SCHRIFTENREIHE
ENERGIESYSTEME DER ZUKUNFT

Analyse

Februar 2021

Resilienz digitalisierter Energiesysteme

Blackout-Risiken verstehen, Stromversorgung sicher gestalten

Christoph Mayer | Gert Brunekreeft (Hrsg.)

Energiesysteme der Zukunft ist ein Projekt von:
Nationale Akademie der Wissenschaften Leopoldina | www.leopoldina.org
acatech – Deutsche Akademie der Technikwissenschaften | www.acatech.de
Union der deutschen Akademien der Wissenschaften | www.akademienunion.de

Impressum

Herausgeber

Dr. Christoph Mayer
OFFIS e.V. - Institute for Information Technology
Escherweg 2
26121 Oldenburg

Prof. Dr. Gert Brunekreeft
Jacobs University Bremen gGmbH
South Hall
Campus Ring 1
28759 Bremen

Autoren

Dr. Marita Blank-Babazadeh
OFFIS, Oldenburg

Dr. Marius Buchmann
Jacobs University Bremen

Prof. Dr. Jochen Kreusel
Hitachi ABB Power Grids

Prof. Dr. Jannika Mattes
Universität Oldenburg

Dr. Christoph Mayer
OFFIS, Oldenburg

Mathias Dalheimer
Fraunhofer ITWM

Prof. Dr. Wolfgang Kröger
ETH Zürich

Prof. Dr. Ellen Matthies
Universität Magdeburg

Prof. Dr. Gert Brunekreeft
Jacobs University Bremen

Dr. Volker Distelrath
Siemens AG

Prof. Dr. Sebastian Lehnhoff
OFFIS, Oldenburg

Dr. Philipp Werdelmann
Westnetz GmbH

Sanja Stark
OFFIS, Oldenburg

Prof. Dr. Bernd Hirschl
IÖW/BTU Cottbus

Dr. Till Luhmann
BTC AG

Prof. Dr.-Ing. Christof Wittwer
Fraunhofer ISE

Reihenherausgeber

acatech – Deutsche Akademie der Technikwissenschaften e. V. (Federführung)
Koordinierungsstelle München, Karolinenplatz 4, 80333 München | www.acatech.de

Deutsche Akademie der Naturforscher Leopoldina e. V.
– Nationale Akademie der Wissenschaften –
Jägerberg 1, 06108 Halle (Saale) | www.leopoldina.org

Union der deutschen Akademien der Wissenschaften e. V.
Geschwister-Scholl-Straße 2, 55131 Mainz | www.akademienunion.de

Empfohlene Zitierweise

Mayer, C./Brunekreeft, G.: Resilienz digitalisierter Energiesysteme. Blackout-Risiken verstehen, Stromversorgung sicher gestalten (Schriftenreihe Energiesysteme der Zukunft), München 2020.

Wissenschaftliche Koordination

Dr. Berit Erlach
acatech

Dr. Marita Blank-Babazadeh
OFFIS

Sanja Stark
OFFIS

Katharina Bähr
acatech

Dr. Achim Eberspächer
acatech

Produktionskoordination und Satz

Annika Seiler, acatech

Grafische Gestaltung

aweberdesign.de . Büro für Gestaltung, Berlin

Druck

Kern, Bexbach (Gedruckt auf säurefreiem Papier, Printed in EC)

ISBN: 978-3-9820053-3-1

Bibliografische Information der Deutschen Nationalbibliothek

Die deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie, detaillierte bibliografische Daten sind im Internet unter http://dnb.d-nb.de abrufbar.

Das Akademienprojekt

Das Akademienprojekt „Energiesysteme der Zukunft“ erarbeitet Stellungnahmen und Analysen zur Gestaltung der Energiewende. Stellungnahmen enthalten Handlungsoptionen für die Transformation des Energiesystems und werden nach externer Begutachtung vom Kuratorium des Akademienprojekts verabschiedet. Analysen sind Ergebnisberichte von Arbeitsgruppen. Die inhaltliche Verantwortung für Analysen liegt bei den Autoren. Sofern eine Analyse Bewertungen enthält, geben diese die persönliche Meinung der Autoren wieder.

Leopoldina
Nationale Akademie der Wissenschaften

acatech
DEUTSCHE AKADEMIE DER TECHNIKWISSENSCHAFTEN

UNION
DER DEUTSCHEN AKADEMIEN DER WISSENSCHAFTEN

Resilienz digitalisierter Energiesysteme

Blackout-Risiken verstehen, Stromversorgung sicher gestalten

Christoph Mayer | Gert Brunekreeft (Hrsg.)

Schriftenreihe Energiesysteme der Zukunft

Vorwort

Das Energiesystem befindet sich im Wandel: Großkraftwerke werden abgeschaltet, kleine Erzeugungsanlagen werden wichtiger und Strom aus Wind- und Solarenergie wird zukünftig zum wichtigsten Energieträger. Zudem wird Strom zunehmend genutzt, um Elektrofahrzeuge anzutreiben und Gebäude zu heizen. Um diesen Wandel zu meistern, braucht es die Digitalisierung, sie ermöglicht es, das Zusammenspiel der verschiedenen Elemente zu beherrschen. Zugleich entwickeln sich hieraus neue Fehlerquellen und Angriffsmöglichkeiten.

Anhand einer Analyse verschiedener Szenarien für 2040 hat die Arbeitsgruppe potenzielle Risiken für Blackouts, also langanhaltende und großflächige Stromausfälle, identifiziert. Solche Blackouts könnten schnell zu einer Belastungsprobe für Gesellschaft und Wirtschaft werden, denn alle anderen kritischen Infrastrukturen (KRITIS) hängen von einer stabilen Stromversorgung ab. Ist sie gestört, folgen bald darauf Probleme in den Bereichen Wasserversorgung- und entsorgung, Transport, Gesundheitswesen oder Informations- und Kommunikationstechnologien (IKT).

Um auf unvorhergesehene und unvorhersehbare Ereignisse adäquat reagieren zu können, sie zu beherrschen und im Falle eines Störfalls die Beeinträchtigungen für die Stromverbraucher möglichst gering zu halten, bedarf es einer neuen Strategie. Das Konzept der Resilienz bietet sich hierfür besonders an, denn ein resilientes System kann die Auswirkungen eines Störereignisses abfangen, ohne dass das System kollabiert, und anschließend zügig wieder in den normalen Betriebszustand zurückzukehren. Eine solche Resilienzstrategie ermöglicht es, Schwachstellen und Risiken möglichst weitgehend zu identifizieren, auch gegen unerwartete Bedrohungen gewappnet zu sein und sich fortlaufend weiterzuentwickeln.

Diese Analyse stellt 15 Handlungsoptionen vor, deren Bandbreite von der systemischen Entwicklung von Cyber-Sicherheit über ökonomische Anreize und Monitoringmaßnahmen bis hin zu Bildungskampagnen reicht. Ein Fokus liegt dabei darauf, auch solche Akteure einzubeziehen, die in einem dezentraleren und stärker vernetzten Energiesystem zunehmend Einfluss auf die Stabilität der Stromversorgung gewinnen – etwa Prosumer, Gerätehersteller oder Betreiber von Plattformen für Energiedienstleistungen.

Es zeigt sich deutlich, dass zeitnah Maßnahmen ergriffen werden müssen, um den digitalen Wandel in der Stromversorgung bewusst zu gestalten und das Risiko von Blackouts dauerhaft zu minimieren. Die hier vorgestellten Handlungsoptionen können als Bausteine dienen, die gewohnt hohe Versorgungssicherheit auch in Zukunft zu gewährleisten.

Dr. Christoph Mayer
Leiter der Arbeitsgruppe
„Resilienz digitalisierter Energiesysteme“

Prof. Dr. Gert Brunekreeft
Leiter der Arbeitsgruppe
„Resilienz digitalisierter Energiesysteme“

Inhalt

Abkürzungen

ARegV	Verordnung über die Anreizregulierung der Energieversorgungsnetze
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSI-KritisV	Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz
BSI-Gesetz	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
BNetzA	Bundesnetzagentur
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CDMA 450	Funkstandard Code Division Multiple Access im Frequenzbereich 450 Megahertz
EE	Erneuerbare Energien
EEG	Erneuerbare-Energien-Gesetz
ENTSO-E	Verband Europäischer Übertragungsnetzbetreiber für elektrische Energie
EnWG	Energiewirtschaftsgesetz
ETSI	European Telecommunications Standards Institute
IKT	Informations- und Kommunikationstechnologie
IoT	Internet der Dinge (englisch Internet of Things)
KRITIS	Kritische Infrastruktur
KWK	Kraft-Wärme-Kopplung
KWKG	Kraft-Wärme-Kopplungsgesetz
OT	Operative Technologien
PLC	Power Line Communication
PV	Photovoltaik
SCADA	Supervisory Control and Data Acquisition – englisch für überwachende Kontrolle und Datenerfassung
StromNEV	Verordnung über die Entgelte für den Zugang zu Elektrizitätsversorgungsnetzen
TK	Telekommunikation
ÜNB	Übertragungsnetzbetreiber (in diesem Text auf die ÜNB für elektrische Energie beschränkt)
VDE/FNN	Verband der Elektrotechnik Elektronik Informationstechnik/Forum Netztechnik/ Netzbetrieb
VK	Virtuelles Kraftwerk
VNB	Verteilnetzbetreiber

Glossar

Aggregator	Ein Aggregator handelt und liefert Energie, ohne selbst Stromlieferant zu sein. Er bündelt Erzeugungsanlagen, flexible Verbraucher und Speichersysteme, um sie zu vermarkten. Damit skaliert er kleine Anlagen auf ein handelbares Volumen.
Aktor	Ein Aktor ist ein Stellglied, das physikalische Größen von technischen Systemen automatisch verändern beziehungsweise einstellen kann.
Aktorik	Aktorik ist die Gesamtheit von Aktoren.
Betriebsmittel	Oberbegriff für elektrische Bauteile, der unter anderem Stromleitungen, Transformatoren und Schaltanlagen umfasst.
Blackout	Ein Blackout ist ein großer Stromausfall in einer Region, der mindestens 500.000 Kunden umfasst und mindestens einige Stunden andauert.
Cyber-Sicherheit	Cyber-Sicherheit befasst sich mit allen Aspekten der Sicherheit in der Informations- und Kommunikationstechnik. Das Aktionsfeld der Informationssicherheit wird dabei auf den gesamten Cyber-Raum ausgeweitet. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein. Häufig wird bei der Betrachtung von Cyber-Sicherheit auch ein spezieller Fokus auf Angriffe aus dem Cyber-Raum gelegt.[1]
Digitalisierung	Der Begriff Digitalisierung bezieht sich in dieser Stellungnahme in erster Linie auf die Digitalisierung des elektrischen Energiesystems und beschreibt das anhaltende Fortschreiten der auf IKT beruhenden Vernetzung von Anwendungen, Prozessen, Akteuren und technischen Geräten oder Objekten der physikalischen Welt. Darüber hinaus beinhaltet Digitalisierung das Erfassen, Verarbeiten, Austauschen und Analysieren von Informationen und Daten in allen Wertschöpfungsstufen und über verschiedene Wertschöpfungsstufen der Stromversorgung hinweg und unterstützt dabei, Wissen zu generieren, Entscheidungen zu treffen und darauf aufbauend Handlungen wie Steuereingriffe abzuleiten. Die daraus resultierenden neu entstehenden Abläufe finden insbesondere automatisiert und unterstützt durch Mechanismen der künstlichen Intelligenz statt.
Emergenz	Der Begriff Emergenz bezeichnet das Phänomen, dass durch das Zusammenspiel einzelner Systemteile vollkommen neues, nicht vorhersehbares Verhalten entsteht.
Informations- und Kommunikationstechnik (IKT)	Informations- und Kommunikationstechniken (auch gebräuchlich: Informations- und Kommunikationstechnologien) umfassen alle Techniken, Anwendungen und Prozesse, die für die elektronische Erfassung und Verarbeitung von Informationen und deren (insbesondere digitale) Kommunikation eingesetzt werden. Dazu zählen Hardware wie Server, Kommunikationsnetze, aber auch Software.
Informationssicherheit	Informationssicherheit hat den Schutz von Informationen zum Ziel. Dabei können Informationen auf Papier, in Rechnern oder auch in Köpfen gespeichert sein. Die Schutzziele oder auch Grundwerte der Informationssicherheit sind Vertraulichkeit, Integrität und Verfügbarkeit. Viele Anwender beziehen in ihre Betrachtungen weitere Grundwerte mit ein.[2] Bedrohungen ergeben sich etwa aus höherer Gewalt, menschlichen oder technischen Fehlern oder vorsätzlichen Handlungen.

1 BSI 2020-1.

2 BSI 2020-2.

Informationstechnologie (IT)	In dieser Analyse sind damit IKT-Systeme gemeint, die keine direkte Anbindung an technische Geräte haben, etwa für Buchhaltung.
Internet der Dinge	Internet der Dinge (englisch Internet of Things; IoT) bedeutet, dass physikalische Objekte oder digitale, virtuelle Objekte mit IKT sowie Sensorik und Aktorik ausgestattet und darüber hinaus mit dem Internet verbunden sind.
IT/OT-Konvergenz	Integration von IT und OT und die gemeinsame Nutzung von Daten.
Kaskade	Eine Abfolge von Ereignissen oder Prozessen, die jeweils aufeinander aufbauen.
Kritische Infrastruktur (KRITIS)	Ein System, von dessen Funktionieren die Gesellschaft in kritischem Maße abhängt.
Last	Summe der Leistung, die einem Netz zu einem bestimmten Zeitpunkt entnommen wird.
Leitsystem	Leitsysteme haben die zwei wesentlichen Aufgaben Überwachung von Prozessen oder Komponenten und deren Steuerung mittels sogenannter Fernwirktechnik.
Nachgelagertes Netz	Ein Netz A ist einem Netz B nachgelagert, wenn es mit dem Netz B verbunden ist und Netz B selbst Übertragungsnetz ist oder die Stromübertragung vom Übertragungsnetz ins Netz A nur über Netz B erfolgt. Das heißt, einem Netz nachgelagerte Netze sind Netze niedrigerer Spannungsebene, die an dieses Netz angeschlossen sind.
Netzbetreiber	Netzbetreiber sind für Planung, Bau und Betrieb des Stromnetzes verantwortlich. Sie sind insbesondere dafür zuständig, durch technische Mittel und Eingriffe in ihrem Netzgebiet eine unterbrechungsfreie Stromversorgung sicherzustellen. Es wird je nach Spannungsebene zwischen Übertragungsnetzbetreibern (ÜNB, Netzspannung ab 220 Kilovolt aufwärts) und Verteilnetzbetreibern (VNB, Netzspannung 110 Kilovolt und geringer) unterschieden.
Netznutzer	Natürliche oder juristische Personen, die Energie in ein Stromnetz einspeisen oder daraus beziehen. Dazu zählen zum Beispiel Betreiber von Erzeugungsanlagen oder Betreiber nachgelagerter Netze.
Netznutzungsentgelte/ Netzentgelte	Entgelte für den Zugang zu den Übertragungs- und Verteilnetzen.
Operative Technologie (OT)	IKT-Systeme, die für Überwachung, Betrieb und Steuerung von physischen Komponenten und Geräten oder technischen Prozessen verwendet werden.
Patch	Ein Patch ist die Verbesserung bestehender Versionen einer Software, etwa um neue Funktionen zu installieren oder Softwarefehler und Sicherheitslücken zu beheben.
Patchability	Patchability beschreibt hier die Eigenschaft einer technischen Anlage, dass installierte Software im laufenden Betrieb und ohne viel Aufwand von fern verändert werden kann, entweder automatisch durch die Hersteller oder durch den Betreiber selbst, soweit dieser qualifiziert ist.
Pfadabhängigkeit	Bezeichnet den Effekt, dass durch einmal getroffene Entscheidungen Hürden aufgebaut werden, die den Umstieg auf eine andere Option erschweren oder verhindern. Diese Hürden können entstehen, wenn Investitionen bei einer Systemveränderung verloren zu gehen drohen (versunkene Kosten). Auch Kostenvorteile durch Massenproduktion (Skaleneffekte) oder eine hohe Nutzerzahl (Netzwerkeffekte) verleihen dem etablierten System einen Vorteil gegenüber seinen Alternativen.
Photovoltaik	Umwandlung von solarer Energie in elektrische Energie.
Primärregelleistung	Gehört zur Regelleistung. Primärregelleistung wird automatisch innerhalb von dreißig Sekunden im gesamten Verbundnetz aktiviert, um das Netz zu stabilisieren und Frequenzabweichungen entgegenzuwirken.
Prosumer	Zusammengesetzt aus den englischen Begriffen Producer und Consumer – Produzent und Konsument. Dies bedeutet, dass Privatakteure nicht mehr nur Strom konsumieren, sondern auch erzeugen können (über zum Beispiel Dach-PV-Anlagen).
Resilienz (Energiesystem)	Resilienz bedeutet, dass die Funktion eines Energiesystems – hier die Versorgungssicherheit – unter Belastungen erhalten bleibt, möglicherweise mit Einschränkungen, oder zumindest innerhalb kurzer Zeit wiederhergestellt werden kann.

Risiko	Das Bewerten des Auftretens spezifizierter, negativer Folgen, die sich etwa aus fehlerhaftem Betrieb oder unerwünschten Ereignissen ergeben können unter Betrachtung der damit verbundenen Unsicherheiten, wie etwa der Wahrscheinlichkeit der Ereignisse.
Sektorenkopplung	Die Sektorenkopplung verbindet die Energiesektoren Strom-, Wärme- und Gasversorgung sowie Mobilität zu einem integrierten Energiesystem, um Haushalt, Gewerbe und Industrie mit den benötigten Energiedienstleistungen zu versorgen. Beispiele sind Kraft-Wärme-Kopplung, Power-to-Gas, Wärmepumpen und Heizstäbe (Power-to-Heat).
Sekundärregelleistung	Gehört zur Regelleistung. Sekundärregelleistung löst die Primärregelleistung ab und muss innerhalb von fünf Minuten in voller Höhe zur Verfügung stehen.
Sensor	Technisches Bauteil, das physikalische oder chemische Eigenschaften aus der Umgebung quantitativ erfassen kann.
Sensorik	Sensorik ist die Gesamtheit von Sensoren.
Smart Connection Agreements	Smart Connection Agreements sind flexible Netzanschlussbedingungen für Erzeuger, die dem Netzbetreiber die Möglichkeit der Abregelung (mit oder ohne Entschädigung für den Erzeuger) einräumen.
Smart Home	Begriff für alle Aspekte und Services, die Geräte innerhalb eines Haushalts vernetzen und Prozesse automatisieren.
Soziotechnisches System	Ein soziotechnisches System ist charakterisiert durch das Zusammenspiel von sozialen und technologischen Faktoren. Dass dieses Zusammenspiel wichtig ist, kann durch die Koevolution von Technologie und Gesellschaft erklärt werden: Sie beeinflussen und formen sich gegenseitig.
Spannungsebenen	Für die Übertragung und die Verteilung von elektrischer Energie gibt es verschiedene Spannungsebenen: • Höchstspannung (220 bis 380 Kilovolt) • Hochspannung (60 bis 110 Kilovolt) • Mittelspannung (3 bis 30 Kilovolt) • Niederspannung (230 bis 400 Volt) Je nach Leistung der Entnahme oder Einspeisung werden Erzeugungs- beziehungsweise Verbrauchsanlagen an verschiedene Spannungsebenen angeschlossen.
Systemdienstleistungen (SDL)	Systemdienstleistungen sind für den sicheren und zuverlässigen Systembetrieb notwendig. Zu den SDL gehören: • Betriebsführung • Frequenzhaltung • Blindleistungsregelung • Netzwiederaufbau
Übertragungsnetz	Übertragungsnetze dienen der Energieübertragung über große Strecken (viele Hundert bis mehrere Tausend Kilometer) und dem großflächigen Ausgleich von Verbrauch und Erzeugung. Darüber hinaus ermöglichen sie den Anschluss sehr großer Kraftwerke oder Verbraucherbetriebe. Übertragungsnetze werden zwischen 220 und 380 Kilovolt betrieben (Höchstspannung).
Übertragungsnetzbetreiber	Netzbetreiber, der für ein Übertragungsnetz verantwortlich ist (siehe Netzbetreiber und Übertragungsnetz).
Verteilnetz	Verteilnetze sind die Netze, die für die Verteilung von elektrischer Energie bis zum Endkunden hin genutzt werden. Verteilnetze werden zwischen 230 Volt und 110 Kilovolt betrieben (Hochspannung bis Niederspannung).
Verteilnetzbetreiber	Netzbetreiber, der für Verteilnetze verantwortlich ist (siehe Netzbetreiber und Verteilnetz).
Virtuelles Kraftwerk	Ein virtuelles Kraftwerk ist ein Zusammenschluss von verschiedenen Erzeugungs-, Verbrauchs- und Speicheranlagen, die gemeinsam vermarktet werden.

Zusammenfassung

Eine hohe Funktionstüchtigkeit kritischer Infrastrukturen (KRITIS) – wie Wasserversorgung und -entsorgung, Energieversorgung, Transport, Gesundheitswesen oder Informations- und Kommunikationssysteme (IKT) – ist für eine moderne Industriegesellschaft unverzichtbar. Die Stromversorgung als Teil der Energieversorgung nimmt unter den KRITIS dabei eine Sonderrolle ein: Alle anderen KRITIS sind nach kürzester Zeit gelähmt oder zumindest empfindlich gestört, wenn die Stromversorgung unterbrochen ist. Lang anhaltende und flächendeckende Stromausfälle – sogenannte **Blackouts** – haben daher gravierende ökonomische und auch politisch-gesellschaftliche Auswirkungen. Je nach Dauer und Reichweite kann ein Blackout enorme volkswirtschaftliche Schäden verursachen, die öffentliche Sicherheit gefährden und die Versorgung der Bevölkerung mit jeglichen Gütern des Grundbedarfs wie Trinkwasser, Heizwärme oder Kälte, medizinischen Leistungen, Nahrungsmitteln- und Geldtransfer – um nur einige Beispiele zu nennen – empfindlich einschränken.

Sowohl die deutsche als auch die europäische Stromversorgung sind heute sehr zuverlässig. Sollte sich die gewohnte hohe Versorgungssicherheit im Zuge der Energiewende verringern, ist mit massiven gesellschaftlichen Akzeptanzproblemen zu rechnen. Die Energiewende darf daher nur erfolgreich fortgeführt werden können, wenn es der Politik gelingt, durch geeignete Rahmenbedingungen die **Zuverlässigkeit und Sicherheit des elektrischen Energiesystems** dauerhaft zu gewährleisten.

Auch heute schon ist das Stromnetz als Rückgrat der Energieversorgung regelmäßig **Störungen** ausgesetzt – beispielsweise durch Ausfall oder Überlastung von Übertragungsleitungen, große Prognoseabweichungen der zunehmenden Einspeisung von wetter- und tageszeitabhängiger Wind- und Solarenergie, unerwartete Ereignisse auf dem Energiemarkt oder auch menschliches Fehlverhalten. Diese Belastungen können bisher weitgehend beherrscht beziehungsweise sicher abgewehrt werden – unter anderem durch Digitalisierung.

Wachsende Komplexität führt zu neuen Herausforderungen

Durch die Umstellung von fossilen Energieträgern und Kernenergie auf erneuerbare Energien mit Einspeisungen auf unterschiedlichen Ebenen wird sich das elektrische Energiesystem in den nächsten Jahren und Jahrzehnten gravierend verändern. So werden **kleine, verteilte Erzeugungsanlagen dominieren**. Durch die **Sektorenkopplung**, das heißt unter anderem die zunehmende Verwendung von Strom in Elektrofahrzeugen, Wärmepumpen und Industrieprozessen sowie durch die Digitalisierung entstehen neue Verknüpfungen zwischen den Sektoren Stromerzeugung, Wärmeversorgung, Mobilität, Haushalte und Industrie. Auch die Struktur des Stromverbrauchs ändert sich. **Neue Akteure wie Prosumer** (das heißt Verbraucher, die selbst Strom

produzieren und diesen selbst verbrauchen oder ins Netz einspeisen, beispielsweise mit einer Solaranlage auf dem eigenen Dach) oder **branchenfremde Marktanbieter** beeinflussen zunehmend das Geschehen. Zunehmend müssen diese und viele andere neue Akteure bei der Sicherung der Stromversorgung miteinbezogen werden, denn viele der Großkraftwerke, die bisher für die Stabilisierung der Netzfrequenz zuständig sind, werden außer Betrieb gehen. Die Verteilnetze werden insgesamt eine aktivere Rolle bei der Systemsicherung spielen. Zudem werden auch die Interaktionen innerhalb Europas zunehmen. Die **steigende Komplexität** des Systems und die **noch fehlende Erfahrung** beispielsweise mit der Stabilisierung der Versorgung durch kleine, dezentrale Anlagen stellen eine große Herausforderung für das Energiesystem dar.

Parallel dazu findet eine **rasant voranschreitende Digitalisierung** des gesamten öffentlichen und privaten Raums statt. So werden perspektivisch fast alle Geräte – von Beleuchtung über Kühlschränke bis zu Industrieanlagen – informationstechnisch verbunden sein. Über dieses sogenannte **Internet der Dinge** (Internet of Things – IoT) werden viele Milliarden Geräte vernetzt sein, die auch an das europäische Stromnetz angeschlossen sind und in ihrer Summe die Stabilität der Stromversorgung beeinflussen können. Während die Informations- und Kommunikationsinfrastruktur großer Kraftwerke und Netzbetreiber bisher gut gesichert war und ist, kommunizieren diese Geräte weitgehend ungeschützt über das Internet. Auch Vernetzung und Interaktionen zwischen verschiedenen Akteuren der Energieversorgung nehmen zu. Viele wünschenswerte Entwicklungen ebenso wie Risiken im Bereich der Digitalisierung sind wegen der **hohen Innovationsgeschwindigkeit**, der **schnellen Marktdurchdringung** und ihres **disruptiven Charakters** unvorhersehbar.

Ohne die **zunehmende Verknüpfung zwischen Energieversorgung und IKT** wäre das immer komplexere Energiesystem gar nicht mehr beherrschbar. Ein funktionierendes Zusammenspiel der vielen dezentralen Erzeugungsanlagen, Speicher und flexiblen Verbraucher benötigt einen hohen Grad an Automatisierung und Digitalisierung: **Ohne Digitalisierung keine Energiewende.** Die Stromnetze – insbesondere die Verteilnetze – können zukünftig besser überwacht und die Verarbeitung der anfallenden Daten durch digitale Technologien verbessert werden. Es kommt zu einer stärkeren Integration zwischen den IKT-Systemen, die für Überwachung, Betrieb und Steuerung von physischen Komponenten und Geräten oder technischen Prozessen verwendet werden (Operational Technology, OT), und IKT-Systemen für administrative Prozesse (hier: Information Technology, IT). Diese sogenannte **IT/OT-Konvergenz** kann Mehrwerte auf beiden Seiten generieren. Es kommt zu einer steigenden Automatisierung und Autonomie in der Betriebsführung in den Verteilnetzen. Jedoch entsteht durch die zunehmende Abhängigkeit des elektrischen Energiesystems von IKT eine **neue Qualität von Risiken**. Branchenfremde Drittanbieter haben potenziell Zugriff auf Anlagen – und auch infolge der IT/OT-Konvergenz wird der Zugriff auf Anlagen erleichtert. Gefahren entstehen nicht nur durch Missbrauch, fehlerhafte Nutzung oder Fehlverhalten von IKT, sondern können im Zuge der weiteren Entwicklung von künstlicher Intelligenz, neuer Vermarktungsmodelle und Dienstleistungen auch systemimmanent sein.

Neue Risikofaktoren für große Blackouts im digitalisierten Energiesystem

Durch die Veränderungen im Energiesystem wird sich die **Bedrohungsstruktur** für die Energieversorgung in den nächsten Jahrzehnten signifikant ändern. Neue Risikofaktoren, die zu großen Blackouts führen können, treten zu den bestehenden hinzu. Für diese neuen Risikofaktoren wurden **vier wesentliche Ursachen** identifiziert:

1. **Die Vielzahl an kleinen, aktiv steuerbaren Erzeugungs- und Verbrauchsanlagen ist durch die Möglichkeit unerwünschten simultanen Verhaltens systemrelevant.** Denn werden viele Anlagen gleichzeitig an- oder abgeschaltet, kann dies Auswirkungen auf die Systemstabilität haben.

2. **Fehler der IKT, wie Softwarefehler oder Cyber-Angriffe, können zu massiven Bedrohungen führen.** Dies bezieht sich besonders auf die IKT, die unmittelbar für den Betrieb des elektrischen Energiesystems eingesetzt wird. Besonders herausfordernd ist, dass auch fehlerhafte IKT-Systeme im laufenden Betrieb nicht einfach abgeschaltet werden dürfen.

3. **Die technische Systemkomplexität erschwert die Vorhersage von Auswirkungen im operativen Betrieb.** Das Geschehen im Stromnetz selbst wird eine größere Eigendynamik entwickeln und damit noch schwerer vorhersehbar sein. Die gegenseitige Abhängigkeit zwischen elektrischem Energiesystem und IKT-System kann zudem zu komplexen Störfallabläufen führen.

4. **Die Ungewissheit über zukünftige Entwicklungen erschwert ein optimales Systemdesign.** In der Regulierung und für das Systemdesign werden verschiedene Annahmen über zukünftige Entwicklungen getroffen, die in der Regel jedoch nur einen kleinen Ausschnitt möglicher Entwicklungen abdecken. Besondere Herausforderungen stellen hierbei Pfadabhängigkeiten durch implementierte Technologien und aufgebaute Infrastrukturen, aber auch verschiedene Entwicklungsgeschwindigkeiten von energietechnischer Infrastruktur und IKT dar. Besonders problematisch wäre es, wenn sich systemstabilisierende Maßnahmen auf bekannte Störereignisse beschränken würden. Auch nicht definierte Verantwortlichkeiten zwischen relevanten Akteuren oder die schwer absehbare Entwicklung gesellschaftlicher Einstellungen und Rahmenbedingungen bergen Risiken.

Es wird notwendig sein, jeden Schritt bei der Umsetzung der Energiewende durch geeignete Strategien und Maßnahmen zu flankieren, um das Risiko schwerwiegender Unterbrechungen in der Stromversorgung dauerhaft zu minimieren.

Unvorhergesehene und unvorhersehbare Risiken erfordern eine Resilienzstrategie

Die für die Systemsicherheit verantwortlichen Netzbetreiber müssen sich also zukünftig auf deutlich mehr Unsicherheit und Überraschungen einstellen. Daher wird es zunehmend wichtig, dass sie auch auf unvorhergesehene und unvorhersehbare Ereignisse reagieren, sie beherrschen und auch im Falle eines Blackouts schnell wieder zum Normalbetrieb des Systems zurückkehren können. Für solche Situationen hat sich das **Konzept der Resilienz** bewährt. Resilienz bedeutet, die Auswirkungen eines

Störereignisses abzufangen – im schlimmsten Fall auch mit kurzzeitig abnehmender Versorgungsqualität –, ohne dass das System kollabiert, um anschließend zügig wieder in den normalen Betriebszustand zurückzukehren.

Eine **Resilienzstrategie** erfordert daher ein Portfolio an Maßnahmen – von der möglichst weitgehenden Identifikation von Schwachstellen und Risiken über Maßnahmen zur Unterstützung der Resilienz bis hin zu lernenden und das System verbessernden Maßnahmen.

Handlungsoptionen für ein resilientes, digitalisiertes Energiesystem

Die folgenden Maßnahmen würden dazu beitragen, die Resilienz des zukünftigen, digitalisierten Energiesystems zu sichern und damit die gewohnte hohe Versorgungssicherheit zu erhalten. Sie können als Bausteine einer Resilienzstrategie gegen einen großen Blackout dienen. Im Fokus steht dabei ein langfristiger **Zeithorizont bis 2040**.

1. Wechselwirkung IKT und Energie verstehen und lenken:
Strom- und IKT-System bilden zukünftig ein komplexes cyber-physisches Energiesystem. Die gegenseitigen Abhängigkeiten gilt es sowohl im Systemdesign als auch im Betrieb zu berücksichtigen und soweit möglich resilient zu gestalten. Ein Fokus sollte darauf liegen, die **Abhängigkeiten zwischen energietechnischer Infrastruktur und öffentlichen Kommunikationsnetzen so zu entschärfen**, dass Ausfälle aufgrund dieser Abhängigkeit unwahrscheinlich bis unmöglich werden. Da die Abhängigkeiten bisher nur unzureichend verstanden und modellierbar sind, ist hier noch viel Forschung erforderlich. Aber auch die **Kommunikationssysteme der Stromversorgung** an sich lassen sich resilienter gestalten: Zentral dafür sind redundante Systeme, die nicht durch die gleiche Ursache (Common Cause Failures) zu Fall gebracht werden können. Zudem sollte ein Teil des Kommunikationsnetzes für einen deutlich längeren Überbrückungszeitraum als heute schwarzfallfest aufgebaut sein, das heißt, die eigene, vom Netz unabhängige Stromversorgung (meist durch Batterien) muss länger durchhalten können. Dies ist unter anderem für den Systemwiederaufbau im Falle eines Blackouts erforderlich. Neben elektrotechnischen Kenngrößen sollten zukünftig auch die **Systemzustände der von den Netzbetreibern eingesetzten IKT-Komponenten** stärker überwacht und **in die Betriebsführung integriert** werden. Werden erforderliche Mess- oder Prognosedaten nicht frühzeitig erkannt und richtig weiterverarbeitet – etwa durch Fehler in der Datenübertragung oder weil Hacker Daten verfälscht haben –, kann dies zu falschen Betriebsentscheidungen führen und so die Systemstabilität beeinträchtigen.

2. Cyber-Sicherheit systemisch entwickeln:
Die Stromversorgung muss stärker abgesichert werden gegen Bedrohungen seitens der IKT, die teilweise auch außerhalb des elektrischen Energiesystems entstehen. Da die über das Internet angebundenen Geräte (IoT, Smart Home, Cloud-Dienste) in ihrer Gesamtheit potenziell systemkritisch werden, muss die Cyber-Sicherheit erhöht werden. Dazu sollten **Sicherheitsstandards für alle relevanten Akteure** eingeführt werden – etwa für kleine Netzbetreiber, Aggregatoren, Plattformen und Geräteherstellern. Bei allen Maßnahmen ist darauf zu achten, **Zertifizierung und Regulierung innovationsfreundlich zu gestalten**. Denn die Energiewende benötigt noch viele

Innovationen, gerade im Bereich der Systemdienlichkeit und neuer Geschäftsmodelle. Damit die erforderlichen Innovationen nicht ausgebremst werden, müssen Sicherheit und Innovation gegeneinander abgewogen werden. Der **Umgang mit Sicherheitslücken** sollte angepasst werden. Da es nicht möglich ist, die IKT-Seite vollständig gegen Cyber-Angriffe oder auch Softwarefehler abzusichern, muss etwa die **OT gegen IT-Fehler abgehärtet** werden. Die OT sollte soweit möglich so gestaltet sein, dass sie auch dann funktionstüchtig ist, wenn IT nicht mehr funktioniert. Der früher gebräuchliche Ansatz, die OT-Sicherheit im elektrischen Energiesystem vor allem durch eine räumliche Trennung der einzelnen Komponenten zu gewährleisten, ist weder für die neuen, IKT-bedingten Bedrohungsfälle geeignet, noch kann er den komplexen Herausforderungen der Energiewende mit den zugehörigen Datenbedarfen gerecht werden. Denkbar wäre zudem die Einrichtung von **Notfallteams, die bei Cyber-Vorfällen schnell eingreifen können**.

3. Technische Resilienz durch Netzbetreiber und Netznutzer stärken:
Wetterabhängige Stromerzeugung in Kombination mit der zunehmenden Akteursvielfalt und neuen digitalen Geschäftsmodellen wird zu Überraschungen im Betrieb der Netze führen – mit Störfallabläufen, die sich gravierend von bekannten unterscheiden. Gleichzeitig stehen den Netzbetreibern ihre erprobten Methoden, mithilfe von Großkraftwerken das System zu stabilisieren, immer weniger zur Verfügung. Die Betreiber kleiner Erzeugungsanlagen und Verteilnetzbetreiber müssen dann europaweit deutlich stärker als bisher zur Versorgungssicherheit beitragen. Eine zentrale Voraussetzung dafür ist eine **umfassende Digitalisierung der Verteilnetze**. Dabei ist insbesondere wichtig, dass auch kleine Akteure (unter anderem kleine Stadtwerke) die notwendige technische Ausstattung und das Know-how für den proaktiven Systembetrieb aufbauen. Interdisziplinäre **Trainings und Stresstests** sollten etabliert und regelmäßig durchgeführt werden. So können das Verhalten während kritischer Situationen, der Umgang mit unbekannten Ereignissen und das Verhalten zur Behebung eines Blackouts oder der Umgang mit neuen Technologien geübt werden. Neben Netzbetreibern sollten verschiedene andere Akteure wie Betreiber von Telekommunikationsnetzen oder spezialisierte Security-Fachleute in solche Übungen einbezogen werden. **Dezentrale Strukturen können die Resilienz des Systems stärken**, wenn sie so ausgelegt werden, dass sie im Störfall eine eingeschränkte Stromversorgung einzelner Netzabschnitte im Inselbetrieb aufrechterhalten oder sogar kritische Verbraucher wie Krankenhäuser oder Polizei bevorzugt mit Strom versorgen können.

4. IKT-Integration kleiner Anlagen netzdienlich gestalten:
Der Großteil kleiner Erzeugungsanlagen, Speicher und energieverbrauchender Geräte wird zukünftig mit dem Internet verbunden sein. Darin liegt einerseits ein großes Potenzial zur Stabilisierung der Stromversorgung – die Anlagen können zukünftig Systemdienstleistungen wie Frequenz- und Spannungshaltung sowie Kurzschlussleistung bereitstellen oder den Wiederaufbau der Stromversorgung nach einem Blackout unterstützen. Andererseits können die vielen kleinen Anlagen bei zeitgleichem unerwünschtem Verhalten in der Summe das System destabilisieren. Um **problematisches simultanes Verhalten zu verhindern**, können Mindeststandards für Geräte eingeführt werden. Diese könnten unter anderem Vorgaben zur Patchability machen, also der Möglichkeit, durch Softwareupdates Anlagen an neue Anforderungen anzupassen. So können die zur Systemsicherheit notwendigen Funktionen, aber auch die neuesten Erkenntnisse zum Stand der Sicherheit über Patches in die Geräte integriert

werden. Eine eigenständige, lokale Plausibilisierung von Schaltbefehlen durch die Erzeugungsanlagen könnte systemschädliches Verhalten insbesondere im Falle eines Cyber-Angriffs verhindern. Um das **Potenzial kleiner Anlagen zur Systemstabilisierung zu nutzen**, müssen Netzbetreiber den Betrieb dieser Anlagen beeinflussen können. Plattformen und Standards zur Interoperabilität können helfen, die Vielzahl der Anlagen ökonomisch effizient zu integrieren. Perspektivisch könnten kleine Erzeugungsanlagen und steuerbare Verbrauchsanlagen mit KI angelernt werden, um auch auf komplexe und unbekannte Störereignisse oder Angriffe angemessen zu reagieren.

5. Anreize für Netzbetreiber zur Steigerung der Resilienz stärken:
Bisher fehlen Anreize für die Netzbetreiber und Marktparteien, ausreichend zur Resilienz des zukünftigen Energiesystems beizutragen. So treffen die Kosten eines sehr seltenen großen Stromausfalls die Stromverbraucher, nicht die Netzbetreiber. Die Netzbetreiber haben somit wenig direkten ökonomischen Anreiz, die Schäden aus großen Stromausfällen zu minimieren. Als natürliches Monopol ist der Netzbetrieb stark reguliert. Durch die sogenannte Anreizregulierung soll sichergestellt werden, dass die Netzbetreiber kosteneffizient wirtschaften und keine unangemessenen Gewinne erzielen. Die Einführung einer **Resilienzkomponente in die Anreizregulierung für Netzbetreiber** könnte sicherstellen, dass den Netzbetreibern durch resilienzerhöhende Maßnahmen keine wirtschaftlichen Nachteile entstehen. Die Berechnung der Netzentgelte ist in der Stromnetzentgeltverordnung festgelegt, die kaum Spielraum lässt, resilienzförderndes Verhalten der Netznutzer durch niedrigere Netzentgelte zu honorieren. Eine Reform der Netzentgeltverordnung könnte **resilienzverbessernde, räumlich und zeitlich differenzierte Netzentgelte** ermöglichen. Damit entstünden Anreize für die Netznutzer, bei Standort- und Betriebsentscheidungen die Netzdienlichkeit ihrer Anlagen stärker zu berücksichtigen. Darüber hinaus könnten **flexible Netzanschlussbedingungen für Erzeuger** helfen, den Netzbetreibern zusätzliche Flexibilität für das Netzengpassmanagement zu erschließen. Diese sogenannten **Smart Connection Agreements** räumen dem Netzbetreiber die Möglichkeit ein, Anlagen abzuregeln – je höher die potenzielle, vertraglich vereinbarte Abregelung, desto kostengünstiger der Anschluss. Die Smart Connection Agreements, die in einigen europäischen Ländern derzeit erprobt werden, müssten um Resilienzkriterien erweitert werden.

6. Beteiligung von Privatpersonakteuren bei der Gestaltung und Umsetzung von Resilienz sicherstellen:
Privatakteure haben mehr und mehr direkten oder indirekten Einfluss auf das elektrische Energiesystem – beispielsweise als Prosumer, die eigene Solaranlagen und Batteriespeicher betreiben, oder als Nutzerinnen und Nutzer von flexiblen Verbrauchsanlagen wie Wärmepumpen oder Elektroautos. Diese Anlagen können und sollten zukünftig so betrieben werden, dass sie die Versorgungssicherheit stützen und die Resilienz des Energiesystems verbessern. Dafür müssen sie in bestimmten Situationen auf Signale von außen – in der Regel vom Netzbetreiber – reagieren. Damit ein solcher Eingriff in das private Umfeld akzeptiert wird, müssen die Eingriffsoptionen den Privatakteuren nachvollziehbar erklärt und transparent gehandhabt werden. Dabei sind insbesondere auch Fragen des Datenschutzes relevant. Um Privatakteure an der Resilienz des elektrischen Energiesystems zu beteiligen, kommen verschiedene Maßnahmen infrage: verpflichtende Beiträge etwa über technische Anschlussbedingungen privater Erzeugungsanlagen, finanzielle und marktliche Anreize wie variable Stromtarife und freiwillige

Selbstbeschränkungen der Verbraucher im Notfall. Um eine breite Akzeptanz für die Maßnahmen zu erzielen, sollten alle relevanten Akteure an der Entscheidungsfindung für neue Regelungen beteiligt werden. Dafür ist zunächst ein **Stakeholder-Gremium zur Berücksichtigung der Belange von Privatakteuren zu entwickeln**. Zudem ist es wichtig, ein stärkeres **Bewusstsein für die Systemrelevanz des Handelns von Privatakteuren zu schaffen**. Hier gilt es, ein Problembewusstsein und digitale Mündigkeit zu fördern.

7. Langfristige Risiko- und Resilienzbewertung institutionalisieren:
Es ist nicht möglich, zum heutigen Zeitpunkt alle Trends in der Digitalisierung und der Energieversorgung vorherzusehen. In den nächsten Jahren und Jahrzehnten könnte es überraschende Entwicklungen geben, die die Systemstabilität gefährden und für die sich die bis dahin eingeführten Resilienzmaßnahmen als unzureichend erweisen. Daher muss das Resilienzkonzept fortlaufend an die aktuellen Entwicklungen angepasst werden. Zu diesem Zweck könnte eine **institutionalisierte Risiko- beziehungsweise Resilienzbewertung** durch eine behördliche oder behördlich beaufsichtigte unabhängige Institution etabliert werden. Diese könnte ein Frühwarnsystem mit Risikoindikatoren etwa zu Marktrisiken, technischen Disruptionen, politischen Verwerfungen oder Veränderungen der gesellschaftlichen Einstellungen erarbeiten, langfristige Entwicklungen beobachten und Anpassungsstrategien erarbeiten; daraus lassen sich Handlungsoptionen für die Politik ableiten. Darüber hinaus könnte eine **europäische Informations- und Meldestelle für Störereignisse** aufgebaut werden, die insbesondere eine Meldestelle für stromnetzrelevante Cyber-Sicherheitslücken umfasst. Die Meldestelle würde bestehendes Wissen über Risiken, Störereignisse und mögliche Gegenmaßnahmen für den Netzbetrieb mehrsprachig verfügbar machen und stetig aktualisieren. Als Übergangslösung könnte zunächst eine nationale Meldestelle eingerichtet werden, die dann später als gutes Beispiel für eine europäische Variante dienen kann. Damit die Akteure zu resilienzfördernden Maßnahmen verpflichtet werden können, ist es zunächst erforderlich, **Resilienz beurteilbar zu machen**. Dazu sind gemeinsame quantitative und qualitative Kenngrößen und Standards zu entwickeln, um Resilienzmaßnahmen bezüglich ihrer Wirksamkeit bewerten zu können. Aufbauend auf den entwickelten Kenngrößen und der institutionalisierten Risikobewertung sollte ein **übergeordneter Begleitprozess** ins Leben gerufen werden, mit dem Ziel, die Resilienzstrategie und deren Umsetzung in Gänze regelmäßig auf ihre Wirksamkeit hin zu beleuchten. Im Rahmen eines solchen „Meta-Monitoring“ würden politische Entscheidungen und deren Umsetzung periodisch von einer unabhängigen Institution im Hinblick darauf evaluiert, ob sie – nach dem Stand des verfügbaren Wissens – große Blackouts effektiv und effizient verhindern können.

Die meisten hier vorgestellten Maßnahmen nehmen in ihrer Umsetzung viel Zeit in Anspruch. Da die Digitalisierung sowohl der Energieversorgung als auch unserer gesamten Lebenswelt in rasantem Tempo voranschreitet, sollten die Maßnahmen zeitnah angegangen werden. Nur wenn die Resilienzstrategie damit Schritt hält, können wir die Potenziale der Digitalisierung für eine effiziente, sichere und nachhaltige Energieversorgung bestmöglich nutzen und gleichzeitig mögliche Risiken begrenzen.

1 Einleitung

1.1 Herausforderungen für das elektrische Energiesystem

Das elektrische Energiesystem, wie es in dieser Analyse verstanden wird, ist viel mehr als nur das Stromnetz, das Europa und Teile von Afrika und Asien umspannt: Es umfasst Schnittstellen zu anderen Sektoren der Energienutzung wie Wärme oder Verkehr im Zuge der Sektorenkopplung. Es umfasst aber auch verschiedene Märkte, Kommunikations- und Informationssysteme, Standards und Normen, Regulierung und Gesetze sowie eine Vielzahl von Akteuren mit jeweils eigenen Interessen. Das elektrische Energiesystem ist Basis unseres täglichen Lebens und unseres Wohlstands; es gehört daher zu den kritischen Infrastrukturen (KRITIS). Andere KRITIS sind etwa Wasserversorgung und -entsorgung, Transport, Gesundheitswesen sowie Informations- und Kommunikationssysteme (IKT). Die meisten KRITIS sind wechselseitig voneinander abhängig, wobei die Abhängigkeit aller anderen KRITIS von der Stromversorgung besonders stark ausgeprägt ist. Selbst kurze Unterbrechungen der Stromversorgung schränken die Funktion anderer KRITIS stark ein. Jeder Schritt bei der Umsetzung der Energiewende darf daher nur gegangen werden, wenn dadurch die heutige hohe Versorgungssicherheit nicht verringert wird, da sonst neben den ökonomischen Auswirkungen voraussichtlich auch massive gesellschaftliche Akzeptanzprobleme bezüglich der Energiewende auf uns zukämen. Versorgungssicherheit unter den neuen Bedingungen der Energiewende und deren Fortschreiten zu garantieren, trägt damit **zum Klimaschutz** bei; die Politik muss durch geeignete Rahmenbedingungen die Zuverlässigkeit des elektrischen Energiesystems gewährleisten.

Das europäische elektrische Energiesystem hat sich bisher auch im internationalen Vergleich als zuverlässig und robust gegenüber Störungen erwiesen.[3] Weltweit belegt das nationale Stromversorgungssystem den Spitzenplatz.[4] Neben operativen Maßnahmen wie Regelleistung und der Möglichkeit, Abschaltmaßnahmen durchzuführen, trägt besonders die strikte Anwendung des sogenannten N-1-Kriteriums zu dieser Sicherheit bei. Dieses Kriterium bedeutet, dass in den oberen Spannungsebenen ausreichend Redundanzen vorhanden sind, sodass bei Ausfall eines Netzelements oder Großkraftwerk keine Störungen und Kaskaden auftreten.

Warum aber ist nun dringender politischer Handlungsbedarf gegeben?

