multiperspectivity; Boundary Objects; Digital Infrastructure; Resilience.

1 Einleitung

Cybersicherheit wird zunehmend als globale und gesamtgesellschaftliche Herausforderung verstanden, die sich längst nicht mehr nur auf den Schutz von Daten und Informationen von einzelnen Organisationen oder Individuen beschränkt. Die Fülle an staatlichen und zivilgesellschaftlichen Institutionen und Organisationen, die sich mit dem Thema Cybersicherheit beschäftigen, die steigende Sichtbarkeit und Relevanz von politischen Programmen und Maßnahmen über alle gesellschaftlichen Teilbereiche hinweg sowie die Zunahme der ökonomischen und militärischen Bedeutung von Cybersicherheit deuten auf einen umfassenden Wendepunkt innerhalb eines globalen Digitalisierungsprozesses hin. Wurde die Logik der Digitalisierung vormals im Sinne eines unvermeidbaren Globalisierungsphänomens noch von Diskursen und Imaginationen von Fortschritt, Informatisierung, Demokratisierung und wirtschaftlicher Entwicklung geprägt, zeichnet sich spätestens seit den Enthüllungen von Edward Snowden im Jahre 2013 ein Wandel von allgemeinen Problembestimmungen und soziotechnischen Bearbeitungsformen innerhalb von digitalisierten Gesellschaften ab (Bauman et al. 2014; Lyon 2015). Die Zunahme und öffentliche Sichtbarkeit von Cyberangriffen von staatlichen wie nicht-staatlichen Akteur*innen, die Normalisierung hybrider Kriegsführung sowie entsprechende Institutionalisierungs- und Vernetzungsprozesse auf den Ebenen lokaler, regionaler, nationaler sowie supranationaler Sicherheitspolitik und schließlich die Kritikalität digitaler Unternehmen, Haushalte und Infrastrukturen deuten auf zunehmende Fragilitäten und Bruchlinien des seit über fünfzig Jahren fortlaufenden Digitalisierungsprozesses hin. Damit einher geht eine Pluralisierung der Akteur*innen, die sich mit Cybersicherheit befassen (z. B. Rupp 2022 zur Komplexität der Europäischen „Cybersicherheits-Architektur“).

Die technischen Infrastrukturen, Diskurse und Praktiken der Cybersicherheit sollen Daten, Geräte und vernetzte IT-Systeme vor externen Angreifer*innen sowie internem Missbrauch schützen und umfassen dabei ein ausdifferenziertes Feld, dessen gesellschaftliche Relevanz sich in Institutionen wie Fachkonferenzen, Ministerien, staatlichen und internationalen Programmen sowie in Ausbildungsgängen und professionalisierten Expert*innenrollen zeigt. Dennoch wurde innerhalb der – nicht nur – deutschsprachigen Soziologie das Thema Cybersicherheit bisher weitgehend ignoriert, obschon Sozialität unter Bedingungen digitalmedialer Kommunikation seit Jahren intensiv diskutiert wird (Seyfert & Roberge 2017; Couldry & Hepp 2017; Hepp 2020; Knoblauch 2020). Dabei ist schwer auszumachen, ob diese bemerkenswerte soziologische Vernachlässigung des praktisch und politisch so relevanten Themas Cybersicherheit daher rührt, dass dieses lediglich als Nebenerscheinung digitaler Gesellschaften aufgefasst wird; oder aber, weil informations-, politik- und technikwissenschaftliche Definitionen und Begrifflichkeiten in der soziologischen Rezeption schlichtweg adaptiert und seltener epistemisch hinterfragt werden. Die spezifischen konstitutiven Leistungen von Cybersicherheit für die Hervorbringung digitaler Gesellschaften – so unser Argument – werden somit nicht angemessen adressiert, und sozialwissenschaftliche Perspektiven bleiben vielfach darauf beschränkt, die Identifikation von technischen Defiziten und Schwachstellen bei Nutzer*innen oder Organisationen zu rekonstruieren (Kocksch & Sørensen 2023). Der soziologische Blick auf Cybersicherheit könnte drängende Fragen digitaler Verhältnisse neu beleuchten, gerade weil digitale Infrastrukturen nicht einfach ‚anfällig‘ sind, ihre Ungewissheiten und Unsicherheiten werden soziotechnisch hervorgebracht: durch digitale, physische und alltagspraktische Komplexitäten, globale und ökonomische Abhängigkeitsverhältnisse, permanente Veränderungs- und Anpassungszwänge, wiederkehrende Update-Zyklen und heterogene Kopplungen. Fragilität und Vulnerabilität sind weder lediglich das Ergebnis von Bedrohungen und Angriffen von ‚außen‘ oder strukturelle Eigenschaften des Forschungsfeldes, sondern selbst materiell- und kontextgebundene Zuschreibungen, die teils strittig und widersprüchlich, aber immer zeitlich situiert sind.

Cybersicherheit betrifft damit Diskurse, Praktiken und Infrastrukturen, die die fortlaufende Generierung sozialen Sinns unter digitalen Bedingungen überhaupt erst ermöglichen, indem sie sich um weitgehend störungsfreie Kommunikationsabläufe bemühen und die zeitübergreifende Stabilisierung kommunikativer Praktiken als Handlungsproblem organisieren. Entsprechend geht es uns nicht nur darum, ein empirisches Desiderat zu bedienen, also neuere professionelle Sicherheitspraktiken und Institutionen zu beschreiben, sondern darum, an Cybersicherheit als ver-

dichteter Problemzone die Dynamiken der informationstechnischen Tiefenstruktur von Gegenwartsgesellschaften beobachtbar und zugänglich zu machen, einschließlich der Frage, wie Ungewissheiten und Risiken produziert, verteilt und bearbeitbar gemacht werden. Der praktische Umgang des Felds ‚Cybersicherheit' mit temporalen Anforderungen erscheint uns hierfür zentral.

Temporalität fungiert in unserem Zugriff nicht als bloßes Merkmal, das sich der unmittelbaren empirischen Beobachtung des Feldes entnehmen ließe, sondern als die Bedingung, unter der dieses heterogene Feld als ein zusammenhängender Gegenstand überhaupt erst erscheinen kann. In dieser grundlegend konstitutiven Position ist Temporalität also nicht einfach *eine* Dimension von Cybersicherheit unter anderen. Ebenso wenig aber ist sie als einfache Möglichkeitsbedingung zu verstehen. Temporalität wird in den Praktiken des Feldes in und um den feldtypischen, materiellen Objektgestalten von Cybersicherheit selbst fortlaufend hervorgebracht, verhandelt und koordiniert. In diesem Sinne liefern wir im Folgenden keine soziologische Definition von Cybersicherheit, sondern bestimmen die prozessuale Bedingung, unter der „Cybersicherheit" als ein Bestimmbares erst auftritt – eine Bedingung, die im Feld zugleich praktisch hervorgebracht und reflexiv bearbeitet wird.

Bei zunehmender Konnektivität, Interaktivität und Ausdifferenzierung soziotechnischer Strukturen bleiben die genannten Dynamiken alltagsweltlich weitestgehend opak und sind zugleich hochgradig volatil. Erst im Moment des Bruchs, etwa bei erfolgten Cyberangriffen, organisationalen Zielkonflikten oder gesamtgesellschaftlichen Krisen, werden latente und neue Verletzlichkeiten offenbar sowie die daraus resultierenden Folgen alltagsweltlich wahrnehmbar. Unsere zentrale These lautet daher, dass die komplexen Akteursarrangements, d. h. private, zivilgesellschaftliche, staatliche und wirtschaftliche Akteur*innen die – vermittelt, indirekt oder direkt – am Feld Cybersicherheit beteiligt sind, jeweils vielfältige Aspekte von Cybersicherheit mit jeweils spezifischen Zeitlichkeitslogiken bearbeiten, hervorbringen und materialisieren. Dabei stehen unterschiedliche technische, infrastrukturelle und politische Ziele und Strategien, praktische Notwendigkeiten und diskursive Formationen sowie die damit verbundenen Disziplinen und Professionen nebeneinander (Deibert 2016: 172).[1]

Dieser Multiperspektivität entspricht die interdisziplinäre Zusammensetzung unserer Autor*innengruppe. Sie vereint soziologische, anthropologische, ethnologische und informatische Perspektiven und bringt damit Disziplinen zusammen, die teils unterschiedliche Begriffe von Praxis, Strukturen, Technik und Wissen einbringen. Anstatt diese Perspektivenheterogenität zu nivellieren, möchten wir sie über den gemeinsamen Fokus auf Zeitlichkeit soziologisch anschlussfähig machen.[2] Cybersicherheit erscheint dann als ein multitemporales Feld, das sich über feldtypische Konstellationen von Grenzobjekten organisiert, deren koordinierende Funktion wir im weiteren Verlauf auf eine infrastrukturell-zeitliche Tiefenschicht zurückführen (vgl. Abschnitt 5). Unsere interdisziplinäre Autor*innengruppe versteht sich insofern als performative Analogie zu diesem Zugriff: Nicht theoretischer Konsens, sondern die gemeinsame analytische Bearbeitung von Zeitlichkeit ermöglicht es, unterschiedliche disziplinäre Perspektiven produktiv aufeinander zu beziehen. Mit unserem Vorgehen ist denn auch der Anspruch und Bedarf einer dialogischen Multiparadigmatik verbunden, die auch das Feld der Cybersicherheit kennzeichnet. Hierdurch tritt dann ein Feld hervor, das sich in empirischen Beobachtungen als Relation heterogener Wissensformen, professioneller Routinen und technischer Artefakte rekonstruieren lässt.

Der Aufsatz ist folgendermaßen strukturiert: Abschnitt (2) zeichnet zentrale, temporale Bestimmungen von Cybersicherheit aus verschiedenen Forschungsperspektiven nach und zeigt, wie diese durch bestimmte, oft implizite Konzeptionen von Akteurskonstellationen und Prozesslogiken geprägt sind. Daraufhin (3) präsentieren wir anhand von drei aktuellen Forschungsprojekten aus dem Kreis des Autor*innengruppe die Differenzen zeitlicher Praktiken und Strukturen innerhalb der Cybersicherheit. Aus jenen empirischen Beobachtungen heraus entwickeln wir (4) den Vorschlag, Cybersicherheit als ein multitemporales Spannungsfeld zu fassen und rekonstruieren hierbei drei Logiken soziotechnischer Zeitlichkeit. Abschließend (5) werden die Einsichten auf eine – insbesondere in Prozessen der Cybersicherheit zu erschließende – temporale Signatur digitaler Gegenwartsgesellschaften zusammengefasst und für eine den multiplen Zeitlichkeiten angemessene, sozialwissenschaftliche Multiperspektivität plädiert.

1 Zu kontroversen Diskussionen über unterschiedliche Sicherheitsverständnisse verschiedener Stakeholder im Bereich der Cybersicherheit vgl. auch Guagnin et al. (2024) sowie Guagnin (2024).

2 Der vorliegende Beitrag sowie der kontinuierliche Austausch des Autor*innengruppe gingen wesentlich aus einer Ad-Hoc-Gruppe im Rahmen des 41. Kongresses der DGS in Bielefeld hervor (organisiert von T. Grenz und S. Sönmez in Kooperation mit dem AK Digitalisierung und Organisation der Sektion Organisationssoziologie der DGS). Anlass war die gemeinsame Beobachtung, dass Cybersecurity zwar über disziplinäre Ränder hinaus an Relevanz gewinnt, eine differenzierte soziologische Auseinandersetzung jedoch bislang ein Desiderat darstellt.

2 Spuren einer (multi)temporalen Bestimmung von Cybersicherheit

Wichtige Impulse für eine disziplinäre Beschäftigung mit Cybersicherheit als Gegenstand eigenen Rechts kommen aus der Politikwissenschaft, in der entlang eines prognostizierten „Cyber Wars" die Rolle staatlicher Akteur*innen in Bezug auf Militarisierung und Multistakeholder-Governance-Prozesse intensiv diskutiert werden (Deibert 2003; Deibert & Crete-Nishihata 2012; Dunn Cavelty 2013, 2015; Liff 2012; Rid 2012; Saco 1999; Stone 2013). Innerhalb der so firmierten und politikwissenschaftlich inspirierten Security Studies wird Cybersicherheit vor allem nach den Snowden-Enthüllungen vermehrt thematisiert und unter anderem als Schauplatz von „Technonationalism" (vgl. Möllers 2021) oder einer „Cyberrevolution" (Kello 2013) konzeptualisiert. Als staatliches Handeln und Instrument der Kriegsführung wird Cybersicherheit synonym für eine Verteidigung eigener Territorien bzw. dem Angriff auf fremde Territorien in digitalisierten Gesellschaften verwendet. Als Sozialfiguren und Akteur*innen jener neuen Dimension gesellschaftlicher Auseinandersetzung wurden u. a. staatliche wie nicht-staatlich organisierte Hackergruppen (Buchanan 2016), ‚Cyber-Söldner' (Maurer 2018), oder Online-Propagandisten (Kamis & Thiel 2015) ausgemacht. Ebenso wurden Technologien wie etwa Viren und Bots wiederkehrend thematisiert (Parikka 2007; Szor 2005). Ein besonders einsichtsreicher Fall stellt der organisatorisch und technisch komplex koordinierte Angriff auf das iranische Atomprogramm durch den Stuxnet-Virus dar, der zeitlich einen erheblichen Vorlauf zur Umsetzung erforderte (Farwell & Rohozinski 2011; Lindsay 2013).

In den International Relations sind es u. a. Gartzke und Lindsay (Gartzke 2013; Gartzke & Lindsay 2015), die den Zusammenhang zwischen einer Militarisierung des Cyberraums und der semantisch-narrativen Einteilung in offensive und defensive Akteur*innen und Kapazitäten aufgegriffen haben. Hierbei gerieten auch Attribution, d. h. die von staatlichen wie nicht-staatlichen Akteur*innen vorgenommene Zurechnung, sowie Legitimation von Cyberangriffen und Cyberabwehrmaßnahmen in den Blick (vgl. Lupovici 2016; Rid & Buchanan 2015). In diesem Umfeld argumentieren Stevens (2012) und Taddeo (2018) für einen Wandel gesellschaftlicher Normen und Standards in Bezug auf ein neues Paradigma der Cybersicherheit.

