10 Resiliente kritische und sensible Infrastrukturen im Kontext moderner Kommunikationssysteme

Kai Börner, Dimitar Kroushkov, Jan-Ole Malchow

Moderne Informations- und Kommunikationstechnologien (IKT) sind das zentrale Nervensystem weltweiter Wirtschaftskreisläufe, des gesellschaftlichen Zusammenlebens und staatlichen Handelns. Sie sind einerseits eine Errungenschaft, ohne die wir unser Leben nicht so führen könnten, wie wir es kennen. Andererseits können schon kleinste Störungen in den unzähligen mit IKT hochgradig vernetzten Systemen ernsthafte Probleme bereiten. Wie also lassen sich vernetzte Systeme, bei deren Ausfall die Gefahr von Versorgungsengpässen oder Störungen der öffentlichen Sicherheit bestehen, resilient machen?

Im Zuge der voranschreitenden Digitalisierung haben die Produkte und Dienstleistungen der Informations- und Kommunikationstechnologien (IKT) unser alltägliches Leben erleichtert und neue Chancen für Volkswirtschaften und Gesellschaften weltweit eröffnet. Moderne IKT sind das Fundament der Globalisierung und bergen die Möglichkeit, die digitale Kluft (engl. „Digital Devide") weltweit zu überwinden und so wesentlich zur Erreichung der 17 Nachhaltigkeitsziele der UN beizutragen. Hier geht es insbesondere darum, mit IKT zur Umsetzung des neunten Nachhaltigkeitsziels beizutragen: also eine belastbare Infrastruktur aufzubauen, eine integrative und nachhaltige Industrialisierung zu fördern sowie Innovationen zu unterstützen.

Effiziente und erschwingliche IKT-Infrastrukturen und -Dienste ermöglichen es allen Ländern weltweit zugleich, an der digitalen Wirtschaft teilzunehmen und ihren wirtschaftlichen Wohlstand und ihre Wettbewerbsfähigkeit zu steigern. Tatsächlich verzeichnen die meisten Entwicklungsländer schon beeindruckende Fortschritte in Richtung des neunten Nachhaltigkeitsziels mit positiven Auswirkungen in den Bereichen finanzielle Inklusion, Armutsbekämpfung und verbesserte Gesundheit.

Gleichzeitig erhöht sich jedoch auch die Abhängigkeit von den Informations- und Kommunikationstechnologien. Bereits geringe Schwankungen in der Leistungscharakteristik können in aktuellen, hochgradig vernetzten Systemen großflächig Probleme auslösen. Systemausfälle können das öffentliche Leben massiv behindern, immense wirtschaftliche Schäden verursachen und sogar Menschenleben kosten. Beispielsweise hat der Ausfall von Systemen im öffentlichen Personennahverkehr Auswirkungen auf zehntausende oder hunderttausende Menschen, der Ausfall von

V. Wittphal, *Resilienz*, https://doi.org/10.1007/978-3-662-66057-7_10

sozialen Netzwerken verursacht in wenigen Stunden wirtschaftliche Verluste in Milliardenhöhe, und der Ausfall der Kommunikation im Rettungswesen kostet im Zweifel Menschenleben. Diese Systeme werden als kritische Infrastruktur (KRITIS) bezeichnet.

Kritische Infrastrukturen

Aufgrund der fatalen Folgen von Störungen und Ausfällen müssen Systeme der kritischen Infrastruktur (KRITIS) so gestaltet sein, dass sie trotz vielfältiger Störungsmöglichkeiten – von veränderten Umweltbedingungen, über den Ausfall von Teilsystemen bis hin zu böswilligen Manipulationen – einen geordneten Betrieb aufrechterhalten können. Sie müssen also resilient sein. Begriffe wie „System" und „Infrastruktur" vermitteln leicht den Eindruck, dass Resilienz ein rein technisches Thema sei. Dies ist jedoch keineswegs der Fall. Resilienz ist letztlich immer nur in einem größeren Zusammenhang zu erreichen, das heißt es gilt, technische, organisatorische und auch gesellschaftliche Rahmenbedingungen zu berücksichtigen und in Einklang zu bringen. Besonders im Fokus für die Resilienz von KRITIS werden aktuelle und zukünftige Funktechnologien wie 5G und 6G stehen sowie IT-Sicherheit als wesentlicher Baustein resilienter, vernetzter, digitaler Systeme.

Kritische Infrastrukturen (Roßnagel et al. 2019) sind nicht in einer zentralen Rechtsnorm definiert, sondern in vielen verschiedenen Gesetzen und Verordnungen. Es handelt sich grundsätzlich um Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung bedrohliche Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. In Deutschland wurden erste Schritte in Richtung Regulierung kritischer Infrastrukturen im Jahr 2008 unternommen, und zwar mit der „Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern" sowie mit dem Raumordnungsgesetz (ROG).

Der eigentliche Grundstein der KRITIS-Regulierung ist dann 2015 das „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)", welches im Jahr 2021 durch das „Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0)" aktualisiert wurde. Diese beiden Gesetze ändern verschiedene weitere Gesetze, insbesondere das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG), auf welchem wiederum die „Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV)" basiert. Diese Verordnung definiert die folgenden KRITIS Sektoren: Energie, Wasser, Ernährung, Informationstechnik und Telekommunikation, Gesundheit, Finanz- und Versicherungswesen sowie Transport und Verkehr. Durch das IT-Sicherheitsgesetz 2.0 kommen noch die Sektoren „Entsorgung" sowie „Unternehmen im besonderen öffentlichen Interesse" hinzu.

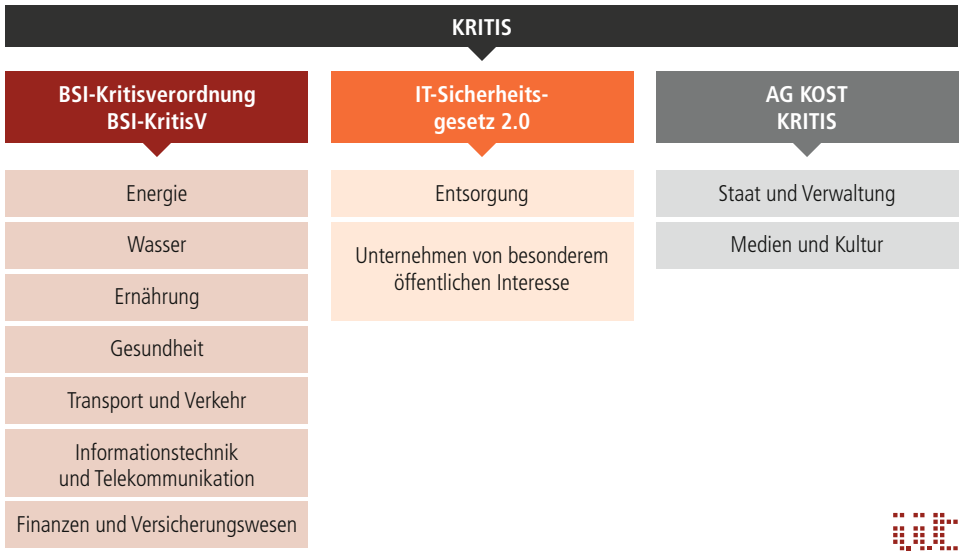

Abb. 10.1 Erweiterte KRITIS-Definition durch drei verschiedene Stellen. (Quelle: Institut für Innovation und Technik (iit), eigene Darstellung)