Die Stromversorgung wird sich in den nächsten Jahrzehnten deutlich von der heutigen unterscheiden. Es ändert sich unter anderem die Erzeugungsstruktur: Die dominierende regenerative Energiebereitstellung hängt von Wetter, Jahres- und Tageszeit ab und stammt zu einem großen Teil aus vergleichsweise kleinen Anlagen. Der Verbrauch steigt durch die Sektorkopplung, und Verbrauchsmuster ändern sich durch neue Abnehmer

3 Ein Ländervergleich in der EU findet sich etwa unter European Commission 2016.

4 Gasser et al. 2020.

und durch die Verbrauchsflexibilisierung in Haushalt und Industrie. Nicht zuletzt verändert die Digitalisierung die Energieversorgung, da zum einen mehr Abhängigkeiten von IKT bestehen und zum anderen digitale Technologien für neue stabilisierenden Mechanismen eingesetzt werden können. Diese Systemtransition führt unter anderem dazu, dass die Mechanismen gegen große Blackouts, die den Netzbetreibern heute zur Verfügung stehen, nicht mehr ausreichen. Bereits heute gilt das elektrische Energiesystem als das System, das in jeder Hinsicht einen „unübertroffenen Grad an Komplexität" aufweist.[5]

Das heutige Systemdesign hat sich über Jahrzehnte entwickelt und wurde nicht darauf ausgelegt, neue Arten von Störungen aufzufangen, die sich aus dem Wandel der Energieversorgung ergeben können. Neben Störungen der IKT-Systeme gehören dazu falsche Einschätzung der Betriebssituation oder auch überraschende Effekte, die derzeit noch nicht auf dem Radar zu erkennen sind.[6,7] Auch die Ungewissheit über das Aussehen des zukünftigen elektrischen Energiesystems erzeugt neue Risikofaktoren, etwa weil Pfadabhängigkeiten[8] entstehen. Die Entwicklung des Energiesystems unterliegt zudem stark politisch-gesellschaftlichen Vorgaben, sodass auch Änderungen von Werteeinstellungen auf regionaler bis globaler Ebene, etwa zum Klimawandel, zum Ausbau von Windkraft oder auch zur Marktgestaltung, die Transformation des Energiesystems beeinflussen. Ungewissheit im Hinblick auf diese Entwicklungen und die hohe Geschwindigkeit des Wandels führen dazu, dass Erfahrungen aus der Vergangenheit keine ausreichende Entscheidungsgrundlage mehr bieten. Dies stellt unter anderem für die staatlichen Akteure eine große Herausforderung dar.

Zwar sind auch andere Bereiche der Energieversorgung als das elektrische Energiesystem von großen Änderungen betroffen. So wurde etwa am 10.06.2020 von der Bundesregierung die „Nationale Wasserstoffstrategie"[9] veröffentlicht, die dazu beitragen soll, Wasserstoff als Energieträger zu etablieren. Besonderer Handlungsbedarf, Resilienz neu zu denken, besteht jedoch heute nur für das elektrische Energiesystem, da dort der Wandel bereits in vollem Gange ist und es empfindlicher gegen Störungen ist. Die Bedeutung des elektrischen Energiesystems wird sich zudem noch vergrößern, da durch die Sektorenkopplung, etwa auch die Wärmeversorgung und der Mobilitätssektor in zunehmendem Maße von elektrischem Strom abhängig werden.

Diese Analyse konzentriert sich auf große Stromausfälle, im Folgenden **Blackouts** genannt, weil diese gravierende gesellschaftliche Auswirkungen haben. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) versteht Stromausfälle als groß, wenn in einem zusammenhängenden Gebiet mindestens 500.000 Kunden betroffen sind[10] und der Stromausfall mehrere Stunden andauert. Dieses Verständnis wird auch der vorliegenden Analyse zugrunde gelegt. Bei einem Blackout dieser Art entsteht ein massiver Schaden für die Gesellschaft – nicht zuletzt dadurch, dass es durch die Größe des betroffenen Gebiets schwerfällt, dieses aus dem umliegenden, nicht betroffenen Gebiet reibungslos zu unterstützen.

5 Schwab 2012, S. 33.
6 Kröger 2017.
7 PSOTF 2004.
8 Zum Thema Pfadabhängigkeiten siehe zum Beispiel Fischedick/Grunwald 2017.
9 BMWi 2020-1.
10 Angelehnt an Büchner et al. 2014, BSI-KritisV 2017, Anhang 1, Teil 2, Nummer 8.

Das **Jahr 2040** wurde als Betrachtungsrahmen gewählt, um einerseits einen eher langen Zeithorizont zu betrachten, andererseits jedoch ein Horizont 2050 aufgrund der raschen und unvorhersehbaren Entwicklung der Digitalisierung zu lang wäre. Betrachtet man die Energiewende über den gesamten Zeitraum bis etwas über die Mitte des Jahrhunderts, findet der für die Systemstabilität kritische Umbau des elektrischen Energiesystems etwa in der Zeit bis 2040 statt (siehe Abbildung 1). In dieser Zeit muss die Gesellschaft die neuen Märkte etablieren, die Digitalisierung gestalten, das Problem der Langzeitspeicherelemente technisch und ökonomisch lösen, die Flexibilitäten bei Haushalten und Industrie weitgehend erschließen – und dies alles in einem europäischen Rahmen und ohne dass die Zuverlässigkeit der Stromversorgung gestört wird. Diese Herausforderung wird nur durch eine achtsame und zügige Umsetzung der Energiewende und der Digitalisierung zu meistern sein.

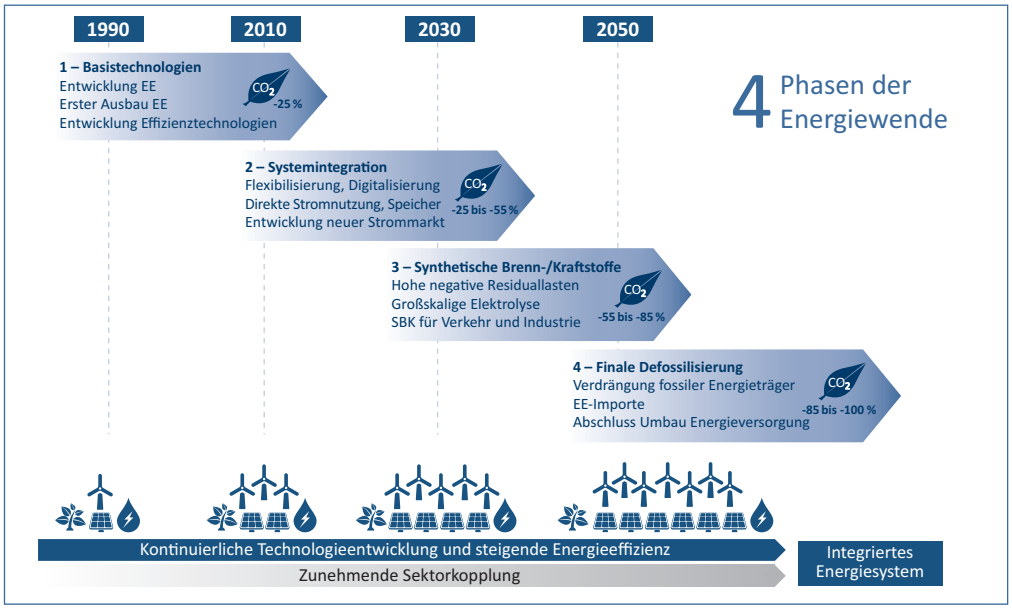


Abbildung 1: Die vier Phasen der Energiewende[11]

1.2 Lang andauernde großflächige Blackouts schaden der Gesellschaft massiv

Eine anschauliche Darstellung für die Folgen großer Blackouts liefert eine Analyse des Büros zur Technikfolgen-Abschätzung beim Deutschen Bundestag aus dem Jahr 2011.[12] Bereits unmittelbar nach dem Stromausfall können ernsthafte Schäden auftreten: Verkehrsunglücke wegen ausgefallener Ampeln, Austreten von Gasen in industriellen Prozessen, Menschen, die in U-Bahnen und Aufzügen festsitzen. Die Festnetztelefonie fällt direkt aus. Eine unmittelbare Auswirkung zeigt sich auch im Gesundheitsbereich: Die unfallbedingten erhöhten Todes- und Verletztenzahlen werden durch eingeschränkte Rettungs- und Transportmöglichkeiten noch gesteigert. Einige Stunden nach dem Stromausfall verschärft sich die Situation: Auch die Mobiltelefonie ist nun stark eingeschränkt. Die Bevölkerung kann nicht ausreichend informiert werden.[13] Dadurch können etwa in Notfällen keine Rettungsdienste wie Krankenwagen, Feuerwehren oder die Polizei gerufen werden. Menschen in Krankenhäusern geraten in kritische

11 acatech/Leopoldina/Akademienunion 2017-1, S. 53. Die Klimaschutzziele haben sich seither verschärft. So wird nun sowohl in Deutschland als auch der EU Klimaneutralität bis 2050 angestrebt.

12 Petermann et al. 2011. Man darf annehmen, dass durch die seitdem fortgeschrittene Digitalisierung die Auswirkungen zumindest nicht weniger gravierend werden.

13 Dies zeigte sich etwa beim Stromausfall 2006 im Münsterland.

Zustände, da sie die Verschlechterung der Behandlungsbedingungen nicht verkraften.[14] Bei einem mehrtägigen Stromausfall sterben Tiere in der Landwirtschaft, etwa durch Unterkühlung oder Überhitzung. Die Lebensmittelversorgung ist gestört, da nur noch Mahlzeiten gekauft werden, die ohne Strom und Wasser zubereitet werden können, sodass aufgrund fehlender Liefermöglichkeiten Engpässe bei diesen Lebensmitteln entstehen. Ein zusätzliches Problem stellt der Mangel an Bargeld dar, der vereinzelt bereits nach wenigen Stunden auftreten wird. Es kommt zu gehäuften Todesfällen in Pflegeheimen – unter anderem, weil Pflegekräfte nicht mehr zur Arbeit kommen können. Letztlich kommt es zu Unruhen und damit zur Gefährdung der öffentlichen Ordnung. Einbrüche, Vandalismus und weitere Verbrechen nehmen dramatisch zu – die Polizei kann kaum noch eingreifen, da sie einerseits die Menge an Vorfällen nicht bearbeiten kann, andererseits durch fehlende Kommunikationsmöglichkeiten oft gar nicht erst von den Vorfällen erfährt. Auch nach Wiederherstellung der Stromversorgung nach einigen Tagen blieben viele Folgen lang oder dauerhaft. Das Vertrauen der Gesellschaft sowohl in die Energieversorger als auch in den Staat und in sich selbst als soziale Gemeinschaft wäre nachhaltig gestört.

Auch die ökonomischen Kosten eines großen Blackouts sind enorm: Für Deutschland wurden die Kosten eines großflächigen, mehrstündigen Stromausfalls auf 8.000 bis 10.000 Euro pro verlorene Megawattstunde geschätzt. Einigen Branchen schadet ein Stromausfall noch in viel höherem Maße, etwa der Finanzbranche.[15] Ein einstündiger Stromausfall allein für Berlin um die Mittagszeit an einem Wochentag im Winter würde nach einer Studie aus dem Jahr 2010[16] einen Schaden von etwa 23 Millionen Euro verursachen, ein entsprechender Stromausfall für ganz Deutschland etwa 600 Millionen Euro. Man nimmt an, dass die ökonomischen Schäden pro Stunde nach kurzer Zeit exponentiell ansteigen, um dann wieder abzusinken.[17] Auch wenn sich die Autorinnen und Autoren solcher Untersuchungen an den Folgen vergangener Stromausfälle orientieren, sind dies nur grobe Schätzungen, da viele Arten von Schäden, etwa in privaten Haushalten oder der Schaden an Produktionsanlagen, nur schwer zu ermitteln sind. Für einige große Stromausfälle in Industrienationen wurden die ökonomischen Kosten abgeschätzt: So berechnete das Electric Power Research Institute (EPRI), dass der große Stromausfall am 14. August 2003, der in den USA und Kanada 50 Millionen Menschen betraf, einen Schaden in Höhe von 6 Milliarden US Dollar[18] verursachte. Der Stromausfall in Italien am 28. September 2003, der wohl durch geeignete reaktive Maßnahmen der verantwortlichen Netzbetreiber hätte verhindert werden können, betraf rund 57 Millionen Menschen und hat vermutlich ähnlich hohe Kosten verursacht. Die jährlichen wirtschaftlichen Schäden, die durch die in den USA häufig auftretenden Stromausfälle verursacht werden, betragen weit über 100 Milliarden US-Dollar.

Es wird vorausgesetzt, dass mit Bezug auf das Risiko großer Blackouts mindestens der heutige Stand der Versorgungssicherheit gehalten werden soll. Im Hinblick auf die beschriebenen Folgen wird deutlich, dass die Aufgabe der Versorgungssicherheit des elektrischen Energiesystems nicht individuell von den einzelnen Akteuren verantwortet werden sollte, sondern eine gesamtgesellschaftliche Aufgabe ist.

---

14 Die essenziellen Systeme in Krankenhäusern sind jedoch über 24 Stunden über eine Notstromeinrichtung versorgt.

15 Schröder/Kuckshinrichs 2015.

16 Piaszeck et al. 2013.

17 Steetskamp/van Wijk 1994, S. 8.

18 Diese und die folgenden quantitativen Aussagen finden sich in Weijen/Bouwmans 2006.

1.3 Was bedeutet Digitalisierung?

Der Begriff Digitalisierung wird in Medien und Politik intensiv diskutiert. Digitalisierung durchdringt annähernd alle gesellschaftlichen Felder, zum Beispiel Arbeitsplatz, Haushalt, Wirtschaft, Freizeitgestaltung, Partnersuche, Freundschaften, politische Prozesse. Das Wort ist in aller Munde – dies beweist zumindest, dass eine Entwicklung existiert, die die Gesellschaft intensiv beschäftigt. Digitalisierung schafft viele Vorteile für den Menschen – durch Erleichterungen im Alltag, durch neue Möglichkeiten der Kommunikation, durch neue Prozesse in der Produktion, weniger Verkehrsunfälle und vieles mehr. Komplexe Systeme wie die Energieversorgung sind ohne Digitalisierung nicht effizient und sicher zu betreiben. Doch weckt Digitalisierung nicht nur positive Assoziationen: Sie wird auch verbunden mit Arbeitsplatzverlusten, Verlust der Kontrolle über persönliche Daten, Verlust des menschlichen Einflusses durch Übertragung von Entscheidungen an „Lernende Maschinen", mit Hackern oder auch der gezielten Manipulation der öffentlichen Meinung. Ein Teil dieser Dualität findet sich auch in der Digitalisierung der Energieversorgung.

Die ursprüngliche Wortbedeutung des Begriffs Digitalisierung bezieht sich darauf, „ein analoges Signal in ein digitales [umzuwandeln]" oder „Daten und Informationen digital [darzustellen]".[19] Im heutigen Sprachgebrauch bedeutet der Begriff jedoch weit mehr. Digitalisierung ist nicht allgemeingültig definierbar. Das Verständnis kann je nach Anwendungskontext variieren. In einigen Bereichen werden auch Synonyme wie „digitale Transformation" oder „digitale Revolution" verwendet.

Eine Definition im Sinne der vorliegenden Analyse benötigt einen systemischen Blick unter Einbezug der verschiedenen Wertschöpfungsstufen und deren Akteure:

Digitalisierung des elektrischen Energiesystems beschreibt das anhaltende Fortschreiten der auf Informations- und Kommunikationstechnologien (IKT) beruhenden Vernetzung von Anwendungen, Prozessen, Akteuren und von mit Sensorik und Aktorik[20] versehenen Geräten oder Objekten der physikalischen Welt. Darüber hinaus beinhaltet Digitalisierung das Erfassen, Verarbeiten, Austauschen und Analysieren von Informationen und Daten in allen Wertschöpfungsstufen und über verschiedene Wertschöpfungsstufen der Stromversorgung hinweg. Sie unterstützt dabei, Wissen zu generieren, Entscheidungen zu treffen und darauf aufbauend Handlungen wie Steuereingriffe abzuleiten. Die daraus resultierenden neu entstehenden Abläufe finden insbesondere automatisiert, unterstützt durch Mechanismen der künstlichen Intelligenz (KI) sowie lernender Systeme, statt.

Die in den verschiedenen Wertschöpfungsstufen erfassten Informationen beinhalten unter anderem das Verhalten technischer Anlagen im Feld, Wetterdaten, Marktdaten oder Daten für kommerzielle Anwendungen wie Kundendaten oder Finanztransaktionsdaten. Diese Informationen können zu verschiedenen Zwecken entlang der Wertschöpfungsstufen erfasst, verarbeitet und analysiert werden. Auf diese Weise werden auch dezentrale, autonome oder automatisierte Entscheidungsprozesse ermöglicht.

19 Duden 2019.

20 Aktorik ist die Gesamtheit von Aktoren. Dabei handelt es sich um Stellglieder, die physikalische Größen von technischen Systemen automatisch verändern beziehungsweise einstellen können.

Alle Geräte, Anlagen, Anwendungen können also prinzipiell Daten austauschen. Zur Verarbeitung und Analyse von Daten sowie zur Entscheidungsfindung können insbesondere Technologien der künstlichen Intelligenz zum Einsatz kommen. Handlungen reichen von der Steuerung von Geräten im Feld bis hin zum Handel am Markt.

Insbesondere KI und lernende Systeme werden alle digitalisierten und digitalisierbaren Vorgänge in den nächsten Jahrzehnten beeinflussen. Um die Wirkungen der Digitalisierung abzuschätzen, reicht es also nicht aus, nur technische und betriebliche Prozesse zu betrachten. Aus der Digitalisierung resultiert eine neue, veränderte gesellschaftliche und ökonomische Dynamik.

Viele Entwicklungen bezüglich der Digitalisierung sind wegen der hohen Innovationsgeschwindigkeit, der schnellen Marktdurchdringung oder des disruptiven Charakters **unvorhersehbar**. Mit digitalen Disruptionen sind hier sich rasch entfaltende Entwicklungen gemeint, die durch digital basierte Innovationen die bisherige Logik einer Wertschöpfung grundlegend verändern – oft, indem bisherige Wertschöpfungsprozesse aufgebrochen und in Wertschöpfungsnetzwerken neu kombiniert werden. Diese Entwicklung hat sich in den vergangenen Jahren noch deutlich beschleunigt, unter anderem dadurch, dass zum Beispiel Cloud-Dienste[21] und Open Source[22] besonders in der Anfangsphase von Innovationen diese massiv beschleunigen, da keine hohen Anfangsinvestitionen notwendig sind, sondern die Investitionen mit dem Wachstum skalieren können. Digitalisierung verändert die Art unseres Zusammenlebens, also auch die Art, wie wir arbeiten und mit anderen Menschen beruflich und privat interagieren. Dies schafft einen Wandel in Einstellungen und Verhaltensweisen, der sich dann wiederum auf die weitere Digitalisierung und deren Regulierung auswirkt.

Die Wertschöpfung durch Digitalisierung benötigt in der Regel nicht nur relativ wenig Energie – was wichtig ist, will man das Wirtschaftswachstum vom Energieverbrauch abkoppeln. Durch Digitalisierung können auch umfangreiche CO_2-Einsparungen erzielt werden, die den CO_2-Ausstoß der IKT um Größenordnungen übersteigen.[23] Dennoch spielen IKT-Systeme beim Energiebedarf eine bedeutende Rolle.[24]

Die Digitalisierung kann die Energiewende unterstützen und beschleunigen. So ermöglicht sie eine viel schnellere Reaktion auf Veränderungen als fest installierte Anlagen und Komponenten der Energiesystemtechnik. Dies verschafft große Vorteile, wenn es darum geht, sich schnell an überraschende Entwicklungen anzupassen. Sie bringt aber auch neue Risiken mit sich: Da der Betrieb des elektrischen Energiesystems zunehmend auf IKT aufbaut, ergibt sich eine neue Qualität von Störungen. So nehmen die Gefahren durch böswilligen Missbrauch von IKT, fehlerhafte Nutzung oder ein Fehlverhalten von IKT zu. Zudem erschweren die gegenseitigen Abhängigkeiten der beiden Systeme im Falle eines Blackouts den Versorgungswiederaufbau. Es gilt also, die Vorteile der Digitalisierung für die Energiewende zu nutzen, gleichzeitig aber die durch sie hinzukommenden Risiken zu beherrschen.

---

21 Als Cloud oder auch Cloud Computing wird eine Vielzahl von angebotenen Dienstleistungen und Technologien auf Basis des Internets und vernetzter Rechenzentren zusammengefasst (siehe Kapitel 3.1.6).

22 Open Source bezeichnet Software, deren Quellcode veröffentlicht und somit Dritten zugänglich gemacht wird.

23 GeSI/Accenture 2015.

24 dena 2015.

1.4 Wie kann Resilienz helfen?

Durch die Veränderungen im Energiesystem und den stärkeren Einfluss der Digitalisierung steigt die Unsicherheit über zukünftige Entwicklungen. Damit sind Wahrscheinlichkeiten für bekannte oder erwartete Ereignisse nicht mehr einfach bestimmbar (wie zum Beispiel Hackerangriffe). Die klassische Risikoanalyse, die auf diesem Prinzip beruht und auf deren Basis das System robust gestaltet wird, ist nicht mehr ausreichend. Zudem können auch Störereignisse auftreten, die es bisher so nicht gab und die nicht vorhersehbar sind. Dementsprechend reichen auch bisherige Maßnahmen zur Systemstabilisierung nicht mehr aus. Für den **Umgang mit unvorhergesehenen und unvorhersehbaren Ereignissen und unerwarteten Entwicklungen hat sich das Konzept der Resilienz bewährt**. Ein resilientes Energiesystem besitzt die Fähigkeit, die Auswirkungen eines Störereignisses mit zum Beispiel eventuell abnehmender Versorgungsqualität abzufangen, ohne dass das System in einem größeren Blackout kollabiert, sondern in der Lage ist, anschließend zügig wieder in den normalen Betriebszustand zurückzukehren (Details siehe Kapitel 5).

Auch unvorhersehbare Ereignisse ohne unmittelbaren Bezug zum Energiesystem können Einfluss auf den sicheren Betrieb des Stromnetzes haben. So könnte etwa eine Pandemie dazu führen, dass Betriebspersonal in der IT oder den Leitwarten ausfällt, sei es durch eigene Erkrankung oder Betroffenheit im direkten Umfeld. Zudem können auch verändertes Verbrauchsverhalten durch schwankende Produktionstätigkeit in der Industrie oder vermehrte Telearbeit zu untypischen Effekten in den Stromnetzen führen.[25] Wie sich im Falle der Covid-19-Pandemie zeigte, kann Digitalisierung einen wertvollen Beitrag leisten, um die Gefährdung der Sicherheit der Stromversorgung beherrschen zu können. So wurden etwa

- die Teams in den Betriebsführungseinheiten verkleinert, sodass komplette Ersatzteams auf Abruf bereitgehalten werden konnten, um im Falle von Erkrankungen sofort einspringen zu können,
- Kasernierungskonzepte erarbeitet, um für den Fall einer erhöhten Infektions- und Gefährdungslage die fest zusammengestellten Teams der Leitzentralen mehrere Wochen lang von Kontakten zur Außenwelt an den Standorten der Leitzentralen arbeitsfähig abzuschotten,
- verschiedene Schichten der Betriebsführung der Übertragunsnetzbetreiber (ÜNB) an verschiedenen Orten (neben der Hauptleitwarte im Reserve Control Center mit redundanten IKT-Systemen) untergebracht,
- IT-Teams, die für kritische Funktionen zuständig waren, komplett räumlich getrennt,
- die Kontakte zwischen Mitarbeiterinnen und Mitarbeitern außerhalb der Leitwarten durch weitgehende Heimarbeit reduziert,
- ein regelmäßiger Austausch zwischen allen relevanten Stakeholdern per Webmeetings organisiert, um mögliche Probleme frühzeitig gemeinsam lösen zu können, und
- von den Betreibern der Telekommunikationsnetze neben vielen anderen Maßnahmen vorgesehen, im Fall von Überlastungen in den Kommunikationsnetzen Priorisierungen der Dienste vorzunehmen.[26]

25 IEEE PES 2020.

26 EPRI 2020 und Paaso et al. 2020, Nordpool 2020, ITU 2020, BNetzA 20201.

Der Rückgang des Stromverbrauchs während der Pandemie ließ aber auch in einigen Regionen ein Szenario entstehen, das in dieser Form erst in vielen Jahren zum Normalfall werden wird:[27] Da der industrielle Energiebedarf aufgrund der eingeschränkten Produktion merklich abnahm, die Einspeisung aus erneuerbarer Erzeugung gleich blieb und daher fossile Kraftwerke heruntergeregelt wurden, stieg der Anteil der erneuerbaren Energien (EE) an der Stromerzeugung deutlich. Die Erfahrung mit diesem Szenario zeigte insbesondere, dass noch viel Digitalisierungsbedarf besteht, um Resilienz und Effizienz auch in der zukünftigen Stromversorgung zu erhalten. Dies gilt ganz besonders für den möglichen Fall einer erneuten Pandemie in der Zukunft.

Das Restrisiko eines mehrtägigen großflächigen Stromausfalls bleibt jedoch auch in einem resilienten System bestehen. Die Politik muss dafür sorgen, dass in diesem Fall umfangreiche Maßnahmen außerhalb des Energiesystems zur Verfügung stehen, etwa im allgemeinen Rahmen der Katastrophenvorsorge.[28] Dies liegt jedoch außerhalb des Untersuchungsrahmens dieser Analyse.

1.5 Aufbau dieser Analyse und methodisches Vorgehen

Diese Analyse möchte die politischen Handlungsbedarfe zum Umgang mit den genannten Herausforderungen erarbeiten und konkrete Möglichkeiten ableiten, wie diesen Herausforderungen begegnet werden kann. Dabei müssen folgende Rahmenbedingungen beachtet werden:

- die Verfasstheit des Energiesystems als soziotechnisches System, also geprägt durch technische, ökonomische, politische, juristische und gesellschaftliche Aspekte mit einer Vielzahl beteiligter Akteure und Institutionen,
- langfristige Entwicklungen, die heute schwer absehbar sind (ganz besonders im Umfeld der Digitalisierung),
- die grundlegende, insbesondere durch die Dekarbonisierung bedingte Transformation des Energiesystems und
- das Nebeneinander der weitgehend unregulierten und hochdynamischen Welt der Digitalisierung und des – soweit die Versorgungssicherheit und natürliche Monopole betroffen sind – hochregulierten elektrischen Energiesystems mit hohen Pfadabhängigkeiten.

Das Vorgehen ist in Abbildung 2 schematisch dargestellt. Angelehnt an die Methodik der Risiko-Governance[29] wurde im ersten Schritt zunächst eine **umfassende Umfeld- und Trendanalyse** durchgeführt: Es wurde eruiert, welche Faktoren das elektrische Energiesystem prägen werden, wie dieses abzugrenzen ist, welchen Veränderungen es unterliegt und welche langfristigen Trends durch die Digitalisierung zu erwarten sind. Dazu wurden mehrere interdisziplinäre (unter anderem Elektrotechnik, Informatik, Ökonomie, Politologie, Psychologie, Recht, Risikoforschung, Soziologie) Workshops mit Expertinnen und Experten aus Wirtschaft, Verwaltung und Wissenschaft durchgeführt und um wissenschaftliche Recherchen ergänzt. Ein besonderes Augenmerk wurde auf die Regulierung und die Hierarchie der regulierenden Institutionen gelegt.

27 Illinois Tech 2020.
28 Vgl. Thoma 2014, S. 120.
29 IRGC 2018.

Die Ergebnisse sind in den Kapiteln 2 und 3 beschrieben. Es zeigt sich, dass sich zukünftige Entwicklungen, die stark von Digitalisierung geprägt werden, durch einen besonders hohen Grad an Ungewissheit auszeichnen.

Im nächsten Schritt wurde eine **Szenario-Analyse** durchgeführt. Für das Jahr 2040 wurden vier Szenarien erzeugt, die sich in Bezug auf die Blackout-Risiken deutlich unterscheiden: „Business as usual“, „Automatisiert und modular“, „Integriertes Europa“ und „Laissez-faire“ (siehe Anhang 8).

Im dritten Schritt wurden von der Arbeitsgruppe für jedes Szenario vier Kategorien identifiziert, in denen Risikofaktoren für einen Blackout eintreten können:

- Ökonomie,
- Technik,
- Werte und Einstellungen und
- Regulierung.

In diesen vier Kategorien wurden über einhundert **Risikofaktoren** identifiziert – mögliche Faktoren, die zukünftig das Risiko für Blackouts erhöhen können. Die jeweiligen Ursachen für diese Risikofaktoren wurden in vier szenarioübergreifende **Basisursachen** zusammengefasst (siehe Kapitel 4).

Auf Basis des Resilienzkonzepts (siehe Kapitel 5) wurden im nächsten Schritt mögliche **Maßnahmen** ermittelt, um den identifizierten Risiken zu begegnen. Um diese Maßnahmen umzusetzen, wurden sie in **politische Handlungsoptionen** übersetzt und im abschließenden Schritt Akteuren zugeordnet und interdisziplinär bewertet (siehe Kapitel 6).

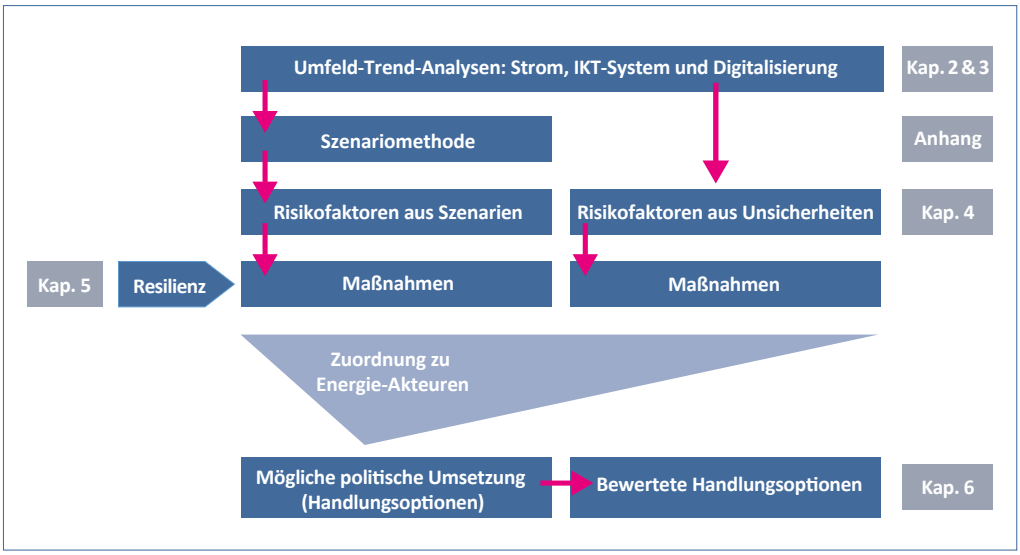


Abbildung 2: Methodisches Vorgehen der Arbeitsgruppe

2 Die elektrische Energieversorgung

Über 530 Millionen Menschen in 34 Ländern nutzen Strom aus dem europäischen elektrischen Energiesystem. Es gilt als eines der komplexesten soziotechnischen Systeme der Welt und verändert sich laufend entsprechend den Anforderungen der Gesellschaft. Es ist eine immens herausfordernde Aufgabe, technische, gesellschaftliche, ökonomische und regulatorische Rahmenbedingungen wieder und wieder auf neue Entwicklungen so anzupassen, dass gesellschaftliche Bedürfnisse befriedigt werden.

Das sogenannte Zieldreieck der Energieversorgung beschreibt die politische Zielvorstellung, dass Umweltverträglichkeit, Wirtschaftlichkeit und Versorgungssicherheit in Einklang gebracht werden sollten – und zunehmend wird die vierte Dimension der gesellschaftlichen Akzeptanz wichtiger. Stand in der Vergangenheit eine immer bessere Versorgungssicherheit im Vordergrund, hat sich der Zielausgleich in den letzten zwei Jahrzehnten verschoben. Der europäische Markt wurde liberalisiert, um damit mehr wirtschaftliche Aspekte und Wettbewerb zuzulassen. Auch etwa bei der Netzregulierung stehen vermehrt Kostenreduktionen im Vordergrund. Das Ziel der Umweltverträglichkeit rückte über die (auch weltweite) Einführung erneuerbarer Energien, den drohenden Klimawandel und den Atomausstieg[30] mehr in den Vordergrund.

Durch die geänderten regulatorischen Rahmenbedingungen hat sich die Landschaft der Energieversorgung in den letzten Jahren stark verändert. Insbesondere stellen das Energiewirtschaftsgesetz (EnWG) und das Erneuerbare-Energien-Gesetz (EEG) wesentliche Treiber für die Integration erneuerbarer Energien in das Energiesystem dar. Durch den diskriminierungsfreien Netzzugang und die Förderung von EE-Anlagen kommt es vermehrt zu dezentraler Stromproduktion durch kleine, verteilte Anlagen. Der Ausbau erneuerbarer Energien, überwiegend in Form kleiner Anlagen, wird sich vervielfachen. Um das politische Ziel „Treibhausneutralität bis 2050“ zu erreichen, muss dieser Anteil auf hundert Prozent steigen. Ein weit schnellerer Ausbau ist daher notwendig. Gleichzeitig ändert sich das Verbrauchsverhalten besonders in den Verteilnetzen in den nächsten Jahrzehnten, etwa durch Wärmepumpen, Elektromobilität und Hausspeicher, die zusammen rechnerisch eine installierte Gesamtentnahmeleistung von mehreren Hundert Gigawatt ausmachen könnten. Strom wird der mit Abstand wichtigste Energieträger werden, da er fossile Energieträger in allen Anwendungsbereichen ersetzen muss.

Eine weitere Veränderung für das elektrische Energiesystem resultiert aus einer weiter zunehmenden Dynamik auf der Marktseite: Der Wettbewerb nimmt von Jahr zu Jahr zu,[31] die an den Börsen gehandelte Strommenge nimmt zu, gleichzeitig werden die handelbaren Mindestenergiemengen kleiner und kurzfristiger handelbar.[32]

30 Jedoch ist der anteilige Rückgang der Atomenergie inzwischen auch wesentlich ökonomisch begründet, ESYS 2019.

31 Über elf Prozent der Stromkundinnen und -kunden wechseln jedes Jahr den Anbieter, Statista 2019.

32 Details dazu in Kapitel 2.1.6

Die Kapazität zum länderübergreifenden Transport elektrischer Energie wird von Jahr zu Jahr ausgebaut.[33] Eine zusätzliche Komplexität entsteht durch die verschiedenen Regulierungssysteme der Nationalstaaten.

Die Netzführung wird sich deutlich verändern. Nicht nur wurde das klassische Prinzip des Stromflusses „von oben nach unten", also von Erzeugern auf höheren Spannungsebenen zu Verbrauchern auf niedrigeren Spannungsebenen, zum Teil umgekehrt – denn insbesondere Solaranlagen speisen vorrangig auf den unteren Spannungsebenen ein: Wird der Solarstrom nicht lokal verbraucht, muss er an die höheren Spannungsebenen weitergereicht werden. Auch werden sich Erzeuger und Verbraucher in Verteilnetzen zunehmend an der Bereitstellung von netzstützenden Maßnahmen beteiligen müssen. Durch die hohe Volatilität der EE-Einspeisung wird außerdem das ursprüngliche Prinzip, dass die Erzeugung dem Verbrauch angepasst wird, vermehrt abgelöst von dem Prinzip, dass der Verbrauch der Erzeugung folgen muss. Zu diesem Zweck wird beispielsweise die Last, das heißt der Verbrauch, von flexiblen Kunden gezielt in Zeiten hoher EE-Einspeisung verschoben werden.

Die Komplexität im elektrischen Energieversorgungssystem steigt durch

- Dominanz kleiner, verteilter Erzeugungsanlagen,
- andere und neue Verbraucheranlagen im Verteilnetz,
- Sektorenkopplung,
- neue Geschäftsmodelle und Marktdynamik,
- mehr Akteure,
- europäische Interdependenzen und
- aktive Verteilnetze.

Die zunehmende Komplexität lässt sich nur durch Digitalisierung und eine stärkere Automatisierung bewältigen. Allerdings kann die Digitalisierung die Komplexität zusätzlich weiter erhöhen und in bestimmten Bereichen die Kontrolle über Teile des Systems sogar erschweren. Dabei spielt vor allem die Tatsache eine Rolle, dass Verbraucher- wie auch Erzeugungsgeräte und -anlagen mit einer Leistung weniger Watt bis in den Megawattbereich direkt oder mittelbar mit dem Internet verbunden sein werden (siehe Kapitel 3).

2.1 Das elektrische Energiesystem im Wandel

2.1.1 Stromnetze

Das Stromnetz wird in Übertragungsnetze und Verteilnetze unterteilt. Die Übertragungsnetze dienen in erster Linie der Energieübertragung über große Strecken (viele Hunderte bis Tausende Kilometer) und somit dem großflächigen Ausgleich von Verbrauch und Erzeugung. Kraftwerke sehr hoher Leistung (zum Beispiel große Braunkohlekraftwerke) und sehr große Verbraucherbetriebe (Leistungen im Bereich mehrerer Gigawatt) sind direkt an das Übertragungsnetz angeschlossen. Die Verteilnetze hatten früher die wesentliche Aufgabe, die elektrische Energie von Großkraftwerken zum Endverbraucher zu bringen („zu verteilen"), müssen aber heute zunehmend die Energie aus

33 Schittekatte et al. 2019, S. 49 ff.

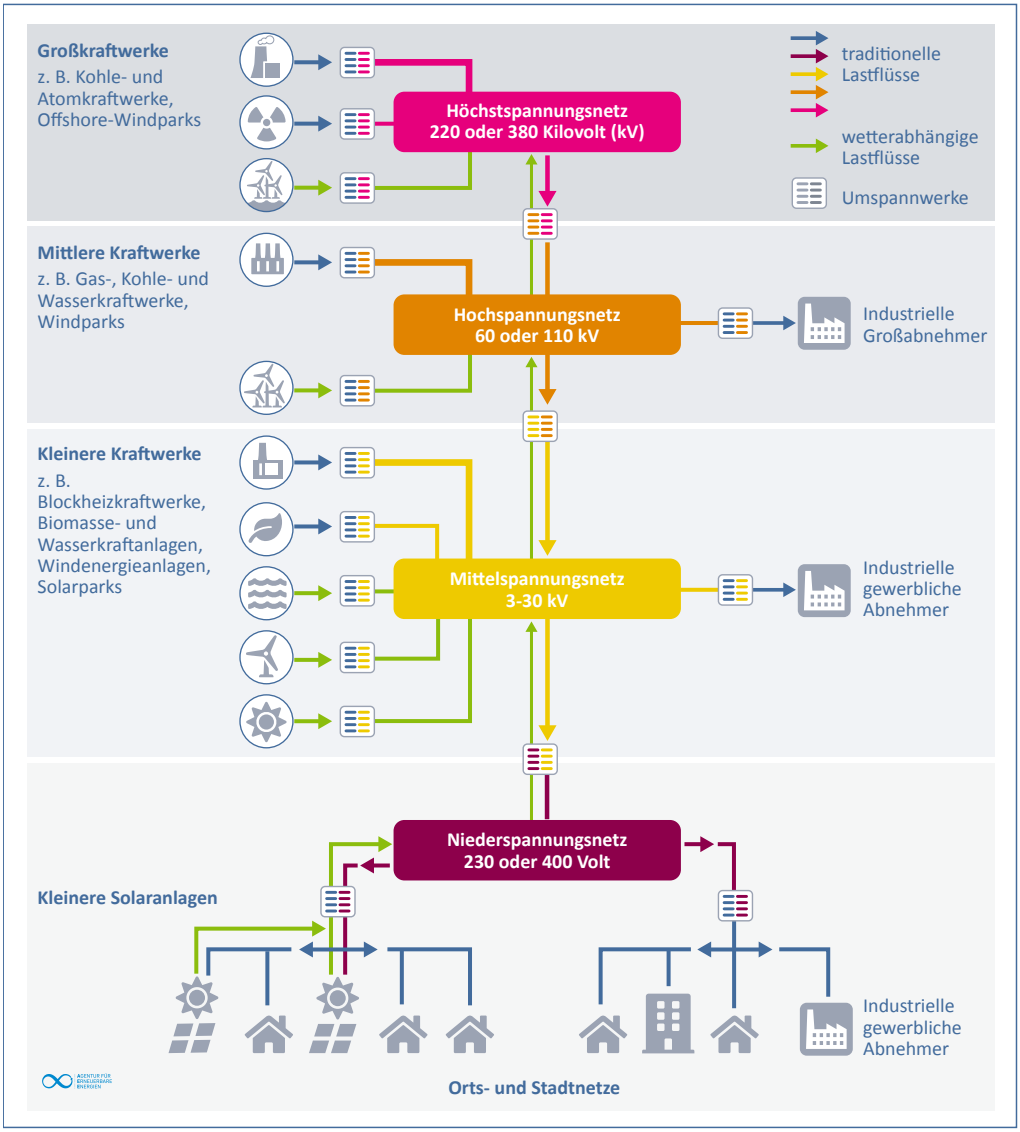


Abbildung 3: Spannungsebenen des Stromnetzes und angeschlossener Anlagen. (Quelle: Angepasst nach https://www.unendlich-viel-energie.de)

Wind- und Photovoltaik (PV)-Anlagen in die höheren Spannungsebenen transportieren. Verteilnetze werden noch einmal in Netze der Hoch-, Mittel- und Niederspannung unterteilt. Je nach Leistung der Entnahme oder Einspeisung werden die Anlagen an verschiedene Spannungsebenen angeschlossen (siehe Abbildung 3). Zwischen den verschiedenen Spannungsebenen befinden sich Umspannwerke oder Transformatorstationen. Dort wird die Spannung auf das Niveau der jeweils vor- beziehungsweise nachgelagerten Spannungsebenen hoch- beziehungsweise heruntertransformiert. Als neues Übertragungsmedium können sogenannte Hochspannungs-Gleichstrom-Übertragungsnetze (HGÜ-Netze) gebaut werden. Mit dieser Technologie ist es möglich, Strom über längere Distanzen mit geringen Verlusten zu transportieren. Allerdings sind die benötigten Umwandlungsprozesse deutlich komplexer als bei dem bestehenden System, weswegen die Kosten deutlich höher sind.

Für Planung, Bau, Wartung und Betrieb des Stromnetzes sind **Netzbetreiber** verantwortlich, die je nach betreffender Spannungsebene Übertragungs- oder Verteilnetzbetreiber (ÜNB beziehungsweise VNB) heißen. In Deutschland gibt es derzeit vier ÜNB und fast 900 VNB, von denen etwa 90 Prozent für weniger als 100.000

Kundenanschlüsse und etwa 73 Prozent für weniger als 30.000 Kundenanschlüsse verantwortlich sind.[34] Besonders kleineren VNB fehlen die notwendigen Ressourcen, um den Anforderungen an die zukünftige Betriebsführung gerecht zu werden. Daher werden bereits heute andere Lösungen gesucht, etwa Verbünde oder Outsourcing.

Das europäische Stromnetz hat physikalische Verbindungen von Nordeuropa bis Nordafrika und von Irland im Westen bis nach Asien im Osten. Dieses Netz besteht aus mehreren Verbundsystemen. Deutschland gehört zu einem Verbundsystem aus über zwanzig Staaten in Kontinentaleuropa (etwa von Spanien bis Skandinavien in Nord-Süd-Richtung, Frankreich bis Polen in West-Ost-Richtung). Darüber hinaus gibt es Verbundsysteme in Skandinavien und Großbritannien. In einem Verbundsystem herrscht überall dieselbe Netzfrequenz. Die Frequenz ist eine physikalische Größe und muss immer mehr oder weniger konstant gehalten werden – im kontinentaleuropäischen Verbundnetz liegt die Frequenz bei fünfzig Hertz. Organisatorisch sind die Verbundsysteme in Regelzonen unterteilt. Jede Regelzone wird von einem ÜNB verantwortet. Dieser hat in seiner Zone unter anderem für die Stabilität des elektrischen Energiesystems zu sorgen. Die Regelzonen sind über sogenannte Kuppelleitungen beziehungsweise Übergabestellen miteinander verbunden, was auch den Austausch von Energie über die Grenzen einzelner Staaten hinweg ermöglicht. Die Verbundsysteme sind zunehmend durch Hochspannungs-Gleichstrom-Übertragungsnetze verbunden.

Die Netzbetreiber tragen die Verantwortung für die Sicherheit des Netzes.[35] Die Sicherheit umfasst die System- und Netzsicherheit. Die Netzsicherheit ist gewährleistet, wenn im Netz die zulässigen technischen Parameter eingehalten werden, im Übertragungsnetz zusätzlich das (n-1-)Kriterium. Systemsicherheit umfasst neben der Netzsicherheit für die ÜNB noch, dass das Gleichgewicht zwischen Erzeugung, Verbrauch und Stromflüssen zu benachbarten Übertragungsnetzen jederzeit im Gleichgewicht ist. Um dies zu erreichen, setzen die Netzbetreiber insbesondere Systemdienstleistungen (SDL) ein. Die SDL sind in vier Teilbereiche gegliedert:[36,37]

- Frequenzhaltung (ÜNB)
  Um die Frequenz stabil zu halten, muss in einem Verbundnetz zu jedem Zeitpunkt genauso viel Strom eingespeist werden, wie in Summe aus dem Verbundnetz entnommen wird. Netzverluste müssen dabei auf der Seite der Einspeisung ausgeglichen werden. Dieses Gleichgewicht kann etwa durch den Ausfall eines großen Kraftwerks gestört werden. Zum Ausgleich von unvorhergesehenen Schwankungen in der Leistungsbilanz wird die sogenannte Regelleistung eingesetzt. Regelleistung lässt sich unterteilen in Primärregelleistung, Sekundärregelleistung und Minutenreserve. Primärregelleistung wird automatisch innerhalb von dreißig Sekunden im gesamten Verbundnetz aktiviert, um das Netz zu stabilisieren und Frequenzabweichungen entgegenzuwirken. Sekundärregelleistung löst die Primärregelleistung ab und muss innerhalb von fünf Minuten in voller Höhe zur Verfügung stehen. Nach 15 Minuten greift die Minutenreserve. Die Frequenz wird heute auch durch rotierende Massen der großen Kraftwerke stabilisiert – ein Effekt, der abnimmt, wenn fossile

34 BNetzA/BKartA 2020, S. 40.
35 EnWG 2020 §§ 13, 14.
36 Hier ohne Vollständigkeit aufgeführt.
37 Vgl. VDE|FNN 2019-1.

Kraftwerke durch regenerative Erzeugungsanlagen (Wind, PV) abgelöst werden, die die Frequenz über Umrichter anpassen.

- Betriebsführung (ÜNB, VNB)
  Dies sind unter anderem die Steuerung (Schalthandlungen) und Überwachung des Stromnetzes und ganz besonders das Engpassmanagement, um die Überlastung von Betriebsmitteln[38] zu vermeiden. Der sich durch die Einspeisung und Entnahme bildende Stromfluss muss die nötigen Leitungskapazitäten vorfinden. Störungen sind zum Beispiel Ausfall von Leitungen oder Transformatoren. Eine Maßnahme zur Behebung ist das Redispatch: Der ÜNB „verschiebt" dazu Stromproduktion, indem auf der einen Seite des Engpasses Anlagen zu geringerer Produktion, auf der anderen Seite zu höherer Produktion in gleicher Leistungshöhe angewiesen werden. Eingriffe zur Vermeidung von Engpässen nehmen durch die fluktuierende Einspeisung durch erneuerbare Energien deutlich zu.

- Spannungshaltung (ÜNB, VNB)
  Für jede Spannungsebene existieren Grenzen für die erlaubte Abweichung von der Nennspannung.[39] Im Gegensatz zur Frequenz ist Spannung eine lokale Größe. So ist die Spannung innerhalb eines Leitungsabschnitts verschieden. Bisher wird die Spannung nur an wenigen Orten im Verteilnetz gemessen, was zukünftig nicht mehr ausreichen wird. Die Netzbetreiber müssen Maßnahmen treffen, um diese Grenzen überall einzuhalten. Ein wichtiges Mittel ist die Bereitstellung von Blindleistung. Die hohe Anzahl an erneuerbaren Energien verlangt hier nach neuen Mechanismen, etwa der Ausschreibung von Blindleistungsbedarf an einem regionalen Markt.

- Versorgungswiederaufbau (ÜNB)
  Nach einem Stromausfall muss die Stromversorgung zügig wiederaufgebaut werden. In einer Regelzone ist dies Aufgabe des ÜNB. Zum Wiederaufbau werden schwarzstartfähige Kraftwerke benötigt, also Kraftwerke, die in der Lage sind, auch autonom, ohne äußere Stromzufuhr, anzufahren (in der Regel Wasserkraftwerke, Gaskraftwerke, aber auch zunehmend Speicher). Diese Kraftwerke können dann den zum Wiederanfahren der übrigen Kraftwerke notwendigen Strom liefern. Der Versorgungswiederaufbau in einem von verteilter Erzeugung mit vielen kleinen Anlagen dominierten System stellt sich offenbar deutlich anders dar als heute.