Obgleich die politikwissenschaftlichen Annäherungen und Bestimmungen wegweisend sind, erscheinen sie sozialwissenschaftlich nicht erschöpfend. Temporale Eigentümlichkeiten von Cybersicherheit werden zwar hervorgehoben, ohne sie jedoch reflexiv zu wenden. Die soziologische Hervorhebung temporaler Aspekte von Cybersicherheit dient daher nicht lediglich der Ergänzung bestehender empirischer Perspektiven. Vielmehr richtet sie den Blick auf die Bedingungen, unter denen sich heterogene Praktiken, Akteur*innen und Wissensformen überhaupt als gemeinsames Feld der Cybersicherheit konstituieren und rekonstruieren lassen.

Zugleich finden sich in der Literatur Betonungen einer temporalen Dimension von Cybersicherheit, die wir an diesem Punkt aufgreifen, bevor wir im weiteren Verlauf über sie hinausgehen. Die Kopenhagener Schule der Sicherheitsstudien verweist auf den Zusammenhang zwischen Prozessen der Versicherheitlichung und diagnostizierter Krisenhaftigkeit. Ein Kernbefund der Securitization-These lautet dann, dass unter dem Verweis auf Krisen außergewöhnliche Maßnahmen als notwendig und legitim dargestellt werden können (Buzan et al. 1998). Hansen und Nissenbaum (2009) zeigen auf, wie Cyberbedrohungen als dringende und existenzielle Herausforderungen dargestellt werden, was zu einer verstärkten politischen und sicherheitspolitischen Aufmerksamkeit führt und Forderungen nach politischen Maßnahmen evozieren. Dies verweist auf die Rolle von Ereigniszeitlichkeit im Zusammenhang mit Cybersicherheit.

An der Schnittstelle von Informatik und Cybersicherheit hat Miller (2007) an der zeitlichen Logik der sogenannten ‚Zero-Day-Exploits' die Ökonomisierung digitaler Sicherheitslücken rekonstruiert. Dabei handelt es sich um Spezialwissen zum Ausnutzen bestimmter sicherheitsrelevanter Schwachstellen in Computersystemen, die von den Verantwortlichen, insbesondere Softwareherstellern, noch unentdeckt geblieben sind und nicht behoben wurden. Bis zu ihrer Entdeckung (und über den Zeitraum der allmählichen Verbreitung und Etablierung der korrigierten Systeme) haben Bedrohungsakteur*innen, oft kriminelle oder staatlich unterstützte Gruppen, ein Zeitfenster, dieses Wissen zu nutzen, um gezielte Angriffe durchzuführen. Miller (ebd.) zeigt auf, wie der Handel mit solchen Exploits zu einem lukrativen Geschäft avanciert ist, das erheblichen Einfluss auf die Dynamik und die zeitliche Struktur von Cybersicherheitsmaßnahmen ausübt.

Stevens (2015) schließt mit seinem Fokus auf heterogen zusammengesetzte Cybersecurity-Communities an anthropologische Arbeiten zu unterschiedlichen kollektiven Zeitvorstellungen sozialer Gruppen an (Gell 1992; vgl. auch Grenz 2023b). Stevens analysiert, wie verschiedene Cybersecurity-Communities bestimmte Zeitlogiken und temporale Strukturen entwickeln, die ihre Praktiken und Interaktionen prägen. Diese zunächst eigenkulturellen Zeitvorstellungen beeinflussen maßgeblich die Art und Weise, wie Sicherheitsmaßnahmen umgesetzt und Bedro-

hungen wahrgenommen werden. Er beschreibt staatliche Sicherheitsbehörden, private Sicherheitsfirmen, zivilgesellschaftliche Hackergruppen und Forschungsabteilungen als zentrale Akteur*innen in der Cybersicherheit, die entsprechend jeweils spezifischer Zeitlogiken und Handlungsweisen verfahren: Behörden planen präventiv und langfristig, Firmen reagieren kurzfristig und flexibel, Hacker agieren dynamisch und opportunistisch, während Forschungsabteilungen zukunftsorientiert arbeiten. Diese Zeitlogiken beeinflussen ihre Prioritäten und Interaktionen in der Cybersicherheitslandschaft. In der Folge akzentuiert Stevens das Konzept der „chronopolitics", da die Konflikte zwischen den verschiedenen Zeitlogiken eine wichtige Rolle in politischen Diskussionen spielen, und an der Schnittstelle von Cybersicherheit und Politik unterschiedliche Zeitperspektiven oft die Debatten und Entscheidungen bestimmen (Stevens 2015: 44).

In (digital-)technischer Perspektive arbeitet Smeets (2018) Besonderheiten in der transitorischen Behandlung von Arbeitsmitteln der Cybersicherheit als ‚Cyberweapons' heraus. Smeets betont, dass moderne Cyberwaffen durch besondere, zeitabhängige Dynamiken gekennzeichnet sind, die komplexe Ereigniskaskaden in Gang setzen. In der Bewältigung von Cyberangriffen spielt die Zeitdimension bei der Erkennung eines Angriffs sowie beim Schließen der ursächlichen Sicherheitslücken und dem Verbreiten korrigierter Software eine kritische Rolle. Umgekehrt bedeutet dies, dass Bedrohungsakteur*innen systematisch Zeitfenster ausnutzen können, um den Zeitpunkt eines Angriffs optimal zu bestimmen und maximale Wirkung zu erzielen (ebd.). Ein aufwändig entwickelter Exploit ist weitgehend nutzlos, sobald die von ihm genutzte Sicherheitslücke im Zuge des Angriffs vom Angegriffenen geschlossen worden ist; dies beschreibt Smeets als eine grundlegende Prämisse moderner Cyberangriffe. Das führt nicht selten dazu, dass Cybersicherheitsspezialist*innen ihre Bewertungen, Beratungen und Maßnahmen auf die Analyse solcher erstmaligen Angriffe stützen, die ex post als einschneidende und grundlegende Ereignisse rekonstruiert werden. Diese sozio-materielle Einmaligkeit von Cyberangriffen (Gazos 2023) prägt die Rolle von Zeitvorstellungen im Feld der Cybersicherheit grundlegend.

Bis hierhin lässt sich zusammenfassen, dass es sich bei Cybersicherheit um ein globales und zugleich regionales, hochgradig fragmentiertes Feld handelt. Gekennzeichnet ist es durch die Bearbeitung unterschiedlich verzeitlichter Vorkommnisse. Neben solchen Cyberwaffen, die kopierbar und modifizierbar sind bzw. die sich Sicherheitslücken in generischen Systemen nutzbar machen und damit kontinuierliche Risiken darstellen (die ebenso kontinuierlich bearbeitet werden) finden sich solche, die außeralltäglich und (noch) unsichtbar sind, d. h. als (noch) unbekannte Ereignisse gekennzeichnet sind – darin eingewoben sind jeweils verschiedene Bezüge auf Basis differenzierter temporaler Logiken (Deibert 2016; Grenz 2023b). ‚Cybersecurity' – in lokal unterschiedlicher Kenn- und Bezeichnung (s. Abschnitt 3) – wird als Bezugsproblem bearbeitet und ermöglicht in dieser Form die Vermittlung mithin sehr heterogener Akteur*innen, Expert*innengruppen und Diskurse. ‚Cybersecurity' bzw. ‚Cybersicherheit' fungiert dabei allerdings als Chiffre, denn in den Aushandlungen kommt eine tieferliegende Multitemporalität zum Ausdruck, die Technologien, Prioritäten und Praxismuster der Cybersicherheit prägt. Zugespitzt lässt sich konstatieren, dass Akteur*innen in der anhaltenden Bearbeitung von Cybersicherheit sich beiläufig mit nichts Geringerem befassen, als der digitaltechnischen Tiefenschicht von Gegenwartsgesellschaften, die sich in diesem Sinne als spezifisch zeitlich konstituiert darstellen bzw. genauer: nicht nur durch Inkohärenz, sondern auch und v. a. durch eine inhärente Asynchronität ihrer soziotechnischen Verfasstheit gekennzeichnet sind. Dieser Zuschnitt ist bis dato nicht systematisch betrachtet worden. Im Folgenden rekonstruieren wir diese Multitemporalität zunächst empirisch und fassen sie anschließend im Rückgriff auf eine erweiterte Perspektive auf Grenzobjekte theoretisch.

Im Lichte dieser Überlegungen lässt sich Cybersicherheit als ein Ensemble aus Vorbeugung, Absicherung und Wiederherstellung begreifen, das in konkreten technischen Praktiken und in verschiedenen sozialen Arenen hergestellt und vermittelt wird. Neben der Ereignishaftigkeit von antizipierten und unvorhersehbaren Bedrohungen haftet Cybersicherheit daher strukturelle Dauerhaftigkeit und Stabilität an. Die digitalen Infrastrukturen, die ihr zugrunde liegen, weisen eine kontinuierlich und aktiv aufrechtzuerhaltende Beständigkeit und zugleich eine passive oder gar fahrlässig vernachlässigte Vergänglichkeit auf – ein Spannungsverhältnis, das nicht zuletzt auf der Begrenztheit der Ressource Zeit beruht. Ihrem chronologischen Verschleiß wird mit situativer Wartung begegnet, damit ihre vermeintliche Durabilität nicht zerfällt (Kocksch et al. 2018). Werden jene Infrastrukturen empfindlich gestört oder angegriffen, lassen sie sich nur mit großem Handlungs- und Kostenaufwand reparieren oder wiederherstellen. Die Möglichkeiten der Aufrechterhaltung sowie der strategischen Störung digitaler Infrastrukturen werden somit zu einer Verteilungs-, Macht- und Ressourcenfrage. Die (De-)Konstruktion digitaler Sicherheit ist keineswegs losgelöst von ökonomischen, politischen und sozialstrukturellen Dimensionen, sondern Teil sozialer und globaler Interdependenzgeflechte, wirtschaftlicher und geopolitischer Verhältnisse der Kooperation bzw. Konkurrenz und bestimmter sozio-räumlicher

Wissensordnungen und Kulturen (Deibert 2011). Da sich der fortwährende Prozess der Erzeugung von Cybersicherheit somit stets gesellschaftlich bestimmen lässt, sind deren soziale Zeitlichkeiten durch Perspektivität und Situiertheit gekennzeichnet, eingebunden in spezifische Erwartungen und Relevanzsetzungen. Dabei weisen sie bestimmte (und empirisch zu bestimmende) strukturelle Machtgefälle, Differenzierungen und Abgrenzungen auf, die unter ihren jeweils eigenen Bedingungen der Entstehung verstanden und erklärbar gemacht werden müssen.

3 Aushandlungen soziotechnischer Ordnung: Einblicke in aktuelle Forschungsprojekte

In diesem Abschnitt führen wir drei heterogene Forschungsprojekte aus den Kontexten der Science and Technology Studies (STS), der Ethnologie sowie der Arbeits- und Organisationssoziologie zusammen. Unserer Zusammenarbeit liegt – wie im zweiten Abschnitt ausgeführt – die Überzeugung zugrunde, dass das technopolitische Feld der Cybersecurity einer soziologischen Theoretisierung bedarf, um seine gesellschaftliche Tiefenstrukturen jenseits rein technischer Logiken freizulegen. Die im Folgenden präsentierten Einblicke verstehen wir im Sinne einer Theoretischen Empirie (Kalthoff et al. 2008) nicht als lückenlose Fallbeschreibungen, sondern als reflexive Sonden einer abduktiven Theoriebildung, in deren Verlauf sich Temporalität als das entscheidende vermittelnde Moment herauskristallisiert hat.

Wir machen damit transparent, dass die zeitliche Dimension und identifizierten Spannungsverhältnisse nicht in jedem ursprünglichen Forschungsdesign als primärer Fokus angelegt waren. Vielmehr erwiesen sie sich in unserem interdisziplinären Austausch als jene analytische Klammer, die die Heterogenität der Feldbefunde erst systematisch vergleichbar machten. Wie wir in Abschnitt 5 theoretisch ausarbeiten, verstehen wir die feldtypischen Objektgestalten der Cybersicherheit als Grenzobjekte, deren koordinierende Funktion über interpretative Flexibilität hinaus auf einer infrastrukturell-zeitlichen Tiefenschicht beruht. ‚Cybersicherheit' kommt also in feldtypischen Objektgestalten zum Tragen, in denen sich die jeweiligen zeitlichen Logiken materialisieren.

Die drei folgenden Einblicke rekapitulieren das empirische Material unter diesem spezifischen Prisma: Teilabschnitt 3.1 skizziert Cybersecurity als mundane Praxis in klein- und mittelständischen Unternehmen. Vor dem Hintergrund aktueller Debatten zu Reparatur, Restauration und Softwarepflege werden hier Zeitlichkeiten sichtbar, die nicht wachstumsorientiert, sondern primär abwartend, andauernd und erhaltend sind. Abschnitt 3.2 befasst sich mit Standardisierungsprozessen in Organisationen. Hier zeigt sich, wie durch Standardisierung eine prekäre Gleichzeitigkeit von technologischer Aktualität und organisationaler Persistenz hergestellt und verstetigt werden soll. Abschnitt 3.3 widmet sich der Cyber-Resilienz kritischer Informationsinfrastrukturen. Im Fokus steht dabei die zeitliche Logik der Resilienz, die darauf abzielt, Beständigkeit und Wandel produktiv miteinander zu verbinden.

