Die soziomaterielle Konstitution von Cybersicherheit in der Dynamik kritischer Informationsinfrastrukturen

Alexandros Gazos

Beitrag zur Ad-Hoc-Gruppe »Cybersicherheit und Soziologie? Infrastrukturelle Dynamiken der Gegenwartsgesellschaft«

Einleitung

Informations- und Kommunikationstechnologien dringen zusehends in gesellschaftliche Routinen vor und werden zu einem kritischen Faktor in ihrer Aufrechterhaltung. Als kritische Informationsinfrastrukturen sind sie zum essenziellen Bestandteil jeder anderen kritischen Infrastruktur geworden. Aufgrund dieser zunehmenden Verstrickungen und damit einhergehenden Interdependenzen wird Cybersicherheit geradezu zu einer *existenziellen* Aufgabe. Folgenschwere Ereignisse wie Cyberangriffe auf das Gesundheitswesen (Knop 2022) und die Energieversorgung (Zetter 2016) machen diesen Umstand deutlich. Dabei sehen sich Organisationen, die kritische Informationsinfrastrukturen betreiben, mit einer Fülle an Herausforderungen in ihrer Umwelt konfrontiert: von einem professionalisierten Cybercrime-Milieu (Bundesamt für Sicherheit in der Informationstechnik 2022) über die Gefahr terroristischer Anschläge bis hin zur Cyberkriegsführung (Nachrichtendienst des Bundes 2022). Doch liegen die Herausforderungen nicht nur in der Umwelt, sondern auch in dem System kritischer Infrastrukturen selbst begründet: von unvorhergesehenen Unfällen über *Social Engineering* bis hin zu *Supply-Chain*-Angriffen (Newman 2021). Darüber hinaus führt die Konvergenz physischer und digitaler Infrastrukturen zu Vulnerabilitäten, die sich durch Innovationsdynamiken, wie dem *Internet of Things* oder *Cyber-Physical-Systems*, nur weiter verschärfen (Henschke 2021). Kaum ein Zusammenhang macht dies so deutlich wie der Umstand, dass Informationsinfrastrukturen vollständig von ihrer Energieinfrastruktur abhängig sind (Petermann et al. 2011), während gleichzeitig eine zunehmende Anzahl kritischer Prozesse im Energiesektor auf Informations- und Kommunikationstechnologien angewiesen ist (acatech et al. 2021).

Trotz aller Widrigkeiten behaupten sich die Betreiber größtenteils *noch* in dem Unterfangen alltäglich eine hohe Verfügbarkeit ihrer Infrastruktur zu gewährleisten und weisen ein relativ geringes Aufkommen von langanhaltenden sowie weiträumigen Ausfällen auf. Da technologische Systeme, wie sie kritische Informationsinfrastrukturen darstellen, immer auch durch soziale Akteure konstruiert und angepasst werden (Hughes 1987), stellt sich die Frage nach den soziomateriellen Faktoren von Cybersicherheit: Welche technischen Strukturen und sozialen Fähigkeiten sind dafür nötig? Wie könnte eine Bewältigungsstrategie aussehen, die einem so schwer zu antizipierendem Feld an potenziellen Bedrohungen noch gerecht wird? Dabei herrschen in der Technik- und Organisationssoziologie unterschiedliche Vorstellungen davon, ob und wie ein sicherer Betrieb in großen technischen Systemen gewährleistet werden kann. Vor allem Charles Perrow (1987) mit seiner *Normal Accident Theory* hielt komplexe und eng gekoppelte Hochrisiko-Systeme für besonders anfällig für Unfälle und schrieb ihnen ein gewisses

Katastrophenpotenzial zu. Prominente Vertreter:innen der *High Reliability Theory* gingen hingegen davon aus, dass Organisationen selbst bei derartigen Systemen unter Beweis stellten, dass sie die Kontrolle bewahren können. Zu diesem Zweck bereiten sich die Organisationen umfassend auf Extremsituationen vor (Todd R. La Porte und Consolini 1991) und kultivieren bestimmte Fähigkeiten (Weick et al. 1999). Doch handeln diese Theorien vor allem von Sicherheit in Systemen, die noch nicht so umfassend von Informationsinfrastrukturen durchdrungen waren und demzufolge in geringerem Ausmaß von ihrer Aufrechterhaltung abhingen.