Dieser schon umfangreiche Katalog wird von der Bund-Länder Arbeitsgruppe für den Schutz Kritischer Infrastrukturen (AG KOST KRITIS) noch um zwei weitere Sektoren ergänzt, und zwar „Staat und Verwaltung" sowie „Medien und Kultur". So sind aktuell zehn KRITIS-Sektoren mit 29 Branchen definiert. Beispielhaft teilt sich Informations- und Kommunikationstechnologie in die Branchen Telekommunikation und Informationstechnik mit den kritischen Dienstleistungen Sprach- und Datenübertragung sowie Datenspeicherung und -verarbeitung. Hinzu kommen noch „Unternehmen im besonderen öffentlichen Interesse", beispielsweise Hersteller von Rüstungsgütern und IT-Produkten für staatliche Verschlusssachen (VS), Unternehmen mit besonderer volkswirtschaftlicher Bedeutung sowie weitere Unternehmen im Bereich Gefahrstoffe, die noch nicht anderweitig von KRITIS erfasst sind (Abb. 10.1).

Über diese klaren KRITIS-Zuordnungen hinausgehend, gilt es, „sensible" Infrastrukturen bei resilienzsteigernden Maßnahmen zu berücksichtigen. Denn aufgrund der weiter fortschreitenden und allumfänglichen Vernetzung entstehen faktisch anfällige Gesamtsysteme in nahezu allen Bereichen, die von der strengen KRITIS-Definition bisher nicht erfasst werden. Teilweise entstehen diese Anfälligkeiten auch aufgrund von komplexen, international verwobenen Abhängigkeiten, die zum einen kaum nachvollziehbar sind und die zum anderen nicht unter die deutsche Regulierung fallen. So waren im Jahr 2021 bis zu 1.500 Unternehmen weltweit von einem

Ransomware Angriff auf einen US-amerikanischen Dienstleister betroffen (Spiegel 2021b) – in Schweden etwa das Kassensystem einer namenhaften Supermarktkette (Schirrmacher 2021).

Unterdessen bilden sich ähnliche Abhängigkeiten in zahlreichen weiteren gesellschaftlichen und technischen Bereichen heraus wie Arztpraxen, Schulen, privaten Energieerzeugungsanlagen oder Fahrzeugen, die über das Internet vernetzt sind. Umfangreiche und enge Verflechtungen zwischen Sektoren und Branchen werden vermutlich auch künftig zunehmen – und damit weitere Abhängigkeiten entstehen. So sind beispielsweise alle Sektoren auf den Energiesektor angewiesen, und in der modernen Digitalgesellschaft ist praktisch nichts mehr ohne IKT funktionsfähig. Hier einige Beispiele für die durch zunehmende Vernetzung hervorgerufenen Veränderungen in den Sektoren Energie, Ernährung, Finanz- und Versicherungswesen, Gesundheit, Informationstechnik und Telekommunikation, Medien und Kultur, Staat und Verwaltung, Transport und Verkehr sowie Wasser (siehe auch Tab. 10.1):

Energie

Das Stromnetz wurde über lange Zeit durch die Netzfrequenz von 50 Hz synchronisiert. Jeder Netzteilnehmer verfügte über die gleiche aktuelle Information über den Netzzustand. Leichte Schwankungen der Frequenz im Netz wurden allein durch bewegte Massen im Netz physikalisch kompensiert und größere Schwankungen z. B. durch Lastabwürfe ausgeglichen. Grundlegende Veränderungen in der Netzinfrastruktur, insbesondere im Zuge der Veränderung der Energieerzeugung – weg von wenigen zentralen Kraftwerken, hin zu vielen verteilten Erzeugern – setzen andere Steuerungsmechanismen voraus. Eine parallele digitale Kommunikationsinfrastruktur wird künftig das Energienetz steuern und somit für dessen Resilienz entscheidend sein. Fällt diese Kommunikationsinfrastruktur einmal aus, ist das Netz nicht mehr regelbar und im schlimmsten Fall bleibt nur eine großflächige Abschaltung.

Auch wird das Netz mit seinen digital strukturierten Steuermechanismen anfälliger für gezielte Angriffe. Während es unmöglich war, die Netzfrequenz zu manipulieren und so fehlerhafte Reaktionen hervorzurufen, ist dies bei digitalen Kommunikationsinfrastrukturen nicht nur grundsätzlich möglich, sondern bei geringer Qualität der entsprechenden elektronischen Bauteile sogar relativ einfach. So konnten zum Beispiel im Februar 2022 tausende Windräder nicht kontrolliert werden, weil ein Satellitennetzwerk ausgefallen war (Wilkens 2022). Da die betroffenen Anlagen aus guten Gründen über Mechanismen zur Selbstregulierung verfügen, folgte in diesem Fall kein direkter Ausfall. Der Vorfall macht jedoch deutlich, dass diese neuen Energieinfrastrukturen verwundbar sind und das gezielte Angriffe auf deren digitale Kommunikation drastische Auswirkungen haben können. Wie im Fall der ausgefallenen Supermarktkassen zeigt sich auch hier eine Kette von Abhängigkeiten. Der ursäch-

lich die Störung verursachende Satellit wird vom US-amerikanischen Unternehmen Viasat Inc. betrieben. Der Dienstleister EuroSkyPark in Saarbrücken nutzt ihn, um Verbindungen für industrielle Anlagen anzubieten. Diesen Verbindungsservice wiederum nutzt der Windanlagenhersteller Enercon zur Wartung der Anlagen bei seinen Kunden, den Betreibern von Windenergieanlagen. Der Fall macht exemplarisch deutlich, dass Resilienz neben technischer Funktionstüchtigkeit immer stärker auf organisatorischen Faktoren beruht. In komplexen Abhängigkeitsverhältnissen muss der Ausfall eines Kettengliedes bei Resilienz-Betrachtungen mitberücksichtigt werden.

