RAT FÜR DIGITALE ÖKOLOGIE

# DIGITALISIERUNG, VULNERABILITÄT UND (KRITISCHE) GESELLSCHAFTLICHE INFRASTRUKTUREN

## POSITIONSPAPIER

VOM INSTITUT FÜR TECHNIKFOLGEN-ABSCHÄTZUNG
DER ÖSTERREICHISCHEN AKADEMIE DER WISSENSCHAFTEN

IM AUFTRAG DES RATES FÜR DIGITALE ÖKOLOGIE

# ÜBER DEN RAT

Der transdisziplinäre Rat für Digitale Ökologie hat es sich zur Aufgabe gemacht, die Digitale Transformation der Gesellschaft aus den Begrenztheiten einer rein wirtschafts- und technikgetriebenen Betrachtung zu befreien. Aus der Sicht des Rats für Digitale Ökologie muss die Gesellschaft definieren, wie und wofür digitale Technologien und Anwendungen eingesetzt werden. Dies ist vor allem deswegen unabdingbar, weil die Digitale Transformation alle Bereiche der demokratischen Gesellschaft betrifft und weil die ökonomischen, kulturellen, politischen, psychologischen und gesundheitlichen Dimensionen der Digitalen Transformation miteinander in Wechselwirkung stehen.

Erst vor dem Hintergrund einer Ökologie digitaler Systeme wird auch eine Politik der Digitalen Transformation denkbar, die Leitlinien für den Technikeinsatz vorgeben kann und muss. Der Rat betrachtet es als seine Aufgabe, Debatten anzustoßen und die Digitale Transformation als zentrales gesellschaftspolitisches Thema begreifbar zu machen. Die Digitale Transformation ist in all ihren Dimensionen eine politische Gestaltungsaufgabe.

**Der Rat besteht aus:**

- **Dr. Stefan Brink**, Wiss. Institut für die Digitalisierung der Arbeitswelt (wida/Berlin)
- **Prof. Dr. Vanessa Miriam Carlow**, Institute for Sustainable Urbanism, TU Braunschweig
- **Prof. Dr. Maja Göpel,** Leuphana Universität
- **Dr. Wolfgang Kaleck,** European Center for Constitutional and Human Rights (ECCHR)
- **Prof. Andrea Krajewski,** Interactive Media Design, Hochschule Darmstadt
- **Prof. Dr. Johannes Merck,** Umweltstiftung Michael Otto
- **Dr. August Oetker,** Unternehmer
- **Prof. Dr. Frederike Petzschner,** Carney Institute for Brain Science, Brown University
- **Prof. Dr. Peter Reichl,** Fakultät für Informatik, Universität Wien
- **Prof. Dr. Tilman Santarius,** IÖW, TU Berlin
- **Prof. Dr. Harald Welzer,** FUTURZWEI. Stiftung Zukunftsfähigkeit (Sprecher)
- **Dr. Marie-Luise Wolff,** ENTEGA AG

Mehr erfahren: **www.rdoe.org**

Der Rat für Digitale Ökologie ist ein Projekt von Futurzwei. Stiftung Zukunftsfähigkeit
– gefördert von Allianz Foundation und Schöpflin Stiftung.

FUTURZWEI ALLIANZ FOUNDATION Schöpflin Stiftung:

# INHALT



## ABBILDUNGSVERZEICHNIS



## TABELLENVERZEICHNIS

# ZUSAMMENFASSUNG

Diese Überblicksstudie befasst sich mit den komplexen Zusammenhängen zwischen der Digitalen Transformation und der Vulnerabilität gesellschaftlicher Infrastrukturen. Der erste Hauptteil (Abschnitte 1 und 2) beleuchtet diese Zusammenhänge genauer und diskutiert die Rolle digitaler Technologien. Im zweiten Hauptteil (Abschnitt 3) werden der gegenwärtige Entwicklungsstand und die Problemfelder anhand ausgewählter Bereiche mit unterschiedlichen Beispielen herausgearbeitet. Daraus werden dann im dritten Hauptteil (Abschnitt 4) wesentliche gesellschaftliche Folgen und zentrale Herausforderungen abgeleitet und diskutiert. Diese werden in Abschnitt 5 zusammenfassend dargestellt.

*Erhebliche Ambivalenz in der Digitalisierung*

Die Analyse zeigt teils erhebliche Ambivalenzen in der Digitalisierung gesellschaftlicher Infrastrukturen, die in praktisch allen Infrastrukturbereichen in unterschiedlicher Form sichtbar werden. Weil in vielen Bereichen die digitale Wertschöpfung sehr stark im Fokus ist, erhöhen sich einige Probleme und Risiken teils drastisch – etwa im Haushalts- und Konsumbereich. Zentrale Problemfelder in allen Bereichen sind: mangelhafte Sicherheit, steigende ökonomische und technologische Abhängigkeiten, wachsende Informations- und Machtasymmetrien – und Beeinträchtigung der Grundrechte.

*Höhere Komplexität und Anfälligkeit für Fehler und Ausfälle*

Dennoch ist die Frage, ob die Digitale Transformation Infrastrukturen per se verwundbarer macht, nicht ohne Weiteres zu beantworten. Das hängt naturgemäß stark von den jeweiligen Rahmenbedingungen und konkreten Anwendungsfällen ab. Generell bedeutet weitere Digitalisierung mehr Komplexität in gesellschaftlichen Infrastrukturen. Wenn diese nicht mit Governance und wirkungsvollen Steuerungsmaßnahmen beherrschbar wird, steigt das Risiko für Fehler und Ausfälle der Systeme. Diese können je nach Infrastrukturbereich unterschiedlich kritisch sein. Das Spektrum kritischer Vorfälle reicht von Angriffen und Softwarefehlern über gravierende Sicherheitsmängel bis hin zum Missbrauch technologischer und ökonomischer Machtpositionen. In Summe verschärft sich hier ein zentrales Grundproblem der Digitalisierung immer weiter: Die Informations- und Machtasymmetrien.

*Wachsende Informations- und Machtasymmetrien*

Dies hat schon jetzt erhebliche Konsequenzen: Kriminelle Akteure nutzen digitale Schwachstellen gezielt aus, um etwa Infrastrukturbetreiber zu erpressen. Staatliche Akteure üben geopolitische Macht durch gezielte Angriffe auf Infrastrukturen aus. Wirtschaftliche Akteure nutzen ihre Marktstellungen über technologische und ökonomische Abhängigkeiten, forcieren damit Lock-Ins – und beeinträchtigen die Handlungsfähigkeit der von ihnen abhängigen Akteure und Endkunden.

*Datengetriebene Geschäftsmodelle*

Ungleiche Machtverhältnisse sind nichts Neues, allerdings verschärft sich diese Situation mit digitalisierten Infrastrukturen erheblich, wie die in Abschnitt 3 aufgezeigten Beispiele verdeutlichen. Probleme der Digitalisierung sind nicht unbedingt nur dem Technikeinsatz geschuldet, sondern auch einer überproportional starken Kapitalisierung von Daten und der Etablierung von datengetriebenen Geschäftsmodellen der Plattformökonomie.

*Schleichende Machtverschiebung*

Durch ihre technische Gestaltungsmacht sind Technologie- und Plattformbetreiber zu machtvollen Akteuren in verschiedenen Sektoren geworden. Aufgrund ihrer Breitenwirkung kommt es in immer mehr Bereichen zu einer schleichenden Machtverschiebung (zum Beispiel im Mobilitätsbereich). Diese erhebliche Marktmacht einiger weniger Akteure erschwert einen differenzierten Umgang mit der Digitalisierung von Infrastrukturen zusätzlich. Sie erzeugt außerdem einen starken Druck zur schnellen Digitalisierung auf verschiedene gesellschaftliche Bereiche. Dieser Druck manifestiert sich auf institutioneller Ebene (bei Infrastrukturbetreibern im weiteren Sinn) und wird über digitalisierte Anwendungen an vielen Stellen auch auf die individuelle Ebene, auf Personen wie Haushalte übertragen. Es wird teils digitalisiert, ohne die längerfristigen Konsequenzen zu berücksichtigen.

*Starker Digitalisierungsdruck*

*Steigende technologische und ökonomische Abhängigkeiten*

Mit der Digitalisierung von Infrastrukturen nimmt so auch die Breiten- und Tiefenwirkung digitaler Technologien zu. Digitalisierte Infrastrukturen sind intrusiver als „klassische“ und wirken wesentlich stärker als bislang in Haushalte und die Sphären einzelner Personen hinein. Problembereiche auf institutioneller Ebene wie steigende ökonomische und technologische Abhängigkeiten, beeinträchtigen daher zusehends stärker auch die individuelle Ebene. In Folge gewinnen auch grundrechtliche und ethische Aspekte wie Datenschutz und Datensicherheit, Schutz der Privatsphäre, Autonomie und Selbstbestimmtheit und damit verbundene Gefahren immer mehr an Bedeutung.

*Schutz der Infrastruktur nicht auf Cybersicherheit reduzieren*

Die Bewältigung dieser Problemfelder und die Stärkung der Resilienz ist mit enormen Herausforderungen verbunden. Derzeit liegt der Fokus sehr stark auf Cybersicherheit, die unbestritten von hoher Relevanz ist. Angriffe auf Infrastrukturen sind besorgniserregend und erfordern wirksame Schutzkonzepte. Das betrifft aber weniger nach außen gerichtete, sondern vielmehr „nach innen“ gerichtete Maßnahmen: Es gilt, die Sicherheitsniveaus von Infrastruktursystemen zu erhöhen und Schwachstellen zu beseitigen. Zudem ist Sicherheit zwar wichtig, aber nur ein Teilaspekt. Denn Vulnerabilität von Infrastrukturen betrifft eben nicht nur physische oder technische Sicherheit und den Schutz vor externen Bedrohungen, sondern auch und vor allem die Versorgungssicherheit von Wirtschaft und Gesellschaft bezüglich der Deckung ihrer Grundbedürfnisse. Wenn sich aber technologische und ökonomische Abhängigkeiten weiter verschärfen, gerät gerade dieser grundlegende Aspekt unter Druck.

*Digitalisierte Infrastrukturen werfen neue Fragen zu Grundrechten auf*

Letztlich wirft die fortschreitende Digitalisierung von gesellschaftlichen Infrastrukturen essenzielle Fragen auf, die zum Teil gerade erst neu verhandelt werden: Welche Akteure haben welche Formen von Kontrolle über Infrastrukturen? Wie ist das Verhältnis zwischen staatlicher und privater Leistungserbringung bei der Daseinsvorsorge? Wie kann die Resilienz von Infrastrukturen gestärkt werden, um die sichere Grundversorgung weiterhin zu gewährleisten? Und wie steht das im Einklang mit Grundrechten und gesellschaftlichen Grundbedürfnissen? Nach derzeitigem Stand gibt es hier noch erhebliche Anstrengungen zu leisten: Eine zentrale Herausforderung in der digitalen Gesellschaft ist es, den Technikeinsatz unter Achtung ethischer und rechtlicher Normen so zu gestalten, dass Infrastrukturen gesellschaftliche Bedürfnisse decken und nicht gefährden.

# EXECUTIVE SUMMARY

This overview study explores the complex interrelations between the digital transformation and the vulnerability of societal infrastructures. The first main part (sections 1 and 2) examines these interrelations in detail and discusses the role of digital technologies. The second main part (section 3), outlines the current state of development and elaborates problem areas on the basis of selected domains based on different examples. The third main part (Section 4) then derives and discusses crucial social consequences and key challenges. These are summarized in section 5.

*considerable ambivalences in the digitization of infrastructures*

The analysis reveals some considerable ambivalences in the digitization of societal infrastructures, which are visible across all infrastructure areas in different respects. As the focus in many areas is very much on digital value creation, some problems and risks increase dramatically in specific domains – for example, in the household and consumer sectors. Essential problems across all domains are: insufficient security, increasing economic and technological dependencies, growing information and power asymmetries – and impairment of fundamental rights.

*Higher complexity and proneness to errors and failure*

Nevertheless, the question of whether the digital transformation makes infrastructures more vulnerable per se cannot be answered without further ado. Naturally, this depends heavily on the respective framework conditions and specific applications. In general, further digitization implies more complexity in societal infrastructures. If this cannot be managed with governance and effective control measures, risks of errors and system failures increase. These can vary in criticality depending on the affected infrastructure sector. The spectrum of critical incidents ranges from attacks and software errors to serious security deficiencies and the abuse of technological and economic power. In sum, a fundamental problem of digitization aggravates further here: information and power asymmetries.

*Increasing information- and power asymmetries*

This is already having significant consequences: Criminal actors are deliberately exploiting digital vulnerabilities to blackmail infrastructure operators, for example. State actors exercise geopolitical power through targeted attacks on infrastructures. Economic players use their market positions to force lock-ins and technological and economic dependencies, and impairing agency of dependent actors and consumers.

*Data-driven business models*

Unequal power relations are not a new problem per se, but digitized infrastructures significantly exacerbate this situation, as the examples highlighted in section 3 point out. Problems of digitization do not merely result from technology usage, but also from a disproportionately strong capitalization of data and the establishment of data-driven business models of the platform economy.

*Creeping power shifts ...*

Through their shaping power, technology and platform providers have become powerful players in various sectors. Due to their broad impact, there is an incremental shift in power in more and more domains (e.g., in the mobility sector).

*... and strong pressure to digitization*

This considerable market power of few players additionally hampers a differentiated approach to the digitization of infrastructures. It also generates strong pressure for rapid digitization on various areas of society. This pressure manifests itself at the institutional level (among infrastructure providers in the broader sense) and affects the individual level (among persons and households) in many respects via digital applications. Digitization proceeds quickly while the longer-term consequences are largely neglected.

*Increasing technological and economic dependencies*

The digitization of infrastructures thus also extends the broad and deep impact of digital technologies. Digitized infrastructures are more intrusive than "conventional" infrastructures and have a much greater impact on households and the spheres of individual persons. Problem domains at the institutional level, such as increasing economic and technological dependencies, therefore increasingly affect the individual level as well. As a result, fundamental rights and ethical issues such as data protection and data security, protection of privacy, autonomy and self-determination, and the associated risks are becoming increasingly pressing.

*Protecting infrastructures requires more than cybersecurity*

Overcoming these problem areas and strengthening resilience involves enormous challenges. Currently, strong focus is on cybersecurity, which is undeniably of high relevance. Attacks on infrastructures are worrying and require effective safeguards. However, external threats are only one side of the coin and many risks result from internal security flaws. Measures thus require to increase the security standards of infrastructure systems and close security gaps. Moreover, security is important, but it is only one aspect. Vulnerability of infrastructures does not only concern physical or technical security to protect from external threats, but particularly also security of supply for society and the economy as well as the coverage of basic needs. But if technological and economic dependencies continue to intensify, this fundamental aspect is increasingly under pressure.

*Digitized infrastructures raise new questions on fundamental rights*

Ultimately, the ongoing digitization of social infrastructures raises essential questions, which are just being renegotiated: Which actors have which forms of control over infrastructures? What is the relationship between public and private provision of services of general interest? How to strengthen the resilience of infrastructures to further ensure secure basic services? And how can this be reconciled with the protection of fundamental rights and basic societal needs? The current state of development requires considerable efforts to be made: a crucial challenge in the digital society is to shape the use of technology while respecting ethical and legal standards so that infrastructures meet societal needs and do not jeopardize them.

# 1 EINLEITUNG

Die digitale Transformation der Gesellschaft, also die weitreichende Umgestaltung gesellschaftlicher Sektoren durch digitale Technologien ist bereits weit fortgeschritten. Neben Wirtschaft und Industrie sind nahezu alle Bereiche des Alltags in irgendeiner Form bereits digitalisiert oder sollen es künftig sein. Dabei spielen vor allem Infrastrukturen und daran gekoppelte Dienste eine zentrale Rolle. Von der Energieversorgung über moderne Haushaltsgeräte, von Verkehr und Mobilität bis zur Gesundheitsversorgung gibt es kaum noch Bereiche, die nicht von der Digitalen Transformation betroffen sind. Nicht immer ist dabei jedoch eindeutig, inwieweit die Digitalisierung eines Bereichs tatsächlich notwendig ist oder nur aufgrund des Hypes umgesetzt wird. Das hat zur Folge, dass sich Digitalisierung fast schon mystisch wie ein undurchsichtiger Schleier über die Gesellschaft legt und Fakten schafft. Hinter diesem „Digital Curtain" bleiben oftmals nicht nur die Funktionsweise digitaler Prozesse und ihrer Datenflüsse verborgen, sondern auch die damit verbundenen Abhängigkeiten der Gesellschaft zu digitalen Technologien. Vor diesem Hintergrund drängt sich die Frage auf, was Digitalisierung für die Vulnerabilität (Verwundbarkeit) der Gesellschaft bedeutet.

*Digitalisierung verändert ganze Infrastrukturbereiche*

Diese Studie geht dieser Frage nach und bietet einen Überblick zu Status-Quo, Entwicklungen und Folgen der fortschreitenden Digitalisierung gesellschaftlicher Infrastrukturen – sowie der damit verbundenen Technologien und Anwendungen. Die Untersuchung orientiert sich dabei an folgenden Leitfragen:

- Wie wirkt sich Digitalisierung auf gesellschaftliche Infrastrukturen (in ausgewählten Bereichen) aus?
- Welche Abhängigkeiten entstehen dadurch?
- Wie und unter welchen Annahmen wird die Digitalisierung in verschiedenen Infrastrukturbereichen gestaltet?
- Welche Folgen hat das auf institutioneller/organisatorischer und individueller/sozialer Ebene – und was bedeutet das für die Vulnerabilität der Gesellschaft?

Methodisch basiert die Überblicks-Studie vor allem auf Desk-Research, Analyse von Fachliteratur und Sekundärquellen wie Web- und Medieninhalten. Im ersten Hauptteil (Abschnitte 1 und 2) werden Grundlagen zu Digitalisierung, (kritischen) Infrastrukturen und Vulnerabilität erläutert. Dabei wird auch diskutiert, wie sich digitale Technologien auf die konzeptuelle Bedeutung von Vulnerabilität auswirken. Der zweite Hauptteil (Abschnitt 3) bietet einen Überblick über relevante technologische Entwicklungen, sicherheitsrelevante Vorfälle wie gravierendere Störfälle oder Angriffe auf kritische Infrastrukturen – und identifiziert Problemfelder der Digitalisierung in ausgewählten Bereichen. Aufgrund der Komplexität des Themas liegt der Fokus hierbei auf den Bereichen Energieversorgung, Mobilität und Verkehr sowie Haushalt und Konsum. Im dritten Hauptteil (Abschnitte 4 und 5) werden anhand der Synthese der Problemfelder gesellschaftliche Auswirkungen auf institutioneller und individueller Ebene identifiziert. Dabei wird diskutiert, welche zentrale Herausforderungen daraus resultieren sowie mögliche Handlungsbedarfe ausgearbeitet.

*Gesellschaftliche Auswirkungen auf institutioneller und individueller Ebene*

## 1.1 DIGITALISIERUNG ZWISCHEN HYPE UND REALITÄT

*Digitalisierungsbegriff oft inflationär*

Digitalisierung ist ein vielschichtiges Phänomen, das in den vergangenen Jahren zu einem omnipräsenten Thema der Gesellschaft wurde. Als stark von Hypes geprägte Entwicklung wird der Begriff oft inflationär als Synonym für technologisch bedingte Veränderungen jeglicher Art verwendet. Die Beschreibungen reichen dabei von irreführenden Erklärungen, die Digitalisierung würde über Computersysteme mittels binärer Logik (0 und 1) die analoge Welt auf zwei Zustände reduzieren, bis hin zu diversen Marketing-Versprechen von angeblichen Technik-Revolutionen – sei es durch Big Data, Internet of Things (IoT), Smart Technologies, Industrie 4.0 oder aktuell Künstlicher Intelligenz und Machine Learning. Ein bekanntes Beispiel für missglückte Phrasen ist etwa die bereits in die Jahre gekommene Aussage: „Daten sind das neue Öl." Diese und ähnliche Aussagen waren vor einigen Jahren im Kontext von „Big Data" als neuem Paradigma der digitalen Wertschöpfung über Dateninfrastrukturen häufig zu vernehmen (vgl. u. a. Arthur 2013; Mayer-Schönberger/Cukier 2013; Wired 2014; Strauß 2015; TE 2017).[1] Die Metapher wurde zwar später auch medial als irreführend und deplatziert kritisiert (u. a. in Welzer 2016; Wired 2019), wird aber zum Teil auch heute noch verwendet, um für Digitalisierung und digitale Wertschöpfung zu werben.[2] Das Eigenleben dieses missglückten Sinnbilds sagt einiges über die Problemfelder der Digitalisierung aus. Digitale Daten gelten demnach als kostbarer Rohstoff für den Motor der Plattformökonomie zur Etablierung neuer Geschäftsmodelle. Die Frage, wieweit das überhaupt zutrifft, geht im Hype ebenso unter wie die Frage, ob das nicht ohnehin eine problematische Begründung für Digitalisierung an sich ist – vor allem wenn es um Infrastrukturen geht und um Bereiche, die die gesellschaftliche und wirtschaftliche Grundversorgung betreffen.

*Unterschätzter Aspekt: bereichsübergreifende Vernetzung*

Ein wesentlicher, oft unterschätzter Aspekt der Digitalisierung ist dagegen die weiter zunehmende bereichsübergreifende Vernetzung über digitale Technologien[3]. Denn das hat längerfristige Folgen: Digitalisierung bedeutet Technologieeinsatz mit dem Ziel, möglichst nahtlose Informationsprozesse zu schaffen, um über verschiedene Anwendungsbereiche hinweg automatisierte, maschinenlesebare Datenströme zu generieren. Diese sollen dann etwa der Optimierung von Prozessen und Abläufen sowie wachsender Wertschöpfung dienen. Dieser erhöhte Vernetzungsgrad eines Bereichs oder einer Anwendung durch digitale Technologien über Bereichs- und Systemgrenzen hinweg ist der zentrale Aspekt, der zu einer folgenreichen Veränderung gesellschaftlicher Prozesse führt.

---

1 Trivia: „Data is the new oil" geht angeblich auf Clive Humbly, einen britischen Mathematiker und Vorstand eines digitalen Werbe-Unternehmens zurück (Arthur 2013).

2 *www.ibm.com/blogs/digital-transformation/in-en/blog/data-is-the-new-fuel-ai-is-the-accelerator/*; *www.mobilevision-group.com/wp-content/uploads/2021/03/2021-1-Insight-Data-Monetization.pdf*.

3 Vor dem breiten Digitalisierungshype besser bekannt als Informations- und Kommunikationstechnologien (IKT).

Diese Entwicklung läuft bereits seit vielen Jahren und die bereits hochgradig vernetzte Gesellschaft ist geprägt von einer stetig wachsenden Konvergenz zwischen analogen und digitalen Umgebungen (Strauß 2019, S. 5). Floridi prägte hierfür den Begriff „Infosphere", der eine quasi allumfassende Informatisierung aller Lebensbereiche mithilfe digitaler Technologien bezeichnet (Floridi 2010). Integraler Bestandteil dieser Entwicklung ist die steigende (Hyper-)Konnektivität von Systemen und Prozessen der digitalisierten Bereiche und die Entstehung neuartiger Netzwerkstrukturen für anwendungsübergreifende Daten- und Informationsverarbeitung (Strauß 2019, S. 82ff.). Dieser Transformationsprozess ist in mehrfacher Hinsicht sehr ambivalent: Die Digitalisierung bringt zweifelsohne viele Vorteile wie Prozessoptimierung, Echtzeit-Analyse von betriebsrelevanten Messdaten, Frühwarnung bei kritischen Betriebsbedingungen und vieles mehr. Allerdings macht sie Systeme und Anwendungen komplexer, wodurch sich die Anfälligkeit für Fehler, Störungen oder Ausfälle deutlich erhöhen kann.

*Hyper-Konnektivität und neuartige Netzwerkstrukturen*

Neben technischen Herausforderungen kann zudem der Zweck der Digitalisierung eines spezifischen Bereichs problematisch sein oder im Widerspruch zu den erhofften Vorteilen stehen. Das ist zum Beispiel der Fall, wenn Digitalisierung nicht primär dazu dient, gesellschaftliche Bereiche oder Infrastrukturen robuster, nachhaltiger, sicherer oder resilienter zu gestalten, sondern dazu, neue Geschäftsmodelle zu etablieren. Digitalisierung ist insofern dort problematisch, wo die Logik der digitalen Wertschöpfung in Bereiche hineinwirkt, die bislang aus gutem Grund nicht nach dieser Logik funktioniert haben. Sehr deutlich wird das im Bereich gesellschaftlicher Infrastrukturen. Der Hauptzweck von Infrastrukturen ist die Versorgung mit essenziellen Ressourcen wie zum Beispiel Energie und die Daseinsvorsorge, von der das Funktionieren gesellschaftlicher und wirtschaftlicher Prozesse abhängig ist.

*Unterschiedliche Logiken zwischen Daseinsvorsorge und digitaler Wertschöpfung*

Die klassische ökonomische Logik bei Infrastrukturen ist: Das Schaffen und Betreiben von Infrastrukturen und die Versorgung mit Ressourcen ist eine Dienstleistung, für die entsprechend vergütet beziehungsweise bezahlt wird. Digitale Wertschöpfung ändert diese Logik und führt zusätzlich Geschäftsmodelle ein, die auf der Vermarktung der entstehenden Daten basiert. Die Grundlage dafür sind oftmals bereits zahlende Kunden, deren Daten hier zusätzlich erfasst und weiterverarbeitet werden. Das geschieht oft ohne deren Wissen und Kontrolle. Dadurch wird der Zweck der Digitalisierung weitgehend entkoppelt von der ursprünglichen Dienstleistung. In der Technologiebranche wird hier häufig der abstrakte Begriff eines digitalen Ökosystems verwendet. Gemeint ist damit aber kein ökologisches, sondern ein ökonomisches System, das mithilfe digitaler Vernetzung neue Geschäftsmodelle ermöglichen und etablieren soll. Erschwerend kommt hinzu, dass gerade durch digitale Vernetzung auch neue Probleme wie erhöhte Abhängigkeiten (auf institutioneller wie individueller Ebene) entstehen. Digitalisierung bringt also sowohl technologische als auch ökonomische Veränderungsprozesse mit sich, die in den Folgekapiteln noch genauer behandelt werden.

## 1.2 WAS BEDEUTET DIGITALISIERUNG VON GESELLSCHAFTLICHEN INFRASTRUKTUREN?

*Kritische Infrastrukturen sind zentral für das Funktionieren der Gesellschaft*

Im klassischen Sinn sind Infrastrukturen all jene staatlichen und privaten Einrichtungen, Anlagen, Strukturen und Systeme, die zur Daseinsvorsorge, also der Funktionsfähigkeit wirtschaftlicher und sozialer Prozesse in der Gesellschaft benötigt werden. Der Begriff „kritische Infrastrukturen" (KRITIS) bezieht sich primär auf die Bedeutung dieser Einrichtungen für die Funktionsfähigkeit eines gesamten Staates. Die Europäische Union definiert dementsprechend kritische Infrastrukturen als in einem Mitgliedstaat gelegene Anlagen, Systeme oder Teile davon, „die von wesentlicher Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen, der Gesundheit, der Sicherheit und des wirtschaftlichen oder sozialen Wohlergehens der Bevölkerung sind und deren Störung oder Zerstörung erhebliche Auswirkungen auf einen Mitgliedstaat hätte, da diese Funktionen nicht aufrechterhalten werden könnten". (EKI 2008). Die Richtlinie dient Mitgliedsstaaten als Rahmen, um den Schutz ihrer Infrastrukturen zu verbessern. Hier wurde in den vergangenen Jahren sehr vieles geleistet und eigene nationale Strategien zum Schutz kritischer Infrastrukturen entwickelt. In Deutschland werden kritische Infrastrukturen nach Sektoren[4] unterschieden:

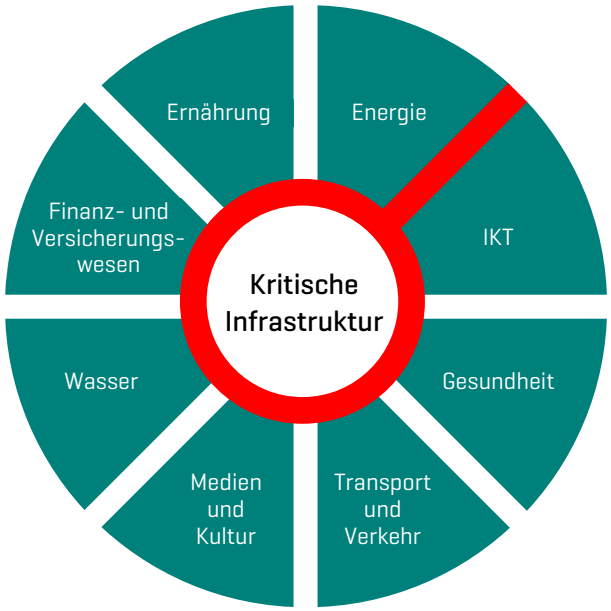



**Abbildung 1: Sektorale Gliederung kritischer Infrastrukturen und Relevanz von Energie und IKT.**
Quelle: adaptiert von (BSI 2014, S. 5 und Strauß/Krieger-Lamina 2017, S. 16)

[4] In neueren Gliederungen gelten zudem auch Staat/Verwaltung und Abfallwirtschaft als eigene Bereiche *https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/Sektoren-Branchen/sektoren-branchen_node.html*.