Viele der SDL müssen in Zukunft angepasst werden, da etwa Hausspeicher, die veränderte Erzeugungsstruktur oder das Laden der Elektrofahrzeuge Einfluss auf die Stromqualität haben werden.

Der Netzbetreiber kann die Betreiber nachgelagerter Netze[40] verpflichten, ihn zu unterstützen, wenn dies zur Behebung einer Gefährdung der Systemsicherheit oder Netzsicherheit beiträgt, und auch direkt jede Einspeisung oder Ausspeisung anpassen beziehungsweise deren Anpassung verlangen. Die europäischen ÜNB sind zudem im Fall von Störungen zur gegenseitigen Unterstützung verpflichtet, soweit nicht die Sicherheit im eigenen Netz dadurch negativ beeinflusst wird.

38 elektrische Bauteile, unter anderem Stromleitungen, Transformatoren und Schaltanlagen.

39 Die Anforderungen an die Stromqualität sind in der europäischen Norm EN 50160 festgelegt.

40 Ein Netz A ist einem Netz B nachgelagert, wenn es mit dem Netz B verbunden ist und Netz B selbst Übertragungsnetz ist oder die Stromübertragung vom Übertragungsnetz ins Netz A nur über Netz B erfolgt. Das heißt, einem Netz nachgelagerte Netze sind Netze niedrigerer Spannungsebene, die an dieses Netz angeschlossen sind.

Der Zubau an erneuerbaren Energien führt so zu einem **erhöhten Bedarf an Netzausbau**, einerseits in den Übertragungsnetzen aufgrund der lastfernen Erzeugung insbesondere durch Windenergieanlagen auf See und in dünn besiedelten Regionen, andererseits in den Verteilnetzen, da Energie aus den Verteilnetzen in die Übertragungsnetze gebracht werden muss. Die Netze werden auch durch sogenannte **Gleichzeitigkeitseffekte**, das heißt gleichzeitige Nutzung der Netzinfrastruktur, durch EE-Einspeisung, gleichzeitige Steuerung durch Marktakteure oder Ladevorgänge, stärker belastet.

In der Öffentlichkeit steht aufgrund von Akzeptanzthemen in der Regel der Ausbau der Übertragungsnetze im Fokus. Ein Teil des Netzausbaus soll daher durch alternative technische Optimierungsmaßnahmen vermieden werden. Das „NOVA-Prinzip“ (Netzoptimierung, -verstärkung und -ausbau), nach dem im Rahmen der Netzplanung Netzoptimierung und -verstärkung Vorrang vor dem Netzausbau haben, führt daher durch verringerten Ausbau zwar zu einer besseren Auslastung der Netze, aber der Betrieb wird auch häufiger näher an die technischen Belastungsgrenzen geführt, und die Anforderungen an die Netzführung werden erhöht. Ökonomisch spielen jedoch die Netze der Mittel- und Niederspannungsebene mit etwa siebzig Prozent der Netzkosten eine viel größere Rolle. In einer Studie wurde ermittelt, dass der Netzausbaubedarf in deutschen Verteilnetzen regional stark unterschiedlich ist. Dieser wird wesentlich durch die Höhe der gesamten installierten Leistung an EE-Anlagen bestimmt. Durch intelligente Maßnahmen wie Erzeugungs- und Lastmanagement oder bestimmte Netztechnologien lässt sich der Netzausbau jedoch reduzieren.[41]

Diese Aufgaben werden bleiben, doch wird die Ausführung dieser Aufgaben komplexer und noch anspruchsvoller als bisher. Auch werden neue Aufgaben hinzukommen. So muss auf den zunehmenden Anteil (insbesondere variabler) dezentraler Erzeugungsanlagen bei der Systemsicherung zurückgegriffen werden, um den Rückgang bei großen Kraftwerken aufzufangen – eine große technische Herausforderung.

2.1.2 Wandel in Stromerzeugung und -verbrauch

Der **Stromverbrauch wird sich in den nächsten Jahren deutlich verändern**. Dies liegt daran, dass vermehrt eine Kopplung verschiedener Sektoren stattfindet. Der Begriff Sektor bezieht sich dabei auf die Art des Energieverbrauchs. Im einfachsten Fall wird unterschieden zwischen den drei Sektoren Strom- und Wärmeverbrauch und Verkehr beziehungsweise Mobilität. Um die Ziele der Energiewende zu erreichen, wird ein **sektorenübergreifender Umbau des gesamten Energiesystems** nötig sein. Diese ganzheitliche Betrachtung des Energiesystems wird oft auch als Sektorenkopplung bezeichnet.[42] Um also mehr Strom aus Erneuerbare-Energien-Anlagen aufnehmen zu können, werden brenn- und kraftstoffbetriebene Anwendungen auf Strom umgestellt. Wesentliche Beispiele hierfür sind Elektrofahrzeuge im Verkehrssektor und Wärmepumpen im Wärmesektor. Zudem kann Strom auch in Wasserstoff umgewandelt werden. Dieser kann dann zwischengespeichert werden, um daraus später wieder Strom zu gewinnen oder Energie für Industrieprozesse bereitzustellen. Eine dritte Möglichkeit ist es, mithilfe von Strom synthetische Brenn- und Kraftstoffe herzustellen, die dann beispielsweise fossile Energieträger ersetzen können. Diese drei Anwendungen werden häufig auch als Power-to-X bezeichnet, da Strom in andere Formen (Wärme,

41 Vgl. Büchner et al. 2014, S. 45, S. 63, S. 122.

42 acatech/Leopoldina/Akademienunion 2017-1.

Gas etc.) umgewandelt wird. Dies führt allerdings unweigerlich zu einem erhöhten Strombedarf und damit einer höheren Belastung des Stromnetzes.

In den vergangenen zehn Jahren hat die Gewinnung von Strom aus erneuerbaren Energieträgern in Deutschland immens an Bedeutung gewonnen. Der Anteil erneuerbarer Energieträger an der Nettostromerzeugung lag 2019 bei über 46 Prozent.[43] Im Jahr 2007 waren es noch 15 Prozent.[44] Davon machte Solarenergie einen Anteil von etwa drei Prozent aus.[45] Um beim Beispiel Solarenergie zu bleiben: Deren installierte Leistung stieg im Zeitraum 2007 bis 2019 von 4.170 Megawatt auf 49 Gigawatt – ein Anstieg um das Elffache. Eine Besonderheit der Solarenergie ist, dass viele kleine Anlagen installiert wurden, und das oft bei Privatpersonen in den niederen Spannungsebenen. So liegt die Anzahl der insgesamt in der Niederspannung installierten Anlagen bei weit mehr als 1,6 Millionen.[46] Das bedeutet, dass die Diversität der Anlagengröße gestiegen ist: Neben der abnehmenden Anzahl an Großanlagen gibt es einerseits eine Vielzahl kleiner Erzeugungsanlagen, die dezentral in untere Spannungsebenen einspeisen. Andererseits sind große Offshore-Windparks entstanden, die mit Leistungen von mehreren Hundert Megawatt in die obere Spannungsebene einspeisen. Die Stromerzeugung erfolgt nicht mehr nur verbrauchsgetrieben, sondern dargebotsabhängig und ist damit zum Teil tages- und jahreszeitlich, witterungsbedingt und geografisch stark fluktuierend. Sie findet meist nicht mehr dort statt, wo der Strom auch abgenommen wird. Zum Beispiel muss Strom von großen Windparks im Norden Deutschlands zu großen industriellen Abnehmern im Süden transportiert werden. Auf lokaler Ebene hingegen können Erzeugung und Verbrauch zusammenfallen, wenn Privatpersonen als sogenannte Prosumer nicht nur Strom verbrauchen, sondern auch selbst produzieren und gegebenenfalls ins Netz einspeisen. So entstehen bidirektionale Lastflüsse, die Einfluss auf die Stabilität des elektrischen Energiesystems haben.

2.1.3 Energiespeicherung

Elektrische Speicher werden bereits heute und in Zukunft vermehrt in die Netze integriert. Dies betrifft sowohl **stationäre Speicher als auch Speicher für Elektromobilität**. Im Fall von Fahrzeugen wird erwartet, dass im Jahr 2030 weltweit bereits mehr Elektrofahrzeuge (batteriebetrieben und mit Hybrid-Antrieben) als mit Verbrennungsmotoren verkauft werden. Für Europa könnte der Anteil von Elektrofahrzeugen insgesamt bei mehr als 25 Prozent liegen.[47] Elektrofahrzeuge werden nicht nur im privaten Bereich zum Einsatz kommen, sondern auch für Lastkraftwagen und allgemein im Logistikbereich. Elektrofahrzeuge eignen sich für die netzdienliche Steuerung im Fall von Netzengpässen,[48] indem Ladevorgänge unterbrochen werden. Außerdem können Elektrofahrzeuge demnächst voraussichtlich auch zur Einspeisung eingesetzt werden. In diesem Fall spricht man von Vehicle to Grid, da das Fahrzeug nicht nur Strom aus dem Netz bezieht, sondern auch zurückspeisen kann. Verbünde aus Elektrofahrzeugen können ebenfalls für Regelleistung eingesetzt werden.

43 Fraunhofer ISE 2020.
44 Fraunhofer ISE 2018.
45 ebd.
46 Eigene Berechnung mit Daten von Netztransparenz 2019.
47 Siehe BCG 2018.
48 Sie eignen sich insbesondere als steuerbare Verbrauchseinrichtungen nach § 14a EnWG 2020.

Im Bereich der stationären Speicher gibt es zahlreiche Anwendungsfälle. So ist beispielsweise die Nachfrage nach Heimspeichern in den letzten Jahren deutlich gestiegen. Nach Branchendarstellung wird bis 2022 mit einer Anzahl von 100.000 Speichern gerechnet. Diese Zunahme wird unter anderem dadurch begründet, dass Batterien häufig mit PV-Anlagen kombiniert werden.[49] Hier werden die dezentralen Batteriespeicher zur Eigenverbrauchsoptimierung eingesetzt. Ein weiterer Anwendungsfall stationärer Speicher ist die sogenannte Multi-Purpose-Nutzung. Dies bedeutet, dass ein Speicher für mehrere Anwendungszwecke eingesetzt werden kann. Neben der Eigenbedarfsoptimierung kann ein Speicher beispielsweise auch für Peak-Shaving – das heißt die Reduzierung von Leistungsspitzen – genutzt werden. Ein dritter Anwendungsfall ist die Direktvermarktung zusammen mit EE zum Beispiel in Form eines virtuellen Kraftwerks (VK, siehe Infobox „Virtuelles Kraftwerk", Abschnitt 3.2.1). Darüber hinaus könnten Batteriespeicher für die Bereitstellung von Regelleistung, netzstützende Maßnahmen wie lokale Spannungshaltung sowie den Aufbau der Versorgung nach einem Stromausfall oder unterbrechungsfreie Stromversorgung eingesetzt werden.[50] Zudem sind Anwendungsfälle für den Inselbetrieb – das heißt eine lokale, in der Regel eingeschränkte, Stromversorgung in einem Verteilnetz – denkbar.[51] Die eingesetzte Technologie und die Auslegung der Batterien hängen von dem entsprechenden Anwendungsfall ab.

Der Markt für stationäre Speicher wird voraussichtlich mittel- bis langfristig weiter wachsen, da der Bedarf durch den Ausbau von EE steigen wird.[52] Die steigende Nachfrage nach Elektromobilität und Speichern für Netzdienstleistungen sorgt für eine Kostenreduktion von Speichern. Auch können Batterien aus Elektrofahrzeugen für eine zweite Nutzung in Form von Haus- oder Großspeichern dienen, was ebenfalls Kosten reduziert. Neben privat und gewerblich genutzten Speichern werden nach Branchendarstellungen vor allem Großspeicher eine Mehrheit der installierten Kapazitäten darstellen.[53]

2.1.4 Gesetzliche Grundlagen der Energiewende

Die zuvor genannten Entwicklungen wurden maßgeblich durch regulatorische Eingriffe vorangetrieben. Als drei wesentliche Gesetze sind hierfür das Erneuerbare-Energien-Gesetz (EEG), das Kraft-Wärme-Kopplungsgesetz (KWKG) und das Energiewirtschaftsgesetz (EnWG) zu nennen. EnWG und EEG setzen EU-Richtlinien um.[54] Diese Gesetze hatten wesentliche Auswirkungen auf das Energiesystem:

- **Erneuerbare-Energien-Gesetz (EEG):**[55] Das EEG hat das Ziel einer nachhaltigen, bezahlbaren Energieversorgung basierend auf EE-Strom. Dazu soll zum einen Strom aus EE ins Stromnetz und zum anderen über Direktvermarktung in die Strommärkte integriert werden. Durch das EEG dürfen EE-Anlagen vorrangig ihren Strom ins Netz einspeisen. Trotzdem ist es Netzbetreibern möglich, bei Netzüberlastungen die Einspeiseleistung zu reduzieren und damit auch EE-Anlagen abzuregeln – das sogenannte **Einspeisemanagement**.

49 Siehe haustec 2018.

50 Vgl. Fraunhofer ISI 2015.

51 Vgl. acatech/Leopoldina/Akademienunion 2020-1.

52 Vgl. Fraunhofer ISI 2015, S. 30.

53 Siehe Hall 2019.

54 „Richtlinien sind Rahmengesetze der EU; sie stellen eine politische Forderung an die Gemeinschaft und müssen von den nationalen Parlamenten der Mitgliedstaaten innerhalb einer gesetzten Frist in nationales Recht umgesetzt werden", siehe Europäisches Parlament 2019.

55 Vgl. EEG 2020.

- **Kraft-Wärme-Kopplungsgesetz (KWKG):**[56] Das KWKG regelt die Abnahme von Strom aus Kraft-Wärme-Kopplung (KWK) und die Zahlung von Zuschlägen durch Netzbetreiber und fördert damit weitere dezentrale Erzeuger zusätzlich zu den durch das EEG geförderten Anlagen. KWK-Anlagen sind Anlagen, durch die sowohl Strom als auch Nutzwärme erzeugt wird.

- **Energiewirtschaftsgesetz (EnWG):**[57] Das EnWG zielt auf einen wirksamen und unverfälschten Wettbewerb bei der Stromversorgung, einen langfristig angelegten leistungsfähigen und zuverlässigen Betrieb von Energieversorgungsnetzen und die freie Bildung von Strompreisen nach wettbewerblichen Grundsätzen – der Strommarkt wurde liberalisiert. Zudem wurde der innereuropäische Wettbewerb gestärkt.

- Das EnWG umfasst unter anderem die Punkte **Entflechtung und Netzbetrieb**. Die Entflechtung führte dazu, dass bisher vertikal integrierte Energieversorgungsunternehmen (Netze, Erzeugung und Vertrieb) mit mehr als 100.000 Kunden ihre Geschäftsbereiche trennen beziehungsweise das Netzgeschäft in Tochterunternehmen auslagern mussten. Dadurch wurden insbesondere die Bereiche Erzeugung und Vertrieb von Übertragung und Verteilung von Strom wirtschaftlich getrennt.

- Der Schwerpunkt Netzbetrieb regelt unter anderem Netzanschluss und Netzzugang. Demnach sind Netzbetreiber verpflichtet, Letztverbraucher, Ladepunkte für Elektromobile, Erzeugungsanlagen und elektrische Speicheranlagen anzuschließen. Zweitens führt ein diskriminierungsfreier Netzzugang dazu, dass alle an das Netz angeschlossenen Teilnehmer die Netze zur Durchleitung von Energie nutzen können. In beiden Fällen müssen die Bedingungen und Entgelte angemessen, diskriminierungsfrei, transparent sowie angemessen bepreist sein.[58] Dies hat zur Folge, dass Netzbetreiber Stromlieferungen fremder Lieferanten zum Kunden innerhalb ihres Versorgungsgebiets durchleiten müssen[59] und Kunden daher freie Lieferantenwahl für ihren Strombezug haben.

Zunehmend findet auch die Digitalisierung Einzug in die Energiegesetzgebung. Besonders ist das „Gesetz zur Digitalisierung der Energiewende“ zu nennen, das Regelungen zum Smart-Meter-Messwesen trifft. Die meisten der weiteren Digitalisierungsbestimmungen dienen unmittelbar einer verbesserten Resilienz und sind daher in Abschnitt 2.3 aufgeführt.

2.1.5 Wertschöpfungsstufen der Energieversorgung

Abbildung 4 stellt die **Wertschöpfungsstufen der liberalisierten und entflochtenen Energieversorgung** dar. Neben den klassischen Stufen Erzeugung, Übertragung und Verteilung treten Bereiche wie Speicherung, Handel sowie eine Vielzahl neuer Geschäftsfelder hervor. Im Zentrum steht der Kunde, der auch als sogenannter Prosumer (zusammengesetzt aus den Begriffen Produzent und Konsument, englisch Producer und Consumer) auftreten kann. Das bedeutet, dass Kunden, die im Besitz von Erzeugungsanlagen sind, nicht mehr nur Energie verbrauchen, sondern auch als

56 Vgl. KWKG 2019.
57 Vgl. EnWG 2020.
58 Vgl. EnWG 2020, § 17, Absatz 1, § 21, Absatz 1.
59 Vgl. Schwab 2012, S. 14.

Erzeuger auftreten können. Verbraucher kommen von einer bisher eher passiven Rolle mehr in eine aktive Rolle und wollen vermehrt Anteil an der Energieversorgung haben (siehe auch Abschnitt 2.2). Durch Entflechtung und Liberalisierung ergeben sich neue Möglichkeiten der Wertschöpfung, deren klassische Stufen mehr und mehr aufgebrochen werden.

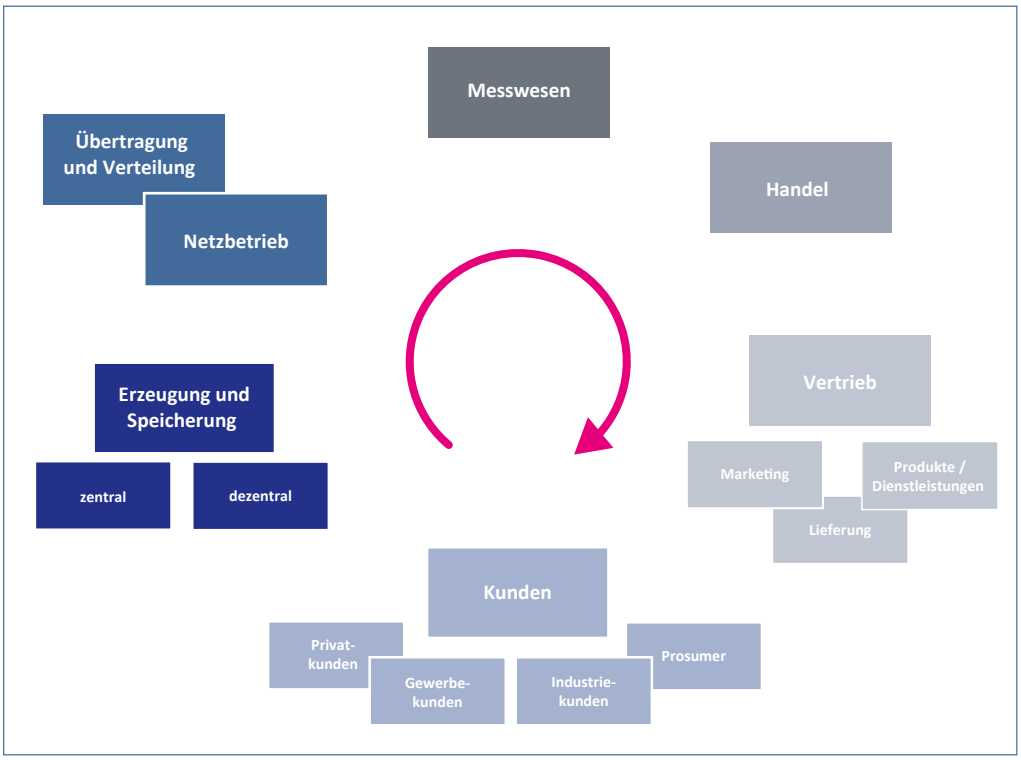


Abbildung 4: Wertschöpfungsstufen der Energieversorgung[60]

Die Liberalisierung hat in den letzten zwanzig Jahren zu mehr Wettbewerb zwischen Erzeugungsunternehmen und auch zwischen Vertriebsunternehmen geführt. Der im EnWG geförderte freie Handel führt insgesamt zu neuen Geschäftsbereichen und **neuen Akteuren innerhalb der verschiedenen Wertschöpfungsstufen**. Teilweise drängen auch branchenfremde Dritte auf den Markt. Die Liberalisierung schafft so zahlreiche zusätzliche Schnittstellen, die einen erheblich höheren Datenaustausch mit sich bringen.[61] Im Bereich Erzeugung beispielsweise veränderte sich die Eigentümerstruktur der konventionellen Erzeugung: Zwischen 2000 und 2004 besaßen die vier großen deutschen Versorgungsunternehmen („die großen Vier“ entsprechend den vier Regelzonen: EnBW, E.ON, RWE, Vattenfall) noch zwischen 80 und 90 Prozent der konventionellen Erzeugungskapazität; im Jahr 2018 lag der Anteil nur noch bei 57 Prozent.[62] Die Integration von EE hat einen ähnlichen Effekt im Hinblick auf die Anzahl der Akteure: Der Markteintritt von neuen Teilnehmern im Bereich verteilte Erzeugung durch EE-Anlagen und kleine KWK-Anlagen änderte die Versorgungsstruktur signifikant.[63] Bereits heute treten dritte Akteure in Form von Aggregatoren in Erscheinung. Aggregatoren bündeln Erzeugungsanlagen, aber auch flexible Verbrauchs- und Speicheranlagen, um sie als virtuelles Kraftwerk zu vermarkten. Damit skalieren sie

60 Angepasst nach BDEW 2016, S. 19 und BMWi 2016, S. 33.
61 Vgl. Schwab 2012, S. 14.
62 Vgl. BNetzA/BKartA 2020, S. 48.
63 Vgl. Brunekreeft et al. 2016, S. 244.

kleine Anlagen auf ein handelbares Volumen (siehe Infobox „Virtuelles Kraftwerk“, Abschnitt 3.2.1). Insgesamt steigt die Anzahl der Akteure – insbesondere auch der dezentralen – im Bereich Erzeugung. Die Beteiligten werden somit noch heterogener als zuvor.

Die Entwicklung der Anzahl der Stromlieferanten zeigt die geänderte Struktur im Vertrieb. Die Möglichkeit, dass Kunden ihre Lieferanten frei wählen können, führte dazu, dass mehr Lieferanten auf den Markt kamen. Während 2008 in 33,6 Prozent aller Netzgebiete über 50 Anbieter tätig waren, stieg der Wert bis 2018 auf 89 Prozent. In 72 Prozent der Netzgebiete sind sogar mehr als 100 Lieferanten aktiv.[64] Außerdem betreten neue Firmen den Markt und bieten neben den Standardlieferprodukten neue Dienstleistungen an. Neben der Anzahl der Lieferanten, zwischen denen Kunden wählen können, ist auch die Anzahl neuer Marktanbieter insgesamt gestiegen.[65]

2.1.6 Energiemärkte und -handel

Wie zuvor beschrieben, müssen für die Stabilität des elektrischen Energiesystems Einspeisung und Entnahme von Strom zu jedem Zeitpunkt im Gleichgewicht sein. Ein entsprechender Ausgleich wird im Wesentlichen durch Stromhandel geregelt. Die Energie wird in Form von Produkten gehandelt, die für die Systemstabilität unterschiedlich kritisch sind. Aus diesem Grund wird zwischen Großhandelsmärkten und Regelleistungsmärkten unterschieden. Über Großhandelsmärkte wird der Handel für die eigentliche Stromversorgung abgewickelt. Regelleistungsmärkte dienen den ÜNB zur Beschaffung von Energie zum genauen Ausgleich von Erzeugung und Verbrauch in den von ihnen verantworteten Regelzonen.

Großhandelsmärkte unterscheiden sich in Strombörsen und OTC-Märkte (englisch Over the Counter – „über den Ladentisch“). Auf Strombörsen, wie zum Beispiel der European-Energy-Exchange(EEX)-Börse oder European Power Exchange (EPEX SPOT), werden sogenannte Termin- und Spotmärkte abgehalten. Terminmärkte dienen im Wesentlichen der Preisabsicherung oder der Spekulation. Spotmärkte ermöglichen den Handel für den nächsten Tag (Day ahead) oder untertäglich (Intraday), das heißt den Handel für Produkte, die am nächsten beziehungsweise am selben Tag zu liefern sind und zu einem physikalischen Stromfluss führen. Auf OTC-Märkten werden bilaterale Geschäfte abgewickelt, das heißt, zwei Parteien einigen sich individuell über gehandelte Produkte und den Preis. Auch hier gibt es entsprechende Spot- oder Terminmärkte.

Das Volumen des Day-Ahead-Handels betrug 2018 an der EPEX SPOT 224,6 Terawattstunden und ist damit im Vergleich zum Vorjahr um 3,7 Prozent gesunken. Das Volumen des Intraday-Handels ist mit 52,8 Terawattstunden um rund 12,5 Prozent gestiegen.[66] Demgegenüber wird im Monitoringbericht der Bundesnetzagentur und des Bundeskartellamts geschätzt, dass das ermittelte Handelsvolumen des OTC-Handels in 2018 im Vergleich zu 2017 mit 5.671 Terawattstunden grob auf dem Niveau des Vorjahres bleibt.[67] Seit vielen Jahren gewinnen die Spotmärkte, insbesondere für den Intraday-Handel, gegenüber dem OTC-Handel an Bedeutung.

64 Vgl. BNetzA/BKartA 2020, S. 267.
65 Vgl. Brunekreeft et al. 2016, S. 245.
66 Vgl. BNetzA/BKartA 2020, S. 248.
67 Vgl. BNetzA/BKartA 2020, S. 262.

In den letzten Jahren zeichnete sich ein weiterer Trend ab: negative Preise. Diese wurden 2008 auf dem deutsch/österreichischen Day-Ahead-Markt und 2007 auf dem deutschen Intraday-Markt eingeführt.[68] Weitere Länder folgten. Negative Preise entstehen, wenn eine hohe Einspeisung aus erneuerbaren Energiequellen erfolgt, die Nachfrage im Verhältnis zur Erzeugung niedrig ist und die Kosten des Nicht-Produzierens bei konventionellen Kraftwerken höher wären als die negativen Preise, die sie für die Produktion zahlen müssen. Es ist durchaus möglich, dass negative Preise irgendwann am Markt nicht mehr vorhanden sein werden, etwa weil überschüssige Energie von Power-to-X-Anlagen abgenommen wird oder flexible Verbraucher sich an das Dargebot stärker anpassen können.

Insgesamt zeigt sich der Trend, dass die **Gegebenheiten an den Energiemärkten zunehmend an den Charakter von EE angepasst** werden, um diese besser an den Märkten zu integrieren: Es werden zunehmend auch kleinere Energiemengen gehandelt, und es vergeht weniger Zeit von der Gebotsabgabe bis zur physikalischen Erfüllung des Handelskontrakts. Denn seit 2011 wurden in vielen europäischen Ländern wie Deutschland, Österreich, Schweiz, Belgien und Niederlande die Produktzeiträume am Intraday-Markt der EPEX SPOT auf 15 Minuten heruntergesetzt. Außerdem wurde in Deutschland der zeitliche Vorlauf des Handels zur Lieferung von 30 auf 5 Minuten gesenkt, das heißt, es kann noch bis fünf Minuten vor Produktlieferung gehandelt werden. Dies wird damit begründet, dass die Vorhersagen insbesondere von Wind- und Solarenergieeinspeisung genauer werden, je kürzer der Vorhersagehorizont ist.[69]

Der Energiehandel bezieht sich auf ein immer größeres räumliches Gebiet, denn es findet eine Kopplung der europäischen Märkte und Regelzonen statt – das sogenannte **Market-Coupling**. Durch dieses werden Regelzonen und Marktgebiete miteinander verknüpft und verschiedene Strombörsen vereinheitlicht. Es beteiligen sich bereits sieben europäische Strombörsen. Durch die Marktkopplung werden insbesondere die Übertragungskapazitäten zwischen den verschiedenen Ländern effizienter genutzt. Zudem führt die Kopplung zu einer Preisangleichung. Sie wird gemeinsam mit den ÜNB und den Strombörsen organisiert. In Europa sind sowohl der Day-Ahead-Markt als auch der Intraday-Markt größtenteils gekoppelt. Das in Europa gekoppelte Gebiet wird Multi-Regional-Coupling (MRC, englisch für multi-regionale Kopplung) genannt und umfasst mittlerweile zwanzig europäische Länder – darunter auch Deutschland.[70] Der grenzüberschreitende Handel nimmt also innerhalb Europas zu. Dies führt zu höheren Belastungen auf den Kuppelleitungen zwischen verschiedenen Regelzonen. Das wiederum hat einen erhöhten Bedarf der Entlastung bestimmter Betriebsmittel wie Leitungen oder Transformatoren zur Folge.

Großhandels- und OTC-Märkte stehen im Grunde beliebigen Akteuren offen. So erscheinen **neue Akteure in verschiedenen Bereichen** wie Produktion, Verbrauch oder Stromhandel.[71] Außerdem ist es Stromhändlern möglich, nur spekulativ am Handel teilzunehmen und keine physikalischen Produkte zu handeln. Das Erfüllen

68 Vgl. EPEX SPOT 20191.
69 Vgl. EPEX SPOT 2017, S. 1.
70 Vgl. BNetzA 2020-2.
71 Brunekreeft et al. 2015, S. 62 ff.

von Produkten (das heißt die vertraglich durch den Handel vereinbarte Energiemenge wird auch tatsächlich physikalisch erzeugt oder verbraucht) ist jedoch kritisch für die Systemstabilität, und das Nicht-Erfüllen von Produkten kann weitreichende – nicht nur finanzielle – Konsequenzen haben.

Um den unverzüglichen Ausgleich von Erzeugung und Verbrauch zu gewährleisten, gibt es sogenannte Regelleistungsprodukte, die an entsprechenden **Regelleistungsmärkten** gehandelt werden. Die Marktteilnehmer sind stark eingegrenzt: Nur ÜNB schreiben entsprechende Produkte aus, und lediglich Betreiber präqualifizierter Anlagen, das heißt Anlagen, die auf technische Eignung geprüft wurden, dürfen bieten.

Die Organisation der Regelleistungsabrufe innerhalb Europas findet durch die **International Grid Control Cooperation** (IGCC, englisch für Internationale Kooperation in der Netzführung) statt. Diese umfasst derzeit 13 ÜNB aus 10 Ländern – neben Deutschland unter anderem Belgien, Dänemark und Tschechien. Ziel ist es insbesondere, dass sich die Mitglieder abstimmen, sodass nicht zur Lösung eines spezifischen Engpasses ein ÜNB negative, ein anderer positive Reserveleistung abruft und somit der Engpass nicht aufgelöst würde.[72]

Neben den genannten etablierten Marktformen rückt die marktbasierte Beschaffung von Netzdienstleistungen durch die europäische Regulierung in den Fokus. Marktbasierte Beschaffung wird aktuell insbesondere für das Thema Flexibilität diskutiert, um Engpässe unter Einbindung von Erzeugern und Lasten auf der Verteilnetzebene zu vermeiden. Neben Produzenten, Verbrauchern und Prosumern könnten künftig auch sehr viele unterschiedliche Anbieter in diesen Märkten aktiv sein (beispielsweise Energieeffizienzdienstleister und Aggregatoren).[73] Für diesen Markt müssen die Netzbetreiber mögliche Netzengpässe prognostizieren und den Bedarf netzdienlicher Flexibilität am Markt ausschreiben. Damit lösen sie die sogenannte gelbe Ampelphase[74] für einen bestimmten Ort und Zeitpunkt aus. Netzbetreiber können dann Flexibilität von Marktteilnehmern abrufen, die zuvor vertraglich vereinbart wurde. Hier zeigt sich bereits eine Tendenz, wie Marktmechanismen genutzt werden können, um auch netzdienliches Verhalten zu erreichen. Aber auch eine Aufteilung der einheitlichen Stromgebotszone Deutschlands ist denkbar. Dadurch würden sich regional verschiedene Strompreise ergeben. Auch über auslastungsabhängige Netzentgelte könnten Anreize für netzdienliches Verhalten gesetzt werden.[75]

Die Anreize für den Netzbetreiber, netzdienliches Verhalten zu honorieren, könnten sich aus der **Anreizregulierung ergeben**. Die Anreizregulierung wird in der Anreizregulierungsverordnung (ARegV)[76] geregelt und soll dazu dienen, dass Netzbetreiber der natürlichen Monopole Strom- und Gasnetz keine Monopolgewinne erzielen und ihre Netze möglichst kostensparend betreiben. Dazu werden Erlösobergrenzen für Netzbetreiber festgesetzt. So wird der Anreiz geschaffen, Kosten zu senken, um so

72 ENTSO-E 2019-1.

73 Vgl. ein erstes White Paper der BNetzA dazu, BNetzA 2011.

74 Siehe Ampelkonzept des Bundesverbands der Energie- und Wasserwirtschaft (BDEW), BDEW 2017.

75 Verschiedene Handlungsoptionen zum Umgang mit Netzengpässen werden in der ESYS-Stellungnahme „Netzengpässe als Herausforderung für das Stromversorgungssystem. Optionen zur Weiterentwicklung des Marktdesigns“ (acatech/Leopoldina/Akademienunion 2020-2) vorgestellt.

76 ARegV 2019.

höhere Gewinne zu erzielen. Aktuell sind resilienzverbessernde Maßnahmen nur dann von der ARegV abgedeckt, wenn diese Maßnahmen zu Kosten führen, die bei dem Netzbetreiber anerkannt werden. Häufig entstehen darüber hinaus allerdings Kosten (etwa die Kosten eines Stromausfalls bei den Netznutzern), die nicht in die Investitionsentscheidung der Netzbetreiber einbezogen werden. Diese Herausforderung wird in Handlungsfeld 5 (Abschnitt 6.5) weiter vertieft.

Auch **Netznutzungsentgelte** können ein Werkzeug zur Steigerung der Resilienz im elektrischen Energiesystem sein. Die Netznutzungsentgelte regeln den Zugang zu den Übertragungs- und Verteilernetzen (Netzentgelte) und umfassen auch die Ermittlung der Entgelte für dezentrale Einspeisungen. Die Netznutzungsentgelte im breiteren Sinne werden in der Verordnung über die Entgelte für den Zugang zu Elektrizitätsversorgungsnetzen (§§ 15 ff. StromNEV) geregelt. Die StromNEV[77] klärt die Struktur der Netznutzungsentgelte, jedoch nicht deren Höhe. Vielmehr leitet sich die Höhe der Netznutzungsgebühren aus der Erlösobergrenze und damit aus der ARegV ab. Zudem werden auch sogenannte **Smart Connection Agreements** (englisch für Vereinbarungen über intelligente Verbindungen) diskutiert. Dies sind flexible Netzanschlussbedingungen für Erzeuger, die dem Netzbetreiber die Möglichkeit der Abregelung (mit oder ohne Entschädigung für den Erzeuger) einräumen. So können insbesondere bereits beim Netzanschluss Netzknappheiten berücksichtigt werden. Solche flexiblen Netzanschlussbedingungen befinden sich aktuell in Erprobung, etwa in Frankreich, Belgien und UK.[78] Diese können auch Möglichkeiten bieten, resilienzverbessernde Maßnahmen zu entwickeln (siehe Abschnitt 6.5).

Neben diesen Märkten entstehen auch neue Modelle, zum Beispiel „Power Purchasing Agreement“ (PPA, englisch für Strombezugsvereinbarung): Ein Investor erbaut eine Anlage, etwa eine große PV-Anlage ohne jede Förderung, und ein Energieunternehmen garantiert über einen längeren Zeitraum die Abnahme der erzeugten Energie zu einem vorab vereinbarten Preis pro Megawattstunde. Für große PV-Anlagen sind solche Modelle schon heute betriebswirtschaftlich tragfähig. Für die Entwicklung im Energiesektor (Investitionsverhalten, Energiepreise usw.) spielt die Höhe des CO_2-Preises eine große Rolle – und auch, auf welche Art dieser ermittelt wird. Jedoch wirkt sich dies kaum auf Digitalisierung und Resilienz aus und wird daher hier nicht weiter betrachtet. Darüber hinaus sind viele Formen zukünftiger Märkte denkbar. Einige dieser Marktformen werden bereits erprobt. Dazu gehören etwa Peer-to-Peer-Märkte (englisch etwa für „zwischen Gleichgestellten“). Dies bedeutet, dass verschiedene Marktakteure nicht mehr über zentrale Instanzen wie Marktplätze agieren, sondern der direkte Zugang zueinander ermöglicht wird (siehe Abschnitt 3.2.3).

77 StromNEV 2019.

78 Vgl. Furusawa et al. 2019.

2.2 Das Energiesystem als soziotechnisches System

Das elektrische Energiesystem als **soziotechnisches System**[79] umfasst alles, was erforderlich ist, um die gesellschaftliche Funktion der Stromversorgung zu erfüllen. Dabei wird in einer breiten Auslegung nicht nur die Angebotsseite (dazu zählen unter anderem Produktion, Infrastruktur, Kapital, Wissen), sondern auch die Nutzer- oder Nachfrageseite (dazu zählen unter anderem Nutzerverhalten) sowie die Verteilung (etwa Märkte, Medien) von Technologien betrachtet. Es werden insbesondere die Wechselwirkungen zwischen technischem System (zum Beispiel Stromnetze, Erzeugungs- und Verbrauchsanlagen, damit verbundene IKT) und Gesellschaft berücksichtigt, denn ein soziotechnisches System ist charakterisiert durch die Co-Evolution beider Bereiche – sie beeinflussen und formen sich gegenseitig. So entstand und wandelt sich das Energiesystem als soziotechnisches System auf Grundlage von gesellschaftlichen Bedürfnissen, Erkenntnissen und Strömungen. Andererseits hat es Rückwirkungen auf die Gesellschaft, da sich zum Beispiel durch Veränderungen in der Stromversorgung Lebensumstände ändern oder neue gesellschaftliche Strukturen geschaffen werden können. Neben den technischen Aspekten ist es also auch wichtig, soziale Aspekte zu berücksichtigen, um die Zusammenhänge und Dynamiken in einem soziotechnischen System zu verstehen und gegebenenfalls zu lenken.

In diesem Zusammenspiel sind nicht nur das soziotechnische System selbst, sondern auch die in ihm aktiven Akteure relevant. Diese umfassen Einzelakteurinnen und -akteure, also Individuen, aber auch soziale Gruppen und Organisationen. Zu den sozialen Gruppen und Organisationen gehören beispielsweise Wissenschaftlerinnen und Wissenschaftler, Konsumentinnen und Konsumenten, Umweltverbände und Bürgerinitiativen, Entscheidungsverantwortliche, Firmen und Universitäten.

Die Energiewende und Liberalisierung sind Beispiele für den soziotechnischen Wandel des elektrischen Energiesystems: So entwickelt sich die Stromproduktion weg von zentralen, fossilen oder nuklearen Großkraftwerken hin zu erneuerbaren Energiequellen (siehe Abschnitt 2.1.2). Zudem schafft die Liberalisierung neue Märkte und bringt neue Akteure hervor (siehe Abschnitt 2.1.5). Durch diese Entwicklungen ändert sich auch die Rolle der Privatakteure. Während im konventionellen elektrischen Energiesystem private Verbraucherinnen und Verbraucher lediglich Nutzer der Stromversorgung waren, nehmen **Privatakteure** in einem dezentralen Energiesystem eine zunehmend **aktive Rolle** ein – beispielsweise als Prosumer –, und ihr Verhalten hat wiederum Rückwirkungen auf das elektrische Energiesystem. Darüber hinaus haben Verbraucherinnen und Verbraucher als Teil des soziotechnischen Systems auch indirekten Einfluss, etwa durch ihr Verbrauchsverhalten oder die Wahl ihrer Stromlieferanten. Dieses Einflusses sind sie sich in den meisten Fällen gar nicht bewusst.

Privatakteure können auch politisch Einfluss auf die Gestaltung des Energiesystems nehmen, indem sie als Gruppen von Privatnutzern oder Organisationen Druck auf Politik und Entscheidungsträger ausüben und so neue Regeln herbeiführen. Dies können auch Regeln sein, die Netzbetreiber aus Stabilitätsgründen als problematisch

79 Der Begriff soziotechnisches System stammt aus der Transitionsforschung, die sich mit den Veränderungsprozessen zu einer nachhaltigeren Gesellschaft beschäftigt. Ein Beispiel dieses Forschungsgebiets ist der Wandel des Energiesystems.

ansehen, wie das Beispiel der sogenannten Balkonsolaranlagen zeigt (siehe Infobox „Steckbare Solargeräte, Balkonkraftwerk, SolarRebell oder Guerilla-PV“).

Generell erwarten die Verbraucher, dass sie zu jeder Zeit so viel Strom beziehen können, wie sie benötigen. Sie erwarten, dass sich Verfügbarkeit und Qualität der Stromversorgung nicht verschlechtern und dass die Politik im Sinne der Daseinsvorsorge alle Maßnahmen für ein zuverlässiges elektrisches Energiesystem trifft.

Steckbare Solargeräte, Balkonkraftwerk, SolarRebell oder Guerilla-PV

Seit dem 27. April 2019 ist es möglich, dass Verbraucher PV-Anlagen bis zu einer Leistung von 600 Watt selbst installieren und beim Netzbetreiber anmelden dürfen. Es bedarf keiner Einwilligung mehr durch den Netzbetreiber oder der Installation durch einen Elektroinstallateur.[80] Somit kann jeder Verbraucher PV-Anlagen installieren – zum Beispiel auf dem Balkon. Nutznießer dieser Entwicklung sind neben Hausbesitzerinnen auch etwa Wohngemeinschaften oder Kleingärtner.

Dies ermöglichte eine Neuregelung der Norm des VDE „VDE-AR_N 4105“, die ihrerseits die EU-Verordnung 2016/631 zum Netzanschluss für Stromerzeuger umsetzt. An dem Normierungsverfahren war die Deutsche Gesellschaft für Sonnenenergie e. V. (DGS) beteiligt, eine Organisation für Belange des Verbraucherschutzes, die sich bereits 2017 dafür einsetzte, dass PV-Module an normale Haushaltsstromkreise angeschlossen werden dürfen. Wesentlicher Treiber der Neuregelung waren laut DGS Einsprüche von über 900 Bürgerinnen und Bürgern.[81] Ob diese Anmeldung beim Netzbetreiber auch tatsächlich erfolgt, wird sehr vom bürokratischen Aufwand abhängen, den der jeweilige Netzbetreiber vorsieht.

Neben den Verbrauchern und Akteuren der Wertschöpfungsstufen der Stromversorgung (siehe Abschnitt 2.1) gibt es eine Reihe **weiterer Akteure**, die mit dem elektrischen Energiesystem interagieren, es beeinflussen beziehungsweise von ihm beeinflusst werden. Diese Akteure und Akteursgruppen sind vielfältig und heterogen und haben unterschiedliche Interessen und Erwartungen.

- **Politik** umfasst die Gesetzgeber und die ausführende Gewalt, also die Regierung, die Ministerien und Behörden (siehe Abschnitt 2.3). Dies gilt sowohl auf nationaler als auch auf europäischer Ebene, da die EU-Richtlinien in nationales Recht umgesetzt werden müssen. Aber auch die regionale Legislative und Umsetzung ist relevant.

- **Regelsetzende Gremien** sind Verbände oder Organisationen (und somit Teil der gesellschaftlichen Akteure), die insbesondere beauftragt wurden, bestimmte technische Regeln zu entwickeln. Grund hierfür ist, dass die Politik die technischen Details für die Umsetzung von Gesetzen oder Verordnungen den Fachleuten überlassen möchte (siehe Abschnitt 2.3).

- **Gesellschaftliche Akteure** umfassen zum einen Verbände oder gesellschaftliche Gruppen, die Interessen unter anderem aus der Wirtschaft oder dem Umweltschutz vertreten. Verbände sind in der Regel Vereine, deren Mitglieder hauptsächlich juristische Personen sind. Zum anderen sind es Vertretungen zivilgesellschaftlicher Gruppen. Dazu zählen Vereine, Stiftungen, Nichtregierungsorganisationen, aber auch Bürgerbewegungen. Diese Akteure können als Interessenvertretung insbe-

80 Siehe: Hannen 2019, DGS/Greenpeace Energy 2019.

81 Vgl. DGS/Greenpeace Energy 2019.

sondere Druck auf Entscheidungsträger ausüben, um mögliche Entscheidungen zu ihren Gunsten beziehungsweise zugunsten der von ihnen vertretenen Personen zu bewegen.

- **Hersteller** für Energietechnik beziehungsweise operative Technik umfassen im Grunde alle Hersteller, die Produkte für die Wertschöpfungsstufen Erzeugung und Speicherung, Netzbetrieb und Messwesen herstellen; hierzu gehören unter anderem Erzeugungs- und Speicheranlagen, intelligente Betriebsmittel und Messgeräte. Insbesondere sind hier auch Hersteller von Software inbegriffen, die als eingebettete Systeme in OT-Geräte integriert ist und somit die Intelligenz der Geräte bestimmt.

Diese Akteure können jedoch nicht frei agieren, sondern sind an bestimmte Regeln gebunden: Ihre sozialen Handlungen sind immer abhängig von dem Kontext, in dem sie sich bewegen. Dazu zählen Regulierungen, Normen, aber auch Werte und Grundannahmen. Historisch gewachsene und weit verbreitete Regeln haben einen stärkeren Einfluss als Regelungen, die gegebenenfalls nur Relevanz für kleine Akteursgruppen haben. Regeln existieren immer im Wechselspiel mit anderen Regeln und lassen sich nicht individuell isolieren. Akteure interagieren innerhalb der Einschränkungen und Möglichkeiten, die ein System von Regeln eröffnen, und andererseits können sie Regeln auch verändern (siehe Beispiel Infobox „Steckbare Solargeräte, Balkonkraftwerk, SolarRebell oder Guerilla-PV“). Demgegenüber stellt ein soziotechnisches System den Rahmen für die Handlungen der Akteure dar. Akteure können allerdings Aspekte eines soziotechnischen Systems auch auf andere Weise verändern, zum Beispiel durch Investitionen sowie Einführung neuer Technologien oder neuer Regulierungen.

Durch das Verständnis von Dynamiken im soziotechnischen System ist es möglich, zu erfassen, wie verschiedene Entscheidungsträger gewünschte Veränderungen herbeiführen können.[82] Versorgungsunternehmen sind wegen ihrer speziellen Charakteristiken besonders resistent gegen Wandel.[83] Dazu zählt auch die Energieversorgung, deren Wandel wegen der festen Infrastruktur sehr träge ist und starke Pfadabhängigkeiten aufweist.

Soziotechnische Veränderungen können als Prozess des institutionellen[84] Wandels gesehen werden.[85] Es können drei Kategorien von **institutionellen** Säulen entsprechend ihrer Wirkung auf die Akteure unterschieden werden[86]. Im Folgenden werden die Eigenschaften dieser Kategorien beschrieben.

- Regulativ: formale Regeln, die das Verhalten durch Belohnungen oder Strafen beschränken. Dazu zählen Gesetze, Verträge oder Regulationen.

- Normativ: Werte, Normen, Erwartungen an bestimmte Rollen, aber auch Verantwortung. Sie werden durch moralischen Druck und gesellschaftliche Sanktionen wie

82 Vgl. Geels 2004, S. 916.

83 Vgl. Fünfschilling 2014, S. 11.

84 Institutionen sind in der Soziologie historisch gewachsene, weit verbreitete und akzeptierte Spielregeln, die die Wahrnehmung und das Verhalten von Akteuren beeinflussen.

85 Vgl. Fünfschilling 2014, S. 20.

86 Scott 2001.

soziale Ächtung durchgesetzt. Es wird angenommen, dass diese durch die Sozialisierung internalisiert, also verinnerlicht werden.[87]
- Kognitiv: meist implizite Regeln, die sich auf die wahrgenommene Realität von Individuen oder Gruppen und das Rahmenwerk beziehen, durch das Bedeutung und Sinn erzeugt wird. Dazu zählen unter anderem Glaube und Überzeugungen, Verhaltensmuster, aber auch Sprache beziehungsweise Jargon.