Herausforderung: *Komplexe Abhängigkeitsverhältnisse in vernetzten Systemen, insbesondere auch grenzüberschreitend.*

Ernährung

Im Wirtschaftssektor Ernährung sind Lebensmittelproduktion, Lebensmittelverarbeitung und Lebensmittelhandel kritische Glieder einer Lieferkette von der Produktion bis zum Endverbraucher, woraus sich unter anderem starke Abhängigkeiten zum Sektor Transport und Verkehr ergeben. Hier sind alle Fragen der Mobilitätswende relevant sowie die digitale Vernetzung auf allen Ebenen – vom kleinsten an einem Produkt angebrachten RFID-Chip über vernetztes Fahren bis hin zu Systemen der internationalen Logistiksteuerung. Sämtliche dieser vielfach interagierenden Systeme müssen resilient und sicher gestaltet werden, um eine Versorgung mit Lebensmitteln unter allen Umständen sicherzustellen.

Zusätzlich zu diesen eher technischen Anforderungen sind Veränderungen im Verbraucherverhalten sowie damit einhergehende zusätzliche Anforderungen und Regulierungen für Resilienz relevant. Beispielsweise wird der Nachweis von Produktionsbedingungen und die Herkunft von Lebensmitteln immer wichtiger. Zudem soll die Produktion effizienter werden. All dies bedeutet, dass nachhaltige Land- und Ernährungswirtschaft künftig auf digitale vernetzte Dienste angewiesen sein wird. Tatsächlich erprobt und nutzt die moderne Landwirtschaft schon heute Campusnetze, also vernetzte Dienste abseits der öffentlichen Mobilfunkinfrastruktur, wobei inzwischen der Grad der Vernetzung und Digitalisierung schon sehr hoch ist (Kirchner 2022). Bereits heute werden Nachweise hinsichtlich Produktherkunft gefordert wie bei Fleisch vorgeschrieben: ein Steak kann bis zur einzelnen Kuh zurückverfolgt werden. Diese Nachweise stärken einerseits das Vertrauen von Verbrauchern und sind andererseits unerlässlich, um etwa Verunreinigungen schnell aufklären zu können. Im Sinne von Resilienz spielt hierbei die Sicherheit dieser Informationsketten, insbesondere die Authentizität der Daten eine große Rolle.

Herausforderung: *Sicherung der Authentizität von Daten entlang von Kommunikationsketten*

Finanz- und Versicherungswesen, Gesundheit

Stationäre und mobile Bezahlsysteme sind heute untrennbar über Kommunikationssysteme verbunden. Hygieneregeln und Kontaktbeschränkungen im Verlauf der Covid-19-Pandemie haben eine enorme Steigerung kontakt- und bargeldloser Zahlungen auch im stationären Handel induziert. Die Abhängigkeit von digitalen Zahlungsinfrastrukturen, auch im Alltag, steigt spürbar und stetig, und dafür werden zwingend verfügbare, ausfallsichere und vertrauenswürdige Kommunikationssysteme und IT-Infrastrukturen benötigt. Diese Kommunikationssysteme und IT-Infrastrukturen müssen als Gesamtsystem – von den Datenübertragungsnetzen über Datenverarbeitungszentren und Terminals bis hin zu den Endgeräten – resilient sein. Unvorhergesehene Störungen entlang der Kette können zu tagelangen Ausfällen führen (Spiegel 2022a), die in der modernen Digitalgesellschaft nicht hinnehmbar sind. In der zunehmend vernetzten Welt, in der moderne Kommunikationssysteme in der Lage sind, sich quasi in Echtzeit auszutauschen, stützt sich das digitale Wirtschaftsleben auf innovative Finanzdienstleistungen und beschleunigte Prozesse bei der Abwicklung des Zahlungsverkehrs. Das kann auch für deutsche Internetunternehmen und innovative Start-ups neue Marktchancen bedeuten (Born 2022). Diese neuen Ökosysteme sind auf verlässliche Kommunikations- und IT-Infrastruktur angewiesen und werden sich nur dann etablieren, wenn Resilienz für die Prozesse gewährleistet werden kann, einen theoretisch möglichen, fortlaufenden Betrieb auch in die Praxis umzusetzen.

Im Gesundheitssektor werden sich künftige vernetzte Plattformdienste ausbreiten: Medizinische Einrichtungen und Bürgerinnen und Bürger partizipieren so an der Digitalisierung im Gesundheitswesen und erhalten einen Mehrwert über die Nutzungsmöglichkeit digitaler Angebote. Die Anzahl der Applikationen wächst stetig (gematik GmbH 2021). Allerdings ist ein möglicher Ausfall der Kommunikationsinfrastruktur ein Risiko, das in diesem sensiblen Bereich nicht hinnehmbar ist. Bereits der Ausfall einfacher Anwendungen wie eines elektronischen Rezepts kann für Patienten schwerwiegende Folgen haben, etwa wenn sie ein dringend benötigtes Medikament nicht rechtzeitig erhalten. Auch hier gilt: Sichere Erfassung, sicherer Austausch, sichere Speicherung, sichere Verarbeitung und die Verfügbarkeit der besonders schützenswerten und wichtigen Daten ist nur mit Hilfe resilienter digitaler Infrastrukturen realisierbar. Monitoring von Vitaldaten und die Versorgung von Patienten aus der Ferne oder medizinische und soziale Robotik sind nur einige Beispiele künftiger Gesundheitsdienste, die die Verfügbarkeit sicherer, robuster, zuverlässiger und schneller Netzinfrastrukturen voraussetzen (Fettweis, et al. 2017).

Herausforderung: *Verlässlichkeit und Verfügbarkeit von Kommunikationssystemen*

Informationstechnik und Telekommunikation

Informations- und Kommunikationstechnologien sind der Schlüssel zu einer allvernetzten Umgebung der Zukunft. Allerdings gilt es auf den Weg dahin, noch wesentliche Herausforderungen zu lösen. Dazu zählt die Aufrechterhaltung von Netzinfrastrukturen und IT-Diensten in Krisen und bei Katastrophen. Geopolitische Entwicklungen und Verwerfungen beeinflussen ebenfalls die Entwicklung der IKT. Staat und Wirtschaft müssen die (IT-)Sicherheit, (Hersteller-)Abhängigkeiten und die Lieferkettenstrukturen für Netztechnik und verteilte Rechen- und Clouddienste unter Abwägung möglicher Risiken gründlich überdenken. Dabei geht es um die zugrundeliegende Software und Hardware ebenso wie um strategische Partnerschaften, die eingegangen worden sind oder eingegangen werden sollen.