Gegenwärtige Infrastrukturen sind komplexer geworden; ihre Umwelt noch undurchsichtiger. Selbst größere Netzwerke aus Organisationen können nur schwer antizipieren, geschweige denn beeinflussen, welche neuen Cyberangriffe entwickelt werden und mit welchen Konsequenzen diese verbunden sind (bspw. *Zero-Day-Exploits*[1]). Umso bedeutsamer ist es, aus den Theorien zu lernen, wie soziomaterielle Systeme zuverlässig aufrechterhalten werden konnten. Damit geht die Hinwendung zu einer systemischen Bewältigungsstrategie einher, die Organisationen in die Lage versetzt mit möglichst vielen Herausforderungen umzugehen, ohne jedwede neue Eigenschaft der Bedrohungen in ihrer Umwelt kennen oder bewältigen zu müssen. Eben eine solche Strategie könnte das Brückenkonzept der Resilienz bieten. In soziotechnischen Systemen beschreibt Resilienz ein Repertoire an Fähigkeiten, mit denen der Bestand an notwendigen Operationen unter erwarteten und unerwarteten Umständen aufrechterhalten werden kann (Hollnagel 2013). Da jede Art des Umstands so bewältigt werden muss, dass kritische Operationen fortbestehen, liegen die entscheidenden Aspekte der Resilienz in der soziotechnischen Beschaffenheit des Systems selbst sowie dem Repertoire an Fähigkeiten, das sie aufrechterhält. Mein Beitrag besteht daher in einem gegenstandsangemessenen, kohärenten sowie soziologisch informierten Resilienzkonzept, welches ein neues Licht auf die drängenden Fragen der Cybersicherheit wirft, ihre soziomaterielle Bedingung beleuchtet und so der Dynamik in digitalen und kritischen Infrastrukturen gerecht wird. Das Konzept ebnet möglichen Antworten den Weg, indem es organisationssoziologische Theorien mit Ansätzen aus dem Sicherheitsmanagement technischer Systeme verbindet und deren Aspekte einer sozialkonstruktivistischen Reflexion unterzieht.

Die soziomateriellen Aspekte der Sicherheit

Um eine Idee von der Beschaffenheit großtechnischer Systeme zu erhalten, bietet sich Perrows Perspektive an (Perrow 1987, S. 108–115): Er unterscheidet zunächst zwischen linearen und komplexen Systemen. Der Betrieb von Systemen mit linearen Interaktionen läuft nach erwartbaren Mustern ab. Wenn beispielsweise auf dem Fließband einer Fabrik ein Stau entsteht, lässt sich relativ leicht der Fehler lokalisieren. Komplexe Systeme zeichnen sich hingegen durch Interaktionen aus, die nicht immer durchschaubar sind. Diese Undurchsichtigkeit entsteht beispielsweise durch zahlreiche Monitoringinstrumente, wodurch immer nur ein abgeleitetes Bild von dem System sichtbar ist oder Informationen nur auf indirektem Weg zugänglich sind. In komplexen Systemen übernehmen Komponenten gleichzeitig mehrere Funktionen, von denen andere Komponenten abhängen. Zudem befinden sich oftmals kritische Komponenten in jenen Systemen in enger Nachbarschaft zueinander. Die hohe Anzahl von Mehrfachverbindungen und die kritischen Knotenpunkte vervielfachen die potenziellen Interaktionen in einem komplexen System. Diese Beschaffenheit hat „neuartige oder unbeabsichtigte Rückkopplungs-

[1] Bei *Zero-Day-Exploits* erfahren die Öffentlichkeit und die Hersteller eines Produkts erst dann von einer Schwachstelle des Produkts, wenn diese Schwachstelle bereits für Angriffe genutzt wurde (Bundesamt für Sicherheit in der Informationstechnik 2023). Der bekannteste Fall eines solchen Angriffs ist der *Stuxnet*-Virus, welcher eine Urananreicherungsanlage im Iran empfindlich störte (Stöcker 2010).

schleifen“ (Perrow 1987, S. 125) zur Folge. Für Perrow sind Kernreaktoren sowie große chemische Anlagen klassische Beispiele komplexer Systeme mit unvermeidbaren Risiken.

Mit der zunehmenden Automatisierung kritischer Infrastrukturen, durch Informations- und Kommunikationstechnologien sowie die Konvergenz in cyber-physischen Systemen, werden auch ihre Interaktionen komplexer. In diesen soziotechnischen Systemen werden zahlreiche Prozesse über Sensoren, Displays, Kontrollinstrumente und Aktuatoren auf verschiedenen Ebenen gebündelt. Die Informationen über den Systemzustand, die Betreiber über solche Instrumente beziehen, bieten somit eine gesammelte und abgeleitete Form der Informationslage. Zudem steigt die Anzahl potenzieller Interaktionen zwischen dem *ersten* Moment der Wahrnehmung einer neuen Information durch die Sensorik und dem *finalen* Moment der Umsetzung eines Kontrollbefehls. Mit diesen Interaktionen steigt auch die Möglichkeit, dass es zu neuen oder unbeabsichtigten Rückkopplungsschleifen kommt.