3.1 Mundane Hoffnung in Klein- und Mittelständischen Unternehmen

In informationstechnologischen Analysen ist die Zeitlichkeit der Cybersicherheit durch ständige Wiederherstellung geprägt: Jede erfolgreiche Attacke erfordert eine zeitnahe Antwort von Programmierer*innen und Nutzer*innen, um Einfallstore zu schließen und Maschinen zu aktualisieren. Während diese kontinuierliche Re-Definition in spezialisierten Diskursen normativ verteidigt wird, ist sie in der Praxis nicht nur schwer zu erreichen, sondern potentiell schädlich. Im Rahmen einer ethnographischen Studie zu alltäglichen Dilemmata in Klein- und Mittelständischen Unternehmen (KMU) wurden Theorien der Science and Technology Studies (STS) mobilisiert, um ständige Aushandlungen von Expertise und „guter" Sicherheit nachzuvollziehen (Kocksch & Sørensen 2023; Kocksch & Jensen 2024). Im Alltag von KMU ist Cybersicherheit kein hochspezialisierter Bereich, sondern Teil von mundanen, dauerhaften und nur partiell-erfolgreichen Praktiken. In KMU überschreitet Cybersicherheit ihre sonst suggerierte Ereignishaftigkeit: Cyber(un)sicherheit geschieht schleichend; wird verschoben oder zeitweise ausgesetzt. Digitale Zusammenbrüche sind partiell, dauern über Monate oder Jahre an (wenn z. B. veraltete Programme verwendet werden, da Ressourcen fehlen) und Reparaturen vollziehen sich ständig, jedoch selten vollständig. Hier sind es nicht plötzliche Einbrüche, sondern ständige Gespräche, Vier-Augen-Absicherungen oder räumlich-materielle Taktiken, in denen Sicherheit verhandelt wird. Während Expert*innen kritisieren, dass KMU nicht hinreichend in Cybersicherheit investieren – und damit ist (immer) die Verhinderung des ‚großen Einbruchs' gemeint – vollziehen KMU Cybersicherheit durch alternative Wege und Logiken. KMU leben in einer andauernden „broken-world" – nicht in einer Welt von ständiger Neu-Erfindung (Jackson 2014; Kocksch & Jensen 2024).

Damit ist eine andere Normativität verbunden: An die Stelle des Strebens nach Idealen tritt der Anspruch, mit den gegebenen Bedingungen so gut wie möglich umzugehen. KMU leben mit Fragilität, mit pragmatischem, jedoch unangenehmem Hoffen statt Hoffnung auf Erlösung (Kocksch 2024). „Vielleicht machen wir gar nichts“, räumt ein IT-Spezialist in einem Produktionsbetrieb während einer ethnographischen Beobachtung ein. Er hat zuvor erklärt, dass Großgeräte nur mit Betriebssystemen funktionieren, die seit den späten 1990er Jahren nicht mehr mit Softwareupdates versorgt werden. Kurz darauf berichtet er jedoch, dass er an Wochenenden auf Flohmärkten Disketten sucht, damit er Daten zumindest partiell sichern kann.

Es wäre nun einfach, diesen Betrieb und den IT-Spezialisten als defizitär zu beschreiben. Jedoch erlaubt eine Betrachtung der lokalen Normativität, inspiriert von Studien zu „Care“ in den STS (Mol 2002), eine zentrale Umdeutung: Als Praxis ist die Ontologie von Cybersicherheit nicht eindeutig bestimmbar. Was als sicher gilt, ist in verteilten und situationsabhängigen soziotechnischen Arrangements verankert. Cybersicherheit bedeutet vor diesem Hintergrund, in einer Vielfalt von Taktiken mit persistenten, konflikthaften und letztlich nicht endgültig ‚lösbaren‘ Technologien umzugehen. Für KMU sind solche Arrangements kein Einzelfall, sondern die Norm; sie agieren in einer Welt, die dauerhaft unsicher ist (Kocksch & Jensen 2024). Cybersicherheit ist hier durch mangelnde Ressourcen und oft veraltete Industrieanlagen eine konstante Abwägung. Cybersicherheit ist nie perfekt, es gibt keine absolute Sicherheit. Cybersicherheit ist allenfalls ‚gut-genug‘. Am Horizont steht nicht die gezielte Identifikation und das Lösen von Cybersicherheitsschwachstellen, sondern das Entwickeln und Erlernen von langfristigen Strategien, um mit mangelhafter Sicherheit bestmöglich zu leben. Die Zeitlichkeit von Angriff und Patch legt einen lösungsfixierten Zugriff nahe, wie er in der ingenieurwissenschaftlichen Cybersicherheit verbreitet ist. Im Vollzug zeigt sich hingegen eine langfristige Bearbeitungsform, die sich in Dialogen, Grauzonen und persistierenden Semi-Lösungen stabilisiert. In KMU, wie auch in vielzähligen alltäglichen Praktiken anderswo, ist Cybersicherheit kein Event, keine absolute Abschottung, keine Lösung für ein klar definiertes Problem, sondern immer schon stückweise gebrochen, immer unvollständig und nie erreicht. Dies bedeutet nicht, dass KMU nichts tun, im Gegenteil: Mit partieller Unsicherheit umzugehen heißt, fortlaufend zu kalibrieren, auszuhandeln und immer wieder neu zu bestimmen, was als ‚gut genug‘ oder ‚ein wenig besser‘ gelten kann. In dieser Form ist Cybersicherheit kein rekursives Wechselspiel zwischen Verbesserung und Wachstum, sondern eine Praxis des Umgangs mit Imperfektionen und fortdauernden Aushandlungen.

Vor diesem Hintergrund lässt sich zusammenfassen, dass das Forschungsprojekt das Spannungsverhältnis zwischen ereignisbezogener Sicherheitslogik und der auf Dauer gestellten Alltäglichkeit infrastruktureller Praxis sichtbar macht. Cybersicherheit wird dabei als fortlaufende Aushandlung zwischen Aktualisierungsdruck und materieller Endlichkeit vollzogen, in der Wartung, Verschiebung und Improvisation zentrale zeitliche Modi darstellen. Damit zeigt sich Cybersicherheit nicht als Reaktion auf singuläre Ereignisse, sondern als dauerhafte Koordination inkompatibler Zeitlichkeiten unter Bedingungen begrenzter Ressourcen.

3.2 Standardisierungsprozesse zur Sichtbarmachung von Informationssicherheit

Im folgenden Abschnitt werden erste Ergebnisse dargestellt, die im Rahmen eines interdisziplinären Forschungsverbundes entstanden sind. Diese entstammen leitfadengestützten Interviews (Helfferich 2022) mit Mitarbeiter*innen aus dem Bereich Kritischer Infrastrukturen (KRITIS) (n= 9) zum Thema Cybersicherheit im Arbeitsalltag, die mit der qualitativen Inhaltsanalyse nach Mayring (2014, 2019) ausgewertet wurden. Die Besonderheit des Forschungsprojektes liegt darin, dass der Blick hier auf die Alltagswelten der Beteiligten im Betrieb gelenkt werden sollte.

Während es kaum mehr Diskussion darüber bedarf, dass Cybersicherheit in Unternehmen von Relevanz ist und ihre Umsetzung geregelte Prozesse benötigt, stellt sich die konkrete Einbindung von IT-Sicherheitsstandards immer noch als schwieriges Unterfangen dar. Informationstechnologische Standards verfolgen das regulatorische Ziel, hochgradig differenzierte technische Apparate miteinander kommunikationsfähig zu machen und zugleich Qualitätskontrolle und Kommunikationssicherheit zu gewährleisten. Das wirkt sich auch auf die Vereinheitlichung übergeordneter organisationaler Prozesse aus. Im Gegensatz zu anderen betrieblichen Standards erscheinen IT-Sicherheitsstandards als bemerkenswert fluide und müssen an ständig neue Anforderungen der vernetzten Gesellschaft angepasst werden. Wir knüpfen hier an bestehende Standardisierungsdiskurse an, die in der Arbeits- und Organisationssoziologie nicht neu sind, durch den Forschungsgegenstand der Cybersicherheit aber neue Impulse bekommen.

Die ersten Ergebnisse zeigen: Standards werden auf Unternehmensseite häufig als abstrakt wahrgenommen, was mit einer Forderung nach mehr Leitlinien zur Umsetzung Hand in Hand geht, so beschreibt es ein Interviewpartner eines Krankenhauses, der sich als Chief Information Security Officer (CISO) und Auditor an der Schnittstelle dieser Aushandlungen befindet. Gleichzeitig sollen etablierte Stan-

dards auf die unterschiedlichen Bedingungen der Unternehmen angepasst und angewendet werden. IT-Standards sind dergestalt durch eine spannungsgeladene Gleichzeitigkeit von Aktualität und (näherungsweise) Persistenz gekennzeichnet, insofern der technischen Veränderbarkeit die Trägheit und zugleich auch notwendige Verbindlichkeit betrieblicher Normen gegenübersteht. Der vielfach geforderte „State of the Art" ist diskursiver Ausdruck dieser spezifischen Anforderung an Technik (so gesehen in der DSGVO, vgl. Art 32, Abs. 1, Satz 1: „Unter Berücksichtigung des Stands der Technik […] treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten […]").

Darin zum Ausdruck kommt ein Widerspruch zwischen der dynamischen Entwicklung neuer Technologien und dem langwierigen Prozess der Veröffentlichung und Etablierung neuer und angepasster Standards zur Informationssicherheit. Obwohl ein großes Interesse der beteiligten Akteur*innen an verbindlichen Regularien besteht, prallen hier die unterschiedlichen zeitlichen Logiken von Infrastruktur und Ereignis aufeinander. Die Erwartung an Standards im Arbeitskontext geht mit der Forderung nach konkreten Handlungsempfehlungen zur Integration von IT-Sicherheitsmaßnahmen einher und steht im Widerspruch zu den sie entwickelnden Gremien. Standards dienen dazu, einen Mindestschutz zu gewährleisten und als zeitlich begrenzte Orientierung zu fungieren. Die oftmals abstrakten und breit formulierten Regularien haben den Zweck, möglichst viele Unternehmensanforderungen erfassen zu können und so ein grundlegendes Maß an Informationssicherheit über die Organisationsformen hinweg zu gewährleisten. Eine deutliche Unterscheidung zeigt sich somit zwischen Kritischen Infrastrukturen, mit einem höheren Maß an Regulierungen, und Nicht-KRITIS-Organisationen.

Hinzu kommt, dass gerade im Unternehmenskontext Standardisierungsprozesse auf die Anforderungen und die Zeitlogik des Arbeitsalltags treffen: Awareness-Schulungen[3] dürfen neben der eigentlichen Arbeitstätigkeit nur begrenzt Zeit beanspruchen, müssen jedoch zugleich hinreichend instruktiv sein, um Mitarbeiter*innen für Einfallstore zu sensibilisieren.

Zeit erscheint somit auch hier als immer begrenzte und begehrte Ressource. Hierfür bilden Awareness-Schulungen eine präventive Maßnahme, die sich zeitlich weit vorgelagert vor dem möglichen Eintritt eines Cyber-Angriffs positionieren soll. Parallel dazu werden fortlaufend Aushandlungen über den Stellenwert von Cybersicherheit zwischen IT-Abteilung und Führungskräften geführt, deren Ergebnisse letztlich festlegen, welche finanziellen und personellen Mittel zur Verfügung stehen, um Sicherheitsinfrastrukturen zu etablieren oder diese aufrechtzuerhalten. Die subjektive Zuschreibung von Relevanz gegenüber dem Management wird zu einem entscheidenden Faktor für die Kontinuität und Nachhaltigkeit von Sicherheitsmaßnahmen. Die Mitarbeitenden konstruieren durch ihre zeitbezogenen Reflexionen und Bewertungen den Forschungsgegenstand aktiv mit (s. 3.3) und machen Zeitlichkeit zu einem inhärenten Element des sozialen Phänomens selbst. Gleichzeitig erscheint Cybersicherheit als allumfassendes Thema, welches das ganze Unternehmen betrifft, auch wenn mit der IT-Abteilung bzw. ihren Dienstleistern nur ein kleiner Teil für deren Umsetzung direkt verantwortlich ist. Zu bedenken ist auch, dass Maßnahmen häufig nicht an die jeweiligen Arbeitskontexte und -praktiken einer Abteilung angepasst werden, sondern vielmehr Top-down entschieden werden, Fragen um deren (Nicht-)Umsetzbarkeit aber dennoch von den Betroffenen selbst gelöst werden müssen.

Während kleinere Unternehmen auf Dienstleister angewiesen sind oder Cybersicherheit nur einen weiteren Tätigkeitsbereich der dafür offiziell zuständigen Person oder Personengruppen darstellt, sind in größeren Unternehmen zunehmend etablierte Security Operation Centers (SOCs) mit einem umfassenden Personalaufgebot vorhanden. Dennoch zeigt sich, dass im Arbeitsalltag häufig weitere Personen mit Teilausschnitten der IT-Sicherheitsinfrastruktur betraut sind, welche diese etablieren, warten oder in ihrer Abteilung die Schnittstelle zur IT bilden. Hier wird prozessbegleitend Zeit für IT-Sicherheit geschaffen: Etwa der Radiologe, der sich aus einem Hobby heraus zum Austauschpartner für die übergeordnete IT des Krankenhauses mausert (Eckhardt et al. 2024):

> „Also im Wesentlichen bin ich Medizinphysiker. Das bedeutet andererseits natürlich, ich habe eigentlich jetzt mal formal IT-mäßig in keinster Weise irgendwie eine Ahnung. Nur irgendwer muss es machen. […] Und über die letzten zehn Jahre habe ich es mir dann halt so draufgeschafft, sag ich mal."

Es zeigt sich ein Spannungsfeld zwischen der kontinuierlichen, meist unsichtbaren Infrastrukturarbeit und den auf Ereignissen ausgerichteten Maßnahmen. Während Infrastrukturarbeit auf die Etablierung dauerhaft belastbarer Strukturen zielt, die potenzielle Angriffe abfedern, orientieren sich viele Maßnahmen an einem imaginierten Großereignis: einem umfassenden Ransomware-Angriff, der unter den Beteiligten als Worst-Case-Szenario zirkuliert und als vorrangig zu verhinderndes Ereignis behandelt wird. Diese Ereignisorientierung wird zugleich in den Schu-

3 Es wurden sieben Interviews in einem Lebensmitteldiscounter nach der Durchführung von Awareness-Schulungen geführt.

lungen der Beschäftigten deutlich, in denen die Bedrohung durch gefälschte Kommunikation, insbesondere per E-Mail („Phishing"), dominiert. Hierbei erhält dieses Einfallstor eine überproportionale Aufmerksamkeit. Langfristige Bemühungen, die Infrastruktur am Laufen zu halten, indem alltagsnahe Praktiken etabliert werden, geraten so in den Hintergrund, womit das Potenzial einer anhaltenden Wartung durch die Partizipation der Beschäftigten verwirkt wird.