Ein gesellschaftlicher Wertewandel benötigt eine lange Zeit. Anreize können diesen Wandel beschleunigen. Ein Wertewandel muss über alle drei institutionellen Säulen vollzogen werden.[88] Die Bereitschaft, Verantwortung zu übernehmen und sein Verhalten anzupassen – also normative Regeln –, kann über Einzelinitiativen oder Lobbyarbeit ermöglicht werden. Die Politik kann explizit bei den regulativen Regeln ansetzen, indem beispielsweise Verbote für Kohlekraftwerke erlassen werden. Normative und kognitive Regeln können eher durch indirekte Maßnahmen der Politik erreicht werden. So ist ein normativer Wandel in dem Umdenken zu sehen, dass erneuerbare Energien als gemeinsames Ziel verstanden werden. Ein kognitiver Wandel wäre gegeben, wenn Stromsparen zur Selbstverständlichkeit würde, die bereits Kindern in der Schule vermittelt wird. Wesentlich ist es hier, die verschiedenen Akteure angemessen einzubeziehen. Bildung und Erziehung spielen ebenfalls eine wichtige Rolle. Ein wesentlicher Aspekt ist hierbei auch die Akzeptanz von Änderungen oder Neuerungen.

Das Konzept der Resilienz (siehe Kapitel 5) kann helfen, dass Entscheidungsträger mit den geänderten Herausforderungen in der Stromversorgung umgehen können. Das stärkt das Vertrauen und damit auch die Akzeptanz gegenüber neuen digitalen Technologien und damit einhergehenden Maßnahmen zur Steuerung. Es gibt **verschiedene Dimensionen von Akzeptanz**:[89]

- Soziopolitische Akzeptanz steht für die generelle Akzeptanz von Politik oder Technologien durch die Gesellschaft, verschiedene Interessengruppen und Entscheidungsträger. Diese ist im Zusammenhang mit Technologien der erneuerbaren Energie in vielen Ländern hoch.

- Community-Akzeptanz (Gemeinschaftsakzeptanz) bezieht sich auf die Akzeptanz der Standortwahl etwa von erneuerbaren Energien durch lokale Beteiligte wie Anwohner und Behörden. Hierunter fällt die NIMBY-Einstellung (englisch für Not in my backyard – nicht in meinem Hinterhof), die beschreibt, dass erneuerbare Energien akzeptiert sind, solange man nicht persönlich betroffen ist. Andererseits kann diese Akzeptanz auch durch Beteiligung der Akteure steigen. Wesentlich sind hier Faktoren wie Vertrauen in die verantwortlichen Akteure und das Gefühl von Gerechtigkeit.

- Markt-Akzeptanz beschreibt die Nachfrageseite etwa nach Strom aus erneuerbaren Energiequellen und die Bereitschaft, in neue Technologien zu investieren.

Das Energiesystem sieht sich vor einem neuen Transformationsprozess durch die Digitalisierung, da mehr und mehr digitale Technologien in das Stromnetz integriert und

87 Vgl. Geels 2004.
88 Vgl. Scott 2001.
89 Vgl. Wüstenhagen et al. 2007, S. 2684 ff.

dort genutzt werden (siehe Abschnitt 3.2). Der Einfluss von Privatakteuren auf die Stabilität des elektrischen Energiesystems wird perspektivisch durch die Digitalisierung noch deutlich steigen. Dies kann auch einen Wandel in Einstellungen und Verhaltensweisen einleiten, was sich dann wiederum auf die weitere Digitalisierung und deren Regulierung auswirkt. Anreize für Wertewandel in einem digitalisierten Energiesystem werden wichtig sein, um Akzeptanz für Resilienzmaßnahmen (siehe Handlungsfeld 6 / Abschnitt 6.6) zu schaffen.

2.3 Akteure und politische Regelungen zur Systemsicherheit

Versteht man die Sicherung der KRITIS Energie als eine wesentliche Aufgabe des Staates, ist darzustellen, durch welche Verantwortlichkeiten und Maßnahmen der Staat dieser Verantwortlichkeit nachkommt. Zudem kann auch die Gesellschaft Einfluss auf Regelungen – etwa durch Bürgerinitiativen oder Interessenvertretungen – nehmen (siehe Abschnitt 2.2 und Infobox „Steckbare Solargeräte, Balkonkraftwerk, SolarRebell oder Guerilla-PV“). Eine umfassende energie- und IT-rechtliche Bewertung und Zusammenfassung ist im Rahmen dieser Analyse zwar nicht leistbar, jedoch soll zumindest überblickartig für wesentliche technische Aspekte dargestellt werden, mit welchen Instrumenten der Staat die KRITIS Energie sichert, indem er Akteure durch Regelsetzungen direkt verpflichtet oder Regelsetzungen an weitere Akteure delegiert. Dies ist notwendig, um möglichen Handlungsbedarf in politische Verantwortlichkeit zu übersetzen. Abbildung 5 gibt einen Überblick dazu.

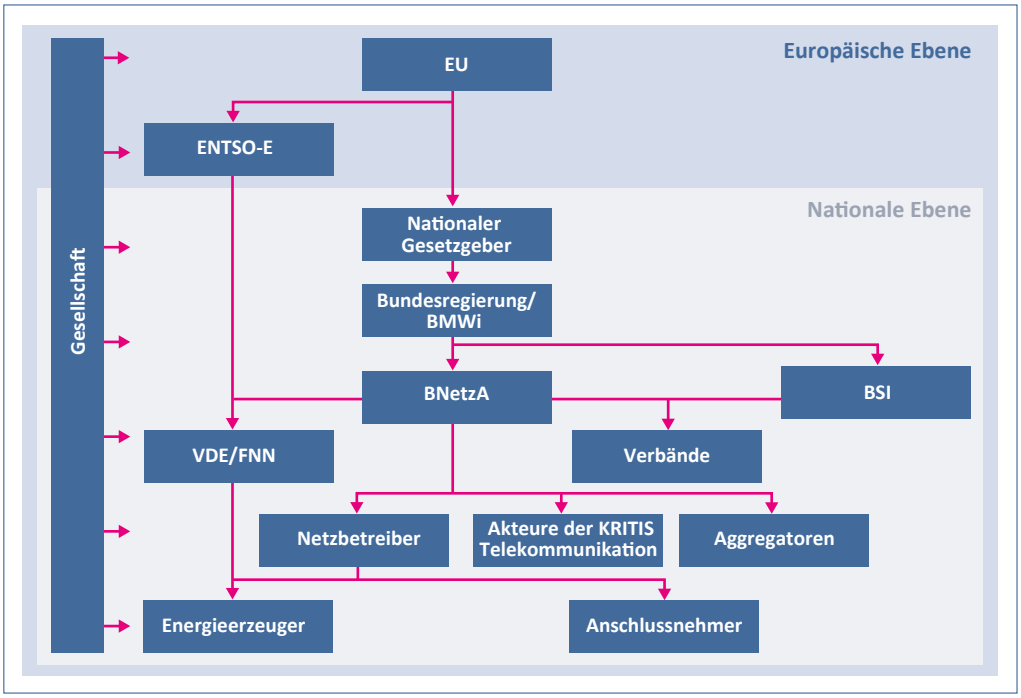


Abbildung 5: Hierarchie der Regulierung und Regelsetzung. Die Pfeile zeigen, wer wem Pflichten auferlegt.

Auf **EU-Ebene** wird für die ÜNB einiges festgelegt, was sie zur Stabilisierung der Netze tun müssen und sollen – insbesondere, wenn mehr als die Versorgungssicherheit des eigenen Landes betroffen ist. Dies geschieht häufig über den Verband **European Network of Transmission System Operators (ENTSO-E)**. Dieser ist das Gremium für die Zusammenarbeit der europäischen ÜNB. ENTSO-E repräsentiert 43 ÜNB aus 36

Ländern.[90] Die Aufgabenbereiche von ENTSO-E umfassen unter anderem die technische Koordination der ÜNB. Die ENTSO-E kann von der Europäischen Kommission beauftragt werden, Netzkodizes zu erarbeiten.[91] Die europäischen Network Codes werden von ENTSO-E mit der Agentur für die Zusammenarbeit der europäischen Energieregulierungsbehörden (englisch: Agency for the Cooperation of Energy Regulators, ACER) und der Kommission erarbeitet und von der EU erlassen und dienen dem Zweck, auf europäischer Ebene einheitliche technische Mindestanforderungen für den Netzzugang und den Netzbetrieb sowie Regeln für die Strommärkte zu harmonisieren, soweit dies auf europäischer Ebene erforderlich ist (ansonsten gilt das Subsidiaritätsprinzip). Sie sind in allen Mitgliedstaaten verbindlich und regeln nicht nur Angelegenheiten der grenzüberschreitenden Netze, sondern setzen auch den Rahmen für nationale Regelungen.[92] Gemäß der novellierten Strommarkt-VO kann neben ENTSO-E auch eine neue, noch zu schaffende Organisation der Verteilernetzbetreiber in der Union entsprechend an den Network Codes mitarbeiten (Artikel 52 ff.). Auch kann die Kommission initiativ vorgehen (siehe Artikel 59 Absatz 14) und Network Codes nach Konsultation von ACER, ENTSO-E und der maßgeblichen Interessenträger erlassen. Zusätzlich existieren Leitlinien (Guidelines), bei denen die Rolle der ENTSO-E wesentlich schwächer ist.[93]

Innerhalb eines Landes ist der **nationale Gesetzgeber** weitgehend für die Absicherung gegen Blackouts zuständig. Doch auch durch die Regulierungsbehörden sind Entscheidungen zu treffen, insbesondere bei den Network Codes. Bis auf wenige Ausnahmen (siehe unten) ist der nationale Gesetzgeber in Bezug auf Resilienz weitgehend von der EU-Ebene unabhängig. Die Vorsorge gegen Stromversorgungskrisen größeren Umfangs und mit weitreichenderen Folgen, die sich nicht mehr durch Vorschriften des Netzbetriebs regeln lassen, wird aber etwa auf EU-Ebene, insbesondere durch die VO (EU) 2019/941, geregelt. In ihr ist festgelegt, was die Mitgliedstaaten tun sollten, um diesen Krisen vorzubeugen, und welche Maßnahmen sie ergreifen können, falls die Bestimmungen für den Netzbetrieb allein nicht mehr ausreichen. Die Regierung hat in einigen Bereichen die Möglichkeit der Ausgestaltung über Verordnungen. Die Ausgestaltung der Gesetze durch Rechtsverordnungen obliegt in aller Regel dem **Bundesministerium für Wirtschaft und Energie (BMWi)** oder der Bundesregierung. Die **Bundesnetzagentur (BNetzA)** setzt den Konkretisierungsprozess durch Festlegungen fort, soweit die entsprechende Ermächtigungsgrundlage vorliegt; juristisch handelt es sich dabei um Allgemeinverfügungen, die gerichtlich überprüfbar sind. Die Standardisierung und die technische Umsetzung in Prozessen, Schnittstellen etc. wird meist an Verbände und Standardisierungsgremien übertragen – insbesondere dem Verband der Elektrotechnik Elektronik Informationstechnik (VDE)/Forum Netztechnik/Netzbetrieb (FNN),[94] der unter anderem (gesetzlich legitimiert) für bindende Normen und Regeln in der Energieversorgung zuständig ist.

Den Netzbetreibern werden umfassende Rechte eingeräumt, Regeln zu erlassen, die festlegen, welche technischen und sonstigen Richtlinien Anlagen befolgen müssen, die sie im Netz anschließen, und legen damit Regeln für die Netzanschlussnehmer fest.

90 ENTSO-E 2019-2.

91 Novellierte Strommarkt-VO (EU) 2019/943, Artikel 58 ff.

92 Weitere Verordnungen der EU zu Grid Codes: Verordnung (EU) 2016/631 der Kommission vom 14. April 2016, Verordnung (EU) 2016/1388 der Kommission vom 17. August 2016.

93 Wie etwa die Verordnung (EU) 2015/1222 der Kommission vom 24. Juli 2015 zur Festlegung einer Leitlinie für die Kapazitätsvergabe und das Engpassmanagement.

94 EnWG 2020 § 49.

Diese Verpflichtung der Netzbetreiber, technische Vorschriften – sie werden auch **technische Anschlussbedingungen** (TAB) genannt – zu definieren, ist in § 19 EnWG geregelt. Der VDE ist durch § 19 EnWG beauftragt, **technische Anschlussregeln** (TAR) festzulegen. Die TAR sind Grundlage für die TAB und fassen die wesentlichen netzübergreifenden, bundesweit einheitlichen Mindestanforderungen für den Anschluss von Kundenanlagen an die öffentlichen Energieversorgungsnetze zusammen und legen Handlungspflichten von Netzbetreibern, Anlagenbetreibern, Planern sowie Kunden fest.[95] Sie werden regelmäßig überarbeitet und angepasst, um veränderten Bedingungen Rechnung zu tragen. Zudem übernimmt der VDE|FNN die Anforderungen aus den europäischen Network Codes in die TAR und gestaltet diese gegebenenfalls aus.[96]

Neben den Rechten gibt der nationale Gesetzgeber den Netzbetreibern, besonders den ÜNB, sowie den Betreibern großer Anlagen der Erzeugung und Speicherung auch Pflichten. Dies geschieht heute überwiegend im EnWG §§ 12–14. Zentraler Paragraf zur Systemsicherheit ist der § 13 EnWG, der die Rechte und Pflichten bezüglich der Systemverantwortung festlegt. Dies gilt sowohl für ÜNB als auch über § 14 für VNB. Die Netzbetreiber können nach § 12 (4) andere Akteure wie Betreiber von Erzeugungsanlagen oder nachgelagerten Netzen sowie industrielle und gewerbliche Letztverbraucher anweisen, Informationen wie Stammdaten, Planungsdaten und Echtzeitdaten zur Verfügung zu stellen, wenn dies der Systemsicherheit dient. Weitere nationale Regelungen betreffen zum Beispiel den „Schutz europäisch kritischer Anlagen“ (§ 12g EnWG). Auch durch die „Netzreserve“ (§ 13d) (Kraftwerke in In- und Ausland, insbesondere für spezielle Belastungssituationen inklusive Blackout) und die „Kapazitätsreserve“ (§ 13e), §§ 13 d) und e) (Bereitstellung von elektrischer Energie, falls der Markt nicht genug Energie zur Verfügung hat) sorgt der Staat dafür, dass Versorgungssicherheit gesichert wird. Ort und Menge der national benötigten Erzeugungskapazitäten werden also nicht vollständig dem Markt überlassen – insbesondere, weil sich dieser wenig eignet, für seltene hochkritische Situationen ausreichend Kapazität bereitzustellen. Das EnWG verpflichtet auch Errichter und Betreiber von Energieanlagen, technische Sicherheit zu gewährleisten und allgemein anerkannte Regeln der Technik zu beachten (§ 49). Dies wird vermutet, wenn sie sich an die Standards und Anschlussregeln des VDE oder alternativ vergleichbarer Vorschriften des europäischen Wirtschaftsraums (vor allem der EU) halten (§ 49). Wie solche Sicherheitsregeln eingeführt werden, kann von der BNetzA bestimmt werden und muss die Grundsätze des Deutschen Instituts für Normung (DIN) berücksichtigen. Im Einzelnen darf auch das **BMWi** mit Zustimmung des Bundesrates technische Vorschriften für Anlagen direkt festlegen (§ 49 Absatz 4 EnWG). Des Weiteren werden auch im EEG Regelungen getroffen – etwa, dass Netzbetreiber Einspeisemanagement (Abregelung von EE-Anlagen) durchführen dürfen.

Die **Verfahren zur Bereitstellung der Regelleistung** werden von der BNetzA[97] bestimmt, doch werden die EU-Vorgaben immer wichtiger. Die technischen Anforderungen für Anbieter von Regelleistung sind von den ÜNB zu spezifizieren. Auch die Regelungen zum Netzausbau hängen zum Teil mit der Versorgungssicherheit zusammen und sind umfangreich im EnWG und weiteren Verordnungen geregelt.

95 Siehe VDE|FNN 2018-1.

96 Siehe VDE|FNN 2019-2.

97 Und der EU, Verordnung (EU) 2017/1485 der Kommission vom 2. August 2017.

Zudem rückten in den letzten Jahren immer mehr die **IKT-Systeme der Energieakteure und deren Sicherheit** in den Fokus der Energieregulierung. Aus diesem Grund hat die Europäische Kommission eine Empfehlung mit Richtlinien verabschiedet, um die Herausforderungen der Cyber-Sicherheit im Energiesektor zu adressieren.[98] Für die IT-Sicherheit in Deutschland ist das **Bundesamt für Sicherheit in der Informationstechnik (BSI)** verantwortlich – es ist die nationale IT-Sicherheitsbehörde. Die Aufgaben und Befugnisse des BSI werden durch das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik[99] (BSI-Gesetz) festgelegt. Das BSI verlangt Informationssicherheit[100] nach dem Stand der Technik und ermächtigt Verbände, verbindliche Richtlinien zu erarbeiten. Zur Abnahme der Umsetzung dieser Regelungen zertifiziert das BSI wiederum spezialisierte Unternehmen, die dann als „Informationssicherheits-TÜV" fungieren. Durch das BSI-Gesetz wird das BSI ermächtigt, zu definieren, was kritische Infrastrukturen sind (siehe Infobox „Kritische Infrastruktur elektrische Energieversorgung"). Wenn es um KRITIS geht, also die Konzentration auf eine möglichst geringe Vulnerabilität gegenüber großen Stromausfällen, enden die Maßnahmen und Verantwortlichkeitsketten gemäß der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) bei sehr großen Leistungsmengen, die operativ *in einer Hand* liegen. Dies ist aus heutiger Sicht auch sinnvoll. Das (gesetzliche) Augenmerk liegt auch wesentlich auf jeweils einer Infrastruktur, nicht auf gekoppelten KRITIS. Dass sich der Fokus ändern muss, ist auf europäischer Ebene bereits diskutiert und insbesondere Teil der Empfehlung der EU-Kommission (siehe oben), die in wesentlichen Teilen in das Clean Energy for All European Package eingegangen ist.[101]

Das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (**IT-Sicherheitsgesetz**, kurz: IT-SiG) enthält Änderungen bereits bestehender Gesetze, unter anderem des EnWG. Die Änderungen beziehungsweise Ergänzungen des EnWG, die im Rahmen des IT-SiG beschlossen wurden, beinhalten technische Mindeststandards für die Sicherheit sowie Meldepflichten für Betreiber kritischer Infrastrukturen. Diese werden in EnWG § 11 1a–c geregelt. Zur Erfüllung von § 11 Absatz 1a des EnWG (sicherer Netzbetrieb) erstellte die BNetzA im Einvernehmen mit dem BSI entsprechende Kataloge an Sicherheitsanforderungen.[102] Diese **IT-Sicherheitskataloge** verpflichten die Betreiber zur Umsetzung IT-sicherheitstechnischer Mindeststandards. Kernforderung ist die **Etablierung eines Informationssicherheits-Managementsystems (ISMS)** gemäß DIN EN ISO/IEC 27001 sowie dessen Zertifizierung. Eine ausführliche Analyse und Bewertung aller im IT-Kontext bestehenden Risiken ist elementarer Bestandteil dieses Prozesses.[103] Das BSI unterstützt KRITIS-Betreiber (Netze, Erzeuger) auch operativ im Falle schwerer Störungen oder besonders ausgeklügelter Angriffe auf informationstechnische Systeme. Das **IT-Lagezentrum** beispielsweise identifiziert, dokumentiert und analysiert Sicherheitsvorfälle und erstellt daraufhin Informationen

98 European Commission 2019.

99 BSIG 2019.

100 Informationssicherheit hat den Schutz von Informationen zum Ziel. Dabei können Informationen sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein. Die Schutzziele oder auch Grundwerte der Informationssicherheit sind Vertraulichkeit, Integrität und Verfügbarkeit. Viele Anwender beziehen in ihre Betrachtungen weitere Grundwerte mit ein. Bedrohungen ergeben sich etwa aus höherer Gewalt, menschlichen oder technischen Fehlern oder vorsätzlichen Handlungen.

101 European Commission 2019.

102 IT-Sicherheitskatalog gemäß § 11 Absatz 1a (Netzbetreiber), 1b (Anlagenbetreiber) EnWG 2020.

103 BSI-Standards 200-1 (BSI 2017-1), 200-2 (BSI 2017-2), 200-3 (BSI 2017-3). Diese sind kompatibel mit internationalen Normen wie DIN ISO/IEC 27001, 27002 und 27019.

und Warnungen. Es reagiert zeitnah auf Schwachstellen und Sicherheitsvorfälle. Außerdem fungiert das IT-Lagezentrum „als zentrale Meldestelle für IT-Sicherheitsvorfälle unter anderem in der Bundes- und Landesverwaltung sowie den Kritischen Infrastrukturen“.[104] Zum IT-Krisenmanagement gehören ebenfalls Übungen, zum Teil mit Partnern aus dem UP KRITIS. Der UP KRITIS ist eine Kooperation zwischen öffentlichen und privaten Partnern wie Betreibern kritischer Infrastrukturen, deren Verbänden und den zuständigen staatlichen Stellen.[105] Für die Umsetzung der Sicherheitsanforderungen dürfen Verbände zusätzlich Standards entwickeln, die, soweit vom BSI abgenommen, für Anlagenbetreiber verpflichtend werden.[106] Zum Beispiel wurde für diejenigen Aggregatoren, die aufgrund ihrer Größe als Teil der kritischen Infrastruktur gewertet werden, vom BDEW in Zusammenarbeit mit entsprechenden Aggregatoren ein Standard für die Erfüllung des BSIG erarbeitet (branchenspezifischer Sicherheitsstandard, B3S). Dieser wurde vom BSI freigegeben.[107]

Für die **KRITIS Telekommunikation** werden ebenfalls Vorschriften erlassen. Das BSI hat darüber hinaus die Aufgabe, Informationen bereitzustellen und auch für das Thema Sicherheit zu sensibilisieren. Für die Anbieter der Regelenergie gibt es wie erwähnt noch einmal besondere Anforderungen, die von den ÜNB unter Berücksichtigung von Empfehlungen des BSI definiert werden, zum Beispiel zu redundanten Rechenzentren. Besonders relevant für Anlagen, die Regelleistung bereithalten, sind Präqualifikationsregeln, die von den ÜNB gemeinsam festgelegt werden und auf deren Webseite[108] veröffentlicht sind.

Das EEG regelt, dass EE-Anlagen ab einer gewissen Größe (100 Kilowatt allgemein, 30 Kilowatt für PV-Anlagen) IT-technisch mit dem System der Netzbetreiber kommunizieren können müssen. Die Kommunikationsanbindung dezentraler Anlagen (Haushalte, EE-Anlagen, Ladesäulen etc.) über intelligente Messeinrichtungen (und sehr viele weitere Fragen, etwa welche Daten mit welcher Granularität an wen übertragen werden dürfen) ist im **Messstellenbetriebsgesetz (MSBG)** geregelt. Insbesondere wird dort auch definiert, was unter Sicherheit der Kommunikation zu verstehen ist. In der Regel sind dazu sowohl die Schutzprofile (die unter anderem Anforderungen an die organisatorischen Sicherheitspolitiken beinhalten) als auch die technischen Richtlinien des BSI durch den verantwortlichen Betreiber der Messstelleninfrastruktur (häufig der lokale Netzbetreiber in seiner Rolle als grundzuständiger Messstellenbetreiber) zu erfüllen.[109] Umfang und Anforderungen an die BSI-Regeln werden ebenfalls hier definiert. Um Geräte wie etwa Ladesäulen oder PV-Anlagen über das Smart Meter Gateway (SMGW) zu regeln oder zu steuern, bedarf es derzeit einer standardisierten Hardware, die „Steuerbox“, da das SMGW die Schaltfunktion nicht aus dem Gerät selbst durchführen kann. Daher wird das Steuersignal durch den sogenannten CLS-Kanal getunnelt.[110] Die Steuerbox wird ebenfalls durch das Forum Netztechnik/Netzbetrieb im Verband der Elektrotechnik, Elektronik und Informationstechnik **(VDE/FNN)**

104 BSI 2018, S. 54.

105 BBK/BSI 2019.

106 BSIG § 8a (2).

107 BDEW 2019 als branchenspezifischer Sicherheitsstandard.

108 www.regelleistung.net

109 Rosinger/Uslar 2017.

110 Ein großer Teil der Windanlagen und vieler weiterer dezentraler Energieanlagen wird heute jedoch über Fernwirktechnik oder das Internet angesteuert.

standardisiert. Die Wichtigkeit dieser gesetzlichen und regulatorischen Setzungen auch für die Resilienz wird deutlich, wenn man sich vorstellt, dass irgendwann Leistungsmengen über diese Steuerboxen (oder Nachfolgetechnologien) angesprochen werden könnten, die die heutige Gesamtleistung aller Kraftwerke um ein Vielfaches übertreffen: Auf der Seite der Einspeisung scheinen etwa über 200 Gigawatt Wind und PV[111], zusätzlich 40 Gigawatt[112] an kleinen Hausspeichern, auf der Seite der Lasten allein schon über 200 Gigawatt[113] an Ladeleistung der Elektrofahrzeuge realistisch. Das **Monitoring** mit dem Ziel, Verbesserungspotenzial zu ermitteln oder Schwächen zu beheben, ist ebenfalls im EnWG geregelt. Monitoringberichte sind insbesondere von den Netzbetreibern für die Netzausbauplanung zu erstellen (unter anderem §§ 12a, 12b, 14 Absatz 1a). Die Berichte gehen überwiegend an die BNetzA, in Teilen auch an das verantwortliche Ministerium. Das BMWi führt fortlaufend ein Monitoring der jetzigen und zukünftigen Versorgungssicherheit durch (§ 51 Monitoring der Versorgungssicherheit). Zusätzlich regelt das BSI-Gesetz das Berichtswesen (§ 8a (3)) zur IKT der Betreiber kritischer Infrastrukturen. Auch die EU sieht dem EnWG analoge Berichtspflichten für die ÜNB vor. ENTSO-E erstellt aus den Berichten der ÜNB zusammenfassende Berichte für die Europäische Kommission.

Die große Sicherheit des Energiesystems entspringt also einer intensiven Zusammenarbeit, geteilten Verantwortungen und Regelungen der Vorbereitung, des Betriebs, des Monitorings und des Verbesserns, die über Jahrzehnte immer wieder weiterentwickelt wurden, um der steigenden Komplexität und dem Wandel im Energiesystem gerecht zu werden.

Kritische Infrastruktur elektrische Energieversorgung

Die Versorgung mit elektrischer Energie ist eine **kritische Dienstleistung**. Dementsprechend definiert die Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (**BSI-Kritisverordnung** – BSI-KritisV), was unter den Begriff **kritische Infrastruktur** fällt.[114] Dazu wird berechnet, welche Nettoleistung zu einem Stromausfall führt, der mindestens 500.000 Personen betrifft. Die folgenden konkreten Anlagentypen werden demnach als kritische Infrastruktur eingestuft:

- **Erzeugungsanlagen** mit einer installierten Nettonennleistung von mehr als 420 Megawatt, dazu zählen: Erzeugungsanlagen, dezentrale Erzeugungsanlagen, Speicheranlagen, Anlage oder System zur Steuerung/Bündelung elektrischer Leistung
- **Übertragungsnetze und Verteilnetze** mit einer entnommenen Jahresarbeit von mehr als 3.700 Gigawattstunden pro Jahr
- Zentrale Anlagen und Systeme für den **Stromhandel**, soweit diese den physischen kurzfristigen Spothandel und das deutsche Marktgebiet betreffen, mit einem Handelsvolumen an der Börse von mehr als 200 Terawattstunden pro Jahr
- **Messstellen**, deren angeschlossene Verbrauchsstelle beziehungsweise Einspeisung eine Leistung von mehr als 420 Megawatt aufweist.

111 Ausfelder et al. 2017.

112 Agora Energiewende 2019.

113 Als konservative Annahme: 10 Millionen Elektrofahrzeuge mit einer Ladeleistung von durchschnittlich (nur) 20 Kilowatt, inklusive der Ladeleistung der öffentlichen Ladeinfrastruktur.

114 Vgl. BSI-KritisV 2017.

Was heißt das genau?

Die folgende Tabelle gibt einige Beispiele, was das für ein zukünftig stark vernetztes Energiesystem bedeutet:

Anlagentyp	Typische installierte Leistung[115]	Anzahl Anlagen, die 420 Megawatt entsprechen	Dies entspricht in etwa:[116]
Dezentrale Erzeugungsanlagen			
Solar (in der Niederspannungsebene)	14,25 Kilowatt	28.000	9,5 Prozent der Anlagen in Baden-Württemberg
Wind an Land (in Hoch- und Höchstspannungsebene)	2 Megawatt	210	13 Prozent der Anlagen in Niedersachsen
Anlagen „hinter dem Zähler“			
Kühlschrank	140 Watt	3.000.000	Alle Haushalte in Berlin und Hamburg zusammen
Wärmepumpe	2 Kilowatt	210.000	9 Prozent der Wohngebäude in Baden-Württemberg (Bundesland mit den meisten Wärmepumpen)
Peer-to-Peer-Märkte am Beispiel des Quartiers Bredburg[117]			
Je Haushalt • Zwei Personen (mit 2.400 Kilowattstunden Jahresverbrauch) • Wärmepumpe	2,5 Kilowatt: • 0,5 Kilowatt • 2 Kilowatt	168.000 Haushalte	1 Prozent der Gemeinden in Deutschland

Tabelle 1: Wie viele dezentrale Anlagen entsprechen zusammengerechnet der Größenordnung einer kritischen Infrastruktur?

Die Beispiele in der obigen Tabelle sind nur eine **grobe Abschätzung** auf Basis der Vorgaben durch die BSI-KritisV. Sie zeigen aber, dass die kritische Masse an elektrischen Anlagen schnell erreicht sein kann. Ab welcher Anzahl an betroffenen Anlagen die Versorgungssicherheit tatsächlich gefährdet ist, hängt von vielerlei Faktoren ab, zum Beispiel dem **Standort der Anlage** und **wie die Anlagen räumlich verteilt sind.** Dies muss im Rahmen der Resilienzmaßnahmen untersucht werden. Gegebenenfalls sind die Mindestgrenzen zur Bestimmung kritischer Infrastrukturen anzupassen. Zudem sollte geprüft werden, ob weitere Akteure berücksichtigt werden müssen (siehe Handlungsoption 4).

115 Eigene Berechnung aus Netztransparenz 2019; BDEW 2017.

116 Eigene Berechnung aus Netztransparenz 2019; Statistisches Amt für Hamburg und Schleswig-Holstein 2020; Statistik Berlin Brandenburg 2020, Statistisches Landesamt Baden-Württemberg 2020.

117 Dieses Quartier besteht unter anderem aus 130 Wohneinheiten mit jeweils einer Wärmepumpe pro Haushalt. Es wird angenommen, dass der Strom über eine Plattform gehandelt wird. Diese Annahmen werden für die Berechnungen zugrunde gelegt. Siehe SmartQuart 2020.

3 Digitalisierung und Energieversorgung

Die Digitalisierung verändert das Energiesystem auf vielfältige Weise. Besonders hervorzuheben ist die kommunikationstechnische Vernetzung, die sowohl innerhalb der Energieversorgung als auch außerhalb stattfindet. Im Stromnetzbetrieb kann die Vernetzung dabei helfen, die vielen verteilten Erzeugungs- und Verbrauchsanlagen zu integrieren. Durch die hohe Vernetzung zwischen einer Vielzahl verschiedenster Komponenten und Akteure entstehen Abhängigkeiten zwischen Strom- und IKT-System, die es vor der Digitalisierung so nicht gab. Aus diesem Grund werden das IKT-System und dessen Akteure wie die Betreiber der öffentlichen Kommunikationsnetze auch für die Resilienz des elektrischen Energiesystems relevant. Außerdem können durch die Digitalisierung der Märkte und Marktabläufe auch Dynamiken entstehen, die Rückwirkungen auf das elektrische Energiesystem haben. Abbildung 6 fasst überblickartig zusammen, welche Vernetzung der Akteure zu erwarten ist und welche digitalen Technologien dabei zum Einsatz kommen werden.

Digitale Technologien werden bereits heute in allen Wertschöpfungsstufen der Energieversorgung eingesetzt und wirken so auf die Stromversorgung ein. Prozesse wie etwa der Kundenwechsel können so effizienter gestaltet, Potenziale aus flexibel steuerbaren Anlagen genutzt und mit der gesteigerten Komplexität in der Energieversorgung umgegangen werden. Innovationen entstehen einerseits aus den konkreten Bedarfen der Energieversorgung („Pull“), andererseits entstehen Innovationsimpulse aus der IKT-Industrie selbst, wie etwa beim Thema künstliche Intelligenz („Push“).[118] Es reicht also nicht, sich bei der Analyse ausschließlich auf Digitalisierungsentwicklungen des Energiesektors zu beschränken: Ein grundlegendes Verständnis der Entwicklungen von digitalen Technologien ist unerlässlich. Neben vielen Vorteilen schafft die Digitalisierung auch neue Vulnerabilitäten. So entstehen neue Risiken, dass die Stromversorgung durch Fehlverhalten von IKT, aber auch gezielte Angriffe von Cyber-Kriminellen beeinträchtigt werden kann.

Der Begriff IKT umfasst alle Technologien (Hardware und Software), Anwendungen und Prozesse, die sich mit der Verarbeitung von Informationen und deren Kommunikation befassen: Informationen in Form von Daten zu erheben, zu verarbeiten, gegebenenfalls zu speichern und zu übertragen, das heißt über ein Kommunikationsmedium zwischen zwei Parteien (Menschen oder Maschinen) zu versenden. IKT bildet damit maßgeblich die Grundlage der Digitalisierung. Auf Hardwareseite umfasst ein IKT-System zum Beispiel Server zur Datenverarbeitung und Router für den Datenverkehr. Softwareseitig gehören dazu zum Beispiel Datenbanken, Algorithmen und Anwendungen für die Aufbereitung und Verarbeitung von Daten sowie Routing-Protokolle

118 Bitkom 2017.

zur Vermittlung von Daten über das Internet. Die beiden Branchen Informationstechnik und Telekommunikation sind zusammengewachsen.[119]

Das IKT-System ist ein komplexes, vielseitiges und sich stetig wandelndes System mit Einfluss auf alle Bereiche unseres heutigen Lebens. Aufgrund ihrer tragenden Rolle für die Gesellschaft zählt auch die IKT zu den kritischen Infrastrukturen. Mehr und mehr Prozesse werden durch IKT überwacht und gesteuert, weswegen andere kritische Infrastrukturen zunehmend abhängig von IKT werden.[120] Dies gilt insbesondere auch für die Energieversorgung (siehe Abschnitt 3.2). Andererseits kann die IKT ohne eine zuverlässige Stromversorgung nicht funktionsfähig sein.

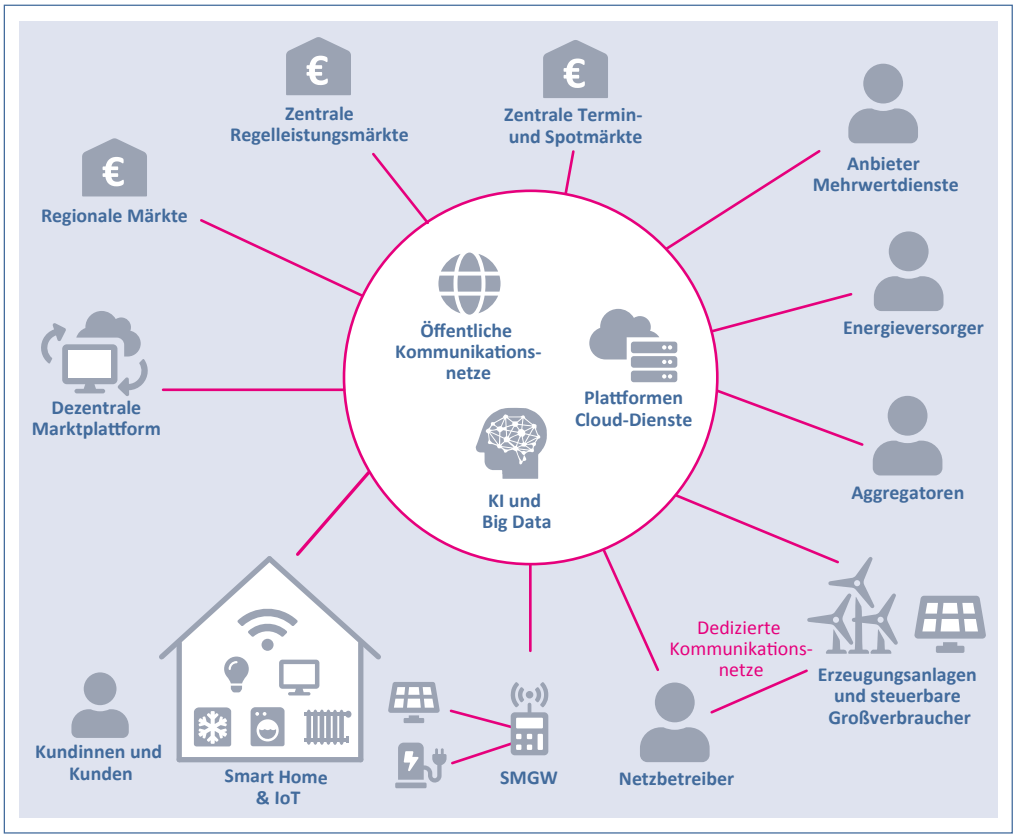


Abbildung 6: Vernetzung im elektrischen Energiesystem – Akteure, Kommunikationsnetze und digitale Technologie

Neben die bereits etablierten Akteure der Stromversorgung treten auch neue Akteure aus dem digitalen Umfeld. Sie waren bisher nicht direkt relevant für die Sicherheit der Stromversorgung, können jedoch in einem digitalisierten elektrischen Energiesystem durch digitale Zugänge systemrelevant werden:

- **IKT-Betreiber**: Betreiber von Kommunikationsnetzen, Rechenzentren, Cloud-Diensten, Plattformen etc., die für die Energieversorgung eingesetzt werden. Insbesondere haben diese Akteure potenziell Zugriff auf Daten von Nutzern oder Prozessen, da sie auf ihrer Infrastruktur gesendet oder gespeichert werden.

- **IKT-Hersteller:** Sie umfassen zum Beispiel Hersteller von IKT-Komponenten,

119 Vgl. BSI 2015, S. 16.
120 Vgl. BBK/BSI 2020.

Ausrüstung und Endgeräte für Kommunikationsnetze. Diese müssen etwa über Softwareupdates einen gewissen Zugriff auf diese Geräte behalten.

- **Drittanbieter**: Dazu zählen etwa Anbieter von Mehrwertdiensten für Smart Meter oder Smart-Home-Lösungen. Diese haben zum Beispiel Zugriff auf Daten von Erzeugungs-, Verbrauchs- oder Speicheranlagen. Gegebenenfalls nutzen sie dafür auch Services von IKT-Betreibern.

Die Digitalisierung ist ein soziotechnischer Transitionsprozess, in dessen Zuge sich nicht nur Technologien verändern, sondern auch die Gesellschaft. Es kommt zu diversen dynamischen Wechselwirkungen zwischen der Entwicklung neuer Technologien und gesellschaftlichen Veränderungsprozessen. So kann der Einsatz digitaler Technologien Veränderungen in der Gesellschaft hervorrufen, zum Beispiel veränderte Verhaltensmuster, wie man besonders deutlich am Umgang mit sozialen Netzwerken erfahren kann. Gleichzeitig kann die Digitalisierung andere technologische und gesellschaftliche Prozesse beschleunigen oder verstärken, wie es etwa für Energiewende und Liberalisierung der Fall ist.

Digitalisierung bedeutet für die Energieversorgung

- unvorhersehbare Entwicklungen wegen der hohen Innovationsgeschwindigkeit der Digitalisierung,
- Konvergenz der IKT-Systeme zur Steuerung energietechnischer Prozesse mit denen der Unterstützung kaufmännischer Prozesse,
- steigende Vernetzung und (steuernde) Interaktionen zwischen den verschiedenen Wertschöpfungsstufen und ihren Akteuren,
- mehr Verfügbarkeit von Daten sowie verbesserte Möglichkeiten zu deren Verarbeitung und Analyse,
- Automatisierung von Verteilnetzen,
- zunehmende Vernetzung von Geräten, die zwar unabhängig vom elektrischen Energiesystem verwendet werden, die aber wegen ihres Energieverbrauchs indirekten Einfluss auf das Energiesystem haben,
- Markteintritt von branchenfremden Drittanbietern, die Zugriff bis auf Anlagenebene haben können,
- Gefahren durch Fehlfunktionen und Angriffe auf die IKT-Systeme.

Digitalisierung ist häufig **monopol- oder oligopolfördernd**. Dafür gibt es mehrere Gründe. Netzwerkeffekte spielen besonders für Plattformen mit vielen Nutzern eine Rolle. Der Nutzen der Plattform entsteht für die Nutzer durch den Kontakt zu anderen Nutzern und erzeugt so eine starke Kundenbindung. Außerdem wächst der Nutzen einer Plattform superlinear mit der Anzahl der Nutzer, sodass die größte Plattform allein aufgrund der Größe so große Wettbewerbsvorteile hat, dass Wettbewerber kaum nachziehen können. Dieser Effekt wird sich durch verbesserte Datenanalysemethoden noch verstärken, da ein Mehr an Kunden auch ein Mehr an Kundendaten liefert und damit durch verbesserte Informationsgewinnung einen Wettbewerbsvorteil verschafft.[121] Auch Modularität und Komplementarität sorgen für Monopole. Eine IKT-Anwendung benötigt viele weitere Module, zum Beispiel Betriebssysteme, Hardware,

121 Barwise/Watkins 2018.

Netzwerkzugänge und weitere Anwendungen. Dadurch entsteht für Hersteller ein Zwang zu Kompatibilität. Aus Kostengründen wird sich also ein Hersteller auf die für seine Anwendungen komplementären Module stützen, die die größte Durchdringung haben. Diese komplementären Module werden dadurch wieder für die Nutzer wertvoller, da sie mehr Anwendungen unterstützen. Komplementarität wird von Unternehmen auch bewusst genutzt, um Marktanteile zu vergrößern oder zu halten, etwa indem ein eigenes Betriebssystem mit eigenen Anwendungen eng verzahnt wird. Ein weiterer Grund sind sehr geringe Kosten für Software, deren Replizierung im Vergleich zu den übrigen Kosten etwa in Erstellung und Vertrieb unbedeutend ist, da die pro Nutzer zusätzlich benötigten Ressourcen minimal sind. Vergleichbares gilt auch in einigen Bereichen des Hardwaremarkts, da ein großer Teil der Kosten durch die kostspielige Entwicklung (Chip-Entwurf) und den Aufbau der Produktion entsteht.[122]

3.1 Digitalisierungstrends

Generell ist anzumerken, dass genaue Vorhersagen über aufkommende Digitalisierungstechnologien und deren Entwicklung und Etablierung schlicht unmöglich sind. Darüber hinaus ist schwer abschätzbar, mit welcher Geschwindigkeit sich digitale Trends durchsetzen und wie ihre Entfaltung voranschreitet. In jedem Fall wird die Herstellung von digitalen Ressourcen (Rechenleistung, Speicher) stetig günstiger, was die Verbreitung von digitalen Technologien befördert. Außerdem weist die Distribution von Software kaum Grenzkosten auf – ist die Software erst implementiert, kann sie leicht und ohne Mehraufwand über das Internet verteilt werden. Die Durchsetzung digitaler Technologien ist oft dynamischer und schreitet mit einer deutlich höheren Geschwindigkeit voran, als es heutige Regulierungsprozesse abbilden könnten. Einige Technologien und Entwicklungen der Digitalisierung beeinflussen bereits heute oder in Zukunft das elektrische Energiesystem; weitere Technologien werden momentan diskutiert und erprobt. Eine Auswahl relevanter Technologien und Trends wird im Folgenden allgemein vorgestellt. Ihre Anwendungsmöglichkeiten im Energiesystem werden in Abschnitt 3.2 diskutiert.

3.1.1 Kommunikationsinfrastrukturen und -systeme

Einen wesentlichen Teil des IKT-Systems bilden die Kommunikationsinfrastrukturen und -systeme. Telekommunikationsnetze und -technologien sind Grundlage für den Austausch von Informationen und Daten und machen die Digitalisierung erst möglich. Die Übertragungssysteme von Telefonie, Fernsehen und Datendiensten wachsen zu einem gemeinsamen Anschluss-, Übertragungs- und Vermittlungssystem zusammen.[123] In diesem System besteht der gesamte Übertragungsweg aus verschiedenen Übertragungsabschnitten, die sich aus verschiedenen Medien zusammensetzen (leitungsgebunden oder über Funk).

Das **Festnetz** war ursprünglich ein Telefonnetz, da der Hauptanwendungsfall die Übertragung der Sprache war. Es wurde entsprechend erweitert, um auch Breitband-Datenübertragung, das heißt hohe Datenübertragungsraten, zu ermöglichen. Das Festnetz basiert auf Kupfer- und Glasfaserleitungen. „Die zentralen Knotenpunkte sind per Glasfaser vermascht miteinander verbunden. Von den Knotenpunkten verlaufen

122 Jones/Mendelson 2011, van der Aalst et al. 2019.

123 Vgl. Schnabel 2015, S. 11 und S. 15.

Kupferleitungen sternförmig in jedes Haus und in jede Wohnung.“[124] Zunehmend kommen auf der „letzten Meile“ auch Glasfasern zum Einsatz.

Für die **Internetübertragung** über weite Strecken wird ein leistungsfähiges Kernnetz benötigt. Dies wird auch „Backbone“ (englisch für Rückgrat) genannt. Es verbindet lokale Subnetze und kann sich überregional oder sogar global erstrecken. Die Backbone-Netze verschiedener Betreiber sind an zentralen Knoten miteinander verbunden. Diese werden auch als Internet Exchange Points bezeichnet und bestehen aus Schaltschränken, Servern oder kleinen Rechenzentren.[125] Der größte Internetknoten der Welt ist der Deutsche Commercial Internet Exchange (DE-CIX) und liegt in Frankfurt. Die übertragene Datenmenge lag 2018 bei sechs Terabit pro Sekunde – Tendenz steigend. Die Infrastruktur für die Stromversorgung des DE-CIX ist mindestens doppelt ausgelegt. Neben zwei Stromkreisen gibt es auch eine Batterie für die Notstromversorgung.[126]

Auch das **Kabelnetz** besteht wie das Festnetz aus fest installierten Leitungen, ergänzt durch Sattelitenübertragung. Es war ursprünglich für die Übertragung von Fernseh- und Radiosignalen ausgelegt. Das Kabelnetz wurde ausgebaut, um die Übertragung von Daten zu ermöglichen und so die Dienste für Kunden auf Internet und Telefonie zu erweitern. Dazu ist das Kabelnetz an das Internet-Backbone angeschlossen.

Der **Mobilfunk** ermöglicht die Übertragung von Sprache und Daten über Funksignale. Das Mobilfunknetz ist in verschiedene Mobilfunkzellen aufgeteilt, die sich jeweils über mehrere Kilometer erstrecken können. Die Reichweite ist unter anderem abhängig von der eingesetzten Technologie, aber auch von der topologischen Beschaffenheit des Gebiets. Im Zentrum einer Zelle befindet sich die Basisstation, die den Übergang zwischen der leitungsgebundenen zur drahtlosen, funkbasierten Übertragung darstellt. Die Basisstation selbst ist mit dem Internet-Backbone verbunden. Die Übertragungsstrecke zwischen Backbone und Basisstation wird Backhaul (englisch für Rücktransport) genannt und verläuft über eine feste Leitung.

Die Funkübertragung ist in **verschiedene Frequenzbereiche** beziehungsweise Funkbänder unterteilt. Jedes Funkband stellt eine bestimmte Bandbreite (siehe Infobox Abschnitt 3.1 „Eigenschaften von Kommunikationsdiensten“) bereit. Mehrere Funksysteme können also nur dann nebeneinander existieren, wenn alle nur auf der Frequenz oder in dem Frequenzband senden, das ihnen zugeteilt wurde. Zu diesem Zweck werden im Bereich des **öffentlichen Mobilfunks** die Frequenzen zur alleinigen Nutzung den Telekommunikations(TK)-Netzbetreibern zugewiesen.[127] Dies wird über Versteigerungen der Frequenzen durch die BNetzA erreicht. Es gibt aber auch lizenzfreie Frequenzbänder. Diese sind sogenannte Industrial, Scientific and Medical (ISM) Bänder, die entsprechend in der Industrie, Medizin oder Wissenschaft, aber auch im häuslichen Bereich durch zum Beispiel Bluetooth genutzt werden. Diese Frequenzen können insbesondere für IoT-Anwendungen (siehe Abschnitt 3.1.8) interessant sein. Darüber hinaus gibt es den **nichtöffentlichen Mobilfunk** für die Nutzung durch Unternehmen, Behörden und vieles mehr. Entsprechende Nutzungsrechte können bei

124 Schnabel 2015, S. 70.
125 Vgl. BSI 2015, S. 25.
126 Vgl. Top 2018.
127 Vgl. Schnabel 2015.

der BNetzA beantragt werden. Ein Beispiel ist der Frequenzbereich 450 Megahertz. Die momentane Zuteilung der Frequenzen lief im Dezember 2020 aus. Sie sollen bundesweit vorrangig für die Anwendungen kritischer Infrastrukturen zur Verfügung gestellt werden[128] und sind daher für die Energieversorgung besonders interessant. In diesem Zusammenhang wird die Verwendung des Standards CDMA 450[129] diskutiert und geprüft. Der Standard bietet für die Energieversorgung einige Vorteile: Er weist sehr hohe Reichweiten auf und ist daher besonders für ländliche Regionen geeignet. So wird etwa nur ein Zehntel der Funkmaste benötigt, die im öffentlichen 5G-Funknetz (siehe untenstehende Infobox) nötig wären. Eine schwarzfallfeste Kommunikation, das heißt Kommunikation, die über eine eigene, vom Stromnetz unabhängige Stromversorgung - etwa auf Basis von Batterien - für eine bestimmte Zeit auch im Blackout aufrechterhalten werden kann, könnte so deutlich kosteneffizienter gewährleistet werden. Außerdem ist diese Frequenz besonders gut geeignet, um Kellerwände oder Betondecken zu durchdringen.