Ob der zunehmenden Komplexität in kritischen Informationsinfrastrukturen jedoch ein Katastrophenrisiko innewohnt, hängt auch davon ab, wie die Komponenten in jenen Systemen aneinandergekoppelt sind. Für Perrow ähneln erneut die Kernkraftwerke in ihrer Beschaffenheit beinahe idealtypisch eng gekoppelten Systemen. Diese Systeme sind tendenziell zeitgebundener in ihren Betriebsabläufen, wobei eine Aktion der Nächsten folgt, und das möglichst ohne Unterbrechungen. Ihre Abläufe weisen eine rigidere Struktur auf und kennen nur „einen Weg zur Verwirklichung des Produktionsziels“ (Perrow 1987, S. 133). Durch die hohe Abhängigkeit in solchen Systemen verbreiten sich auch Fehler sowie Unfälle schnell und umfassend. In lose gekoppelten Systemen (bspw. Universitäten) können sich Abläufe ohne Probleme verzögern. Sie verfügen über eine Bandbreite alternativer Möglichkeiten und bieten einen größeren Spielraum hinsichtlich der Substitution von Ressourcen, Ausrüstung und Personal. Für die Regeneration nach einem Fehler oder Unfall hat dieser Unterschied zur Folge, dass Betreiber in lose gekoppelten Systemen über flexiblere Kapazitäten verfügen, mit denen sie eher improvisieren können (Perrow 1987, S. 130–139).

Kritische Informationsinfrastrukturen sind in mehrfacher Hinsicht eng an andere Infrastrukturen gekoppelt:

(1) Informations- und Kommunikationstechnologien sind zur Grundlage des beschleunigten und (teil-)automatisierten Betriebs anderer Infrastrukturen geworden.
(2) Mit dieser Entwicklung geht der Anspruch an eine ununterbrochene sowie beschleunigte Funktionstüchtigkeit einher, dem die digitalen Infrastrukturen gerecht werden müssen.
(3) Digitale Infrastrukturen sind unmittelbar von physischen Infrastrukturen abhängig; vor allem von der infrastrukturell bereitgestellten Ressource *Strom*.
(4) Eine zunehmende Anzahl kritischer Prozesse in der Energieversorgung ist wiederum abhängig von der Funktionalität kritischer Informationsinfrastrukturen.

Wo Perrow noch unvereinbare Anforderungen an die Kontrolle eng gekoppelter und komplexer Systeme sah – nämlich zentralisierte Autorität für Erstere und autonome Entscheidungsfindung für Letztere – sahen die Vertreter:innen der *High Reliability Theory* die Möglichkeit zur Kontrolle über eine simultan dezentralisierte und zentralisierte Autoritätsstruktur (Hopkins 1999, S. 98). So würden sich formale Hierarchien, Routinen und Bürokratie in Zeiten hoher Belastung auflösen, um die Entscheidungsfindung Mitarbeiter:innen zu überlassen, die unmittelbar vor Ort sind (Todd R. La Porte und Consolini 1991). Für eine soziotechnische Bewältigungsstrategie, die *Normal Accident Theory* und *High Reliability Theory* zusammen denkt und mit einer neuen Linse auf kritische Informationsinfrastrukturen blickt, hilft es Perrows 2x2 Matrix zur Systembeschaffenheit (linear bis komplex & eng bis lose gekoppelt) als ein dynamisches Raster zu verstehen (Weick 2004, S. 29 f.): Sowohl erwartbar und erwünscht als auch unvorhergesehen und nicht intendiert können Systeme graduell oder plötzlich in eine andere Beschaffenheit übergehen und so ihre Funktionalität bewahren, aber auch katastrophale Konsequenzen zeitigen.

Ob sich ein System somit in einem sicheren oder unsicheren Zustand befindet, hängt somit zwar von der Beschaffenheit ab, wird aber auch entscheidend von dem Repertoire an Fähigkeiten bestimmt, über das eine Organisation zur Kontrolle ihres Systems verfügt. *High Reliability Organizations (HRO)* stellen sicher, dass sich ihre Mitarbeiter:innen komplexer Interaktionen bewusst sind. Zu diesem Zweck unternehmen sie erhebliche Anstrengungen, um Notfallsituationen zu simulieren (Todd R. La Porte und Consolini 1991, S. 31). Mitarbeiter:innen gehen davon aus, überrascht zu werden, da sie bereits mit der Möglichkeit rechnen, einen analytischen Fehler begangen zu haben. HROs ermutigen ihr Personal dazu, von kleinsten Fehlern zu berichten, um so den Horizont an Ereignissen zu erweitern, aus denen sie lernen. Neben dieser Fehlerkultur generieren HROs Erfahrung und eine übergreifende Einsicht bei ihren Mitarbeiter:innen, indem sie Zuständigkeiten untereinander rotieren. Eine Bandbreite an diversen Perspektiven soll im offenen Austausch eine Form von sozialer Redundanz erzeugen, bei der Skepsis sogar erwünscht ist, um nicht einer unterkomplexen Darstellung der Betriebsabläufe oder Störungen zu verfallen. Mitarbeiter:innen bewahren sich selbst in zeitkritischen Situationen ein ganzheitliches Bild des Systems und eine situationsadäquate Wachsamkeit. HROs und ihre Belegschaft verschreiben sich vollumfänglich dem Resilienzgedanken. Sie unterstützen ausdrücklich Improvisation und organisieren sich in ad hoc Netzwerken, sollten es die Umstände erfordern. Ihre flexiblen Strukturen lassen zu, dass die Entscheidungsfindung mit den auftretenden Problemen migriert. Anpassungsfähig rekombinieren sie bewährte Handlungen in ihrem Repertoire zu neuartigen Mustern (Weick et al. 1999, S. 39–49).