Diese klassische sektorale Gliederung ist für die staatliche Schutzfunktion der verschiedenen Bereiche durchaus sinnvoll. Allerdings vernachlässigt diese Perspektive den hohen Stellenwert von zwei Infrastrukturbereichen: Energieversorgung und digitale Systeme (IKT). Beide sind als Querschnittsbereiche entscheidend für die Funktionsfähigkeit in allen anderen Bereichen (vgl. Strauß/Krieger-Lamina 2017). Hinzu kommt, dass Digitalisierung die Bedeutung von Infrastrukturen insgesamt weiter verändert. In dieser Lesart wird Infrastruktur in der Wissenschafts- und Technikforschung (STS) daher sehr breit gefasst als eine Form der Verteilung von Aufgaben und Eigenschaften zwischen Hardware, Software und Menschen (Star/Bowker 2006, S. 232). Gerade aufgrund ihres Querschnittscharakters hängt die Vulnerabilität der Gesellschaft zusehends stark von digitalen Infrastrukturen ab. Das betrifft sowohl Organisationen und Institutionen als auch Haushalte und Individuen. Der Fokus dieser Überblicks-Studie liegt daher auf der Frage, inwieweit und wodurch sich gesellschaftliche Vulnerabilität durch Digitalisierung von Infrastrukturen und daran gekoppelte Anwendungen verändert. Dementsprechend wird Infrastruktur hier breiter verstanden als Systeme, Systemteile und Anwendungen, die für eine funktionsfähige Grundversorgung (mit Energie, Information oder anderen Grundbedürfnissen) relevant sind.

*Querschnittsbereiche Energieversorgung und IKT vernachlässigt*

Ein wesentliches Merkmal von Infrastrukturen ist ihre Netzwerkform. Infrastrukturen sind vernetzte Systeme, die verschiedene Bereiche verbinden können. Diese Verbindung ist meist implizit. Eine weitere Eigenschaft ist daher ihre relative Verborgenheit: Infrastrukturen funktionieren im Hintergrund und ihr Einfluss auf wirtschaftliche und gesellschaftliche Abläufe ist meist „unsichtbar" (vgl. Bowker et al. 2010). Sie gelten schlicht als gegeben und werden, wenn sie funktionieren, meist gar nicht bewusst wahrgenommen. Die Funktionsfähigkeit von Infrastrukturen hängt von vielen Faktoren ab. Einer davon ist ihre Komplexität. Infrastrukturen sind auch in analoger Form komplexe Systeme. Die zunehmende Integration digitaler Technologien in Infrastrukturen aber hat erhebliche Auswirkungen auf den Komplexitätsgrad: Systemisch betrachtet erhöht sich mit steigender Anzahl integrierter Subsysteme (zum Beispiel digital vernetzter Elemente) auch die Komplexität des Gesamtsystems. Im technischen Sinn wird die Verbindung zwischen mechanischen Komponenten und digitalen Technologien auch als cyber-physisches System bezeichnet (Drossel et al. 2018), die unter anderem im Bereich der industriellen Automatisierung mit digitalen Technologien von Bedeutung sind (Aichholzer et al. 2015). Die Vernetzung selbst hängt wiederum in fast allen Bereichen zunehmend von Dateninfrastrukturen und Konzepten ab, die auf Cloud Computing basieren – wie Software-as-a-Service (Saas), Infrastructure-as-a-Service (IaaS), Network-as-a-Service (Naas), oder Platform-as-a-Service (Paas) (Leimbach et al. 2014). In Abschnitt 3 wird noch genauer auf die Bedeutung verschiedener Technologien eingegangen.

*Zentrale Merkmale: Netzwerkform und relative Verborgenheit*

Durch Digitalisierung kann es also zu einer Verschränkung zwischen physischen und virtuellen Infrastrukturbereichen kommen. Digitale Technologien lassen sich selbst als eine Art Meta-Infrastruktur begreifen, oder systemisch als Metasystem, das die Qualität eines klassischen Infrastruktursystems verändert. Diese Qualitätsänderung basiert auf zwei wesentlichen Faktoren: Digitaler Informationsverarbeitung und digitaler Vernetzung. Digitale Infrastruktur wird damit selbst zur kritischen Infrastruktur, weil sie maßgeblich die Funktionsweise digital vernetzter Infrastrukturbereiche beeinflusst.

*Digitale Technologien als Meta-Infrastruktur*

# 2 VULNERABILITÄT UND DIGITALISIERUNG

## 2.1 ZENTRALE EIGENSCHAFTEN VON VULNERABILITÄT

*Unterschiedliche Konzepte zu Vulnerabilität*

Vulnerabilität bedeutet wörtlich Verwundbarkeit oder Verletzlichkeit und bezeichnet allgemein formuliert Zustände, in denen die Anfälligkeit für Gefahren erhöht ist. Je nach Perspektive und Kontext kann sich das auf einzelne Personen, Gruppen, soziale Gemeinschaften oder auch Objekte, Prozesse sowie soziotechnische Systeme beziehen – wie eben Infrastrukturen. Es gibt zahlreiche theoretische Rahmenkonzepte zu Vulnerabilität und entsprechend viele Bedeutungen, die je nach disziplinärem Fokus variieren. In den Sozialwissenschaften oder der Psychologie ist Vulnerabilität etwa auf soziale Faktoren oder intersubjektive Prozesse bezogen und daher ganz anders konnotiert als in den Naturwissenschaften oder in der Risikoforschung, wo es um Verwundbarkeit gegenüber Natur- und Umwelteinflüssen geht (Lenz 2009; Bürkner 2010; Birkmann et al. 2010). Die Vereinten Nationen definieren Vulnerabilität recht breit als „the conditions determined by physical, social, economic and environmental factors or processes, which increase the susceptibility of a community to the impact of hazards" (UN/ISDR 2004, 16). Demnach bezeichnet Vulnerabilität verschiedene Faktoren und Prozesse, die Risiken für die Allgemeinheit erhöhen. Dieser Ansatz ist vor allem in der Risikoforschung und im Katastrophenschutz von Bedeutung.

*Wechselwirkungen zwischen Risikoexposition und Bewältigungskapazität*

Abseits unterschiedlicher Bedeutungen und konzeptioneller Zugänge gibt es auch Gemeinsamkeiten. Eine wesentliche liegt im Aspekt der Wechselwirkungen zwischen verschiedenen Faktoren, die Vulnerabilität beeinflussen. Weit verbreitet etwa das Modell von Turner et al. (2003), das sozial- und naturwissenschaftliche Perspektiven kombiniert und Vulnerabilität als Wirkungskette zwischen Risikoexposition, Sensitivität und Resilienz darstellt. Im Zentrum steht dabei eine systemische Sicht auf wechselseitige Mensch-Umwelt-Interaktionen, die sehr starken Einfluss auf diese Wirkungskette und daher den Umgang mit Vulnerabilität haben. Auch Birkmann et al. (2010) legen das Ausmaß an Vulnerabilität anhand des Wechselspiels zwischen Risikoexposition und Bewältigungskapazität („Coping Capacity") fest. Ähnlich beziehen sich Sperstad et al. (2020) explizit auf die kritische Infrastruktur Stromnetz und stellen hier das Zusammenspiel zwischen Kritikalität[5] und Coping-Strategien als zentrale Wirkfaktoren von Vulnerabilität in den Vordergrund. Vulnerabilität bezieht sich systemisch betrachtet auf eine Zustandsänderung – hervorgerufen durch ein oder auch mehrere Ereignisse, die zu Problemen führen, die wiederum kritische Auswirkungen auf die Stabilität und Funktionsfähigkeit eines Systems haben. Im Kontext gesellschaftlicher Infrastrukturen ist die Frage wesentlich, wie anfällig die damit verbundenen Systeme für Ausfälle oder Störungen sind, die ihre Funktionsfähigkeit gefährden (vgl. Birkmann et al. 2010; Strauß/Krieger-Lamina 2017). Diese Anfälligkeit lässt sich mit verschiedenen Eigenschaften von Vulnerabilität näher beschreiben (Lenz 2009, S. 29ff.):

[5] Hier verstanden als gesellschaftliche Konsequenzen von Systemfehlern.

*Eigenschaften von Vulnerabilität*

- **Mehrdimensional:** Als mehrdimensionales Konzept hängt das Ausmaß von Vulnerabilität von unterschiedlichen, aber miteinander verbundenen Einflussfaktoren unterschiedlicher Dimensionen ab. Typischerweise sind das physische, soziale, ökonomische und ökologische Faktoren.
- **Objektbezogen:** Vulnerabilität ist immer bezogen auf ein Risikoelement in einem bestimmten räumlichen und strukturellen Kontext. Risikoelemente können einzelne Komponenten eines Infrastruktursystems sein, genauso Subsysteme, Prozesse, Anlagen, Sachgüter oder auch Menschen, die in irgendeiner Form in Infrastrukturen eingebunden sind.
- **Immanent:** Vulnerabilität ist ein fortwährender Zustand, egal, ob gerade eine unmittelbare Gefahr besteht oder nicht. Beispielsweise sind Schulkinder grundsätzlich vulnerabel gegenüber Verkehrsunfällen. Diese Gefahr lässt sich z. B. mit Sicherheitsmaßnahmen am Schulweg verringern, die Vulnerabilität besteht aber grundsätzlich.
- **Gefahrenspezifisch:** Manifest und sichtbar wird Vulnerabilität, wenn ein schädigendes Ereignis eintritt, das eine Auswirkung hat. Das können physische Schäden sein, aber auch weniger offenkundige Beeinträchtigungen (was gerade bei digitalen Systemen besonders relevant ist). Art und Ausmaß eines Ereignisses können dabei auf unterschiedliche Weise auf Risikoelemente wirken. Insofern lässt sich Vulnerabilität nicht per se ermitteln, weil sie immer kontextabhängig ist. Die Gefahrenart hat daher nur bedingt Einfluss auf das Vulnerabilitätsausmaß.
- **Skalenbezogen:** Die Einflussfaktoren hängen naturgemäß auch von der Skala der Betrachtung auf ein Risikoelement ab. Die Vulnerabilität eines gesamten Infrastruktursektors im nationalen oder internationalen Kontext ist natürlich von anderen Faktoren abhängig als eine technische Sichtweise auf einzelne Teile eines Infrastruktursystems. Deshalb sind unterschiedliche Betrachtungsebenen wichtig.
- **Dynamisch:** Vulnerabilität ist grundsätzlich keine statische Größe, sondern ein Zustand, der sich mit der Zeit und mit sich ändernden Einflussfaktoren verändern kann. Zum Beispiel können die Zunahme an Hitzewellen oder das Integrieren höherer Anteile von Solarenergie in bestehende Stromnetze einen Einfluss auf seine Vulnerabilität haben.

*Bewältigungskapazität wesentlich für Resilienz*

Für den vorsorgenden Umgang mit Vulnerabilität ist die Stärkung von Resilienz entscheidend, die ebenso je nach Disziplin unterschiedliche Bedeutungen haben kann. Allgemein bedeutet Resilienz Widerstandsfähigkeit (Turner 2003; Birkmann et al. 2010; Brinkmann et al. 2017). Systemisch ist Resilienz die Fähigkeit eines Systems, trotz Störung oder schädigendem Ereignis, seine Strukturen und Funktionen aufrechtzuerhalten (vgl. Turner et al. 2003). Wichtige Faktoren sind dabei die Einschätzung von Risiken und Vorsorge im Umgang damit. Im Bereich kritischer Infrastrukturen ist vor allem die Bewältigungskapazität wesentlich, um Resilienz zu stärken (Birkmann et al. 2010). Es gibt verschiedene, eng miteinander verknüpfte Indikatoren für die Bewältigungskapazität (Lenz 2009; Strauß/Krieger-Lamina 2017):

*Indikatoren für Bewältigungskapazität*

- **Robustheit:** Die Fähigkeit einer kritischen Infrastruktur, ihre Funktion trotz physischer Einwirkung eines Ereignisses mit Schadenspotenzial nicht zu verlieren. Typischerweise sind hier Natureinflüsse wie Unwetter gemeint. Art, Dauer und Intensität eines Ereignisses beeinflussen die Robustheit.
- **Pufferkapazität:** Fähigkeit, einem schädigenden Ereignis über eine bestimmte Dauer hinweg ohne Funktionsverlust standzuhalten. In der Energieversorgung ist Reserveenergie ein Beispiel für einen Puffer, der eingespeist wird, um Netzausfälle zu verhindern.
- **Abhängigkeit:** Die Funktionsfähigkeit einer Infrastruktur hängt von vielen Faktoren ab wie technischen, organisatorischen und ökonomischen Bedingungen. Einfluss haben aber auch die natürliche Umwelt oder andere Infrastruktursysteme.
- **Anpassungsfähigkeit:** Die Rahmenbedingungen (zum Beispiel rechtliche, geografische, wirtschaftliche, politische) haben Einfluss auf den Betrieb einer Infrastruktur. Gemeint ist hier ihre Fähigkeit, auch bei veränderten Rahmenbedingungen funktionsfähig zu bleiben.
- **Qualitätsniveau:** Der qualitative Zustand einer Infrastruktur beeinflusst ihre Funktionsfähigkeit. Klassische Beispiele sind Abnutzung und entsprechendes Vermeiden von Verschleiß durch regelmäßige Wartung, aber auch Sicherheitsvorkehrungen.
- **Schutzniveau:** Das relative Maß des Schutzes in Bezug auf eine bestimmte Gefahr.
- **Bereitschaft:** Inwieweit Vorbereitungen im Umgang mit Störungen und Ausfällen existieren (zum Beispiel Notfallpläne, Sicherheitskonzepte und Backup-Systeme).
- **Redundanz:** Existenz von Strukturen oder auch Ressourcen, die Leistungsausfälle unmittelbar kompensieren können (im Stromnetz sind das zum Beispiel doppelt geführte Leitungen).
- **Substituierbarkeit:** Ersetzbarkeit der Leistung einer Infrastruktur-Komponente bei Ausfall durch eine Alternative.
- **Transparenz:** Die Nachvollziehbarkeit der Funktionsweise und des strukturellen Aufbaus einer Infrastruktur und ihrer Komponenten.
- **Wiederherstellungsaufwand:** De**r (**zum Beispiel zeitliche, personelle, organisatorische, finanzielle) Aufwand, der betrieben werden muss, um eine Störung oder einen Ausfall zu bewältigen.

## 2.2 TECHNOLOGIE ALS UNTERSCHÄTZTER EINFLUSSFAKTOR

*Klassische Ansätze vernachlässigen technologische Einflussfaktoren*

All die genannten Eigenschaften und Faktoren für Vulnerabilität und Bewältigungskapazität gelten grundsätzlich auch für digitalisierte Infrastrukturen. Das klassische Verständnis von Infrastrukturen als relativ stabile, mehr oder weniger nahtlos mit gesellschaftlichen Strukturen und Abläufen verbundene Einheiten steht jedoch durch Digitalisierung auf dem Prüfstand. Das hat auch Auswirkungen auf das Verständnis von Vulnerabilität, was sich bereits durch den starken Fokus vulnerabilitätsorientierter Ansätze auf Mensch-Umwelt-Systeme zeigt, in denen Technik keine oder nur eine sehr untergeordnete Erwähnung findet. In den verschiedenen Modellen spielen daher technologische Einflussfaktoren und Risiken keine explizite Rolle. Das erschwert es, den Einfluss von Technologie auf Vulnerabilität analytisch zu erfassen. In Anbetracht einer angenommen weitreichenden digitalen Transformation der Gesellschaft kann das zu einem kritischen Versäumnis werden.

*Einseitiger Fokus auf Cybersecurity*

Es gibt zwar sehr viel Literatur über die digitalen Gefahren für kritische Infrastrukturen, allerdings ist das häufig auf Warnungen vor diversen Angriffen durch Hacker und Cyberkriminelle unter dem Schlagwort „Cybersecurity“[6] fokussiert (z. B. Lechner 2017; Dürig/Fischer 2018; Bitkom 2019). Das ist zwar nicht falsch, denn derartige Gefahren sind unbestritten ein wachsendes Problem. Trotzdem verstellt ein zu einseitiger Fokus auf diese Aspekte den Blick darauf, inwiefern und wodurch Digitalisierung selbst die Vulnerabilität von Infrastrukturen beeinflusst. Angriffe auf IT-Systeme sind dabei zwar kein unwesentlicher, aber dennoch nur ein Teilaspekt. Auch digitale Systeme können etwa durch technische Fehler, systemimmanente Schwachstellen oder Überlastung ausfallen.

Gerade moderne Softwaresysteme und deren Architekturen sind hochkomplex und ihre Integration in Infrastrukturen bringt zusätzliche Komplexität mit sich. Hinzu kommt der Trend, keine fertigen Softwareprodukte, sondern „minimal viable products“ (MVP) zu entwickeln (Nguyen-Duc 2020). Moderne Konzerne sowie auch Startups reduzieren so ihre Entwicklungskosten. Auch das Testen wird mitunter auf die Benutzer:innen ausgelagert und die Weiterentwicklung ist Teil des Geschäftsmodells. MVPs können daher auch eine höhere Fehleranfälligkeit aufweisen. Es ist also davon auszugehen, dass gesellschaftliche Infrastrukturen und ihr Betrieb durch Digitalisierung deutlich komplexer und fehleranfälliger werden. Dieser Aspekt ist derzeit nicht hinreichend in Vulnerabilitätskonzepten abgebildet. Im Kontext von Infrastrukturen ist Vulnerabilität daher bislang eine größtenteils „statische“ Größe, trotz des Komplexitätsanstiegs durch die Integration von digitalen Systemen, in denen eine andere Dynamik vorherrscht als in klassischen analogen beziehungsweise mechanischen Systemen.

[6] Früher geläufiger: Informationssicherheit oder IT-Sicherheit. Der Begriff Cybersecurity ist in der Sicherheitsforschung teils umstritten, weil er suggeriert, Gefahren lauerten „nur im Cyberraum“ und Sicherheit wäre hier etwas völlig anders als in der physischen Welt.

*Vulnerabilität wird durch Digitalisierung dynamischer und unberechenbarer*

Die Digitalisierung kann daher auch die Bedeutung von Vulnerabilität verändern und zu einer Art „Dynamisierung" von Vulnerabilität führen. Damit ist gemeint, dass die Faktoren, die Vulnerabilität beeinflussen, sich durch Digitalisierung verändern. Im klassischen Verständnis kann sich Vulnerabilität durch den Eintritt eines externen Ereignisses wie zum Beispiel eines schadenauslösenden Umwelteinflusses erhöhen. Das ist ein eher monokausales Verständnis, wo etwa ein sichtbarer Schaden entsteht, der dann eben je nach Bewältigungskapazität schnell oder langsam wieder behoben werden kann.

Bei digitalisierten Systemen kann dagegen auch Schaden entstehen, der nicht unmittelbar sichtbar ist; genauso kann ein sichtbarer Schaden entstehen, bei dem das Schadensereignis im Verborgenen bleibt. Beispiele sind vorhandene Schwachstellen, systemimmanente Fehler oder auch Hintertüren in Softwaresystemen, die im System schlummern und erst auffallen, nachdem sie ausgenutzt wurden. Das kann die Bewältigungskapazität erheblich verringern, weil mit dieser Art Schaden nicht gerechnet wurde. Fällt dann ein kritisches digitales System oder eine Komponente davon aus, fehlt es an der entsprechenden Schutzvorkehrung – und es kommt womöglich zum Totalausfall der gesamten Infrastruktur.

*Digitale Vernetzung kann Resilienz stärken, erhöht aber auch Ausfallrisiken durch Kettenreaktionen*

Digitalisierung bedeutet zudem stärkere Vernetzung. Das kann einerseits die Resilienz stärken, da so mehr Möglichkeiten entstehen, um bei Ausfällen eines Systems auf ein anderes umzustellen. Auch bieten digitale Systeme erhebliche Vorteile zur Verarbeitung von Messdaten: Betriebszustände kritischer Infrastrukturen wie zum Beispiel das Stromnetz können laufend in Echtzeit kontrolliert und analysiert werden. Das unterstützt Frühwarnsysteme und das Abwenden von Gefahren. So können kritische Systemzustände früher erkannt und Ausfälle verhindert werden (Alstone et al. 2015; IEA 2022a). Die Kehrseite ist jedoch ein erhöhtes Risiko für Kaskadeneffekte – also Kettenreaktionen: Der Ausfall eines Teilsystems oder einer kritischen Komponente kann über wechselseitige Abhängigkeiten im Gesamtsystem zu größeren Ausfällen führen. Zum Beispiel können auch einzelne kritische Ausfälle in Teilen der Dateninfrastruktur wie Server oder Cloud-Dienste, in Folge ganze Systeme zum Erliegen bringen – und enorme Schäden verursachen. In der Praxis gelten zwar für kritische Infrastrukturen wie dem Stromnetz besonders hohe Sicherheitsbestimmungen. Unter anderem ist Redundanz hier ein zentraler Faktor: Das sogenannte N-1-Sicherheitskriterium gewährleistet etwa, dass Ersatzkomponenten (zum Beispiel bei Stromleitungen) unmittelbar bei Störungen oder Schäden aktiviert werden, um das Risiko von größeren Ausfällen zu minimieren (vgl. Allhutter et al. 2022). Allerdings ist in der aktuellen Umbruchsphase unklar, ob diese klassischen Sicherheitsvorkehrungen auch bei der Digitalisierung hinreichend beachtet werden.

*Zentralisierung durch digitale Plattformen verstärkt Abhängigkeiten*

Die grundsätzlich dezentrale Struktur des Internets und digitaler Systeme im Allgemeinen kann zwar hilfreich sein. Das gilt jedoch nicht grundsätzlich, denn dieser allgemeine Umstand sagt noch nichts aus über die tatsächliche Beschaffenheit eines digitalisierten Infrastruktursystems und seiner sicherheitsrelevanten Redundanzen. Zudem ist die Digitalisierung in den vergangenen Jahren begleitet von erheblichen Zentralisierungstendenzen, insbesondere durch die zunehmende Bedeutung digitaler Plattformen. Die digitale Transformation ist daher auch ein Verstärker wechselseitiger Abhängigkeiten. Die zunehmende technologische und ökonomische Abhängigkeit von Infrastrukturen zu Technologieher-

stellern und ihren digitalen Plattformen wird besonders zum Problem, wenn es kaum Möglichkeiten gibt, das Sicherheitsniveau der Technologien zu erhöhen oder einzufordern (z. B. durch höhere Sicherheitsstandards und staatliche Regulierung).

*Digitalisierte Infrastrukturen sind intrusiver*

Digitalisierung verändert sukzessive auch die Bedeutung von Infrastrukturen in der Gesellschaft. Grundsätzlich sind Aspekte von Vulnerabilität seit jeher sehr eng mit der Sicherheit der Grundversorgung in der Gesellschaft und der Deckung von Grundbedürfnissen verbunden – wie eine stabile Versorgung mit Energie, Nahrung, Kleidung sowie Konsumgütern. Allerdings kann sich durch Digitalisierung auch das Anwendungsspektrum von Infrastrukturen erweitern, wenn zusätzliche Daten erfasst und verarbeitet werden. Neben ihrer Kernfunktionalität zur Grundversorgung entstehen so – verstärkt durch die datengetriebene Plattformökonomie – teils zusätzliche datenbasierte Anwendungen.

Dadurch sind digitalisierte Infrastrukturen intrusiver als klassische und wirken wesentlich stärker als bislang in Haushalte und die Sphären einzelner Personen hinein. Problembereiche auf institutioneller Ebene wie steigende ökonomische und technologische Abhängigkeiten, wirken sich daher zusehends stärker auch auf die individuelle Ebene aus. In Folge gewinnen auch grundrechtliche und ethische Aspekte wie Datenschutz und Datensicherheit, Schutz der Privatsphäre, Autonomie und Selbstbestimmung immer mehr an Bedeutung. Im folgenden Kapitel werden diese Problemfelder anhand von praktischen Beispielen in drei ausgewählten Bereichen herausgearbeitet.

# 3 ENTWICKLUNGSSTAND UND ZENTRALE PROBLEMFELDER AUSGEWÄHLTER BEREICHE

*Mehr Vernetzung, Flexibilisierung und Automatisierung*

Die Digitalisierung umfasst bereits ein breites Spektrum an Infrastrukturbereichen sowie damit verbundener Dienstleistungen und Anwendungen. Gemeinsame Nenner in allen Bereichen sind stärkere Vernetzung, Flexibilisierung, Automatisierung von Prozessen und Abläufen, um diese effizienter zu gestalten. Im Energiesektor sind unter anderem Smart Grids und Smart Meter ein zentrales Thema, im Mobilitätsbereich sind es digital vernetzte Fahrzeuge und auch in der Landwirtschaft werden zunehmend digitale Technologien eingesetzt (von Wetter-Apps, digitalen Sensoren, Drohnen bis zu automatisierten Anlagen).[7] So unterschiedlich diese Entwicklungen im Detail sind, so eng sind sie mit gemeinsamen technologischen Trends verbunden. Ein genereller Trend ist hierbei das Internet of Things (IoT). Hinter dem IoT steht die Vision einer umfassenden digitalen Vernetzung aller möglichen Systeme und Objekte in der Gesellschaft. Diese Vision ist keineswegs neu und wurde bereits in den 1990er Jahren mit anderen Buzzwords wie zum Beispiel „Ubiquitous Computing" (Weiser 1991) oder später „Pervasive Computing" oder auch „Ambient Intelligence" propagiert.

*Mobilfunk und Satellitensysteme gewinnen weiter an Bedeutung*

Schätzungen zufolge gibt es bereits heute etwa 14 Milliarden vernetzte Geräte weltweit, Tendenz steigend (Hasan 2022). Je nach Bereich sind damit weitere Trends verbunden wie zum Beispiel Industrie 4.0 oder cyber-physische Systeme im Industriesektor, oder spezifischer auf Hardware-Ebene das eng mit Mobilfunktechnologie verbundene Konzept Machine-to-Machine-Kommunikation (M2M) sowie die 5G-Technologie. Auch Satellitensysteme wie GPS gewinnen mit der Digitalisierung von Infrastrukturen als Teilsysteme an Bedeutung. Hierbei geht es nicht nur um Navigation, sondern immer mehr auch um automatisierte Steuerungen. Bereits heute werden solche Systeme etwa zur Zeitsynchronisation in Computersystemen, im Börsenhandel oder auch in Umspannwerken eingesetzt (vgl. Strauß/Krieger-Lamina 2017). Sie sind häufiger Bestandteil der digitalen Automatisierung (zum Beispiel bei selbstfahrenden Fahrzeugen, in Smart Grids oder Industrie 4.0). Mit dem Hype um künstliche Intelligenz und Machine Learning fließen auch diese Trends immer mehr in unsere Infrastruktursysteme ein.

Die von Digitalisierung betroffenen Bereiche verändern sich auf mehreren Ebenen: Auf institutioneller Ebene werden zum Beispiel Betriebs- und Steuerungsanlagen digitalisiert, um die damit verbundenen Prozesse zu optimieren, Messgenauigkeit von Betriebszuständen zu erhöhen und so weiter. Auf der Ebene von Haushalten und Privatpersonen sind es vor allem Anwendungen, die mit Infrastruktursystemen vernetzt sind, um etwa Haushaltsgeräte per Smartphone

[7] *www.bmel.de/DE/themen/digitalisierung/digitalisierung-landwirtschaft.html*; *www.idtechex.com/en/research-report/agricultural-robots-and-drones-2018-2038-technologies-markets-and-players/578*.

zu steuern. Zwischen diesen beiden Ebenen liegen Dateninfrastrukturen, die als Knotenpunkt fungieren, an dem mehrere Systeme miteinander verknüpft sind. Kern dieser Infrastrukturen sind oftmals Cloud Computing-Systeme und entsprechende Konzepte wie Software-as-a-Service (Saas), Infrastructure-as-a-Service (IaaS), Network-as-a-Service (Naas) oder Platform-as-a-Service (Paas) (Leimbach et al. 2014), sowie Edge Computing (vgl. z. B. Naveen 2016; Minh et al. 2022) relevant. Diese Konzepte werden dann je nach Bereichen adaptiert, zum Beispiel im Bereich Verkehr als Mobility-as-a-Service. Je nach technischer Gestaltung werden so einzelne Softwareanwendungen oder ganze Plattformen zum Bestandteil eines Infrastruktursystems. Insbesondere Plattformen gewinnen noch weiter an Bedeutung, was zu einer erheblichen Zentralisierung von digitalen Daten und Informationsflüssen führt.

*Cloud Computing, Servicemodelle und Plattformen*

Neben technologischen Veränderungen durch die Verzahnung zwischen physischen und digitalen Systemen kommt es auch zu ökonomischen Veränderungen: Die im Infrastrukturbetrieb generierten Daten lassen sich auswerten und darauf neue Geschäftsmodelle etablieren. Das geht bereits aus verschiedenen Cloud-Konzepten hervor, die allesamt als Servicemodelle konzipiert sind. Ein neuerer Trend sind dabei etwa Mikroanwendungen, bei denen Kund:innen neben einer Basisdienstleistung zusätzliche Anwendungen als Bezahlabo aktivieren können (wie etwa im Mobilitätsbereich). Auch im Energiesektor nehmen auf Verbrauchsdatenanalysen basierende Geschäftsmodelle zu.

Bereits seit einigen Jahren werden wachsende Sicherheitsprobleme sichtbar: Der Ausbau des IoT und vernetzter Geräte begünstigt Missbrauch und Angriffe. Schätzungen zufolge gab es allein im Jahr 2021 mehr als eine Milliarde Angriffe über IoT-Geräte, wobei Internetzugänge und Router eingerechnet sind (Cyrus 2021; SAM 2021). Die Aussagekraft solcher Zahlen ist zwar beschränkt, aber es ist evident, dass mit der Zunahme digital vernetzter Infrastrukturen auch Angriffe und kritische Systemfehler häufiger werden, wie sie Tabelle 1 exemplarisch darstellt. Die beschriebenen Fälle sind nur ein minimaler Auszug und dienen lediglich zur Veranschaulichung der breiten Palette von Attacken und Ausfällen.