Generationen des Mobilfunks

Mobilfunktechnologien werden in verschiedene Generationen unterteilt. Jeder Generation werden verschiedene Mobilfunkstandards zugeordnet. Die Generationen unterscheiden sich dabei im Wesentlichen durch ihre technischen Eigenschaften, insbesondere durch die Nutzung verschiedener Frequenzbereiche, die zu höheren Bandbreiten führen. Abbildung 7 zeigt verschiedene Technologien mit den verschiedenen Anwendungsbereichen.

Die sogenannten Netze A-Netz, B-Netz und C-Netz nutzten die analoge Sprachübertragung. Die analogen Mobilfunknetzte A bis C gehören der ersten Generation (1G) an. Sie wurden von digitalen Technologien abgelöst: Das D-Netz schuf eine einheitliche, europäische Lösung für den Mobilfunk.[130] Eine Weiterentwicklung stellt das E-Netz dar, das wiederum in höheren Frequenzbereichen arbeitet. Das D- und das E-Netz gehören der zweiten Generation (2G) an. Sie basieren auf dem Standard Global System for Mobile Communications (GSM) und setzen bereits auf die Digitalisierung der Sprache. Der dritten Generation (3G) wird das Universal Mobile Telecommunications System (UMTS) zugeordnet, der vierten Generation (4G) das Long Term Evolution Advanced (LTE-Advanced).

Die **nächste Generation des Mobilfunks ist 5G** und verspricht viel Potenzial für zahlreiche Anwendungen. Im Juni 2019 wurden die Frequenzbereiche für 5G unter vier Wettbewerbern versteigert (siehe unten). Damit kann der Aufbau der Infrastruktur erfolgen. 5G baut auf der bestehenden LTE-Technologie auf und arbeitet in weitaus höheren Frequenzbereichen als die Vorgänger-Generationen. Damit ist es weniger störanfällig. Darüber hinaus arbeitet 5G effizienter, was zu höheren Übertragungsgeschwindigkeiten und damit zu geringeren Verzögerungen führt. 5G kann deutlich mehr Geräte und Verbindungen gleichzeitig bedienen als 4G.

Aufgrund dieser Eigenschaften ist 5G interessant für eine Vielzahl von Anwendungen, die hohe Bandbreiten und geringe Verzögerungen erfordern, vom autonomen Fahren bis hin zu künstlicher Intelligenz. Außerdem schafft 5G neues Potenzial für IoT-Anwendungen insbesondere im Smart-Home-Bereich (Details siehe Abschnitt 3.2.3). Viele verschiedene Geräte und Verbindungen können gleichzeitig bedient werden und direkt miteinander kommunizieren. Dadurch können Regelungen im Smart Home besser aufeinander abgestimmt und in Echtzeit umgesetzt werden. Die Nutzung der hohen Datenrate ist allerdings nur bei geringen Reichweiten möglich. Dies macht die Verwendung insbesondere im ländlichen Raum schwierig.

128 BNetzA 2017, S. 1

129 „Code Division Multiple Access“ im Frequenzbereich 450 Megahertz.

130 Vgl. Haaß 1997, S. 27.

Zunehmend wird auch der Einsatz von **satellitengestützter Kommunikation** für die Energieversorgung diskutiert[131] und in vielen Anwendungsfeldern erprobt.[132] Satelliten sind Empfangs- und Sendestationen im Weltall, die die Kommunikation zwischen zwei Funkstationen auf der Erde herstellen. Heute umkreisen rund 2.000 Satelliten die Erde, doch wird die Anzahl in den nächsten Jahren deutlich zunehmen – die Satellitenindustrie ist ein hochlukrativer Wachstumsmarkt. So werden inzwischen zu geringen Kosten Kleinstsatelliten mit wenigen Kilogramm Gewicht ins All verbracht. Pro Raketenstart können über hundert Satelliten transportiert werden. Diese sind ausfallsicher, da sie ihre Formation selbstorganisiert ausbilden können. Die Kosten für Kommunikation und terrestrische Kommunikationsgeräte sind bereits heute so günstig, dass etwa der Einsatz in der Windparksteuerung dort in Betracht gezogen wird, wo auch mittelfristig weder leistungsfähige 5G noch breitbandiger Netzausbau zu erwarten ist. Zudem könnten Satelliten zukünftig eine Lösung für redundante, aber auch schwarzfallfeste Kommunikation darstellen, da sie ihren Betrieb unabhängig von einem Stromausfall am Boden fortsetzen können.

Satelliten spielen darüber hinaus noch eine andere wichtige Rolle für das elektrische Energiesystem: Mithilfe von GPS-Signalen lassen sich Uhren extrem genau stellen beziehungsweise synchronisieren. Spezielle Messgeräte (Phasor Measurement Units, PMU) benötigen diese genaue Uhrzeit, damit deren hochaufgelöste Messungen zur Berechnung des dynamischen Netzzustands verwendet werden können. Diese dienen nicht nur als Basis einer besseren Auslastung der Infrastruktur, sondern auch zum Erkennen kritischer Situationen, etwa eines drohenden Blackouts.

Es wird erwartet, dass die für die Endkunden zur Verfügung gestellte Bandbreite sowohl im mobilen wie auch im leitungsgebundenen Internet bei gesteigerter Kommunikationsqualität (etwa verringerte Latenzen) weiterhin exponentiell zunehmen wird.

Durch die stetig wachsende Vernetzung im Energiebereich bestehen in Zukunft **Abhängigkeiten von den Betreibern der IKT-Infrastruktur** und anderen Akteuren, die dieselben Kommunikationsnetze nutzen. Durch die Verlagerung von Anwendungen und Diensten in das Internet findet eine Entkopplung zwischen Übertragung und Anwendungen statt. Folglich sind die Rollen TK-Netzbetreiber und Dienstanbieter (auch Service-Provider) getrennt. Die **Betreiber von Kommunikationsnetzen** sind für den Betrieb der Netze zuständig. Das Festnetz in Deutschland gehört zum großen Teil der Deutschen Telekom. In einigen Regionen gibt es andere TK-Netzbetreiber mit eigenen Netzen. In der Regel wird die Teilnehmeranschlussleistung zum Kunden – die sogenannte letzte Meile – durch die Deutsche Telekom an andere TK-Netzbetreiber vermietet.[133] TK-Netzbetreiber für den Mobilfunk in Deutschland sind derzeit die Firmen T-Mobile, Vodafone, Telefonica Deutschland sowie seit der Versteigerung der 5G-Frequenzen demnächst auch 1&1 Drillisch.

131 Etwa als „Maßnahme 8“ in der „Strategie Intelligente Vernetzung“ der Bundesregierung aus dem Jahr 2015, BMWi 2015.

132 Zum heutigen Stand der in der Energieversorgung verwendeten Kommunikationskanäle siehe Kapitel 3.2.

133 Vgl. Schnabel 2015, S. 70.

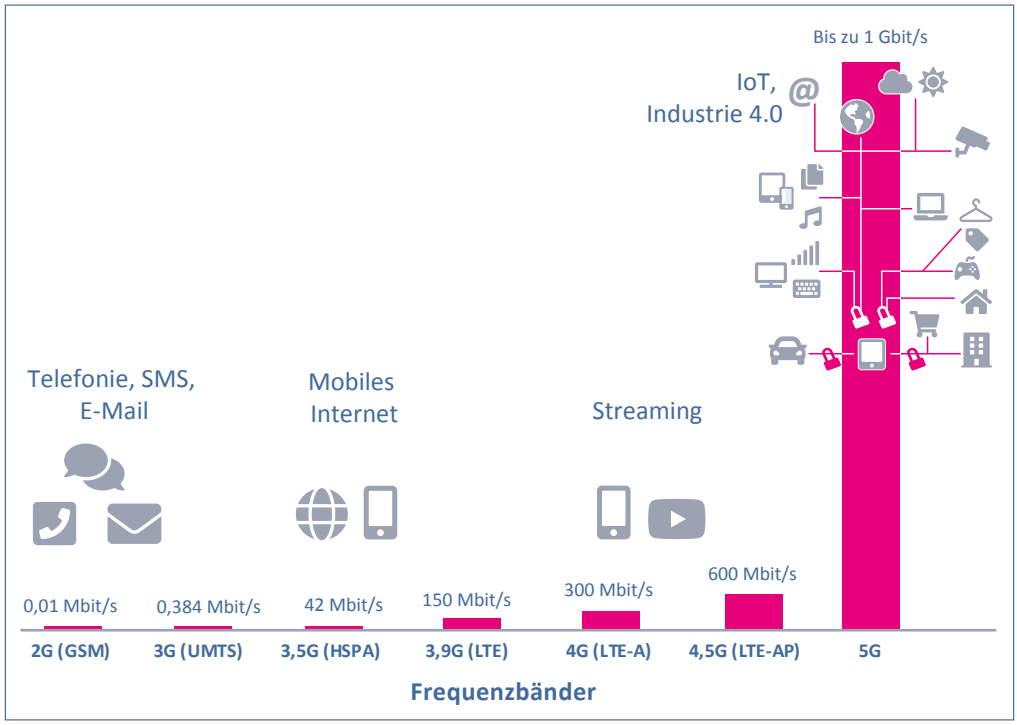


Abbildung 7: Übertragungsraten der verschiedenen Mobilfunktechnologien und ihre Anwendungsbereiche ab der zweiten Generation

TK-Netzbetreiber öffentlicher Netze können bestimmte Bandbreiten vermieten, sodass diese exklusiv von den Kunden genutzt werden können (siehe auch Infobox „Virtualisierung Abschnitt 3.1.6“: Network Slicing). Solche **Vereinbarungen zur Dienstgüte** (auch Quality of Service, siehe auch Infobox „Eigenschaften von Kommunikationsdiensten“) können für Stromnetzbetreiber für deren Netzbetrieb und die Ansteuerung dezentraler Anlagen interessant sein, da so die für diese Anwendungen benötigte kommunikative Anbindung in der nötigen Qualität sichergestellt werden kann. Bislang werden in der Energieversorgung üblicherweise physikalisch getrennte Kommunikationsnetze zur exklusiven Nutzung durch die Stromnetzbetreiber errichtet und durch diese selbst betrieben. Setzen Stromnetzbetreiber zukünftig hingegen auf die Kommunikationsnetze von unabhängigen TK-Netzbetreibern, so geben sie die Verantwortung für die Servicequalität aus der Hand. Ob die tatsächliche Dienstgüte eingehalten wird, können die Stromnetzbetreiber dann technisch nicht mehr selbst beeinflussen. Sie müssen sich dann auf die vertraglich vereinbarten Leistungen unbedingt verlassen können. Unsicherheit über hinreichende Verlässlichkeit steht hier der größeren Flexibilität und den umfangreicheren Ressourcen der TK-Netzbetreiber sowie gegebenenfalls Kostenvorteilen gegenüber.

Service-Provider mit eigener Netzinfrastruktur stellen die Zugänge zum Telefon- und Datennetz bereit. Service-Provider ohne eigene Netzinfrastruktur mieten diese, um über sie ihre Dienste anzubieten. Sie werden dann als sogenannte Reseller bezeichnet. Darüber hinaus gibt es **Knotenbetreiber**, deren Knoten die verschiedenen Telefon- und Datennetze verbinden. Dadurch übernehmen sie eine Schnittstellenfunktion zwischen TK-Netzbetreibern und Service-Providern sowie zwischen den verschiedenen TK-Netzbetreibern selbst.[134] Für den Betrieb von Backbones gibt es verschiedene Festnetz- oder Kabelnetzbetreiber, aber auch Betreiber anderer Branchen wie der Energiebranche. Insbesondere für Energieversorger oder Tochtergesellschaften

134 BSI 2015, S. 29.

Eigenschaften von Kommunikationsdiensten

Kommunikationsinfrastrukturen sind die Grundlage für Vernetzung, Datenaustausch und -verarbeitung, die Bereitstellung von Diensten und vieles mehr. An die unterschiedlichen Dienste werden jeweils spezifische Kommunikationsanforderungen gestellt. Beispielsweise muss ein Videodienst eine höhere Bandbreite zur Verfügung haben als ein Nachrichtendienst. Es gibt eine Reihe von Eigenschaften, die die Leistungsfähigkeit beschreiben. Über diese Eigenschaften können auch Mindestanforderungen seitens der Anwender definiert werden.

Dienstgüte

Die **Dienstgüte**, englisch **Quality of Service** (QoS), beschreibt die Eigenschaften eines Kommunikationsnetzwerks bezüglich der Leistungen, die für einen bestimmten Netzwerkdienst erbracht werden.[135] Dazu zählen unter anderem die folgenden Faktoren:

- Die **Bandbreite** ist die Datenübertragungsrate, das heißt die Menge an Daten, die in einer bestimmten Zeiteinheit übertragen werden können. In der digitalen Vermittlungstechnik entspricht die Bandbreite der möglichen Übertragungsgeschwindigkeit von Daten.
- Der **Durchsatz** bezeichnet die Menge der tatsächlich übertragenen Daten. Oft wird Durchsatz fälschlicherweise mit Bandbreite synonym verwendet.
- Die **Verzögerung** oder Latenz bezeichnet die Zeitdauer zwischen dem Start und dem Abschluss einer Datenübertragung. Die Verzögerung kann stark schwanken, da sie abhängig ist von den Übertragungsmedien, die genutzt werden, aber auch vom Datenverkehr, der Menge an Daten, die gleichzeitig übertragen werden. Die Reihenfolge, in der Daten übertragen werden, hängt ab von dem Übertragungssystem und gegebenenfalls von einer Priorisierung durch die TK-Netzbetreiber.

Die Verantwortung für die Dienstgüte tragen die jeweiligen TK-Netzbetreiber zusammen mit den Service-Providern.

Interoperabilität und Standardisierung

Interoperabilität bezeichnet die Fähigkeit von zwei oder mehr Komponenten oder Systemen, Informationen auszutauschen und diese Informationen auch benutzen zu können.[136] Das heißt, die Komponenten beziehungsweise Systeme sind kompatibel und können zusammenarbeiten.

Um auch herstellerübergreifend Interoperabilität zu gewährleisten, sind **Interoperabilitätsstandards** notwendig. Im technischen Bereich wird dabei unterschieden zwischen De-jure-Standards und De-facto-Standards. **De-jure-Standards** basieren auf einer formellen Rechtsgrundlage. Sie wurden von nationalen oder internationalen Standardisierungsgremien entwickelt und verabschiedet. Von besonderer Bedeutung für den Stromsektor sind etwa die Organisationen „Deutsche Kommission Elektrotechnik Elektronik Informationstechnik“ (DKE) und „International Electrotechnical Commission“ (IEC). **De-facto-Standards** werden auch als Industriestandard bezeichnet. Diese sind von der Industrie geschaffen, weit verbreitet und anerkannt. Solche Standards können durch Standardisierungsgremien auch zu einem De-jure-Standard ernannt werden.

Protokolle sind eine bestimmte Form von Standards und meinen in der Informationstechnik einheitlich definierte Regeln, die festlegen, wie verschiedene Kommunikationspartner untereinander Daten austauschen. Das bekannteste Protokoll stellt das Internetprotokoll dar, auf dem die Kommunikation im Internet basiert.

Für die Standardisierung sind häufig verschiedene nationale und internationale Organisationen und Gremien verantwortlich. Standardisierung ist nicht nur eine Aufgabe in der Kommunikationstechnik, sondern in vielen technischen Bereichen unabdingbar. Standardisierungsprozesse sind in der Regel aufwendig – nicht zuletzt, weil sie einen Konsens vieler Akteure mit verschiedenen Interessen erfordern.

135 Vgl. Meinel/Sack 2009, S. 128.

136 Vgl. IEEE 1991.

können Glasfaserkabel relativ kostengünstig verlegt werden, weil sie in die bestehende Energienetzinfrastruktur integriert werden können – **Stromnetzbetreiber verlegen Kommunikationsleitungen** neben bestehende oder neue Stromleitungen.[137] Darüber hinaus können Stromnetzbetreiber auch auf die Kommunikationstechnologien Power Line Carrier Communication oder einfach Power Line Communication (PLC, englisch für Stromleitungen als Übertragungsmedium) zurückgreifen. So werden bestehende Stromleitungen in den Verteilnetzen auch für die Kommunikation genutzt. Stromnetzbetreibern steht somit ein dezidiert eigenes Kommunikationsnetz zur Verfügung.

3.1.2 Konvergenz von Informationstechnologie und operativer Technologie (IT/OT-Konvergenz)

OT (Operative Technologien oder englisch Operational Technology) bezeichnet Hardware und Software, die für **Überwachung, Betrieb und Steuerung von physischen Komponenten und Geräten** oder technischen Prozessen verwendet wird. OT wird entsprechend oft auch Industrial Control System (ICS) genannt. Besonders bei Einsatz in sicherheitskritischen Systemen (etwa Flugzeugen) oder kritischen Infrastrukturen wie der Energieversorgung werden höchste Anforderungen an die Zuverlässigkeit von OT gestellt. In diesem Kontext kommen oft **eingebettete Systeme** zum Einsatz, das heißt Computersysteme, die direkt an oder in die Geräte integriert sind und überwachende und steuernde Aufgaben übernehmen. OT-Kommunikation findet meist direkt zwischen den Geräten oder zwischen Gerät und zugehörigem Computer statt. OT-Prozesse sind zum Teil stark automatisiert und laufen oft in Echtzeit ab. Direkte Interaktionen mit Menschen finden kaum statt. Der Mensch kann über sogenannte Mensch-Maschine-Schnittstellen (HMI, englisch Human-Machine-Interface) Prozesse einsehen oder auf sie einwirken.

IT (Informationstechnologien oder englisch Information Technology) umfasst die IKT-Infrastruktur für die Abwicklung von **geschäftlichen oder administrativen Prozessen und Transaktionen** wie Rechnungswesen, Vertragswesen oder Kundenmanagement. Es handelt sich bei IT also in der Regel um Server oder Rechner in Unternehmen, die keine direkte Anbindung an technische Geräte haben. IT-Datenverarbeitung und Datenaustausch sind zumeist nicht zeitkritisch. Kleinere Fehler oder Schwächen der Software werden vom Markt akzeptiert, wenn dem ein deutlicher Kundennutzen – etwa durch höhere Effizienz kaufmännischer Prozesse – gegenübersteht. In einigen Teilen der Branche hat sich sogar der Wahlspruch „Move fast and break things“[138] etabliert – eine Philosophie, die den Grundsätzen bei der Entwicklung von OT-Systemen diametral entgegensteht.

Früher war ein direkter Austausch von Informationen zwischen IT und OT nicht möglich – beide Systeme waren physikalisch voneinander getrennt. Dieser sogenannte Air Gap war bis vor einigen Jahren State-of-the-Art, um die OT abzusichern. IT/OT-Konvergenz bedeutet hingegen eine **vermehrte Integration von IT und OT** und die gemeinsame Nutzung von Daten. Durch IT/OT-Konvergenz werden IT-Funktionen in die OT-Systeme eingebunden und umgekehrt. Dies kann Mehrwerte in beiden Bereichen schaffen, wie beispielsweise schnellere Informationsflüsse oder reduzierte Kosten. Zum Beispiel können Daten von OT-Sensoren und OT-Überwachungssystemen

137 Siehe zum Beispiel EnBW 2019.

138 Vardi 2018.

in der IT-Umgebung genutzt werden, um dort betriebliche Entscheidungsprozesse anzustoßen. Neue Methoden der Big Data Analytics und künstlichen Intelligenz spielen dabei eine zunehmende Rolle (siehe Abschnitt 3.1.7 und 3.1.4).

Die Konvergenz von IT und OT findet bereits in vielen Branchen statt – so auch in der Energieversorgung (siehe Abschnitt 3.2). Die Verbindung dieser beiden bisher getrennten Welten muss also sorgfältig gestaltet werden, um mögliche Risiken zu vermeiden.

3.1.3 Cyber-Sicherheit

Aus der Bedeutung der Digitalisierung ergibt sich sofort die Wichtigkeit des Schutzes und der Sicherheit von Daten und Informationen. Zunächst einmal sind Informationen interpretierbare Daten – Daten bekommen erst eine Bedeutung durch ihren Kontext (zum Beispiel Zahlen durch Maßeinheiten). Informationen können in verschiedenen Formen auftreten: gedruckt auf Papier oder elektronisch gespeichert. Sie können auf verschiedenen Wegen, etwa per Post oder elektronisch, übermittelt werden. Insbesondere im Fall der Speicherung, Vermittlung und Verarbeitung personenbezogener Daten werden die Aspekte des Datenschutzes relevant, um die Informationen vor Zugriffen Dritter und Unbefugter zu schützen. Datenschutz ist ein eigenständiges Thema und wird hier nur soweit berücksichtigt, als es für einen resilienten Betrieb relevant ist. Im Falle der Sicherheit wird unterschieden zwischen Informations-, IT- und Cyber-Sicherheit, da jeweils andere Aspekte betrachtet werden müssen und die Schwachstellen unterschiedliche Qualitäten aufweisen können.

Informationssicherheit befasst sich allgemein mit dem Schutz von Informationen und Informationssystemen vor unautorisiertem Zugriff, Nutzung, Offenlegung, Unterbrechung, Änderung oder Zerstörung, um die folgenden drei Schutzziele zu gewährleisten:[139]

- Vertraulichkeit: Aufrechterhaltung autorisierter Zugangs- und Offenlegungsbeschränkungen von Informationen, einschließlich Mittel zum Schutz der Privatsphäre und geschützter Informationen.

- Integrität: Schutz vor unsachgemäßer Änderung oder Zerstörung von Informationen, einschließlich der Gewährleistung der Unleugbarkeit und Authentizität von Informationen.

- Verfügbarkeit: Gewährleistung eines rechtzeitigen und zuverlässigen Zugangs zu Informationen sowie deren Nutzung.

Dies wird auch oft als „CIA-Dreieck“ bezeichnet (von Confidentiality – Vertraulichkeit, Integrity – Integrität, Availability – Verfügbarkeit). Die Priorisierung der Schutzziele ist für IT und OT unterschiedlich. Während in der IT die Prioritäten der Reihenfolge CIA folgen, da Vertraulichkeit am wichtigsten ist, ist bei Systemen, die kritische technische Prozesse steuern (OT), die Reihenfolge AIC, da die Verfügbarkeit am relevantesten ist.

139 Vgl. Nieles et al. 2017, S. 2 f.

Die Sicherheit von Informationen kann durch verschiedene Auslöser bedroht sein:[140]

- vorsätzliche Handlungen wie Schadsoftware oder Abhören von Kommunikation; Akteure, die hierbei eine Rolle spielen, können staatliche Akteure oder Hacker sein,
- höhere Gewalt (zum Beispiel werden durch Feuer Datenträger zerstört),
- Softwarefehler (zum Beispiel missglückte Updates),
- menschliches Versagen (zum Beispiel fehlerhaftes Verhalten aus Unwissen oder versehentliche Weitergabe vertraulicher Informationen).

IT-Sicherheit ist ein Teilbereich der Informationssicherheit, der sich auf den Schutz von elektronisch gespeicherten Informationen und deren Verarbeitung bezieht.

Cyber-Sicherheit (englisch: Cyber Security) befasst sich mit allen Aspekten der Sicherheit in IKT und weitet damit das Spektrum der Informationssicherheit auf den „virtuellen Raum aller weltweit auf Datenebene vernetzten beziehungsweise vernetzbaren informationstechnischen Systeme“[141] aus. Ziel ist es also nicht mehr, nur Informationen zu schützen, sondern auch alle Kommunikations- und Informationssysteme, die an der Verarbeitung und Übertragung dieser Informationen beteiligt sind. Ein besonderer Fokus liegt dabei auf Angriffen über das Internet. Dieser Zugriff kann oft als Einfallstor dienen, um anderweitig – auch physikalisch – Schaden anzurichten. Ein Aspekt von Cyber-Sicherheit ist daher auch der Schutz kritischer Infrastrukturen wie des elektrischen Energiesystems (siehe auch Infobox „Ein paar Worte zum Thema Hacking“). Angriffe auf dieses können zum Beispiel indirekt durch Beeinflussung der Verfügbarkeit von Daten (Denial of Service[142]) oder direkt durch Zugriff auf Software von Leitsystemen[143] erfolgen. Beispielsweise ist ein Trend zu sogenannten Advanced Persistent Threats (englisch für fortgeschrittene, andauernde Bedrohungen) zu beobachten. Hierbei handelt es sich um Cyber-Angriffe auf ausgewählte Einrichtungen, auf deren Netzwerke sich Angreifer dauerhaft Zugriff verschaffen und den Angriff auf weitere Systeme ausweiten. Diese Angriffe sind in der Regel schwer zu erkennen und erfordern einen erheblichen Ressourceneinsatz und technische Fähigkeiten.[144]

Die Nutzung der Begrifflichkeiten ist in der Literatur und in den Medien nicht immer eindeutig – zum Teil werden die Begriffe auch synonym verwendet, und es ist nicht immer klar, welche Aspekte genau gemeint sind. Im Folgenden wird durchgängig der Begriff Cyber-Sicherheit verwendet, der die beiden anderen Konzepte einschließt.

Um mit Gefahren für die Cyber-Sicherheit umzugehen, gibt es verschiedene Möglichkeiten (sogenannte **Mitigation Actions**). Zum einen können technische Maßnahmen ergriffen werden, die zur Realisierung der Schutzziele (Vertraulichkeit, Integrität,

140 Vgl. BSI 2017-1, S. 8.

141 Vgl. BSI 2020-1.

142 Denial of Service bedeutet Dienstverweigerung. Dies kann durch eine Vielzahl gleichzeitiger, gezielt verursachter Anfragen verursacht werden, um ein System gezielt zu überlasten.

143 Die wesentlichen Aufgaben von Leitsystemen sind die Überwachung von Prozessen und Komponenten sowie deren Steuerung mittels sogenannter Fernwirktechnik.

144 BSI 20191.

Verfügbarkeit) führen. Dazu zählen zum Beispiel Verschlüsselungsverfahren, Absicherung der Kommunikationsinfrastruktur durch Firewalls, Zugangsberechtigung zu Systemen, das zeitnahe Durchführen von Sicherheitsupdates und Patches – das heißt die Verbesserung bestehender Versionen, um Softwarefehler oder Sicherheitslücken zu beheben – aber auch Maßnahmen, um mit erfolgreichen Cyber-Attacken umzugehen. Darüber hinaus sind jedoch auch organisatorische Maßnahmen unabdingbar. Hierzu gehören Mitarbeiterschulungen, klare Prozesse für Dokumentation und Datenweitergabe oder die Etablierung eines Risikomanagements.

Für die **kritischen Infrastrukturen der Stromversorgung** gibt es bereits zahlreiche Sicherheitsvorgaben, deren Umsetzung behördlich geprüft wird und die auch permanent weiterentwickelt werden (siehe Abschnitt 2.3).[145] In einer immer stärker vernetzten Welt wird es auch vermehrt Einfallstore und Angriffsflächen geben, die im heutigen elektrischen Energiesystem so noch nicht existieren. Andererseits können die Digitalisierung und die technischen Lösungen, die mit ihr einhergehen, sowohl auf technischer als auch auf organisatorischer Seite unterstützen, die Systeme sicherer zu gestalten.

Trotz aller Maßnahmen, die getroffen werden, um die Cyber-Sicherheit zu erhöhen, wird es immer Sicherheitslücken geben. Neben Privatakteuren, die in der Regel durch finanziellen Gewinn motiviert sind, bereiten sich zunehmend auch Staaten darauf vor, selbst Angriffe durchführen zu können, abzuwehren[146,147] oder auch mit militärischen Maßnahmen auf Cyber-Angriffe zu antworten. So beginnen etwa die USA, Angriffskapazitäten aufzubauen, um in anderen Ländern durch Cyber-Attacken Stromausfälle zu verursachen.[148] Zudem werden massive Cyber-Angriffe unter gewissen Umständen konventionellen physischen, militärischen Angriffen gleichgestellt, sodass zukünftig Cyber-Angriffe auf die USA möglicherweise auch mit konventionellen militärischen Angriffen beantwortet werden.[149] Der britische Geheimdienst glaubt, dass Energieversorger weltweit bereits erfolgreich kompromittiert wurden.[150] Wie wahrscheinlich ein solcher Angriff auf das europäische elektrische Energiesystem zukünftig ist, ist zwar umstritten,[151] doch müssen diese Möglichkeiten nach heutigem Wissensstand in Betracht gezogen und dementsprechend Vorkehrungen getroffen werden.

Zunehmend gibt es staatliche Bestrebungen, die darauf zielen, sich über vermeintlich geheime Zugangswege auf Geräte auch der eigenen Bürgerinnen und Bürger Zugriff verschaffen zu können oder gar die Daten und Software auf den Geräten zu manipulieren oder zu löschen.[152,153] Dies kann zum Beispiel zur Terrorabwehr und/oder Kriminalitätsbekämpfung genutzt werden.[154] Dazu werden entweder Zugänge

145 Dennoch sind Probleme der Cyber-Sicherheit laut ENTSO-E höchste Priorität bei zukünftigen Network Codes, ENTSO-E 2020.

146 Tagesspiegel 2019.

147 The Economist 2019-1.

148 Congress Gov 2018 und Sanger/Perlroth 2019.

149 Chesney 2020.

150 Hern 2017.

151 Rid 2012 oder als Gegenposition McGraw 2013.

152 Biselli 2020.

153 Ein Überblick für die EU-Staaten findet sich unter Gutheil et al. 2017.

154 In Deutschland bekannt wurden besonders die vom BKA eingesetzten „Staatstrojaner", insbesondere die kommerziell vertriebene Software FinFisher/FinSpy des deutsch-britischen Entwicklers Elaman/Gamma und die Eigenentwicklung „Remote Communication Interception Software" (RCIS).

absichtlich aufgrund staatlicher Aufforderung eingebaut[155,156] oder vorhandene Sicherheitslücken genutzt und Softwarewerkzeuge entwickelt, um diese Sicherheitslücken auszunutzen. Diese Sicherheitslücken werden daher nicht den Herstellern der Software mitgeteilt, damit sie weiterhin von staatlichen Stellen genutzt werden können. Sowohl Softwarewerkzeuge als auch das Wissen über Sicherheitslücken können jedoch auch in die Hände von Dritten gelangen und so für bösartige Zwecke, etwa den Angriff auf Infrastrukturen, genutzt werden.[157] Es hat sich inzwischen ein spezialisierter Markt für Produkte und Services rund um das Thema Cyber-Angriffe entwickelt.[158,159] Als zusätzliche Gefahr gilt „Cyber-Warfare“: Staaten entwickeln Kapazitäten, um per Hacking die IKT-Systeme einer anderen Nation empfindlich zu stören.

Die Professionalisierung und Kommerzialisierung von Angriffen auf IKT-Systeme sowie die dafür aufgewendeten Ressourcen werden sich in den nächsten Jahren voraussichtlich noch deutlich verstärken.

Ein paar Worte zum Thema Hacking

Spätestens der Technikthriller „BLACKOUT – morgen ist es zu spät“ von Marc Elsberg aus dem Jahr 2012 lenkte die öffentliche Aufmerksamkeit auf die Gefahr eines durch Hacking verursachten großen Stromausfalls. Tatsächlich ist der Roman gut recherchiert und beschreibt (mit den notwendigen künstlerischen Freiheiten) anschaulich, wie die Folgen eines solchen Szenarios sein könnten, und auch, welche softwarebasierten Elemente im Energiesystem gegebenenfalls angreifbar sind. Am 23. Dezember 2015 wurde dann ein Teil dieses Szenarios Realität: Nachdem die IT/OT-Systeme mehrerer Stromnetze in der Ukraine über viele Monate, vermutlich von Russland aus, infiltriert und ausgespäht wurden, wurde an diesem Tag die Stromversorgung mehrere Stunden lang für Hunderttausende Endkunden unterbrochen.[160] Sehr präsent in den Medien war auch der Angriff durch die Schadsoftware „Stuxnet“ 2009/2010, die gezielt für einen Angriff auf die Steuerung bestimmter Geräte entwickelt wurde, um diese mechanisch zu zerstören. Obwohl vermutlich viele Millionen Rechner mit der Schadsoftware infiltriert waren, war das Verhalten so spezifisch, dass es nur an den iranischen Anlagen zu Schäden kam.[161]

Die anschließenden Analysen zeigten, dass es für solche Angriffe eines erheblichen technischen Aufwands und hochspezialisierter Teams bedarf. Zwar lassen sich die Stromnetze gegen einen aufwendigen Angriff dieser Art nicht vollständig schützen, jedoch kann die Wahrscheinlichkeit eines solchen schwerwiegenden Cyber-Angriffs verringert werden:

- Durch ausreichende Security-Vorkehrungen lassen sich die Kosten für einen Angreifer auf ein Niveau steigern, das die Kosten für einen „konventionellen“ kriminellen oder terroristischen Angriff (etwa mechanische Zerstörung von wenigen Komponenten des Übertragungsnetzes) auf das Stromnetz deutlich übersteigt.
- Politische Konflikte, die zu solch einem massierten Cyber-Angriff führen könnten, haben große Vorlaufzeiten, sodass viele Maßnahmen möglich sind, um die Wahrscheinlichkeit eines solchen Ereignisses zu verringern.

155 Beuth 2019.

156 Etwa im Referentenentwurf des Bundesministeriums des Innern zum Bundesverfassungsschutzgesetz (BVerfschG), § 2 Absatz 1a Satz 1 Nummer 4 in Kombination mit § 11 Absatz 1a , vom 13.06.2020.

157 Loleski 2018.

158 Für ein Beispiel vgl. Brühl et al. 2019.

159 The Economist 2019-2.

160 Vgl. Liang et al. 2017 und Whitehead et al. 2017.

161 Vgl. Langner 2011.

3.1.4 Künstliche Intelligenz

Künstliche Intelligenz beschreibt Technologien, die basierend auf Computerprogrammen in irgendeiner Form intelligent Informationen aufnehmen und erkennen, diese verarbeiten und schlussfolgern und darauf aufbauend adäquat handeln.[162,163] Als ein wesentlicher Aspekt der künstlichen Intelligenz werden oft sogenannte intelligente Agenten gesehen; als Teilgebiet zählen aber auch Verfahren des maschinellen Lernens dazu.

Intelligente **Agenten** können Informationen ihrer Umgebung durch Sensoren wahrnehmen und über Aktoren Handlungen ausführen und damit wiederum auf ihre Umgebung einwirken.[164] Ein wesentliches Merkmal eines Agenten ist die Autonomie, das heißt die Fähigkeit, ohne menschliche Eingriffe oder Interventionen anderer (technischer) Systeme zu handeln, um ein bestimmtes Ziel zu erreichen. Sie können auf Änderungen in ihrer Umgebung reagieren, aber auch proaktiv Handlungen ausführen und darüber hinaus mit anderen Agenten kommunizieren.[165] Diese soziale Fähigkeit ist wesentlich, damit sich Agenten mit anderen Agenten koordinieren können, um so ein übergeordnetes Ziel zu erreichen. Werden mehrere Agenten zusammengeschlossen, spricht man von einem **Multiagentensystem** (MAS). Durch dieses Zusammenspiel einzelner Agenten kann auch emergentes Verhalten auftreten, das heißt, es können vollkommen neue Effekte entstehen, die aus dem Verhalten der einzelnen Agenten nicht vorhersehbar sind. Eine wesentliche Rolle spielt hierbei auch das maschinelle Lernen, sodass Agenten im laufenden Betrieb auf Basis historischer Daten ihr Wissen erweitern und ihre Entscheidungen und Performanz verbessern können – man spricht auch von **lernenden Systemen**.

Maschinelles Lernen stellt ein Teilgebiet im Bereich der künstlichen Intelligenz dar. Lernen ist dann relevant, wenn beim Design eines Systems nicht vorhersehbar ist, auf welche Situationen das System reagieren können muss. Lernen bezieht sich im Wesentlichen darauf, aus Daten Informationen abzuleiten. Man unterscheidet zwischen verschiedenen Formen des Lernens. Beim überwachten Lernen wird computerbasiert aus bekannten Eingabe- und Ausgabedaten der Zusammenhang zwischen diesen gelernt und durch mathematische Modelle dargestellt. Auf diese Weise ist es möglich, die Ausgaben für neue Eingabewerte vorherzusagen. Zum Beispiel kann auf Basis von vorhandenen handgeschriebenen Ziffern ein Muster gelernt werden, sodass eine neue per Hand geschriebene Ziffer erkannt werden kann. Dazu werden Bilder dieser Ziffern eingescannt und so aufbereitet, dass sie durch ein entsprechendes Computerprogramm verarbeitet werden können. Beim unüberwachten Lernen ist eine konkrete Zuordnung zu Zielwerten (beispielsweise Ziffern) nicht bekannt – diese Zuordnung muss durch das Verfahren selbst gelernt werden. Hierzu zählt die Mustererkennung, eine Methode, bei der in Daten Muster etwa in Form von Ähnlichkeiten, gemeinsamen Eigenschaften oder Trends identifiziert werden. Es gibt auch Mischformen – das semi-überwachte Lernen. Beim sogenannten bestärkenden Lernen (englisch Reinforcement Learning) wird ein Agent über Interaktionen mit der Umwelt durch positive oder negative Belohnungen angelernt.

Maschinelles Lernen ist insbesondere hilfreich, um mit vielen Eingabedaten umzugehen und komplexe Zusammenhänge darzustellen. Allerdings hängt die Güte

162 Vgl. Russel/Norvig 2010, S. 1 ff.
163 dena 2019, S. 16.
164 Vgl. Russel/Norvig 2010, S. 34.
165 Vgl. Wooldridge/Jennings 1995.

des maschinellen Lernens erheblich von den verfügbaren Daten und Informationen ab. Diese sind besonders sensibel, sobald es um personenbezogene Daten geht. Datenschutzaspekte spielen hier eine wesentliche Rolle. Gerade bei Komplexität aufgrund großer Datenmengen können Verfahren des maschinellen Lernens dabei helfen, die Komplexität zu erschließen und zu reduzieren. KI kann dazu eingesetzt werden, Systeme vorhersehbarer und effizienter zu gestalten, zum Beispiel durch die Erkennung von Fehlern und Anomalien, die vorausschauende Wartung von Anlagen oder die Unterstützung von IT-Sicherheit (siehe Abschnitt 3.2 zu Anwendungen in der Energieversorgung).

Darüber hinaus gibt es auch sogenannte Expertensysteme beziehungsweise wissensbasierte Expertensysteme, die Wissen zu einem bestimmten Gebiet repräsentieren, anreichern und daraus automatisch schlussfolgern können.[166] Diese können besonders interessant sein, wenn sie zusammen mit maschinellem Lernen verwendet werden. So können zum Beispiel bestimmte KI-Systeme abschalten oder an Menschen delegieren, falls kritische Situationen auftreten.

Bei stark aus den Mustern fallenden Ereignissen oder sich stark verändernden Systemen kann allerdings auch unangemessenes und eventuell kritisches Verhalten entstehen. Dies könnte zu Unsicherheiten führen. Es kann daher notwendig sein, bestimmte Anforderungen wie etwa die Robustheit solcher KI-Systeme anzulegen.[167] An dieser Stelle ist es auch wichtig, welcher Automatisierungsgrad des KI-Systems vorliegt (siehe Abschnitt 3.1.9). Es wäre etwa denkbar, dass automatisierte KI-Systeme in Extremfällen auf niedrigere Automatisierungsgrade „zurückschalten“ oder an Expertensysteme „abgeben“ (siehe oben). Es könnte auch problematisch sein, wenn Resultate oder Entscheidungen von KI-Systemen nicht nachvollziehbar sind. Dies würde bedeuten, dass an die KI-Systeme bestimmte Anforderungen der Transparenz und Nachvollziehbarkeit gestellt werden müssten.[168]

Künstliche Intelligenz wird in vielen Anwendungsbereichen höchst erfolgreich eingesetzt und hat nach Einschätzung der meisten Expertinnen und Experten weiterhin eine steile Wachstumskurve vor sich. Doch lassen einige Innovationen wie selbstfahrende Fahrzeuge länger auf sich warten als noch vor wenigen Jahren angenommen.

3.1.5 Digitale Plattformen

Eine digitale Plattform ist eine einheitliche Softwaregrundlage,[169] in die Dritte eigene Komponenten und Anwendungen einbringen können. Dazu zählt zum Beispiel das Betriebssystem eines Computers, Smartphones oder Smart TVs, auf dem Anwendungsprogramme beziehungsweise Apps auch von dritten Anbietern laufen können. Digitale Plattformen sind aber auch Intermediäre, die auf Basis digitaler Technologien zwei oder mehr Marktteilnehmer verbinden.[170] Die Plattformbetreiber müssen die angebotenen Assets selbst nicht besitzen, sondern nehmen eine vermittelnde Rolle ein und stellen die Infrastruktur bereit. Der Datenaustauch zwischen den Nutzern der Plattform findet direkt über die Plattform selbst statt.

166 Vgl. Plattform Lernende Systeme 2020.

167 Vgl. Heesen et al. 2020, S. 6 und 12.

168 Vgl. Kersting/Tresp 2019, S. 11 f.

169 Es gibt auch Hardwareplattformen, auf denen Software und Anwendungen ausgeführt werden. Diese sind für die vorliegende Analyse jedoch nachrangig.

170 Vgl. BDI 2019, S. 6.

Verschiedene Arten von Plattformen umfassen zum Beispiel soziale **Netzwerke** wie Facebook oder Twitter, **Marktplattformen**, auf denen Verkäufer ihre Produkte oder Dienstleistungen den Kunden direkt über die Plattform anbieten können – etwa Amazon, eBay oder Airbnb – und **Industrieplattformen** (oft auch B2B-Plattformen genannt für Business-to-Business, englisch für Unternehmen zu Unternehmen), über die Dienste für Unternehmen an andere Unternehmen bereitgestellt werden. Über Industrieplattformen ist es möglich, dass Funktionen für ein System von verschiedenen Herstellern bereitgestellt werden können und so der Nutzer einer Plattform nicht mehr von einzelnen Herstellern abhängig ist. Dazu müssen den Entwicklern von Anwendungen die Schnittstellen zur Plattform bekannt sein. Schnittstellen legen fest, wie Informationen und Daten zwischen Plattform und Anwendung ausgetauscht werden.

Digitale Plattformen haben sich in den vergangenen Jahren in vielen Branchen zu einem dominierenden Geschäftsmodell entwickelt. Als ein Grund für diesen Erfolg wird der sogenannte **Netzwerkeffekt** gesehen: Nutzer einer Plattform – sowohl Kunden als auch Anbieter – profitieren von der steigenden Anzahl an Nutzern.[171] Je mehr aktive Akteure es auf einer Plattform gibt, desto höher ist der Nutzen für alle Akteure. Auf diese Weise können neue und auch disruptive Geschäftsmodelle entstehen, das heißt, bestehende Geschäftsmodelle werden gegebenenfalls durch digitale Geschäftsmodelle abgelöst, da sie für Kunden und Anbieter einen Mehrwert bieten. Der Trend hin zur sogenannten **Plattformökonomie** beziehungsweise Plattformwirtschaft basierend auf dem Geschäftsmodell der Bereitstellung von Plattformen wird zukünftig – auch im Rahmen der Energieversorgung – bestehen bleiben: „Der Aufbau und die Nutzung von internetbasierten Plattformen zur Bekanntmachung, Bereitstellung und zum Vertrieb energiebezogener Produkte und Dienstleistungen wird einer der Schlüsselfaktoren für das Bestehen in einer digitalen Welt sein.“[172] Auf den Plattformen werden viele Daten und Informationen ausgetauscht, daher spielen hier Datenschutzaspekte eine wesentliche Rolle.

3.1.6 Cloud Computing

Cloud Computing ermöglicht es, jederzeit und überall auf **konfigurierbare Rechenressourcen** zuzugreifen. Diese Ressourcen werden gegebenenfalls mit anderen Nutzern geteilt.[173] Beim Einsatz von Cloud Computing wird die Seite der Anwendungen und Dienstleistungen getrennt von der Infrastruktur. Dies führt dazu, dass sich der Nutzer von Cloud-Diensten nicht mit den technischen Aspekten auseinandersetzen muss. Auch können IT-Ressourcen flexibler und dynamischer genutzt werden. Um dies zu erreichen, wird die Methode der sogenannten Virtualisierung (siehe Infobox „Virtualisierung“) eingesetzt.

Für Cloud-Dienste werden **verschiedene Diensttypen** unterschieden.[174] Sie reichen von der Bereitstellung virtueller Hardware oder Infrastruktur wie Speicherplatz, Rechenleistung oder Netzwerkbandbreite über die Bereitstellung von zugehörigen Plattformen, um Anwendungen unter eigener Kontrolle auf Cloud-Infrastrukturen bereitstellen zu können, bis hin zu vollständigen Anwendungen, die auf Cloud-Infrastrukturen betrieben werden und beispielsweise über einen Webbrowser aufrufbar sind. Bei den

171 Vgl. zum Beispiel BDEW 2016, S. 32.
172 BBH 2017, S. 28.
173 Vgl. acatech 2014-1, S. 14.
174 Vgl. acatech 2014-1, S. 14 f.

letzten beiden Diensttypen muss sich der Anwender nicht um die zugrunde liegende Infrastruktur wie Netzwerk, Server, Betriebssysteme oder Speicher kümmern.

Cloud-Dienste sind eine gute Möglichkeit, Geschäftsmodelle zu realisieren, ohne das nötige technische Wissen und die Ressourcen selbst bereitstellen zu müssen. Dies kann ein Hebel für Innovationen und neue Geschäftsmodelle sein, da sich Cloud-Dienste mit dem Wachsen des Geschäfts schnell anpassen lassen. Allerdings machen sich die Dienstnehmer auch ein Stück weit abhängig von den Dienstleistern, die die Cloud-Dienste bereitstellen. Dies kann insbesondere bei sensiblen oder kritischen Services problematisch sein.

Virtualisierung

Virtualisierung bezeichnet eine Methode aus der Informatik, mit der IT-Ressourcen und Anwendungen voneinander abstrahiert werden. Das bedeutet, die Anwendungen werden von den IT-Ressourcen getrennt – beispielsweise müssen Programme nicht mehr auf bestimmten Rechnern laufen. Zu den IT-Ressourcen, die virtualisiert werden können, zählen unter anderem Hardware wie Server oder Speicher, Software wie Betriebssysteme oder Applikationen, aber auch Netzwerkkomponenten wie Kommunikationsleitungen. Durch die Virtualisierung können die Ressourcen flexibel zusammengefasst oder aufgeteilt und so besser ausgenutzt werden. Für die Anwender unterscheidet sich in der Nutzung nichts – die virtuellen Ressourcen verhalten sich nach außen wie die physikalischen Komponenten.

Beispiele für Virtualisierung, die bereits gängige Praxis sind:

- **Servervirtualisierung:** Dienste müssen nicht mehr auf bestimmten Servern ausgeführt werden. Sie können auf verschiedenen Servern betrieben werden, was es erlaubt, Dienste auch bei Ausfall von Servern weiterhin bereitzustellen, da diese auf andere Server „verschoben" werden. Zudem können Server besser ausgelastet werden, weil mehrere und auch unterschiedliche Dienste auf ihnen ausgeführt werden können.

- Ein verbreitetes Beispiel für **Netzwerkvirtualisierung** ist **Network Slicing** (englisch etwa für Netzwerkaufteilung). Dabei wird die Kommunikationsinfrastruktur wie Kommunikationsleitungen logisch aufgeteilt, sodass über sie unterschiedliche Dienste laufen können. Insbesondere findet diese Methode Anwendung bei Telekommunikationsanbietern. Sie teilen ihre kabelgebundenen oder drahtlosen Netzwerke auf, um so verschiedene Profile im Hinblick auf zum Beispiel Bandbreite, Verzögerung und Kosten anzubieten und so auf die Anforderungen des Kunden zugeschnittene Lösungen zu ermöglichen.