Zu modernen Kommunikationsnetzen zählen die Weitverkehrsnetze, weltumspannende Satellitennetze, öffentliche und private Mobilfunknetze und örtliche Netze. Die selbstbestimmte Entwicklung künftiger Kommunikationstechnologien wie der Mobilfunk der sechsten Generation (6G) erweist sich als eine tragende Säule für Resilienz. Eine Konsequenz aus dieser Erkenntnis ist, dass es für die Entwicklung und den Aufbau vertrauenswürdiger Netz- und Dateninfrastrukturen notwendig ist, Know-how zu haben, um Anforderungen an Netzkomponenten formulieren und Netze souverän und sicher betreiben zu können. Dazu müssen Schlüsselkomponenten aus eigener Produktion („made in Europe“) oder aus vertrauenswürdigen Quellen stammen.

Herausforderung: *Kommunikationsinfrastrukturen müssen technisch von Grund auf resilient und sicher konzipiert und umgesetzt werden.*

Medien und Kultur

Neben den teils sehr stark technisch geprägten Aspekten hat die zunehmende Vernetzung auch eine starke gesellschaftliche Komponente. Deutlich wird dies zum Beispiel in tiefgreifenden Veränderungen des Arbeitslebens. Befördert durch die Corona-Krise wurden Möglichkeiten des auf Vernetzung beruhenden Arbeitens im Homeoffice drastisch ausgeweitet, und es wird erwartet, dass diese Veränderungen auch nach dem Ende der eigentlichen Krise fortbestehen werden (Peters 2022). Eine weitere besonders relevante Veränderung auf Grundlage neuer Informations- und Kommunikationstechniken erfährt zurzeit die Medienkultur. Es ist nicht auszuschließen, dass die IKT Entwicklungen befördert, die zu kulturellen Zerwürfnissen und politischen Zerreißproben führen, die die Demokratie gefährden können und im schlimmsten Fall Krieg und Gewalt heraufbeschwören. Der unmittelbare, gezielte und direkte Zugang zu Zielgruppen – letztlich zu jedem Einzelnen individuell – macht es vor dem Hintergrund nur noch niederschwellig vorhandener technischer Barrieren möglich, mit relativ geringem Aufwand teils große Wirkung zu erzielen.

Viele soziale Netzwerke bieten zum Beispiel die Möglichkeit, Werbung gezielt zu platzieren – ein Umstand, der auch für politische Zwecke im Umfeld von Wahlen genutzt wird. Derart gezielte Wahlwerbung war in der Vergangenheit unmöglich. (Roßnagel et al. 2019). Neben den technischen Möglichkeiten, sehr viele Menschen sehr schnell und günstig zu erreichen, hat sich auch der Umgang mit den Medien an sich verändert. Gelogen wurde, gerade in der politischen Kommunikation, zwar schon immer (Marschall 2017), aber Art und Frequenz haben sich verändert. Heute ist es häufig ausreichend, eine Verunsicherung zu erzeugen. Gesellschaftliche und politische Strukturen werden also durch neue digitale Systeme, insbesondere durch die umfassende Vernetzung, laufend herausgefordert. Freie, unabhängige Medien sowie Meinungs- und Redefreiheit sind Grundpfeiler funktionierender demokratischer Gesellschaften. Gleichwohl ist inzwischen klar, dass eine völlig unkontrollierte Verbreitung von Informationen gleichfalls eine Bedrohung für demokratische Gesellschaften ist. Ein Dilemma, für dessen Auflösung im Rahmen eines gesellschaftlichen Dialoges und unter Berücksichtigung technischer Möglichkeiten, dringend ein Mediations- und Aushandlungsprozess einzurichten ist.

Herausforderung: *Nichttechnische Dimensionen von Resilienz müssen in einem breiten gesellschaftlichen Dialog erörtert und ausgehandelt werden.*

Staat und Verwaltung

Für Staat und Verwaltung sind im digitalen Zeitalter eine resiliente Kommunikationsinfrastruktur gleichsam das Fundament für die Sicherstellung der Funktionsfähigkeit von Legislative, Exekutive und Judikative. Insbesondere bei Katastrophenereignissen rettet die überall und jederzeit verfügbare Kommunikationsinfrastruktur des Notfall- und Rettungswesens Leben. Moderne Katastrophenfrühwarnsysteme für die Bevölkerung nutzen interaktive Applikationen für mobile Endgeräte (BBK o. J.). Rein App-basierte Warnsysteme für die Bevölkerung stoßen allerdings rasch an ihre Grenzen, wenn Datendienste über Mobilfunknetze nicht verfügbar sind oder der Verbreitungsanteil der Applikationen auf den Endgeräten die kritische Schwelle nicht erreicht hat. Zur Resilienz gehört auch die technische Möglichkeit, textbasierte Nachrichten über Cell Broadcast (Spiegel 2022b) zu versenden, um im Katastrophenfall die Bevölkerung effektiv zu warnen. Die Notwendigkeit resilienter digitaler Systeme ist im Cloudzeitalter gegeben, auch ohne extreme Szenarien von (Natur-)Katastrophen heranziehen zu müssen: Schon ein isolierter Brand in einem Datenzentrum ist ausreichend, um die Verfügbarkeit von Webdiensten bei betroffenen Kommunen massiv einzuschränken (Spiegel 2021a).

Demokratische Wahlen sind die Grundlage für das Funktionieren des Staates in Deutschland. Doch auch der eigentliche Akt der Wahl ist nicht davor gefeit, von fehlerhafter IKT und Vernetzung betroffen zu sein. So wurden bereits verschiedent-

lich, auch in Deutschland, Wahlen „online“ durchgeführt. Im Jahr 2009 hat das Bundesverfassungsgericht „In den Verfahren über die Wahlprüfungsbeschwerden“ dazu zwei Leitsätze verfasst. Hieraus ergibt sich, dass Wahlen grundsätzlich „online“ durchgeführt werden können, jedoch bestimmte Anforderungen erfüllt sein müssen. Es muss also die Resilienz des eigentlichen Wahlvorgangs gewährleistet sein.