*Mehr vernetzte Systeme und Sicherheitsprobleme*

**Tabelle 1: Auswahl an (Cyber-)Angriffen und kritischen Systemfehlern.**

| Vorfall | Bereich | Folgen |
|---|---|---|
| 2003: Softwarefehler begünstigt Blackout in Nordamerika.[8] | Energieversorgung | Verkettung von Alarmen, automatisierten Schutzschaltungen und ein Softwarefehler im Kontrollsystem bei Stromnetzbetreiber führt zu großflächigen Ausfällen. |
| 2016: Softwarefehler[9] und DDOS-Attacke[10] bei der Bank HSBC führt zu mehrfachen Systemausfällen. | Banken/ Finanzsystem | Kunden können weder ihre Kontostände überprüfen noch Überweisungen tätigen. |

8 *www.heise.de/newsticker/meldung/Software-Fehler-verursachte-US-Stromausfall-2003-93493.html*.

9 *www.businessinsider.com/hsbc-online-banking-down-reasons-and-compensation-2016-1*.

10 *arstechnica.com/information-technology/2016/01/hsbc-online-banking-suffers-major-outage-blames-ddos-attack/*.

| Vorfall | Bereich | Folgen |
|---|---|---|
| 2017: Großflächiger Cyberangriff mit Schadsoftware WannaCry[11] über verborgene Schwachstelle. | IKT, Verkehr, Gesundheitswesen, Logistik und andere | Weltweit über 230.000 Computer in 150 Ländern infiziert und Personen mit Lösegeldzahlungen erpresst. |
| 2017: Ausfall der Betriebssoftware am Flughafen Heathrow in Folge eines kurzen Stromausfalls.[12] | Luftfahrt | Zehntausende Passagiere bleiben über zwei Tage weltweit gestrandet. |
| 2017: Bauern in USA klagen gegen Gerätehersteller John Deere für das Recht ihre Traktoren selbst zu reparieren.[13] | Landwirtschaft | Durch die restriktiven Software-Settings bei neuen Landmaschinen können Landwirte diese nicht mehr eigenständig reparieren. |
| 2019: Die Biometrie-Datenbank einer globalen Firma für biometrische Zugangs-systeme ist ungeschützt im Internet.[14] | Staatliche und private Infrastrukturen | Rund 28 Millionen Datensätze samt Fingerabdrücken, Gesichtsbildern und Passwörtern sind offen zugänglich. |
| 2020: Cyberangriff über Solarwinds Plattform für Netzwerkmanagement.[15] | Staatliche und private Infrastrukturen | Datendiebstahl, Spionage, Manipulation von kritischer Software und daran gekoppelter Prozesse. |
| 2020: Erpressung mit Ransomware Uniklinik Düsseldorf.[16] | Gesundheitswesen | Krankenhausbetrieb massiv eingeschränkt. Patientin stirbt durch notwendiges Ausweichen auf eine andere Klinik. |
| 2020: Eindringen in SharePoint-Umgebung des europäischen Verbandes der Übertragungsnetzbetreiber.[17] | Energieversorgung | Die weit verbreitete Kollaborationssoftware ist nicht direkt mit den Betriebssystemen der Netzbetreiber verbunden. Keine weiteren Auswirkungen bekannt. |
| 2020: Ransomware Angriff auf kanadischen Energieversorger.[18] | Energieversorgung | Angreifer kompromittieren die Website und die Geschäftssysteme des Versorgers. Das E-Mail-System wird abgeschaltet. Die Stromsysteme sind nicht betroffen. |
| 2020: Ransomware legt Produktion bei Traktorenhersteller Fendt lahm.[19] | Landwirtschaft | Auswirkungen auf Produktionsanlagen weltweit, Geschäftsbetrieb für mehrere Tage gestört, tausende MitarbeiterInnen betroffen. |
| 2021: Ransomware-Attacke auf Funke Mediengruppe.[20] | Medienunternehmen | Mehr als einen Monat lang können viele der Funke-Zeitungen nur als Notausgabe erscheinen. |

11 *de.wikipedia.org/wiki/WannaCry*.
12 *www.zeit.de/2017/31/computer-software-fehler-systeme*.
13 *www.vice.com/en/article/xykkkd/why-american-farmers-are-hacking-their-tractors-with-ukrainian-firmware*.
14 Schaber et al. 2020.
15 *www.spektrum.de/news/solarwinds-ein-hackerangriff-der-um-die-welt-geht/1819187*
*www.wired.com/story/solarwinds-hack-supply-chain-threats-improvements/*.
16 *www.heise.de/news/Uniklinik-Duesseldorf-Ransomware-DoppelPaymer-soll-hinter-dem-Angriff-stecken-4908608.html*.
17 *www.entsoe.eu/news/2020/03/09/entso-e-has-recently-found-evidence-of-a-successful-cyber-intrusion-into-its-office-network/*.
18 *www.cbc.ca/news/canada/north/ntpc-apparent-ransomware-attack-1.5551603*.
19 *www.heise.de/news/Ransomware-laesst-bei-Traktorenhersteller-Fendt-die-Baender-stillstehen-7079945.html*.
20 *www.sueddeutsche.de/medien/cyberverbrecher-nrw-1.5763821*.

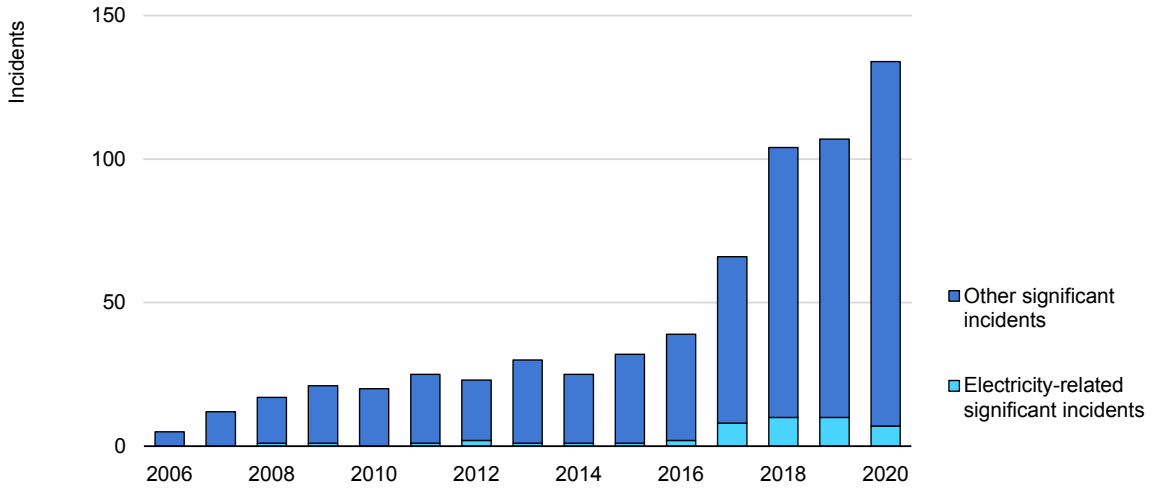
| Vorfall | Bereich | Folgen |
|---|---|---|
| 2021: Angriff auf Trinkwasserversorgung in Florida über kaum gesichertes, veraltetes IT-System.[21] | Wasserversorgung | Die Angreifer erhöhen den Anteil von Natriumhydroxid (Ätznatron) im Wasser. Der Vorfall wird rechtzeitig entdeckt und rückgängig gemacht. |
| 2022: Erpressung einer französischen Klinik mit Ransomware.[22] | Gesundheitswesen | Zugang zu Patientensystem unterbrochen, Notfallpatienten müssen teilweise abgewiesen werden. |
| 2022: Sabotage an Kabeln des Deutsche-Bahn-Funknetzes.[23] | Öffentlicher Verkehr | Über Stunden kurzfristige Zug- und Haltausfälle im norddeutschen Raum |
| 2022: Software-Fehlfunktion in Kartenzahlungssystemen von deutschen Supermärkten.[24] | Handel/ Bezahlsysteme | Kartenzahlungen bei Aldi Nord, Edeka und Netto über Tage nicht möglich. |
| 2022: 600 PCs der Bezirksbehörde des Rhein-Pfalz-Kreises durch Ransomware-Attacke lahmgelegt.[25] | Öffentliche Verwaltung | Regulärer Betrieb über ein halbes Jahr lang gestört. Schaden summiert sich auf 1,7 Million Euro. |
| 2022: Softwarefehler zwingt BMW, weltweit über 61.000 Pkws zurückzurufen.[26] | Verkehr | Möglicher Drehmomentverlust und Motorausfall durch fehlerhaftes Softwareupdate. |
| 2022: Cyber-Angriff auf Zugangssystem der Hochschule Heilbronn.[27] | Bildungswesen | E-Mail-System, VPN-Zugänge und E-Learning-Plattform über längere Zeit gestört. Verdacht auf Datendiebstahl. |

***Wachsende Anzahl kritischer Vorfälle im Stromsektor***

Obige Tabelle stellt nur eine lose Sammlung dar. Die Anzahl kritischer Vorfälle nimmt seit Jahren über alle Bereiche hinweg zu.[28] Das gilt auch für den besonders kritischen Stromsektor, wie die folgende Auswertung der Internationalen Energieagentur veranschaulicht (IEA 2021).

Insgesamt zeigt Abbildung 2 hier einen eindeutigen Anstieg. Dabei ist zu berücksichtigen, dass viele Angriffe, vor allem gegen Unternehmen, aus Furcht vor Imageschäden gar nicht gemeldet werden. Im Stromsektor ist interessant zu sehen, dass es vor 2016 kaum Vorfälle gab. Seitdem steigt die Zahl der Vorfälle. Im Jahr 2020 gab es zwar einen leichten Rückgang, der generelle Trend deutet aber auf eine weitere Zunahme hin.

21 *www.sueddeutsche.de/digital/it-sicherheit-hacker-wasserwerk-florida-1.5205113*.
22 *www.spiegel.de/netzwelt/web/frankreich-krankenhaus-weist-wegen-cyberattacke-notfallpatienten-ab-a-ed843e1a-7cdc-4236-9cdc-e34f55689775*.
23 *www.heise.de/news/Stoerung-bei-der-Deutschen-Bahn-in-Norddeutschland-Ausfaelle-von-Zuegen-7288474.html*.
24 *futurezone.at/digital-life/softwarefehler-bei-kartenzahlung-supermaerkten-verifone/402024108*.
25 *www.swr.de/swraktuell/rheinland-pfalz/ludwigshafen/neuer-stand-hackerangriff-100.html*.
26 *www.sueddeutsche.de/bayern/fahrzeugbau-muenchen-softwarefehler-bmw-muss-mehr-als-61-000-autos-zurueckrufen-dpa.urn-newsml-dpa-com-20090101-220526-99-442827*.
27 *www.golem.de/news/security-hackerangriff-auf-hochschule-heilbronn-2211-169444.html*.
28 Für aktuelle Fälle siehe auch *konbriefing.com/de-topics/cyber-angriffe.html*.






Note: "Significant" cyber incidents are defined as cyberattacks on government agencies, defence and high-tech companies, or economic crimes with losses of more than a USD 1 million.

**Abbildung 2: Anzahl gemeldeter Cyberattacken mit Verlusten größer als 1 Million US-Dollar – gesamt und auf die Stromversorgung bezogen (hellblau).**

Die Motive der Angriffe sind sehr unterschiedlich, sofern sie überhaupt bekannt werden. Häufig geht es um Lösegeldforderungen über Ransomware[29]. In den vergangenen Jahren aber mehren sich offenbar die Versuche staatlicher Akteure, gezielt kritische Infrastrukturen wie Energie- oder Wasserversorgung zu kompromittieren. Vor einigen Monaten wurde in Deutschland etwa eine groß angelegte Spionageoperation aus russischem Umfeld aufgedeckt, die mehr als 150 Unternehmen vor allem im Bereich kritischer Infrastrukturen zum Ziel hatte (Tanriverdi/Flade 2022). Wie in Tabelle 1 exemplarisch angeführt, sind neben Angriffen allerdings auch Softwarefehler, gravierende Sicherheitsmängel oder Stromausfälle Ursachen für Störfälle aller Art.

*Schwachstellen und Zero-Day-Exploits besonders problematisch*

Diese Entwicklungen und die generelle Zunahme an Cyberattacken sind besorgniserregend. Nicht außer Acht zu lassen ist aber auch, dass das Ausmaß an Vulnerabilität von Infrastruktursystemen nicht primär von externen Angriffen abhängt, sondern davon, wie robust, abgesichert oder anfällig die Systeme für Störungen, Ausfälle oder unberechtigte Zugriffe sind. Ein erhebliches Problem sind dabei sogenannte Zero-Day-Exploits[30]. Dabei werden Schwachstellen ausgenutzt, die dem Entwickler noch nicht bekannt waren, für die es also noch keine Lösung gibt in Form eines Patches (auch Sicherheitsupdate oder Aktualisierung genannt). Dabei kommt es immer wieder vor, dass auch Sicherheitsbehörden gezielt solche Zero-Day-Exploits einsetzen – wie das Beispiel „WannaCry" beweist. Hintergrund diesen Vorfalls ist ein ursprünglich vom US Auslandsgeheimdienst NSA jahrelang genutzter Zero-Day-Exploit namens „Eternal Blue". Dieser Exploit wurde am 14. April 2017 durch die Hacker-Gruppe „Shadow Brokers" öffentlich bekannt und die WannaCry Schadsoftware machte sich die Lücke im Mai 2017 zu Nutze – mit globalen Folgen. Microsoft veröffentlichte etwa einen Monat vor dem

*Beispiel „WannaCry" und globale Folgen*

[29] Ransomware missbraucht Verschlüsselung, um Systeme nicht mehr nutzbar zu machen.

[30] *en.wikipedia.org/wiki/Zero-day_(computing)*.

Leak einen Patch, was zu Spekulationen über mögliche Vorinformationen seitens der NSA führte (Hilary 2017; Nakashima/Timberg 2017; Trautman/Omerod 2019). Das Beispiel verdeutlicht: Wenn Systeme derartige technische Schwachstellen aufweisen, liegt es nahe, dass dies die Vulnerabilität erhöht und dass solche Schwachstellen auch früher oder später gezielt genutzt werden.

## 3.1 ENERGIEVERSORGUNG

Die Energiewende hin zu Erneuerbaren Energien bedeutet auch eine Flexibilisierung im Energiesystem zu kleinteiligeren und dezentraleren Strukturen (Bettin 2020). Von der Digitalisierung erhofft man sich hier eine effizientere Steuerung[31] der Energieversorgung (IEA 2022a, Alstone et al. 2015). Während die Digitalisierung somit auf der einen Seite den Wechsel zu umweltfreundlicher Energieerzeugung unterstützt, führt sie auf der anderen Seite zu mehr Energieverbrauch, insbesondere von Strom (IEA 2022b). Besonders deutlich wird das beim Phänomen der Kryptowährungen wie Bitcoins. Diese werden mittels Blockchain-Technologie „geschürft", also digital errechnet. Dieser Vorgang benötigt sehr viel Rechenleistung und ist deshalb sehr ressourcenintensiv. Dem Bitcoin-Electricity-Consumption-Index der Universität Cambridge zufolge betrug der Energieaufwand von Bitcoin im Jahr 2022 rund 108 Terawattstunden (TWh).[32] Zum Vergleich: Das entsprach etwa dem Nettostromverbrauch Nordrhein-Westfalens.[33]

*Effizienzgewinne, mehr Energieverbrauch und Abhängigkeiten*

Aber auch weniger spektakuläre Technologien erhöhen den Strombedarf, wie etwa das für Dateninfrastrukturen relevante Cloud Computing. Hier wird mit einem weiter steigenden Energiebedarf gerechnet, der Schätzungen zufolge allein in Europa bis 2025 auf mehr als 90 Terawattstunden pro Jahr ansteigen wird (Montevecchi et al. 2020). Nichtsdestotrotz besteht im Energiesektor erheblicher Bedarf, die Potenziale digitaler Technologien (etwa für das Lastmanagement und zur Schaffung flexiblerer Strukturen für erneuerbare Energiequellen) zu nutzen. Durch die Integration digitaler Technologien in Energienetze entsteht eine Art Energie-Informationssystem, da beide Bereiche immer weiter verschmolzen werden. Dadurch wird jedoch auch die wechselseitige Abhängigkeit weiter erhöht (Gheorghe et al., 2006). Teil des Wandels ist auch der wachsende Stellenwert sogenannter „Prosumenten" (Parag/Sovacool 2016). Dies sind Akteure, die sowohl Energieproduzenten sind (zum Beispiel über PV-Anlagen auf dem Dach) als auch Konsumenten. Somit wird die klassische Struktur von wenigen organisierten Produzenten und vielen Konsumenten aufgebrochen. Das führt dazu, dass nun immer mehr Akteure im Energiesektor zu finden sind. Diese vielen dezentralen Akteure müssen jedoch koordiniert werden, insbesondere im Strombereich. Denn hier ist es technisch notwendig, dass sich Erzeugung und Verbrauch stän-

*Mehr Komplexität im Gesamtsystem und Missbrauchspotenzial*

[31] Bisher wurde die Frequenzhaltung des Stromsystems durch die Schwungmassen von Großturbinen in Kraftwerken sichergestellt. Da ein Großteil dieser (fossilen) Kraftwerke zur Erreichung des 1,5-Grad-Ziels vom Netz genommen werden müssen, werden in Sekundenbruchteilen reagierende Systeme wie Grid-Booster diese Aufgaben übernehmen. Deren Ansteuerung ist nur digital in ausreichender Geschwindigkeit möglich.

[32] *ccaf.io/cbeci/index*.

[33] *www.energieatlas.nrw.de/energiestatistik/Pages/Content.aspx*.

dig die Waage halten, um die für den Netzbetrieb notwendige Spannung und Stromfrequenz zu halten. Eine Folge davon ist mehr Komplexität im Gesamtsystem. Die Koordination unterschiedlicher Komponenten innerhalb eines solchen Systems wird häufig „Smart Grid" genannt (Hirschl et al. 2018). Diese Koordination ermöglicht jedoch theoretisch Angriffsmöglichkeiten und Missbrauchspotential, wie im Weiteren erläutert wird (Cassotta 2019).

Ein weiterer Aspekt der laufenden Energiewende betrifft stärkere Umwelt-Einflüsse auf die von vielen Wetterfaktoren abhängigen Energie-Erzeugungsleistung (Windräder und Photovoltaik). Hier wird davon ausgegangen, dass sich der Verbrauch stärker an die Erzeugung anpassen muss. Verkürzt ausgedrückt: Wenn nicht ausreichend Erzeugungskapazitäten zur Verfügung stehen, zum Beispiel weil gerade kein Wind weht, sollen Konsumenten ihren Stromverbrauch anteilsmäßig reduzieren. So werden über Steuerungssignale große, aber zunehmend auch kleinere Verbraucher dazu angehalten, den Stromverbrauch anhand der Verfügbarkeit von Erneuerbaren auszurichten (Christensen et al. 2020). Das Steuerungssignal ist meistens der Preis. In Stunden mit wenig Erneuerbarer Energie wird der Stromverbrauch somit teurer.

***Zusammenhänge zwischen Energiewende und Digitalisierung***

Durch die genannten Vorbedingungen finden sich neue Akteure am Strom- und Energiemarkt, welche Erzeuger und Verbraucher als Intermediäre koordinieren – und meist auch von außen direkt lenken.[34] Dies ist in dieser Form ausschließlich durch die Digitalisierung möglich. Ein prominentes Beispiel sind hierfür die deutsche SONNEN und Next Kraftwerke, welche Nutzer:innen Batteriespeicher verkaufen, diese jedoch von außen über das Internet koordinieren.[35] Sie sind somit in der Lage, Regelenergie durch die Aggregation all dieser Speicher am Strommarkt für Regelenergie anzubieten (Sterner et al. 2019).

***Automatisiertes Lastmanagement und Verbrauchsmusteranalysen***

Die Koordinierung dieser Märkte, unterschiedlicher technischer Domänen und buchhalterischer Herausforderungen wird mit diversen Kommunikationsprotokollen durchgeführt, die häufig unzureichend geschützt sind (Qi et al. 2016; Hirschl et al. 2018). Außerdem werden immer mehr Messungen am Stromnetz über Internet-Plattformen gesammelt und verarbeitet. Dies dient dazu, Verbrauch und Erzeugung in Echtzeit zusammenzuführen – und somit Netzstabilität bei schwankender Erzeugung zu gewährleisten (Pearson 2011). Während diese Informationen bisher auf den jeweiligen Verteilernetz- oder Übertragungsnetzebenen separat durch Netzmessung und dem aggregierten Verhalten von Verbrauchern ermittelt wurden,[36] werden diese Echtzeitinformationen nun zunehmend an Netzbetreiber weitergeleitet. Dies bietet für eine Vielzahl an möglichen Marktakteuren Anreize, Effizienzgewinne zu erzielen. Hierbei geht es um zwei verschiedene Vorgänge, die getrennt werden sollten, obwohl sie in der Praxis gleichzeitig vorkommen: Zum einen das automatisierte Lastmanagement, das heißt die Reaktion der Verbraucher:innen auf externe Steuerungssignale, meistens in

[34] Siehe zum Beispiel die Erklärung des österreichischen Regulators E-Control: *https://www.e-control.at/aggregatoren*.

[35] *https://sonnen.de/presse/sonnen-und-next-kraftwerke-kooperieren-bei-lieferung-von-primaerregelleistung/*.

[36] Diese wurden dann mit bisherigem Nutzungsverhalten und typischen Lastkurven in sogenannten Normverbräuchen abgeglichen.

Form von Preissignalen. Zum anderen Verbrauchsmusteranalysen von Haushalten, aber auch von Gebäuden oder Quartieren, die mittels „maschinellen Lernens" erstellt werden. Bisher wurden die Prozesse der Energieinfrastruktur hauptsächlich durch sogenannte Supervisory-Control-and-Data-Acquisition-Systeme (SCADA) gesteuert – wie in vielen anderen Infrastrukturbereichen auch (Pearson 2011, Sajid et al. 2016). SCADA-Systeme aber haben eine gänzlich andere Funktion als die plattformbasierten digitalen Systeme, die nun eingesetzt werden (mehr dazu siehe Abschnitt 4.1).

Digitalisierung im Energiebereich wird auf unterschiedlichsten Akteursebenen verhandelt, weiterentwickelt und vorangetrieben. Erstens auf Haushaltsebene, zweitens auf Gebäude- oder Quartiersebene und drittens bei den (vor allem niederen) Netzebenen und Netzen. Bei Haushalten werden vermehrt digitale Messgeräte („Smart Meter") eingesetzt, die nicht nur den Strom und Energieverbrauch messen können, sondern ebenso die lokale Erzeugung, zum Beispiel durch Dach-Photovoltaik. Smart Meter sind eine Weiterentwicklung der traditionellen Stromzähler, die nun Echtzeitdaten über das Internet an externe Systeme weitergeben und auch von außen über diesen Weg angesprochen werden können. Eine zentrale Begründung für die Nutzung von Smart Metern liegt in der zeitnahen Information über tatsächliche Verbräuche von Haushalten, um somit von Seiten der Netzbetreiber durch effizientes, bedarfsgerechtes Lastmanagement reagieren zu können. Darüber hinaus sind sie in der Regel mit dem Internet verbunden und sind von außen kontrollier- und steuerbar(Pearson 2011). Über Steuerungseinheiten innerhalb eines Haushaltes können Geräte zentral angesteuert werden und dabei auch Preisinformationen mit dem tatsächlich erwartbaren Nutzverhalten zusammengebracht werden. Oder aber, die Haushaltsgeräte werden separat an- und ferngesteuert (in Verbindung mit weiteren Funktionen von Smart Geräten; siehe oben sowie Abschnitt 3.2).

*Smart Meter werfen Datenschutzfragen auf*

Das wirft Fragen des Datenschutzes auf: Denn mit Smart Meter entsteht etwa die Möglichkeit, von außen aus den Daten auf die An- oder Abwesenheit der Haushaltsmitglieder zu schließen sowie auf die Art der Geräte – und somit auch Schlüsse über Lebensumstände zu ziehen (Peissl et al. 2012). Während für die Nutzung von Smart-Meter-Daten prinzipiell die Zustimmung der Stromkund:innen Voraussetzung ist (ACER 2022), besteht immer die Gefahr, dass deren Wahlfreiheit durch die Verknüpfung verschiedener Zwecke oder durch Gebührenanreize behindert wird (Peissl et al. 2012).

Auf der Gebäude- und Quartiersebene kommen zusätzliche Steuerungssysteme zum Einsatz, manchmal „Building Information Model (BIM)" genannt. Diese koordinieren die verschiedenen Erzeuger (zum Beispiel Wärmepumpen, Wärmetauscher, Photovoltaik, oder Solarthermie) und Speicher (Niedrigtemperaturnetze sowie elektrische und thermische Speicher) mit den verschiedenen Geräten, die heizen, kühlen, lüften und Warmwasser bereitstellen. Hierbei werden Informationen zum Wetter, zur Gebäudebelegung (zum Beispiel über Dienstpläne oder $CO_2$-Messgeräte) und zu den Energiepreisen mittels Maschinellen Lernens miteinander verknüpft, um die Energie möglichst effizient und günstig zu nutzen (Ornetzeder et al. 2017).

*Effizienzgewinne durch Smart Grids auf verschiedenen Netzebenen*

Smart Grids finden sich aber nicht nur in einzelnen Gebäuden oder Quartieren, sondern werden auf den niederen Netzebenen – auch von den Verteilnetzbetreibern – ausgerollt. Ziel ist, die Netzstruktur möglichst effizient zu nutzen, und so weniger große Netzleitungen bauen zu müssen (IEA 2017, Ornetzeder et al. 2017). Obwohl die Hochspannungsnetze schon länger digitalisiert und „intelligent" gesteuert werden, gibt es noch Potential für Effizienzgewinne durch eine stärkere Verschränkung der unterschiedlichen Netzebenen. Dies zeigt sich auch in Initiativen wie der zunehmenden europäischen Zusammenarbeit auf der Verteilernetzbetreiberebene und der institutionellen Einbettung in neuen Organisationen wie der europäischen DSO Entity[37].

Während viele der Beispiele bisher eher theoretischer Natur sind, zeigt die aktuelle Entwicklung der Netzwerkcodes auf EU-Ebene, welche Geschäftsmodelle und Anwendungsformen in Zukunft ermöglicht werden sollen.[38] Ausgehend von diesen Entwicklungen lassen sich einige Abhängigkeiten und neue Problematiken herausstellen, die eine eingehende Beschäftigung auf politischer und gesellschaftlicher Ebene verlangen. Im Fall der Digitalisierung im Energiebereich sind dies die drei großen Themenbereiche Cybersecurity, ökonomische Abhängigkeiten und soziale Abhängigkeiten.

*Zentrale Problemfelder Cybersecurity, ökonomische und soziale Abhängigkeiten*

Unter dem Schlagwort Cybersecurity (siehe auch Abschnitt 2.2) lassen sich schon heute eine Reihe von Systemabhängigkeiten, Sicherheitsrisiken und neuen Angriffsvektoren ausmachen. Diese resultieren zum einen aus verstärktem Informationsaustausch als Hauptgrund für die zunehmende Digitalisierung und zum anderen aus der Vernachlässigung von Security-by-Design-Prinzipien (Hirschl et al. 2018). Viele zusätzliche vertiefende Abhängigkeiten lassen sich schon heute aufgrund von derzeit erarbeiteten rechtlichen Rahmen erahnen,[39] finden sich jedoch derzeit noch zu einem eher geringen Maße in der Praxis wieder. Auf institutioneller Ebene zielen die meisten Cyberattacken im Energiebereich derzeit auf die traditionellen Kraftwerksstruktur ab (siehe auch Tabelle 1 mit beispielhaften Ereignissen). Prominente Beispiele waren der Ransomware-Angriff auf die Colonial Pipeline in den USA im May 2021 sowie Malware-Angriffe auf deutsche Windkraftanlagen, auf amerikanische, niederländische und deutsche Terminals für Flüssiggas und Öl im Frühjahr 2022[40]. Die stärkere digitale Integration von unterschiedlichen Energiesystemkomponenten kann diese Art von Angriffen noch deutlich erleichtern – insbesondere, wenn hiermit bestehende Infrastrukturen einfach ergänzt und nicht neu gedacht werden (Pearson 2011; Hirschl et al.

*Digitale Komponenten im Energiesystem erhöhen Angriffsrisiken*

---

37 Eingerichtet durch die Electricity Regulation (EU) 2019/943 und – Stand 10.10.2022 – schon 906 teilnehmende Organisationen. *www.eudsoentity.eu*.

38 Eine Entwurfsversion des 2. Generation Netzwerkcodes zu Demand Response wurde im Juni 2022 von ACER zur öffentlichen Konsultation vorgelegt. ACER 2022 „Framework Guideline on Demand Reponse (Draft for public consultation)".

39 Bedeutsam ist die sich abzeichnende Regulierung im Framework Guideline on Demand Response, welche von der europäischen Agentur ACER im Juni 2022 zur öffentlichen Konsultation veröffentlicht wurde.

40 Siehe weitere Informationen zu den Angriffen, hier *www.weforum.org/agenda/2022/02/cyberattack-amsterdam-rotterdam-antwerp-energy-sector/*, hier *www.washingtonpost.com/technology/2022/04/13/pipedream-malware-russia-lng/* und hier *www.ft.com/content/4d38e508-6b0a-4074-8978-3feca795a90f*.

2018). die Cyberangriffe auf das ukrainische Stromsystem im Jahr 2015 verdeutlichten bereits die Vulnerabilitäten.[41] In Zukunft ist aufgrund der stärkeren Integration digitaler Komponenten in bestehende Infrastruktursysteme ohne gesamtheitliches Schutzkonzept mit steigenden Vulnerabilitäten zu rechnen.