Das Forschungsprojekt verdeutlicht – wiederum zusammenfassend – das Spannungsverhältnis zwischen der ereignisgetriebenen Forderung nach Aktualität („State of the Art") und der Trägheit organisationaler Routinen. IT-Sicherheitsstandards fungieren als temporale Grenzobjekte, die kurzfristige Bedrohungsdynamiken in langfristig verbindliche Arbeits- und Entscheidungsprozesse übersetzen sollen. Sichtbar wird Cybersicherheit als Koordinationsleistung konkurrierender Zeitlogiken, in der Persistenz nur durch selektive Anpassung und institutionalisierte Verzögerung aufrechterhalten werden kann.

3.3 Die zeitlich bedingte Cyberresilienz in kritischen Informationsinfrastrukturen

Im Rahmen einer noch unveröffentlichten Dissertation wurde eine Bewältigungsstrategie erarbeitet, die sich mit den systemischen Vulnerabilitäten kritischer Informationsinfrastrukturen befasst. Zu diesem Zweck wurden organisations- und sicherheitstheoretische Konzepte (Hollnagel 2014; T.M. LaPorte 2006; T.R. LaPorte & Consolini 1991; Perrow 1999; Weick et al. 1999/2008) in einer holistischen Konzeption von Resilienz zusammengeführt. Resilienz wurde dabei als erwartungsabhängige Bezugsgröße aufgefasst, wonach soziale Beobachter*innen definieren, worin der schützenswerte Kernbestand besteht und wie er durch Transformation aufrechterhalten werden kann (Endreß & Rampp 2014). Das aus der Literatur entwickelte Resilienzkonzept wurde am empirischen Material evaluiert und weiterentwickelt. In einer ersten Phase (2021–2022) wurden fünf problemzentrierte Interviews (Witzel 2000) mit Akteur*innen an der Schnittstelle kritischer Informations- und Energieinfrastrukturen geführt und mithilfe einer zusammenfassenden sowie strukturierenden qualitativen Inhaltsanalyse (Mayring 1991) kodiert und interpretiert. Auf Basis der Interviewanalyse wurde das Codesystem überarbeitet und in einer zweiten Phase auf 18 Dokumente angewandt, die entlang der Relevanzsetzungen der Befragten recherchiert und ausgewählt wurden. Der Korpus umfasst nationale Gesetzestexte, europäische Richtlinien und (inter-)nationale Standards zur Informationssicherheit, Positionspapiere der Arbeitsgruppe Kritische Infrastrukturen (AG KRITIS) sowie Guidelines und White Paper privatwirtschaftlicher Sicherheitsdienstleister und Produktanbieter/-entwickler (bspw. Microsoft, T-Systems, Schneider Electric, Hitachi Energy). Interviews und Dokumente beziehen sich wiederholt auf physische Infrastruktursicherheit, Cybersicherheit und organisationale Prozesse.

Im Verlauf von Erhebung und Analyse wurde Cybersicherheit im Material wiederholt als dringliches Problem markiert. Die folgenden Dokumentausschnitte skizzieren, wie sich die Verhältnismäßigkeit von Cyberresilienz zeitlich formiert und wandelt. Dabei ist zu berücksichtigen, dass Resilienz hier als Darstellung erscheint, die an Ressourcenlagen, organisationale Erwartungen und erlebte Ereignisse gekoppelt ist. Im Korpus überwiegen große Unternehmen und staatliche Institutionen mit vergleichsweise hohen Kapazitäten; zudem wurden ausschließlich von den Organisationen veröffentlichte Dokumente ausgewertet. Auch die Interviewaussagen sind organisationslogisch gerahmt und geben primär idealisierte Soll- und Selbstbeschreibungen wieder; Einblicke in die alltägliche Praxis und ihre möglichen Widersprüchlichkeiten bleiben damit begrenzt.

Die Erwartungen im Material unterstreichen eine wandelbare Konzeption der Resilienz:

> „Fundamental cyber resilience must be integral not only to technical systems but also in teams, the organizational culture and the daily way of working. […] The approach to cyber resilience must also be free from the fear-driven limitations caused by merely preserving the status quo, which are so often then followed by attempts to return to a demonstrably fragile state when disruption predictably happens. […] This indicates that as organizations, ecosystems, supply chains and relationships become more connected and interdependent and the pace of change accelerates, not only is resilience lagging, but a cohesive approach for how to architect for resilience is lacking. It has become increasingly clear that despite this interconnection, no alignment to transcend disruptive cyber events exists." (World Economic Forum [WEF] 2022, S. 3)

Technische Systeme, Teams, organisationale Kultur und alltägliche Arbeit gelten im Material nur bis zur ereignisbedingten Disruption als resilient. Cyberresilienz ist an den Ereignisfall gebunden: Nach Störungen soll nicht bloß der Status quo wiederhergestellt, sondern Transformation angestoßen werden. Damit wird die ereigniszeitliche Bedingtheit von Resilienzzuschreibungen sichtbar. Resilienz-Erwartungen sind dabei mit einer Hyperfokussierung auf Vulnerabilität oder Fragilität (s. obiges Zitat und 3.1) verbunden. Um Unsicherheiten zu reduzieren, werden Technologien getestet, Notfälle geübt und – sofern Ressourcen es erlauben – externe Dienstleister zur Schwachstellenprüfung hinzugezogen.

Für ressourcenschwächere Organisationen, insbesondere KMU (s. 3.1), gewinnen organisationsübergreifende Netzwerke an Bedeutung, wie auch das World Economic Forum in seinem Whitepaper hervorhebt („ecosystems, supply chains and relationships"). Auch kapazitätenreiche Organisationen nutzen solche Netzwerke aus Betreibern, Dienstleistenden und staatlichen Institutionen, um Ressourcen zu bündeln und entlang vergleichbarer Systeme (bspw. Zertifizierung nach BSI 200-1, siehe unten und auch 3.2) aus Ereignissen zu lernen, etwa in Form von Austauschformaten zu bereits erfolgten Angriffen. Diese Netzwerke reichen vom Dienstleisterkontakt bis zu supraorganisationalen Verbünden (bspw. die Allianz für Cyber-Sicherheit) und reagieren darauf, dass Bewältigungskapazitäten angesichts komplexer Systeme, organisationaler Erwartungen und dynamischer Ereignisse den einzelnen Organisationshorizont überschreiten. Ferner werden multiple, simultan wirkende und schwer vorhersehbare Bedrohungen erwartet, wie das Zitat aus der NIS2-Richtlinie zeigt:

> „Wegen dieser gegenseitigen Abhängigkeiten kann jede Störung, auch wenn sie anfänglich auf eine Einrichtung oder einen Sektor beschränkt ist, zu breiteren Kaskadeneffekten führen, die weitreichende und lang anhaltende negative Auswirkungen auf die Erbringung von Diensten im gesamten Binnenmarkt haben können. Die verstärkten Cyberangriffe während der COVID-19-Pandemie haben gezeigt, wie anfällig zunehmend interdependente Gesellschaften für Risiken mit geringer Eintrittswahrscheinlichkeit sind." (EU-Richtlinie, 2022/2555, S. 9)

In der Gemengelage potenzieller Bedrohungen und wirkmächtiger Ereignisse antizipieren Organisationen kaskadenartige Angriffseffekte. Gegen die Undurchsichtigkeit werden Monitoring- und Überwachungsroutinen aufgebaut; im sog. ‚Event Logging' werden Systemzustände als Protokolldaten historisiert und als chronologische Ereignisfolgen rekonstruierbar. Unter Unsicherheit (wer greift wann, was und wie an?) soll kontinuierliche Reaktionsfähigkeit (bspw. 24/7-Bereitschaft) ein Mindestmaß an beständiger Kontrolle stabilisieren. Diese Stabilisierung wird prozessförmig organisiert: Schulungen, formalisiertes ‚Incident'- und Notfallvorgehen (bspw. Notfallprotokolle) sowie der Ausbau materieller Redundanzen sind modular angelegt, um den Betrieb trotz Ereignissen zu ermöglichen (bspw. unterbrechungsfreie Stromversorgung) oder die Wiederherstellung zu beschleunigen (etwa durch Datensicherungen). Leitlogik ist ein iteratives Verfahren, das der BSI-Standard 200-1 (Bundesamt für Sicherheit in der Informationstechnik 2017) als PDCA-Zyklus bzw. Lebenszyklus-Modell fasst („Plan, Do, Check, Act"). Dass diese Verfahren nur idealtypisch sind, zeigt sich jedoch in deren Kontextabhängigkeit: Sie bieten zwar eine allgemeine Orientierung, müssen aber von Behörden und Unternehmen jeweils entlang ihrer Ausgangsbedingungen, Sicherheitsanforderungen und finanziellen Möglichkeiten organisationsspezifisch ausgestaltet werden.

Die Ausschnitte veranschaulichen bereits die mehrdeutigen Temporalitätsverhältnisse, die sich im weiteren Korpus verdichten: Organisationen beobachten, antizipieren und intervenieren im Rahmen ihrer Ressourcen und Erwartungshorizonte, indem sie Entwicklungen verfolgen, Unsicherheiten einkalkulieren und Maßnahmen vorbereiten. Ereignisse, die unerwartet in Zeitpunkt, Ort oder Wirkmächtigkeit eintreten und den Betrieb empfindlich stören, werden auf eine rasche Rückkehr zur Normalität hin bearbeitet. Zugleich erzwingen sie Lernprozesse: Erst im Ereignis werden soziale und materielle Folgen sichtbar, die zuvor als resilient geltende Arrangements als vulnerabel markieren, weil Kapazitäten fehlen oder Erwartungen irritiert werden. Ransomware-Kampagnen, Zero-Day-Angriffe und verwandte Vorfälle produzieren damit ereignisspezifische Überwerfungen stabiler Selbstverständlichkeiten; die vermeintliche Funktionstüchtigkeit der IT-Architektur wird im Zusammenprall von System und Ereignis temporär unverständlich, bis die bislang unbekannte Schwachstelle identifiziert, geschlossen und in neue Routinen übersetzt ist. Aus der Bewältigung emergieren revidierte Erwartungshorizonte, die sich mit der Zeit verfestigen und bis zum nächsten Ereignis als fragile Stabilität fortbestehen.

In der Vermittlung aus Theorie und Empirie zeigt sich, dass die Erwartungen an die Cyberresilienz kritischer Informationsinfrastrukturen darin begründet liegen, im Angesicht einer schnelllebigen und erratischen Umwelt möglichst beständig dafür zu sorgen und zu reflektieren, wie Infrastrukturen im Kern bestehen können und dabei stets wandelbar bleiben (Gazos 2023). Im stetigen Wandel aus neuen Herausforderungen und dynamischen Ereigniseventualitäten rekonstituieren Organisationen, im Laufe der Zeit und immer wieder aufs Neue, langfristige Beständigkeit. Obwohl hier ein relativ einheitliches Bild skizziert wird, sind die organisationalen Erwartungen an Cyberresilienz und die Zeitlichkeit keinesfalls harmonisch aufeinander abgestimmt. Im empirischen Material, wie auch in den vorangegangenen empirischen Beispielen, zeigen sich variable Erwartungen, die in Abhängigkeit begrenzter Ressourcen (3.1), fluider Standards (3.2) und unterschiedlicher Unternehmenskontexte (3.1, 3.2) zeitlich situiert sind und kontinuierlich neu verhandelt werden müssen.

In diesem Forschungsprojekt lässt sich Cyberresilienz somit als Spannungsverhältnis zwischen der Erwartung dauerhafter Funktionsfähigkeit und der ereignisbedingten Irritation komplexer Infrastrukturen aufzeigen. Resilienzkonzepte fungieren als temporale Grenzobjekte, die zukünftige

Störereignisse antizipieren, vergangene Vorfälle retrospektiv integrieren und organisationale Lernzyklen strukturieren. Sichtbar wird eine reflexive Zeitlichkeit, in der Stabilität nur als vorläufige Errungenschaft unter Bedingungen beschleunigten Wandels und permanenter Ereignisoffenheit hergestellt werden kann.

4 Rekonstruktion temporaler Spannungsverhältnisse in der Cybersicherheit

Die drei Einblicke in aktuelle Forschungsprojekte zeigen, dass Cybersicherheit sich zu einer zentralen Komponente von Digitalisierungsprozessen entwickelt hat, die in der Soziologie bislang erst in Ansätzen theoretisch aufgearbeitet wird. Die laufenden Projekte versuchen sich an dieser Theoretisierung. Im Rahmen dieses Artikels nutzen wir die Einsichten der Projekte, um einen Aspekt von Cybersicherheit für die Theoretisierung der Soziologie besonders nahe zu legen: Alle Projekte zeigen temporale Spannungsverhältnisse, die für die Bearbeitung von Cybersicherheit zentral sind. Die Spannungsverhältnisse verlaufen quer zu den Projekten und ergeben sich nur aus ihrer Synthese. Sie gehen gleichsam über nur implizierte temporale Vorstellungen von Cybersicherheit hinaus, und eröffnen soziologische Denk- und Forschungsfelder in denen Multitemporalität als untersuchbare Bedingung von Cybersicherheit erscheint.