Es gibt zahlreiche Argumente dafür, warum „online“ durchgeführte Wahlen erstrebenswert sind. Angeführt wird zum Beispiel eine drastische Zeitersparnis bei den Wählenden. Auf der anderen Seite ist es aktuell nicht möglich, digitale System hinreichend abzusichern. Auch wenn dies möglich wäre, ist es äußerst fraglich, ob der zweite vom BVG definierte Grundsatz eingehalten werden könnte. Somit besteht also durchaus die Möglichkeit, dass im Sinne eines resilienten Systems, die Urnenwahl dauerhaft die optimale Lösung bleiben wird. Ein wesentlicher Grundsatz für Resilienz ist es, jeweils die „passenden“ Technologien und Organisationsformen einzusetzen. Modern erscheinende Technologien und aktuelle Trends sind im Sinne von Resilienz nicht immer die besten Lösungen.

Herausforderung: *Wahl der adäquaten Technologien und Organisationsformen unabhängig von Trends.*

Transport und Verkehr

Verkehrsleitsysteme sind bereits seit langem vernetzt – jedermann kennt zum Beispiel die steuerbaren Geschwindigkeitsschilder im Straßenverkehr. Etwas weniger bekannt sind die Systeme zur Vorrangsteuerung für Rettungsfahrzeuge oder des ÖPNV an Ampeln. Im Zuge voranschreitender Digitalisierung schließt diese Vernetzung zunehmend nicht nur die Infrastruktur, sondern auch Fahrzeuge ein. Bis 2023 werden knapp 780 Millionen vernetzte Fahrzeuge erwartet (Tyborski 2019). Allerdings wurden bereits 2015 Jeep-Fahrzeuge über das vernetzte Entertainmentsystem gehackt. Rund 1,4 Millionen dieser Pkw mussten für ein Update zurückgerufen werden (Villasenor 2015). Doch nicht nur der Verkehr auf der Straße, auch Schiffe erweisen sich als extrem verwundbar. Berichte sprechen von einem gehackten Schiff pro Tag (Osler 2021). Und bereits seit 2015 ist öffentlich bekannt, dass Bahnen und ihre Steuerungssysteme verwundbar sind (Drozhzhin 2015). Dies alles unterstreicht, wie verletzlich die kritische Verkehrsinfrastruktur heute ist. Gleichzeitig werden Pkw immer häufiger vernetzt. Die dabei entstehenden Abhängigkeiten gehen deutlich über klassische Sicherheitsprobleme hinaus. So konnten im Jahr 2021 die Türen von Tesla Fahrzeugen nicht geöffnet werden, weil es ein Netzwerkproblem gab (The Guardian 2021).

Autonom vernetzter Verkehr und die Logistik der Zukunft können nur mithilfe resilienter Kommunikationsinfrastruktur realisiert werden, denn die zukünftige Mobilität

wird wesentlich durch unbemannte Fahrzeuge zu Wasser, in der Luft, auf der Straße und auf der Schiene geprägt sein. Insbesondere für die Netzabdeckung auf dem Meer oder in der Luft gilt es, neue Wege für eine verlässliche Konnektivität zu finden. Fliegende Netzzugangsknoten, die Integration von Satellitennetzen, aber auch die Bereitstellung von KI- und Rechendiensten in der Edge-Cloud lauten einige der erkennbaren Herausforderungen.

Herausforderung: *Zuverlässige Kommunikation auch abseits öffentlicher Mobilfunkinfrastruktur, um Betriebssicherheit zu gewährleisten.*

Wasser

Eine vermeintlich „analoge" und damit sichere Infrastruktur wie die Wasserversorgung ist im Zeitalter allumfassender Vernetzung ebenfalls nicht per se ungefährdet. Der Hackerangriff auf ein Trinkwasserwerk in Florida und der damit gestartete – jedoch zum Glück vereitelte – Manipulationsversuch der Säureregulierung mit potenziell gesundheitsschädigenden und lebensbedrohlichen Folgen zeigt, wie fragil Versorgungsinfrastrukturen in einer immer komplexeren digitalisierten Gesellschaft und Wirtschaft sind (Sokolov 2021). Die beschriebene Attacke kann sich in ähnlicher oder abgewandelter Form theoretisch überall auf der Welt wieder ereignen, wenn nicht entsprechende Vorkehrungen getroffen werden. Terroristen könnten bei der Planung von Sabotageaktionen vernetzte Industrieanlagen jeglicher Art ins Visier nehmen, mit entsprechend verheerenden Folgen für Mensch und Umwelt. Die Wasserwirtschaft steht hier stellvertretend für viele Branchen, in denen es gegenwärtig um den Wechsel von isolierten, analogen Systemen hin zu vernetzten, digitalen Systemen geht. Im Zuge der Umstellung müssen bestehende Systeme angepasst werden, aber auch organisatorische Maßnahmen und Verfahrensabläufe teils völlig neu gedacht und geplant werden.

Herausforderung: *Migration zu vernetzten Anlagen unter Berücksichtigung der Anforderungen der IT-Sicherheit.*

Resilienz in vernetzten Systemen

Eine einfache Lösung zum Erreichen von Resilienz ist es, Systeme redundant auszulegen, sodass beim Ausfall einer Komponente nahtlos auf eine Reserve umgeschaltet werden kann. Dieses Vorgehen ist wohlbekannt und wird in kritischen Systemen seit langem praktiziert. Aufgrund umfangreicher Digitalisierung und Vernetzung sind inzwischen jedoch so viele System kritisch, dass eine vollständig redundante Auslegung kaum mehr möglich ist, oder zumindest sehr teuer wäre. Es sind also neue Konzepte, Methoden und Werkzeuge gefragt. Es geht darum, Resilienz mit modernen technischen Lösungen zu erreichen – bloß wie? Resiliente Systeme müssen zu-

nächst als solche geplant sein. Dies bedeutet insbesondere, dass die Organisation der Arbeitsabläufe im Zusammenhang mit dem System entsprechend geplant und auch einzuüben ist. Diese Prozessorganisation ist vom Einzelfall abhängig und muss individuell analysiert und geplant werden. Allerdings gibt es einige Aspekte, die es immer zu berücksichtigen gilt. Dies betrifft die Wartung, Reparatur oder Austausch defekter Komponenten. Auch wenn das System die Störung auffangen und die Leistungscharakteristik automatisch gewährleisten kann, muss die Ursache der Störung behoben werden. Weiterhin sind Prozesse zu etablieren, welche einen Wiederanlauf des Systems nach einem Totalausfall ermöglichen. Hierzu zählen Maßnahmen wie das Erstellen von Backups und die Kenntnis darüber, wie ein Prozess wiederhergestellt werden kann. Aber gegebenenfalls auch Dinge wie eine definierte Einschaltreihenfolge. Diese Planung muss vorgehalten, angepasst und in den Prozessen regelmäßig geübt werden. Kurzum: Resiliente Systeme müssen auf allen Ebenen technisch und organisatorisch resilient geplant werden.