*Kritische Netzwerkeffekte erfordern höheres Sicherheitsniveau*

Mit dem großflächigen Ausrollen von Smart Metern in Europa und der Implementierung von Nachfragemanagement auf nationalen Ebenen entsprechend der EU-Vorgaben können weitere Probleme entstehen. Das gilt insbesondere für Sicherheit und Datenschutz, die im Zusammenhang mit der relativ langsamen Verbreitung mitunter als Hindernis dargestellt werden. In Deutschland wurde etwa im Januar 2023 das Gesetz zur Einführung von Smart Metern vereinfacht, um die Umsetzung zu beschleunigen. Das betrifft unter anderem die Zertifizierung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI), die zwar bestehen bleibt, aber vereinfacht werden soll.[42] Standardisierte Produkte und Geräte sind wichtig, um ökonomische Skaleneffekte zu erreichen.[43] Aus Sicherheitsperspektive wird dadurch jedoch grundsätzlich auch der Aufwand für Angreifer erheblich vereinfacht (Pearson 2011). Diese Geräte sind zudem leicht physisch erreichbar, da sie direkt in vielen Haushalten eingesetzt werden. Verstärkt werden die kritischen Netzwerkeffekte, durch die Nutzung des Internetprotokolls (IP) und durch die Vernetzung mit anderen Systemen (zum Beispiel dem Stromtransport). Zudem gibt es einen viel größeren Kreis von Nutzer:innen und Stakeholdern und somit mehr Angriffsvektoren. Die auftretenden Vulnerabilitäten sind dann jedoch nicht mehr nur institutioneller Natur, sondern betreffen genauso einzelne Individuen. Ein angemessenes Sicherheitsniveau ist daher wichtig, um das Risiko zunehmender Vulnerabilität gering zu halten.

Dem Thema Cybersecurity sind nicht nur mutwillige Angriffe zuzuordnen, sondern ebenso Softwarefehler, die akkumuliert ein gesamtes System zusammenbrechen lassen können (Hirschl et al. 2018). Ein eindrückliches Beispiel, was so ein Softwarefehler auslösen kann, stammt bereits aus dem Jahr 2003: Damals blieben acht Staaten im Nordosten der Vereinigten Staaten sowie Teile Kanadas für fünf Tage ohne Strom.[44] In Europa verursachte 2013 ein Softwarefehler erhebliche Probleme, die beinahe zu gravierenden Stromausfällen führten. Eine simple Gaszählerabfrage aus dem Leitsystem des süddeutschen Gasnetzes brachte Österreichs Stromnetz erheblich in Gefahr. Denn die Zählerabfrage übertrug sich ins Leitsystem des europäischen Stromnetzes fort, das offenbar dieselben Steuerprotokolle verwendete. Die Abfrage löste eine Flut von Abfragen und Antworten aus, die in Folge das österreichische Leitsystem überlastete, das somit stunden-

41 *www.cisa.gov/uscert/ics/alerts/IR-ALERT-H-16-056-01*.

42 *https://www.golem.de/news/smart-meter-rollout-wenn-der-installateur-keine-hochsicherheitsbox-mehr-braucht-2210-169190.html*; *https://www.hausundgrund-verband.de/aktuelles/einzelansicht/bundesregierung-beschleunigt-umruestung-auf-smart-meter-6423/*.

43 Was die aktuell geplante Regulierung sogar explizit begrüßt. Siehe wieder ACER 2022.

44 Eine Kombination von Ereignissen und Alarmen sorgte dafür, dass das System dien Dienst einstellte. Mehr: *www.heise.de/newsticker/meldung/Software-Fehler-verursachte-US-Stromausfall-2003-93493.html*.

lang nicht angemessen auf Lastschwankungen reagieren konnte.[45] Nicht nur das Stromsystem ist für Softwareprobleme anfällig. Am 1. Januar 2022 führte etwa ein Softwarefehler für mehrere Tage zum Ausfall der Warmwasserversorgung in einer Reihe von Haushalten im österreichischen Bundesland Kärnten (Proschofsky 2022).

*Institutionelle Pfadabhängigkeiten und Folgen für Haushalte*

Ökonomische Abhängigkeiten auf systemischer/institutioneller Ebene ergeben sich vor allem aus Pfadabhängigkeiten beziehungsweise Lock-Ins (vgl. u. a. David 1985; Werle 2007). Dies bedeutet, dass es schwer möglich ist, von einem einmal gewählten technologischen Entwicklungspfad wieder abzuweichen. In unserem Kontext bedeutet es, dass sich bestehende Abhängigkeiten von digitalen Technologien in der Energieversorgung tendenziell eher weiter fortschreiben. Dementsprechend sind diese Abhängigkeiten auch auf individueller Ebene sichtbar. Das mussten zum Beispiel Stromkunden in Colorado im Jahr 2022 erleben: Dort konnten Kund:innen in 22.000 Haushalten ihre vernetzten Thermostate für eine Stunde nicht verstellen. Sie hatten einen vergünstigten Tarif gebucht, der sie im Kleingedruckten dazu verpflichtete, in Fällen von ungenügender Energieverfügbarkeit ihre Thermostate fernsteuern zu lassen.[46] Während das aus Perspektive des Stromsystems sinnvoll ist, bedeutet das zugleich, dass Nutzer:innen mit geringerem Einkommen eher gezwungen sind, Tarife mit solchen Einschränkungen abzuschließen, die sie nötigen, ihre Nachfrage dem Preis anzupassen; all jene also, die sowieso eher von Energiearmut betroffen sind (Peissl et al. 2012).

*Neue Geschäftsmodelle und stärkere Kundenbindung*

Ein weiteres Beispiel für ökonomische Abhängigkeiten findet sich in dem oben erwähnten Geschäftsmodell, wobei Hersteller von Geräten zur Stromerzeugung, Energiespeichern und sonstiger Energietechnik wie die deutschen SONNEN oder Senec auch gleichzeitig als Stromanbieter auftreten. Darüber hinaus ermöglichen sie zudem noch den Handel mit Strom zwischen ihren Kunden:innen über die eigene Plattform. All dies führt dazu, dass diese immer stärker in das proprietäre Ökosystem dieser Anbieter eingebunden werden. Durch die vereinfachte Abwicklung all ihrer Energiebedürfnisse über einen externen Dienstleister und Hersteller wird Kundenbindung hergestellt, mit der Gefahr eines ökonomischen Lock-ins, das einen späteren Wechsel, zum Beispiel im Fall von steigenden Kosten, stark erschwert.

*Soziale Abhängigkeiten, Datenschutz und Lebensqualität*

Weitere soziale Abhängigkeiten, die sich aus der Digitalisierung im Energiebereich für Individuen und Haushalt ergeben, betreffen Grundrechte und Selbstbestimmung. Energieverbrauchsdaten beinhalten viele sensible Informationen über das private Leben und Verhalten und berühren daher den Datenschutz (Peissl et al. 2012). Inwieweit der technisch gewährleistet werden kann und gleichzeitig möglichst viele Verbrauchsdaten nutzbar sind, ist jedoch noch weitgehend unklar.[47] Auch haben solche Preismodelle direkten Einfluss auf die Lebensqualität: In aktuellen Versuchen wurde Stromkund:innen durch Ampelsysteme angezeigt, wann der Stromverbrauch besonders günstig ist. Die Auswertung zeigte, dass

---

45 Mehr hier: *www.heise.de/newsticker/meldung/Chaos-im-Stromnetz-durch-verirrte-Zaehlerabfrage-1865269.htm lfm4v3.orf.at/stories/1717900/index.html*.

46 Siehe *www.heise.de/news/Vernetzte-Thermostate-in-Hitzewelle-ferngesteuert-Amerikaner-schockiert-7255410.html*.

47 All dies hängt wieder von der genauen regulatorischen Ausgestaltung ab.

diese ihr Verhalten so stark anpassen, dass sie sich permanent überwacht und kontrolliert fühlen – und in ihrem Wohlbefinden eingeschränkt (Christensen et al. 2020).

Zusammenfassend lässt sich für die Auswirkung der Digitalisierung im Energiesystem sagen, dass in der Europäischen Union durch kommende gesetzliche Regelwerke und technischen Rahmen eine ganze Reihe von neuen Geschäftsmodellen und Anwendungsfeldern entstehen werden, die weitere Herausforderungen mit sich bringen. Abschnitt 3.2 geht noch näher auf die Problematik mit Geräten in Haushalten ein.

## 3.2 MOBILITÄT UND VERKEHR

Auch im Bereich Mobilität und Verkehr wird die Verbindung zwischen Digitalisierung und Energiewende deutlich sichtbar. Die schrittweise Abkehr von Verbrennungsmotoren und die steigende Verbreitung von Elektrofahrzeugen bedeutet sowohl mehr Bedarf an flexibel verfügbarem Strom als auch eine Zunahme digital vernetzter Fahrzeugsysteme. Neben neuen Strategien zur Dekarbonisierung verfolgt die Automobilindustrie auch Digitalisierungsstrategien (PWC 2017; Beutler et al. 2021). Das ist zum Teil dem steigenden Marktdruck durch neue Konkurrenten im Mobilitätssektor geschuldet. Prominentestes Beispiel hierfür ist Tesla, aber auch andere große Technologiekonzerne wie Alphabet/Google, Apple oder auch Amazon entwickeln eigene E-Fahrzeuge. Auch chinesische Hersteller wie Nio oder BYD haben bereits Modelle für den europäischen Markt (Ulrich 2022). Anpassungsdruck zu mehr Digitalisierung kommt zudem auch von großen Softwarekonzernen, die Mobilität als Teil ihrer Marktstrategie in der digitalen Transformation erschließen wollen. Für diesen Zweck werden dann entsprechende Konzepte für möglichst nahtlose Daten-Infrastrukturen entwickelt, die unter anderem (in Anlehnung an das Cloudcomputing-Konzept Software-as-a- Service – SaaS) auf Mobility-as-a-Service (MaaS) setzen (IBM 2022; Krauss et al. 2022).

*Starker Marktdruck zur Digitalisierung und neue technologische Abhängigkeiten*

Der digitale Wandel im Mobilitätssektor bringt eine Reihe von Herausforderungen: Hersteller sind zusehends abhängig von digitalen Technologieherstellern wie Plattformbetreibern. Es kommt dadurch auch zu einer strukturellen Veränderung des Automobilsektors, bei der Technologieunternehmen mehr Marktmacht erlangen. Von dieser Seite wird der technologische Wandel mit Marketing-Strategien unter anderem mit Schlagwörtern wie ACES (Autonomous, Connected, Electric and Shared) umworben.[48] Durch den Mangel an digitalem Knowhow entstehen hier auf Herstellerseite neue technologische Abhängigkeiten. Hardwareseitig werden neue Chips benötigt[49], und softwareseitig sind Fahrzeuge zusehends mit wesentlich mehr und komplexeren digitalen Systemen ausgestattet und vernetzt. Hersteller sind auf eine Reihe von Kooperationen mit Hard- und Softwareherstellern angewiesen.

[48] Zum Beispiel *www.t-systems.com/at/de/branchen/automotive*.

[49] Dass ein Mangel hier kritisch ist, hat sich auch in der Corona-Pandemie und Engpässe in globalen Lieferketten gezeigt.

BMW und Mercedes kooperieren etwa mit Chipherstellern wie Nvidia und Qualcomm. Viele Hersteller setzen entweder ganz auf externe Fahrzeugbetriebssysteme wie Apple Car, Android Automotive oder nutzen deren Systeme für die Infotainment-Konsolen im Fahrzeug (zum Beispiel Apples CarPlay oder auch Amazons Echo Auto) (Hubik et al. 2022). Dadurch gewinnen Technologiehersteller weiter an Einfluss und erhalten viele neue Möglichkeiten zur Generierung von Daten. Ein weiterer wesentlicher, aber weniger offenkundiger Bestandteil der digitalen Vernetzung sind satellitenbasierte Systeme. Bislang werden damit vor allem GPS-basierte Navigationssysteme für Fahrer:innen assoziiert. Die steigende Relevanz betrifft aber nicht nur die Navigation, sondern auch neue Möglichkeiten der Fahrzeugsteuerung und Kontrolle – auch in Hinblick auf das automatisierte Fahren (TB 2017; EUSPA 2022). Eng damit verbunden ist die Mobilfunktechnologie 5G, die für den Datenaustausch zwischen Fahrzeugen (sogenannte Car2Car Communication oder Car2X für generell vernetzte Fahrzeuge) genutzt wird (Pillau 2021). Die damit verbundenen Problemfelder wie Sicherheit und Datenschutz werden politisch bislang kaum thematisiert.

*Technologiehersteller gewinnen durch vernetzte Systeme an Einfluss*

Die Digitalisierung von Fahrzeugen hat sowohl Folgen für die Systemsicherheit der Fahrzeuge und die dahinter liegende Infrastruktur als auch für die Sicherheit und Privatsphäre auf individueller Ebene: Die für E-Fahrzeuge notwendige Energieinfrastruktur hat völlig andere Anforderungen als das derzeit dominierende Tankstellensystem. Stromtankstellen und Ladestationen benötigen flexiblere Energieversorgungsnetze (Ornetzeder et al. 2017) und sind ohne digitale Systeme kaum noch nutzbar. Besonders vulnerabel sind die Steuerungssysteme der Ladestationen[50], die für Lade- und Bezahlvorgänge sowie für Systemwartungen mit dem Internet verbunden sind. Sicherheitsforscher deckten erhebliche Schwachstellen und Mängel in solchen Ladesystemen und ihren Komponenten auf, die sehr leicht missbraucht werden können: Teilweise fehlen Schutzvorkehrungen völlig oder sind sehr leicht zu umgehen, wodurch ganze Ladesysteme kontrolliert und manipuliert werden können. Die Angriffsmöglichkeiten reichen hier vom Fernzugriff für Datendiebstahl bis zur Manipulation der Ladeleistung, die durch gezielte Störungen des Ladebedarfs sogar die Stabilität des Stromnetzes gefährden könnten (PTP 2021). Viele dieser Probleme sind bereits seit Jahren bekannt (Vaas 2013), die Risiken bestehen aber offenbar nach wie vor und nehmen mit steigendem Ausbau unzureichend geschützter Systeme weiter zu.

*Digitalisierte Fahrzeuge haben Sicherheitsmängel und bringen neue Angriffsformen*

Auch die Sicherheit der Fahrzeuge selbst und damit ihrer Besitzer/Nutzer:innen ist durch digitale Schwachstellen gefährdet. Aktuelle Fahrzeugsysteme verfügen bereits über digitale Infotainment-Konsolen genauso wie über digitale Komponenten und Sensoren zu Fahrzeugsteuerung, Messungen von Tankfüllung oder Batteriestatus – und sind mit der Dateninfrastruktur[51] des Herstellers vernetzt. Damit besteht eine hohe technologische Abhängigkeit zu externen Systemen.[52] Die verschiedenen Systeme sind zudem oftmals technisch unsauber voneinander

*Hohe Abhängigkeit zu externen Systemen*

50 Im Fachjargon auch EVCSMS – Electronic Vehicle Charging Station Management System.

51 Zum Beispiel SaaS/Cloud, *www.digital-manufacturing-magazin.de/digitalisierung-in-der-automobilindustrie-das-sind-die-trends/*.

52 Beim Cloud Computing wird die hohe Abhängigkeit zu einem Betreiber und das damit verbundene Problem der Alternativlosigkeit auch als „Vendor Lock-In" bezeichnet.

getrennt. 2021 führte etwa ein Server-Ausfall der Cloud-Infrastruktur bei Tesla dazu, dass einige Fahrzeugfunktionen für mehrere Stunden inklusive der Schlüssel-App nicht mehr nutzbar waren (Futurezone 2021). Außerdem gibt es zahlreiche Varianten, um Fahrzeuge über digitale Systeme zu hacken, die von Zugriffen über im System verbaute Mobilfunk- oder Bluetooth-Schnittstellen (Presse 2011; Harder 2014) über digitale Autoradios (Diedrich 2015) bis zum digitalen Fahrzeugschlüssel oder der entsprechenden Smartphone-App reichen. 2015 kam es bei Fiat-Chrysler zu einer groß angelegten Rückrufaktion von 1,4 Millionen Autos aufgrund eines Hacks, über den das Fahrzeug fernsteuerbar wurde (Schesswendter 2015). Ein Sicherheitsexperte fand Anfang 2022 eine kritische Schwachstelle in Tesla-Fahrzeugen, über die er Fernzugriff auf 25 Fahrzeuge in unterschiedlichen Ländern erhielt (Nedelea 2022).

Neben Autos betrifft die Digitalisierung auch öffentliche Verkehrsmittel wie Züge, U-Bahnen oder Busse. Über digitale Anwendungen lässt sich etwa die Anzahl von Reisenden dynamisch erfassen, um die Steuerung in Verkehrsleitzentralen effektiver zu gestalten. Auch die digitalen Systeme im öffentlichen Verkehr (Fahrkarten- ebenso wie Verkehrskoordinationssysteme) sind anfällig für Sicherheitsvorfälle und Angriffe von außen (Ivanova 2022). Beispielhaft sei hier der Diebstahl von Kundendaten über ein Fahrkartensystem bei den Schweizer Bundesbahnen Anfang 2022 genannt (SWI 2022). Einen weiteren bedeutsamen Hack auf ein zentrales IT-System meldete 2022 Go-Ahead, der größte Betreiber von Bussen im Vereinigten Königreich (Kollewe 2022).

***Sicherheits- und Datenschutzprobleme verschärfen sich***

Aus Sicht von Kund:innen problematisch ist zudem der schrittweise Zwang zur Nutzung und Vernetzung digitaler Anwendungen wie Smartphone-Apps. Zum einen können solche Apps zum Sicherheitsproblem werden: Erst kürzlich wurde demonstriert, wie über eine Sicherheitslücke in der Tesla-App relativ einfach Nachschlüssel für Tesla-Fahrzeuge generierbar sind (Standard 2022a). Zum anderen erhöhen sie die technologische Abhängigkeit der betroffenen Person, die so schrittweise verleitet wird, eine Smartphone-App zu nutzen, um das eigene Auto nutzen zu können. Das verschärft die Datenschutzproblematik, da über Apps meist auch personenbezogene Daten zur Profilbildung erfasst werden. Das gilt insbesondere für integrierte externe Systeme, die sehr viele personenbezogene Daten sammeln.

***Datensammlungen und Tracking nehmen zu***

Zum Beispiel setzen einige Hersteller bereits auf Systeme wie Google Assistant oder Amazon Echo zur Sprachsteuerung im Fahrzeug[53]. Im Hintergrund fließen so auch Daten der Fahrzeugnutzung in die jeweiligen Benutzerprofile der Betroffenen. Auch im öffentlichen Verkehr werden immer häufiger Apps genutzt, die je nach Bereich deutlich mehr Daten sammeln als für den Zweck erforderlich. Datenschützer kritisierten kürzlich etwa die Navigator-App der Deutschen Bahn, die Tracking betreibe und Nutzer:innen-Daten auch an externe Dienstleister weitergebe. Die Bürgerrechtsorganisation Digitalcourage reichte im Oktober

[53] Zum Beispiel Mercedes-Benz *www.mercedes-benz.at/passengercars/being-an-owner/mercedes-me-connect.pi.html/being-an-owner/mercedes-me-connect/mercedes-me-connect-products/third-party-interface*.

2022 Klage[54] gegen die DB-Vertriebsgesellschaft ein. Begründet wird der Schritt unter anderem damit, dass die App ohne Zustimmung mehrere Verbindungen zu kommerziellen Drittanbietern herstelle, darunter auch die Adobe Marketing Cloud, die so Daten Reisender für Trackingzwecke erlange. Es liege somit ein Verstoß gegen die Datenschutzgrundverordnung vor. Die DB weist den Vorwurf zurück, die Klage ist noch anhängig (Krempl 2022b).

*Erfassung biometrischer Daten besonders kritisch*

Das Problem von möglichen Datenschutzverstößen und Eingriffen in die Privatsphäre ist besonders ausgeprägt bei Apps, die unterschiedliche Mobilitätsbereiche wie Bahn, Mietwagen und Taxis miteinander kombinieren und potenziell auch personenbezogene Daten zwischen diesen Services austauschen (Creutzig 2021). Noch kritischer wird es, wenn auch biometrische Daten erfasst werden. Biometrie nimmt generell zu, speziell über das Smartphone und diverse Apps (Schaber et al. 2020) – und mittelfristig sollen auch bei Fahrzeugen biometrische Merkmale als Schlüsselersatz genutzt werden[55]. Das kommt einem Zwang zur Identifizierung zur Fahrzeugnutzung gleich. Zudem ist davon auszugehen, dass besonders sensible biometrische Daten sowohl von Herstellern als auch von externen Technologie-Dienstleistern verarbeitet werden – und das häufig nicht lokal, sondern über Cloud-Infrastrukturen. Das bringt gerade bei biometrischen Daten erhebliche Datenschutz- und Sicherheitsprobleme mit sich und erhöht das Risiko von Identitätsdiebstahl.

*Digitale Automatisierung und Fernzugriffe erhöhen Missbrauchsgefahr*

Ein weiterer Aspekt betrifft die digitale Automatisierung. Im Bereich globaler Lieferketten ist das bereits weit fortgeschritten. Digitale Systeme werden genutzt, um jederzeit nachvollziehen zu können, wo sich welche Güter befinden und um deren weiteren Weg zu planen und zu koordinieren. Dazu werden zunehmend auch Anwendungen aus dem Bereich KI/Machine Learning genutzt (Ahmed/Rios 2022). Inzwischen dienen sie auch der direkten und indirekten Steuerung von Güterschiffen. Diese können inzwischen teils sogar ferngesteuert werden. Entweder um das Personal an Bord zu unterstützen oder sogar teilweise einzusparen. Das bedeutet ganz neue Angriffspunkte für Cyberattacken. Während die häufigste derzeit noch die Hafenanlagen sind, ist auch ein Angriff auf Schiffe selbst denkbar, zum Beispiel um sie vom Kurs abzubringen. Im Jahr 2022 wurde zum Beispiel das globale Logistik-Unternehmen Hellmann aus Osnabrück über eine Phishing Attacke erfolgreich gehackt (Shead 2022).

Im Individualverkehr hat der Trend zur Automatisierung der Fahrzeugsteuerung („autonomes" Fahren) auch Effekte auf die Sicherheit der Fahrzeuginsassen. Es gibt eine steigende Anzahl an Unfällen mit Autopilotsystemen, wie auch eine Untersuchung der US Verkehrssicherheitsbehörde belegt. Im Jahr 2021 gab es etwa knapp 400 gemeldete Unfälle mit Beteiligung von Autopilotsystemen verschiedener Hersteller, 273 davon bei Tesla (Krisher 2022; Siddiqui et al. 2022).

---

[54] Die Klagschrift im Wortlaut: *https://media.kuketz.de/blog/artikel/2022/db-navigator/Klage-Deutsche-Bahn_20.10.2022.pdf*.

[55] Siehe zum Beispiel *www.golem.de/news/hyundai-fingerabdruck-startet-auto-1812-138409.html*; *https://www.industr.com/de/autos-mittels-iris-scan-und-gesichtserkennung-entriegeln-2355771*.

*Softwareprobleme können Unfallgefahr erhöhen*

Neben einer Reihe von Auffahrunfällen mit Teslas (Standard 2022b) sind auch bereits mehrere Fälle dokumentiert, bei denen Personen ums Leben kamen (Wilkens 2022). Zudem gibt es immer wieder kritische Probleme: Im September 2022 kam es etwa zu einer Rückrufaktion aufgrund eines Prozessorfehlers, der zu Überhitzung und automatischer Schutzabschaltung des Fahrerdisplays in Teslas führen kann (Abrahamczyk 2022). Zwar sind vereinzelte Rückrufaktionen bei Fahrzeugen nicht ungewöhnlich, allerdings scheinen die Vorfälle bei digitalisierten Fahrzeugen zuzunehmen. Weitere Beispiele sind Phantombremsungen in Folge eines Softwareupdates im Jahr 2021 und der damit verbundene Rückruf der Beta-Version von Teslas System zur vollständigen Fahrautomatisierung aufgrund fehlerhafter Kollisionswarnungen (davon waren über 360.000 Fahrzeuge betroffen[56]). CEO Elon Musk beschwichtigte den Vorfall mit der Aussage, das wäre normal bei Beta-Software und es wäre unmöglich, alle Hardwarefunktionen bei internen Qualitätstests zu überprüfen.[57] Es ist allerdings fraglich, ob der reale Straßenverkehr mit echten Menschen eine geeignete Testumgebung für Beta-Software ist. Musks Argumentation verdeutlicht, welche Probleme entstehen können, wenn neue Akteure mit ihren eigenen Marktlogiken in andere Bereiche hineinwirken, die stärkere Regulierung erfordern, wie hier das Beispiel Automobilsektor zeigt.

*Steigende ökonomische und technologische Machtstellung durch neue Geschäftsmodelle*

Ein zentrales Problemfeld ist die steigende ökonomische und technologische Machtstellung durch neue Geschäftsmodelle, die zu mehr Abhängigkeit und Kontrollverlust auf individueller Ebene führen können. Die steigende Abhängigkeit zu digitalen Systemen hat Auswirkungen auf den Lebenszyklus der Fahrzeuge und von integrierten Systemen. Hersteller erlangen über die digitalen Systeme zum Beispiel Möglichkeiten zum Fernzugriff. Das bringt neben Vorteilen etwa zur erleichterten Wartung von Systemen durch Einspeisung notwendiger, sicherheitsrelevanter Software-Updates auch erhebliche Probleme mit sich. Einige Hersteller etwa nutzen die Digitalisierung für neue Abo-Modelle, um softwarebasierte Anwendungen im Fahrzeug nur gegen Aufpreis freizuschalten. BMW verlangt zum Beispiel 17 Euro monatlich für die Sitzheizung oder 390 Euro für eine dauerhafte Freischaltung, wobei dies unter dem Vorbehalt erfolgt: „Solange die technischen Voraussetzungen für das Fahrzeug gegeben sind." Ähnliche Modelle gibt es auch für Fahrzeugassistenz-Systeme (Standard 2022c).

Teilweise sind sogar so zentrale Eigenschaften wie die Fahrleistung des Fahrzeugs durch extern steuerbare Software per Fernzugriff beeinflussbar. Das kann unter anderem zu Problemen zwischen Besitzer und Hersteller führen, wie etwa das Beispiel einer gedrosselten Akkuleistung und damit Reichweite bei Tesla zeigt: Der Hersteller wollte zunächst 4.500 US-Dollar von einem Tesla-Besitzer für die Reaktivierung der vollen Leistung. Erst nach öffentlichem Druck wurde die Forderung revidiert. Der Fall ist jedoch kompliziert: Tesla bietet für verschiedene Fahrzeugmodelle unterschiedliche Akkuleistungen an, die sich nur durch die softwareseitige Drosselung unterscheiden. Zustande kam das Problem im Zuge eines Gebrauchtwagenkaufs: Der Privatkäufer erwarb von einem privaten Händler ein Tesla Modell S 90, das ursprünglich ein S 60 mit geringerer Reich-

[56] *https://www.cnbc.com/2023/02/16/tesla-recalls-362758-vehicles-says-full-self-driving-beta-software-may-cause-crashes.html*.

[57] *https://www.golem.de/news/automatisiertes-fahren-teslas-autopilot-erzeugt-gefaehrliche-phantombremsungen-2111-161104.html*.

weite war. Nach Tausch des Akkus im Zuge einer Garantieleistung wurde die Drosselung zunächst übersehen. Der neue Besitzer wusste davon nichts. Als Tesla den Fehler bemerkte, kündigte es die Drosselung im Nachhinein an, sofern die Akkuleistung des S 90 nicht bezahlt wird, was zur öffentlichen Empörung führte (Lambert 2022; Standard 2022d). Der Fall zeigt auf, wie Digitalisierung auch Interessenskonflikte (hier zwischen Hersteller und Endkunden) verschärfen kann.

*Geschäftsmodelle mit künstlicher Verknappung*

Zudem gibt es eine steigende Tendenz, dass ökonomische und technologische Abhängigkeiten bewusst eingesetzt werden, um Macht auszuüben. Durch neue digitale Geschäftsmodelle ist mit einer Zunahme an dieser neuen digitalisierten Variante künstlicher Verknappung auch in anderen digital vernetzten Bereichen und Anwendungen zu rechnen. Die damit einhergehenden Abhängigkeiten können also Auswirkungen auf den Lebenszyklus der Fahrzeuge sowie anderer digital vernetzter Geräte und Systeme haben.

## 3.3 HAUSHALT UND KONSUM

*Vernetzte Geräte sammeln viele Daten*

In privaten Haushalten bringt die Digitalisierung auf sehr unterschiedliche Weise Veränderungen mit sich. Im Zuge von Trends wie Smart Home oder noch breiter Internet of Things (IoT) sind immer mehr Geräte digital vernetzt und häufig auch auf dauerhaften Online-Betrieb ausgerichtet, also direkt mit dem Internet verbunden. Die Bandbreite reicht von „smarten" Fernsehgeräten, Lautsprechern mit Sprachsteuerung (zum Beispiel Amazon Echo) über Glühbirnen, Staubsauger, Waschmaschinen, Kühlschränken, Türschlösser bis hin zum vollvernetzten Haushalt im Sinne des „Smart Home", wo sämtliche Geräte digital steuerbar sind. So zumindest die Visionen der Hersteller, die sehr stark mit Komfort werben.

Die Digitalisierung des Energiebereichs führt, wie schon in Abschnitt 3.1 ausgeführt, beim Endverbraucher auch zur Integration von sogenannten Smart Metern, die vor allem wesentlich mehr Messgenauigkeit mit sich bringen. Diese „smarten" Stromzähler ermöglichen es, den Verbrauch in Echtzeit zu messen und diese Informationen an Netzbetreiber, Energieversorger und weitere Akteure mitzuteilen. Während diese Informationen dabei helfen können, Stromnetze besser zu steuern, besteht durch sie jedoch auch die Möglichkeit, dass die privaten Daten der Nutzer:innen zu gänzlich anderen kommerziellen Zwecken oder aber von schädlichen Akteuren missbraucht werden (Peissl et al. 2012).[58]

[58] Auf europäischer wie auch auf deutscher Ebene ist die Umstellung auf Smart Meter gesetzlich eigentlich beschlossene Sache. Urteile wie jenes des nordrhein-westfälischen Veraltungsgerichts, welches Einbaupflichten vorerst gestoppt hatte, bis das BSI dies über eine Verwaltungsanordnung wieder aufhob, und erneute politische Anläufe zeigen jedoch (Enkhardt 2022b), dass der Umstieg auf Smart Meter nicht ohne Hürden und Kontroversen vonstattengeht. In Deutschland wurde im Januar 2023 das Gesetz zur Einführung von Smart Metern vereinfacht, um die Umsetzung zu beschleunigen (siehe auch Abschnitt 3.1., S. 26).