3.1.7 Big Data und Big Data Analytics

Wie der Name **Big Data** suggeriert, handelt es sich hierbei um eine große Menge an Daten. Jedoch umfasst der Begriff auch die Zusammenfassung, Verarbeitung und Nutzung dieser Daten. Neben der Datenmenge, die insbesondere Einfluss auf die Speicherung und Auswertung von Daten hat, spielt auch die Geschwindigkeit, mit der die Daten anfallen und ausgewertet werden können, eine wesentliche Rolle. Zudem können die Daten aus verschiedenen Quellen anfallen. Diese können gegebenenfalls verschiedene Formate aufweisen (neben Zeitreihen zum Beispiel Emails, Videos, Daten aus sozialen Medien, sozioökonomische Daten).

Für die Umsetzung von Big-Data-Lösungen können Cloud-Dienste genutzt werden. Durch Big-Data-Anwendungen können Daten quasi in Echtzeit ausgewertet werden. Für die Analyse – dies fällt unter den Begriff **Big Data Analytics** – kommen häufig Methoden des maschinellen Lernens zum Einsatz (siehe Abschnitt 3.1.4).

Durch sie können Mehrwerte in den verschiedensten Bereichen wie Betrieb, Organisation oder Vertrieb geschaffen werden.

Im Zusammenhang mit Big Data sind auch Datenschutzaspekte zu berücksichtigen. Auch datenethische Gesichtspunkte werden relevant, um Fragen zu beantworten, für welchen Zweck Daten erhoben und verarbeitet werden, welche Informationen aus den Daten gefiltert werden dürfen und welche rechtlichen Implikationen dies hat.

3.1.8 Internet der Dinge

Der Begriff **Internet der Dinge** (englisch Internet of Things, IoT) bedeutet, dass die Gegenstände/Dinge der physikalischen (oder virtuellen) Welt mit IKT sowie Sensorik und Aktorik ausgestattet und darüber hinaus mit dem Internet oder einem anderen Kommunikationssystem verbunden sind. Auf diese Weise werden die „Dinge" aktive Teilnehmer eines Systems und können Daten bereitstellen, miteinander und der Umgebung kommunizieren, auf Services zugreifen, mit Menschen interagieren oder autonom auf Ereignisse reagieren.

Im Bereich der Logistik oder Produktion gibt es bereits viele Anwendungsfälle wie zum Beispiel zur automatischen Identifikation von Transporteinheiten beziehungsweise Prozessschritten. Weitere Anwendungsbereiche finden sich im Gesundheitswesen, etwa zur Überwachung und Unterstützung von Aktivitäten und Gesundheit von Menschen. Vorteile von IoT sind Effizienzsteigerung, Kostenreduktion, besserer Service, bessere Kundenbindung und -ansprache, neue Geschäftsmodelle und Dienstleistungen. Andererseits gibt es auch eine Reihe an Herausforderungen, unter anderem Fragen des Datenschutzes oder die Abhängigkeit der Technologie von der Stromversorgung.[175] Darüber hinaus besteht eine der größten Herausforderungen für Europa darin, die Souveränität der zugrunde liegenden Kerninfrastruktur, die sensible Informationen berechnet und speichert, zu erhalten und IoT-Geräte vor Missbrauch zu schützen.[176]

IoT bringt eine Reihe digitaler Technologien zusammen. Neue IoT-Architekturen und Plattformen werden sich herausbilden und Technologien wie KI (siehe Abschnitt 3.1.4) sichere Distributed Ledger Technologies (siehe Abschnitt 3.1.10) oder fortschrittliche Kommunikationsnetzwerke integrieren, um neuen Nutzeranforderungen an Leistungsfähigkeit, Servicequalität, Vertrauen und Datenkontrolle gerecht zu werden. Darüber hinaus werden sich isolierte Plattformen hin zu einem Ökosystem verbundener Plattformen entwickeln.[177] In vielen Anwendungen werden zentrale Dienste wie Cloud Computing (siehe Abschnitt 3.1.6) durch verteilte Lösungen wie Edge Computing (siehe unten) basierend auf künstlicher Intelligenz ersetzt oder ergänzt werden.[178] Bei vielen Milliarden IoT-Geräten ist es nicht mehr sinnvoll, die Daten in der Cloud zu speichern, sondern die Datenübertragung zu begrenzen und nur notwendige Informationen in der Cloud abzulegen, um eine unnötige Datenflut zu vermeiden.

IoT kann auch Implikationen für die Gesellschaft haben: Dadurch, dass zum Beispiel Haushaltsgeräte wie Waschmaschinen oder Spülmaschinen zu anderen Zeiten

175 Vgl. Jacoby 2018, Mattern/Flörkemeier 2010.
176 Vgl. Bacquet et al. 2018, S. 10.
177 Vgl. Bacquet et al. 2018, S. 10 ff.
178 Vgl. Vermesan et al. 2018, S. 24.

als bisher genutzt werden, kann sich das Verhalten der Menschen ändern. Dies kann sich wiederum auf die häusliche Arbeitsteilung, Rollenbilder, Familienstrukturen etc. auswirken.

3.1.9 Automatisierung

Automatisierung verfolgt die Absicht, in technischen Systemen durch selbsttätiges beziehungsweise selbstständiges Handeln (Messen, Steuern, Regeln) Ziele zu erreichen, veränderliche Zielen zu folgen, abgeleitete Ziele zu bilden und aufrechtzuerhalten oder Aktivitäten zur Stabilisierung des Systems trotz vorhandener Störungen zu entfalten. Dabei gibt es verschiedene Automatisierungsgrade.[179] In teilautomatisierten oder interaktiven Systemen wird der Mensch mit in die Ableitung von Aktivitäten einbezogen. In hochautomatisierten Systemen wird die Wissensbasis des Systems fortlaufend aktualisiert. Vorgegebene Handlungsabläufe werden automatisch ausgeführt. Der Mensch muss auch hier noch oft miteinbezogen werden. Autonome Systeme sind selbstlernend und kommen weitestgehend ohne menschliches Zutun aus.

Automatisierung ist Voraussetzung für die Optimierung (zum Beispiel Kosten, Ressourcen, Akzeptanz, Umweltwirkung) und wesentlich für eine erfolgreiche digitale Transformation in vielen gesellschaftlichen und wirtschaftlichen Bereichen. Voraussetzung für die Automatisierung von (komplexen) Systemen ist zum einen die möglichst vollständige sensorische Abtastung des Systems sowie zum anderen die Verwendung von Software zur Erstellung wiederholbarer Anweisungen und Prozesse. Durch die zunehmende kommunikative Vernetzung sowie Miniaturisierung von Hardware hat die Automatisierung in den vergangenen Jahren in vielen Domänen erheblich zugenommen. Durch die Verbindung mit übergeordneten Steuersystemen, etwa Supervisory-Control-and-Data-Acquisition-Systemen (siehe auch Abschnitt 3.2.1), und neuen Möglichkeiten der Datenanalyse werden effizientere und sicherere Prozesse ermöglicht oder sogar komplett neu gestaltet – wie etwa im Umfeld Industrie 4.0. Hieraus können auch Datenschutzproblematiken resultieren, wenn Menschen Teil der Umgebung sind und somit auch persönliche Daten oder Daten über ihr Verhalten betroffen sind.

3.1.10 Weitere Trends

Neben den genannten Technologien, die sich bereits in vielen Bereichen etabliert haben, gibt es einige weitere Trends, deren Einsatz perspektivisch auch im Energiesystem denkbar ist und die in Teilen bereits erprobt werden.

Bei der **Distributed-Ledger-Technologie** (DLT, englisch für verteiltes Kontenbuch) handelt es sich um eine dezentrale Datenbank, die auf verschiedene Standorte, Regionen oder Teilnehmer verteilt ist. Im Gegensatz zur klassischen Datenbank gibt es keine zentrale Instanz, sondern jeder Teilnehmer hat seine eigene Instanz und kann die darin enthaltenen Datensätze anzeigen, verändern oder neue hinzufügen. Durch einen Aktualisierungsprozess können alle Teilnehmer ihre lokale Instanz auf den neuesten Stand bringen. Über DLT können insbesondere dynamische Daten wie zum Beispiel Transaktionen erfasst werden. Dabei wird die Historie der Informationen in den Datensätzen überprüft und so verifiziert. Auf diese Weise kann Vertrauen unter den Teilnehmern geschaffen werden, da Manipulationen ersichtlich werden. Über DLT können also insbesondere sogenannte Peer-to-Peer-Transaktionen durchgeführt

179 Vgl. Dumitrescu et al. 2018, S. 9 f.

werden, das heißt Transaktionen direkt zwischen zwei Parteien ohne Intermediär.[180] Aus heutiger Sicht ist noch nicht abzusehen, welche Bedeutung diese Technologie in Zukunft haben wird.

Blockchain ist eine spezielle Art von Distributed Ledger, die besonders dann geeignet ist, wenn sich Teilnehmer nicht vertrauen, aber trotzdem eine Transaktion ohne einen zentralen Akteur (wie etwa eine Bank) durchführen möchten. Bei dieser Umsetzung werden die Transaktionen und auch andere Daten in Blöcken zusammengefasst. Diese Blöcke werden an eine bestehende Kette von Blöcken angehängt. Dabei sind die bestehenden Blöcke bereits verifiziert worden. Für die Aktualisierung und die Verifizierung der Datensätze ist eine hohe Rechenleistung und damit einhergehend ein hoher Stromverbrauch notwendig. Die Kryptowährung Bitcoin, eine Variante der Blockchain-Technologie, verursacht jährlich einen weltweiten Stromverbrauch von knapp 46 Terawattstunden.[181]

Edge Computing: Mit Edge Computing ist die dezentrale Verarbeitung von Daten „am Rande" des Netzwerks gemeint. Edge Computing profitiert besonders von immer kleineren, günstigeren und schnelleren Chips. Es können also Daten lokal erhoben und auch lokal verarbeitet und insbesondere für lokale Steuerungsprozesse verwendet werden. Diese Art der Verarbeitung ermöglicht Reaktionen in quasi Echtzeit und ist ideal für Services, die nur sehr geringe Verzögerungen tolerieren.[182] Für die lokale Verarbeitung von Daten wird eine Vorverarbeitung der Daten notwendig. Dazu kommen Methoden der KI (siehe Abschnitt 3.1.4) infrage. Zum Beispiel können Agenten im Namen von Endnutzern mit den geeigneten Sensoren interagieren und auf Daten zu den aktuellen Aktivitäten des Nutzers zugreifen. In gewissem Maße können diese Agenten autonom und proaktiv handeln für einen nahtlosen Übergang zwischen realer und digitaler Welt.[183] Edge Computing ist also gewissermaßen das Gegenteil von Clouds: wenn die Nutzung von lokaler Rechenleistung wichtiger ist als die Verarbeitung und Speicherung großer Datenmengen.

Quantum Computing: Die meisten der heute gebräuchlichen Verschlüsselungsverfahren beruhen darauf, dass die Zerlegung großer Zahlen in ihre Teiler (Faktorisierung) zu rechenaufwendig ist. Quantencomputer, die für Berechnungen quantenmechanische Phänomene nutzen, sind unter anderem in der Lage, die Faktorisierung um ein Vielfaches schneller als die schnellsten konventionellen Computer auszuführen. Hinreichend leistungsfähige Quantencomputer, die nach sehr optimistischen Schätzungen schon in zehn Jahren einsatzfähig sein könnten,[184] könnten die bisherigen Verschlüsselungsverfahren, die auch in den Stromnetzen eingesetzt werden, unwirksam machen.

180 Vgl. Metzger 2018.
181 Siehe Stolle et al. 2019.
182 Vgl. Vermesan et al. 2018, S. 20.
183 Vgl. Bacquet et al. 2018, S. 12.
184 Ob und wann Quantencomputer marktreif werden, ist nicht seriös zu prognostizieren, Gast 2019.

3.2 Digitalisierung und IKT-Infrastruktur der Stromversorgung

Die Digitalisierung der Stromversorgung erstreckt sich durch alle Wertschöpfungsstufen. Schon früh wurde darauf hingewiesen, dass zur Integration der erneuerbaren Energien besonders zur Koordinierung, Steuerung und Stabilitätssicherung neue Anforderungen entstehen und dafür der Begriff Smart Grids geprägt.[185] Innerhalb von Smart Grids koordinieren sich die Akteure mithilfe der Digitalisierung entlang der Wertschöpfungsstufen.[186] Die Digitalisierung verwirklicht also den Übergang vom klassischen Betrieb des elektrischen Energiesystems hin zum Smart Grid. Tabelle 2 gibt einen beispielhaften Überblick, in welchen Bereichen der Stromversorgung digitale Technologien (siehe Abschnitt 3.1) bereits heute beziehungsweise perspektivisch zum Einsatz kommen.

3.2.1 Erzeugung, Transport und Verteilung

In den Wertschöpfungsstufen Erzeugung, Transport und Verteilung kommen sogenannte SCADA-Systeme zum Einsatz. SCADA steht dabei für Supervisory-Control-and-Data-Acquisition, englisch für überwachende Kontrolle und Datenerfassung. SCADA-Systeme werden in verschiedenen Branchen eingesetzt. Der Begriff wird häufig verwendet, wenn sich das zu kontrollierende System weiträumig erstreckt – so wie das Energieversorgungssystem. **SCADA-Systeme** haben zwei wesentliche Aufgaben: **Überwachung von Prozessen oder Komponenten und deren Steuerung** mittels sogenannter Fernwirktechnik. SCADA-Systeme bestehen aus Remote Terminal Units (RTU, englisch für Fernsteuerungseinheit) oder Intelligent Electronic Devices (IED, englisch für intelligente elektronische Geräte), einem Kommunikationssystem, einer Masterstation und einer Mensch-Maschine-Schnittstelle (HMI, englisch Human-Machine-Interface),[187] wie in Abbildung 8 schematisch gezeigt. Die wesentliche Aufgabe von RTU beziehungsweise IED ist es, die Daten von Geräten im Feld zu sammeln und Steuersignale an die Geräte zu geben. IED sind moderner und leistungsfähiger als RTU, weswegen sie diese zunehmend ersetzen. Masterstationen sind in der Regel Leitwarten, die jedoch unterschiedlich groß sein können, da sie unterschiedlich große Netzbereiche wie zum Beispiel Verteil- oder Transportnetze oder unterschiedlich große Anlagenpools überwachen. Leitwarten unterstützen den Betreiber, den Zustand des Systems zu überprüfen und bei Bedarf Steuerungen vorzunehmen. Das Kommunikationssystem kann sowohl aus kabelgebundenen als auch aus drahtlosen Medien bestehen; es kommen auch vermehrt Internettechnologien zum Einsatz. Im Fall der Netzbetreiber können die Komponenten des Kommunikationssystems dem Netzbetreiber selbst gehören oder gemietet sein. Während die Anlagen heutzutage oft noch über ein dediziertes Kommunikationsnetz angesteuert werden, müssen in Zukunft aufgrund der räumlichen Verbreitung und Anzahl der Komponenten auch öffentliche Kommunikationsnetze zusätzlich miteinbezogen werden.

185 European Commission 2006.

186 Vgl. IEA 2011, S. 6.

187 Vgl. Thomas/McDonald 2015, S. 23.

Wertschöpfungsstufen	Digitale Technologie	Beispiele für Anwendungen im Energiekontext
Erzeugung, Transport, Verteilung		• Dezentral gesteuertes virtuelles Kraftwerk • Prognose: Erzeugung und Verbrauch • Predictive Maintenance • Anomalie-Erkennung • Angriffserkennung • Digitaler Zwilling • Beobachtbarkeit, Steuerbarkeit und Automatisierung
		• Industrieplattformen basierend auf Open-Source-Standards
		• Zentrales virtuelles Kraftwerk
		• Edge Computing
Messwesen		• Erfassen und Verarbeiten von Messdaten etwa für Mehrwertdienste
Handel		• Marktprognosen • Automatisierter Handel
		• Zentrale Marktplattformen • Peer-to-Peer-Märkte für lokalen Energiehandel
		• Blockchain
Vertrieb und Kunden		• Analysen von Verbrauchsverhalten für personalisierte Produkte
Cloud-Dienste		• White-Label-Plattformen • Vermarktungsplattformen als beidseitige Schnittstelle zwischen Kunden und Energieversorger • Soziale Netzwerke
		• Smart Home, Smart Facility, Smart City

 Agenten
 Big Data
 Cloud-Dienste
 IoT
 Maschinelles Lernen
 Plattformen
 Weitere Trends

Tabelle 2: Anwendung digitaler Technologien in der Stromversorgung (Beispiele)

In der Energieversorgung finden die Veränderungen durch die Automatisierung (siehe Abschnitt 3.1.9) ganz wesentlich im Verteilnetz statt. Während dort bislang nur sehr wenig kommunikativ angebundene Aktorik und Sensorik installiert wurde – in der Regel ohne Vorverarbeitung und -auswertung (lokale Intelligenz) –, ändert sich dies bereits heute. In den nächsten Jahren werden weitere umfangreiche Investitionen vorgenommen, unter anderem um (teil-)autonome Reaktionen von Komponenten zu ermöglichen. So werden beispielsweise Umspannwerke durch dezentral vorhandene Intelligenz direkt miteinander kommunizieren, um dann den für das Netz optimalen Schaltzustand umzusetzen. Auch die Regelung von Komponenten wie Transformatoren im Niederspannungsnetz durch eine zentrale Anwendung aufseiten des Netzbetreibers wird zunehmend ermöglicht.

SCADA-Systeme sind Teil der OT-Infrastruktur. Darüber hinaus gehören beispielsweise auch schaltbare Transformatoren, Spannungsregler oder Schalter mit lokaler oder integrierter Regelung zu OT. Im Bereich der Erzeugung sind es die Erzeugungsanlagen selbst sowie ihre internen und externen Regelungssysteme, die Teil der OT sind.

Die Daten aus OT-Systemen können von IT-Seite bei Anlagen- oder Netzbetreibern eingesetzt werden, um Prozesse auf OT-Seite effizienter zu machen. Zwei Beispiele aus dem Jahr 2012 zeigen, dass die IT-/OT-Konvergenz bereits heute Realität ist: Ein Beispiel ist die Verwendung von geografischen Informationen auf IT-Seite, die benutzt werden können, um fehlerhafte Komponenten auf OT-Seite zu lokalisieren.[188] Ein weiteres bereits in der Praxis umgesetztes Beispiel im Bereich Verteilung ist die modellbasierte Spannungsoptimierung.[189] Ein Modell des Systems auf IT-Seite kann mit Daten aus dem Betrieb, also von OT-Seite im Feld, gespeist werden. Mit diesem Modell wird eine optimale Steuerung berechnet, die wiederum an die OT-Geräte übermittelt wird. Für solche und ähnliche Aufgaben können perspektivisch auch sogenannte digitale Zwillinge eingesetzt werden. Der **digitale Zwilling** eines Systems ist eine digitale, modellhafte Abbildung eines Objekts oder Systems der realen Welt. Hierbei handelt es sich um ein detailliertes und dynamisches Modell des Systems, das den Systemzustand sowie dessen Entwicklung über die Zeit simuliert und die Auswirkungen von Schalthandlung vor deren Durchführung simulativ überprüfen kann.

Für die Zukunft wird ein **weiterer Einsatz digitaler Technologien** auf OT-Seite erwartet und daher bereits heute in Forschungs- und Entwicklungsprojekten erforscht und erprobt. Zum Beispiel können Methoden des maschinellen Lernens genutzt werden, um Vorhersagen der Stromerzeugung vorzunehmen. Darüber hinaus kann auch prognostiziert werden, wann verschiedene technische Anlagen gewartet werden müssen – dies fällt unter den Begriff **Predictive Maintenance**[190] (englisch für vorausschauende Instandhaltung). So kann der Wartungsprozess effizienter geplant und überraschende Ausfälle von technischen Anlagen können reduziert werden. Auf ähnliche Weise funktionieren die **Anomalie-Erkennung**[191] (englisch Anomaly

188 Vgl. Taylor 2012, S. 25.
189 Vgl. Taylor 2012, S. 25.
190 Siehe zum Beispiel dena 2019, S. 36.
191 Siehe zum Beispiel Fraunhofer IOSB 2019.

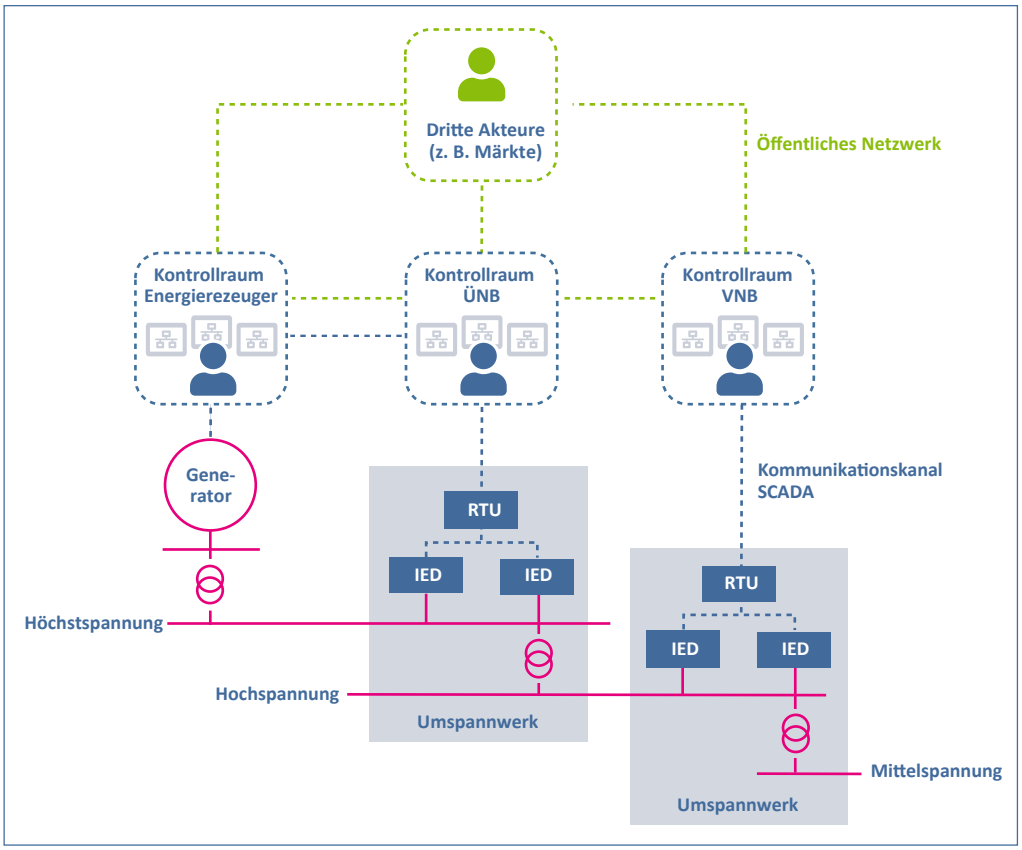


Abbildung 8: Komponenten eines SCADA-Systems[192]

Detection) und die **Angriffserkennung**[193] (englisch Intrusion Detection). Mit der ersten Methode kann durch die Überwachung technischer Daten erkannt werden, wann sich eine Anlage oder ein System unregelmäßig verhält und so Fehlverhalten identifiziert werden. Bei der Angriffserkennung werden Computersysteme oder Netzwerke überwacht, um so auffälligen Datenverkehr – etwa in SCADA-Systemen – zu erkennen. Dadurch können Cyber-Angriffe auf ein System erkannt werden. Hierfür kann auch Edge Computing (siehe Abschnitt 3.1.10) interessant werden, da in diesem Fall die Daten von OT-Geräten lokal verarbeitet werden, bevor sie an die Netzleitwarte kommuniziert werden. Dies verringert die zu übertragenden Datenmengen und den Rechenaufwand in der Netzleitwarte selbst und schafft auch Redundanz.

In fernerer Zukunft sind auch autonome Abwehrsysteme denkbar, die selbstlernend in der Lage sind, komplexe Angriffe zu erkennen und abzuwehren: Das Adversarial Resilience Learning beruht auf Methoden der KI und bedeutet so viel wie **Erlernen resilienter Betriebsführungsstrategien**. Zu diesem Zweck werden zwei Agenten definiert: ein Angreifer-Agent und ein Verteidiger-Agent. Das Ziel des Angreifers ist es, das elektrische Energiesystem zu destabilisieren. Der Verteidiger versucht hingegen, einen stabilen Betriebszustand aufrechtzuerhalten. Er lernt auf Basis der Angriffe, wie er sich in verschiedenen Situationen verhalten kann, und entwickelt dadurch eine resiliente Betriebsstrategie.[194] Die Angriffe müssen dabei nicht realen Ereignissen entsprechen, die tatsächlich passiert sind. Vielmehr können verschiedene denkbare Situationen in Simulationen umgesetzt werden. Je mehr Angriffssituationen „durchgespielt“ werden,

192 Angepasste Darstellung nach Tondel et al. 2018, S. 19.
193 Siehe zum Beispiel Müller-Quade et al. 2019, S. 6 f.
194 Siehe Fischer et al. 2019.

desto besser kann die Strategie des Verteidigers werden. Erste Untersuchungen zeigen, dass der Einsatz dieser Technologie zu Vorteilen für den Verteidiger führt, denn für das Lernen sind umfangreiche Daten und spezifische Systemkenntnisse erforderlich, über die nur der Verteidiger verfügt.[195]

Eine besondere Herausforderung – insbesondere für VNB – wird es zukünftig sein, die vielen **dezentralen Anlagen in ihre Netzsteuerung zu integrieren** und in besonderen Belastungsfällen (automatisiert) zu steuern. Dazu müssen auch kleine Anlagen kommunikationstechnisch in das SCADA-System eingebunden sein. Wie in Abschnitt 3.1.1 erwähnt, können dazu Technologien wie CDMA 450 oder PLC eingesetzt werden.

Für die Realisierung von Anwendungen können Plattformen ein probates Mittel sein. Plattformen auf Basis von Open-Source-Standards werden bereits erprobt. Zum Beispiel wird die Plattform openKonsequenz[196] durch ein Konsortium aus VNB und Entwicklungsunternehmen entwickelt. OpenKonsequenz ist eine **Open-Source-Plattform**, die es ermöglicht, Funktionalitäten für ein Verteilnetzmanagementsystem in Form von Softwaremodulen verschiedener Hersteller standardbasiert zu integrieren. Es wurden bereits Module für das Einspeisemanagement entwickelt und erprobt. Module können sowohl als Open-Source-Software durch das openKonsequenz-Konsortium als auch als Closed-Source-Software von interessierten Herstellern entwickelt und an die Plattform angeschlossen werden.[197]

Neben der kommunikationstechnischen Anbindung müssen viele weitere Aufgaben gelöst werden, etwa die Zusammenfassung der Flexibilitäten der einzelnen Anlagen zu einer Gesamtflexibilität, die automatisierte Ausführung von Funktionen, da eine manuelle Steuerung zu aufwendig werden wird, oder die Einbindung von marktlichen Elementen wie regionalen Systemdienstleistungen. Cloud-Services eignen sich hierzu besonders. Ein Projekt zum Datenaustausch ist etwa CONNECT+,[198] das Datenwege zwischen Netzbetreibern und den Betreibern dezentraler Anlagen definieren will, um die Beseitigung von Netzengpässen ökonomisch effizienter zu ermöglichen.

Des Weiteren treten im Bereich der Erzeugung sogenannte **Aggregatoren** in Erscheinung (siehe Abschnitt 2.1.5). Diese verfügen über eine kommunikationstechnische Verbindung zu den Anlagen in ihrem virtuellen Kraftwerk (siehe Infobox Abschitt 3.2.1) und über ein Leitsystem, mit dem sie die Anlagen steuern können. Dies kann zum Beispiel über Plattformen oder Cloud-Dienste realisiert sein. Darüber können etwa Messdaten von Prosumern erhoben und mit relevanten Partnern Details zum Status der Erzeugung, Netzauslastung und Speicherkapazitäten ausgetauscht werden, um auf Marktpreise oder Engpässe zu reagieren. Die Plattformen oder Cloud-Dienste können wiederum in der Hand von unabhängigen Dienstleistern sein. Für die Erbringung von Regelleistung müssen sie zudem über eine präqualifizierte Kommunikationsverbindung zum ÜNB der jeweiligen Regelzone verfügen.

195 Fischer et al. 2019.
196 https://www.openkonsequenz.de
197 Vgl. Göring et al. 2016.
198 CONNECT+ 2020.

Virtuelles Kraftwerk

Ein Anlagenpool ist ein durch kommunikationstechnische Vernetzung erreichter logischer Zusammenschluss von verschiedenen Erzeugungs-, Verbrauchs- und Speicheranlagen, der den von ihnen erzeugten Strom koordiniert und ins Stromnetz einspeist. Der Anlagenpool wird von einem sogenannten Aggregator betrieben und koordiniert. Werden die Anlagen des Pools gemeinsam vermarktet, spricht man von einem **virtuellen Kraftwerk** (VK). Der Aggregator ist für Aufgaben wie Prognose, Vermarktung und Einsatzplanung der Anlagen verantwortlich.

Durch das Zusammenspiel der Anlagen im VK können Einspeisung und Verbrauch optimiert und so zum Beispiel Schwankungen von erneuerbarer Erzeugung ausgeglichen werden. Zu diesem Zweck verfügt ein VK über ein gemeinsames Leitsystem – wie das folgende Praxisbeispiel zeigt:

Die Einsatzplanung kann automatisch über einen Algorithmus im Leitsystem des VK bestimmt werden. Die Anlagen des VK sind durch eine Fernwirkeinheit in das VK über eine idealerweise gesicherte, jedoch über das Internet laufende Verbindung mit dem Leitsystem verbunden. So können Daten von den Anlagen an das Leitsystem und andererseits Steuerbefehle von der Leitwarte an die Anlage gesendet werden. Hierbei handelt es sich um eine sogenannte Maschine-zu-Maschine-Kommunikation, da sie unabhängig von Menschen besteht.[199]

Wenn die Energie eines VK am Day-Ahead-Markt gehandelt wurde, kann es sein, dass dies aufgrund von Prognoseabweichungen am Tag der Lieferung nicht erfüllt werden kann. Um dies auszugleichen, können entweder die Einsatzplanung innerhalb des VK angepasst oder entsprechend Energiemengen am Intraday-Markt nachgehandelt werden. Aber auch Regelleistungen sind ein bereits in der Praxis realisierter Geschäftsbereich für VK.

Perspektivisch können für den Betrieb virtueller Kraftwerke verteilte, dezentrale Technologien wie **Multiagentensysteme** (siehe Abschnitt 3.1.4) eingesetzt werden. Intelligente Agenten repräsentieren Energieanlagen, die einerseits ihre eigenen lokalen Optimierungsziele verfolgen und sich andererseits mit anderen Agenten koordinieren, um gemeinsam beispielsweise Energieprodukte zu vermarkten.[200] Der Einsatz dieser Technologie würde nicht nur die Automatisierung im Betrieb des elektrischen Energiesystems erhöhen, sondern zu einer autonomen, dezentralen Steuerung führen, sodass kaum noch menschliche Eingriffe und auch kein zentrales Leitsystem mehr nötig wären. Andererseits könnten die einzelnen Entscheidungen der Agenten für ungeschultes Personal oder Anwender schwer nachvollziehbar und intransparent wirken. Zudem könnten unerwünschte emergente Effekte das Systemverhalten komplexer und schwieriger handhabbar machen.

3.2.2 Messwesen

Das Messwesen steht am Anfang einer starken Umwälzung. Werden heute noch die meisten Stromverbräuche in den privaten Haushalten mit dem Ferraris-Zähler, einem elektromechanischen Messgerät, gemessen und jährlich ausgelesen, werden dies in Zukunft elektronische, kommunikativ angebundene Zähler übernehmen: Das Messstellenbetriebsgesetz (MsbG) beziehungsweise Gesetz zur Digitalisierung der Energiewende setzt fest, dass Verbraucher mit einem Jahresverbrauch von mehr als 6.000 Kilowattstunden bis 2028 und Erzeuger mit einer installierten Leistung von mehr als 7 Kilowatt bis 2025 mit intelligenten Messsystemen ausgestattet werden müssen. Die Ausstattung von kleineren Verbrauchern oder Erzeugern ist optional.

199 Vgl. zum Beispiel Quark 2014.

200 Siehe zum Beispiel Hofmann/Sonnenschein 2015, Arbeitspakete 1.2 und 1.4 (S. 51 ff. und S. 69 ff.).

Ein intelligentes Messsystem ist ein digitaler Stromzähler - ein sogenanntes Smart Meter -, der zusätzlich mit einer Kommunikationseinheit ausgestattet ist.[201] Diese Kommunikationseinheit wird als Smart Meter Gateway (SMGW) bezeichnet und stellt die Kommunikationsschnittstelle des intelligenten Messsystems zu verschiedenen anderen Komponenten dar. Zum einen kann der Zähler in das Heimnetzwerk des Kunden eingebunden werden. So können die Zählerdaten, die den Elektrizitätsverbrauch und die Nutzungszeit erfassen, digital ausgelesen werden. Darüber hinaus stellt das SMGW eine Schnittstelle zum steuerbaren lokalen System (CLS, englisch Controllable Local System) auf Kundenseite dar. Die Schnittstelle zum CLS ermöglicht den Fernzugriff auf regelbare Erzeuger wie Solaranlagen oder Blockheizkraftwerke und unterbrechbare Verbrauchseinrichtungen wie Wärmepumpen. Der technische Betrieb des intelligenten Messsystems wird vom sogenannten Smart-Meter-Gateway-Administrator übernommen, der Fernzugriff auf das SMGW hat. Für die Kommunikation über das SMGW schreibt das Messstellenbetriebsgesetz (MsbG) die Erfüllung hoher Sicherheitsstandards vor.[202]

Neben dem SMGW-Administrator wird es **neue Rollen im Messwesen** geben. Der Endkunde kann wählen, welcher Anbieter bei ihm Installationen vornehmen oder den Betrieb von Messsystemen übernehmen darf. So können neue Geschäftsmodelle und Wettbewerber auf den Markt treten, die Zusatzleistungen im Energieumfeld anbieten können. Ein weiterer Kundennutzen soll durch einen neuen Markt für sogenannte **Mehrwertdienste** entstehen. Ein Mehrwertdienst ist eine Dienstleistung, die die Infrastruktur des Smart Meter Gateways benutzt und von Unternehmen angeboten werden kann, die nicht Teil der Energieversorgung sein müssen.[203] Dadurch können zukünftig insbesondere autorisierte Drittanbieter auftreten, um die Zählerinfrastruktur auch für neue Dienste außerhalb der Energiebranche zu nutzen. Beispiele für solche Mehrwertdienste sind die Ansteuerung von steuerbaren Erzeugungs- und Verbrauchsanlagen durch etwa Aggregatoren, die mit dem SMGW verbunden sind, oder auch Services außerhalb der Energieversorgung wie Gesundheitsdienste oder Dienste im Umfeld „Smart Home“. Hierzu werden Technologien aus dem Bereich Big Data eingesetzt werden. Diese Mehrwertdienste hätten auch direkte gesellschaftliche Auswirkungen, da Kunden eine aktivere Rolle in der Energieversorgung bekämen. Allerdings entstehen auch gesellschaftliche Risiken, da Datenschutzaspekte berührt werden. Die vom Kunden autorisierte Auswertung der bei den Dienstleistungen anfallenden Daten heißt nicht unbedingt, dass der Kunde auch versteht, welchen Verwendungen er zugestimmt hat und welches Wissen über ihn aus diesen Daten gewonnen werden kann. Künstliche Intelligenz und Fortschritte der Datenanalyse werden dieses Problem noch verschärfen.[204] Durch solche Eingriffe könnten sich die Menschen verunsichert oder sogar bevormundet fühlen, wenn sie nicht transparent und nachvollziehbar gestaltet werden. Auch wenn diese Aspekte zunächst keinen unmittelbaren Berührungspunkt mit der Versorgungssicherheit haben, entscheiden sie dennoch mit über die Akzeptanz gegenüber der Energiewende und damit auch die zukünftige Energieversorgung insgesamt.

Entsprechend der Standardisierungsstrategie von BMWi und BSI sollen neben Anwendungsfällen zur Messung und Abrechnung des Energieverbrauchs auch

201 BNetzA 2019.

202 Siehe zum Beispiel BSI 2019-2.

203 Vgl. Deutscher Bundestag 2016, § 2, Nummer 9. „Energieversorgungsfremd“ bedeutet jenseits der Belieferung mit Energie.

204 Fredersdorf et al. 2015.

Anwendungsfälle für Einspeise- und Lastmanagement zur netzdienlichen Steuerung sowie zur Integration von Ladesäulen für Elektromobilität identifiziert werden. Erst im Anschluss ist die Weiterentwicklung der Mehrwertdienste vorgesehen.[205]

Die Zähler selbst gehören zu den OT. Über die Schnittstelle des SMGW lassen sich die Messwerte aus dem Smart Meter leicht in die weitere Datenverarbeitung integrieren. So können die Messwerte für Zwecke der Rechnungsstellung durch den Energieversorger schnell und zeitnah erfasst und verarbeitet werden. Diese Daten kann ein Netzbetreiber ebenfalls nutzen, um insbesondere im Verteilnetz den Zustand im Gesamtsystem besser abschätzen zu können – das heißt, Verteilnetze werden besser überwachbar. Darüber hinaus können die Daten für die genannten Mehrwertdienste verwendet werden und sind damit auch in IT-Systeme von dritten Akteuren eingebunden, die sogar zu steuernden Eingriffen auf OT-Seite des Kunden befugt sein können – ein weiteres Beispiel für IT/OT-Konvergenz.

Derzeit verzögert sich der Rollout der Smart Meter, denn die Voraussetzung ist, dass SMGW von mindestens drei voneinander unabhängigen Herstellern durch das BSI zertifiziert wurden[206] und so den Nachweis erbringen, dass sie die Sicherheitsanforderungen erfüllen. Die Zertifizierung umfasst dabei nicht nur die Sicherheit der Kommunikation, sondern auch den Herstellungs- und Entwicklungsprozess der Geräte. Das dritte SMGW konnte erst Ende 2019 zertifiziert werden. Weitere befinden sich noch im Zertifizierungsverfahren. Der nächste Schritt, bevor der Rollout der Smart Meter begonnen werden kann,[207] ist eine Marktanalyse durch das BSI, um die Anforderungen für verschiedene Einsatzbereiche mit den technischen Möglichkeiten zu vergleichen.[208] So kann die wirtschaftliche Vertretbarkeit gezeigt werden. Am 31. Januar 2020 hat das BSI die Marktanalyse aktualisiert und den Verwaltungsakt zur Feststellung der technischen Möglichkeit zum Einbau intelligenter Messsysteme veröffentlicht. Damit konnte der Rollout offiziell beginnen.[209]

Die Verzögerungen im Zertifizierungsprozess haben zu Verunsicherung am Markt und damit zu Schwierigkeiten der Umsetzung der Gateway-Administration und von Mehrwertdiensten geführt.[210] Weitere Verzögerungen sind zu erwarten, da Mehrwertdienste oft mit proprietären Lösungen schneller und preiswerter in den Markt gebracht werden können, was die Wirtschaftlichkeit der Smart-Meter-Infrastruktur weiter schmälert. Zudem ist die Sicherheitszertifizierung der Mehrwertdienste noch ungeklärt, und es fehlen große Marktanbieter, die in diese Mehrwertdienste investieren könnten.[211] Die Verzögerungen können dazu führen, dass Lösungen außerhalb der sicheren Smart-Meter-Infrastruktur entstehen. Das Praxisbeispiel „smart-me“ zeigt, dass bereits Daten aus Stromzählern von Privat- und Industriekunden digital ausgelesen und über das Internet – ohne Verwendung der SMGW-Kommunikation – in Cloud-Diensten bereitgestellt werden.[212]

205 BSI/BMWi 2019.
206 MsbG 2019 § 30.
207 Der freiwillige Einbau zertifizierter Geräte ist bereits jetzt möglich.
208 Vgl. BMWi 2019.
209 BMWi 2020-2.
210 Enkhardt 2019.
211 EY et al. 2019.
212 Vgl. smart-me 2020.

3.2.3 Handel

Die Marktkommunikation für den **Handel an Märkten findet in Echtzeit** statt. Dies gilt sowohl für Terminmärkte als auch für Spotmärkte der EEX und EPEX Spot und Regelleistungsmärkte der ÜNB.[213] In diesen Fällen wird der Handel über eine zentrale Onlineplattform abgewickelt. Dies gilt ebenfalls für regionale Märkte, die sich momentan in Erprobung befinden.[214] Für den OTC-Handel kommen häufig Handelsvermittler, sogenannte Broker, zum Einsatz. In diesem Fall findet der Handel oft über elektronische Brokerplattformen, ebenfalls internetbasiert, statt. Ein direkter Zugriff auf OT wird nicht vorgenommen, da der Handel durch die Handelsakteure getätigt wird und mit zeitlichem Vorlauf zu der Lieferung stattfindet. Trotzdem können durch den elektronischen Handel auch Probleme für die Energieversorgung entstehen. Dies zeigte sich am 7. Juni 2019, als ein fehlerhaftes Datenpaket den Day-Ahead-Handel an der EPEX zum Stillstand brachte, wodurch in der Folge die verschiedenen europäischen Marktbereiche entkoppelt wurden (siehe Abschnitt 2.1.6). Infolgedessen fand der Handel also nicht mehr europaweit, sondern in den einzelnen Ländern statt, was zu großen Preisschwankungen und Ungleichgewichten auf dem Markt führte.[215] Dies könnte umso kritischer werden, je näher der Handelsabschluss an der tatsächlichen Lieferung liegt, wie das etwa bei Intra-Day-Produkten der Fall ist.

Bereits heute wird der Handel häufig automatisiert, mit Unterstützung durch Algorithmen ausgeführt – dies wird Algo Trading genannt. Hier kommt auch KI zum Einsatz, um etwa Marktprognosen zu erstellen, aber auch basierend auf Marktanalysen Geschäfte zu tätigen. Zudem kann KI auch eingesetzt werden, um den Stromhandel am Markt zu überwachen und so Missbrauch zu erkennen.

Viel diskutiert wird, hauptsächlich für den lokalen Energiehandel, der Einsatz der **Blockchain-Technologie** (allgemeiner Distributed-Ledger-Technologien, siehe Abschnitt 3.1.10). Dies bedeutet, dass verschiedene Marktakteure nicht mehr über zentrale Instanzen wie Marktplätze oder Broker, sondern ohne Intermediäre direkt miteinander handeln und dabei das Internet zur Kommunikation nutzen können. Dies wird auch **als Peer-to-Peer-Handel** (englisch etwa für „Handel zwischen Gleichgestellten“) bezeichnet, da damit miteinander agierenden Marktakteuren der direkte Zugang zueinander ermöglicht wird. Die Schnittstelle zwischen den Handelstransaktionen und der physikalischen Lieferung könnten zum Beispiel die intelligenten Messsysteme bereitstellen. So kann sichergestellt werden, dass der tatsächliche Energieverbrauch mit der eingekauften Energiemenge übereinstimmt.[216] Ähnlich wie bei der Steuerung eines VK basieren die Transaktionen auf automatisiert ausgeführten Algorithmen.

3.2.4 Vertrieb und Kunden

Die Bedeutung digitaler Marketing- und Vertriebskanäle nimmt deutlich zu.[217] Es werden vermehrt Services wie Rechnungsdownload oder Tarifwechsel über Kundenportale im Internet bereitgestellt. Darüber hinaus gewinnen **soziale Medien und Industrieplattformen** immer mehr an Bedeutung. Das heißt, dass Produkte von einem

213 Siehe EEX 2019, EPEX SPOT 2019-2 und Regelleistung 2019-1.
214 Hermann et al. 2018.
215 Vgl. ENTSO-E 20193, EPEX SPOT 2020..
216 Vgl. Kreuzburg 2018, S. 4.
217 Vgl. BDEW 2016, S. 24.

Energievertrieb auf Plattformen angeboten werden können, die durch Dritte, gegebenenfalls Branchenfremde, erstellt und betrieben werden. Auf diesen Plattformen können auch Produkte anderer Vertriebe angeboten werden. Auch sogenannte **White-Label-Plattformen** werden von Anbietern genutzt. Das heißt, Plattformdienste werden durch einen erfahrenen Anbieter bereitgestellt, treten aber für den Kunden als Dienst des Energieversorgers auf. Über solche Plattformen können Kunden unter anderem personalisierte Produkte angeboten werden, die auf Basis der Kundendaten mithilfe von KI und Big Data erstellt werden. Produkte umfassen nicht mehr nur klassische Lieferverträge. Zum Beispiel kann dem aktiveren Charakter von Kunden mehr Rechnung getragen werden, indem Plattformen als **digitale Kundenschnittstelle** für den beiderseitigen Informationsaustausch zwischen Versorger und Kunden dienen können. So könnte es beispielsweise über die Plattform ermöglicht werden, dass Kunden eigene Produktlösungen wie Smart-Home-Anwendungen erstellen.[218]

Bereits heute findet auch im häuslichen Bereich vermehrt eine Vernetzung mit dem Internet statt. Dies betrifft Haustechnik wie Licht oder Heizung, Haushaltsgeräte wie Waschmaschinen oder Kühlschränke sowie Unterhaltungselektronik wie Smart TVs. Durch die Vernetzung können automatisierte Abläufe wie das Starten der Geschirrspülmaschine, wenn die Sonne scheint und PV-Strom produziert wird, oder das Betätigen von Rollläden abhängig von der Sonneneinstrahlung stattfinden – so werden Haushalte zum sogenannten **Smart Home**. Es gibt bereits viele Anbieter, die solche smarten Systeme anbieten und somit auf Kundengeräte zugreifen können. Bereits heute ist es möglich, über eine App im Heimnetzwerk oder über das Internet als Anwender auf Geräte wie Heizung, Kühlschrank, Waschmaschine oder Kaffeemaschine zuzugreifen, den Status abzufragen oder die Geräte zu steuern. Zudem werden auch Prozesse im Haushalt automatisiert. Neben der selbstständigen Reaktion von Hausgeräten wie Jalousien, Heizkörpern und Beleuchtung nach den Vorgaben und Bedürfnissen der Bewohnerinnen und Bewohner werden zunehmend auch Multimedia, sogenannte Ambient-Assisted-Living-Anwendungen, für die Erhöhung der Lebensqualität (etwa in der häuslichen Pflege), Sprachsteuerung und weitere Services integriert.

Neben dem Smart-Home-Bereich für Privatkunden werden auch vermehrt Produkte im Bereich Smart Facility (englisch für Einrichtung) für Gewerbekunden, Industriekunden oder öffentliche Einrichtungen sowie Smart City oder Quartierslösungen angeboten. Wie Plattformen in **Quartieren** genutzt werden können, zeigen Projekte wie die Reallabore SmartQuart[219] und Energetisches Nachbarschaftsquartier[220]. Letzteres Quartierskonzept aus etwa 110 Wohneinheiten stellt einen Zusammenschluss aus Erzeugern und Verbrauchern dar mit dem Ziel, den Energiebedarf möglichst aus lokal erzeugter Energie zu decken. Dazu wird eine digitale Plattform entwickelt, die sowohl für den lokalen Energiehandel zwischen Teilnehmenden als auch für das Energiemanagement innerhalb des Quartiers eingesetzt wird.[221] Diese Peer-to-Peer-Plattform ist unabhängig von zentralen Marktplätzen. Es werden hierfür Blockchain-Technologien erprobt (siehe Abschnitt 3.1.10).

218 Vgl. BDEW 2016, S. 62.
219 Vgl. www.smartquart.energy.
220 Vgl. https://www.enaq-fliegerhorst.de/.
221 Vgl. ENaQ 2019.

Durch die Smart-Home-Anwendungen und den flexiblen Einsatz von Verbrauchsgeräten (wie beispielweise das wetterabhängige Einschalten der Geschirrspülmaschine) verändern sich die Verbrauchsprofile von Haushalten. Auch in der Industrie kommt es durch die Digitalisierung zu einer stärkeren Vernetzung von Maschinen und industriellen sowie kaufmännischen Abläufen – auch als **Industrie 4.0** bezeichnet. So können Produktionsprozesse flexibilisiert werden, um den Stromverbrauch – durch die Preise an der Strombörse angereizt – flexibel auf das Dargebot von Wind- und Solarstrom anzupassen.[222] Überdies leistet Digitalisierung auch Beiträge zu einer ressourcenschonenden Produktion.[223] Die Digitalisierung ermöglicht, zukünftig Produktionsprozesse klimaschonend oder sogar klimaneutral zu gestalten. Dazu gehört nicht nur der Ersatz von Erdgas, Erdöl und Kohle durch Erneuerbare Energien, sondern auch teilweise eine völlige Umgestaltung der Produktionsverfahren (beispielsweise Direktreduktion statt Hochofenverfahren in der Stahlerzeugung[224]). Auch hierdurch können sich Verbrauchsmuster ändern.