Wie moderne Kommunikationssysteme zu Bausteinen resilienter Systeme werden

Resilienz in vernetzten digitalen Systemen hängt maßgeblich von sicheren und vertrauenswürdigen Kommunikationstechnologien ab. Heutige Kommunikationssysteme erfüllen zwar essenzielle Funktionen in der digitalen Gesellschaft und Wirtschaft. Sie sind jedoch nicht durchgängig darauf ausgelegt, mit unbekannten und unvorhersehbaren netzinternen wie auch netzexternen Störereignissen umzugehen (Fettweis, et al. 2017). Die umfassende Vernetzung ist ein Erfordernis für mehr Effizienz und Automatisierung in der industriellen Produktion, erzeugt aber zugleich die Notwendigkeit von Resilienz. Denn mutwillige (Ermert und Briegleb 2022) oder nachlässige menschliche Eingriffe wie auch Katastrophen, verursacht durch Naturgewalten oder Kriege, können die Kommunikationsnetze und alle damit verbundenen Dienste empfindlich stören. In alltäglichen Nutzungsszenarien wie dem Videostreaming oder dem Masseging ist eine temporär eingeschränkte Verfügbarkeit ärgerlich. In Katastrophenfällen hingegen kann die Verfügbarkeit oder Nichtverfügbarkeit von Kommunikationsnetzen über Leben und Tod entscheiden. Eine grundlegende Anforderung bei der Entwicklung künftiger Kommunikationssysteme wie dem kommenden Mobilfunkstandard 6G besteht deshalb darin, die Fähigkeit zur Regeneration oder Selbstheilung des Netzes bereits in der Netzarchitektur und der verwendeten Komponenten und Netzsoftware zu verankern (The 5G Infrastructure Association 2021) – knapp zusammengefasst unter dem Begriff Resilience-by-Design. Die Resilienz beinhaltet technologische Entwicklungen bei der Netzinfrastrukturentwicklung, bei den Transport- und Funkzugangsnetzen, sowie bei der Cloudinfrastruktur (Fettweis et al. 2017).

Der Einsatz von Technologien wie Künstliche Intelligenz (KI), Quantenkommunikation oder Konzepten wie Open RAN, der offenen Auslegung von Funkzugangsnetzen mit

interoperablen Komponenten verschiedener Hersteller zur Diversifizierung der eingesetzten Netzkomponenten beim 5G Mobilfunk, könnten bei der Weiterentwicklung zukünftiger resilienter Kommunikationssysteme eine Rolle spielen. International ist ein Wettlauf um die technologische Führerschaft bei der Entwicklung des Mobilfunkstandards der 6. Generation entstanden, verbunden mit massiven Investitionen in Forschung und Entwicklung in den führenden Wirtschaftsnationen. In Ländern wie den USA, China, Japan oder Südkorea entstanden auf nationaler Ebene strategische Programme, um die Entwicklung von 6G zu beschleunigen und die Resilienz der IKT für eine Zukunft zu gewährleisten, in der alles vernetzt ist. Inmitten dieses Technologiewettlaufs findet gerade eine Konsultation für den zukünftigen „Cyber Security Act" auf EU-Ebene statt, mit dem in Europa die digitale Zukunft gestaltet werden soll. Die Gefahr besteht, dass auch in dieser von den Industrienationen weltweit sowohl in Konkurrenz als auch in Zusammenarbeit angestrebten IKT-Welt der Zukunft Cyberunfälle ganze Ökosysteme, oder die Wirtschaft und damit die Gesellschaften empfindlich gefährden. Resilienz muss ein Kernanliegen bei der Entwicklung künftiger Kommunikationssysteme sein.

IT-Sicherheit als Baustein resilienter Systeme

IT-Sicherheit ist essenzielle Voraussetzung für die Resilienz vernetzter digitaler Systeme. Nicht nur die KRITIS-Sektoren, sondern die Digitalgesellschaft und -wirtschaft insgesamt können bei Cyberangriffen empfindlich in Mitleidenschaft gezogen werden. Das Paradigma Resilience-by-Design ist ohne Security-by-Design und Values-by-Design nicht realisierbar. Aufgrund der Schwere möglicher Sicherheitsvorfälle im Bereich KRITIS, wäre beweisbare Sicherheit über alle Komponenten eines Systems hinweg wünschenswert. Aufgrund der Komplexität und des Umfangs von Systemen ist dies jedoch, zumindest aktuell, nicht umsetzbar. Noch müssen sich Beweise auf absolut zentrale Komponenten beschränken. Es ist jedoch zu bedenken, dass die Sicherheit von Systemen in diesem Kontext von so großer Relevanz ist, dass Kosten hierfür nicht immer das ausschlaggebende Argument sein dürfen.

Wenn bestimmte zentrale Sicherheitsbausteine für sich genommen nicht wirtschaftlich entwickelt werden können, hilft es, die Dinge aus einer anderen Perspektive zu betrachten: Denn begreift man solche Komponenten als gemeinsame Infrastruktur – als kritische Infrastruktur – verspricht ein solchermaßen kooperativer, wenn auch zunächst kostspielig erscheinender Ansatz einen Vorteil für alle. Die eigentliche Wertschöpfung erfolgt in vielen Fällen durch spezifische und individuelle Dienstleistungen. Zugrundeliegende Hardware- und Softwarekomponenten sind dabei meist gleich. Ein Beispiel ist der Einsatz von Linux als Betriebssystem, aber auch von diversen Softwarebibliotheken von node.js bis OpenSSL und Bouncy Castle. Häufig erfolgt aus den Anwendungen leider kein ausreichender finanzieller Rückfluss sodass letztlich Mittel fehlen, um die Qualität dieser Komponenten langfristig zu verbessern. Hier ist Besserung notwendig.