*Kritische Sicherheitsprobleme und Missbrauchsgefahren durch IoT-Geräte*

Die Digitalisierung auf Haushaltsebene bringt eine ganze Reihe von Problemen mit sich. Es gibt immer wieder kritische Sicherheitsprobleme in digital vernetzten Geräten. Beispielsweise zeigte eine Sicherheitsanalyse des weit verbreiteten Netzwerkprotokolls ZigBee Light Link (ZLL) gravierende Schwachstellen und Missbrauchsmöglichkeiten auf. Unter anderem waren die Systeme über Kommunikationsschnittstellen völlig ungeschützt vor externen Zugriffen (Morgner et al. 2017). ZLL ist ein sehr verbreiteter Standard für IoT-Geräte, der insbesondere in intelligenten Beleuchtungssystemen und Smart Home-Systemen eingesetzt wird. Mittlerweile gibt es eine Vielzahl von Plattformen für Smart-Home-Produkte, die es Nutzer:innen ermöglichen, unterschiedliche Geräte und Anwendungen mit einem System zu verbinden und zu steuern (Kafle et al. 2021). Dies können auf der einen Seite offene API[59]-Manager und zentrale Plattformen sein. Beispiele für diese Plattformen sind Googles Nest Plattform[60], Samsungs SmartThings[61] und Philipps Hue[62]. Sicherheits-Forscher:innen haben zahlreiche Sicherheitslücken in solchen Systemen gefunden, die mit steigender Verbreitung problematischer werden, solange Sicherheit nicht bereits im Entwicklungsprozess mitgedacht wird (Kafle et al. 2021). Schwachstellen in solchen Systemen haben daher ein sehr hohes Schadenspotenzial. Angreifer können etwa von außen die Verfügbarkeit der Geräte einschränken und die Kontrolle über ein ganzes Smart-Home Netzwerk erlangen (ebd.).

*Risiko von „Seitenkanalangriffen" steigt mit IoT*

Über das Ausnutzen von Schwachstellen in Endgeräten können auch weitreichendere Infrastruktur-Systeme angegriffen werden. Gerade in Zeiten von Homeoffice und privat genutzter Firmengeräte können zum Beispiel potenzielle Angreifer über das Heimnetzwerk auch in Unternehmensnetzwerke eindringen (IT-Daily 2020). Solche sogenannten „Seitenkanalangriffe" sind ein Problem, das mit der weiteren Verbreitung des IoT zunimmt (Dettmer et al. 2019). Es gibt unzählige dokumentierte Schwachstellen in IoT-Geräten, wie etwa nicht gepatchte Sicherheitslücken und unsichere Logins (ebd.; O'Donnell 2019; Gstaltmayr 2020; Shea 2020; Cyrus 2021; Megas et al. 2021). Erschwerend kommt hinzu, dass sich unsichere IoT-Geräte auch als Botnetze für größere Angriffe missbrauchen lassen, wie etwa das 2016 erstmals entdeckte Mirai-Botnetz, über das mehre Angriffe durchgeführt wurden. Mirai und diverse andere solcher Botnetze sind nach wie vor ein Problem, das an Brisanz gewinnt (Shea 2020). Die meist unzureichende Systemsicherheit von solchen Endgeräten (seien es IoT-Geräte, Hausautomationssysteme oder per Apps integrierte Geräte wie Smartphones oder Tablets) ist daher ein grundlegendes Problem der Digitalisierung auf Haushaltsebene.

*Mobile Geräte als Infrastruktur-Knoten auf Benutzerebene*

Das naheliegendste Beispiel für digitale Vernetzung im Haushalt und bei Einzelpersonen ist aber immer noch das Smartphone, das sich bereits seit Jahren zu als Universalgerät der Digitalisierung etabliert hat. Über Apps können bekanntermaßen einfach neue Anwendungen integriert und genutzt werden (Messenger-Diensten, soziale Medien, E-Banking, Shopping-Apps mit Bezahlfunktion und so weiter). Mobile Endgeräte wie Smartphones werden dadurch immer mehr zu

---

59 API bedeutet Application Progamming Interface, also Programmierschnittstellen, um z. B. verschiedene Systeme zu verbinden oder Daten auszutauschen.

60 *developers.google.com/assistant/smarthome/overview*.

61 *www.smartthings.com/*.

62 *www.philips-hue.com*.

einer Art Infrastruktur-Knoten auf Benutzerebene, über das auch verschiedene, mit Infrastrukturen verbundene Anwendungen nutzbar sind. Das bringt zweifelsohne Vorteile, allerdings werden viele dieser Apps nicht primär zum Nutzen für Kunden entwickelt, sondern für Unternehmen, um Kundenbindung und Personalisierung zu verstärken. Dementsprechend viele personenbezogene Daten werden dabei gesammelt.

*Konsuminfrastruktur über personalisierte Apps verstärkt Profiling*

Im Konsumbereich entsteht so eine Art digitale „Konsuminfrastruktur", die Personalisierung und Kundenbindung verstärkt. Dieses „Profiling" ermöglicht für die Unternehmen Konsum- und Verhaltensmusteranalysen. Kunden bezahlen somit quasi mit ihren Daten, meist ohne sich dessen bewusst zu sein. Das gilt bereits seit langem im Onlineshopping, das ursprünglich auf Online-Bestellungen am Computer zuhause beschränkt war. Seit einigen Jahren wird auch dieser Bereich immer mehr mit mobilen Endgeräten verknüpft und digitaler Konsum findet auch vor Ort in Shops statt: bei Bezahlvorgängen, als digitale Kundenkarten am Smartphone oder über diverse Kundenapps. So werden unterschiedlichste digitale Anwendungen zum mobilen Dauerbegleiter im Alltag, die erhebliche Datenmengen sammeln.

Die bereits sehr stark ausgeprägte Abhängigkeit zu digitalen Plattformen nimmt so weiter zu. Das hat weitere Folgen für Datenschutz und Sicherheit, weil durch Mobile Computing und Smartphone noch mehr personenbezogene Daten inklusive Bewegungsmustern erfasst und ausgewertet werden. Diese Daten werden über digitale Plattformen aus unterschiedlichen Beständen zusammengeführt, um detaillierte Kundenprofile zu erstellen. Es gibt hierfür bereits seit einigen Jahren auf Kundenprofile spezialisierte Anwendungen, die über alle möglichen Geräte hinweg möglichst genaue Daten über die Identität einer Person digital abbilden. Manche Unternehmen bewerben das etwa als „Cross-Channel Identity" (Oracle 2015), um Identitätsdaten quer über verschiedene Medien und Geräte hinweg in einem umfassenden Profil zu erfassen (Strauß 2020).

*Integrierte Technologien können Sicherheits- und Datenschutzprobleme verschärfen*

Eng damit verbunden sind auch vermeintlich beiläufige Technologien zur Identifizierung und Authentifizierung, also etwa der Entsperrung des Smartphones oder zur Nutzung von Apps. Ein wichtiges Beispiel hierfür ist Biometrie. Biometrische Technologien werden immer häufiger in verschiedene Anwendungen integriert – für Logins und Zugang zu Plattformen, diversen Apps, bis zum Schlüsselersatz etwa bei digital vernetzten Fahrzeugen oder auch „smarten" Türschlössern. Das bringt kaum Sicherheitsvorteile, dafür aber erhebliche Datenschutzprobleme und neue Sicherheitsrisiken. Im Gegensatz zu herkömmlichen Authentifizierungsformen (wie Benutzername und Passwort) sind biometrische Merkmale nicht einfach änderbar. Es gibt zahlreiche Angriffsvarianten auf biometrische Systeme und mit wachsender Verbreitung biometrischer Anwendungen werden Angriffe lukrativer und das Risiko von Missbrauch und Identitätsdiebstahl erhöht sich. Zudem sind biometrische Merkmale Identitätsdaten, die unweigerlich mit dem Körper einer Person verknüpft sind und ihre Identifizierbarkeit weiter erhöhen. Dadurch erhöht sich auch das Risiko von Überwachung durch biometrische Systeme (Strauß 2019; Schaber et al. 2020).

*Biometrie als Beispiel für eine unscheinbare aber folgenreiche technologische Abhängigkeit*

Auch integrierte digitale Kameras sind ein Beispiel für eine eher unscheinbare Technologie, die in zahlreichen Geräten im Spektrum von Smart Home integriert sein können. Smarte TV-Geräte haben oftmals sowohl Kameras und Mikrofone, die in der Standard-Einstellung aufzeichnen. Beispielsweise warnte der Hersteller Samsung Kunden sogar davor, keine privaten Gespräche vor dem TV-Gerät zu führen, da die Mikrofone grundsätzlich aufzeichnen (Schmid 2015). Selbst smarte Staubsauger können ungewollte Einblicke in private Haushalte offenbaren, wie Sicherheitsforscher demonstrierten (Edmunds 2020). Ein weiteres Beispiel sind smarte Lautsprecher und Sprachsteuerungsassistenten wie zum Beispiel Amazon Echo mit der Sprachsoftware Alexa oder auch die Sprachassistenten am Smartphone (zum Beispiel Google Assistant, Siri von Apple) (vgl. Schaber et al. 2019). Auch diese Technologien erfassen biometrische Daten, in diesem Fall menschliche Stimmmuster. Neben dem Einsatz am Smartphone und als Lautsprecher gewinnen diese Technologien etwa auch in digitalen Fahrzeugen mit Sprachsteuerung an Bedeutung (siehe Abschnitt 3.2). Biometrie ist daher ein Beispiel für eine relativ unscheinbare, verborgene technologische Abhängigkeit auf individueller Ebene, die stetig zunimmt, aber kaum als Abhängigkeit wahrgenommen wird.

*Kundenbindung und individuelle Abhängigkeiten nehmen zu*

Aufgrund der steigenden Verbreitung von Apps auch für digitalisierte Infrastrukturanwendungen können so weitere Daten etwa über das Nutzungsverhalten in Profile diverser Plattformen einfließen, wenn diese mit der Infrastrukturanwendung vernetzt sind. Über engmaschigere Kundenbindung als Bestandteil von Infrastrukturanwendungen nimmt daher auch die individuelle Abhängigkeit zum jeweiligen Dienstleistungsunternehmen und den damit verbundenen Plattformen weiter zu. Auf Smartphones zeigt sich das neben der Abhängigkeit auf Betriebssystemebene (zum Beispiel zu Apple oder Google Android) auch über App-Stores, die wiederum von großen Technologiekonzernen wie Google, Apple oder Amazon dominiert werden und ohne die kaum Apps zugänglich sind. Der hohe Verbreitungsgrad von Apps macht auch die Verbreitung von Schadsoftware über diese Kanäle sehr lukrativ, da so mit relativ geringem Aufwand Millionen von Geräten kompromittiert werden können.[63] Zwar sind insbesondere große App-Store-Betreiber bemüht, das Sicherheitsniveau zu erhöhen (etwa durch automatisierte Scans nach Schadsoftware), allerdings mit mäßigem Erfolg. Es sind immer wieder auch betrügerische Apps über offizielle Stores verfügbar.[64] Zudem ändert das nichts an der Problematik datensammelnder Apps.

*Steigendes Schadenspotenzial und verringerter Handlungsspielraum*

Durch die steigende Relevanz des Smartphones als Infrastruktur-Knoten auf Benutzerebene steigt das Schadenspotenzial und die starke Abhängigkeit zu Plattformen führt auch hier zu weniger Handlungsspielraum bei Ausfällen. Diese Probleme sind nicht neu, verschärfen sich durch die fortschreitende Digitalisierung aber erheblich. Bei physischem Verlust oder technischem Defekt des Geräts kann das zu individuellen Problemen führen, wenn etwa wichtige Anwendungen

63 *www.heise.de/news/Eine-Million-Downloads-Boesartige-Android-Apps-leiten-auf-Phishing-Seiten-7327239.html*.

64 Zwei Beispiele: Adware on Google Play and Apple Store installed 13 million times *https://www.bleepingcomputer.com/news/security/adware-on-google-play-and-apple-store-installed-13-million-times/*; Great, Now the Apple App Store Has Malware Too *https://lifehacker.com/great-now-the-apple-app-store-has-malware-too-1849386738*.

nicht mehr funktionieren (zum Beispiel das Auto nicht mehr entsperrbar ist oder die Heizung nicht mehr steuerbar). Gravierender als Probleme am Gerät, die oftmals leicht substituierbar sind, sind aber auch hier die starken Abhängigkeiten von externen Diensten und Plattformen auf institutioneller Ebene. Fällt bei einem lokalen Internetprovider etwa ein Server aus, so ist grundsätzlich mit rascher Problembehebung zu rechnen; zudem bestehen Alternativen etwa durch Umstieg auf andere Betreiber. Fällt ein kritischer Dienst eines externen Plattformbetreibers aus, ist es dagegen wesentlich schwieriger, auf Alternativen auszuweichen. Insbesondere dann, wenn für solche Ausfälle gar keine Alternativen ausgearbeitet wurden – diese also erst im Problem- und Anlassfall gesucht werden müssen. Ebenfalls problematisch kann es sein, wenn Technologiebetreiber oder Plattformen bestimmte Anwendungen einfach einstellen oder nicht weiter betreuen. Wenn Hersteller keine Updates mehr liefern, werden die betroffenen Anwendungen im Lauf der Zeit unsicherer oder verlieren gänzlich ihre Funktionalität (Gstaltmeyr 2020).

*Haushalte und Einzelpersonen besonders verwundbar bei Ausfällen*

Auch wenn dadurch die Funktionsfähigkeit der Infrastruktur selbst nicht beeinträchtigt ist, kann das für Einzelpersonen zum Problem werden, wie einige Fälle aus der Praxis zeigen. So zeigt der Fall von Insteon, eines Herstellers von „smarten" Lichtschaltern, Dimmern und Thermostaten, der aufgrund von Insolvenz seine Dienstleistungen einstellte, die Verwundbarkeit von Haushalten (Voronova 2022). Diese konnten nämlich ihre eigenen Hausgeräte nicht mehr bedienen und standen plötzlich wortwörtlich „im Dunkeln". Ähnliche Fälle gab es bereits mit anderen Herstellern (Hern 2016; Patterson 2020; Miller 2022) und ein generelles Problem liegt hier darin, dass Technologiefirmen bei Änderung ihrer Geschäftsmodelle oftmals auch Produkte oder Anwendungen einstellen. Auch diverse Ausfallprobleme sind bei vielen Geräten und Anwendungen des IoT quasi programmiert, sofern sie auf aktive Onlineverbindungen angewiesen sind.

# 4 GESELLSCHAFTLICHE AUSWIRKUNGEN UND WESENTLICHE HERAUSFORDERUNGEN

Wie die angeführten Beispiele verdeutlichen, hat die weiter fortschreitende Digitalisierung erhebliche Auswirkungen auf gesellschaftliche Infrastrukturen auf unterschiedlichen Ebenen. Der zunehmende Vernetzungsgrad und Trends in Richtung Hyperkonnektivität (vgl. Strauß/Krieger-Lamina 2017) verändern die Systemarchitekturen (also Struktur und Organisation) von Infrastrukturbereichen und den daran gekoppelten Diensten und Anwendungen. Zum einen können dadurch Strukturen und Abläufe dynamischer gestaltet werden. Zum anderen führt das jedoch zu noch mehr Komplexität und weiteren technologischen und ökonomischen Abhängigkeiten. Das hat institutionelle und organisatorische ebenso wie individuelle Folgen.

*Steigender Vernetzungsgrad verändert Infrastrukturen erheblich*

## 4.1 AUSWIRKUNGEN AUF INSTITUTIONELLER EBENE

Institutionell sind Unternehmen und Infrastrukturbetreiber durch Lock-ins und Pfadabhängigkeiten noch stärker abhängig von externen digitalen Technologien und deren Anbietern sowie Betreibern. Auf den verschiedenen Infrastrukturbereichen liegt ein starker Anpassungsdruck zur Digitalisierung, der vor allem von Technologieherstellern und Plattformbetreibern kommt, also letztlich wirtschaftsgetrieben ist. Die Bereiche reagieren unterschiedlich auf diesen Druck. Manche Branchen mit direkter Relevanz für die Grundversorgung wie der Energiesektor sind weniger unmittelbar betroffen als andere wie zum Beispiel Mobilität und Konsum. Aber in jedem Fall verändern digitalisierte Infrastrukturen aufgrund der steigenden Abhängigkeiten auch die Bedeutung von Versorgungs- und Ausfallsicherheit. Inwieweit digitale Komponenten tatsächlich kritisch für den Gesamtbetrieb einer Infrastruktur sind, hängt sehr stark von der Systemarchitektur ab. Die enge Verzahnung und Integration digitaler Komponenten in technische Infrastruktursysteme verändert deren Beschaffenheit, wodurch Ausfälle solcher Systemteile mitunter die Funktionsfähigkeit des Gesamtsystems gefährden können. Sicherheit ist daher ein zentraler Aspekt und wie die in Abschnitt 3 angeführten Beispiele zeigen, gibt es hier in verschiedenen Bereichen teilweise erhebliche Probleme.

*Starker Anpassungsdruck zur Digitalisierung*

Ein wesentliches Problem sind dabei mangelhafte Mindestsicherheitsstandards. Dadurch erhöht sich das Risiko von Ausfällen in den betroffenen Infrastrukturen und die Ausfallsicherheit nimmt ab. Wie aus den Beispielen hervorgeht, können Ausfälle sehr unterschiedliche Gründe haben, Softwarefehler ebenso wie gezielte Angriffe durch Missbrauch von Schwachstellen. Grundsätzlich bringen zusätz-

*Zentrales Problem: Mangelhafte Sicherheitsstandards*

liche digitale Systemkomponenten und mangelhafte Sicherheitskonzepte auch zusätzliche Ausfallrisiken und Angriffsflächen, wie die wachsende Zahl von Cyberangriffen auf Infrastrukturen verdeutlicht. Gerade bei industriellen Steuerungssystemen gibt es hier spezielle Probleme aufgrund der sich schrittweise verändernden Technologien: Bisher kamen zur Steuerung von Prozessen in Energieinfrastrukturen und vielen anderen Bereichen hauptsächlich sogenannte Supervisory-Control-and-Data-Acquisition-Systeme (SCADA) zum Einsatz (Pearson 2011). Zum einen sind sie nicht ohne Weiteres von außen erreichbar und sollten es auch nicht sein, weil hier erhebliche Angriffsflächen entstehen können. Es gab jedoch in der Vergangenheit einige Fälle, wo gravierende Mängel bei SCADA-Systemen festgestellt wurden, darunter sogar Atomkraftwerke, die über das Internet erreichbar waren, wie etwa in Frankreich (Baylon et al. 2015; vgl. auch Strauß/Krieger-Lamina 2017). Zum anderen haben diese Systeme andere Funktionsweisen als plattformbasierte digitale Systeme, das heißt sie sind gar nicht für externe Zugriffe konzipiert. Die Systeme gelten zwar als veraltet, sind zugleich aber (sofern oben genannte Mängel nicht bestehen) nicht ohne Weiteres von außen angreifbar, auch deshalb, weil es sich um industrielle Expertensysteme handelt. Daher setzten Angriffe bisher hohe Ressourcen und einen großen Organisationsgrad voraus[65] (Pearson 2011).

*Teils gravierende Mängel in SCADA-Systemen*

Die Digitalisierung verändert das schrittweise. Besagte Interneterreichbarkeit war dabei bislang ein Kernproblem. Im Zuge des technologischen Wandels wurden teils alte SCADA-Systeme vernetzt, was zu Sicherheitsproblemen führt. Dieses Problem wird sich zwar längerfristig lösen lassen, gleichzeitig entstehen aber neue Probleme aufgrund der sich verändernden Funktionsweise technologischer Systeme. Moderne Infrastruktursysteme bauen zusätzlich auf digitalen Plattform-Infrastrukturen auf und integrieren diese. Während diese neuen integrierten Systeme präzisere Steuerung zum Beispiel durch maschinelles Lernen, dezentralere Steuerung und so weiter versprechen, bringen sie auch die Sicherheitslücken dieser Systeme mit (wie zum Beispiel unautorisierte Fremdzugriffe) (Sajid et al. 2016; Strauß/Krieger-Lamina 2017; Hirschl et al. 2018).[66]

Eng mit dieser Problematik verbunden ist das Entstehen neuer, relativ verborgener Abhängigkeiten durch erhöhten Vernetzungsgrad. Ein Beispiel für eine eher neue technologische Abhängigkeit, die weiter zunehmen wird, ist die stärkere Nutzung von Satellitensystemen in der Infrastruktur. Bereits heute nutzen viele Anwendungen Satellitensysteme zur Navigation, Kommunikation, Erdbeobachtung sowie zur Synchronisation von Computernetzwerken. Das ist für den Bahn- und Flugverkehr ebenso relevant wie für die präzise Steuerung des Stromnetzes (Umspannwerke werden etwa per Satellit synchronisiert); ebenso für die Abwicklung von Finanztransaktionen im Börsenhandel, die Koordinierung von Einsatzkräften im Katastrophenschutz oder im militärischen Bereich (Strauß/Krieger-Lamina 2017; BSI 2022a). Mit der weiteren Zunahme digital automatisierter Systeme werden auch Satellitensysteme als integrierte Steuerungskomponente wichtiger. Das betrifft beispielsweise die Transportlogistik sowie die Automati-

*Erhöhter Vernetzungsgrad bringt neue, verborgene Abhängigkeiten*

[65] Angriffe kamen daher in der Regel von staatlichen Organisationen wie Geheimdiensten.

[66] Ein ausführlicher Review findet sich bei(Sajid et al. (2016).

sierung von Fahrzeugsteuerungen in Pkws, Lkws, aber auch in automatisierten Transportschiffen (TB 2017; EUSPA 2022). Ein Problem ist wie so oft die Abhängigkeit von Technologiebetreibern.

Welche Auswirkungen die Störung eines Satellitensystems auf Infrastrukturen haben kann, zeigt etwa der Angriff auf das US-Unternehmen Viasat kurz nach Beginn des Ukraine-Krieges im Februar 2022: Dessen Satellitennetz KA-SAT wurde gezielt gestört, wodurch der Betrieb mehrerer Tausend Windkraftanlagen in Deutschland beeinträchtigt wurde (Krempl 2022c; BSI 2022a). Der Angriff erfolgte nicht auf das Satellitensystem selbst, sondern auf das daran gekoppelte IT-Netz: Durch Schadsoftware („Wiper-Malware") wurden die nötigen Breitbandmodems unbrauchbar gemacht. Es wird vermutet, dass der Angriff vor allem dem ukrainischen Militär galt – und dass die Auswirkungen in Deutschland also Kollateralschäden waren (Krempl 2022c; Spiegel 2022). Dieser Vorfall und die generelle Zunahme an Cyberangriffen hat die Sorge vor weiteren Ausfällen in der Industrie erhöht (Murphy/Fasse 2022). Zudem warnen Geheimdienste vor der wachsenden geopolitischen Problematik durch die Abhängigkeit von Satellitensystemen autokratischer Staaten wie China, dessen System Beidou als Konkurrenz zu GPS neben der Navigation unter anderem für das IoT, sowie in der Logistik oder für Steuerungssysteme von Zügen an Bedeutung gewinnen könnte (Wang/Qiu 2020; Spinsante/Stallo 2020; Corera 2022).

*Zunahme an Cyberangriffen und Ausfällen*

Aber auch unabhängig von Angriffen und geopolitischen Spannungen kann die Abhängigkeit von Satellitenbetreibern problematisch sein, insbesondere, wenn diese über eine starke Machtstellung verfügen. Im Ukrainekrieg spielt etwa Elon Musks Unternehmen SpaceX mit seinem Satellitennetzwerk Starlink eine militärische Rolle, die aber von Seiten des Unternehmens spontan eingeschränkt werden kann (wie im Februar 2023 im Kontext eines eigenen „Friedensplans" praktiziert). Dass ein nichtstaatlicher Akteur einen solchen Einfluss auf einen militärischen Konflikt ausüben kann, stellt eine neue Dimension dar. SpaceX ist mit derzeit über 2.400 Satelliten der weltweit größte Satellitenbetreiber und hat Anträge für weitere 30.000 Satelliten gestellt.[67] Starlink betreibt vordergründig Satelliteninternet, das aber künftig gerade für den Ausbau des IoT eine gewichtige Rolle spielen dürfte. Auch andere Technologiekonzerne wie zum Beispiel Amazons Tochterfirma Kuiper Systems planen verstärkt in private Satellitensysteme zu investieren. Hier zeichnet sich längerfristig bereits eine zunehmende Kommerzialisierung des Weltraums ab. In Europa wurde 2022 der Aufbau einer eigenen Satellitenkonstellation Iris² (Infrastructure for Resilience, Interconnection and Security by Satellites) beschlossen, um die starke Abhängigkeit zu Satellitensystemen von Drittstaaten zu verringern. Hierbei geht es sowohl um staatliche als auch wirtschaftliche Interessen. Iris² soll auch kommerziell nutzbar sein. Der Fahrplan zur Umsetzung des Systems bis 2027 gilt unter Experten als sehr ambitioniert (Lehner 2022; Sawall 2022).

*Wachsende Abhängigkeit zu Satellitensystemen*

Neben technologischen steigen auch ökonomische Abhängigkeiten in Infrastrukturbereichen. Die Plattformökonomie spielt hierbei eine mächtige Rolle, da sie sehr stark von Netzwerkeffekten profitiert und mit ihrer Marktmacht entspre-

*Die Plattformökonomie verstärkt ökonomische Abhängigkeiten*

[67] *de.wikipedia.org/wiki/Starlink*.

chende Geschäftsmodelle durchsetzen kann. Diesbezüglich wird auch häufig der Begriff „digitales Ökosystem" bemüht, hinter dem sich aber keine ökologischen, sondern ökonomische Ziele zur Erweiterung der Wertschöpfung verbergen. Im Kern ist Plattformökonomie eine neuartige Form des Outsourcings, die zu einer starken Zentralisierung von dienstleistungsrelevanten Daten führt. Plattformbetreiber bieten sich als Dienstleistungsvermittler zwischen Unternehmen und Endkunden an (vgl. Kenney et al. 2016; Srnicek 2017; Kirchner 2021). Plattformen werden dabei selbst zu einem zentralen Knotenpunkt einer digitalen Infrastruktur. So laufen verschiedene, anwendungsspezifische Daten- und Informationsströme über digitale Plattformen zusammen, die auch weiteren Geschäftsmodellen dienen können. Durch diese Form von Zentralisierung erlangen Plattformbetreiber eine sehr machtvolle Position mit starkem Einfluss auf die Funktionsfähigkeit von Infrastruktursystemen.

## 4.2 AUSWIRKUNGEN AUF INDIVIDUELLER EBENE

Die oben genannten Abhängigkeiten übertragen sich auf Haushalte und Einzelpersonen weiter. Neben Fragen für die Versorgungssicherheit haben digitalisierte Infrastrukturen auch erhebliche Auswirkungen auf Sicherheit und Privatsphäre. Wie an unzähligen Beispielen ersichtlich, bedeutet mehr Digitalisierung auch mehr Sammlung und Verarbeitung von personenbezogenen Daten. Neben der grundlegenden Problematik, dass Daten missbraucht oder zweckentfremdet werden können, ist vor allem die zunehmende Verknüpfung „klassischer" Infrastrukturdienste mit datenbasierten Geschäftsmodellen problematisch. Dadurch werden Anwendungen immer intrusiver und dringen über digitalisierte Infrastrukturen noch stärker in Haushalte und individuelle Lebensbereiche ein. Daher werden grundrechtliche und ethische Aspekte wie Datenschutz und Datensicherheit, Schutz der Privatsphäre, Autonomie und Selbstbestimmtheit für private Haushalte immer relevanter.

*Datenbasierte Geschäftsmodelle dringen in individuelle Lebensbereiche hinein*

Längerfristig verändert sich auch der klassische Zweck von Infrastruktursystemen: In verschiedenen Bereichen kommen zur Deckung der Grundversorgung datenbasierte Geschäftsmodelle hinzu. Das zeigt sich auch in der steigenden Anzahl von Apps und Kundenprofilen, die auch den Zweck haben, Personalisierung und Kundenbindung zu stärken. Über diesen Weg entsteht zusätzlich eine Art Konsuminfrastruktur (siehe auch Abschnitt 3.3), die je nach Anwendungsbereich auch zu mehr Profiling führt, wenn zum Beispiel die anfallenden Daten über Verbrauchsmuster von Strom mit anderen Kundendaten verknüpft werden.

*Weitreichende Folgen für Datenschutz*

Das führt zu einer weiteren Verschärfung der Datenschutzproblematik. Laut europäischer Datenschutzgrundverordnung (DSGVO) ist Profiling[68] grundsätzlich verboten, außer die betroffene Person hat explizit zugestimmt. Allerdings ist in der Praxis eine Zustimmung häufig reine Formsache, da eine Anwendung ohne Zustimmung zu den AGBs meist gar nicht nutzbar ist. Das ist kein neues Prob-

[68] Profiling gilt laut Art. 4 Z 4 DSGVO als jede Art der automatisierten Verarbeitung personenbezogener Daten, um auf dessen Grundlage bestimmte persönliche Aspekte zu bewerten.

lem, kann im Kontext von Infrastrukturen aber noch weitreichendere Folgen haben. Das ist insbesondere der Fall, wenn personenbezogene Daten auch über externe Plattformen verarbeitet werden. Gerade größere Plattformbetreiber erstellen sehr detaillierte Kundenprofile und führen Daten aus verschiedenen Beständen mit dem Ziel zusammen, möglichst umfassende Daten über die Identität einer Person zu erfassen und digital in Form von sogenannten Identity Graphs abzubilden (Strauß 2020).