Wir haben bis hierhin Cybersicherheit als Feld und zugleich Bezugsproblem gekennzeichnet, das durch vielfältige und oft friktionale Aushandlungen und Bedeutungszuweisungen gekennzeichnet ist. Die darin zum Ausdruck kommenden Spannungen kennzeichnen wiederum sozio-materielle Gestaltungen und Umgestaltungen. Unterschiedliche Eigenzeitlichkeiten technischer (Sicherheits-)Infrastrukturen prägen das Handeln von Akteur*innen ebenso, wie Akteur*innen unterschiedliche Zeitlichkeitserwartungen an digitale Infrastrukturen richten. In der Cybersicherheit tritt diese komplexe soziale, technische und zeitliche Gemengelage in Gestalt verschiedener Spannungsverhältnisse zutage. In diesem Abschnitt fokussieren wir drei Spannungsverhältnisse, die auf die anhaltende Bearbeitung und Aushandlung von Multitemporalität hinweisen: Dauer und Ereignis (Ereigniszeitlichkeit, 4.1), Beständigkeit und Endlichkeit im Kontext von Wartung und Reparatur (infrastrukturelle Zeitlichkeit, 4.2) sowie Reflexivierung (reflexive Zeitlichkeit, 4.3).

4.1 Dauer und Ereignis (Ereigniszeitlichkeit)

Eine wesentliche Bedeutung für die Temporalisierung von Cybersicherheit kommt der Wahrnehmung, Einordnung, Erzeugung und Klassifikation sicherheitsrelevanter Ereignisse *als* Ereignisse zu und wie institutionalisierte Akteur*innen im Feld der Cybersicherheit diese fortwährend reproduzieren: Sei es die antizipatorische Problematisierung und der Umgang mit der zukünftigen Bedrohung eines ‚größten anzunehmenden Unfalls' (z. B. Cyberangriffe auf kritische Infrastrukturen) (Kocksch 2020) oder die ex-post-Rekonstruktion eines Sicherheitsvorfalls zur zukünftigen Schadensbegrenzung und Resilienzsteigerung digitaler Systeme.[4] Die Handlungslogiken der Cybersicherheit sind in hohem Maße auf Sicherheitsereignisse ausgerichtet, die von den Teilnehmer*innen als außeralltäglich verstanden werden. Die beteiligten Diskurse, Akteur*innen und Praktiken erzeugen hierbei eigene Historizitäten und zeitliche Einordnungen eines Vorfalls; eine jeweils spezifische Relevanzsetzung hinsichtlich der Ereignisse, sei es ein antizipierter Routineangriff von geringer Bedeutung oder ein ernstzunehmendes Krisenereignis. Aus den jeweiligen Einordnungen und Ereignisklassifikationen speisen sich wiederum zahlreiche Ereignis-Antizipationen, die mit umfangreichen strukturellen organisationalen Veränderungen einhergehen, um unter erwartbaren und unerwarteten Bedingungen möglichst resilient zu bleiben (T.M. LaPorte 2006; Hollnagel 2014). Das Krisenereignis ist in der antizipatorischen Cybersicherheits-Arbeit fortlaufend präsenter Horizont, und ist für ebenjene Arbeit und ihre eigenen situationalen Zeitstrukturen ko-konstitutiv.

Diese Krisenhaftigkeit kann Antizipationen bestimmter (Einzel-)Vorfälle beinhalten, wie die in Abschnitt 2 beschriebene Gefahr unentdeckter Zero-Day-Exploits oder Ransomware-Angriffe, ebenso wie das Bedrohungsszenario von Ereignisketten und Kaskadeneffekten, auf die es sich technisch und organisatorisch vorzubereiten gilt.[5] Zu diesem Zweck werden im Idealfall nicht nur regelmäßig Datensicherungen und Softwareupdates vorgenommen, sondern es werden auch die menschlichen Teilnehmer*innen (der „Human Factor") der betreffenden Organisationen, Infra-

4 Diese forensische Rekonstruktionsleistung der Teilnehmer*innen stellt in Bezug auf Begegnungen mit Angreifer*innen die Regel dar: Einbrüche in Computersysteme werden oftmals signifikant später bemerkt, und es geht im Nachgang vor allem um Schadensbegrenzung.
5 Einschneidende Kampagnen mit datenverschlüsselnder Ransomware (‚Erpressertrojaner') wie der 2021 erfolgte Angriff auf Colonial Pipeline, der dem für die US-amerikanische Ölinfrastruktur hochrelevanten Unternehmen 4,4 Millionen US-Dollar in Bitcoin an Lösegeld für die Entschlüsselung seiner Daten abverlangte, sind hierfür ein prominentes Beispiel.

strukturen und Systeme regelmäßig durch Sicherheitsfortbildungen wie Übungen, Testläufe, Handlungsszenarien und Testverfahren (wie etwa sog. Penetrationstests oder CERT Trainings) sensibilisiert und über Schulungen, Zertifizierungen sowie Beratungsstellen mit Kontextwissen in Berührung gebracht. Es geht stets darum, antizipierte sicherheitsrelevante Ereignisse für die jeweils aktuellen Arbeitstätigkeiten in Relevanz zu setzen und sie dadurch mit ihrer spezifischen sicherheitsarchitektonischen Zeitstruktur zu konfrontieren. Durch die Antizipation eines Sicherheitsereignisses nicht als ‚Naturgewalt', sondern als von *anderen* (feindlichen) Akteur*innen intentional verursachtes Ereignis, wird die Frage nach der Attribution von Angriffen ebenso relevant. Das Wissen über den möglichen nächsten Angriff gestaltet sich damit als ein auf Ereignisverläufe gerichtetes Wissen, das in mehrfacher Hinsicht zeitlich strukturiert. Es ist durch die Auseinandersetzung mit den Erwartungen und Erwartungserwartungen sozialer Konflikt- und Konkurrenzverhältnisse im Hinblick auf vergangene und potenzielle Ereignisse geprägt. Im Umkehrschluss ko-konstituieren Ereignisse die Vermittlungsbedingungen sozialer Erwartungsverhältnisse, da sie als unmögliche Möglichkeit die Erwartungen sozialer Akteure heimsuchen (Derrida 2003).

Jegliche Vorbereitung, die einer Antizipation folgt, stößt immer wieder an Grenzen von Realisier- und Kalkulierbarkeit. Das Verhältnis zwischen Cybersicherheit und den für ihr fortlaufendes Operieren zentralen, mithin konstitutiven, antizipierten Krisenereignissen erscheint damit ambivalent: Das Ereignis soll ja gerade nicht eintreten, wofür umfassend sicherheitsrelevante Daten generiert und analysiert werden, und doch wird zugleich erheblicher Aufwand betrieben, seine Folgeschäden möglichst gering zu halten. Es ist eine Ambivalenz, die auch die Definition reflexivmoderner Risiken prägt: (Cyber)Risiken sind einerseits Zuschreibungsprodukte, insofern sie wissenskulturell geprägter Beobachtungen entspringen und entsprechend in Stellung gebracht werden. Die Effekte und gleichsam existenzielle Bedrohung, wie sie von Cyberrisiken ausgehen, führen andererseits ihren objektivierten Charakter vor Augen, sodass es verkürzt wäre, sie auf ihre Deutungsdimension zu reduzieren; sie fordern vielmehr eine integrative Haltung ein (Beck 2009: 21; Rasborg 2021: 40).

Für digitale und digitalisierte Alltagspraktiken hat die andauernde Antizipation cybersicherheitskritischer Ereignisse unmittelbar affektive Auswirkungen. Nachrichten von Cyberangriffen werden öffentlich verbreitet, dramatisiert und diskutiert (‚zum Glück hat es uns nicht erwischt'), es werden regelmäßig Tipps zum Umgang mit Sicherheitsrisiken gegeben und die Sorge vor digitaler Vulnerabilität zu Marketingzwecken eingesetzt (‚nur mit Software XY bin ich geschützt'). Gleichermaßen adressiert Cybersicherheit die Temporalitäten sozio-technischen Wandels materiell: In der Praxis müssen, wie in 3.2 beschrieben, durch das Bedrohungsszenario der Ereigniskategorie „Cyberangriff" ‚alternde' internetfähige Geräte durch fortlaufende Wartung über Softwareupdates ebenso ‚aktuell gehalten' werden. Mithin wird also eine marktkonforme Zeitlogik, die wenig Interesse an langlebigen Produkten besitzt, einer sicherheitssensiblen Zeitlogik gegenübergestellt.[6] Darüber hinaus existiert keine einheitliche Sicht darauf, wie ‚unsicher' heterogene, technische Bestandssysteme im Einzelnen wirklich sind, wenn sie nicht auf dem neuesten Stand sind. Über den Aufruf der Ereignislogik lanciert der Markt für Cybersicherheit in regelmäßigen Abständen einzelne Sicherheitsprodukte, kann hierdurch aber, gemäß seiner Funktionsweise fortlaufender Bedürfniserzeugung, die arbeitsteiligen und komplexen technischen Landschaften von Unternehmen oder Universitäten kaum gegenüber ebenso komplexen Angriffsinfrastrukturen resilient machen. In den Projekten wird deutlich, dass dieser Antizipation diskreter Krisen beständige, andauernde sowie verspätete Praktiken gegenüberstehen, die Cybersecurity als kontinuierliche infrastrukturelle Sorge markieren.

4.2 Beständigkeit und Endlichkeit im Kontext von Wartung und Reparatur (Infrastrukturelle Zeitlichkeit)

Auch wenn die Logik ständigen Aktualisierens und Instandhaltens nur vor dem Hintergrund des antizipierten Ernstfalls ihre Bedeutung erlangt, vollzieht sie sich in eigenen Zeitstrukturierungen. In der Praxis des fortlaufenden *Doing Cybersecurity* werden digitale Technologien in ihrer Eigenschaft als alltägliche Kommunikationsmedien gewartet und, im Hinblick auf praktische, aber auch wirtschaftliche oder politische Überlegungen, stabilisiert und verfestigt. Alltäglich verfasst ist Cybersicherheit fern eines normativen Ideals vollkommener Sicherheit, es geht nicht um ‚richtige', nicht mal ‚gute' Vorbereitung, sondern um lokale Adaptationen, langfristige finanzielle und arbeitsintensive Zuwendungen und Verstetigungen (s. 3.1). Verantwortlichkeiten werden in diesem Modus der Cybersicherheit durch situative Aushandlungen im Hinblick auf Geräte und Technologien hergestellt (Kocksch et al. 2018).

6 Im April 2024 wurde mit der EU-Richtlinie zum „Recht auf Reparatur" denn auch politisches Gewicht in die Waagschale dieser Auseinandersetzung geworfen. [https://www.europarl.europa.eu/news/de/press-room/20240419IPR20590/recht-auf-reparatur-reparieren-einfacher-und-attraktiver-machen, abgerufen 13.09.24].

Das Feld der Cybersicherheit verdeutlicht, dass digitale Technologien zur unverzichtbaren Hintergrundausstattung kritischer Infrastrukturen digitaler Gesellschaften geworden sind. Ihre Störung, ihr Nicht-Funktionieren, ihre Nicht-Erreichbarkeit oder gar die Abstinenz von ihnen kann erhebliche Auswirkungen in der physischen Versorgung der Bürger*innen zeitigen. Über ihre Rolle in kritischen Infrastrukturen erhalten digitale Technologien die Grundfunktionen vernetzter Gesellschaften aufrecht und stellen die Verfügbarkeit essenzieller Leistungen sicher. Von der eigenen Nachbarschaft, kleinen und mittelständischen Betrieben, über staatliche Institutionen, bis hin zu multinationalen Konzernen und globalen Lieferketten – gesellschaftliche Akteur*innen in jeder Konfiguration hängen zusehends von Informationsinfrastrukturen ab. Die ständigen Herausforderungen, vor denen Cybersicherheit fortlaufend vollzogen wird, verdeutlichen, wie digital, aber auch physisch vulnerabel unsere Ressourcen (bspw. Strom und Wasser), unsere Kommunikation sowie soziale, kulturelle und politische Aushandlungsprozesse sind. Cybersicherheit führt uns die Kernaussagen aus Soziologie und STS zu Infrastruktur, Wartung und Reparatur vor Augen (Bowker & Slota 2017; Niewöhner 2014), wenn durch sie Dauerhaftigkeit in Wartungs- und Reparaturpraktiken hergestellt und Ereignishaftigkeit durch digitale Infrastrukturen konfiguriert werden.

Cybersicherheit zeichnet sich durch besondere infrastrukturelle Tiefe aus. ‚Tiefe' bezieht sich hier auf zwei Aspekte gleichzeitig. Zum einen haben wir es mit „material processes" zu tun (Couldry & Hepp 2017: 3), die im Hintergrund das Funktionieren von Frontend-Arrangements wie Plattformen und Medien der alltäglichen Lebens- und Arbeitsverrichtung überhaupt erst ermöglichen. Cybersicherheit ist die meist unsichtbare Arbeit an den unsichtbaren (Infra-)Strukturen der digitalen Gesellschaft. Zum anderen sind Handlungsträgerschaft sowie infrastrukturelle Reichweite hochgradig verteilt. Sie reicht von Entscheidungsträgern wie einer Krankenhausleitung, einer Landesregierung oder der CEO eines Unternehmens, über die Mitarbeitenden, die Verfahren und Prozesse der Cybersicherheit ausführen, lernen und entwickeln, bis hin zu denjenigen in Firmen, die nach der Attacke das System wieder aufräumen, sichern und wiederherstellen, sowie den digitalen Forensiker*innen, die Spuren des Angriffs nachgehen und Methoden entwickeln, dieses Nachspüren zu ermöglichen. Cybersicherheit erweist sich, wie auch die Sicherheit kritischer Infrastrukturen, als Ergebnis konzertierter, überorganisationaler Anstrengungen (LaPorte 2006).