Sektor	Herausforderung	Lösungsbausteine
Energie	Komplexe Abhängigkeitsverhältnisse in vernetzten Systemen, insbesondere auch grenzüberschreitend	› Vorausschauende Wartung › Kryptographie, Netzsicherheit
Energie	Sicherung der Authentizität von Daten entlang von Kommunikationsketten	› (Infrastrukturfreie) taktile Kommunikation › Kommunikations- und Datensicherheit
Finanz- und Versicherungswesen / Gesundheit	Verlässlichkeit und Verfügbarkeit von Kommunikationssystemen	› Privatheitschutz, IT-Sicherheit › Kryptographie, Usable Security und Privacy
Informationstechnik und Telekommunikation	Kommunikationsinfrastrukturen müssen technisch von Grund auf resilient und sicher konzipiert und umgesetzt werden	› Resilience-by-Design › Security-by-Design, Beweisbare Sicherheit, Software Defined Security
Medien und Kultur	Nichttechnische Dimensionen von Resilienz müssen in einem breiten gesellschaftlichen Dialog erörtert und ausgehandelt werden	› Allgegenwärtige Vernetzung › Values-by-Design Privacy-by-Design
Staat und Verwaltung	Wahl der adäquaten Technologien und Organisationsformen unabhängig von Trends	› Netzsicherheit › Sichere Authentifizierung, Usable Security und Privacy
Transport und Verkehr	Zuverlässige Kommunikation auch abseits öffentlicher Mobilfunkinfrastruktur, um die funktionale und die Betriebssicherheit (Safety) zu gewährleisten	› Zuverlässige taktile Kommunikation › Cloud und Edge Security
Wasser	Migration zu vernetzen Anlagen unter Berücksichtigung der Anforderungen der IT-Sicherheit	› Vorausschauende Wartung › Security Retrofitting

Tab. 10.1 Überblick Herausforderungen und Lösungsbausteine aus Kommunikationssystemen und IT-Sicherheit anhand von KRITIS Sektoren (Quelle: Institut für Innovation und Technik (iit), eigene Darstellung)

Zusammenfassung

Kommunikationssysteme sind als zentrales Nervensystem der digitalen Gesellschaft und Wirtschaft einerseits unerlässlich für ihre Resilienz, andererseits müssen Kommunikationssysteme in einer allvernetzten Gesellschaft als zentrale kritische Infrastruktur mit funktionalen Verknüpfungen zu allen KRITIS-Sektoren und sensiblen Infrastrukturen selbst resilient sein. Resilienz ist in diesem Zusammenhang immer als ein ganzheitliches Konzept zu verstehen und beschränkt sich nicht nur auf die Cyber-Resilienz. Zur Realisierung der digitalen Resilienz in einer allvernetzten Struktur müssen alle Aspekte technischer und nichttechnischer Natur zusammengedacht werden. Herausforderungen dabei erwachsen unter anderem daraus, dass die Systeme auch künftig klassisch analog funktionieren müssen – beispielsweise Energie, Ernährung, Finanzen, Gesundheit, Transport, Wasser – diese aber in einer digitalisierten Welt für ihre Funktionsfähigkeit zwangsläufig auf Kommunikationssysteme angewiesen sind, welche resilient sein müssen.

Eine weitere Herausforderung ergibt sich aus dem Umstand, dass heutzutage Systeme, die über Jahre zusammengewachsen sind, sozusagen evolutionär mit resilienzstärkenden Eigenschaften versehen werden. Resilienz ist jedoch kein Stückwerk – es kommt darauf an, sie im Entwurfsprozess zu berücksichtigen und ganzheitlich umzusetzen. Der Einsatz innovativer Technologien wie KI oder Quantenkommunikation kann dabei hilfreich sein. Schließlich können eine durchdachte Kombination und Nutzung vorhandener Technologien der Kommunikationstechnik und IT-Sicherheit zum Aufbau von Resilienz eine kurzfristige Überbrückungslösung sein – bis Resilient-by-Design-Netze entwickelt werden können. Die Notwendigkeit zur Entwicklung resilienter digitaler Infrastrukturen wurde weltweit in entsprechenden (nationalen) Strategien verbrieft. In Deutschland und Europa sind diese Bestrebungen unter dem Begriff der technologischen Souveränität beziehungsweise strategischen Autonomie zusammengefasst und werden die künftige Entwicklung unserer Digitalgesellschaft prägen.

Zehn Grundgedanken zur Resilienz von vernetzten Systemen

1. Moderne IKT birgt die Möglichkeit, die digitale Kluft zu überwinden.
2. Durch die vollständige Vernetzung werden nahezu alle Systeme kritisch.
3. In einer vernetzten Welt stellen künstlich gezogene Grenzen Hemmnisse dar.
4. Resilienz bedeutet gesamtsystemisches Denken, Planen und Handeln.
5. Resilienz bedeutet neben technischen und organisatorischen Aspekten auch gesellschaftliche Fragen zu berücksichtigen.

6. Wesentlicher Grundsatz für Resilienz ist es, jeweils die passenden Technologien und Organisationsformen einzusetzen.
7. Es ist notwendig, Resilienz bereits im Entwurfsprozess zu berücksichtigen.
8. Modern erscheinende Technologien und aktuelle Trends sind im Sinne von Resilienz nicht immer die zu bevorzugenden Lösungen.
9. Kooperative Entwicklung von zentralen Komponenten kann für alle vorteilhaft sein.
10. Es gibt noch umfangreichen Forschungsbedarf.

Literatur

Born, Achim (2022): SAP steigt bei US-amerikanischem Fintech Taulia ein. In: Heise, 27.01.2022. Online verfügbar unter https://www.heise.de/news/SAP-steigt-bei-US-amerikanischen-Fintech-Taulia-ein-6340777.html, zuletzt geprüft am 06.08.2022.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) (o. J.): Warn-App NINA. Online verfügbar unter https://www.bbk.bund.de/DE/Warnung-Vorsorge/Warn-App-NINA/warn-app-nina_node.html.

Drozhzhin, Alex (2015): Kann man einen Zug hacken? In: Kaspersky Daily, 29.12.2015. Online verfügbar unter https://www.kaspersky.de/blog/train-hack/6650/, zuletzt geprüft am 06.08.2022.

Ermert, Monika; Briegleb, Volker (2022): Frankreich: Unbekannte durchtrennen Glasfaser-Backbones. In: Heise, 28.04.2022. Online verfügbar unter https://www.heise.de/news/Frankreich-Unbekannte-durchtrennen-Glasfaser-Backbones-7068664.html, zuletzt geprüft am 06.08.2022.

Fettweis, Gerhard P. et al (2017): Resiliente Netze mit Funkzugang. VDE-Positionspapier, 20.03.2017. Online unter: https://shop.vde.com/de/vde-positionspapier-resiliente-netze-mit-funkzugang, zuletzt geprüft am 06.08.2022.

gematik GmbH (Hrsg.) (2021): Atlas zur Telematikinfrastruktur. Zahlen. Daten. Fakten. Online verfügbar unter www.ti-atlas.de, zuletzt geprüft am 06.08.2022.