Beispielsweise bietet der auf Datenbanksysteme spezialisierte Konzern Oracle spezifische Anwendungen zur Generierung sogenannter Cross Channel Identity (Oracle 2015), wonach Identitätsdaten quer über verschiedene Medien und Geräte hinweg in einem umfassenden Profil erfasst werden (Strauß 2020). Es ist derzeit nicht auszuschließen, dass solche Daten über digitalisierte Infrastrukturen auch von Plattformen erfasst werden, wenn diese entsprechend integriert sind. In Summe erhöht sich über engere Kundenbindung als Bestandteil einer Infrastrukturanwendung auch die individuelle Abhängigkeit vom jeweiligen Dienstleistungsunternehmen und den damit verbundenen Plattformen noch weiter.

Das kann auch verborgene Abhängigkeiten umfassen, die zunehmen, aber kaum als solche wahrgenommen werden. Ein Beispiel für eine eher unscheinbare Abhängigkeit auf individueller Ebene ist die zunehmende Verwendung von biometrischen Daten. Biometrie gewinnt als Zugangs- und Authentifizierungstechnologie an Bedeutung in verschiedenen Anwendungen von Zugang zu Plattformen und Apps, bis zum Schlüsselersatz etwa bei digital vernetzten Fahrzeugen oder „smarten" Türschlössern. Das führt zu weiteren Problemfeldern wie etwa dem wachsenden Risiko von Identitätsdiebstahl, neuen gravierenden Datenschutz- und Sicherheitsproblemen und zunehmender Überwachung durch biometrische Systeme (Schaber et al. 2020). Dass Biometrie die Sicherheit nicht unbedingt erhöht, zeigt auch der in Tabelle 1 angeführte Fall der ungeschützten Biometrie-Datenbank mit Millionen von Datensätzen. Zahlreiche weitere Beispiele (ebd.) verdeutlichen, wie riskant ein Ausbau von Biometrie grundsätzlich ist.

***Biometrie nimmt zu und verstärkt individuelle Abhängigkeiten***

Digitalisierte Infrastrukturen und das IoT begünstigen zudem auch staatliche und private Überwachungsformen. Einige Länder, insbesondere autokratische Staaten wie China, nutzen digitale Infrastrukturen sehr stark zu Überwachungszwecken. Unter harmlos klingenden Schlagwörtern wie „Smart City" wurden städtische Infrastrukturen bereits weitreichend digitalisiert. Das betrifft jedoch nicht nur digitale Anwendungen zum effizienteren Betrieb der Infrastrukturen, sondern umfasst auch die Integration tiefgreifender Überwachungstechnologien wie etwa biometrische Gesichtserkennung, Stimmmuster, persönliche Verhaltensmuster und vieles mehr (Kynge et al. 2021; Mattheis 2022; Qian et al. 2022). Auch außerhalb von China werden entsprechende Technologien teils explizit zur urbanen Überwachung konzipiert (z. B. Chen/Chen 2018).

***Staatliche und private Überwachungsformen durch digitalisierte Infrastrukturen***

In abgeschwächter Form sind Überwachungstendenzen auch anderswo beobachtbar. Das gilt insbesondere in US-amerikanischen Metropolen, es gibt aber auch Beispiele in Afrika oder Europa: London hat seit Jahrzehnten die höchste Anzahl an Überwachungskameras in Europa – aktuellen Schätzungen zufolge bereits über

940.000, Tendenz steigend).[69] Allerdings gibt es einen generellen Zuwachs auch in anderen Ländern, der in den vergangenen Jahren verstärkt im Zusammenhang mit Smart City Projekten entsteht. In Serbien soll beispielsweise ein umstrittenes Smart-City-Projekt zum Ausbau von intelligenten Überwachungskameras führen (Kynge et al. 2021). Ähnliche Entwicklungen gibt es zum Beispiel auch in Amsterdam (Galič 2022). Problematisch ist hier unter anderem, wenn Smart City und ähnliche Konzepte und die entsprechenden Technologien unkritisch übernommen werden, die effizientere Gestaltung städtischer Infrastrukturen aber nur zum Schein im Vordergrund steht. Gerade bei Smart-City Projekten spielen chinesische Technologien oftmals eine starke Rolle, wie auch im oben genannten Beispiel Serbien. Sicherheitsexperten sehen darin eine besorgniserregende Entwicklung (Ekman 2019; Kynge et al. 2021). Die Zusammenhänge zwischen Überwachung und IoT sind aber nicht auf Technologien aus bestimmten Ländern beschränkt, sondern bestehen schon länger. Der ehemalige Direktor der nationalen Nachrichtendienste in den USA, James Clapper, gab schon vor einigen Jahren offen zu, dass IoT-Geräte auch zur Überwachung genutzt werden (Guardian 2016). Mit dem Ausbau des IoT haben tatsächlich auch die Überwachungsformen und negativen Folgen für die Privatsphäre zugenommen (Henschke 2020).

*Zusammenhänge zwischen Überwachung, Iot und Smart-City Projekten*

Die Coronapandemie hat Überwachungstendenzen im privaten Bereich zum Teil erheblich begünstigt. Das zeigt zum Beispiel der zunehmende Missbrauch von Webcams. In Italien wurde im Juni 2022 bekannt, dass Hacker Bilder und Streams aus öffentlichen Videoüberwachungssystemen sowie privaten Haushalten über Webcams sammelten und die Zugriffe gegen Bezahlung anboten (Straub 2022). Nicht nur Kriminelle machen sich Webcams zu nutze. Seit der Coronapandemie überwachen zum Beispiel Arbeitgeber in den USA immer häufiger ihre Mitarbeiter im Homeoffice über Webcams und spezielle Kontrollsoftware (Abril/Harwell 2021). Auch in Europa ist diese Technik inzwischen angekommen, wie ein Fall in den Niederlanden zeigt: Ein Mitarbeiter wollte nicht dauerhaft seine Webcam aktivieren, was zur Entlassung führte. Der Fall ging vor Gericht und das Unternehmen wurde zu einer Strafzahlung von rund 75.000 Euro verurteilt. Das Gericht argumentierte mit Artikel 8 der Europäischen Menschenrechtskonvention, dass die Forderung, Webcams dauerhaft aktiv zu halten, im Sinne des Grundrechts auf Privatsphäre unverhältnismäßig und damit illegal sei (NLT 2022).[70] Grundsätzlich ist eine steigende Tendenz zur Arbeitsplatz-Überwachung zu verzeichnen (Riso 2021).

*Überwachung im Privatbereich*

Ein weiterer Aspekt betrifft Einschränkungen der Handlungsfähigkeit und den Verlust von Kontrolle über digitale Technologien. Ein altbekanntes Problem sind kurze Lebenszyklen und geringe Reifegrade von Software, die einerseits zu ständigem Aktualisierungsbedarf etwa an sicherheitskritischen Updates, aber auch zu Änderungen in Design und Funktionalität der Anwendungen führen. Das bedeutet, dass regelmäßig nicht hinreichend für den Praxisbetrieb erprobte Anwendungen eingesetzt werden. Dieser Trend hat bereits mit dem Web 2.0 begonnen und wird über Plattformen fortgeführt. Das ist schon im privaten Kontext nicht

*Eingeschränkte Handlungsfähigkeit als wachsendes Problem*

[69] *https://clarionuk.com/resources/how-many-cctv-cameras-are-in-london/*.

[70] Homeoffice: Webcam Pflicht ist Menschenrechtsverletzung *www.derstandard.at/story/2000139842102/niederlande-gericht-sieht-webcam-pflicht-im-homeoffice-als-menschenrechtsverletzung*.

nur schwierig und unpraktisch, sondern kann zu erheblichen Sicherheitsproblemen führen (etwa beim Onlinebanking). Besonders problematisch wird es bei Infrastrukturen und damit verbundenen Systemen. Denn mangelhafte Sicherheitskonzepte begünstigen Ausfallrisiken mit potenziell gravierenden Folgen. In einigen Fällen kann das sogar fatal enden, wie einige Unfälle von teil-automatisierten Fahrzeugen zeigen (siehe Abschnitt 3.2).

*Digitale Souveränität zusehends auf dem Prüfstand*

Damit verbunden ist das Problem eines schleichenden Zwangs: Die fortschreitende Digitalisierung führt schrittweise zu einem Abbau des Prinzips der Wahlfreiheit, also der Freiheit selbst zu entscheiden, welche digitalen Dienste eine Person nutzen möchte. Etwa durch alternativlos erforderlich gewordene Installation von Apps, um Infrastruktur-Dienste oder bestimmte Geräte überhaupt nutzen zu können (wie IoT, Smart-Home-Steuerungen, Fahrzeuge siehe Abschnitt 3). Hier offenbaren sich Widersprüche zu den von der Europäischen Kommission vorgeschlagenen digitalen Rechten und Grundsätzen wie etwa „Menschen und ihre Rechte in den Mittelpunkt der digitalen Transformation stellen“ oder besagte Wahlfreiheit.[71] Zudem ist fraglich, wie das damit verbundene Ziel, die digitale Souveränität in Europa zu sichern, erreichbar ist. Digitale Souveränität ist als Begriff aus der Industrie in den politischen Diskurs übergegangen (Bendiek/Stürzer 2022) und wird in Deutschland definiert als „die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können“[72]. In Anbetracht der tendenziell abnehmenden Handlungsfähigkeit auf individueller wie institutioneller Ebene steht das Prinzip digitale Souveränität zumindest auch weiterhin erheblich auf dem Prüfstand.

*Fernzugriffe und Fernabschaltungen als neue Gefahr*

Problematisch auf individueller Ebene sind insbesondere Tendenzen, die Funktionalität infrastrukturbezogener Dienste gezielt einzuschränken oder Druck auf Endkunden auszuüben, beispielsweise, um Bezahl-Abos für zusätzliche Dienste abzuschließen. Fernzugriffe und Fernabschaltungen sind technisch nicht nur möglich, sondern häufig explizit von Technologiebetreibern vorgesehen. Neben den in Abschnitt 3 beschriebenen Fällen besteht das Problem auch in anderen Kontexten. Der deutsche Bundesgerichtshof hat erst kürzlich in einem Urteil eine Klausel zur Fernabschaltung einer Autobatterie für unwirksam erklärt[73]. Im konkreten Fall ging es um eine AGB-Klausel bei Renault, mit der sich der Hersteller das Recht einräumte, per Fernzugriff das Wiederaufladen eines gemieteten Akkus in verkauften oder geleasten Autos zu unterbinden. Der BGH sah darin einen übermäßigen Eingriff in den Besitz des Autofahrers (Greis 2022). Auch im Energiebereich gibt es bereits Fälle von per Fernzugriff gedrosselter Leistung, wie etwa bei Smart Home-Systemen, Strom oder Heizungsanlagen (siehe Abschnitt 3). Im März 2022 kam es in Deutschland beim PV-Anbieter Senec zu einer Fernabschaltung von Heimspeichern bei mehreren Tausend Kunden (Enkhardt 2022a). Diese Fälle zeigen, wie schmal der Grat zwischen zulässiger Kundenbin-

71 *digital-strategy.ec.europa.eu/de/policies/digital-principles*.

72 *https://www.cio.bund.de/Webs/CIO/DE/digitale-loesungen/digitale-souveraenitaet/digitale-souveraenitaet-node.html*.

73 *juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&sid=16456c1a72b3c428ac1b20f1984d79c2&nr=131509&linked=pm&Blank=1*.

dung und unzulässigem Missbrauch einer technologisch bedingten Machtstellung sein kann. Mit dem weiteren Ausbau solcher Geschäftsmodelle ist eine Zunahme von Streitfällen um Fernzugriffe nicht unwahrscheinlich.

*Zunehmende Informations- und Machtasymmetrien als Grundproblem der Digitalisierung*

Insgesamt verschärft sich ein Grundproblem der Digitalisierung: zunehmende Informations- und Machtasymmetrien (vgl. Strauß 2019, S.145ff.). Das betrifft die verschiedenen Akteure auf unterschiedliche Weise: Kriminelle Akteure nutzen digitale Schwachstellen gezielt aus, um etwa Infrastrukturbetreiber zu erpressen. Staatliche Akteure üben geopolitische Macht durch gezielte Angriffe auf Infrastrukturen aus. Wirtschaftliche Akteure nutzen ihre Marktstellungen über technologische und ökonomische Abhängigkeiten und forcieren damit Locks-Ins und beeinträchtigen die Handlungsfähigkeit der von ihnen abhängigen Nutzer:innen. Das ist grundsätzlich nichts Neues, allerdings verschärft sich diese Situation mit digitalisierten Infrastrukturen. Durch die Plattformökonomie und die damit verbundene technische Gestaltungsmacht werden Technologie- und Plattformbetreiber auch über ihre Kernbereiche hinaus zu machtvollen Akteuren in verschiedenen Sektoren. Aufgrund ihrer Breitenwirkung kommt es zu einer schleichenden Machtverschiebung mit Tendenzen zur Quasi-Monopolisierung. Praktische alle großen Technologiekonzerne wie Alphabet (Googles Mutterkonzern), Meta (mit Facebook, Instagram, Whatsapp), Apple, Amazon und Microsoft haben eigene IoT-Plattformen und entsprechende Marktstrategien. Unter anderem ist Amazon über seine AWS[74]-Plattform immer mehr auf IoT-Anwendungen präsent. Große Technologiekonzerne etablieren neue Geschäftsmodelle und gewinnen weiter an Marktmacht. Zu diesen großen Konzernen gehört inzwischen auch das Unternehmenskonglomerat von Elon Musk, das mit Feldern wie E-Mobilität, virtuelle Kraftwerke, IoT, Satellitensysteme, Raumfahrt und Kommunikationsinfrastruktur (Twitter) inzwischen eine erhebliche Bandbreite abdeckt. Neben US-amerikanischen Konzernen spielen vor allem chinesische Unternehmen (z. B. Huawei, Baidu, Alibaba oder Tencent) eine starke Rolle.

Für Infrastrukturbetreiber bedeutet dieses sich verschiebende wirtschaftliche Machtgefüge mehr Marktdruck und stärkere Abhängigkeiten von Sektoren, mit denen es ursprünglich wenig oder keine Schnittmengen gab. Bezogen auf den Umgang mit Vulnerabilität bedeutet das eine tendenziell sinkende Bewältigungskapazität (vgl. Abschnitt 2), weil die Menge der Risiken eher zu- als abnimmt.

74 Amazon Web Services.

## 4.3 ZENTRALE HERAUSFORDERUNGEN

*Differenziertes Problembewusstsein für Vulnerabilität digitalisierter Infrastrukturen nötig*

Es gibt eine Reihe von Herausforderungen, um die zahlreichen Problemfelder zu entschärfen, auf die hier nicht alle im Detail eingegangen werden kann. Grundsätzlich braucht es ein stärkeres und differenziertes Problembewusstsein für die Vulnerabilität digitalisierter Infrastrukturen. Die Debatte um Cybersecurity wird relativ stark dominiert von Gefahren für Infrastrukturen aufgrund externer Angriffe. Hier gibt es unbestritten erhebliche Risiken, die besser wirksame Schutzmaßnahmen erfordern. Das betrifft aber weniger nach außen gerichtete, sondern vielmehr nach innen gerichtete Schutzmaßnahmen zur Erhöhung des generellen Sicherheitsniveaus von Infrastruktursystemen. Das bedeutet vor allem das Identifizieren und Beseitigen von Schwachstellen, die die Systemsicherheit gefährden.

*Relativ hohes Problembewusstsein im KRITIS-Bereich*

Für Infrastrukturbetreiber sind hierfür systematische Vulnerabilitätsanalysen ein wesentliches Instrument, das speziell bei Betreibern kritischer Infrastrukturen das Sicherheitsniveau erhöhen kann. Dabei ist wichtig, auch die Indikatoren für Bewältigungskapazität zu berücksichtigen (Lenz 2009; siehe Abschnitt 2). Für die klassischen KRITIS-Bereiche (vom Energiesektor über Ernährung, Wassermanagement bis hin zum Gesundheitswesen) gibt es bereits zahlreiche Untersuchungen sowie praktische Leitfäden (z. B. Menski 2016; IBH 2017; UBA 2021; BBK 2022). Zudem gibt es eine Reihe von Maßnahmenkatalogen und Handbüchern für den Schutz von IT-Systemen und für bessere Informationssicherheit, wie etwa das regelmäßig aktualisierte IT-Grundschutz-Kompendium des BSI (BSI 2022b), oder auch spezifische Leitfäden und Empfehlungen zur Absicherung von industriellen Steuerungssystemen (z. B. BSI 2013; vgl. Hirschl et al. 2018). Diese Leitfäden sind grundsätzlich wichtig und das Problembewusstsein ist im KRITIS-Umfeld bereits sehr hoch.

*Es fehlt an systemischer Perspektive auf Problemfelder der Digitalisierung*

Allerdings fehlt neben diesen wichtigen technisch und organisatorisch zentrierten Anleitungen eine breitere systemische Perspektive auf die Problemfelder, die aus der Digitalisierung von Infrastrukturen resultieren. Am ehesten ist dies noch im Stromsektor gegeben, weil hier technische Abhängigkeiten und Schwachstellen oft unmittelbar sichtbar werden (etwa, wenn die Stromversorgung beeinträchtigt ist). Zudem gibt es bereits Studien, die sich explizit mit Vulnerabilität und Resilienz im digitalen Stromnetz befassen (vgl. Hirschl et al. 2018). Allerdings fehlt es offenbar an ganzheitlichen Ansätzen, die über eine zweifelsohne wichtige sektorale Fokussierung hinausgehen. Dadurch ist es schwierig, bereichsübergreifende Problemfelder wirksam zu entschärfen. Das bedeutet, es besteht auch zusätzlicher Wissensbedarf über die mittel- und längerfristigen Folgen digitalisierter Infrastrukturen.

*Wechselseitige Abhängigkeiten können kritisch werden*

Ein Kernproblem digitalisierter Infrastrukturen liegt in den wechselseitigen Abhängigkeiten zwischen vernetzten Teilsystemen. Schwachstellen in Teilsystemen müssen nicht unmittelbar die Grundfunktionalität des Gesamtsystems sichtbar beeinträchtigen, können aber im Verborgenen „schlummern“ und erst später zu kritischen Problemen führen (Fehler ebenso wie Angriffe). Ausfälle eines Teilsystems (zum Beispiel einer wichtigen Steuerkomponente) können zu Kaskadeneffekten und damit zu weiteren Störungen führen. Dieses Problem verschärft sich mit zunehmender Vernetzung weiter. Eine Grundvoraussetzung, um Systeme

zu vernetzen, sind technische Schnittstellen, die unterschiedliche technologische Komponenten miteinander verbinden (typisches Beispiel: mit dem Internet verbundene Steuerungssysteme, wie in Abschnitt 4.1 erläutert). Durch den Trend zur multiplen Vernetzung (Hyperkonnektivität) nimmt die Anzahl an Schnittstellen eher zu als ab. Dabei gilt die Faustregel „Schnittstellen erhöhen die Komplexität des Systems und machen es somit potenziell anfälliger" (Strauß/Krieger-Lamina 2017, 74). So entstehen viele technische Schwachstellen nicht originär bei den Infrastrukturbetreibern, sondern sie werden über externe Technologien und Schnittstellen in die Infrastrukturen quasi hineingetragen.

Das hat zur Folge, dass der Handlungsspielraum bei technologischen Schwachstellen begrenzt ist. Um dieses Problem zu verringern, braucht es neben eines hohen Sicherheitsbewusstseins bezüglich der generellen Gefahr von Schadsoftware, Ransomware und dergleichen wesentlich mehr Bewusstsein für die grundsätzliche Problematik von vernetzten externen Schnittstellen – also welche Art von externen Technologien in welcher Form in ein Infrastruktursystem eingebunden sind, was sie vernetzen und wozu. Gerade die Frage nach der Notwendigkeit gerät durch den stetigen Trend zur Vernetzung immer mehr in den Hintergrund. Es mag zwar anachronistisch anmuten, aber die gängige Vernetzung „per Default" ist oft fragwürdig. Aus systemischer Perspektive ist ein System, bei dem Komponenten nur im konkreten Bedarfsfall vernetzt werden, resilienter. Denn nach dem dominierenden Paradigma einer dauerhaften Vernetzung bedeutet jede weitere Schnittstelle, dass ein weiteres externes System kontinuierlich mit dem Gesamtsystem Infrastruktur vernetzt ist. Das bedeutet mehr Komplexität und damit auch höhere Anfälligkeit für Systemfehler, Schwachstellen oder Angriffe von außen – und daher Vulnerabilität. Diese Probleme sind vor allem dann verschärft, wenn es zu einer nicht nötigen Vernetzung von unterschiedlichen Systemen kommt oder Teilsysteme unsauber voneinander getrennt sind. Ein Beispiel sind vernetzte Fahrzeuge, wo häufig kritische Steuerungselemente und Unterhaltungssysteme nicht klar getrennt sind (siehe Abschnitt 3.2). Ähnliche nicht notwendige Dauerverknüpfungen gibt es in vielen Bereichen.

*Vernetzung „per Default" macht Systeme anfälliger*

Ein stärkeres Bewusstsein für diese Problematik kann dazu beitragen, kritische technologische Abhängigkeiten besser zu erkennen und Schutzkonzepte sowie Workarounds zur Aufrechterhaltung der Grundfunktion zu erarbeiten für den Fall, dass Teilsysteme versagen. Fernabschaltungen über technische Schnittstellen von Herstellern, Technologie- oder Plattformbetreibern sollten eben nicht ohne Weiteres möglich sein, was aber schlicht erstmal die Kenntnis dieser Möglichkeit voraussetzt. Das gilt insbesondere für die Problematik verdeckter, nicht-offensichtlicher Abhängigkeiten (Beispiele sind die oben angeführten Abhängigkeiten von Satellitensystemen sowie biometrische Technologien). Wenn die Kenntnis über die kritische Relevanz eines externen Systems fehlt, dann ist auch die Fehlersuche bei einem Ausfall beeinträchtigt. Deshalb ist das Wissen über externe Schnittstellen beziehungsweise extern eingebundene Technologien eine wichtige Grundvoraussetzung für die Bewältigungskapazität. Schnittstellen und extern eingebundene Systeme sind kritische Teile eines Infrastruktursystems, die daher unbedingt explizit in Vulnerabilitätsanalysen einbezogen werden sollten.

*Wissen über externe Systeme wesentlich*

Um die Resilienz von digitalisierten Infrastrukturen zu erhöhen, ist die Stärkung der Bewältigungskapazität wesentlich. Grundsätzlich gelten die generellen Indikatoren für Bewältigungskapazität (vgl. Abschnitt 2) auch für digitale Systeme. Allerdings können gerade die zentralen Faktoren Redundanz und Substituierbarkeit je nach Infrastrukturbereich unterschiedlich realisierbar sein. Kurz gefasst bezieht sich das auf die Fragen: Welche Alternativen gibt es, um einen Totalausfall zu vermeiden? Wie kann trotz Ausfall die Grundleistung eines Infrastrukturdienstes erbracht werden? Hier können digitale Systeme erhebliche Vorteile bringen, weil es mehr Möglichkeiten gibt, bei Ausfällen einer Technologie auf eine andere auszuweichen. Beispielsweise gibt es zahlreiche alternative Systeme für Kommunikation oder auch Datenaustauch (zum Beispiel Ausweichen auf andere Mobilfunkbetreiber, Plattformen, Clouddienste, Mesh-Netzwerke[75]). Allerdings hängt das sehr stark vom konkreten Störfall ab. Neben technischen Alternativen ist zudem wichtig, sofern möglich auch analoge beziehungsweise manuelle Notmaßnahmen vorzusehen. In jedem Fall ist ein Bewusstsein für die kritische Bedeutung von Redundanzen und Substituierbarkeit in einem Krisenfall zentral, um diese auch explizit vorsehen zu können. Denn so lässt sich auch das Risiko eines Kontrollverlusts bei einem Störfall relativieren. Aufgrund hohen ökonomischen Drucks werden gerade diese zentralen Aspekte häufig vernachlässigt.

*Redundanz und Substituierbarkeit sind wichtige Faktoren für Resilienz*

Das Grundproblem wachsender Informations- und Machtasymmetrien durch Digitalisierung wird bei Infrastrukturen immer mehr zu einem Problem der Grundversorgung, der Grundrechte und der Deckung gesellschaftlicher Grundbedürfnisse. Wie oben erläutert, sind einige Problemfelder eng mit den Paradigmen und Marktmechanismen der Plattformökonomie verwoben. Eine zentrale Herausforderung sind daher die wirksamere Kontrolle digitaler Plattformen sowie der Plattformökonomie als Ganzes. Regulierungsansätze spielen hier eine wichtige Rolle. In Deutschland gibt es seit 2017 das Netzwerkdurchsetzungsgesetz, das aber primär den Umgang mit „Hate Speech" und rechtswidrigen Inhalten in sozialen Medien regelt. Auf EU-Ebene wurden nun im September und Oktober 2022 zwei wichtige Rahmenwerke für Onlineplattformen beschlossen: Der Digital Markets Act (DMA) und der Digital Services Act (DSA).[76] Der DSA zieht primär einen Rahmen zur Regulierung von großen Online-Medien und Suchmaschinen. Die Verordnung konzentriert sich auf den Umgang mit illegalen Inhalten und Falschinformationen – sowie bessere Kontrolle personalisierter Werbung (EDRi 2022). Für die Entschärfung der in dieser Studie thematisierten Infrastrukturprobleme ist im DSA wenig enthalten.

*Informations- und Machtasymmetrien erfordern wirksame Regulierung*

Stärker in Richtung Marktregulierung geht der Digital Markets Act, der neue Vorgaben für sogenannte Gatekeeper vorsieht, also Konzerne, die durch ihre marktbeherrschende Position den Zugang für andere Firmen kontrollieren. Das bezieht sich auf die derzeit dominierenden Plattformbetreiber wie Alphabet/Google, Amazon oder Apple. Der DMA enthält auch zusätzliche Datenschutz-Bestimmungen, zum Teil in Ergänzung zur Datenschutz-Grundverordnung, um

*Neue Regulierungsansätze setzen Impulse*

[75] Mesh-Netzwerke ermöglichen es, mehrere Geräte so zu verbinden, dass sie auch als Überbrückung bei Ausfällen einsetzbar sind. Ein einfaches Beispiel ist die Nutzung eines Smartphones als Internetrouter via Mobilfunk zur Überbrückung bei Ausfall der herkömmlichen Internetversorgung.

[76] *https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package*.

etwa Profiling und Kundenbindung stärker zu regulieren. So mussten Nutzer:innen bislang oftmals jeder Art von Datenverarbeitung zustimmen, um Plattformdienste überhaupt nutzen zu können. Diese Art des Zwangs zur Einwilligung soll künftig nicht mehr ohne Weiteres erlaubt sein. Allerdings verbietet auch der DMA das Profiling nicht, sondern knüpft es lediglich an mehr Bedingungen. Zudem schränkt der DMA die Datenweitergabe nicht ein, sondern ermöglicht sogar mehr, weil die Verordnung ja die Herrschaft der großen Plattformbetreiber aufbrechen will. Das heißt, es finden sich letztlich nur wenige Regelungen, die explizit auf Verringerung von Vulnerabilität und den hier angesprochenen Problemfeldern abzielen. Aufgrund der Komplexität des Themas wäre eine umfassende Regulierung hier auch kaum möglich.

Einige der bereits existierenden oder neu geschaffenen Regelungen leisten zweifelsohne Beiträge. Neben der DSGVO bringen auch DSA und DMA einige Verbesserungen für Datenschutz und Verbraucherrechte. Auch im Problemfeld (Cyber-)Sicherheit gibt es Regulierungen wie etwa die bereits 2016 geschaffene NIS-Richtlinie (EU-Richtlinie zur Netz- und Informationssicherheit). Sie macht Betreibern und Anbietern digitaler Dienste strengere Vorgaben für technische und organisatorische Mindeststandards zur Sicherung ihrer Netzwerke und Informationssysteme. Zudem müssen Sicherheitsvorfälle seitdem an die Behörden gemeldet werden. Die NIS-Richtlinie gilt als wichtiger Impulsgeber für mehr Cybersicherheit in Richtung mehr digitaler Souveränität (Bendiek/Stürzer 2022)[77]. Im Stromsektor ist vom Verbund der Europäischen Übertragungsnetzbetreiber eine spezifische Regulierung (Network Codes on Cybersecurity) geplant, die zu einer Erhöhung der Sicherheitsstandards im Europäischen Stromnetz führen soll.[78] Auch gibt es einige Anstrengungen in Deutschland und Europa, um die digitale Souveränität zu stärken, bei der es um ökonomische und technologische Handlungsfähigkeit geht (z. B. Bitkom 2019). Allerdings geht es hier eher um Wettbewerbsvorteile und die Stärkung digitaler Binnenmärkte als um die Erhöhung von Resilienz im Sinne von Sicherheit, Datenschutz und anderen Grundrechten.

***Höhere Sicherheitsstandards und digitale Souveränität nötig***

Ein wichtiger Aspekt zur Stärkung institutioneller wie individueller Handlungsfähigkeit als Gegenmaßnahme zum zunehmenden Kontrollverlust durch externe Technologien wäre etwa eine klare Regelung von Fernzugriffen. Das oben erwähnte BGH-Urteil ist ein kleiner Schritt in diese Richtung. Hier gibt es Bedarf an klaren Europäischen Vorschriften, die nicht nur auf einzelne Fälle oder Bereiche beschränkt sind, sondern generell die Möglichkeit zur Einschränkung wesentlicher Grundfunktionen über technische Fernzugriffe unterbindet.