Diese Entwicklungen bedeuten bedeuten, dass verschiedenste Anlagen und Geräte vernetzt werden und je nach Vertragsdetails direkte Zugriffe auf die OT-Infrastruktur auf Kundenseite wie zum Beispiel regelbare Verbrauchsanlagen wie Wärmpumpen, aber auch Haushaltsgeräte möglich sind. Dieser Zugriff kann zukünftig auch durch dritte Akteure erfolgen. Darüber hinaus können perspektivisch auch Erzeugungs- oder Verbrauchsanlagen von Privat- oder Industriekunden in virtuelle Kraftwerke eingebunden werden, um so die Vermarktung dezentraler Anlagen zu erleichtern. Hier können Smart Meter die Schnittstellen zu den Anlagen darstellen.

3.2.5 Kosten und wirtschaftliches Potenzial der Digitalisierung

Die Digitalisierung des Energiesystems bietet neben technischen Vorteilen auch ein enormes Marktpotenzial – also gute Möglichkeiten für den deutschen Standort. Dabei besteht eine enge Kooperation zwischen Produktion und Forschungsinstitutionen. Laut einer Untersuchung von Bloomberg sind bereits im Jahr 2025 Umsätze in Höhe von 64 Milliarden US-Dollar zu erwarten.[225]

Darüber hinaus birgt die Digitalisierung des Energiesystems umfassende Kosteneinsparungspotenziale im Bereich des Stromverteilnetzausbaus. In Deutschland könnten sich bei konventionellem Ausbau die Investitionen auf der Verteilnetzebene für die EE-Integration im Vergleich von 2012 bis 2032 auf bis zu 49 Milliarden Euro belaufen, wenn die Ziele der Bundesregierung für den Ausbau der erneuerbaren Energien erreicht werden sollen.[226] Bereits siebzig Prozent dieser Investitionen werden bis 2022 erforderlich sein.[227] Diese Kosten werden von den Verbrauchern getragen werden müssen, da die Netzinvestitionen über Netzentgelte finanziert werden. Durch den Einsatz digitaler Technologien in Kombination mit neuen Planungsmethoden können diese Kosten voraussichtlich halbiert werden.

222 Beispiele siehe: Ecofys 2016.
223 Vgl. Plattform Industrie 4.0 2020.
224 Vgl. Agora Energiewende/Wuppertal Institut 2020.
225 Vgl. BNEF 2017.
226 Vgl. dena 2012 und Büchner et al. 2014.
227 Büchner et al. 2014.

4 Basisursachen und Risikofaktoren für große Blackouts

In unserem heutigen elektrischen Energiesystem sind Blackouts selten. Grund dafür ist, dass die Netzbetreiber Störungen durch eine Vielzahl an Maßnahmen verhindern. Zudem verpflichtet ein umfangreiches Regelwerk alle Akteure, zur Störungsfreiheit beziehungsweise zum schnellen Wiederaufbau nach Störungen beizutragen. Die in den Kapitel 2 und 3 beschriebene Umfeld- und Trendanalyse zeigt, dass sich das elektrische Energiesystem massiv wandeln wird. Dadurch wird es in Zukunft schwerer werden, die Versorgungssicherheit mit dem gewohnten Niveau aufrechtzuerhalten. Es ergeben sich neue und auch unvorhersehbare Risiken, die große Blackouts wahrscheinlicher machen können. Insbesondere wegen der Geschwindigkeit, mit der die Digitalisierung voranschreitet, sind viele Entwicklungen nicht vorhersehbar. Anhand der zu beobachtenden und zu erahnenden Entwicklungen durch Energiewende und Digitalisierung hat die Arbeitsgruppe dennoch versucht, zentrale Risikofaktoren für das Energiesystem im Jahr 2040 zu ermitteln. Üblicherweise sind die Zieljahre für die Energiepolitik zwar 2030 und 2050; 2040 wurde jedoch als Zwischenjahr gewählt, um einerseits einen eher langen Zeithorizont zu betrachten, andererseits ist ein Horizont 2050 nicht geeignet, da die Digitalisierung dazu zu unvorhersehbar und zu rasch voranschreitet. Zunächst wurden Zukunftsszenarien für das Jahr 2040 identifiziert, die mögliche unterschiedliche Entwicklungen des zukünftigen Energiesystems darstellen (siehe Anhang 8). Anschließend hat die Arbeitsgruppe untersucht, wie sich durch eine mögliche Änderung von Risikofaktoren die Wahrscheinlichkeit für große Blackouts erhöhen kann und welche Risikofaktoren neu hinzutreten. Es zeigt sich, dass sich die Ursachen für diese Risikofaktoren grob in vier Gruppen einteilen lassen – im Folgenden als Basisursachen bezeichnet.

Diese Basisursachen ergeben sich aus den zukünftigen Entwicklungen, durch die sich die Risikostruktur im Energieversorgungssystem fundamental ändern wird. Diese Darstellung erhebt nicht den Anspruch auf Vollständigkeit, spiegelt aber die Einschätzung der in der AG vertretenen Expertinnen und Experten wider. Die sich aus den vier Basisursachen ergebenden Risikofaktoren kommen zu den bisherigen „konventionellen“ Störursachen hinzu, wie Ausfall von Übertragungsleitungen, menschliches Versagen in der Netzführung oder auch durch den Markt initiierte Störungen. Dazu kommen Ursachen, die nicht aus den absehbaren Trends folgen, weil sie entweder eigenen, noch nicht absehbaren Entwicklungen folgen oder bereits im heutigen System angelegt sind. Diese vier Basisursachen entfalten ihre Wirkung weitgehend *unabhängig* von zukünftigen Entscheidungen der Politik.

4.1 Basisursache 1: Die Vielzahl an kleinen, aktiv steuerbaren Erzeugungs- und Verbrauchsanlagen ist durch die Möglichkeit unerwünschten simultanen Verhaltens systemrelevant

Dezentrale Erzeugungsanlagen sind bereits heute systemrelevant. Für große Aggregatoren gelten daher die KRITIS-Verordnung des Bundesamts für Sicherheit in der Informationstechnik (BSI)[228] und das BSI-Gesetz, das unter anderem den Betreibern kritischer Infrastrukturen das Einhalten von Mindestsicherheitsstandards auferlegt sowie eine Meldepflicht erheblicher IT-Vorfälle vorschreibt. In einer durchgehend digitalisierten Welt werden jedoch auch kleinere Geräte durch ihr potenziell simultanes Verhalten systemrelevant. Dazu zählen das zeitgleiche Abschalten oder Reduzieren von Leistung, aber auch Gleichzeitigkeiten, das heißt die gleichzeitige Nutzung der Netzinfrastruktur durch viele Erzeugungs- oder Verbrauchsanlagen. Mit dem Begriff „Gerät" werden im Folgenden solche elektrischen Verbraucher „hinter dem Zähler", also in den Haushalten, zusammengefasst, die zusammengenommen einen kritischen Einfluss auf den Netzzustand haben könnten. Dies betrifft etwa Geräte wie Wärmepumpen, Hausspeicher, elektrische Heizungen oder weiße Ware, aber auch Elektroautos. Diese werden potenziell in der Lage sein, automatisiert an Märkten teilzunehmen. Dadurch ergibt sich eine große Anzahl sehr kleiner Einzeltransaktionen, die sich zu sehr großen gebündelten Energiemengen aufsummieren. Diese Handelsgeschäfte am Markt können eine eigene Dynamik entfalten, ohne dass Netzbelange berücksichtigt werden. Darüber hinaus kann unkoordiniertes Verhalten – automatisiert oder durch menschliches Handeln, etwa durch Privatpersonen – die Systemstabilität beeinflussen. Beispiele sind das gleichzeitige An- oder Abschalten von Verbrauchsanlagen etwa durch variable Tarife oder wegen Softwareupdates sowie das Laden von Elektrofahrzeugen. Des Weiteren kann unkoordiniertes Verhalten auch nach einem Blackout simultanes Verhalten verursachen und somit das Anfahren des Systems erschweren.

Das Verhalten der kleinen, verteilten Erzeugungsanlagen könnte besonders dann zu Problemen führen, wenn diese keinen hinreichenden Beitrag zur Resilienz des Gesamtsystems leisten – etwa, weil sie nicht ansteuerbar oder technisch nicht in der Lage sind, sich netzdienlich zu verhalten (zum Beispiel einen Beitrag zur Blindleistungsregelung zu erbringen). Die Netzdienlichkeit von Erzeugungsanlagen ist keinesfalls selbstverständlich – die Hersteller optimieren ihren Betrieb nach größtem Ertrag für die Kunden. Innovationen zur Netzstützung werden besonders für kleine Erzeugungsanlagen nicht vom Markt belohnt. Wird netzdienliches Verhalten jedoch nicht gefördert, können sich entsprechende Innovationen nicht entwickeln. Darüber hinaus können Privatpersonen gegenüber technischen Lösungen, die in ihre Entscheidungshoheit eingreifen, skeptisch sein. Dies kann zur Folge haben, dass mögliche stabilisierende Innovationen nicht eingesetzt werden können.

Werden die vielen dezentralen Erzeugungsanlagen zukünftig überwiegend nur von wenigen Unternehmen betrieben beziehungsweise vermarktet, entstehen ebenfalls Risiken: Durch die gebündelte Verwaltung etwa über Cloud-Dienste entstehen zentrale Angriffspunkte für Cyber-Angriffe, und eine Vielzahl von Erzeugungsanlagen kann ungewollt gleichzeitig gesteuert werden.

228 BSI-KRITIS-Verordnung – Verordnung zur Bestimmung kritischer Infrastrukturen nach dem BSI-Gesetz (vgl. BSI-KritisV 2017).

Viele dieser Themen sind in der einen oder anderen Form schon auf dem Radar der Energieversorgung – so werden zum Beispiel Anforderungen an Clouds und deren Sicherheit explizit in den Präqualifikationsbedingungen für Regelleistung beschrieben. Viel weniger im Fokus steht eine Bedrohung, die sich durch Entwicklungen komplett außerhalb des eigentlichen Energiesystems ergeben kann: Zukünftig werden annähernd alle Verbrauchsgeräte in irgendeiner Form mit dem Internet verbunden sein – vom Leuchtmittel bis zum Hausspeicher. Viele werden sogar mit lokaler Rechenleistung versehen sein.[229] Im europäischen Stromnetz wird sich die Anzahl dieser Geräte also auf viele Milliarden belaufen. Ein nicht regulierter und nicht zertifizierter Internetzugang ist ein potenzieller Angriffspunkt. Cyber-Angreifer können durch Ausnutzung von Sicherheitslücken gezielte Cyber-Angriffe (siehe auch Basisursache 2) durchführen, um so Einfluss auf die Leistungsaufnahme oder -abgabe der Geräte zu nehmen. Durch hohe Gleichzeitigkeiten können sie dann die Frequenz so beeinflussen, dass es zum Blackout kommt.

4.2 Basisursache 2: Fehler der IKT können zu massiven Bedrohungen führen

Als Fehlerkategorien in den IKT-Systemen sind hier besonders zwei relevant: Sicherheitslücken, die einen nicht autorisierten Zugriff erlauben, und funktionale Fehler, die dazu führen, dass sich das System in einer Weise verhält, die nicht der Anforderungsspezifikation genügt.[230]

Offensichtlich ist die Bedrohung in Fällen, bei denen die IKT des eigentlichen Energiesystems betroffen ist: Da IKT zunehmend notwendiger und vom physischen System weitgehend untrennbarer Bestandteil des Energiesystems wird – man spricht auch von einem cyber-physischen System –, kann Fehlverhalten oder Ausfall der IKT sowohl einen Blackout auslösen als auch das Wiederanfahren des Systems massiv erschweren.

Ein adäquates Instrumentarium zu entwickeln, um auf die Bedrohungen durch Ausfall oder Fehlverhalten von IKT reagieren zu können, ist besonders herausfordernd, da auch fehlerhafte, kompromittierte oder manipulierte IKT-Systeme nicht abgeschaltet werden dürfen, wenn sie für den Systembetrieb kritisch sind – wie etwa die IT-Systeme zur Überwachung und Steuerung des Netzes. Denn die IKT-basierte Fähigkeit zur Kontrolle des elektrischen Energiesystems und damit die Reaktionsfähigkeit ist jederzeit notwendig, um auf Störereignisse angemessen reagieren zu können. Daher ist die Verfügbarkeit der IKT in der Stromversorgung das am höchsten priorisierte Schutzziel der Informationssicherheit.

Die Resilienzmaßnahmen des elektrischen Energiesystems wurden bislang hauptsächlich auf physikalische Fehlerursachen, zum Beispiel den Ausfall eines großen Kraftwerks, oder eine Überlastung eines Netzelements ausgelegt. Neuartige Störereignisse wie Fehler in der Software oder ein Cyber-Angriff mit dem Ziel, einen großen

229 IBM hat angekündigt, in Kürze einen Computer (!) mit CPU, Kommunikationsanbindung und autarker Energieversorgung auf den Markt zu bringen, der „kleiner als ein Salzkorn“ ist, sich autonom mit Strom über PV versorgt und in der Herstellung nur zehn Cent kostet (vgl. Jones/Wagner 2018).

230 Sicherheitslücken und funktionale Fehler werden hier im weiteren Sinne verstanden: Sicherheitslücken können auch durch Schwächen der betriebsinternen Sicherheitspolitik entstehen.

Blackout herbeizuführen, können das elektrische Energiesystem daher zukünftig vor Herausforderungen stellen, für die es bisher nicht gerüstet ist. Das Störungsbild kann sich von konventionellen Fehlern unterscheiden, oder die Störung kann sogar lange Zeit unbemerkt bleiben. Auf diese Weise könnte nicht nur ein Blackout verursacht, sondern auch das Wiederanfahren des Systems extrem erschwert werden.

Eine Bedrohung kann jedoch zukünftig auch von IKT-Systemen ausgehen, die bisher überhaupt nicht als Bestandteile des Energiesystems gesehen werden und die daher noch nicht auf dem Radar der für Systemsicherheit verantwortlichen Akteure in Betrieb und Regulierung angekommen sind. Dies sind zum einen die in der Basisursache 1 beschriebenen kleinen, kommunikativ angebundenen Geräte, die, sollte eine ausreichend große Anzahl unter Kontrolle eines Angreifers gebracht werden, das elektrische Energiesystem empfindlich stören können. Auch weitere Angriffspunkte außerhalb der Energiesysteme werden möglich.

Die Digitalisierung führt zur Plattformökonomie, das heißt, große Plattformen wirken als Knotenpunkt für viele Geschäftsprozesse. Sind technische Prozesse oder Systeme mit diesen Plattformen verknüpft, etwa die Steuerung von IoT-Geräten, ist die Plattform ein Single Point of Failure.[231] Ein Fehlverhalten dieses Systems hätte weitreichende Konsequenzen für die Funktionalität der verbundenen Geräte. So könnte über einen erfolgreichen Angriff auf die Plattform Schadsoftware in alle angeschlossenen Geräte eingebracht werden. Beispielsweise könnte ein Hersteller weißer Ware[232] alle seine ausgelieferten Geräte an eine zentrale Plattform anschließen, um die Wartung zu verbessern. Gewänne ein Angreifer die Kontrolle über diese Plattform, könnte er die angeschlossenen Geräte zu bösartigem Verhalten motivieren.

Im IKT-Bereich sind sehr kurze Innovationszyklen notwendig, um sich schnell einen Wettbewerbsvorteil zu verschaffen, einen großen Marktanteil oder eine marktdominierende Position zu sichern. Denn der Digitalisierungsmarkt belohnt die schnelle Markteinführung neuer Funktionen. Dies kann zu Kompromissen bei Sicherheitsstandards oder Softwarequalität führen. Entdeckte Fehler und Sicherheitslücken werden dann kontinuierlich erst in späteren Updates behoben. Besonders für Hersteller von IoT-Geräten ist es in der Regel nicht ausreichend lukrativ, in die Sicherheit von Einzelgeräten zu investieren, soweit für den einzelnen Käufer dadurch kein Problem entsteht. Dies vergrößert das Risiko für eine großflächige Kompromittierung der Systeme, bei der Angreifer eine systemkritische Anzahl von Geräten unter ihre Kontrolle bringen und sie so zur Herbeiführung eines Blackouts nutzen. Andererseits führen zu strikte Vorgaben dazu, dass notwendige Innovationen nicht entstehen.

Eine weitere Besonderheit der IKT-Branche hat Einfluss auf die Bedrohungssituation: Die Branche ist aufgrund von Netzwerkeffekten und sehr geringen Grenzkosten in vielen Anwendungsfeldern eine Winner-Takes-it-All-Industrie.[233] Herstellergebundene Software (wie etwa Microsoft Windows, SAP, Android) kann in einigen Märkten schnell zum Standard werden und Alternativen verdrängen. Ähnlich gilt dies auch für Hardware: Prozessoren auf ARM-Architektur laufen im weit überwiegenden Teil der

231 Single Point of Failure bedeutet, dass ein Fehler eines Systembestandteils zu einem Ausfall des Gesamtsystems führen kann.

232 Unter weißer Ware versteht man Haushaltsgeräte wie Kühlschränke oder Geschirrspülmaschinen.

233 London Business School 2020.

Mobiltelefone, PC-CPU werden im Wesentlichen von zwei Herstellern entworfen und gefertigt. Es bilden sich perspektivisch Oligo- oder Monopole. Ein Angreifer kann deshalb in Zukunft unter Ausnutzung derselben Sicherheitslücken in sehr viele Systeme von kleineren VNB eindringen. Ein Großteil dieser Netzbetreiber könnte beispielsweise dasselbe Softwaresystem zur Regelung von Erzeugung oder Verbrauch verwenden. Falls der Angreifer eine Schwachstelle in diesem Softwaresystem entdeckt, kann er dadurch sofort eine systemkritisch große Energiemenge unter Kontrolle bringen. Das Gleiche trifft auch auf Privatakteure zu, die die gleichen Smart-Home-Systeme verwenden. Im Gegensatz dazu kann bei sehr großen Netzbetreibern ein einziger erfolgreicher Angriff ausreichend sein, um einen Blackout herbeizuführen.

Die Bedrohung durch Cyber-Angriffe wächst, da komplexe und hochprofessionalisierte Wertschöpfungsketten für Produkte und Dienstleistungen für Cyber-Angriffe entstanden sind und eine „Wachstumsbranche" – oft im illegalen Bereich – bilden. Für unbekannte Sicherheitslücken gibt es ebenfalls einen hochspezialisierten Markt, der insbesondere von böswilligen Akteuren genutzt wird. Professionelle Werkzeuge mit hohem Bedienkomfort sind für wenig Geld oder sogar quelloffen (Open Source) und damit leicht anpassbar legal im Internet erhältlich. Darüber hinaus verschaffen sich staatliche Akteure zunehmend die Möglichkeit, die elektrischen Energiesysteme anderer Staaten über Cyber-Angriffe abzuschalten.[234] Da zunehmend Staaten solche Angriffe als Bestandteil ihrer Militärstrategie sehen, lässt sich vermuten, dass jede denkbare Möglichkeit, über Cyber-Angriffe erfolgreich das elektrische Energiesystem in die Knie zu zwingen, auch untersucht und vorbereitet wird.

In den Medien wird vermehrt über staatliche Bestrebungen berichtet, die darauf zielen, sich über vermeintlich geheime Zugangswege auf alle Geräte der eigenen Bürgerinnen und Bürger Zugriff verschaffen zu können oder gar die Daten und Software auf den Geräten zu manipulieren oder zu löschen.[235] Dazu werden entweder Zugänge absichtlich aufgrund staatlicher Aufforderung eingebaut oder vorhandene Sicherheitslücken genutzt. Dies kann zum Beispiel zur Terrorabwehr und/oder Kriminalitätsbekämpfung zum Einsatz kommen. Da aus Geheimhaltungsgründen wenig über die Überprüfung dieser oder auch vergleichbarer Software anderer Staaten bekannt ist, werden viele dieser Lücken wiederum selbst wenig abgesichert sein. So finden erfahrungsgemäß auch Dritte diese Sicherheitslücken. Im besten Fall werden diese veröffentlicht, damit die Lücken geschlossen werden, im schlimmeren Fall gelangen diese Lücken auf den Markt, um von bösartigen Akteuren eingekauft zu werden. Ebenso gelangen die staatlichen Angriffswerkzeuge auf den Markt[236] – mit verheerendem Schadenspotenzial für die KRITIS Strom.

Bei einer rasant zunehmenden Digitalisierung innerhalb und außerhalb des Stromsektors werden sich all diese Bedrohungspotenziale in den nächsten Dekaden vervielfachen. Eine besondere Herausforderung ergibt sich aus den verschiedenen Entwicklungsgeschwindigkeiten von energietechnischer Infrastruktur. Viele Komponenten, wie Transformatoren, Leitungen oder auch Erneuerbare-Energie-Anlagen, verrichten

234 Das CRO (Chief Risk Office)-Forum, ein Verband der großen internationalen Versicherer, sieht in seinem „Emerging Risk Radar" Blackouts durch Cyber-Angriffe in der höchsten Risikokategorie, Tendenz weiter steigend (CRO 2020).

235 Biselli 2020.

236 Für ein Beispiel vgl. Brühl et al. 2019.

ihre Dienste unverändert über Jahrzehnte, während manche Software mehrfach pro Jahr aktualisiert wird und Innovationszyklen der IKT-Branche nur wenige Jahre dauern.

4.3 Basisursache 3: Die technische Systemkomplexität erschwert die Vorhersage von Auswirkungen im operativen Betrieb

Das Geschehen im Stromnetz wird eine größere Eigendynamik entwickeln als bisher. Das liegt daran, dass es immer mehr Abhängigkeiten zwischen verschiedenen Teilen des Systems – auch organisationsübergreifend – gibt und geben wird, unter anderem, weil die Anzahl der Erzeugungseinheiten größer wird und Strom tages- und jahreszeitabhängig erzeugt wird. Damit steigt die Komplexität. Die Auswirkungen zeigen sich insbesondere während des operativen Betriebs und erfordern deshalb schnelle Reaktionen – zum Teil in Echtzeit. Deren Folgen lassen sich oft schwer abschätzen, da sich aufgrund der komplexen Abhängigkeiten unvorhergesehene oder gar unvorhersehbare, sich gegenseitig verstärkende Effekte einstellen können. Auch fehlende Kenntnis über den Zustand der IKT-Systeme kann zu Fehleinschätzungen der aktuellen Lage und damit zu Fehlern in der Betriebsführung führen.

Auch die Störereignisse samt Kaskaden selbst können komplexer werden. In einem digitalisierten Energiesystem können IKT und energietechnische Komponenten nicht voneinander getrennt werden: Die energietechnischen Systembestandteile sind weitgehend mit eingebetteten Computern ausgestattet und untereinander vernetzt. Während die Netzbetreiber einen Teil ihrer Informationsflüsse über Kommunikationsnetze führen, die physisch von der öffentlichen Kommunikationsinfrastruktur getrennt sind, sind viele Erzeugungsanlagen im Verteilnetz über das Internet zu erreichen. Dies verursacht sowohl eine komplexe gegenseitige Abhängigkeit zwischen elektrischem Energiesystem und Kommunikationsinfrastruktur als auch stark unterschiedliche Sicherheits- und Zuverlässigkeitsanforderungen. Ein Ausfall von Teilen der Kommunikationsinfrastruktur kann zum Ausfall von Teilen der Energieinfrastruktur führen und umgekehrt. Diese Wechselwirkung kann im Fall eines Blackouts dazu führen, dass es sehr schwierig wird, ein Lagebild zu erstellen und das System wieder anzufahren.

Auch die IKT-Systemlandschaft selbst wird komplexer: Wie bereits erwähnt bringt IT/OT-Konvergenz bereits heute Anwendungen in Wechselwirkung, die früher vollständig getrennt waren. Dies schafft weitere Komplexität und damit zusätzliche Vulnerabilitäten. In der Folge kann in Krisen- oder Störfällen der Netzbetreiber nur schwer einschätzen, wie seine systemstabilisierenden Maßnahmen wirken, oder es herrscht Unklarheit darüber, welche Maßnahmen überhaupt zu ergreifen sind. Auch der Wiederaufbau des Systems kann durch unvorhersehbares Verhalten behindert werden. Ein Resilienzkonzept, das alle denkbaren Störungen und Wechselwirkungen von vornherein miteinbezieht, ist damit unmöglich geworden.

Viele der vernetzten Erzeugungsanlagen werden zukünftig über KI und lernende Systeme gesteuert werden. Dies kann zu unerwünschtem emergentem[237] Verhalten führen, auch durch unvorhersehbares Verhalten von Verbrauchern oder Erzeugern. Aber auch

237 Der Begriff Emergenz bezeichnet das Phänomen, dass durch das Zusammenspiel einzelner Systemteile vollkommen neues, nicht vorhersehbares Verhalten entsteht.

kleinteilige Märkte[238] in Kombination mit kleinen Verbrauchs- und Erzeugungsanlagen wie Wärmepumpen und PV-Dachanlagen, die automatisiert durch KI und lernende Systeme handeln, können die Systemstabilität aufgrund von unerwartetem Verhalten bedrohen.

Auch die Märkte werden mehr als heute dazu beitragen, dass die Systemdynamik steigt. Das Marktgeschehen kann insbesondere dann Einfluss auf die Systemstabilität haben, wenn die Märkte losgelöst von der physikalischen Realität im Stromnetz ausgestaltet sind. Die Liberalisierung der Stromversorgung kann zu Problemen führen, wenn die Schaffung von Wettbewerbsstrukturen zu sehr in den Vordergrund rückt und die Idee eines integrierten Energiesystems mit hierarchischer Steuerung aus dem Blick gerät. Das heutige Energiemarktdesign ist darauf ausgelegt, die Systemsicherheit nicht zu gefährden. Falls doch neue Gefährdungen für die Systemsicherheit erkennbar werden, wird in der Regel schnell nachgesteuert.[239] Die Unvorhersehbarkeit des Effekts von Märkten auf das Systemverhalten kann jedoch durch neue Marktformen wie Peer-to-Peer-Märkte[240] oder lokale Märkte, die etwa durch lokale Genossenschaften mit eigenen Netzen und eigener Erzeugung entstehen können, verstärkt werden.

Die schnelle Automatisierung kann zudem zu einer nachlässigen oder übervorsichtigen persönlichen Haltung gegenüber Risiken führen, was wiederum risikobehaftetes Verhalten begünstigen würde: Auf der einen Seite verlässt sich das Betriebspersonal möglicherweise zu sehr auf die intelligente Automatisierung, wird zu sorglos und verliert die Erfahrung im Umgang mit dem System. Auf der anderen Seite führt ein zu starker Fokus auf die Gefahren der Automatisierung dazu, dass resilienzsichernde Maßnahmen und Lösungen, die auf Automatisierung beruhen, nur zögerlich umgesetzt werden. Dadurch kann deren Potenzial nicht voll ausgeschöpft werden.

4.4 Basisursache 4: Ungewissheit über zukünftige Entwicklungen erschwert ein optimales Systemdesign

Regulierung und Systemdesign enthalten implizit-unbewusste sowie explizit-bewusste Annahmen über die Zukunft – etwa über Ort und Art der Stromerzeugungskapazitäten, den europäischen Markt, die denkbaren Disruptionen durch Digitalisierung oder die Risikobewertung gewisser Schadensereignisse. Zudem führen Fehler der Vergangenheit, die aus einer Ungewissheit entstanden sind, meist nicht dazu, die Existenz dieser Ungewissheiten anzuerkennen und damit umzugehen – genau das wäre die Idee der Resilienz. Stattdessen wird lediglich analysiert, was genau zu diesem Fehler geführt hat, um daraus Konsequenzen für die zukünftige Vorgehensweise zu ziehen. Der Lerneffekt beschränkt sich also darauf, den gleichen Fehler in Zukunft zu vermeiden. Außerdem neigen Gruppen von Expertinnen und Experten ähnlichen Hintergrunds zu einem „kognitiven Bias“: Die für möglich gehaltenen zukünftigen Entwicklungen bilden einen viel zu kleinen Ausschnitt der möglichen Entwicklungen ab.

238 Die Mindestenergiemengen pro Transaktion (heute: mindestens 0,1 Megawatt), die gehandelten Zeiten (heute: mindestens 15 Minuten) und die Zeit bis zur physischen Erfüllung eines Kontrakts (heute: mindestens 5 Minuten im Intra-Day-Handel) werden kleiner – ein Trend, der auch in den nächsten Jahrzehnten anhalten kann.

239 Vgl. zum Beispiel Mihm 2019.

240 Peer-to-Peer-Märkte kommen ohne zentrale Instanz aus. Stattdessen wird der Handel zwischen zwei Parteien direkt abgewickelt.

Aus diesen Ungewissheiten entstehen weitere Risikofaktoren. Implementierte Technologien und die aufgebauten Infrastrukturen könnten eine Pfadabhängigkeit geschaffen haben, sodass das Energiesystem nicht ausreichend robust an neue, unerwartete Entwicklungen anpassbar ist. Es ist insbesondere zu beachten, dass es bisher einen Mangel an Methoden und Werkzeugen gibt, mit denen das System analysiert und verstanden werden kann. Wenn sich Politik, Verbände und Energieunternehmen nicht ausreichend mit der Möglichkeit unbekannter gravierender Störereignisse auseinandersetzen, ist eine mögliche Folge, dass die Fähigkeit zur Störungsbehebung zu sehr auf bekannte Fälle ausgelegt ist. Das Betriebsführungspersonal bereitet sich unzureichend auf Bedrohungsereignisse vor, in denen flexibel oder sogar improvisierend reagiert werden muss. Auch die Resilienzmechanismen beruhten dann weiterhin ausschließlich auf bekannten Mustern und Abläufen bei Störereignissen. In diesem Fall wären viele Netzbetreiber zögerlich bei der Finanzierung und Einführung von Technologien und Prozessen, die sich für den Umgang mit unerwarteten Ereignissen eignen könnten. Darüber hinaus könnte ein Mangel an Expertinnen und Experten, die das Energiesystem sowohl elektrotechnisch als auch IKT-technisch verstehen, dazu führen, dass die technischen Potenziale für ein resilientes System nicht ausreichend genutzt werden.

Die Zuständigkeit für die Störungsbehebung während des Betriebs verschiebt sich mit der Einführung neuer technischer Mechanismen. Wenn die Verantwortlichkeiten zwischen Netzbetreibern, Lieferanten und weiteren Akteuren wie Aggregatoren nicht ausreichend definiert sind, kann im Falle eines Störereignisses nicht adäquat reagiert werden. Dadurch erhöht sich das Risiko eines Blackouts.

Richtlinien und Verordnungen, die für alle Länder des europäischen Verbundnetzes festgelegt wurden, werden in jeweils unterschiedlichen nationalen Rechtssystemen umgesetzt. Dadurch kann es zu sehr unterschiedlichen Umsetzungen kommen. Dies könnte insbesondere dann der Fall sein, wenn die Umsetzung sehr teuer ist, die Regulierung große Spielräume zulässt oder auch Akzeptanzfragen nicht ausreichend beachtet wurden und in den Mitgliedstaaten unterschiedlich adressiert werden. Da jeweils verschiedene Institutionen und Gremien (Europäische Kommission, nationale Regulierer, VNB, Standardisierungsgremien, Behörden) für die Regelsetzung verantwortlich sind, könnten sich diese Regeln nicht ausreichend ergänzen.

Ein Teil der zu verabschiedenden Regelwerke wird möglicherweise nur zur gewünschten Resilienz führen, wenn auch Eingriffe in die Haushalte möglich werden – etwa die Möglichkeit, bei drohendem Blackout in die Ladevorgänge der elektrischen Fahrzeuge einzugreifen. Da solche Regeln sehr auf Akzeptanz angewiesen sind, spielt die zwar langsame, aber sehr schwer absehbare Entwicklung von gesellschaftlichen Einstellungen dabei eine große Rolle. So könnte etwa der Wunsch nach Selbstwirksamkeit[241] verhindern, dass der Netzbetreiber Schalthandlungen an kleinen Anlagen vornehmen kann und darf. Möglicherweise benötigte Systemreserven würden dadurch nicht zur Verfügung stehen.

241 Die Überzeugung, eine Situation aus eigener Kraft zu bewältigen (Selbstwirksamkeit), ist hier eine notwendige Voraussetzung für Akzeptanz.

5 Resilienz als Ansatz für die Systemsicherheit

Wie die Basisursachen zeigen, ergeben sich neue und unvorhersehbare Risiken, die große Blackouts wahrscheinlicher machen könnten, wenn keine angemessenen Maßnahmen eingeleitet werden (siehe Kapitel 4). Für den Umgang mit Unsicherheiten in komplexen soziotechnischen Systemen hat sich das Konzept der **Resilienz** bewährt.

Um das elektrische Energiesystem ausfallsicher zu gestalten, wurde bisher weitgehend ein risikobasierter Ansatz verfolgt: Um Risiken zu messen und zu bewerten, wird der Schaden von möglichen Störereignissen bewertet und die Wahrscheinlichkeit des Eintritts der Schadensereignisse abgeschätzt. Mit diesem Wissen werden dann Schwachstellen beseitigt und das System robust gestaltet. **Robustheit** gegenüber einem gravierenden Störereignis bedeutet hier, dass ein Störereignis keinen großen Blackout zur Folge hat. Auslösende Störereignisse, die in der Folge zu großen Blackouts führten, waren in der Regel Ausfälle großer Komponenten, gefolgt von weiteren Fehlern. Ein Beispiel für ein solches Störereignis ist etwa der große Stromausfall in Italien im Jahr 2003: Das erste auslösende Störereignis war ein Lichtbogen, der sich zwischen einer Leitung und einer Tanne spannte und so zu einem Ausfall der Leitung führte. Dies hätte wegen des N-1-Kriteriums noch nicht zu einem Blackout führen müssen, jedoch hatte eine unzureichende Leistungsanpassung in Italien und nachfolgende Kettenreaktion einen totalen Stromausfall in Italien zur Folge.[242]

Zunehmend führen jedoch auch andere Auslöser zu Blackouts. So kam es im November 2006 zu einem großflächigen Stromausfall, von dem in Europa über 15 Millionen Haushalte betroffen waren. Dieser wurde ursächlich durch menschliches Versagen verursacht (fehlende N-1-Analyse, mangelhafte Abstimmung zwischen den ÜNB, Fehlkonfigurationen im technischen System).[243] Der Ausfall konnte nach weniger als einer Stunde behoben werden – ein Indiz dafür, dass das heutige System bereits resilient auf konventionelle Störungen reagiert.

Generell sorgt das bisherige Systemdesign dafür, dass die Wahrscheinlichkeit für einen großen Blackout extrem gering gehalten wird.[244] Bei der langfristigen Entwicklung des elektrischen Energiesystems verhindern jedoch Unsicherheit über die zukünftigen Entwicklungen und zunehmende Komplexität des Systems nicht nur eine verlässliche Abschätzung von Wahrscheinlichkeiten neuer relevanter Störereignisse – wie die eines erfolgreichen Hackerangriffs auf ausreichend viele verteilte, aber vernetzte Erzeugungsanlagen – , sondern es können auch bisher unbekannte Störereignisse auftreten oder sich die Wahrscheinlichkeiten bekannter Störereignisse deutlich verändern. Dementsprechend reichen die bisherigen Maßnahmen und Werkzeuge nicht mehr aus, die für die Gesellschaft notwendige und gewohnte Sicherheit der Stromversorgung zu garantieren.

242 UCTE 2004-1.
243 UCTE 2006.
244 Siehe UCTE 2004-2, S. 4 ff.

Man unterscheidet drei Merkmale,[245] die das Wissen beziehungsweise Unwissen über Risiken beschreiben und so indizieren, wie groß der Bedarf nach Resilienz als Methode zum Umgang mit Unsicherheit ist:

- **Komplexität**: In einem System sehr vieler heterogener Komponenten mit enger vielfacher Wechselwirkung hängen Ursache und Wirkung auf nichtlineare Weise zusammen. Kausalität ist schwer zu rekonstruieren, vollständiges Wissen über den Systemzustand ist nicht annähernd zu erlangen. Traditionelle statistische Methoden allein eignen sich nicht zur Beschreibung des Systemverhaltens.

- **Unsicherheit**: Es gibt Unsicherheiten, wie sich ein System in Zukunft entwickeln wird. Prinzipiell unvorhersehbar sind etwa langfristige Entwicklungen gesellschaftlicher Einstellungen oder politische oder auch technische Disruptionen. Andere („epistemische“[246]) Unsicherheiten lassen sich hingegen durch Forschung oder bessere Methoden beziehungsweise Werkzeuge zur Erfassung und Bewertung von Informationen verringern.

- **Soziopolitische Ambiguität**: Selbst aus umfangreichem und allgemein geteiltem Wissen ziehen die Akteure unterschiedliche Schlüsse. Informationen werden unterschiedlich interpretiert. Werteinstellungen der Akteure bestimmen, welche Informationen aufgenommen werden und welche Art von Risiko wie akzeptabel ist beziehungsweise wie viel die Gesellschaft bereit ist, zur Vermeidung dieses Risikos auszugeben.

Auf die zukünftige Entwicklung des elektrischen Energiesystems treffen alle drei Merkmale in deutlichem Maße zu. Erhöhte Komplexität ergibt sich etwa durch die vielen neuen Erzeugungskomponenten und deren schwer erfassbare Wechselwirkungen, die Digitalisierung und neue Marktmodelle. Die Unsicherheit ergibt sich unter anderem durch den langen Zeithorizont, zu erwartende Disruptionen bei der Digitalisierung und erst recht die Ungewissheiten politischer Entwicklungen. Es besteht zwar allgemein Einigkeit, dass große Blackouts zu vermeiden seien, es gibt aber viele unterschiedliche Meinungen, welche Entwicklungen wie wahrscheinlich und gravierend sind. Auch die Frage, welche Maßnahmen und Eingriffe als gerechtfertigt angesehen werden sollten, um der Bedrohung eines Blackouts zu begegnen, wird kontrovers diskutiert. Als Beispiel mag das Störungsereignis „Cyber-Angriff“ dienen: Die Eintrittswahrscheinlichkeit dieses Ereignisses kann nicht verlässlich angegeben werden und wird zudem von den Stakeholdern sehr verschieden eingeschätzt, die komplexen Auswirkungen auf das elektrische Energiesystem sind kaum absehbar und werden unterschiedlich beurteilt. Zudem kann ein erfolgreicher Angriff die Wahrscheinlichkeit für den nächsten erfolgreichen Angriff deutlich erhöhen, wenn die Schwachstelle bekannt ist, nicht behoben wurde und der Angreifer somit den nächsten Angriff einfacher durchführen kann. Eine allgemein und überall verbesserte Cyber-Sicherheit erhöht zwar die Sicherheit des elektrischen Energiesystems, erschwert den Behörden aber die Verbrechensbekämpfung – ebenfalls ein Beispiel für unterschiedliche Interessen, für Ambiguität.

In solcher Ausgangslage hat sich das Konzept der **Resilienz** bewährt. Der Begriff **Resilienz** wird in verschiedenen Wissenschaftsgebieten verwendet – „angefangen von

245 Nach Aven/Renn 2009.

246 Siehe Thunnissen 2003. Dort finden sich auch weniger vereinfachte Klassifikationen von Unsicherheiten.

der Entwicklungspsychologie über die Ökologie und die Sozialwissenschaften bis hin zum Ingenieurwesen".[247] Im Kontext der Energieversorgung gilt: „Ein Energiesystem, dessen Funktion – hier die Versorgungssicherheit – unter Belastungen erhalten bleibt oder zumindest innerhalb kurzer Zeit mit (vertretbaren Mitteln) wiederhergestellt werden kann, ist ein resilientes Energiesystem."[248] Dieser Analyse liegt daran angelehnt die folgende Definition bezogen auf das elektrische Energiesystem zugrunde:

> Ein resilientes Energiesystem besitzt die Fähigkeit, die nachteiligen Auswirkungen eines spontanen oder schleichenden Störereignisses mit zwar eventuell abnehmender Versorgungsqualität abzufangen, aber ohne dass das System mit einem grösseren Blackout kollabiert, um anschliessend zügig wieder in den normalen Betriebszustand zurückzukehren.

Das klassische Risikomanagement mit Fokus auf der Identifizierung von Schwachstellen in der Systemauslegung versucht unter Berücksichtigung von Schadensauswirkung und Eintrittswahrscheinlichkeiten, gefährdete Komponenten zu „härten". Es strebt somit nach Prävention und Milderung aus der Vergangenheit bekannter Vorfälle. Das Resilienzkonzept zielt jedoch auf die Zeit nach dem Ereignis ab[249] und kann besser mit Entwicklungen und Ereignissen umgehen, die sich schwer aus den bisherigen Erfahrungen und dem vorhandenen Wissen ableiten oder erkennen lassen. Wie auch in der obigen Definition schließt man im Verständnis der Resilienz in der Regel auch Robustheit mit ein. Ein weiteres Wesensmerkmal der Resilienz ist Lernfähigkeit: Das System sollte so gestaltet werden, dass es aus vorgefallenen Ereignissen lernt und sich auf das Wiederauftreten eines solchen oder ähnlichen Störereignisses vorbereitet.[250]

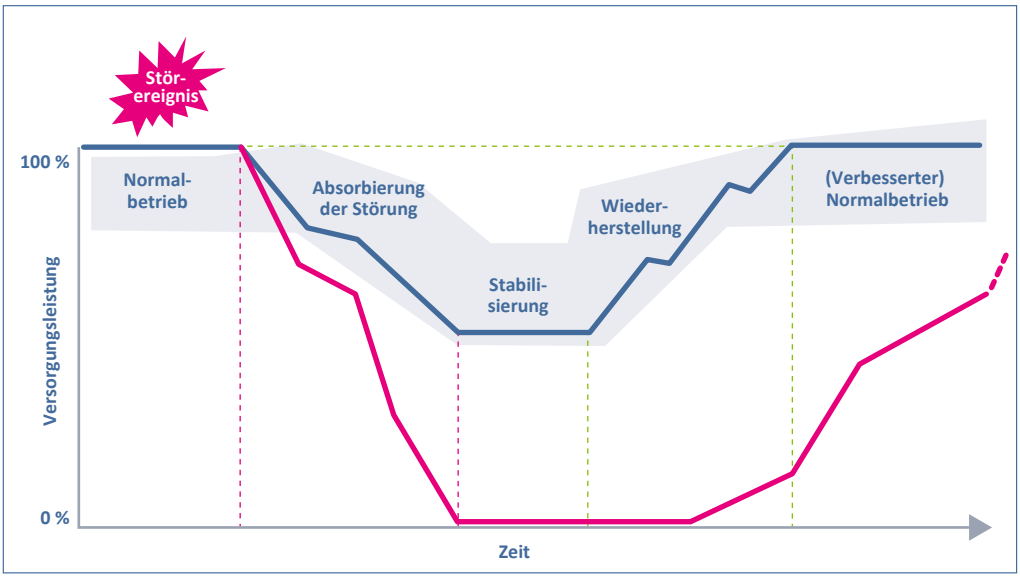


Abbildung 9: Resilienzkurve: Wiederherstellung der Funktionsfähigkeit eines Systems: *„die geeignete Reaktion auf ein Ereignis (Absorbieren der Störung), das Zurückfallen auf kritische Funktionen und Stabilisierung des Systems (Stabilisierung) und zuletzt das kontrollierte Zurückbringen zum Normalbetrieb des Systems (Wiederherstellung)"*[251]

247 acatech 2014-2, S. 4.

248 acatech/Leopoldina/Akademienunion 2017-2, S. 10.

249 Nach Kröger 2019, S. 291.

250 Lernfähigkeit ist bereits heute wesentlicher Bestandteil der Energieversorgung. Die Analysen der ENTSO-E (beziehungsweise UCTE) wie in UCTE 2004-1 und UCTE 2006 führen immer auch zu Maßnahmen, um solche Ausfälle in Zukunft zu vermeiden.

251 Babazadeh et al. 2018, S. 32 f.

Abbildung 9 stellt den resilienten Wiederherstellungsprozess der Versorgungsleistung nach einem gravierenden Störereignis grafisch dar: Tritt das Störereignis ein, muss zunächst die Störung absorbiert werden, um weitere Verluste zu vermeiden. Auf Übertragungsebene kann dies etwa durch die Auftrennung des Verbundnetzes in verschiedene Frequenzgebiete erreicht werden. In dieser Phase gilt es in erster Linie, die kaskadenartige Ausbreitung zu vermeiden. Ist dies gelungen, muss das System stabilisiert werden: Es können etwa große Lasten abgeworfen (bei zu niedriger Frequenz) oder auch Kraftwerke gedrosselt werden (bei zu hoher Frequenz). Sobald das (Teil-)System wieder beherrscht wird, beginnt die Wiederherstellung (manchmal auch „Restauration“ genannt). Im betrachteten Fall hieße dies, die verschiedenen Teilnetze wieder zu synchronisieren und zusammenzuschalten. Aufwendiger gestaltet sich die Wiederherstellung, wenn größere Reparaturarbeiten notwendig sind, etwa wie beim Stromausfall 2005 im Münsterland, bei dem Strommasten durch das Gewicht des Schnees auf Leitungen umknickten. Auch eine langwierige Wiederherstellung der IKT-Systeme nach einem erfolgreichen Cyber-Angriff könnte dazu führen, dass die Restaurationsphase länger dauert. Nachdem die Stromversorgung wiederhergestellt wurde, werden Analysen vorgenommen und aufgrund dieser Analyse Maßnahmen durchgeführt, um die Resilienz des elektrischen Energiesystems weiter zu erhöhen. Dies kann etwa durch Trainings, Austausch von Komponenten, verbesserten Informationsaustausch der Akteure oder die Anpassung technischer Prozesse erreicht werden.

Dass die Resilienzkurve, wie sie Abbildung 9 darstellt, auch bereits heute eine Rolle spielt, zeigt das Beispiel der Stromausfälle, die im Oktober 2012 durch den Hurrikan Sandy verursacht wurden.[252] Es waren über acht Millionen Anschlüsse betroffen, die zum Teil wochenlang ohne Strom waren. Abbildung 10 zeigt, wie zunächst ein großer

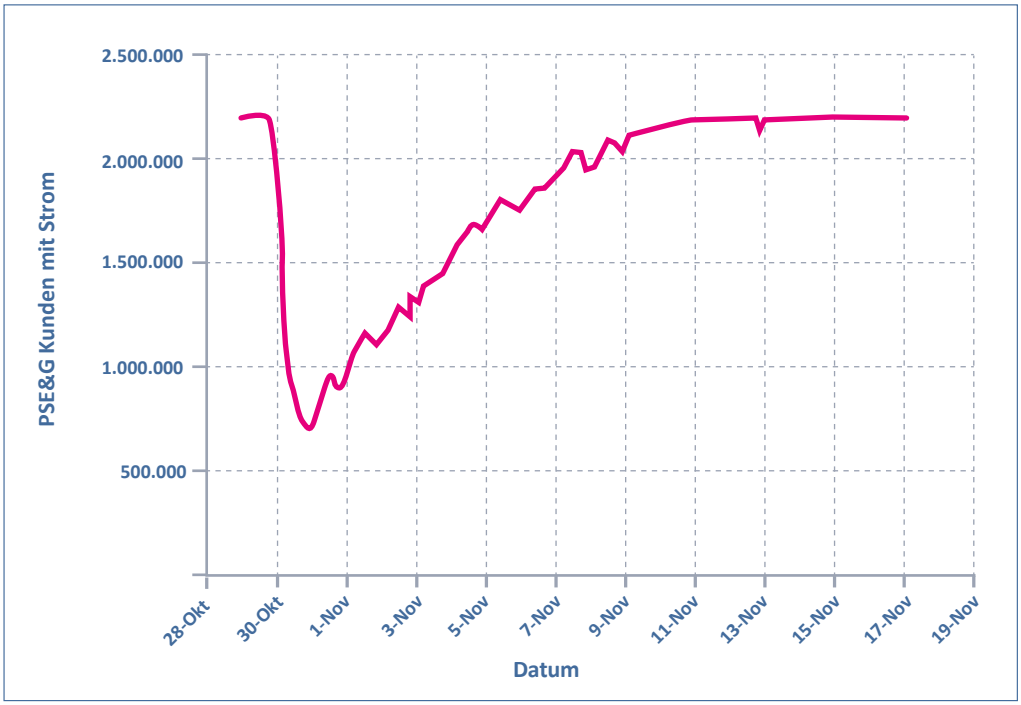


Abbildung 10: Anzahl der Stromanschlüsse des Energieversorgers PSE&G, die von Stromausfällen durch den Hurrikan Sandy betroffen waren. Zu erkennen ist die typische Resilienzkurve[253]

252 Henry/Ramirez-Marquez 2016.

253 Angepasste Darstellung nach Kröger 2019

Anteil der Anschlüsse schwarzfällt und nach und nach die Versorgung wieder aufgebaut wird: Nach dem Störereignis bleibt eine Versorgung von etwa dreißig Prozent der Anschlüsse möglich (Absorbierung), es folgt eine kurze Phase der Stabilisierung, die dann gleich in eine etwa acht Tage währende Systemwiederherstellung übergeht, bis die volle Versorgungsleistung wiederhergestellt ist. Die lange Dauer bis zur vollständigen Versorgungswiederherstellung zeigt eine geringe Resilienz der Stromversorgung gegenüber Hurrikans. Jedoch sind die Erwartungen an die Resilienz der Energieversorgung gesellschaftsabhängig: So wird in Deutschland ein besonders hoher Anspruch an die Qualität der Stromversorgung gestellt.