Kirchner, Malte (2022): Nach Diebstahl aus der Ukraine: Digitale Landmaschinen aus der Ferne gesperrt. In: Heise, 02.05.2022. Online verfügbar unter https://www.heise.de/news/Nach-Diebstahl-aus-der-Ukraine-Digitale-Landmaschinen-aus-der-Ferne-gesperrt-7071729.html, zuletzt geprüft am 06.08.2022.

Marschall, Stefan (2017): Lügen und Politik im "postfaktischen Zeitalter". In: APuZ - Aus Politk und Zeitgeschichte. Online verfügbar unter https://www.bpb.de/shop/zeitschriften/apuz/245217/luegen-und-politik-im-postfaktischen-zeitalter/, zuletzt geprüft am 06.08.2022.

Osler, David (2021): One ship is hacked every day on average. Ships and shipping companies are regularly targeted by cyber criminals, webinar discussion hears. In: Lloyd's List, 06.07.2021. Online verfügbar unter https://lloydslist.maritimeintelligence.informa.com/LL1137457/One-ship-is-hacked-every-day-on-average, zuletzt geprüft am 06.08.2022.

Peters, Benedikt (2022): Wie geht es mit dem Home-Office nach der Pandemie weiter? In: Süddeutsche Zeitung, 26.01.2022. Online verfügbar unter https://www.sueddeutsche.de/wirtschaft/home-office-corona-zahlen-1.5515722, zuletzt geprüft am 06.08.2022.

Roßnagel, Alexander; Eckert, Claudia; Hauschild, Timo; Müller-Quade, Jörn; Paar, Christof; Gabi, Dreo Rodosek; Waidner, Michael (2019): Gefährdung demokratischer Willensbildung durch Desinformation. Impulspapier. Online verfügbar unter https://www.forschung-it-sicherheit-kommunikationssysteme.de/dateien/forschung/2019-11-impuls-papier-willensbildung_desinformation.pdf, zuletzt geprüft am 06.08.2022.

Schirrmacher, Dennis (2021): Hunderte Coop-Supermärkte in Schweden nach REvil-Ransomwarebefall geschlossen. In: Heise 2021, 04.07.2021. Online verfügbar unter https://www.heise.de/news/Hunderte-Coop-Supermaerkte-in-Schweden-nach-REvil-Ransomwarebefall-geschlossen-6128251.html, zuletzt geprüft am 06.08.2022.

Sokolov, Daniel AJ (2021): Florida: Hacker wollte Trinkwasser aus der Ferne vergiften. In: Heise, 09.02.2021. Online verfügbar unter https://www.heise.de/news/Satelliten-Stoerung-Tausende-Windraeder-nicht-steuerbar-6529189.html, zuletzt geprüft am 06.08.2022.

Spiegel (2021a): Großbrand in Datenzentrum sorgt für Ausfall von Websites. Feuer bei Cloud-Anbieter. In: Spiegel, 10.03.2021. Online verfügbar unter https://www.spiegel.de/netzwelt/web/ovh-grossbrand-in-datenzentrum-in-strassburg-sorgt-fuer-stoerungen-a-dff1fc32-8bd0-4305-a026-b6221e079455, zuletzt geprüft am 06.08.2022.

Spiegel (2021b): "REvil" erpresst bis zu 1500 Firmen. Ransomware-Angriff. In: Spiegel, 06.07.2021. Online verfügbar unter https://www.spiegel.de/netzwelt/web/ransomware-bis-zu-1500-firmen-werden-von-revil-erpresst-a-4144c655-54d2-454a-b50c-c8ddbe8f161e, zuletzt geprüft am 06.08.2022.

Spiegel (2022a): IT-Probleme bei der Postbank verärgern Kunden. Kein Zugang zu Konten. In: Spiegel, 11.02.2022. Online verfügbar unter https://www.spiegel.de/netzwelt/kein-zugang-zu-konten-it-probleme-bei-der-postbank-veraergern-kunden-a-ad9afc70-7653-4d47-ab44-40ecdc96106d, zuletzt geprüft am 06.08.2022.

Spiegel (2022b): Cell Broadcast wird erstmals bundesweit getestet. Alarmmeldungen auf allen Handys. In: Spiegel, 25.04.2022. Online verfügbar unter https://www.spiegel.de/netzwelt/netzpolitik/cell-broadcast-wird-am-warntag-2022-erstmals-getestet-a-f56d271c-cdc5-402a-86c9-298b23fd92be, zuletzt geprüft am 06.08.2022.

The 5G Infrastructure Association (Hg.) (2021): European Vision for the 6G Network Ecosystem. Online verfügbar unter https://5g-ppp.eu/european-vision-for-the-6g-network-ecosystem/, zuletzt geprüft am 06.08.2022.

The Guardian (2021): App outage locks hundreds of Tesla drivers out of cars. Dozen of motorists report error as company's CEO, Elon Musk, apologises on Twitter. In: The Guardian, 20.11.2021. Online unter: https://www.theguardian.com/technology/2021/nov/20/tesla-app-outage-elon-musk-apologises, zuletzt geprüft am 06.08.2022.

Tyborski, Roman (2019): Risiko vernetzte Autos: Wenn Hacker plötzlich Gas- und Bremspedal bedienen. Digitale Revolution. In: Handelsblatt, 19.11.2019. Online verfügbar unter https://www.handelsblatt.com/technik/digitale-revolution/digitale-revolution-risiko-vernetzte-autos-wenn-hacker-ploetzlich-gas-und-bremspedal-bedienen/25244352.html, zuletzt geprüft am 06.08.2022.

Villasenor, John (2015): Five Lessons On The 'Security Of Things' From The Jeep Cherokee Hack. In: Forbes, 27.07.2015. Online verfügbar unter https://www.forbes.com/sites/johnvillasenor/2015/07/27/five-lessons-on-the-security-of-things-from-the-jeep-cherokee-hack/?sh=66c4adf8692a, zuletzt geprüft am 06.08.2022.

Wilkens, Andreas (2022): Satelliten-Störung: Tausende Windräder nicht steuerbar. In: Heise, 01.03.2022. Online verfügbar unter https://www.heise.de/news/Satelliten-Stoerung-Tausende-Windraeder-nicht-steuerbar-6529189.html, zuletzt geprüft am 06.08.2022.