Zudem sind nach derzeitigem Stand zwar viele Regulierungen bezüglich Plattformökonomie und Cybersicherheit vorhanden. Diese haben aber kaum Bezug zu den diversen Problemfeldern hinsichtlich Vulnerabilität und Resilienz gesellschaftlicher Infrastrukturen. Am ehesten in diese Richtung geht der aktuell diskutierte Entwurf für ein EU-Gesetz zur Cyberresilienz (Cyber Resilience Act – CRA).[79] Ziele dieses Gesetzesvorhabens sind unter anderem die Stärkung der

***Geplantes Gesetz zu Cyberresilienz***

[77] Siehe auch Abschnitt 4.2., S. 46.

[78] Die Maßnahme ist derzeit noch im Entwurfsstadium *eepublicdownloads.entsoe.eu/clean-documents/Network%20codes%20documents/NC%20CS/220114_NCCS_Legal_Text.pdf*.

[79] *digital-strategy.ec.europa.eu/en/library/cyber-resilience-act*.

Sicherheit von Hard- und Software während des gesamten Lebenszyklus und verbesserte Möglichkeiten für Unternehmen und Verbraucher zur sicheren Nutzung von Produkten mit digitalen Elementen. Das sind relevante Punkte, die zu einer Milderung einiger Probleme beitragen können, etwa durch Verbesserung von Mindeststandards für Datenschutz und Sicherheit in digitalen Technologien. Inwieweit das tatsächlich gelingt, ist derzeit nicht absehbar.

*Aufweichen von Verschlüsselung erhöht Vulnerabilität*

In mehrfacher Hinsicht problematisch sind dagegen die Pläne der EU-Kommission, die Möglichkeiten zur verschlüsselten Kommunikation aufzuweichen: Internetdienstanbieter wie digitale Plattformen sollen rechtlich zur Schaffung von Hintertüren in Technologien für Zugriffe durch die Strafverfolgung gezwungen werden. Zum einen könnte das zu einen erheblichen Ausbau staatlicher Überwachung privater Kommunikation führen – und damit zu einer Erosion der Privatsphäre (Krempl 2022a). Zum anderen könnten damit de facto essenzielle Sicherheitsstandards ausgehebelt werden. Selbst wenn man die Überwachungsproblematik außen vorlässt, würde das noch mehr Anreize für Missbrauch schaffen, da Hintertüren in Technologien Schwachstellen darstellen, die zu mehr Vulnerabilität führen. Bedenkt man zudem, dass gerade diese Internetdienstanbieter und Plattformen immer mehr mit Infrastruktursystemen vernetzt sind, stellt sich die Frage, wie man Resilienz stärken will, wenn man gleichzeitig Hintertüren einbauen lässt und damit die Vulnerabilität erhöht.

*Bedarf an Forschung, Digitalisierungs- und Sicherheitsexpertise*

Neben organisatorischen und regulatorischen Herausforderungen gibt es zudem erheblichen Bedarf an Forschung sowie inter- und transdisziplinärem Wissens- und Erfahrungsaustausch zwischen den verschiedenen Infrastrukturbereichen. Es gibt seit Jahren einen erheblichen Mangel an Expertise zu Digitalisierung, IT und Systemsicherheit in den klassischen Infrastruktursektoren, wie auch der deutsche Verband der Elektrotechnik, Elektronik und Informationstechnik (VDE) betont.[80] Vor allem im Strom- und Energiebereich ist das ein wachsendes Problem, das sich im wachsenden Fachkräftemangel widerspiegelt (vgl. Burstedde 2021; Allhutter et al. 2022). Wichtig wäre allerdings, dass beim Aufbau von Expertise stärker auf systemisches Wissen über die gesellschaftlichen Effekte vernetzter Infrastruktursysteme und die Problematik von wechselseitigen Abhängigkeiten geachtet wird. Denn diese beeinflussen wesentlich das Ausmaß an Vulnerabilität.

[80] *https://www.vde.com/de/presse/pressemitteilungen/cybersecurity-fachkraeftemangel-herausforderung-bei-energiewende*.

# 5 FAZIT UND AUSBLICK

*Digitalisierung und Vulnerabilität hängen eng zusammen*

Diese Überblicksstudie hat sich mit den komplexen Zusammenhängen zwischen Digitalisierung und Vulnerabilität gesellschaftlicher Infrastrukturen befasst. Im ersten Hauptteil (Abschnitte 1 und 2) wurden diese Zusammenhänge konzeptionell beleuchtet und die Rolle (digitaler) Technologien diskutiert. Im zweiten Hauptteil (Abschnitte 3 und 4) wurden Entwicklungsstand und Problemfelder anhand von Beispielen herausgearbeitet – sowie die gesellschaftlichen Folgen. Als zentrale Problemfelder ergaben sich mangelhafte Sicherheit, steigende ökonomische und technologische Abhängigkeiten, wachsende Informations- und Machtasymmetrien und schließlich eine Beeinträchtigung der Grundrechte.

*Ohne politisches Gegensteuern werden Infrastrukturen anfälliger werden*

Trotz der zahlreichen Problemfelder ist die Frage, ob Digitalisierung Infrastrukturen per se verwundbarer macht, nicht ohne Weiteres zu beantworten – die Vulnerabilität hängt naturgemäß sehr stark von den jeweiligen Rahmenbedingungen und konkreten Anwendungsfällen ab. Grundsätzlich muss mit der wachsenden Digitalisierung aber von einer weiteren Komplexitätssteigerung in gesellschaftlichen Infrastrukturen ausgegangen werden. Wenn diese Komplexität nicht entsprechend mit Governance und wirkungsvollen Steuerungsmaßnahmen beherrschbar gemacht wird, werden die Systeme anfälliger werden. In Summe steigt das Risiko für Störfälle aller Art. Ausfälle, die je nach Infrastrukturbereich unterschiedlich kritisch sein können, werden also wahrscheinlicher.

*Die Digitalisierung schafft in Haushalten oft unnötige Risiken*

Die in dieser Studie angeführten Beispiele in Abschnitt 3 und 4 zeigen, dass es bereits jetzt in unterschiedlichsten Bereichen erhebliche Probleme und entsprechend großen Handlungsbedarf gibt. Die Ambivalenz der Digitalisierung spiegelt sich auch im Energiebedarf digitaler Technologien wider (siehe Abschnitt 3.1). Das ist im Energiesektor besonders deutlich, in abgeschwächter Form aber auch im Mobilitätsbereich und vielen anderen Sektoren, die eng mit der Energiewende verbunden sind. In manchen Bereichen ist durchaus fragwürdig, welchem Zweck Digitalisierung folgt und ob sich – wie etwa im Haushalts- und Konsumbereich – Probleme und Risiken erhöhen.

*Die Marktmacht der Plattformbetreiber erschwert eine behutsame Digitalisierung*

In Summe pendelt die Digitalisierung von Infrastrukturen derzeit sehr stark zwischen real nötigem und konstruiertem Bedarf zur technologischen Umgestaltung. Starke marktwirtschaftliche Interessen von Technologieherstellern und Plattformbetreibern sowie die starke Marktmacht einiger dieser Akteure erschweren einen differenzierteren und womöglich behutsameren Umgang mit der Digitalisierung von Infrastrukturen. Digitalisierungsnotwendigkeiten werden meist mit Wirtschaftlichkeit oder Wettbewerbsfähigkeit begründet. Inwieweit dies tatsächlich zutrifft, bleibt jedoch oft vage. Insgesamt lastet ein sehr starker Druck zur Digitalisierung auf verschiedenen Branchen und gesellschaftlichen Bereichen.

Dieser Druck manifestiert sich auf institutioneller Ebene und wird über digitalisierte Anwendungen in verschiedenen Bereichen auch auf die individuelle Ebene, auf Personen wie Haushalte übertragen. Beispielhaft kann hier die Implementierung von 5G- und 6G-Mobilfunktechnologie gesehen werden, über deren Erfordernisse und Problematiken bislang wenig gesellschaftlicher Diskurs geführt

wurde. Das kann Bedenken und Ängste in der Bevölkerung verstärken. Das geht auch aus einem Bericht des Deutschen Bundestags hervor, der auf den geringen Wissenstand zu 5G-Technologien hinweist, der keine belastbaren Aussagen zum Fehlen von Gesundheitsrisiken zulässt und neben Forschungsbedarf die Relevanz von unvoreingenommenen Dialogen zwischen Wissenschaft, Öffentlichkeit und Politik betont (Deutscher Bundestag 2023). Zu ähnlichen Schlüssen kam auch eine Studie für das österreichische Parlament (Kastenhofer et al. 2020). Trotz etwaiger Bedenken und begrenztem Wissenstand zu möglichen gesellschaftlichen Risiken werden die Notwendigkeit zum weiteren Ausbau und ihre gesellschaftlichen Folgen kaum thematisiert. Entsprechendes gilt auch für andere Bereiche der Digitalisierung.

*Bedarf nach sachlichen gesellschaftlichen Debatten im Vorfeld*

Das hat zur Folge, dass zum Teil rasch digitalisiert wird, ohne längerfristige Konsequenzen und das Entstehen von Pfadabhängigkeiten zu berücksichtigen. Das wiederum begünstigt das Entstehen von Spannungen und von nicht antizipierten Problemfeldern. Allein die Vielzahl von Schwachstellen und entsprechender Cyberattacken führen die Verwundbarkeit von Infrastrukturen und damit der Gesellschaft als Ganzes vor Augen – und diese haben in den vergangenen Jahren deutlich zugenommen (siehe Abschnitt 3).

*Zu rasche Digitalisierung übersieht Schwachstellen und längerfristige Folgen*

Aufgrund der starken Abhängigkeit von digitalen Technologien scheint zugleich der Handlungsspielraum in den abhängigen Bereichen gering. Insofern sind Infrastrukturbereiche der Digitalisierung gewissermaßen ausgeliefert. Zwar ist das Problembewusstsein gerade im KRITIS-Umfeld bereits hoch, aber die Maßnahmen konzentrieren sich noch sehr stark auf den Umgang mit Cyberangriffen und den Problemkomplex Cybersicherheit generell. Es braucht darüber hinaus ein genaueres konzeptionelles Verständnis von Vulnerabilität.

*Schutzmaßnahmen konzentrieren sich zu sehr auf Angriffe*

Aus technisch-organisatorischer Sicht sind die größten Probleme immer noch mangelhafte Sicherheitsstandards und ganz besonders Systeme, die direkt mit dem Internet verbunden sind. Solche Infrastruktursysteme sind wesentlich vulnerabler als Systeme, die unabhängig und entsprechend abgesichert sind. Vulnerabilität resultiert nicht nur aus der Offenheit für Angriffe, sondern auch aus Fehler- und Störanfälligkeit (siehe Abschnitt 3 und 4). Externe Schnittstellen sowie der Vernetzungsgrad eines Infrastruktursystems und der daran gekoppelten Anwendungen sind dabei ein kritischer Faktor, für den es noch wesentlich mehr Bewusstsein braucht.

*Die starke Vernetzung ist ein großes und unterschätztes Sicherheitsproblem*

In Bereichen wie etwa dem Energiesektor ist auch ein Mangel an Fachexpertise Teil des Problems: Es braucht nicht nur Expertise zur digitalen Vernetzung, sondern auch kritisches systemisches Wissen über die sichere und sozialverträgliche Gestaltung von Infrastrukturen. Das gilt letztlich für alle Infrastrukturbereiche, auch die indirekten wie Mobilität und Haushalt.

Vulnerabilität von Infrastrukturen betrifft nicht nur physische oder technische Sicherheit und Schutz vor externen Bedrohungen, sondern vor allem Versorgungssicherheit von Wirtschaft und Gesellschaft und die Daseinsvorsorge generell. Da digitalisierte Infrastrukturen noch viel stärker in private Lebensbereiche hineinwirken, wirft das auch einige neue Fragen über sozialverträgliche Gestaltung von Technologien, die Bewahrung von Grundrechten wie dem Recht auf

*Versorgungssicherheit und Daseinsvorsorge müssen stärker in den Blick genommen werden*

Privatsphäre, informationelle Selbstbestimmung und Autonomie auf. Es braucht daher auch wirksamere regulatorische Maßnahmen (wie in Abschnitt 4 diskutiert). Ein einseitiger Fokus auf Cyberangriffe einerseits und auf Marktregulierung andererseits verstärkt jedoch technologische und ökonomische Abhängigkeiten eher als sie zu verringern.

*Durch die Möglichkeit von Fernzugriffen entsteht ein neues Machtmittel auf Seiten der Hersteller*

Der steigende Einfluss von Technologiebetreibern in unterschiedlichste Branchen verschärft die Abhängigkeiten und stärkt die Marktmacht einzelner Unternehmen weiter. Ein praktisches Beispiel für diese Macht liegt in der technischen Möglichkeit für Fernzugriffe oder Abschaltungen von Systemen. Das kann neben Auswirkungen auf Infrastrukturbetreiber oder Konsumenten im größeren Rahmen durchaus ein gesamtgesellschaftliches Problem werden, besonders dann, wenn diese Möglichkeiten gezielt als Machtmittel missbraucht werden. Diese Entwicklung ist auch demokratiepolitisch gefährlich. Das zeigen auch aktuelle Beispiele mit Bezug zum Ukraine-Krieg: Etwa das von Elon Musk betriebene Satellitensystem Starlink, das den ukrainischen Streitkräften bereitgestellt wurde, dann aber aus finanziellen Gründen mit Abschaltung gedroht wurde (Donath 2022). Ein weiteres Beispiel betrifft den US-Landmaschinenkonzern John Deere, der per Fernzugriff von ihm hergestellte Landmaschinen deaktivierte, nachdem diese in der Ukraine von russischen Truppen gestohlen wurden (Tangalakis-Lippert 2022). Das mag aus Gründen der Sympathie für den angegriffenen Staat als positiv erscheinen, verdeutlicht aber auch die Macht von Unternehmen, die aus Technologie resultiert. Diese Entwicklung sollte Staaten weitaus sensibler dafür machen, in welche Abhängigkeiten sie sich gegenüber privaten Akteuren begeben.

*Zunehmende Nutzung biometrischer Daten birgt neue Risiken*

Ähnliches gilt auch bei der steigenden Verbreitung biometrischer Technologien, die immer stärker in diverse Anwendungen integriert werden. Der Ausbau von Biometrie wird meist mit Sicherheitsgewinnen begründet. Doch welche Sicherheitsvorteile das de facto bringt und vor welchen Gefahren sie schützen, wird kaum thematisiert. Zudem bringt diese Entwicklung auch neue Risiken für Missbrauch sowie für staatliche und private Überwachung mit sich. Das ist beispielhaft für Technologien, die relativ beiläufig eingeführt werden, aber erhebliche gesellschaftliche Folgen nach sich ziehen.

*Die Vernachlässigung der Folgen digitalisierter Infrastrukturen kann Probleme verstärken*

Gerade die scheinbare Beiläufigkeit der Implementierung immer neuer digitaler Möglichkeiten, die Etablierung von „Digital Curtains“ vor Infrastrukturen, und die offensichtliche Macht von Technologiekonzernen werfen Probleme auf, die in der Gesellschaft meist nur unzureichend debattiert werden. Ein aktuelles Beispiel dieser mangelnden Vorsorge bietet die deutsche 5G-Infrastruktur: Im März 2023 forderte das Bundesinnenministerium die Netzbetreiber auf, eine Liste aller sicherheitsrelevanten Komponenten zu erstellen. Konkret geht es hier vor allem um integrierte Technologien chinesischer Hersteller wie Huawei und ZTE, die beim Ausbau des 5G-Netzes in Deutschland sowie in anderen Ländern häufig zum Einsatz kommen. Die Befürchtung ist, China könnte solche Komponenten nutzen, um Spionage zu betreiben oder die Funktion des Netzes zu beeinträchtigen. Die Untersuchung könnte auch eine aufwändige und kostspielige Deinstal-

lation der entsprechenden Komponenten nach sich ziehen.[81] Damit ist eine Fülle von rechtlichen, technischen und sicherheitsrelevanten Fragen verbunden. Das Beispiel verdeutlicht, welche Probleme die digitale Transformation ohne vorherige Prüfung über Nutzen und Risiken aufwerfen kann.

Digitalisierung gilt in vielen Bereichen schlicht als alternativlose Notwendigkeit zur Verbesserung von Wertschöpfungsketten. Die gesellschaftlichen Rahmenbedingungen für eine sozialverträgliche Gestaltung werden dabei eher vernachlässigt. Daher kann man sagen: Viele Probleme, die daraus für die Gesellschaft und die Individuen resultieren, sind nicht unbedingt dem Technikeinsatz geschuldet, sondern auch einer überproportional starken Kapitalisierung von Daten und der Etablierung von datengetriebenen Geschäftsmodellen der Plattformökonomie. Dies verstärkt auch das klassische Problem der zunehmende Informations- und Machtasymmetrien in der Gesellschaft (siehe Abschnitt 4).

*Nicht unbedingt die Technik ist das Problem, sondern die Geschäftsmodelle dahinter*

Die fortschreitende Digitalisierung von gesellschaftlichen Infrastrukturen wirft viele essenzielle Fragen auf, die zum Teil gerade erst neu verhandelt werden: Welche Akteure haben welche Form von Kontrolle über Infrastrukturen? Wie ist das Verhältnis zwischen staatlicher und privater Leistungserbringung bei der Daseinsvorsorge? Und wie kann die Resilienz von Infrastrukturen gestärkt werden, um die Grundversorgung weiterhin zu gewährleisten? Und zwar im Einklang mit den Grundrechten und Grundbedürfnissen – und auch unter dem wachsenden Stress von extremen Wetterlagen durch den anthropogenen Klimawandel.

Die digitale Transformation braucht sozialverträgliche und nachhaltige Technikgestaltung und gerade bei Infrastrukturen auch demokratische Legitimation. Die Beobachtung der wachsenden Vulnerabilität von Infrastrukturen und der invasive Charakter der digitalen Transformation sollte in Erinnerung rufen, dass Staat und Gesellschaft demokratisch legitimiert sind, der Einsatz von Technologie, zumal von privater Seite, aber immer legitimationsbedürftig ist. Das gilt besonders für die gesellschaftliche Grundversorgung. Wird das zu wenig beachtet, werden nicht nur die Infrastrukturen verletzlicher, sondern auch der Staat, der für sie Sorge trägt.

*Die digitale Transformation braucht nachhaltige und sozialverträgliche Technikgestaltung*

[81] *https://www.faz.net/aktuell/politik/inland/bmi-prueft-huawei-komponenten-beim-5-g-ausbau-auf-sicherheit-18730170.html*; *https://www.derstandard.at/story/2000144243807/berlin-verschaerft-gangart-gegen-5g-zulieferer-aus-china*.

# 6 LITERATUR


Abrahamczyk, M. (2022) Systemausfall droht: Großer Tesla-Rückruf, 01.09., t-online, *https://www.t-online.de/auto/elektromobilitaet/elektroauto/id_100046900/systemausfall-droht-grosser-tesla-rueckruf.html*.

Abril, D., Harwell, D. (2021) Keystroke tracking, screenshots, and facial recognition: The boss may be watching long after the pandemic ends, 24.09., Washington Post online, *https://www.washingtonpost.com/technology/2021/09/24/remote-work-from-home-surveillance/*.

ACER – European Union Agency for the Cooperation of Energy Regulators (2022) Draft framework guidelines on demand response.

Ahmed, W.A.H., Rios, A., (2022) Chapter 18 – Digitalization of the international shipping and maritime logistics industry: a case study of TradeLens, in: MacCarthy, B.L., Ivanov, D. (Eds.), The Digital Supply Chain. Elsevier, pp. 309–323. *https://doi.org/10.1016/B978-0-323-91614-1.00018-6*.

Aichholzer, G., Gudowsky, N., Saurwein F., Rhomberg, W., Weber, M., Wepner, B. (2016) Industrie 4.0: Foresight & Technikfolgenabschätzung zur gesellschaftlichen Dimension der nächsten industriellen Revolution. Zusammenfassender Endbericht.

Allhutter, D., Bettin, S., Brunner, Helfried., Kleinferchner, J., Krieger-Lamina, J., Ornetzeder, M., Strauß, S., Weber, M., Nentwich, M., (2022) Sichere Stromversorgung und Blackout-Vorsorge in Österreich. Entwicklungen, Risiken und mögliche Schutzmaßnahmen (Endbericht) (No. ITA-AIT-17). Institut für Technikfolgen-Abschätzung (ITA) und AIT Austrian Institute of Technology, Wien. *https://doi.org/10.1553/ITA-pb-AIT-17*.

Alstone, P., Gershenson, D., Kammen, D.M., (2015) Decentralized energy systems for clean electricity access. Nat. Clim. Change 5, 305–314. *https://doi.org/10.1038/nclimate2512*.

Arthur, C. (2013) Tech giants may be huge, but nothing matches big data. The Guardian, 23. August, *https://www.theguardian.com/technology/2013/aug/23/tech-giants-data*.

Baylon, C., Brunt, R., Livingstone, D. (2015) Cyber Security at Civil Nuklear Facilities – Understanding the Risks. Chatham House Report. Royal Institute of International Affairs, London.

BBK – Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2022) 10 Jahre „KRITIS-Strategie" Einblicke in die Umsetzung der Nationalen Strategie zum Schutz Kritische Infrastrukturen. *https://www.bbk.bund.de/SharedDocs/Downloads/DE/Mediathek/Publikationen/PiB/PiB-21-zehn-jahre-kritis-strategie.pdf?__blob=publicationFile&v=7*.

Bendiek, A., Stürzer, I. (2022) Die digitale Souveränität der EU ist umstritten. April 30, SWP-Aktuell Nr. 30, *https://www.swp-berlin.org/publications/products/aktuell/2022A30_DigitaleSouveraenitaetEU.pdf*.

Bettin, S.S. (2020) Electricity infrastructure and innovation in the next phase of energy transition—amendments to the technology innovation system framework, Review of Evolutionary Political Economy, 1(3), pp. 371–395. *https://doi.org/10.1007/s43253-020-00021-4*.

Beutler, F., Brümmer, U., Ertner, S., Evenson, D., Obermauer, R., Schroeder, W. (2021) Transformation der Automobilindustrie. Böll.brief Grüne Ordnungspolitik #18. Heinrich Böll Stiftung, *https://www.boell.de/sites/default/files/2021-12/boell.brief%20G18%20Transformation%20der%20Automobilindustrie.pdf*.

Birkmann, J., Bach, C., Guhl, S., Witting, M., Welle, T., Schmude, M. (2010) State of the Art der Forschung zur Verwundbarkeit kritischer Infrastrukturen (No. 2). Forschungsforum.

Bitkom (2019) Digitale Souveränität: Anforderungen an Technologie- und Kompetenzfelder mit Schlüsselfunktion. Stellungnahme, Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. *https://www.bitkom.org/sites/default/files/2020-01/200116_stellungnahme_digitale-souveranitat.pdf*.

Bowker, C.G., Baker, K., Miller and, F., Ribes, D. (2010) Toward Information Infrastructure Studies: Ways of Knowing in a Networked Environment. In: International Handbook of Internet Research, pp. 97-117.

Brinkmann, H., Harendt, C., Heinemann, F. & Nover, J. (2017) Ökonomische Resilienz – Schlusselbegriff für ein neues wirtschaftspolitisches Leitbild? Inklusives Wachstum für Deutschland Band 11. Gütersloh: Bertelsmann Stiftung.

BSI – Bundesamt für Sicherheit in der Informationstechnik (2013) ICS-Security-Kompendium Version 1.23, *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security-Kompendium-Hersteller.pdf*.

BSI – Bundesamt für Sicherheit in der Informationstechnik (2014) UP KRITIS: Öffentlich-Private-Partnerschaft zum Schutz Kritischer Infrastrukturen. Grundlagen und Ziele, Bundesamt für Sicherheit in der Informationstechnik Geschäftsstelle UP KRITIS *https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/bevoelkerungsschutz/up-kritis-fortschreibung.pdf;jsessionid=452715D22F6467EB3AD7D74446006A1F.2_cid295?__blob=publicationFile&v=4*.

BSI – Bundesamt für Sicherheit in der Informationstechnik (2022a) Cybersicherheit für Weltrauminfrastrukturen: Positionierung des Bundesamts für Sicherheit in der Informationstechnik, Bundesamt für Sicherheit in der Informationstechnik (BSI), *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Weltrauminfrastrukturen/Cyber-Sicherheit_Weltrauminfrastrukturen.pdf?__blob=publicationFile&v=3*.

BSI – Bundesamt für Sicherheit in der Informationstechnik (2022b) IT-Grundschutz-Kompendium *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2022.pdf?__blob=publicationFile&v=3#download=1*.

Bürkner, H.J. (2010) Vulnerabilität und Resilienz: Forschungsstand und sozialwissenschaftliche Untersuchungsperspektiven. IRS Leipzig für Regionalentwicklung und Strukturplanung.

Burstedde, A. (2021) Digitalisierung der Wirtschaft in Deutschland Kompetenzbarometer: Fachkräftesituation in Digitalisierungsberufen – Beschäftigungsaufbau und Fachkräftemangel. Studie im Auftrag des Bundesministeriums für Wirtschaft und Klimaschutz, *https://www.iwkoeln.de/fileadmin/user_upload/Studien/Gutachten/PDF/2022/Fachkr%C3%A4ftesituation_in_Digitalisierungsberufen.pdf*.

Cassotta, S., Sidortsov, R., (2019) Sustainable cybersecurity? Rethinking approaches to protecting energy infrastructure in the European High North. Energy Res. Soc. Sci. 51, 129–133. *https://doi.org/10.1016/j.erss.2019.01.003*.

Chen, N., Chen, Y. (2018) Smart City Surveillance at the Network Edge in the Era of IoT: Opportunities and Challenges. In: Mahmood, Z. (eds) Smart Cities. Computer Communications and Networks. Springer, Cham. pp 153–176. *https://doi.org/10.1007/978-3-319-76669-0_7*.

Christensen, T.H., Friis, F., Bettin, S., Throndsen, W., Ornetzeder, M., Skjølsvold, T.M., Ryghaug, M., (2020) The role of competences, engagement, and devices in configuring the impact of prices in energy demand response: Findings from three smart energy pilots with households. Energy Policy 137, 111142. *https://doi.org/10.1016/j.enpol.2019.111142*.

Corera, G. (2022) Chinese technology poses major risk – GCHQ Chief, 11.10., BBC News, *https://www.bbc.com/news/uk-63207771?at_medium=RSS&at_campaign=KARANGA*.

Creutzig, F., (2021) From smart city to digital urban commons: Institutional considerations for governing shared mobility data. Environ. Res. Infrastruct. Sustain. 1, 025004. *https://doi.org/10.1088/2634-4505/ac0a4e*.

Cyrus, C. (2021) IoT Cyberattacks Escalate in 2021, According to Kaspersky, 17.09., IoT world today, *https://www.iotworldtoday.com/2021/09/17/iot-cyberattacks-escalate-in-2021-according-to-kaspersky/*.

David, P.A., (1985) Clio and the Economics of QWERTY. The American Economic Review 75, 332–337. *http://www.jstor.org/stable/1805621*.

Dettmer, H., Doms, T., Schwald, C., Spahovic, E. (2019) Iot im Smart Home – Seitenkanalangriffe als neue Angriffsform. TÜV Austria. *https://www.tuv.at/fileadmin/user_upload/tuv-austria-white-paper-v-iot-im-smart-home_web.pdf*.

Deutscher Bundestag (2023) Drucksache 20/5646: Technikfolgenabschätzung. Seite 140ff. Berlin: Bundestag. *https://dserver.bundestag.de/btd/20/056/2005646.pdf*.

Diedrich, O. (2015) Sicherheitsforscher: Autos können auch per Digitalradio gehackt werden, 26.07., Heise online, *https://www.heise.de/security/meldung/Sicherheitsforscher-Autos-koennen-auch-per-Digitalradio-gehackt-werden-2763086.html*.

Donath, A. (2022) Musk droht wohl mit Abschaltung von Starklink für die Ukraine. 14.10., Golem, *https://www.golem.de/news/satelliteninternet-musk-droht-wohl-mit-abschaltung-von-starlink-fuer-die-ukraine-2210-168946.html*.

Drossel, WG., Ihlenfeldt, S., Langer, T., Dumitrescu, R. (2018) Cyber-Physische Systeme. In: Neugebauer, R. (eds) Digitalisierung. Springer Vieweg, Berlin, Heidelberg. *https://doi.org/10.1007/978-3-662-55890-4_12*.

Dürig, M., Fischer, M. (2018) Cybersicherheit in kritischen Infrastrukturen. In: Datenschutz und Datensicherheit (DuD) **42**, pages 209–213 (2018) *https://link.springer.com/article/10.1007/s11623-018-0909-1*.

Edmunds, D. R., (2020) Smart vacuums could allow hackers a view inside your home – researchers, 26.02., Jerusalem Post online, *https://www.jpost.com/HEALTH-SCIENCE/Smart-vacuums-could-allow-hackers-a-view-inside-your-home-researchers-618919*.

EDRi – European Digital Rights initiative (2022) Public statement on new crisis response mechanism and other last minute additions to the DSA *https://edri.org/wp-content/uploads/2022/04/EDRi-statement-on-CRM.pdf*.

EKI – (2008) EU-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 *https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32008L0114&from=DE*.

Ekman, A. (2019) China's Smart Cities: The New Geopolitical Battleground. Études de l'Ifri, Ifri, December, French Institute of International Affairs. *https://www.ifri.org/sites/default/files/atoms/files/ekman_smart_cities_battleground.pdf*.

Enkhardt, S. (2022a) Kulanzregelung: Nach Fernabschaltung der Photovoltaik-Speicher zahlt Senec 25 Euro pro angefangener Woche. 14.03., PV Magazin online, *https://www.pv-magazine.de/2022/03/14/kulanzregelung-nach-fernabschaltung-der-photovoltaik-speicher-zahlt-senec-25-euro-pro-angefangener-woche/*.

Enkhardt, S. (2022b) BSI erlässt Übergangsregelung für Fortsetzung des Smart-Meter-Rollouts. pv magazine Deutschland, *https://www.pv-magazine.de/2022/05/23/bsi-erlaesst-uebergangsregelung-fuer-fortsetzung-des-smart-meter-rollouts/*.