Ein großer Teil der Forschung um IT-Sicherheit dreht sich daher um die Frage der Umsetzung von sicheren Design-Strukturen (Privacy/Security by Design) einerseits und der Herstellung von sicheren Praktiken im Umgang mit IT andererseits (Usable Security und Security Awareness). Mit dem Einbezug menschlicher Teilnehmer*innen in organisationale Sicherheitspraktiken stehen IT-Sicherheitsforscher*innen und Expert*innen vor der Herausforderung, nicht nur Hard- und Software, sondern auch das soziotechnische Gefüge der alltäglichen Nutzung auf dem neuesten Stand zu halten. Konfrontiert werden sie dabei nicht nur mit habitualisierter Hysteresis (Bourdieu 1987: 117), sondern auch mit betrieblichen und organisationalen Eigenheiten, an die sie ihre Sicherungspraktiken anpassen müssen, wie das Projekt in Abschnitt 3.2. verdeutlicht. Die zum Teil rapiden, aus sicherheitstechnischer Sicht geforderten Aktualisierungen, die ein Ideal vollkommener Sicherheit vorschreiben würde, sind in der Praxis gar nicht möglich und erzwingen fortlaufend Kompromisslösungen – oder gar Verzicht (s. 3.1). In einer soziologischen Lesart von Resilienz zeichnet sich auch Cybersicherheit durch ihre Erwartungsabhängigkeit und Fähigkeit zur kontinuierlichen Transformation aus (Endreß & Rampp 2014). Da der zu sichernde Kernbestand sozial definiert wird, muss seine Definition kontinuierlich hervorgebracht und stabilisiert werden. Die Zeitlichkeit der Ereignisse sowie Veränderungen der technischen Infrastrukturen und sozialen Erwartungserwartungen ringen der Cybersicherheit eine grundlegende Wandelbarkeit ab, die sie als fortwährende soziotechnische Gestaltungsaufgabe markiert.

Die Dynamiken ‚guter' Sicherheitspraxis und eine entsprechende, breit angelegte Wissensvermittlung fordert von den Teilnehmer*innen immer auch eine reflexive Berücksichtigung unterschiedlicher Zeithorizonte und Verbreitungslatenzen sicherheitsrelevanten Wissens ein. Es entsteht ein Wettbewerb um knappe Ressourcen (Zeit und Geld), im Hinblick auf die Opportunitätskosten der Entscheidung zwischen Innovation und Instandhaltung (Entwicklung), ‚Sicherheitshygiene' und Alltagsgeschäft (Nutzung), defensive Cybersicherheitsstrategien (z. B. Investitionen in die Strukturen für das Schließen von Sicherheitslücken, s. 3.3) und offensive Cybersicherheitsstrategien (z. B. Investitionen in die Ausnutzung von Sicherheitslücken für Überwachung und ‚Gegenangriffe' im Cyberraum).

4.3 Reflexivierung (Reflexive Zeitlichkeit)

Die vorgebrachten Einsichten verdeutlichen die Bedeutsamkeit und Verletzlichkeit digitaler Technologien, die im Laufe der Zeit vernachlässigt und in Abwesenheit von Wartung allmählich zerfallen können, aber auch ereignishaft gestört und angegriffen werden. Ihre Kopplung an gesellschaftliche Grundfunktionen lässt die Cybersicherheit von Informati-

onsinfrastrukturen als ein existentielles Problem im Sinne Scheffers (2020, 2021) erscheinen, da ihr Scheitern potenziell die gesellschaftliche Reproduktionsfähigkeit gefährdet.

Damit ist eine kritische soziologische Perspektive auf Cybersicherheit nahegelegt, die nach den Reproduktionsmechanismen von Cybersicherheit selbst fragt und auslotet, wie weit ihre existentielle Relevanz trägt. Ein erheblicher Bestandteil einer solchen Perspektive ist die Betrachtung von und Auseinandersetzung mit feldimmanenter Kritik und Reflexion (s. 3.3). Es handelt sich hierbei um ein stark akademisiertes Feld,[7] das praxisbezogene Kritik methodisch integriert und sich dadurch selbst beobachtet und reflektiert. Die Bandbreite reicht von Kritik am Narrativ eines möglichen „Cyber Dooms" globalen Ausmaßes (Stevens 2015) bis hin zur lakonischen Feststellung „Cybersecurity is not very important" (Odlyzko 2019). Akteur*innen im Feld der Cybersicherheit rahmen Bedrohungen zunehmend als existenziell und propagieren entsprechend radikale Bewältigungsstrategien wie jüngst das Zero-Trust-Modell: Der bloße Schutz der Systemgrenzen („Perimeter Defense") gilt hierbei als unzureichend und die Position innerhalb des Systems legitimiert noch keinen Zugriff („never trust, always verify"). Stattdessen solle eine dynamische, risikobasierte Verifizierung eines jeden einzelnen Datenzugangs erfolgen, um den steigenden Cyberrisiken gerecht zu werden (s. etwa Spreti & Maatman 2022). Im wissenschaftlichen Cybersicherheitsdiskurs wird Zero Trust intensiv untersucht; so analysieren Weinberg und Cohen (2024) den Übergang vom Perimetermodell zum Zero-Trust-Framework und heben dessen Relevanz angesichts moderner Bedrohungen hervor. Je nach Wahrnehmung und Erwartungshaltung wandeln sich dergestalt die Erzählungen von und über Cybersicherheit. Von graduellen Anpassungen für ein bewältigbares Problem bis hin zu radikalen Bewältigungsstrategien für ein existentielles Problem zeigen sich Nuancen und Dynamiken, die nicht nur für heterogene Narrative im Wandel sprechen, sondern auch kontinuierliche Selbstbeobachtung und kritische Begleitung erfordern.

Wie in den aktuellen Forschungsprojekten gezeigt, setzen sich die Teilnehmer*innen selbst mit der multiplen zeitlichen Strukturierung ihres Feldes auseinander, erkennen die unterschiedlichen, praktischen temporalen Konturierungen an, setzen sie in Relation und extrapolieren Konsequenzen. Es liegt daher nahe, aus der Begegnung mit dem Feld zeitsoziologische Überlegungen anzustoßen – Überlegungen, die von der Beschreibung der Verhältnisse des Feldes ausgehen, aber nicht bei ihnen stehen bleiben können, sondern sich wiederum ins Verhältnis zum Feld setzen und die spezifischen, sozialtheoretischen Relevanzsetzungen ihrer Fachkolleg*innen anerkennen. Im Gemeinplatz dreifacher Reflexivität des Gegenstands (Bergmann 2006: 22–25) – als Eigenschaft fortlaufenden und minutiösen *sense makings* (1), feldimmanenter Selbstbezüglichkeiten (2) sowie dem Verhältnis zwischen Forscher*innen und Beforschten (3) – wird dieses Verhältnis durch die drängenden Probleme, vor denen das Forschungsfeld steht, auf ihre Zeitdimension hin spezifiziert und auf Fragen praktisch vollzogener und koordinierter Multitemporalität zugespitzt: Die Teilnehmer*innen sind fortlaufend und situativ dem Problem multizeitlicher Koordination ausgesetzt. Sie sind gefordert, diese Koordination zu theoretisieren, in ihre feldspezifische Praxis zu integrieren und die integrative Leistung zu kommunizieren. Unwillkürlich präsentieren sie sich damit in der soziologischen Beobachtung als ein Forschungsfeld, das der Soziologie ihre eigenen zeittheoretischen Defizite aufzeigt und in Aussicht stellt, in dessen Untersuchung die theoretische Betrachtung von Zeit zu erweitern und somit diese Defizite zu reduzieren.

5 Cybersecurity als temporales Grenzobjekt

Wir sind dem Befund gefolgt, dass die Soziologie Cybersicherheit bislang kaum als eigenständigen Gegenstand bearbeitet. Das ist bemerkenswert, weil der gestiegenen Aufmerksamkeit in Informations- und Politikwissenschaften sowie in den interdisziplinären Security Studies eine soziologische Leerstelle gegenübersteht. Zugleich hat sich „Digitalisierung" als Querschnittsthema in nahezu allen Debatten etabliert und gesellschaftstheoretische Diagnosen hervorgebracht, die die digital-infrastrukturelle Verfasstheit der Gegenwart betonen, jedoch die von Cybersicherheit und einschlägigen Vorfällen ausgehenden Dynamiken weitgehend ausblenden.

Anstatt Cybersicherheit vorschnell in ein bestehendes theoretisches Gerüst zu integrieren oder lediglich als weiteres empirisches Forschungsfeld zu behandeln, haben wir einen multiperspektivischen Zugang zu Cybersicherheit entwickelt: In Abschnitt 2 haben wir das Feld der Cybersicherheit skizziert und Zeitlichkeit bzw. Multitemporalität als sensibilisierendes Konzept in seiner wissenschaftlichen

7 In Deutschland und Europa hat die Anzahl der Lehrstühle für Cybersicherheit in den letzten zehn Jahren stark zugenommen, etwa mit acht Lehrstühlen an der TU München und 13 Professuren im Bereich IT-Sicherheit an der Hochschule Darmstadt. Auf europäischer Ebene fördert das EU-Zentrum für Cybersicherheit seit seiner Gründung 2020 die Weiterentwicklung und Zusammenarbeit in einem Bereich, der seit 2010 eine Verdopplung der akademischen Kapazitäten erlebt hat.

Verhandlung wie auch in unserer eigenen Beschäftigung herausgearbeitet. Abschnitt 3 hat anhand selektiver Einblicke aus drei voneinander unabhängigen Forschungsprojekten der Autor*innen illustriert, wie Cybersicherheit temporale Dimensionen der Digitalisierung konflikthaft hervorbringt. Abschnitt 4 hat daran anschließend allgemeinere, multitemporale Spannungsverhältnisse rekonstruiert.

Mit Deibert (2016) als prominentem Vertreter der interdisziplinären Cybersecurity Studies ließen sich diese Spannungen gleichsam diagnostisch für eine digitale Gegenwartsgesellschaft deuten „[which] is entering into a period of intense contests and potential chaos, as a multitude of different actors (states, civil society, businesses, militants, and organized criminal groups) compete to shape the domain in their strategic interests“ (ebd.: 172). Unser Argument ist, dass Cybersecurity solch einer kampf- und konfliktlastigen Vorstellung digitaler Risikogesellschaften empirisch widerspricht. Es findet sich vielmehr ein komplexes Gefüge verschiedener Akteur*innen und Akteursgruppen, deren Relation nicht einfach als Gegen- oder Miteinander beschrieben werden kann. Aus unserer Sicht ist dieses Arrangement stattdessen als noch unterbelichtetes Spezifikum einer komplex verteilten, inkongruenten Wissenskultur der Cybersicherheit zu begreifen (Grenz 2023a). Dessen Akteur*innen sind aufgrund der umfassenden Netzwerkarchitektur digitaler Gesellschaften wechselseitig aufeinander verwiesen und berücksichtigen sich in ihren Planungen gegenseitig genauso wie etwaige digitale Innovationen. Es wäre zugleich verkürzt, dieses Gefüge in einem behavioristischen Sinne als reaktiv zu begreifen, da damit eine vereinfachte lineare Vorher-Nachher-Zeitlichkeit impliziert wäre. Vielmehr wird uns eine disperse Wissenskultur gewahr, die von der Auseinandersetzung mit inkongruenten zeit-technischen Arrangements digitaler Gegenwartsgesellschaften geprägt ist und prototypisch in Gestalt von Cyberangriffen zum Ausdruck kommt.

Das Spezifikum dieser nicht-konsensuellen Interaktion, die imaginative und sozio-technische Folgen zeitigt, lässt sich zunächst mit dem Konzept der „Boundary Objects“ (Bowker & Leigh Star 2000; Leigh Star 2010) greifen. Boundary Objects sind ein Gefüge („set“) material-prozessualer „work arrangements“, die in lokalen Praktiken unterschiedlich spezifiziert sind und gruppenübergreifendes Kooperieren „without consensus“ ermöglichen, indem Teilnehmer*innen zwischen gemeinsamer, unscharfer und spezifisch lokaler Form oszillieren (Leigh Star 2010: 604 f.). In unseren empirischen Fällen treten solche Grenzobjekte im Feld der Cybersicherheit in unterschiedlichen Objektgestalten auf: als institutionalisiertes Prinzip der Vier-Augen-Absicherung, das sich als materielle Taktik alltäglicher Sicherungsmaßnahmen erweist (3.1), mittels IT-Sicherheitskonzepten, spezifischen Schulungen, Szenarien und Simulationen (3.2), oder in Gestalt von verstetigten Konzepten der Resilienz, die nach bestimmten Logging-Systemen verlangen (3.3).

Im Anschluss an dieses Verständnis argumentieren wir, dass sich Grenzobjekte im Feld der Cybersicherheit nicht allein als interpretativ flexible Vermittlungsobjekte zwischen sozialen Welten verstehen lassen, sondern zugleich als Träger und Ausdruck technischer Zeitlichkeiten. In ihnen verdichten sich infrage stehende Temporalitäten – etwa die Latenz von Zero-Day-Exploits, die Geschwindigkeit digitaler Übermittlung (und Ausbreitung z. B. von Viren), oder der rhythmische Takt von Datensicherung und Fehlerbehebung. Diese Zeitlichkeiten sind infrastrukturell sedimentiert, in einem nicht-explikativen Sinne feldübergreifend ‚normiert‘ und damit transsituativ wirksam. Diese Dimension von Grenzobjekten überschreitet lokale und situative Bedeutungszuschreibungen und verweist auf ihre infrastrukturelle Verfasstheit. Im Anschluss an Arbeiten, die Boundary Infrastructures als relationale Konstellationen von Grenzobjekten begreifen (Bowker & Star 2000; Nicolini et al. 2012; Tuertscher et al. 2014; Hummel et al. 2025), schlagen wir vor, diese infrastrukturelle Dimension im Feld der Cybersicherheit als infrastrukturell-zeitliche Tiefenschicht zu fassen.

Anhand unserer drei Forschungsprojekte wird deutlich, dass technische Zeitlichkeit nicht nur als Hintergrundrauschen wirkt, sondern die Praktiken, Konflikte und Aushandlungen aktiv strukturiert. In kleinen und mittleren Unternehmen (3.1) prägt eine auf Dauer gestellte Endlichkeit die Praktiken der Cybersicherheit. In organisationalen Standardisierungsprozessen (3.2) zeigt sich ein Spannungsverhältnis zwischen „aktuellem Stand der Technik“ und träger Wirklichkeit betrieblicher Routinen, in denen die Sicherheit nur nebenbei berücksichtigt wird. In der Resilienzarbeit kritischer Infrastrukturen (3.3) begegnen uns schließlich latente, auf Vorrat gehaltene Reaktionsformen, die zugleich auf plötzliche Ereignisse wie Kaskaden oder systemische Angriffe abzielen.