Die Ausführungen zeigen eindrücklich, dass jene Organisationen nicht nur ein Repertoire an Fähigkeiten zur Kontrolle ihres Systems kultivieren, sondern auch kontinuierlich an der Weiterentwicklung desselben arbeiten. Ein System entwickelt sich jedoch nicht in einem Vakuum und Betreiber kritischer (Informations-)Infrastrukturen können auch keine (Cyber-)Sicherheit herstellen oder bewahren, ohne ihre Umwelt zu berücksichtigen. Andere Systeme und Betreiber, regulierende Behörden und Kunden haben einen Einfluss auf die *eigene* Systemdynamik. Aufgrund der hohen Interdependenzen sind Betreiber kritischer Informationsinfrastrukturen auf die Leistung anderer kritischer Infrastruktursysteme angewiesen und benötigen zum Teil auch die Unterstützung und Kooperation anderer Betreiber.

In interdependenten Systemen drohen Gefahren zu den schwächsten Gliedern in der Kette überzugehen und kaskadierende Ausfälle zu provozieren. Im Angesicht der hohen Variabilität und dynamischen Unsicherheit in ihrer Umwelt reicht es somit nicht, dass sich Betreiber intern zusehends komplexer organisieren, sie müssen Formen multi-organisationaler Koordination etablieren. Um über die Bewältigung akuter Ereignisse hinaus eine nachhaltige Kooperationsbasis zu schaffen, benötigt es ein Netzwerk, das die Lehren aus den Krisen auch regulatorisch institutionalisiert. In diesen Netzwerken zeichnen sich die resilienten Systeme dadurch aus, dass sie schnell Informationen über ihre Umwelt einholen und sich entsprechend schnell an wandelnde Umstände anpassen. Sie kommunizieren gründlich untereinander und mobilisieren so Expertise sowie materielle Unterstützung (Todd M. La Porte 2006, S. 139–149).

Das Konzept der Resilienz ist dabei auch das entscheidende Bindeglied, um die blinden Flecken der *Normal Accident Theory (NAT)* und *High Reliability Theory (HRT)* zu füllen und ihre Erkenntnisse in die gegenwärtige Realität der kritischen Informationsinfrastrukturen zu überführen. Erik Hollnagel (2013) entwickelt mit seinem Konzept des *resilience engineering* eine Perspektive, mit der ein neuer Knoten geknüpft werden kann. Er setzt Resilienz in Zusammenhang mit der Leistung, die ein System erbringt, anstatt sich auf Qualitäten oder Eigenschaften zu beschränken. Das bedeutet, dass Resilienz hergestellt werden muss oder anders ausgedrückt eine Fähigkeit ist, die sich angeeignet werden kann. Bei Hollnagel setzt sich Resilienz aus vier Faktoren zusammen (Hollnagel 2013, S. 4 f.):

(1) Zu wissen, was zu tun ist; mit einem Repertoire an vorbereiteten oder situativen Maßnahmen auf Disruptionen reagieren. Die Fähigkeit, die aktuelle Lage zu adressieren.

(2) Zu wissen, nach was man Ausschau hält; ein Monitoring von System und Umwelt. Die Fähigkeit, das Kritische zu adressieren.
(3) Zu wissen, was passiert ist; aus den Erfahrungen von Fehlern und Erfolgen lernen. Die Fähigkeit, das Geschehene zu adressieren.
(4) Zu wissen, was zu erwarten ist; mögliche Entwicklungen, Bedrohungen und Chancen antizipieren. Die Fähigkeit, das Potenzial zu adressieren.

Die ersten beiden Faktoren lassen sich auf die Systembeschaffenheit bei Perrows 2x2 Matrix anwenden. So können Betreiber kritischer Informationsinfrastrukturen Maßnahmen vorab implementieren, um Komplexität zu entschärfen oder lose Kopplungen einzubauen. Mit einem Monitoring kritischer Komponenten und Prozesse in System und Umwelt der kritischen Informationsinfrastrukturen können auftretende Vulnerabilitäten und Rückkopplungsschleifen identifiziert werden. Die *High Reliability Theory* bietet einen ergänzenden Katalog zum ersten Faktor, den vorbereitenden sowie situativen Maßnahmen zur Systemkontrolle. Zudem finden sich in der Theorie aufschlussreiche Hinweise darüber, wie Organisationen für den dritten Faktor kontinuierlich die Entwicklung ihres Systems vorantreiben können (bspw. Fehlerkultur).