EUSPA – European Union Agency for the Space Programme (2022) Satellite navigation at core of future connected car systems, *https://www.gsc-europa.eu/news/satellite-navigation-at-core-of-future-connected-car-systems-3*.

Floridi, L. (2010) Ethics after the information revolution. In: Floridi, L. (ed.), The Cambridge Handbook of Information and Computer Ethics. Cambridge/UK: Cambridge University Press, 3-19.

Futurezone (2021) Ausfall bei Tesla-App: Probleme beim Öffnen der Fahrzeuge, 20.11., Futurezone online, *https://futurezone.at/produkte/ausfall-tesla-app-probleme-beim-oeffnen-model-3-serverausfall-fehler/401813197*.

Galič, M., (2022), Smart Cities as 'Big Brother only to the Masses': The Limits of Personal Privacy and Personal Surveillance (September 5, 2022). Surveillance & Society 2022, Available at SSRN: *https://ssrn.com/abstract=4228444* or *http://dx.doi.org/10.2139/ssrn.4228444*

Gheorghe, A., Weijnen, Margot, Masera, Marcelo, Bouwmans, I., (2006) Introduction, in: Gheorghe, A.V., Masera, M., Weijnen, M., Vries, D.L. (Eds.), Critical Infrastructures at Risk: Securing the European Electric Power System. Springer Netherlands, Dordrecht, pp. 1–18. *https://doi.org/10.1007/1-4020-4364-3_1*.

Greis, F. (2022) Fernabschaltung gemieteter Batterien ist unzulässig. 26.10., Golem, *https://www.golem.de/news/bgh-urteil-fernabschaltung-gemieteter-batterien-ist-unzulaessig-2210-169241.html*.

Gstaltmeyr, A. (2020) Von Updates bis zum Datenschutz: Was im Smart Home schief läuft. 16.10., Der Standard online, *https://www.derstandard.at/story/2000115279759/was-im-smart-home-schieflaeuft-von-updates-bis-zum-datenschutz*.

Harder, S. (2014) Bremsenversagen via Bluetooth, 11.08, Spiegel Online, *https://www.spiegel.de/auto/aktuell/hacker-koennen-autos-ueber-funkverbindungen-aus-der-ferne-angreifen-a-985464.html*.

Hasan, M. (2022) State of IoT 2022: Number of connected IoT devices growing 18% to 14.4 billion globally. 18.05., IoT blog, *https://iot-analytics.com/number-connected-iot-devices/*.

Henschke, A. (2020) Privacy, the Internet of Things and State Surveillance: Handling Personal Information within an Inhuman System. Moral Philosophy and Politics 7(1): 123-149 *https://doi.org/10.1515/mopp-2019-0056*.

Hern, A. (2016) Revolv devices bricked as Google's Nest shuts down smart home company. 05.04., Guardian online, *https://www.theguardian.com/technology/2016/apr/05/revolv-devices-bricked-google-nest-smart-home*.

Hilary, G. (2017) WannaCry and the Diffusion of Zero Day Exploits. CREOGN Research Note no.25, hal-03225147. *https://hal.archives-ouvertes.fr/hal-03225147/document*.

Hirschl, B., Aretz, A., Bost, M., Tapia, M., Gößling-Reisemann, S., (2018) Vulnerabilität und Resilienz des digitalen Stromsystems. Schlussbericht. Institut für ökologische Wirtschaftsforschung (IÖW) und Universität Bremen, Fachgebiet Resiliente Energiesysteme, Berlin und Bremen.

Hubik, F., Menzel, S., Tyborski, R. (2022) So überfordert die Software-Entwicklung Deutschlands Autobauer, 17.06., Handelsblatt online *https://app.handelsblatt.com/unternehmen/bmw-vw-und-mercedes-so-ueberfordert-die-software-entwicklung-deutschlands-autobauer/28415862.html*.

IBH – Informations- und Beratungszentrum Hochwasservorsorge Rheinland-Pfalz (2017) Leitfaden zur Hochwasserrisikoanalyse für kritische Infrastrukturen, *https://hochwassermanagement.rlp-umwelt.de/servlet/is/200124/Leitfaden_Risikoanalyse_kritische_Infrastruktur.pdf?command=downloadContent&filename=Leitfaden_Risikoanalyse_kritische_Infrastruktur.pdf*.

IBM (2022) IoT, edge computing, and AI combine to disrupt the automotive industry, IBM online *https://www.ibm.com/cloud/architecture/architectures/automotive/*.

IEA – International Energy Agency (2017) Commentary: Who wants to be in charge? International Energy Agency, Paris.

IEA – International Energy Agency (2021) Enhancing cyber resilience in electricity systems. Electricity security 2021. Report, *https://iea.blob.core.windows.net/assets/0ddf8935-be23-4d5f-b798-3aad1f32432f/Enhancing_Cyber_Resilience_in_Electricity_Systems.pdf*.

IEA – International Energy Agency (2022a) Smart Grids, IEA, Paris *https://www.iea.org/reports/smart-grids*.

IEA – International Energy Agency (2022b) Digitalisation, IEA, Paris *https://www.iea.org/reports/digitalisation*.

Ivanova, M., (2022) Cyber Security in Public Transport Networks. TRONTEQ. *https://www.tronteq.com/en/cyber-security-in-public-transport-networks/*.

Kafle, K. et al. (2021) 'Security in Centralized Data Store-Based Home Automation Platforms: A Systematic Analysis of Nest and Hue', ACM Trans. Cyber-Phys. Syst., 5(1). *https://doi.org/10.1145/3418286*.

Kastenhofer, K., Mesbahi, Z., Schaber, F. (2020) 5G-Mobilfunk und Gesundheit. Studie im Auftrag des Österreichischen Parlaments. Wien, Jänner, doi:/10.1553/ITA-pb-ITA-AIT-11.

Kenney, Martin, and John Zysman. (2016) The Rise of the Platform Economy. *Issues in Science and Technology 32*, no. 3 (Spring 2016). *https://issues.org/rise-platform-economy-big-data-work/*.

Kirchner, S. (2021) Kommt jetzt die Plattformgesellschaft? Grundlagen, Organisationen und Perspektiven in der digitalen Transformation. Working Paper „Fachgebiet Digitalisierung der Arbeitswelt", Nr. 03, Technische Universität Berlin: Berlin. *https://www.da.tu-berlin.de/fileadmin/i62_datypo3/PDF/DP_No_3_Paper.pdf*.

Kollewe, J., (2022) Major UK transport company Go-Ahead battles cyber-attack. The Guardian. URL *https://www.theguardian.com/business/2022/sep/06/go-ahead-cyberattack-bus-services-thameslink-rail*.

Krauss, K., Moll, C., Köhler, J., Axhausen, K.W., (2022) Designing mobility-as-a-service business models using morphological analysis. Res. Transp. Bus. Manag. 100857. *https://doi.org/10.1016/j.rtbm.2022.100857*.

Krempl, S. (2022a) „Böses Problem“ Verschlüsselung: EU-Staaten wollen Sicherheitslücken ausnutzen. 04.10., Heise online, *https://www.heise.de/news/Boeses-Problem-Verschluesselung-EU-Staaten-wollen-Sicherheitsluecken-ausnutzen-7284074.html*.

Krempl, S. (2022b) Bahn-App: Bürgerrechtler klagen gegen „DB Schnüffel-Navigator“. 20.10., Heise online, *https://www.heise.de/news/Bahn-App-Buergerrechtler-klagen-gegen-DB-Schnueffel-Navigator-7314938.html?utm_source=pocket-newtab-global-de-DE*.

Krempl, S. (2022c) Viasat: Wiper-Malware hat Ausfall des Satellitennetzwerks KA-Sat verursacht. 02.04., Heise online, *https://www.heise.de/news/Viasat-Wiper-Malware-hat-Ausfall-des-Satellitennetzwerks-KA-Sat-verursacht-6661499.html*.

Krisher, T. (2022) US report: Nearly 400 crashes of automated tech vehicles. Associated press, June 15, *https://apnews.com/article/self-driving-car-crash-data-ae87cadec79966a9ba56e99b4110b8d6*.

Kynge, J., Hopkins, V., Warrell, H., Hille, K. (2021) Exporting Chinese surveillance: the security risks of ‘smart cities’, 09.06., Financial Times online, *https://www.ft.com/content/76fdac7c-7076-47a4-bcb0-7e75af0aadab*.

Lambert, F. (2022) Tesla locks 80 miles of customer’s battery range for $4,500 ransom. Electrek July 26, *https://electrek.co/2022/07/26/tesla-ransom-customer-over-80-miles-battery-range/*.

Lechner, U. (2017) Verwundbarkeiten und Sicherheitsstrategien in kritischen Infrastrukturen. Ökologisches Wirtschaften – Fachzeitschrift, 32(4), 19–21. *https://doi.org/10.14512/OEW320419*.

Lehner, K. (2022) Krieg als Faktor: EU baut Starlink-Alternative auf. 18.02., ORF online, *https://orf.at/stories/3305570/*.

Leimbach, T., Hallinan, D., Bachlechner, D., Weber, A., Jaglo, M., Hennen, L., Nielsen, R., Nentwich, M., Strauß, S., Lynn, T. and Hunt, G. (2014) Potential and Impacts of Cloud Computing Services and Social Network Websites—Study. Report no. IP/A/STOA/FWC/2008-096/Lot4/C1/SC8; Science and Technology Options Assessment—European Parliamentary Research Service: Brussels.

Lenz, S. (2009) Vulnerabilität Kritischer Infrastrukturen. Forschung im Bevölkerungsschutz Band 4, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Bonn.

Mattheis, P. (2022) Chinas Überwachungsstaat weitreichender als gedacht, 22.06., *https://www.derstandard.at/story/2000136787294/chinas-ueberwachungsstaat-weitreichender-als-gedacht*.

Mayer-Schönberger, V., Cukier, K. (2013) Big Data: a revolution that will transform how we live, work and think. Boston, MA/New York: Houghton Mifflin Harcourt.

Megas, K. N., Fagan, M., Cuthill, B., Raguso, M., Wiltberger, J. (2021) Workshop Summary Report for „Cybersecurity Risks in Consumer Home Internet of Things (IoT) Devices“ Virtual Workshop. National Institute of Standards and Technology (NIST) *https://doi.org/10.6028/NIST.IR.8333*.

Menski, U. (2016) Neue Strategien der Ernährungsnotvorsorge, Ergebnisse aus dem Forschungsverbund NeuENV, Forschungsforum öffentliche Sicherheit, Schriftenreihe Sicherheit Nr. 18, *https://refubium.fu-berlin.de/bitstream/handle/fub188/17786/sr_18_a.pdf?sequence=1&isAllowed=y*.

Miller, K. (2022) What Happens When the Company Behind Your Smart Home Devices Suddenly Disappears? 04.20., InsideHook, *https://www.insidehook.com/daily_brief/tech/insteon-ihome-smart-home-shut-down*.

Minh, Q.N., Nguyen, V-H., Quy, V.K., Ngoc, L.A., Chehri, A. (2022) Edge Computing for IoT-Enabled Smart Grid: The Future of Energy. Energies 2022, 15,6140, *https://www.mdpi.com/1996-1073/15/17/6140/pdf*.

Montevecchi, F., Stickler, T., Hintemann, R., Hinterholzer, S. (2020) Energy-efficient Cloud Computing Technologies and Policies for an Eco-friendly Cloud Market. Final Study Report. Vienna.

Morgner, P. Mattejat, S. Benenson, Z., Müller, C. und Armknecht, F. (2017b) Insecure to the touch: Attacking ZigBee 3.0 via Touchlink Commissioning. In: Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks – WiSec ‘17, S. 230–240. Boston, MA, USA. *http://dl.acm.org/citation.cfm?doid=3098243.3098254*.

Murphy, M., Fasse, M. (2022) Industrie fürchtet Angriffe auf Satelliten: „Europa würde hart getroffen werden“. *https://www.handelsblatt.com/technik/it-internet/ukraine-krieg-industrie-fuerchtet-angriffe-auf-satelliten-europa-wuerde-hart-getroffen-werden/28724338.html*.

Nakashima, E., Timberg, C. (2017) NSA officials worried about the day its potent hacking tool would get loose. Then it did. Washington Post Mai 17, *https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html*.

Naveen, P. (2016) Cloud computing for energy management in smart grid – an application survey. IOP Conf. Ser.: Mater. Sci. Eng. 121 012010 *https://iopscience.iop.org/article/10.1088/1757-899X/121/1/012010/pdf*.

Nedelea, A. (2022) Hacker Says He Has 'Full Remote Control' Of Over 25 Teslas, 12.01., Inside EVs, *https://insideevs.com/news/560350/hacker-full-control-25-teslas/*.

Nguyen-Duc, A. (2020). An Analytical Framework for Planning Minimum Viable Products. In: Nguyen-Duc, A., Münch, J., Prikladnicki, R., Wang, X., Abrahamsson, P. (eds) Fundamentals of Software Startups. Springer, Cham. *https://doi.org/10.1007/978-3-030-35983-6_5*.

NLT (2022) Dutch employee fired by U.S. firm for shutting off webcam awarded €75,000 in court. 09.10., NL Times online, *https://nltimes.nl/2022/10/09/dutch-employee-fired-us-firm-shutting-webcam-awarded-eu75000-court*.

O'Donnell, L. (2019) Top 10 IoT Disasters of 2019. 23.12., Threat post, *https://threatpost.com/top-10-iot-disasters-of-2019/151235/*.

Oracle (2015): Oracle Buys Datalogix Creates the World's Most Valuable Data Cloud to Maximize the Power of Digital Marketing. Company presentation, January 23. Online: *www.oracle.com/us/corporate/acquisitions/datalogix/general-presentation-2395307.pdf*.

Ornetzeder, M., Bettin, S., Pavlicek, A., (2020) E-Fahrzeuge in Wiener Flotten, ITA-Dossier. Institut für Technikfolgen-Abschätzung, Wien.

Ornetzeder, M., Sinozic, T., Gutting, A., Bettin, S., (2017) Case study report: Austria Findings from case studies of Model Village Köstendorf, HiT Housing Project and VLOTTE (No. MATCH Deliverable D2.1), Institute of Technology Assessment, Austrian Academy of Sciences.

Parag, Y., Sovacool, B.K., (2016) Electricity market design for the prosumer era. Nat. Energy 1, 16032. *https://doi.org/10.1038/nenergy.2016.32*.

Patterson, B. (2020) Osram says it's turning off cloud servers for Lightify smart bulbs next August, 11.03., TechHive, *https://www.techhive.com/article/578405/osram-turning-off-cloud-servers-for-lightify-smart-bulbs-next-august.html*.

Pearson, I.L.G., (2011) Smart grid cyber security for Europe. Energy Policy 39, 5211–5218. *https://doi.org/10.1016/j.enpol.2011.05.043*.

Peissl, W., Čas, J., Sterbik-Lamina, J., Suschek-Berger, J., (2012) Smart New World? Key Factors for an Effective and Acceptable Deployment of Smart Meters – Projekt-Endbericht. Institut für Technikfolgen-Abschätzung (ITA), Wien.

Pillau, F. (2021) Car2X: Schneller Datenaustausch zwischen Autos mit 5G und dezentralen Computern. 29.06., Heise online, *https://www.heise.de/hintergrund/Car2X-Schneller-Datenaustausch-unter-Autos-mit-5G-und-dezentralen-Computern-6122523.html*.

Presse (2011) Auto-Bremsen per Bluetooth und MP3-Trojaner gehackt, 16.03., Die Presse online, *https://www.diepresse.com/642320/auto-bremsen-per-bluetooth-und-mp3-trojaner-gehackt*.

Proschofsky, A. (2022) Tausende Kärntner Haushalte wegen Softwarefehlers zum Jahreswechsel ohne Warmwasser, DER STANDARD. *https://www.derstandard.at/story/2000132308073/jahr-2022-bug-tausende-kaerntner-haushalte-wegen-softwarefehlers-zum-jahreswechsel*.

PTP – Pen Test Partners (2021) Smart car chargers. Plug-n-play for hackers?, 30.07, PTP security blog, *https://www.pentestpartners.com/security-blog/smart-car-chargers-plug-n-play-for-hackers/*.

PWC – Pricewaterhouse Cooopers (2017) eascy – die fünf Dimensionen der Transformation der Automobilindustrie. *https://www.pwc.de/de/automobilindustrie/pwc_automotive_eascy-studie.pdf*.

Qi, J., Hahn, A., Lu, X., Wang, J., Liu, C.-C., (2016) Cybersecurity for distributed energy resources and smart inverters. IET Cyber-Phys. Syst. Theory Appl. 1, 28–39. *https://doi.org/10.1049/iet-cps.2016.0018*.

Qian, I., Xiao, M., Mozur, P. and Cardia, A. (2022) Four Takeaways From a Times Investigation Into China's Expanding Surveillance State. 21.06., New York Times online, *https://www.nytimes.com/2022/06/21/world/asia/china-surveillance-investigation.html*.

Riso, S. (2021) Monitoring and surveillance of workers in the digital age. Eurofound research digest, Dec. 15, European Foundation for the Improvement of Living and Working Conditions, *https://www.eurofound.europa.eu/data/digitalisation/research-digests/monitoring-and-surveillance-of-workers-in-the-digital-age*.

Sajid, A., Abbas, H., Saleem, K., (2016) Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges. IEEE Access 4, 1375–1384. *https://doi.org/10.1109/ACCESS.2016.2549047*.

SAM (2021) IoT Security Landscape 2021, SAM seamless network *https://iotac.eu/sam-more-than-1-billion-iot-attacks-in-2021/*.

Sawall, A. (2022) EU beschließt LEO-Satelliteninternet für Kriegszeiten. Golem, 18.11., *https://www.golem.de/news/iris-eu-beschliesst-leo-satelliteninternet-2211-169878.html*.

Schaber, F., Krieger-Lamina, J., Peissl, W. (2019) Digitale Assistenten. Institut für Technikfolgen-Abschätzung der Österreichischen Akademie der Wissenschaften, Studie in Kooperation mit der Bundesarbeitskammer. *https://www.arbeiterkammer.at/beratung/konsument/Datenschutz/Studie_Alexa_Sprachassistenten_2019.pdf*.

Schaber, F., Strauß, S., Peissl, W. (2020) Der Körper als Schlüssel? Biometrische Methoden für Konsument:innen. Institut für Technikfolgen-Abschätzung der Österreichischen Akademie der Wissenschaften, Studie in Kooperation mit der Bundesarbeitskammer. *https://www.arbeiterkammer.at/infopool/akportal/Der_Koerper_als_Schluessel-Biometrische_Methoden_fuer_Konsum.pdf*.

Schesswendter, R. (2015) Nach Fernsteuerungs-Hack ruft Fiat Chrysler 1,4 Millionen Autos zurück. 24.07., Heise online, *https://www.heise.de/newsticker/meldung/Nach-Fernsteuerungs-Hack-ruft-Fiat-Chrysler-1-4-Millionen-Autos-zurueck-2762914.html*.

Schmid, F. (2015) Samsung warnt Nutzer, nichts Privates vor Smart-TV zu besprechen. 09.02., Der Standard online, *https://www.derstandard.at/story/2000011440822/samsung-warnt-nutzer-nichts-privates-vor-smart-tv-zu-besprechen*.

Shea, S. (2020) The Mirai IoT botnet holds strong in 2020. TechTarget, *https://www.techtarget.com/searchsecurity/feature/The-Mirai-IoT-botnet-holds-strong-in-2020*.

Shead, S., (2022) Hackers can bring ships and planes to a grinding halt. And it could become much more common. 27.06., CNBC. *https://www.cnbc.com/2022/06/27/hackers-can-now-bring-cargo-ships-and-planes-to-a-grinding-halt.html*.

Siddiqui, F., Lerman, R., Merrill, J. (2022) Teslas running Autopilot involved in 273 crashes reported since last year. Washington Post, June 15, *https://www.washingtonpost.com/technology/2022/06/15/tesla-autopilot-crashes/*.

Sperstad, I.B., Kjølle, G.H., Gjerde, O. (2020) A comprehensive framework for vulnerability analysis of extraordinary events in power systems. Reliability Engineering and System Safety 196, *https://doi.org/10.1016/j.ress.2019.106788*.

Spiegel (2022) US-Geheimdienst untersucht Cyberangriff auf Satelliteninternet, 13.03., Spiegel online, *https://www.spiegel.de/netzwelt/web/viasat-nsa-untersucht-hacker-angriff-auf-satellitennetzwerk-a-caab89d0-7eac-444f-b488-b51369762749*.

Spinsante, S., Stallo, C. (2020) Hybridized-GNSS Approaches to Train Positioning: Challenges and Open Issues on Uncertainty. Sensors 20(7): 1885. doi: *10.3390/s20071885*.

Srnicek, N., (2017) Platform Capitalism. Cambridge: Polity Press.

Standard (2022a) Tesla: Sicherheitslücke erlaubt unkompliziertes Stehlen des E-Autos, 08.06., Der Standard online, *https://www.derstandard.at/consent/tcf/story/2000136376428/tesla-sicherheitsluecke-erlaubt-unkompliziertes-stehlen-des-e-autos*.

Standard (2022b) US-Untersuchung von Teslas „Autopilot"-System ausgeweitet, 10.06., Der Standard online, *https://www.derstandard.at/story/2000136444484/us-untersuchung-von-teslas-autopilot-system-ausgeweitet*.

Standard (2022c) Mikrotransaktionen im Auto: BMW bietet nun Sitzheizung gegen Gebühr im Abo an, 13.07., Der Standard online, *https://www.derstandard.at/story/2000137412974/mikrotransaktionen-im-auto-bmw-bietet-nun-sitzheizung-gegen-gebuehr-im*.

Standard (2022d) Tesla drosselt Akku eines Kunden und zwingt ihn zur Zahlung von 4.500 Dollar, 30.07., Der Standard online, *https://www.derstandard.at/story/2000137905623/tesla-drosselt-akku-eines-kunden-und-verlangt-zahlung-von-4*.

Star, S.L. & Bowker, G.C. (2006) How to infrastructure. In: L.A. Lievrouw & S. Livingstone (Eds), Handbook of New Media: Social Shaping and Social Consequences of ICTs (pp. 230-245. London: Sage.

Sterner, M., Stadler, I., Eckert, F., Gerhardt, N., von Olshausen, C., Thema, M., Trost, T., (2019) Storage Integration for Coupling Different Energy Sectors, in: Sterner, M., Stadler, I. (Eds.), Handbook of Energy Storage: Demand, Technologies, Integration. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 757–803. *https://doi.org/10.1007/978-3-662-55504-0_14*.

Straub, D. (2022) Hacker in Italien spionierten tausende Haushalte mit Webcams aus, 10.06., Standard online, *https://www.derstandard.at/story/2000136429640/hacker-in-italien-spionierten-tausende-haushalte-mit-webcams-aus*.

Strauß, S. (2015) Datafication and the seductive power of uncertainty – A critical exploration of big data enthusiasm. Information, 6(4): 836–847. *www.mdpi.com/2078-2489/6/4/836*.

Strauß, S. (2019) Privacy and Identity in a Networked Society: Refining Privacy Impact Assessment. Abingdon/New York: Routledge.

Strauß, S. (2020) Vom „Global Village" zur „Blackbox Society"? Digitale Identitäten und politische Kommunikation in Zeiten des Überwachungskapitalismus. Momentum Quarterly – Zeitschrift Für Sozialen Fortschritt, *9*, 85-102. doi:10.15203/momentumquarterly.vol9.no2.p85-102.

Strauß, S., Krieger-Lamina, J. (2017) Digitaler Stillstand: Die Verletzlichkeit der digital vernetzten Gesellschaft – Kritische Infrastrukturen und Systemperspektiven. Bericht Nr. ITA 2017-01, Wien: ITA.

SWI (2022) Hacker finds data security weak spot in Swiss railway system. SWI Swissinfoch. *https://www.swissinfo.ch/eng/sci-tech/hacker-finds-data-security-weak-spot-in-swiss-railway-system/47287534*.

Tangalakis-Lippert, K. (2022) Russische Truppen stahlen in der Ukraine teure Landmaschinen – doch der Hersteller John Deere legte sie per Fernsteuerung still. 06.05., Business Insider, *https://www.businessinsider.de/wirtschaft/russische-truppen-stahlen-in-der-ukraine-landmaschinen-hersteller-john-deere-legte-sie-per-fernsteuerung-komplett-still-d/*.

Tanriverdi, H., Flade, F. (2022) „Russland ist in unseren Netzen", 28.07., Tagesschau online, *https://www.tagesschau.de/investigativ/br-recherche/stromnetz-hacker-russland-101.html*.

TB – Tech Briefs (2017) Developing a Satellite-Based Autonomous Vehicle Control System, *https://www.techbriefs.com/component/content/article/tb/pub/briefs/machinery-and-automation/27047*.

TE – The Economist (2017), The worlds most valuable resource is no longer oil but data. 6. Mai, *https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data*.

Trautman, L J., Ormerord, P. C. (2019) WannaCry, Ransomware, and the emerging threat to corporations. Tennessee Law Review Vol. 86.503, pp. 505-556. *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3238293*.

Turner, B.L., et al. (2003) A framework for vulnerability analysis in sustainability science. Proceedings of the National Academy of Sciences of the United States of America, 100 (14), 8074-8079.

UBA – Umweltbundesamt (2021) Vulnerabilitätsanalyse 2021, *https://www.umweltbundesamt.de/vulnerabilitaetsanalyse-2021*.

Ulrich, K. (2022) China will mit Elektroautos Europa erobern, 14.10., DW online *https://www.dw.com/de/china-will-mit-elektroautos-europa-erobern/a-63440017*.

UN/ISDR (2004) Living with Risk – A global review of disaster reduction initiatives. International strategy for disaster reduction (ISDR) Volume I, United Nations.

Vaas, L.(2013) How to hack an electric car-charging station, 17.05., Sophos security blog, *https://nakedsecurity.sophos.com/2013/05/17/how-to-hack-an-electric-car-charging-station/*.

Voronova, A. (2022) Insteon abruptly shuts down, users left smart-home-elss. 25.04., Hackaday, *https://hackaday.com/2022/04/25/insteon-abruptly-shuts-down-users-left-smart-home-less/*.

Wang, L., Qiu, R. (2020) BeiDou Satellite Positioning Method Based on IoT and Edge Computing, Sensors 20(3):889, DOI:*10.3390/s20030889*.

Weiser, M. (1991) The Computer of the 21st Century. Scientific American, 265(3): 94-104.

Welzer, H. (2016). Die smarte Diktatur. Der Angriff auf unsere Freiheit. Frankfurt/M.: Fischer.

Werle R. (2007) Pfadabhängigkeit. In: Benz A, Lütz S, Schimank U, Simonis G, Handbuch Governance. Theoretische Grundlagen und empirische Anwendungsfelder. Wiesbaden: VS Verlag für Sozialwissenschaften. p. 119–31.

Wilkens, A. (2022) Weiterer Tesla mit aktiviertem „Autopilot“ in tödlichen Unfall verwickelt, 02.08., Heise online, *https://www.heise.de/news/Teslas-Autopilot-erneut-in-toedlichem-Unfall-verwickelt-7199459.html*.

Wired (2014) Data is the new oil of the digital economy. Toonders, J. in Wired, Juli, *https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/*.

Wired (2019) No, data is not the new oil. Wired, 26. Februar, *https://www.wired.com/story/no-data-is-not-the-new-oil/*.

Alle URLs zuletzt aufgerufen am 04.05.2023.

RAT FÜR DIGITALE ÖKOLOGIE

# BISHER ERSCHIENEN

**MAI 2021**
FÜR EINE NACHHALTIGE DIGITALPOLITIK


**OKTOBER 2021**
DIE DIGITALE TRANSFORMATION DER ARBEIT


**JUNI 2022**
DIGITALISIERUNG UND TREIBHAUSGASE


# IMPRESSUM

**Herausgeber**
Rat für Digitale Ökologie (RDÖ)
Ein Projekt von Futurzwei. Stiftung Zukunftsfähigkeit
– gefördert von Allianz Foundation
und Schöpflin Stiftung.

**FUTURZWEI. Stiftung Zukunftsfähigkeit**
Lehrter Straße 57, Haus 6, 10557 Berlin

Herausgegeben im **Juni 2023**

**Autoren**
Stefan Strauß
und Steffen Bettin
vom Institut für Technikfolgen-Abschätzung der
Österreichischen Akademie der Wissenschaften

**Kontakt**
www.rdoe.org
info@rdoe.org

RAT FÜR DIGITALE ÖKOLOGIE

www.rdoe.org

# SUMMARY

Gesellschaftliche Infrastrukturen werden mit wachsendem Tempo digitalisiert und vernetzt, die Maßnahmen schwanken zwischen notwendigem und konstruiertem Bedarf. Das führt noch viel zu oft zu mangelhafter Sicherheit, vor allem aber zu wachsenden ökonomischen und technischen Abhängigkeiten. Viel zu oft wird einfach drauflos digitalisiert, ohne die langfristigen Konsequenzen zu bedenken.

Zwar gibt es bei kritischen Infrastrukturen wie Strom oder Finanzwesen ein hohes Problembewusstsein, doch verengt sich die Sorge meist auf Cyberattacken. Dabei wächst mit zunehmender Vernetzung auch ganz allgemein die Anfälligkeit für folgenschwere Fehler und Störungen.

Oft ist gar nicht unbedingt die Technik das Problem, sondern das Geschäftsmodell der Technologiekonzerne. So entsteht zum Beispiel durch die Möglichkeit von Fernzugriffen ein neues Machtmittel auf Seiten der Anbieter.

Die digitale Transformation braucht eine nachhaltige und sozialverträgliche Technikgestaltung – und gerade bei Infrastrukturen auch demokratische Legitimation. Wird das zu wenig beachtet, werden nicht nur die Infrastrukturen verletzlicher, sondern auch der Staat, der für sie Sorge trägt.