Davon auszugehen, dass beteiligte Akteur*innen mit Multitemporalität befasst sind, bedeutet, eine bestimmte wissenschaftstheoretische Annahme stark zu machen: dass nämlich Multiperspektivität *selbst* konstitutiv für den Gegenstand ist und dass diese Multiperspektivität nicht aufgelöst werden sollte. Dies ist das leitende epistemologische Prinzip, dem wir als Autor*innengruppe hier folgen. Einerseits finden sich, wie gezeigt, in den Feldern selbst zeitlich situierte Praktiken und Materialisierungen von Cybersicherheit, andererseits re-situieren die disziplinär geprägten Blickwinkel der Autor*innen die Gewichtung der drei zeitlichen Spannungsverhältnisse im Feld und bringen

unterbeleuchtete sowie neuartige Konstellationen hervor. Durch Zeitlichkeit wird Cybersicherheit als ein multiparadigmatischer Gegenstand sichtbar, in dem sich im Laufe der Zeit Symptome, Probleme und Lösungsverfahren einer gegenwärtigen wie zukünftigen sozio-digitalen Ordnung und Dynamiken digitaler Gesellschaften in besonderer Weise entfalten.

Damit präsentieren sich Cybersicherheit und dessen Zeitlichkeiten schließlich als keine austauschbaren, sondern in unserer Auswahl als wohl gewählte Gegenstände (Amann & Hirschauer 1999). Am Beispiel multipler Zeitlichkeiten in den Forschungsprojekten sowie in der Literaturrecherche haben wir gezeigt, dass Cybersicherheit als Feld und Forschungsfeld selbst interdisziplinär, pluralistisch sowie mithin widersprüchlich organisiert ist. Ein zentraler Modus der direkten und indirekt vermittelten Interaktion sind Zeit und Zeitlichkeit, wie sie mit vielfachen Erwartungen an Technologien und Akteur*innen verknüpft sind. Zugleich verweisen permanente Bearbeitung, vorauseilende Absicherung (Resilienz) sowie Versuche dynamischer Standardisierung von Cybersicherheit auf die bemerkenswerte Bedeutung von Inter-Konnektivität sowohl als Imaginäres als auch als technosoziale Interdependenz (Cunneen et al. 2020; Dijck 2013). Indem wir Cybersicherheit als Feld permanenter Aushandlung an den digital-infrastrukturellen Tiefenschichten konturieren, möchten wir deren Relevanz als ein eigenständiges soziologisches Forschungsfeld, das über ein rein technisches Verständnis hinausgeht, konstatieren und zur Diskussion stellen.

Anmerkungen

Wir bedanken uns für Kommentare und hilfreiches Feedback bei Rafael Mrowcynski und Alexander Antony.

Literatur

Amann, K. & S. Hirschauer, 2007: Soziologie treiben. Für eine Kultur der Forschung. Soziale Welt 50: 495–506.

Bauman, Z., D. Bigo, P. Esteves, E. Guild, V. Jabri, D. Lyon & R. B. J. Walker, 2014: After Snowden: Rethinking the Impact of Surveillance. International Political Sociology 8: 121–144. https://doi.org/10.1111/ips.12048

Beck, U., 2009: World at Risk. Cambridge: Polity Press.

Bergmann, J., 2006: Qualitative Methoden der Medienforschung – Einleitung und Rahmung. S. 13–41 in: R. Ayaß & J. Bergmann (Hrsg.), Qualitative Methoden der Medienforschung. Reinbek: Rowohlt.

Bourdieu, P., 1987: Sozialer Sinn. Kritik der theoretischen Vernunft. Frankfurt/Main: Suhrkamp.

Bowker, G.C. & S. Leigh Star, 2000: Sorting Things Out: Classification and Its Consequences. Cambridge: MIT Press. https://doi.org/10.7551/mitpress/6352.001.0001

Bowker, G.C. & S.C. Slota, 2017: How Infrastructure Matters. S. 529–554 in: U. Felt, R. Fouché, C. A. Miller & L. Smith-Doerr (Hrsg.), The Handbook of Science and Technology Studies. Cambridge: MIT Press.

Bundesamt für Sicherheit in der Informationstechnik, 2017: BSI-Standard 200–1. Managementsysteme für Informationssicherheit (ISMS). Version 1.0.

Buchanan, B., 2016: The Cybersecurity Dilemma: Hacking, Trust, and Fear between Nations. Oxford: Oxford University Press. https://doi.org/10.1093/acprof:oso/9780190665012.001.0001

Buzan, B., O. Wæver & J. de Wilde, 1998: Security. A New Framework for Analysis. Boulder: Lynne Rienner. https://doi.org/10.1515/9781685853808

Couldry, N. & A. Hepp, 2017: The Mediated Construction of Reality. Cambridge: Polity.

Cunneen, M., M. Mullins & F. Murphy, 2020: Artificial Intelligence Assistants and Risk: Framing a Connectivity Risk Narrative. AI & SOCIETY 35: 625–634.

Deibert, R.J., 2003: Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace. Millennium 32: 501–530.

Deibert, R.J., 2011: Ronald Deibert: Tracking the Emerging Arms Race in Cyberspace. Bulletin of the Atomic Scientists 67: 1–8. https://doi.org/10.1177/0096340210393703

Deibert, R.J., 2016: Cyber-Security. Kap. 16 in: M. Dunn Cavelty & T. Balzacq (Hrsg.), Routledge Handbook of Security Studies. London: Routledge.

Deibert, R.J. & M. Crete-Nishihata, 2012: Global Governance and the Spread of Cyberspace Controls. Global Governance 18: 339–361. https://doi.org/10.1163/19426720-01803006

Derrida, J., 2003: Eine gewisse unmögliche Möglichkeit, vom Ereignis zu sprechen. Berlin: Merve.

Dijck, J. van, 2013: The Culture of Connectivity: A Critical History of Social Media. Oxford: Oxford University Press.

Dunn Cavelty, M., 2013: From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. International Studies Review 15: 105–122. https://doi.org/10.1111/misr.12023

Dunn Cavelty, M., 2015: Die materiellen Ursachen des Cyberkriegs. Cybersicherheitspolitik jenseits diskursiver Erklärungen. Journal of Self-Regulation and Regulation 1: 167–184.

Eckhardt, D., N. Feist & S. Pfeiffer, 2024: Work Based Human Factor: Vom Mensch als Störfaktor zum Mensch als Sicherheitsgewährleister. S. 274–289 in: Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Cybernation Deutschland: Kooperation gewinnt. Die Themen des 20. Deutschen IT-Sicherheitskongresses. Bonn: Bundesamt für Sicherheit in der Informationstechnik.

Endreß, M. & B. Rampp, 2014: Resilienz als Prozess transformativer Autogenese. Schritte zu einer soziologischen Theorie. BEHEMOTH – A Journal on Civilisation 7: 73–102.

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

Farwell, J.P. & R. Rohozinski, 2011: Stuxnet and the Future of Cyber War. Survival 53: 23–40. https://doi.org/10.1080/00396338.2011.555586

Gartzke, E., 2013: The Myth of Cyberwar: Bringing War in Cyberspace Back down to Earth. International Security 38: 41–73. https://doi.org/10.1162/ISEC_a_00136

Gartzke, E. & J.R. Lindsay, 2015: Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace. Security Studies 24: 316–348. https://doi.org/10.1080/09636412.2015.1038188

Gazos, A., 2023: Die soziomaterielle Konstitution von Cybersicherheit in der Dynamik kritischer Informationsinfrastrukturen. In: P.I. Villa (Hrsg.), Polarisierte Welten: Verhandlungen des 41. Kongresses der Deutschen Gesellschaft für Soziologie.

Gell, A., 1992: The Anthropology of Time: Cultural Constructions of Temporal Maps and Images. Oxford: Berg.

Grenz, T., 2023a: Mediatisation, Economy, and Infrastructural Dynamics in the Digital Risk Society. S. 96–110 in: K. Kopecka-Piech & G. Bolin (Hrsg.), Contemporary Challenges in Mediatisation Research. London: Routledge. https://doi.org/10.4324/9781003324591-9

Grenz, T., 2023b: Cybersecurity Events und die Reflexivität eruptiver Ereignisse. S. 411–425 in: H. Knoblauch & A. Singh (Hrsg.), Kommunikative Gattungen und Events. Wiesbaden: Springer VS. https://doi.org/10.1007/978-3-658-41941-7_19

Guagnin, D., 2024: IT-Sicherheit vs. Sicherheit in der IT – Ein unlösbarer Widerspruch? FifF Kommunikation 41: 29.

Guagnin, D., L. Kocksch & B. Wiesse, 2024: Für eine De-Militarisierung von Cybersicherheit. FifF Kommunikation 41: 36–42.

Hansen, L. & H. Nissenbaum, 2009: Digital Disaster, Cyber Security, and the Copenhagen School. International Studies Quarterly 53: 1155–1175. https://doi.org/10.1111/j.1468-2478.2009.00572.x

Helfferich, C., 2022: Leitfaden- und Experteninterviews. S. 875–892 in: N. Baur & J. Blasius (Hrsg.), Handbuch Methoden der empirischen Sozialforschung. Wiesbaden: Springer VS. https://doi.org/10.1007/978-3-658-37985-8_55

Hepp, A., 2020: Deep Mediatization: Key Ideas in Media & Cultural Studies. Milton: Taylor & Francis. https://doi.org/10.4324/9781351064903

Hollnagel, E., 2014: Resilience Engineering and the Built Environment. Building Research & Information 42:1–8.

Hummel, J.T., H. Berends & P. Tuertscher, 2025: From Boundary Objects to Boundary Infrastructure: A Process Study of Collaboration between Big Science and Big Business. Journal of Management Studies 62, 1644–1679. https://doi.org/10.1111/joms.13118

Jackson, S.J., 2014: Rethinking Repair. S. 221–239 in: T. Gillespie, P.J. Boczkowski & K.A. Foot (Hrsg.), Media Technologies: Essays on Communication, Materiality, and Society. Cambridge: MIT Press. https://doi.org/10.7551/mitpress/9780262525374.003.0011

Kalthoff, H., S. Hirschauer & G. Lindemann (Hrsg.), 2008: Theoretische Empirie. Zur Relevanz qualitativer Forschung. Frankfurt/Main: Suhrkamp.

Kamis, B. und T. Thiel, 2015: The Original Battle Trolls: How States Represent the Internet as a Violent Place. PRIF Working Paper No. 23. Frankfurt/Main.

Kello, L., 2013: The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. International Security 38: 7–40. https://doi.org/10.1162/ISEC_a_00138

Knoblauch, H., 2020: The Communicative Construction of Reality. London: Routledge.

Kocksch, L., 2020: Knowing IT-Security Emergencies: Die Herstellung von Unsicherheit. S. 175–210 in: A. Wiedman, K. Wagenknecht, P. Goll & A. Wagenknecht (Hrsg.), Wie forschen mit den „Science and Technology Studies“? Bielefeld: Transcript. https://doi.org/10.14361/9783839443798-007

Kocksch, L., 2024. Fragile Computing: How To Live with Insecure Technologies. London: Palgrave Macmillan. https://doi.org/10.1007/978-981-99-9807-4

Kocksch, L., M. Korn, A. Poller & S. Wagenknecht, 2018: Caring for IT Security: Accountabilities, Moralities, and Oscillations in IT Security Practices. Proceedings of the ACM on Human-Computer Interaction 2, CSCW, Art. 92. https://doi.org/10.1145/3274361

Kocksch, L. & Sørensen, E., 2023: Towards a typology of interdisciplinarity in cybersecurity: Trade, choice, and agnostic-antagonist. S. 116–129 in: Proceedings of the 2023 New Security Paradigms Workshop.

Kocksch, L. & T.E. Jensen, 2024: The Mundane Art of Cybersecurity: Living with Insecure IT in Danish Small- and Medium-Sized Enterprises. Proceedings of the ACM on Human-Computer Interaction 8, CSCW2, Art. 354. https://doi.org/10.1145/3686893

LaPorte, T.M., 2006: Organizational Strategies for Complex System Resilience, Reliability, and Adaptation. S. 135–154 in: P.E. Auerswald, L.M. Branscomb, T.M. LaPorte & E.O. Michel-Kerjan (Hrsg.): Seeds of Disaster, Roots of Response. Cambridge: Cambridge University Press.

LaPorte, T.R. & P. Consolini, 1991: Working in Practice But Not in Theory: Theoretical Challenges of „High-Reliability Organizations“. Journal of Public Administration Research and Theory 1: 19–48. https://doi.org/10.1093/oxfordjournals.jpart.a037070

Leigh Star, S., 2010: This Is Not a Boundary Object: Reflections on the Origin of a Concept. Science, Technology, & Human Values 35: 601–617. https://doi.org/10.1177/0162243910377624

Liff, A.P., 2012: Cyberwar: A New ‚Absolute Weapon‘? The Proliferation of Cyberwarfare Capabilities and Interstate War. Journal of Strategic Studies 35: 401–428. https://doi.org/10.1080/01402390.2012.663252

Lindsay, J.R., 2013: Stuxnet and the Limits of Cyber Warfare. Security Studies 22: 365–404. https://doi.org/10.1080/09636412.2013.816122

Lupovici, A., 2016: The ‚Attribution Problem‘ and the Social Construction of ‘Violence’: Taking Cyber Deterrence Literature a Step Forward. International Studies Perspectives 17: 322–342.

Lyon, D., 2015: Surveillance After Snowden. Cambridge: Polity Press.

Maurer, T., 2018: Cyber Mercenaries. Cambridge: Cambridge University Press. https://doi.org/10.1017/9781316422724

Mayring, P., 1991: Qualitative Inhaltsanalyse. S. 209–213 in: U. Flick, E. v. Kardoff, H. Keupp, L. v. Rosenstiel & S. Wolff (Hrsg.), Handbuch qualitative Forschung: Grundlagen, Konzepte, Methoden und Anwendungen. München: Beltz.