Auch der vierte Faktor der Antizipation findet sich in der HRT bereits in Form der Simulationen und der ständigen Erwartung, dass etwas Unerwartetes eintreten könnte. In der Literatur besteht darüber hinaus eine Idee davon, dass *high reliability organizations* bedeutsame Analogien explorieren, indem sie sich an den möglichen Chancen anderer Systeme orientieren. Karl Weick (1999, S. 54) führt hier das Beispiel von Flugzeugträgermannschaften an, die aus den Fehlern von Waldbrand bekämpfenden Feuerwehrmannschaften lernen, da diese ebenfalls kontinuierlich ihr Personal rotieren. Mit anderen Worten lernen sie von Organisationen in ihrer Umwelt, die mit ähnlichen strukturellen Herausforderungen zu kämpfen haben oder ähnliche Maßnahmen einsetzen. Dem Faktor der Antizipation schreibt Hollnagel einen gesonderten Stellenwert zu und macht ihn zu einem integralen Bestandteil von Resilienz: Antizipation ist die Grundlage für die Entwicklung neuer Reaktionsmuster, die über das hinausgehen, was man aus der Vergangenheit des eigenen Systems lernen kann. Sie hilft dabei das Monitoring zu fokussieren und ist essenziell für eine proaktive Langzeitstrategie, die wiederum unverzichtbar für den Erhalt eines jeden Systems ist. Die vier Faktoren beeinflussen sich gegenseitig, hängen voneinander ab und sollen ein System in die Lage versetzen, interne und externe Ereignisse zu adressieren. Letzten Endes könne nur das System kontrolliert werden, aber nicht die Umwelt (Hollnagel 2013, S. 5 ff.). Diese Beobachtung deckt sich mit der Dynamik der schwer zu antizipierenden und unkontrollierbaren Bedrohungen, mit denen sich die Cybersicherheit kritischer Informationsinfrastrukturen konfrontiert sieht.

Die drei diskutierten Theorien verdeutlichen die soziomaterielle Bedingtheit von Cybersicherheit in der Dynamik kritischer Informationsinfrastrukturen. Eine Synthese aus den Faktoren des *resilience engineering* mit den Konzepten der *Normal Accident Theory* und *High Reliability Theory* deutet vier übergeordnete Aspekte an, die eine resiliente Bewältigungsstrategie adressieren sollte:

(1) Systembeschaffenheit
(2) Systemkontrolle
(3) Systementwicklung
(4) Systemumwelt

Zu diesen vier Aspekten gehören (1) die Komplexität und Kopplung eines Systems, (2) das Monitoring und die getroffenen Maßnahmen im System, (3) die Fähigkeit der Organisation zu lernen und zu antizipieren sowie (4) die multi-organisationale Koordination im Umgang mit der Umwelt des Systems. Ist eine Organisation in der Lage, diese vier Aspekte zu adressieren und die in ihnen enthaltenen Konzepte adäquat umzusetzen, ist sie der Theorie nach besser positioniert, um die Vulnerabilitäten im System und die Bedrohungen aus der Umwelt zu bewältigen. Auf diese Weise werden Systeme in die Lage

versetzt, notwendige Operationen im Angesicht erwartbarer und unerwarteter Umstände aufrechtzuerhalten (Hollnagel 2013, S. 7). Wenn diese Konzeption der Resilienz eine mögliche Bewältigungsstrategie nahelegt, dann bleiben für den Betrieb kritischer Informationsinfrastrukturen dennoch zentrale Fragen offen: Welche Operationen sind es, die notwendigerweise aufrechterhalten werden müssen? Und ab wann sind diese Operationen resilient? Mit dem Blick auf die Bedeutsamkeit kritischer Informationsinfrastrukturen stellt sich die noch viel grundlegendere Frage: Welche Infrastrukturen müssen notwendigerweise bewahrt werden, um gesellschaftliche Routinen aufrechtzuerhalten?

Resilienz im Kontext von Erwartung und Ereignis

Die Antworten auf diese Fragen sind immer auch das Ergebnis von Erwartungshaltungen und Aushandlungsprozessen zwischen Betreibern kritischer Infrastrukturen, staatlicher Institutionen sowie der breiteren Öffentlichkeit. Staatliche Institutionen definieren kritische Infrastrukturen womöglich anders oder verfolgen eine andere Strategie als Betreiber. Genauso ist es vorstellbar, dass die Resilienz einer lokalen Bevölkerung im Angesicht eines Desasters unerwünscht ist, da sie im Konflikt mit Strategien anderer Organisationen oder staatlicher Institutionen steht (Krüger und Albris 2020). Selbst für die Betreiber ist Resilienz nicht immer eindeutig oder einheitlich besetzt. Resilienz steht bei ihnen in Relation zu anderen übergeordneten Zielen, wie Effizienz oder Rentabilität. An anderer Stelle integrieren sie ungeachtet dieser Ziele institutionelle Mythen ihrer Umwelt, um das Überleben ihrer eigenen Organisation sicherzustellen (Meyer und Rowan 1977). Schließlich können Betreiber, staatliche Institutionen oder die breitere Öffentlichkeit auch wertebasierte Erwartungen an den Betrieb oder die Regulierung kritischer Infrastrukturen herantragen, wie soziale Verträglichkeit oder Nachhaltigkeit. All diese Faktoren prägen die Definition von notwendigen Operationen und ihrer Resilienz.

Was also letztendlich zum Kern kritischer Infrastrukturen gezählt wird und wie dieser Kern resilient gemacht werden soll, ist weder gegeben noch eine feststehende Einheit. Martin Endreß und Benjamin Rampp bieten einen sozialkonstruktivistisch informierten Zugang, indem sie den resilienten Kern als etwas sehen, das durch Beobachtungseinheiten identifiziert wird. Sie fassen Resilienz als eine Form „transformativer Autogenese“ (Endreß und Rampp 2014, S. 93), bei der es sozialen Einheiten gelingt, Bedrohungen, Störungen und Krisen für den von ihnen identifizierten Kern zu bewältigen, indem sie intern ihre Identifikationsoptionen reorganisieren. Da der Kern überhaupt erst durch „(unterschiedlich ausgeprägte) Transformationsprozesse“ (Endreß und Rampp 2014, S. 94) bestimmt wird, zeichnet sich Resilienz nicht nur durch Beständigkeit aus, sondern auch durch die Fähigkeit zur Transformation. Resilienz bedeute „eben nicht die Bestandserhaltung eines Kerns trotz Transformation, sondern *gerade durch* Transformation“ (Endreß und Rampp 2014, S. 94, Hervorhebungen im Original). Dieser Umstand macht Resilienz zum Ergebnis von Grenzziehungsprozessen sozialer Akteurskonstellationen und eröffnet eine Perspektive auf Resilienz durch die Beobachtung von Erwartungskontinuitäten und -diskontinuitäten. Sobald es jedoch zu Disruptionen kommt, die den jeweiligen Erwartungshorizont des Vorstellbaren übersteigen, stellt sich die Frage, ob das Beobachtete noch einem transformierten Kern entspricht oder schon einem grundlegenden Wandel unterzogen wurde. Die Frage, um welche Form es sich handelt, ließe sich nur nach der Wandlung im spezifischen Fall beantworten (Endreß und Rampp 2014, S. 93 ff.).

Diese Perspektive lässt sich auf kritische Informationsinfrastrukturen anwenden. Auch in dieser Konstellation sind es soziale Akteure, die beobachten und identifizieren, was zu dem Kern ihrer Infrastrukturen gehört. Mit ihren Erwartungen ziehen sie die Grenze zwischen einem resilienten und nichtresilienten Kern. Die Grenzziehung lässt sich als das dynamische Ergebnis von Rückkopplungsschleifen verstehen. Sie sind das soziale Pendant zu den neuen und unerwarteten Rückkopplungsschleifen der

materiell komplexen Systembeschaffenheit. In diesen Schleifen wird der Kern kritischer Informationsinfrastrukturen und seine Resilienz kontinuierlich durch Erwartungs(dis-)kontinuitäten aus dem System und der Umwelt transformiert, um im Angesicht dieser Impulse ihren Fortbestand zu garantieren. Die Betreiber kritischer Infrastrukturen stellen ein soziales System dar, dessen interne Erwartungskonstellationen auf die externen Erwartungskonstellationen ihrer Umwelt (bspw. staatliche Institutionen, potenzielle Angreifer:innen, NGOs und die breitere Öffentlichkeit) treffen. Damit wird die Frage nach den Grenzen des Kerns kritischer (Informations-)Infrastrukturen und ihrer Resilienz auch eine empirische: Welche Transformationen durchlief der Kern, um fortzubestehen? Worauf geht diese Transformation zurück? Wie konstituierten soziomaterielle Aspekte Cybersicherheit in einem spezifischen Fall? Welche Aspekte erachten beteiligte oder betroffene Akteure gegenwärtig als konstitutiv für Resilienz, nachdem sie bereits eine Historie an Ereignissen und Transformationen durchlaufen haben?

Da die Art des Wandels und die Form des Kernbestands erst nach dem Eintritt eines Ereignisses nachvollziehbar werden, stellt sich auch die Frage: Welche Wirkmächtigkeit tragen die Ereignisse selbst an das System heran? Die zuvor dargelegten Herausforderungen im System und die Bedrohungen in der Umwelt machen deutlich, dass eine materiell drängende Dimension kritischer Informationsinfrastrukturen existiert, die über das hinaus geht, was die Summe aller sozialen Erwartungshaltungen vermuten lässt. Die Ereignisse, welche auf die kritischen Informationsinfrastrukturen treffen, entfalten ihre jeweils einzigartige Wirkmächtigkeit, welche sich aus soziomateriellen Faktoren zusammensetzt; sei es ein Schadprogramm, eine Hackergruppe, unachtsame Mitarbeiter:innen, ein Patch oder ein vulnerables Rechenzentrum. Das Ereignis sucht nach seinem Eintritt die Akteure im System heim und entfaltet so seine idiosynkratische Wirkung (Derrida 2003). Die Heimsuchung wirkt transformativ auf die Erwartungs(dis-)kontinuitäten und ihre systemischen Konstrukte, indem sie enthüllt, was nicht ausfallen darf, was kritisch ist, ob es standgehalten hat und ob es in den Augen der Beobachtenden resilient war.