Mayring, P., 2014: Qualitative content analysis: Theoretical background and procedures. S. 365–380 in: A. Bikner-Ahssbahs, C. Knipping & N. Presmeg (Hrsg.), Approaches to qualitative research in mathematics education: Examples of methodology and methods. Dordrecht: Springer. https://doi.org/10.1007/978-94-017-9181-6_13

Mayring, P., 2019. Qualitative Content Analysis: Demarcation, Varieties, Developments. Forum Qualitative Sozialforschung Forum: Qualitative Social Research 20. https://doi.org/10.17169/fqs-20.3.3343

Miller, C., 2007: The Legitimate Vulnerability Market: The Secretive World of 0-Day Exploit Sales. Workshop on the Economics of Information Security.

Mol, A., 2002: The body multiple: Ontology in medical practice. Durham: Duke University Press.

Möllers, N., 2021: Making Digital Territory: Cybersecurity, Techno-Nationalism, and the Moral Boundaries of the State. Science, Technology, & Human Values 46: 112–138. https://doi.org/10.1177/0162243920904436

Nicolini, D., J. Mengis & J. Swan, 2012: Understanding the Role of Objects in Cross-Disciplinary Collaboration. Organization Science 23: 612–629. https://doi.org/10.1287/orsc.1110.0664
Niewöhner, J., 2014: Perspektiven der Infrastrukturforschung: care-full, relational, ko-laborativ. S. 341–352 in: D. Lengersdorf & M. Wieser (Hrsg.), Schlüsselwerke der Science & Technology Studies. Wiesbaden: Springer. https://doi.org/10.1007/978-3-531-19455-4_28
Odlyzko, A., 2019: Cybersecurity Is Not Very Important. Ubiquity 2019: 1–23. https://doi.org/10.1145/3333611
Parikka, J., 2007: Digital Contagions: A Media Archaeology of Computer Viruses. Lausanne: Peter Lang.
Perrow, C., 1999: Normal Accidents: Living with High Risk Technologies – Updated Edition. Princeton: Princeton University Press. https://doi.org/10.2307/j.ctt7srgf
Rasborg, K., 2021: Ulrich Beck. Theorising World Risk Society and Cosmpolitanism. Cham: Palgrave McMillan. https://doi.org/10.1007/978-3-030-89201-2
Rid, T., 2012: Cyber War Will Not Take Place. Journal of Strategic Studies 35: 5–32.
Rid, T. & B. Buchanan, 2015: Attributing Cyber Attacks. Journal of Strategic Studies 38: 4–37.
Rupp, C., 2022: (Inter-)Nationales Sicherheitsgeflecht: Mapping der deutschen staatlichen Cybersicherheits-Architektur. kes 3/2022. https://www.kes-informationssicherheit.de/print/titelthema-sicherheits-bewusstsein-und-kultur/inter-nationales-sicherheitsgeflecht/. Aufruf 06.07.26.
Saco, D., 1999: Colonizing Cyberspace: National Security and the Internet. S. 266–270 in: J. Weldes, M. Laffey, H. Gusterson & R. Duvall (Hrsg.), Cultures of Insecurity. Minneapolis: University of Minnesota Press.
Scheffer, T., 2020: Kritische Ethnomethodologie. Zeitschrift für Soziologie 49: 218–235. https://doi.org/10.1515/zfsoz-2020-0020
Scheffer, T., 2021: Existentielle Probleme, soziologisch. Zeitschrift für Theoretische Soziologie 10: 3–33. https://doi.org/10.3262/ZTS2101003
Seyfert, R. & J. Roberge (Hrsg.), 2017: Algorithmuskulturen: über die rechnerische Konstruktion der Wirklichkeit. Bielefeld: Transcript. https://doi.org/10.14361/9783839438008
Smeets, M., 2018: A Matter of Time: On the Transitory Nature of Cyberweapons. Journal of Strategic Studies 41: 6–32. https://doi.org/10.1080/01402390.2017.1288107
Spreti, M. v. & M. Maatman, 2022: Zero Trust: Paradigmenwechsel in der Cybersecurity. https://www.deloitte.com/de/de/services/risk-advisory/perspectives/zero-trust.html, Aufruf 19.02.25.
Stevens, T., 2012: A Cyberwar of Ideas? Deterrence and Norms in Cyberspace. Contemporary Security Policy 33: 148–170. https://doi.org/10.1080/13523260.2012.659597
Stevens, T., 2015: Cyber security and the politics of time. Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9781316271636
Stone, J., 2013: Cyber War *Will* Take Place! Journal of Strategic Studies 36: 101–108. https://doi.org/10.1080/01402390.2012.730485
Szor, P., 2005: The Art of Computer Virus Research and Defense. London: Pearson.
Taddeo, M. 2018: Deterrence and Norms to Foster Stability in Cyberspace. Philosophy & Technology 31: 323–329. https://doi.org/10.1007/s13347-018-0328-0
Tuertscher, P, R. Garud & A. Kumaraswamy: Justification and Interlaced Knowledge at ATLAS, CERN. Organization Science 25: 1579–1608. https://doi.org/10.1287/orsc.2013.0894
Weick, K.E., K.M. Sutcliffe & D. Obstfeld (1999/2008). Organizing for High Reliability: Processes of Collective Mindfulness. S. 31–66 in: A. Boin (Hrsg.), Crisis management London: SAGE.
Weinberg, A.I. & K. Cohen, 2024: Zero Trust Implementation in the Emerging Technologies Era: Survey. Arxiv, Cryptography and Security. arXiv:2401.09575 [cs.CR]. https://doi.org/10.48550/arXiv.2401.09575
Witzel, A., 2000: Das problemzentrierte Interview. Forum Qualitative Sozialforschung 1. https://doi.org/10.17169/fqs-1.1.1132
World Economic Forum, 2022: The Cyber Resilience Index: Advancing Organizational Cyber Resilience. White Paper.

Autor*innen

Dennis Eckhardt
Institut für Kulturanthropologie und Europäische Ethnologie
Goethe-Universität
Norbert-Wollheim-Platz 1
60629 Frankfurt am Main
E-Mail: dennis.eckhardt@fau.de
https://orcid.org/0000-0002-5935-9144

Dennis Eckhardt ist Vertretungsprofessor für Kulturanthropologie und Europäische Ethnologie an der Goethe-Universität in Frankfurt/Main. Studium der Europäischen Ethnologie und Soziologie in Frankfurt/Main und Berlin. Anschließend wissenschaftlicher Mitarbeiter am Institut für Soziologie der FAU Erlangen-Nürnberg.
Forschungsschwerpunkte: Digitale Anthropologie; Arbeitsanthropologie; ko-laboratives Arbeiten in interdisziplinären Kontexten; ethnografische Methoden.

Nelli Feist
FAU Erlangen-Nürnberg
Lehrstuhl für Soziologie (Technik – Arbeit – Gesellschaft)
Fürther Str. 246c
90429 Nürnberg
E-Mail: nelli.feist@fau.de
https://orcid.org/0009-0008-9712-1218

Nelli Feist ist wissenschaftliche Mitarbeiterin und Doktorandin am Institut für Soziologie an der FAU Erlangen-Nürnberg. Studium der Sozialwissenschaften in Göttingen sowie Soziologie und Sozialforschung an der Universität Bremen. Aktuell forscht sie im Projekt „emGAI“ zu den Auswirkungen generativer KI auf die Arbeitsorganisation in der medizinischen Versorgung.
Forschungsschwerpunkt: Betriebliche Integration von Cybersicherheit, u. a. im Zusammenspiel mit den Anforderungen generativer KI.
Wichtigste Publikationen: Work Based Human Factor: Vom Mensch als Störfaktor zum Mensch als Sicherheitsgewährleister, in: Bundesamt für Sicherheit in der Informationstechnik (Hrsg.), Cybernation Deutschland: Kooperation gewinnt. Die Themen des 20. Deutschen IT-Sicherheitskongresses 2024 (mit D. Eckhardt & S. Pfeiffer); The Complexity of Cyber Security in Private and Professional Everyday Life – An Ethnographic-Informatic Collaborative Approach, in: Moallem, A. (Hrsg.), HCI for Cybersecurity, Privacy and Trust. HCII 2025. Lecture Notes in Computer Science, Vol 15814. Wiesbaden 2025 (mit H.C. Pöhls, D. Eckhardt, S. Pfeiffer, D. Herrmann & S. Katzenbeisser).

Alexandros Gazos
Institut für Technikfolgenabschätzung und Systemanalyse
Karlsruher Institut für Technologie
Karlstraße 11
76133 Karlsruhe
E-Mail: alexandros.gazos@kit.edu
https://orcid.org/0000-0002-4779-6179

Alexandros Gazos ist Projektleiter und wissenschaftlicher Mitarbeiter am Institut für Technikfolgenabschätzung und Systemanalyse (ITAS). Studium der Soziologie in Frankfurt/Main. Seit 2021 Doktorand am Karlsruher Institut für Technologie (KIT). Derzeit leitet er das Projekt „MOTRA-TM – Technologiemonitoring“ im Rahmen des Verbundprojektes „Monitoringsystem und Transferplattform Radikalisierung“.
Forschungsschwerpunkte: Techniksoziologie; Organisationssoziologie; Technikfolgenabschätzung; Resilienz; Risiken künstlicher Intelligenz; extremistische/terroristische Innovationen.
Wichtigste Publikationen: Die soziomaterielle Konstitution von Cybersicherheit in der Dynamik kritischer Informationsinfrastrukturen, in P.-I. Villa (Hrsg.), Polarisierte Welten: Verhandlungen des 41. Kongresses der Deutschen Gesellschaft für Soziologie 2022; Organising AI for safety: Identifying structural vulnerabilities to guide the design of AI-enhanced socio-technical systems. Safety Science, 184/2025, 106731 (mit J. Kahn, I. Kusche, C. Büscher & M. Götz).

Tilo Grenz
Pädagogische Hochschule Thurgau
Unterer Schulweg 3
Postfach
CH-8280 Kreuzlingen 1
E-Mail: Tilo.Grenz@phtg.ch
https://orcid.org/0000-0002-6255-3060

Tilo Grenz, Dr. phil., Stabsstelle Forschung und Dozierender an der Pädagogischen Hochschule Thurgau.
Forschungsschwerpunkte: Mediatisierung und De-Mediatisierung; Plattformkontroversen; infrastrukturelle Dynamiken der Digitalen Risikogesellschaft; Cybersicherheit und Cyberangriffe.
Wichtigste Publikation: Temporary Infrastructure, Temporal Boundary Work, Form Investments, and Delayed Endings. Science, Technology, & Human Value, online first. 2026 (mit P. Knopp).

Daniel Guagnin
Freier Mitarbeiter
nexus Institut für Kooperationsmanagement und interdisziplinäre Forschung GmbH
EUREF-Campus 15a
D-10829 Berlin
E-Mail: soziologe@guagnin.de
https://orcid.org/0009-0009-7715-0270

Daniel Guagnin, Dr. phil., freiberuflicher Berater zu Technikgovernance und Technikfolgenabschätzung. Studium der Soziologie, Informatik und Finanzwissenschaften an der Albert-Ludwigs-Universität in Freiburg/Breisgau.
Forschungsschwerpunkte: Datenschutz, Cybersicherheit, Digitale Grundrechte und Algorithmen-Ethik.
Wichtige Publikationen: Demokratie ist auch eine Frage der technischen Gestaltung, in: K. Späte et al. (Hrsg.), Künstliche Intelligenz und soziologische Berufspraxis. Zum Einsatz von KI-Tools. Springer Nature (i.E.); Praxisorientierter Ansatz zur partizipativen Entwicklung von KI-Systemen, Mensch und Computer 2025-Workshopband 2025 (mit A. Hazim); Für eine De-Militarisierung von Cybersicherheit, FifF Kommunikation 41/2024, 36–42 (mit L. Kocksch & B. Wiesse).

Laura Kocksch
The Techno-Anthropology Lab
Department of Culture and Communication
Aalborg University Copenhagen
A C Meyers Vænge 15
2450 København SV
Denmark
E-Mail: laurak@ikk.aau.dk
https://orcid.org/0000-0003-4661-2638

Laura Kocksch ist Assistant Professor und Leiterin Experimenteller Praktiken am Techno-Anthropologie Labor der Aalborg Universität Kopenhagen. Studium der Kulturanthropologie und Europäischen Ethnologie sowie Informatik an der Goethe Universität Frankfurt/Main; Promotion 2023.
Forschungsschwerpunkte: Science and Technology Studies, Infrastruktur, Feministische und Umwelt-Anthropologie.
Wichtigste Publikationen: Fragile Computing: How To Live With Insecure Technologies. Palgrave Macmillan 2024. https://doi.org/10.1007/978-981-99-9807-4; The Mundane Art of Cybersecurity: Living with Insecure IT in Danish Small- and Medium-Sized Enterprises. Proceedings of the ACM on Human-Computer Interaction, 8/2024 (CSCW2), 1–17. (mit T.E. Jensen).

Sezgin Sönmez
Institut für Soziologie
Technische Universität Berlin
Fraunhoferstraße 33-36
10587 Berlin
E-Mail: sezgin.soenmez@tu-berlin.de
https://orcid.org/0009-0003-7583-3779

Sezgin Sönmez, Dr. phil., ist Soziologe und wissenschaftlicher Mitarbeiter am Institut für Soziologie sowie am Sonderforschungsbereich (SFB) 1265 „Re-Figuration von Räumen“ an der Technischen Universität Berlin.
Forschungsschwerpunkte: Wissens- und Kultursoziologie, die Governance des Internets und die räumlichen Figurationen digitaler Infrastrukturen.

Basil Wiesse
Soziologie III
KU Eichstätt-Ingolstadt
Kapuzinergasse 2
85072 Eichstätt
E-Mail: basil.wiesse@ku.de
https://orcid.org/0000-0002-3606-7798

Basil Wiesse ist wissenschaftlicher Mitarbeiter an der Professur für Prozessorientierte Soziologie an der KU Eichstätt-Ingolstadt und Crew Member des Centre for Practice Theory at Lancaster. Forschungsschwerpunkte: Praxistheorie; Ethnomethodologie; Epistemologie; qualitative Methoden und Soziologie des Digitalen.