Ausblick: Soziomaterielle Resilienz im Werden

Die Dynamik kritischer Informationsinfrastrukturen und ihrer Umwelt legen eine Strategie nahe, die betreibende Organisationen in die Lage versetzt, im Angesicht von erwarteten und unerwarteten Umständen, notwendige Operationen aufrechtzuerhalten. In einem schwer zu antizipierenden Umfeld aus Bedrohungen für die Cybersicherheit bietet sich daher die systemische Bewältigungsstrategie der Resilienz an. Organisationssoziologische Theorien und Ansätze aus dem Sicherheitsmanagement technischer Systeme verweisen für eine solche Strategie auf die soziomaterielle Bedingtheit von Cybersicherheit. Eine Synthese aus den Konzepten jener Theorien ermöglicht den Blick auf vier Aspekte der Resilienz: Systembeschaffenheit, -kontrolle, -entwicklung und -umwelt. Dementsprechend bedeutet eine resiliente Bewältigungsstrategie, Organisationen vorab in die Lage zu versetzen, die Tücken potenzieller Cyberattacken bestmöglich zu antizipieren, mit eng gekoppelter Komplexität in der Beschaffenheit umzugehen und sich ein Repertoire an Fähigkeiten anzueignen, mit denen das soziotechnische System kontrolliert und weiterentwickelt werden kann.

Die soziomateriellen Aspekte der Resilienz sind jedoch auch das Konstrukt multipler Erwartungs(dis-)kontinuitäten und sich wandelnder Grenzziehungsprozesse durch Beobachtende. Zudem werden die Akteure hinter dem Konstrukt von Ereignissen heimgesucht, die ihre idiosynkratischen Wirkungen im System entfalten. Folgt man einer konstruktivistischen Perspektive auf Resilienz, hätte dies eine Strategie zur Folge, die nur das nächste Ereignis abwartet, auf dessen Eintritt sie schnell reagiert, alle notwendigen Operationen wiederherstellt, ihre Lehren daraus zieht und immer wieder einen neuen oder alten Kern für resilient erklärt. Doch über die Erwartungshaltungen und wirkmächtigen Ereignisse

hinaus besteht eine soziomaterielle Bedingtheit und existenzielle Dringlichkeit in der Dynamik kritischer Informationsinfrastrukturen, die auch soziale Akteure bindet, welche Cybersicherheit herstellen wollen. Die vier Aspekte der Resilienz könnten eine Annäherung an eine systemische Bewältigungsstrategie darstellen, so lange beteiligte Akteure sich die Vermittlung sozialer Erwartungen bewusst machen. Demzufolge müssten sie gemeinsam eine Vorbereitung und Antizipation definieren, mit denen ihr jeweiliges System die Konsequenzen eines jedweden Ereignisses so unter Kontrolle bringt, dass sie ihre Erwartungen nach einer Systemtransformation erneut um eine stabile und geteilte Definition von resilienter Systembeschaffenheit formieren können.

Bestehende Debatten zum menschlich zentrierten Ansatz (Deibert 2018) und dem *social layer* (Gioe et al. 2019) können mit der Bewältigungsstrategie der Resilienz um eine Perspektive auf die soziomaterielle Organisation hinter Cybersicherheit ergänzt werden. Versteht man soziomaterielle Resilienz als eine Strategie im Werden, dann bietet sich mit dieser Perspektive auch ein empirischer Zugang. Die Konstitution des sonst so diffusen Konzepts der Resilienz kann in der Untersuchung verschiedener Systeme möglichst trennscharf nachvollzogen werden. In Anbetracht der existenziellen Herausforderung, die von kritischen Informationsinfrastrukturen ausgeht, sollte sich zukünftige Forschung mit den vorab definierten Kernbeständen von Systemen und deren Resilienz auseinandersetzen, um deren Transformationen nach wirkmächtigen Ereignissen nachzuvollziehen und so zu einem besseren Verständnis von dem gelangen, was resiliente Infrastruktur war, ist und sein kann.

Literatur

Bundesamt für Sicherheit in der Informationstechnik. 2022. Die Lage der IT-Sicherheit in Deutschland 2022. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf?__blob=publicationFile&v=6 (Zugegriffen: 27.1.2023).

Bundesamt für Sicherheit in der Informationstechnik. 2023. Zero-Day-Exploit. https://www.bsi.bund.de/SharedDocs/Glossareintraege/DE/Z/Zero-Day-Exploits.html?nn=132646 (Zugegriffen: 27.1.2023).

Deibert, Ronald J. 2018. Toward a Human-Centric Approach to Cybersecurity. *Ethics & International Affairs* 32(4):411–24. https://doi.org/10.1017/S0892679418000618.

Derrida, Jacques. 2003. *Eine gewisse unmögliche Möglichkeit, vom Ereignis zu sprechen*. Berlin: Merve Verlag.

Endreß, Martin, und Benjamin Rampp. 2014. Resilienz als Prozess transformativer Autogenese. Schritte zu einer soziologischen Theorie. *BEHEMOTH – A Journal on Civilisation* 7(2):73–102. https://doi.org/10.6094/BEHEMOTH.2014.7.2.834.

Gioe, David V., Michael S. Goodman, und Alicia Wanless. 2019. Rebalancing cybersecurity imperatives: patching the social layer. *Journal of Cyber Policy* 4(1):117–37. https://doi.org/10.1080/23738871.2019.1604780.

Henschke, Adam. 2021. Terrorism and the Internet of Things: Cyber-Terrorism as an Emergent Threat. In *Counter-Terrorism, Ethics and Technology*, Hrsg. Adam Henschke, Alastair Reed, Scott Robbins und Seumas Miller, 71–87. Advanced Sciences and Technologies for Security Applications. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-90221-6_5.

Hollnagel, Erik. 2013. Resilience Engineering and the Built Environment. *Building Research & Information* 42(2):1–8. https://doi.org/10.1080/09613218.2014.862607.

Hopkins, Andrew. 1999. The Limits of Normal Accident Theory. *Safety Science* 32(2–3):93–102. https://doi.org/10.1016/S0925-7535(99)00015-6.

Hughes, Thomas P. 1987. The Evolution of Large Technological Systems. In *The Social Construction of Technological Systems. New Directions in the Sociology and History of Technology,* Hrsg. Wiebe E. Bijker, Thomas P. Hughes und Trevor Pinch,51-82. Cambridge, Massachusetts & London, England: MIT Press,

Knop, Dirk. 2022. Versailler Krankenhaus muss nach Cyber-Angriff Patienten verlegen. *heise online*. https://www.heise.de/news/Franzoesisches-Krankenhaus-muss-nach-Cyber-Angriff-Patienten-verlegen-7367288.html (Zugegriffen: 27.1.2023).

Krüger, Marco, und Kristoffer Albris. 2020. Resilience Unwanted: Between Control and Cooperation in Disaster Response. *Security Dialogue* 52(4):343–60. https://doi.org/10.1177/0967010620952606.

La Porte, Todd M. 2006. Organizational Strategies for Complex System Resilience, Reliability, and Adaptation. In *Seeds of Disaster, Roots of Response*, Hrsg. Philip E. Auerswald, Lewis M. Branscomb, Todd M. LaPorte und Erwann O. Michel-Kerjan, 1. Aufl., 135–54. Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9780511509735.012.

La Porte, Todd R., und Paula Consolini. 1991. Working in Practice But Not in Theory: Theoretical Challenges of "High-Reliability Organizations". *Journal of Public Administration Research and Theory* 1(1):19–48, Januar. https://doi.org/10.1093/oxfordjournals.jpart.a037070.

Meyer, John W, und Brian Rowan. 1977. Institutionalized Organizations: Formal Structure as Myth and Ceremony. *American Journal of Sociology* 83(2):340–63.

Nachrichtendienst des Bundes. 2022. Sicherheit Schweiz 2022. https://www.newsd.admin.ch/newsd/message/attachments/72368.pdf (Zugegriffen: 27.1.2023).

Newman, Lily Hay. 2021. A Year After the SolarWinds Hack, Supply Chain Threats Still Loom. *Wired*. https://www.wired.com/story/solarwinds-hack-supply-chain-threats-improvements/ (Zugegriffen: 27.1.2023).

Perrow, Charles. 1987. Normale Katastrophen. Die unvermeidbaren Risiken der Großtechnik. In *Theorie und Gesellschaft*, Hrsg. Axel Honneth, Hans Joas und Claus Offe, übersetzt von Udo Rennert, Bd. 8. Frankfurt/Main; New York: Campus Verlag.

Petermann, Thomas, Harald Bradke, Arne Lüllmann, Maik Poetzsch und Ulrich Riehm. 2011. *Was bei einem Blackout geschieht. Folgen eines langandauernden und großflächigen Stromausfalls.* Bd. 33. Studien des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag. Nomos Verlag, Berlin. http://www.tab-beim-bundestag.de/de/pdf/publikationen/buecher/petermann-etal-2011-141.pdf (Zugegriffen: 27.1.2023).

Stöcker, Christian. 2010. Angriff auf Irans Atomprogramm: Stuxnet-Virus könnte tausend Uran-Zentrifugen zerstört haben. *Der Spiegel* 26. Dezember 2010, Abschn. Netzwelt. https://www.spiegel.de/netzwelt/netzpolitik/angriff-auf-irans-atomprogramm-stuxnet-virus-koennte-tausend-uran-zentrifugen-zerstoert-haben-a-736604.html (Zugegriffen: 27.1.2023).

Weick, Karl E. 2004. Normal Accident Theory as Frame, Link, and Provocation. *Organization & Environment* 17(1):27–31. https://doi.org/10.1177/1086026603262031.

Weick, Karl E., Kathleen M. Sutcliffe und David Obstfeld. 1999. Organizing for high reliability: Processes of collective mindfulness. In *Research in Organizational Behavior,* Hrsg. R. I. Sutton & B. M. Staw, Vol. 21, 81–123. US: Elsevier Science/JAI Press.

Zetter, Kim. 2016. Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. *Wired*. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.