Um ein resilientes System aufzubauen, beizubehalten und kontinuierlich zu verbessern, benötigen die verantwortlichen Akteure eine Resilienzstrategie.[254] Im ESYS-Projekt wurde dazu ein Schema aus vier aufeinander aufbauenden Feldern entwickelt[255] (siehe Abbildung 11):

- Im Feld A *Risiken und Schwachstellen identifizieren* wird versucht, Belastungen zu identifizieren, die das Energiesystem schädigen könnten, die Vulnerabilitäten dazu festzustellen und Präventivmaßnahmen abzuleiten. Dazu können Informationen aus der Überwachung des Systems, historische Daten sowie Zukunftsprojektionen herangezogen werden.

- Das Feld B *Das System robust und vorsorgend gestalten* setzt die Erkenntnisse aus Feld A um. Zu diesem Zweck können etwa Redundanzen oder Puffer (zum Beispiel Speicher) in das System integriert werden. Aber auch durch ergänzende neue Techniken oder Prozessschritte ließe sich die Resilienzkurve optimieren. Wird das System offen und nachjustierbar gestaltet, kann später eine Adaption auf unerwartete Entwicklungen leichter erfolgen.

- Im Feld C *Ausfälle überbrücken und Systemdienstleistung wiederherstellen* handelt es sich hauptsächlich um die Durchführung der Prozessschritte der Resilienzkurve: Absorbieren, Stabilisieren, Wiederaufbau. Auch die Notversorgung ist Teil dieses Schrittes. Zusätzlich (aber hier nicht betrachtet) gehören Maßnahmen des Katastrophenschutzes in diesen Bereich.

- Feld D *Lernende und adaptive Systeme aufbauen* hat einerseits zum Ziel, aus jedem eingetretenen oder auch vermiedenen Störfall zu lernen, um die Resilienz zu verbessen und das System anpassungsfähig zu halten; dazu bedarf es unter anderem der Dokumentation und der Analyse bisheriger Störungen und deren Bewältigung. Es soll aber auch die Reaktion auf Unerwartetes, etwa durch Improvisationsfähigkeit, von den Akteuren geübt und erlernt werden. Nicht zuletzt helfen Stresstests und Simulationen, mit denen die Akteure prüfen, ob sie in der Lage sind, resilient zu reagieren.

254 acatech/Leopoldina/Akademienunion 2017-2, S. 10.
255 acatech/Leopoldina/Akademienunion 2017-2, S. 18.

Das Restrisiko eines mehrtägigen großflächigen Blackouts bleibt auch in einem resilienten Energiesystem immer bestehen. Diese Art der Störungen (etwa ein extremer Sonnensturm mit Schäden an Großkomponenten wie Transformatoren und tage- oder gar wochenlangem Stromausfall) erfordert es, umfangreiche gesellschaftliche Resilienzmaßnahmen außerhalb des hier betrachteten elektrischen Energiesystems, unter anderem im Katastrophenschutz, zu implementieren. Mit dieser Aufgabe befasst sich etwa das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.

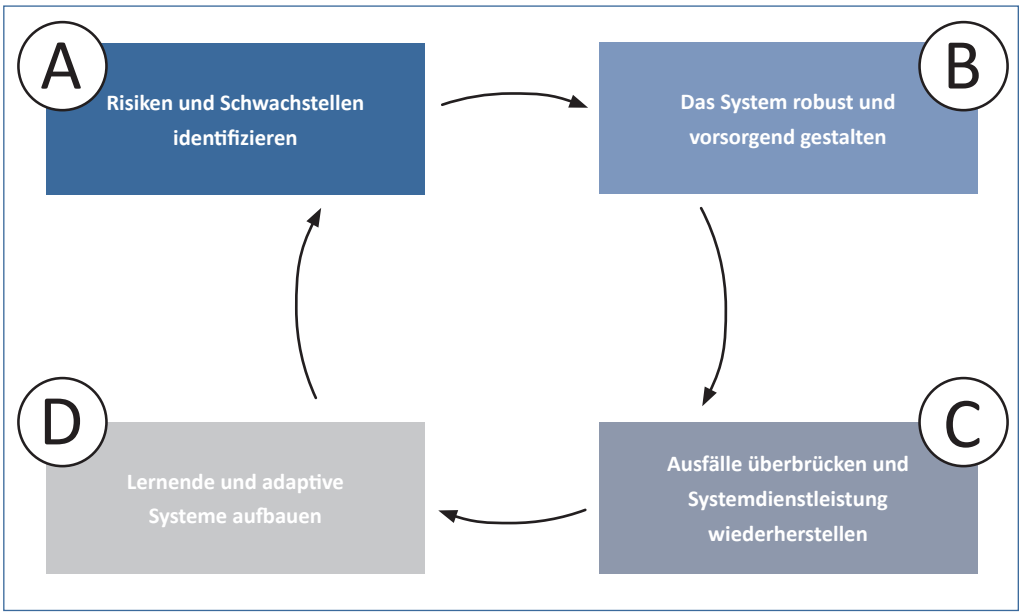


Abbildung 11: Resilienzstrategie[256]

256 acatech/Leopoldina/Akademienunion 2017-2, S. 18.

6 Handlungsoptionen

Um den im Kapitel 4 skizzierten Risiken wirksam zu begegnen und unsere Versorgungssicherheit auch zukünftig sicherzustellen, sind zum Teil völlig neue Denkansätze erforderlich. Dazu wird das Konzept der Resilienz genutzt (siehe Kapitel 5). Effektive Resilienzstrategien müssen entwickelt und bestehende Resilienzkonzepte angepasst und umgesetzt werden. Die ESYS-Arbeitsgruppe hat hierzu einen Katalog von insgesamt 15 Handlungsoptionen erarbeitet, die thematisch in sieben problemorientierte Handlungsfelder gruppiert sind. In den Handlungsoptionen werden verschiedene Maßnahmen für deren Umsetzung beschrieben.

Abbildung 12 gibt einen Überblick der sieben Handlungsfelder und zeigt, welche der vier Basisursachen (Kapitel 4) sie jeweils adressieren.

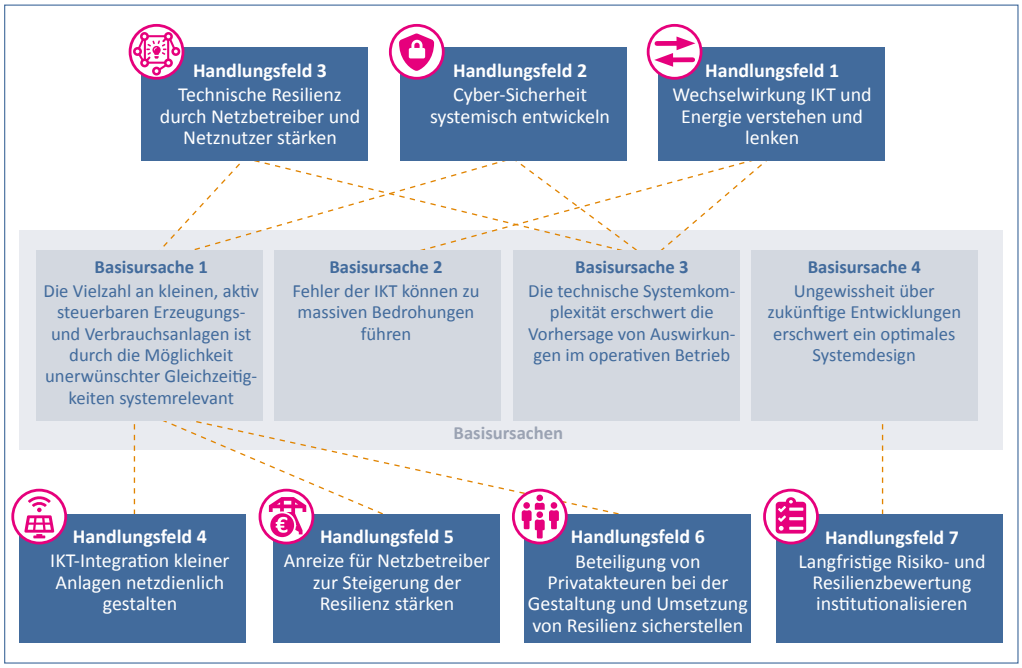


Abbildung 12: Übersicht der Handlungsfelder und auf welche Basisursachen sie wirken

In dem vorliegenden Kapitel werden die einzelnen Handlungsfelder (Kapitel 6.1 bis 6.7) jeweils ausführlich beschrieben:

- Zu jedem Handlungsfeld wird unter dem Stichwort **„Problem 2040“** erläutert, welche Herausforderungen sich im Betrachtungszeitraum bis 2040 aus den Basisursachen ergeben.

- In der anschließenden **„Erläuterung“** wird das Problem ausführlicher beschrieben und im Kontext des heutigen elektrischen Energiesystems und aktueller Entwicklungen analysiert.

- **„Zeithorizont des Problems“** dient der Verdeutlichung des Handlungsdrucks im Hinblick auf bestimmte Maßnahmen.

- Unter **„Heute bereits bestehende Maßnahmen“** wird aufgegriffen, wie sich die jeweils relevanten Akteure bereits heute mit dem Handlungsfeld beschäftigen.

Die einzelnen Handlungsoptionen werden in Unterkapiteln zu jedem Handlungsfeld vertieft:

- Die **Dringlichkeit** gibt einen Hinweis darauf, wann mit der Umsetzung der Handlungsoption begonnen werden sollte (●●● in den nächsten zwei Jahren, ●● in zwei bis vier Jahren, ● in fünf bis zehn Jahren). Die **Wirksamkeit** schätzt den Beitrag der Handlungsoption zur Resilienz ab (●●● erhöht die Resilienz deutlich, ●● trägt wesentlich bei, ● geringerer Beitrag).

- Eine Zuordnung zu den vier Schritten der Resilienzstrategie wird gegeben (siehe Kapitel 5, hier abgekürzt als „Risikoanalyse“, „Robustheit“, „Wiederherstellen“, „Anpassung“).

- Der **„Langfristige Lösungsbeitrag“** führt aus, was bis zum Jahr 2040 erreicht werden sollte, um das eingangs beschriebene „Problem 2040“ zu lösen.

- Das **„Ergebnis“** in der Übersichtsbox fasst den durch die vorgeschlagenen Maßnahmen angestrebten „langfristigen Lösungsbeitrag“ knapp zusammen.

- Der Teil **„Was kann man heute tun?“** stellt den heute notwendigen Handlungsbedarf dar, um den Weg zum „langfristigen Lösungsbeitrag“ einzuschlagen. Darüber hinaus werden konkrete Maßnahmen benannt, die nach Ansicht der ESYS-Expertinnen und Experten aus heutiger Sicht angegangen werden sollten, um den langfristigen Beitrag sicherzustellen.

- Zu welchem Zeitpunkt die Optionen angegangen werden sollten, wird neben Vorteilen, Nachteilen und Umsetzungshürden in der jeweiligen **„Bewertung“** spezifiziert. Diese Angaben sind nicht immer vollständig, da teilweise noch weitere Analysen notwendig sind.

Für die konkrete Umsetzung der Handlungsoptionen kann die Politik im Wesentlichen Maßnahmen aus vier **Wirkungsbereichen** nutzen:

Prozesse, Produkte und Regeln: Akteure werden verpflichtet oder motiviert, betriebliche Prozesse oder Produkte anzupassen. Maßnahmen, die diesem Wirkungsbereich zugeordnet werden, sind dann angebracht, wenn heute schon bekannt ist, dass ein Problem besteht und bewertbare Lösungen zur Erhöhung der Resilienz vorliegen.

Forschung: Wissenslücken über das – heute noch nicht ausreichend verstandene –digitalisierte Energiesystem werden geschlossen, um daraus Maßnahmen zur Resilienzerhöhung abzuleiten. Dazu dienen insbesondere Analysen und Forschungsarbeiten.

Organisationen: Behörden und Gremien können neu aufgebaut oder angepasst werden, um politische Verantwortung zu delegieren und zu operationalisieren.

Partizipation: Dialog und Transparenz führen dazu, dass von verschiedenen Akteuren akzeptierbare Maßnahmen gefunden werden und das Vertrauen in die Angemessenheit von Entscheidungen wächst.

6.1 Handlungsfeld 1: Wechselwirkung IKT und Energie verstehen und lenken

Problem 2040: Die Stromversorgung der Zukunft wird noch viel mehr als heute von dem Funktionieren der IKT-Systeme abhängig sein. Dazu gehören sowohl Systeme, die Teil des Energiesystems sind, wie etwa Leitsysteme der Netzbetreiber, als auch solche, die nicht zum Energiesystem gehören, wie etwa Systeme der Cloud-Anbieter oder Smart-Home-Systeme. Umgekehrt ist die Kommunikationsinfrastruktur empfindlich von der Stromversorgung abhängig. Strom- und IKT-System bilden zukünftig also ein cyber-physisches Energiesystem, das in seiner Komplexität weit über das heutige technische Systemdesign hinausgeht. Werden die gegenseitigen Abhängigkeiten zwischen Strom- und IKT-System nicht im Systemdesign und während des Betriebs berücksichtigt, kann dies zu großen Blackouts führen.

Erläuterung: Die Abhängigkeit zwischen Strom- und Kommunikationssystem wird außerhalb der Systeme der Netzbetreiber bisher wenig berücksichtigt: So wird heute etwa beim Aufbau der Mobilfunknetze nicht beachtet, ob diese für die Stromversorgung in kritischen Situationen eine Rolle spielen könnten. Ähnliches gilt für öffentliche, leitungsgebundene Kommunikationsnetze der Telekommunikationsprovider. Die Betreiber von Kommunikations- beziehungsweise Stromnetzen stimmen sich nur wenig untereinander ab, wenn Infrastrukturen errichtet oder Instrumente zur Vermeidung kritischer Störsituationen konzipiert werden. In Zukunft wird es jedoch nicht mehr ausreichen, die zur Planung, Überwachung und Steuerung notwendigen IKT-Anwendungen als externe Systeme „neben“ dem eigentlichen elektrischen Energiesystem anzusehen.

Zukünftig werden Erzeugungsanlagen, steuerbare Verbrauchsanlagen, Betriebsmittel wie Ortsnetztransformatoren und sogar kleine Haushaltsgeräte kommunikationstechnisch angebunden sein. Wie sich in diesen zukünftigen Szenarien Störungen der Kommunikation auf das Energiesystem auswirken werden, ist noch nicht abzusehen. Es kann die Gefahr von kritischen Wechselwirkungen entstehen: Fehler, die in isolierten Systemen unter Umständen unkritisch wären, können zu Folgefehlern in verbundenen Systemen und so letztlich zu kritischen Situationen führen, zum Beispiel durch kaskadierende Effekte.

Kommunikation ist zudem nicht nur für den Normalbetrieb des elektrischen Energiesystems nötig, sondern auch zum Wiederanfahren des Systems nach Stromausfällen: Die Netzbetreiber müssen sich untereinander synchronisieren, Kraftwerke müssen kommunikativ angesteuert und zugeschaltet werden, Informationen über den – während des Hochfahrens noch fragilen – Netzzustand und das Gleichgewicht zwischen Last und Einspeisung müssen laufend ausgewertet werden. Wenn ein Großteil der Stromversorgung dezentral erfolgt, müssen auch die dezentralen Anlagen aktiv im Wiederaufbau mitwirken. Dazu müssen auch diese Anlagen, die über öffentliche IKT angebunden sein können, in die genannten Prozesse integriert werden.

Zeithorizont des Problems: Durch die Abhängigkeiten von Strom- und IKT-System gewinnt die Bedrohung durch kaskadierende Störungen bereits heute und in den nächsten Jahren an Relevanz. Das Risiko eines großen Blackouts durch massive Störungen an der Kommunikationsanbindung von neuen Akteuren wie beispielsweise Plattformbetreibern ist eher in der Zukunft relevant. Denn bisher existieren keine Plattformbetreiber, die mit Schalthandlungen zur Systemstabilisierung beitragen müssen. Hingegen könnte ein erfolgreicher Angriff auf Plattformen selbst schon in näherer Zukunft eine Bedrohung sein, etwa indem durch den Angriff ungewollte Last- und Erzeugungsspitzen herbeigeführt würden.

Heute bereits bestehende Maßnahmen: Die Kontrollzentren der Netzbetreiber sind bereits heute redundant, also mehrfach abgesichert, beziehungsweise georedundant, das heißt an weit voneinander entfernten Orten ausgelegt und mit Notstromversorgungssystemen abgesichert. Die Netzbetreiber verwenden zur Steuerung und Überwachung ihrer wichtigsten Betriebsmittel eigene, vom öffentlichen Netz unabhängige Kommunikationsnetze, die – inklusive der eingesetzten IKT-Komponenten – ebenfalls redundant ausgelegt sind. Große Betriebsmittel und Erzeugungsanlagen, die physikalisch an die oberen Spannungsebenen angeschlossen sind, wie zum Beispiel Umspannwerke oder große Wind- und Solarparks, können über die abgeschirmte Netzleittechnik der Netzbetreiber direkt angesteuert werden.

Auch viele Betriebe sichern sich schon seit Langem gegen Stromausfälle ab. So verfügen große Rechenzentren über eine redundante Anbindung an verschiedene Mittelspannungsnetze, eine eigene Notstromversorgung über Generatoren oder auch einen georedundanten Betrieb mit mehreren Rechenzentren an weit voneinander entfernten Orten. Plattformanbieter aus anderen Domänen greifen schon heute auf große Rechenzentren und hochverfügbare Kommunikationsinfrastrukturen zurück, die gegen mehrstündige Stromausfälle gewappnet sind.

Von den ÜNB wird bereits heute für 72 Stunden Schwarzfallredundanz verlangt – einhergehend mit der Verpflichtung, ihre versorgungsrelevanten IKT-Systeme bei

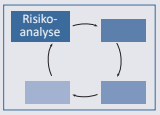
einem Blackout dieser Dauer zuverlässig betreiben zu können. Dasselbe gilt für Betreiber von Anlagen, die für die Ausführung der Systemdienstleistung „Versorgungswiederaufbau“ benötigt werden.[257] Die öffentlichen Kommunikationsnetze bleiben bei einem Stromausfall allerdings nur für mehrere Stunden betriebsbereit. Dies reicht nicht aus, um die für die KRITIS Stromversorgung notwendigen Kommunikationsanbindungen bereitzustellen, um die für den Systemwiederaufbau notwendigen Systemdienstleistungen abzurufen. Dies wäre in Zukunft jedoch nötig, um auch kleinere Anlagen zu annehmbaren Kosten für diese Systemdienstleistungen nutzen zu können.

Für die Höchst- und Hochspannungsebene haben Informationen zum Zustand des IKT-Systems für die Kommunikation bereits heute Relevanz: Ein Ausfall eines Teils dieser IKT-Systeme kann unmittelbar zu einem Blackout führen. Die Kommunikationssysteme werden daher von diesen Netzbetreibern auch schon überwacht. Aufgrund der geringen IKT-Durchdringung der unteren Spannungsebenen wird es hingegen noch lange dauern, bis dies für die Verteilnetzbetreiber relevant wird.

Die Netzbetreiber tauschen untereinander umfänglich Informationen aus – insbesondere, um sich in der Betriebsführung abstimmen zu können. Dieser Austausch wird regelmäßig evaluiert und verbessert. Grundlage für diesen Austausch sind bei den VNB überwiegend Vereinbarungen, die in technischen Richtlinien und Regeln festgehalten sind. Das EnWG regelt, dass die Netzbetreiber alle Anschlussnehmer zur Datenlieferung verpflichten können, soweit dies zum sicheren Betrieb der Netze notwendig ist.

Aus regulatorischer Sicht sind umfassende Regelungen für die Vergütung der IKT-Kosten der Netzbetreiber geschaffen worden. Die Netzbetreiber dürfen diese Kosten auf die Netzentgelte umlegen. Damit sind bereits viele Anreize zum Ausbau der IKT seitens der Netzbetreiber geschaffen worden.

Handlungsoption 1:
Abhängigkeiten zwischen Stromversorgung und Kommunikationsnetzen analysieren lassen



Ergebnis: Die energietechnische Infrastruktur und die Kommunikationssysteme sind jeweils so aufeinander abgestimmt, dass die gegenseitigen Abhängigkeiten kein Risiko mehr darstellen.

Dringlichkeit: ● ● ● **Wirksamkeit:** ● ● ●

Was kann man heute tun?

- Wissen zu den Abhängigkeiten zwischen den beiden Infrastrukturen erlangen.
- Europaweite Leitlinien im Austausch mit Verbänden und politischen Gremien erarbeiten.

Langfristiger Lösungsbeitrag: Die gegenseitigen Abhängigkeiten zwischen der energietechnischen Infrastruktur und IKT-Systemen müssen so gestaltet werden, dass

257 Mit diesen Regeln geht Deutschland deutlich über die Mindestregelungen der EU zur Systemsicherheit gemäß Verordnung (EU) 2017/2196 Artikel 41, 42 hinaus.

kaskadierende Ausfälle unmöglich oder zumindest extrem unwahrscheinlich werden. Dafür muss verhindert werden, dass bei einem Stromausfall in einem Netzgebiet IKT-Systeme ausfallen, die für die Aufrechterhaltung der Stromversorgung in einem anderen Netzgebiet benötigt werden. Dies kann etwa durch Aufteilung einzelner Netzgebiete gelingen: Die verantwortlichen Netzbetreiber sorgen dafür, dass jedes nicht von einem potenziellen Stromausfall betroffene Netzgebiet zur Aufrechterhaltung der Stromversorgung weder direkt noch indirekt IKT-Systeme benötigt, die im Netzgebiet des Stromausfalls liegen. Dadurch wären bei einem Stromausfall ausschließlich IKT-Systeme im Gebiet des Stromausfalls betroffen (und können abgesichert werden), während andere Netzgebiete keine Störungen ihrer IKT-Systeme feststellen. Wie vollständig dies gelingen kann, ist allerdings unklar, da Überlegungen dieser Art bei den bis heute errichteten Systemen keine Rolle spielten.

Zusätzlich sollte der Ausfall der Kommunikationssysteme in einem Netzgebiet nicht dazu führen, dass andere Netzgebiete gefährdet werden. IKT-Systeme werden häufig – und in Zukunft eher mehr als heute – ihre Funktionen und Daten aus einer geografisch nicht zuordenbaren Cloud beziehen. Dies stellt neue Anforderungen an IKT-Systemarchitekturen und Systembetrieb, die IKT-Dienstleister berücksichtigen müssen.

Was kann man heute tun? Im ersten Schritt gilt es zu verstehen, welche Abhängigkeiten in jedem Netzgebiet zwischen den beiden Infrastrukturen IKT und Strom bereits bestehen und welche Abhängigkeiten zukünftig zu erwarten sind oder sich durch den Einsatz neuer Technologien ergeben können. Dazu könnten die beiden Infrastrukturen erfasst und die Abhängigkeiten in Simulationen erprobt werden. Im Zuge dessen sollten auch mögliche Cyber-Sicherheitslücken identifiziert werden, die sich aus den Abhängigkeiten ergeben. Anschließend können Lösungen entwickelt werden, um Abhängigkeiten – insbesondere kaskadierende Effekte – zu verhindern oder zu entschärfen. Die verschiedenen Lösungsoptionen (etwa Redundanz oder Aufteilung der Netzgebiete mit jeweils unabhängigen Kommunikationssystemen) können dann technisch und ökonomisch bewertet und priorisiert werden.

Um dieses nötige Verständnis zu erlangen, bieten sich drei Maßnahmenbündel an, die im besten Fall parallel verfolgt werden:

1. Das Thema strukturieren und konkrete Fragestellung entwickeln: Dies sollte unter Leitung neutraler Verbände – wie etwa VDE – in Zusammenarbeit mit einer Auswahl an Vertretern von Netzbetreibern, Erzeugern, Herstellern sowie Anbietern und Betreibern von IKT-Lösungen unter Einbindung der Wissenschaft geschehen. Die Begleitung durch eine für die KRITIS Strom verantwortliche Behörde ist empfehlenswert.

2. Praxisbezogene Forschungsprojekte: An realen, konkreten Beispielen untersuchen, wie Lösungsansätze aussehen können. Da es nicht möglich ist, ein fehlerhaftes oder angegriffenes IKT-System für die Dauer eines Wiederaufbaus abzuschalten oder neu zu starten, müssen geeignete Wiederaufbaustrategien entwickelt werden, die mögliches Fehlverhalten berücksichtigen. Es bietet sich an, eine spezifische Ausschreibung im Rahmen des 7. Energieforschungspro-

gramms der Bundesregierung zu initiieren, die dieses Thema beinhaltet. Ergebnisse (wie etwa Modelle von Stromnetzen und Kommunikationsnetzen) sollten allgemein zur Verfügung gestellt werden. Dabei ist abzuwägen zwischen den berechtigten Interessen der Unternehmen an Geheimhaltung, möglichen Gefahren durch Sabotage und dem Allgemeinwohl einer gesicherten Energieversorgung.

3. Forschungsprojekte näher an der Grundlagenforschung: Diese werden in der Regel durch das BMBF initiiert und gefördert. Hier werden Grundlagen für Anwendungsfälle entwickelt, die perspektivisch in einem Energiesystem in den nächsten zehn Jahren erwartet werden. Der Fokus sollte dabei auf dem Einfluss der Abhängigkeiten auf die Resilienz liegen.

Die Ergebnisse der Studien und Projekte sollten handhabbare Verfahren und Regeln (Richtlinien zur Durchführung, Simulationen, Tests etc.) enthalten, um den ersten Schritt der Umsetzung starten zu können.

Zudem sollten die Ergebnisse auf europäischer Ebene besprochen und mit europäischen Verbänden und politischen Gremien ausgetauscht und in Verfahren und Regeln überprüft werden. Dies sind, nach heutigem Stand, neben der Politik insbesondere der europäische Verband der ÜNB (ENTSO-E) und der durch die Europäische Union geförderte Verband der europäischen VNB[258,259] sowie Standardisierungsverbände wie ETSI und CEN/CENELEC.

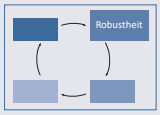
Bewertung: Die Maßnahmen sollten kurzfristig angegangen werden, da mit einem langen Umsetzungszeitraum zu rechnen ist. Jede Lösung dieses Problems ist voraussichtlich technisch komplex und aufwendig. Der hier vorgeschlagene Weg verursacht zu Beginn wenig Kosten zur Förderung der Pilotprojekte und Studien und vermeidet zunächst Pfadabhängigkeiten. Nicht geförderte Studien belasten den Staat nicht, da Ressourcen der Wirtschaft eingesetzt werden. Durch das BMWi vergebene und bezahlte Studien sind teurer, in der Regel im kleinen einstelligen Millionenbereich, ermöglichen der Politik jedoch, auf die genaue Fragestellung der Studie Einfluss zu nehmen, die Mitarbeiterinnen und Mitarbeiter auszuwählen und stärker auf Neutralität zu achten. Forschungs- und Entwicklungsprojekte zum Thema Abhängigkeiten zwischen IKT und Energie können eine größere Anzahl an technischen Fragestellungen, Optionen und Lösungsansätzen erarbeiten und breit diskutieren. Je nach Zuschnitt benötigen Projekte dieser Art Fördergelder ab zwei Millionen Euro. Ein späterer Ausbau zu Reallaboren ist möglich und zu empfehlen.

Umsetzungshürden bei der Entwicklung von Lösungen sind nicht zu erwarten. In der späteren Implementierung der Lösungen, die durch die Maßnahmen vorgeschlagen werden, sind dagegen umfangreiche Umsetzungshürden möglich, die sich aus der Komplexität des Systems ergeben: Hier sind große technische und regulatorische Herausforderungen zu erwarten.

258 Verordnung (EU) 2019/943, Artikel 52–56.

259 Derzeit existieren auf EU-Ebene noch vier Verbände, die für VNB sprechen, nämlich E.DSO, Eurelectric, CEDEC und GEODE. Dies macht Abstimmungen schwierig.

Handlungsoption 2:
Regeln für resiliente Kommunikationsnetze schaffen



Ergebnis: Die Kommunikationsnetze weisen eine ausreichend große Redundanz auf und sind – wo nötig – schwarzfallfest.

Dringlichkeit: ● ● **Wirksamkeit:** ● ● ●

Was kann man heute tun?

- Anforderungen schwarzfallfester Kommunikation für das Stromnetz ermitteln.
- Gegebenenfalls Vorgaben zu den verwendeten Technologien machen.

Langfristiger Lösungsbeitrag: Für die Kommunikation zu den dann in ihrer Gesamtheit systemnotwendigen Anlagen im Verteilnetz muss so viel Redundanz in der Kommunikationsinfrastruktur vorgesehen werden, dass das Risiko eines für das elektrische Energiesystem bedrohlichen Ausfalls von Kommunikationsanlagen und -strecken auf ein akzeptables Restrisiko gedrückt wird. Diese Redundanz sollte so gestaltet sein, dass dieselbe Ursache nicht auch die redundanten Systeme ausfallen lässt. Zusätzlich sollten die Betreiber einen bestimmten Teil des Kommunikationsnetzes schwarzfallfest aufbauen, indem sie eine eigene unabhängige Stromversorgung etwa auf Basis von Batterien gewährleisten. Dies wird unter anderem nötig sein, um im Falle eines Blackouts den Systemwiederaufbau durch die Netzbetreiber oder auch einen Inselbetrieb zu unterstützen (siehe Handlungsoption 7).

Was kann man heute tun? Durch die Netzbetreiber gilt es, technisch zu bestimmen, welche Teile der Kommunikationsnetze schwarzfallfest sein müssen, welche Zeitdistanzen im Blackout überbrückt werden müssen und welcher Technologiemix sich am besten technisch und ökonomisch dafür eignet. Die BNetzA sollte für das Verfahren, das diese Fragestellungen beantwortet, einen Leitfaden aufstellen, anhand dessen die Netzbetreiber das Vorgehen in der Praxis umsetzen können.

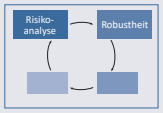
Ein redundantes beziehungsweise schwarzfallfestes Kommunikationssystem gewährleistet auch die im Krisenfall beziehungsweise Blackout notwendige Sprachkommunikation der beteiligten Akteure. Alternativ oder parallel zu privaten Kommunikationssystemen (siehe Abschnitt 3.1.1) sollten öffentliche Kommunikationsnetze in Betracht gezogen werden. Neben dem aktuell diskutierten Mobilfunkstandard CDMA 450 sollten auch weitere zusätzliche Technologieoptionen überprüft werden. Für die Nutzung von öffentlichen Kommunikationsnetzen kann das sogenannte Network Slicing (siehe Infobox Abschnitt 3.1.6 „Virtualisierung“) eingesetzt werden. Hierbei können Betreiber von Kommunikationsnetzen für bestimmte Anwendungen, wie etwa für die Kommunikation im Stromnetzbetrieb, bestimmte Dienstgüte-Qualitätseigenschaften, wie zum Beispiel eine garantierte Mindest-Datenrate, bereitstellen. Der Regulierer muss dazu prüfen, ob und in welchem Umfang es gesetzliche Vorgaben für den Vorrang von Services für das Stromnetz geben kann, um die skizzierte Priorisierung gegenüber anderen Anwendungen zu gewährleisten. Der VDE oder eine Behörde wie die BNetzA sollten wenn notwendig zusätzliche Zertifizierungen einführen.

Bewertung: Ein schwarzfallfester Technologiemix, der auch dezentrale Erzeugungsanlagen einbindet und eine Notversorgung im Inselbetrieb gewährleistet, muss

erst in einigen Jahren angegangen werden und ist derzeit noch Thema der Forschung. Die Entscheidung für oder gegen eine vorrangige oder sogar exklusive Nutzung von Kommunikationstechnologien sollte bald (und sehr sorgfältig) von der Politik getroffen werden, da umfangreiche Investitionen notwendig sind und eine starke Pfadabhängigkeit geschaffen wird. Bezüglich der Vor- und Nachteile des Einsatzes verschiedener Kommunikationstechnologien liegen bereits ausführliche Analysen vor.[260]

Für die Umsetzung der Maßnahmen ist mit höheren Kosten zu rechnen – sowohl für den Aufbau als auch für die Nutzung von Infrastruktur, wobei zwischen der Errichtung einer dedizierten Infrastruktur und der Nutzung öffentlicher Infrastruktur unterschieden werden muss.[261]

Handlungsoption 3:
Akteure zu einer integrierten Betriebsführung der IKT-Systeme und Stromnetze hinleiten



Ergebnis: Ein integriertes Lagebild von Strom- und IKT-Netzen ermöglicht es, Fehlverhalten auf IKT-Seite zu identifizieren, das zu Störungen im Betrieb führen könnte.

Dringlichkeit: ● ● **Wirksamkeit:** ● ●

Was kann man heute tun?

- IKT-Überwachung in Netzleittechnik integrieren.
- Abstimmung der IKT-Statusübertragung zwischen den Akteuren durch Verbände planen und verbindlich abstimmen.

Langfristiger Lösungsbeitrag: Der Status der IKT-Systeme muss in Zukunft in die Betriebsführung elektrischer Netze integriert werden. Zur Lagebeurteilung müssen dem Netzbetreiber auch Monitoringdaten aus IKT-Komponenten übertragen werden, die teilweise anderen Akteuren gehören, etwa Aggregatoren oder vor- und nachgelagerten Netzbetreibern. Die Betriebsführungssysteme der Netzbetreiber und weiterer Akteure, die bei Störereignissen Blackouts zu vermeiden helfen oder bei einem Blackout den Systemwiederaufbau unterstützen, müssen potenzielles Fehlverhalten der IKT-Systeme möglichst frühzeitig erkennen, bewerten und angemessen für nachfolgende Aktionen berücksichtigen. Die Hersteller von Netzleitsystemen müssen diese neuen IKT-Überwachungsfunktionen in ihre Produkte integrieren und so ein integriertes Lagebild aus Energiesystem- und IKT-Systemzuständen erschaffen.

Was kann man heute tun? Im ersten Schritt sollten die ÜNB die Informationen über Kommunikationsstörungen in ihre Leitsysteme integrieren. Diese Informationen sind in der Regel aus ihren Bestandssystemen zum Monitoring der Kommunikationssysteme extrahierbar. Zudem können heute bereits verfügbare Technologien zum System- und Netzwerk-Monitoring in IT-Systemen und Rechenzentren auf die Belange der Betriebsführung von Energiesystemen angepasst und dort eingesetzt werden. Es sollte dann in Stresstests geübt werden, wie diese Informationen im Störfall genutzt werden können (siehe Handlungsoption 6). Dazu könnten etwa Netzbetreiber zunächst anhand definierter Anwendungsfälle in Pilotprojekten die Wirkung erproben. Je nach

260 Siehe etwa EY et al. 2018.
261 EY et al. 2018, S. 103.

Ergebnissen lassen sich durch die Verbände oder VDE/FNN weitere Schritte in drei Richtungen planen:

1. Von hohen zu niedrigeren Spannungsebenen: Die großen VNB der Hochspannungsebene integrieren IKT-Informationen zur Kommunikation analog zu den ÜNB.

2. Von Netzbetreibern zu weiteren Akteuren: Werden Maßnahmen zur Systemsicherung zunehmend von Kommunikationsnetzen abhängig, die nicht der Kontrolle der Netzbetreiber unterliegen und Anlagen wie etwa Windparks steuern, so müssen die Netzbetreiber den Status dieser Kommunikationsnetze ebenfalls berücksichtigen.

3. Vom einzelnen Netzbetreiber zur Kaskade: Um die Systemsicherheit beurteilen zu können, benötigt der Netzbetreiber Informationen, inwieweit nachgelagerte Netze seine Anweisungen ausführen können.

Im nächsten Schritt müssen verbindliche Regeln wie Datenformate und Austauschhäufigkeit für diesen Austausch von IKT-Kenngrößen festgelegt werden – für ÜNB übernimmt diese Aufgabe der Verband ENTSO-E.

Zudem benötigen Netzbetreiber Konzepte für das Nebeneinander von Altsystemen und neuen Komponenten. Energietechnische Komponenten stehen meist sehr lange im Feld – dementsprechend ist weder die Rechenleistung der eingebauten eingebetteten Systeme zeitgemäß, noch sind die gewünschten Softwareinnovationen (zum Beispiel KI-basierte Vorverarbeitungs- und Erkennungsverfahren) auf diesen Systemen lauffähig. Auch wird sich dann veraltete IKT-Technologie im Feld nicht eignen, um bei der Virtualisierung und Auslagerung kritischer Funktionen eine Rolle zu übernehmen (siehe Infobox Abschnitt 3.1.6 „Virtualisierung“). Virtualisierungskonzepte könnten aber zukünftig eine wichtige Rolle in der Systemführung bekommen, indem durch Redundanz ein resilienteres System erzeugt wird: Je nach Situation kann dazu eine IKT-technische Funktion, die eine elektrotechnische Aktion berechnet, auf andere Computer verschoben werden, während die elektrotechnische Aktion auch von verschiedenen Geräten durchgeführt werden kann. Das Vorhandensein von Altsystemen beeinflusst auch die Möglichkeiten, die dem Netzbetreiber für Systemdienstleistungen zur Verfügung stehen – unter anderem, weil die Rechenzeit zur Ausführung von gewünschten Funktionalitäten schlicht zu lang ist. Auch diese Informationen, inwieweit Virtualisierung mit bestehenden Geräten überhaupt möglich oder welche Software lauffähig ist, sollten zukünftig von Herstellern und Betreibern dem Netzbetreiber zur Verfügung gestellt werden.

Bewertung: Der erste Schritt – also die Integration von Informationen, die Aufschluss über die Funktionsfähigkeit der IKT-Systeme geben, in die Leitsysteme und die Betriebsführung – sollte kurzfristig angegangen werden.

Allerdings hat diese erweiterte Betriebsführung nicht nur Vorteile. Durch die zusätzlichen Informationsbereitstellungen wächst die Komplexität der Betriebsführung. Inwieweit dies zur Überforderung des zuständigen Personals oder aufgrund der gesteigerten Komplexität zu neuen Fehlern führen kann, sollte ebenfalls in den Pilotprojekten und Stresstests ermittelt werden.

6.2 Handlungsfeld 2: Cyber-Sicherheit systemisch entwickeln

Problem 2040: Das Risiko, dass von der IT-Seite Störungen auf die OT-Systeme ausgehen und damit große Bedrohungen für das elektrische Energiesystem erzeugen, gewinnt heute und in den nächsten Jahren an Relevanz. Die vermehrte Integration von IKT in das Stromnetz eröffnet neue Angriffsflächen, die frühzeitig im Systemdesign berücksichtigt werden müssen. Dies wird unter dem Begriff Cyber-Sicherheit zusammengefasst, der insbesondere auch das Feld der IT-Sicherheit umfasst (siehe auch Abschnitt 3.1.3). Alle Informationen, die gespeichert und verarbeitet werden, sind potenziell Bedrohungen durch Angriffe, technische oder menschliche Fehler oder Naturereignisse (zum Beispiel Überschwemmung oder Feuer) ausgesetzt.

Erläuterung: Die Sicherheit der OT im elektrischen Energiesystem basierte in der Vergangenheit hauptsächlich auf einer physischen Trennung der OT von den IT-Systemen. Viele OT Systeme wurden daher ursprünglich nicht für eine Anbindung an IT-Systeme konzipiert. Daher wurden die daraus entstehenden Sicherheitsrisiken nicht in ihr Design miteinbezogen. Durch die in Abschnitt 3.1.2 beschriebene IT/OT-Konvergenz entsteht daher eine potenziell neue Angriffsfläche.

Cyber-Angriffe sind eine neue Form der Bedrohung im zukünftigen Stromnetz, die insbesondere durch den Stromausfall in der Ukraine 2015 an Sichtbarkeit gewann.[262] Da es sich um ein europäisches Verbundnetz handelt, können auch Cyber-Angriffe in einem anderen Land zu einem großflächigen Blackout in Deutschland führen. Hinzu kommt, dass im Falle eines Angriffs das System nicht einfach als Notfallmaßnahme abgeschaltet werden kann. Die Funktionalität der KRITIS Strom muss auch bei einem infiltrierten System sichergestellt sein.

Ein Blackout könnte zukünftig auch durch einen Cyber-Angriff auf einen großen Schwarm „kleinerer“ Systeme verursacht werden, die in Massen im Energiesystem verbaut sind (etwa Steuerungsboxen für Photovoltaik-Anlagen oder Elektrogeräte in privaten Haushalten, auf die zukünftig über das Internet zugegriffen werden kann).Doch auch IKT-Systeme außerhalb der Energieinfrastruktur, da über sie sehr viele Geräte angesteuert und somit auch fehlerbedingt lahmgelegt oder sabotiert werden können. Dazu zählen zentrale Serviceplattformen, Smart-Home-Dienste oder Fernwartungsleitstellen von Herstellern, die in der Gesamtheit systemkritisch sein können. Aufgrund der Vielzahl und Vielfalt dieser Systeme und IKT-Komponenten, sind bisherige Cyber-Sicherheitsmaßnahmen für die KRITIS-Energie nicht mehr ausreichend: Erfolgreiche Angriffe auf diese Systeme sind eine Gefahr, für die bisher kaum Abwehrmaßnahmen existieren.

Der „Feind“ sitzt dabei oft im System selbst, in Form von Sicherheitslücken oder sogenannten „Hintertüren“ (auch Backdoors genannt), über die der Zugriff auf Computersysteme auch ohne die normalen Zugriffsrechte möglich ist (siehe Abschnitt 3.1.3). Über die so geschaffenen Zugänge können aufgrund der IT/OT-Konvergenz auch Gefahren für die Stromnetze entstehen.

262 Whitehead et al. 2017.

Cyber-Sicherheit kann niemals durch rein technische Lösungen erreicht werden. Im Gegenteil: Sich auf technische Lösungen zu verlassen, führt zu einem falschen Sicherheitsgefühl und erhöht sogar die Vulnerabilität. Die für die IKT-Systeme Verantwortlichen müssen daher technische und organisatorische Maßnahmen in ihren Prozessen kombinieren. Auch die Lernkurve bei neuen Technologien muss berücksichtigt werden: Die in der Branche tätigen Mitarbeiterinnen und Mitarbeiter sind in der Regel entweder Fachleute für IT oder Elektroingenieure, haben aber nur selten ein kombiniertes Wissen, das auch Cyber-Sicherheit beinhaltet.

Sicherheit und Innovation müssen außerdem gegeneinander abgewogen werden: Träge und umständliche Verfahren bergen nicht nur die Gefahr von Effizienzverlusten, sondern auch von verringerter Sicherheit. Ein aktuelles Beispiel hierfür ist die Verzögerung des flächendeckenden Smart Meter Rollout aufgrund der Standardisierungsverfahren: Durch das Fehlen einer wichtigen Infrastruktur besteht die Gefahr, dass sich unregulierte und damit weniger sichere Behelfslösungen etablieren.

Zeithorizont des Problems: Die beschriebene Problematik entwickelt sich parallel zur Digitalisierung des Systems. Da die Entwicklung und Umsetzung entsprechender Gegenmaßnahmen jedoch Zeit braucht, sollten sie bereits jetzt verstärkt mitberücksichtigt werden.

Heute bereits bestehende Maßnahmen: Im deutschen IT-Sicherheitsgesetz werden umfangreiche Regelungen für die Betreiber von Energieversorgungsnetzen und Energieanlagen festgelegt, die zur kritischen Infrastruktur zählen (siehe Infobox Abschnitt 2.3 „Kritische Infrastruktur elektrische Energieversorgung“). Die Betreiber dieser Infrastrukturen werden durch das IT-Sicherheitsgesetz und das EnWG dazu verpflichtet, „angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen“.[263] Für ÜNB ist zusätzlich durch die EU-Verordnung 2017/1485 (2017) „zur Festlegung einer Leitlinie für den Übertragungsnetzbetrieb“ vorgeschrieben, dass ein Sicherheitsplan erstellt werden muss, der explizit neben physischen Bedrohungen auch Cyber-Bedrohungen berücksichtigt. Dabei wird jedoch nicht genauer spezifiziert, welche Art von Cyber-Bedrohungen berücksichtigt werden sollen oder wie ein solcher Sicherheitsplan aussehen könnte. Mit den „Richtlinien zur IT-Sicherheit und Resilienz für die Smart-Energy-Einsatzumgebung“ zielt der VDE insbesondere auf Unternehmen, die für kritische Infrastrukturen zuständig sind.[264]

Die europäische Expertengruppe Smart Grid Task Force Expert Group 2 hat in ihrem Abschlussbericht[265] Empfehlungen an die Europäische Kommission zur Umsetzung sektorspezifischer Regeln im Energiebereich für IT-Sicherheit veröffentlicht. Dieser „Network Code on Cybersecurity“ richtet sich an alle Netzbetreiber (ÜNB und VNB) mit dem Ziel, das Stromnetz gegen aktuelle und zukünftige Cyber-Risiken abzusichern. Es wird unterschieden zwischen einem Basisschutz für alle Netzbetreiber und einem erweiterten Schutz für solche, die als „Betreiber wesentlicher Dienstleistungen“ klassifiziert werden.

263 EnWG 2020, § 11 Absatz 1a bis 1c.

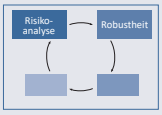
264 VDE 2019.

265 Vgl. SGTF EG2 2019.

Der Basisschutz umfasst die Einrichtung eines Information Security Management System nach ISO/IEC 27001:2013 sowie die Umsetzung des EU Cybersecurity Act.[266] Der erweiterte Schutz ergänzt diese Maßnahmen um den Schutz der bestehenden Infrastruktur, einen Risikomanagementprozess in der Lieferkette der verwendeten Hard- und Software, Schutz vor grenz- und organisationsübergreifenden Risiken und Teilnahme an einem Frühwarnsystem. Zur Unterstützung der Netzbetreiber werden hierfür sektorspezifische Anleitungen zum Thema Krisenmanagement und Schutz der Lieferkette vorgeschlagen. Außerdem soll ein Reifegradmodell zur Bewertung und Steuerung der Umsetzung von IT-Sicherheitsmaßnahmen entwickelt werden. Die konkrete Umsetzung dieser Empfehlungen ist jedoch noch unklar. Außerdem basiert die Teilung in Basis- und erweiterten Schutz auf der Annahme, dass kleine und mittlere Netzbetreiber in der Regel nicht über die Ressourcen und Fähigkeiten verfügen, um die Cyber-Sicherheit in gleicher Weise anzugehen wie Netzbetreiber, die eine große Region und eine beträchtliche Anzahl von Verbrauchern abdecken. Durch die zunehmende Digitalisierung in den Verteilnetzen werden aber auch kleine Netzbetreiber relevant. Zudem richtet sich der Network Code nur an Netzbetreiber, während andere Akteure nicht berücksichtigt werden.

Es existieren bereits verschiedene Stellen und Notfallteams für Cyber- und IT-Sicherheit. Eine zentrale Stelle ist der **Computer-Emergency-Response-Team(CERT)-**Bund. Ein CERT ist im Allgemeinen eine Gruppe von Fachkräften, die sich um IT-Sicherheitsvorfälle kümmern. Sie übernehmen in der Regel präventive und reaktive Aufgaben, das heißt das Erkennen und Vermeiden von Angriffen, Vorfällen oder Sicherheitslücken beziehungsweise das Reagieren auf Angriffe und Vorfälle sowie das Beheben oder Vermeiden von Schäden. Das CERT-Bund ist in erster Linie für die IT-Systeme der Bundesbehörden verantwortlich. Es sammelt Informationen zu Sicherheitsvorfällen in Bezug auf IT-Systeme in Deutschland.[267] Der Fokus liegt jedoch nicht nur auf der KRITIS Energie, sondern allgemein auf Cyber-Angriffen auf Informationsinfrastrukturen. Zudem ist die personelle Ausstattung völlig unzureichend.

Handlungsoption 4: Cyber-Sicherheitsstandards für alle Blackout-relevanten Akteure einführen



Ergebnis: Sowohl kleinere als auch branchenfremde Akteure werden bei Cyber-Sicherheitsvorschriften im Sinne der BSI-KritisV berücksichtigt – möglichst europäisch abgestimmt. Diese Vorschriften werden innovationsfreundlich gestaltet.

Dringlichkeit: ● ● ● **Wirksamkeit:** ● ●

Was kann man heute tun?

- Risikoszenarien als Grundlage für Vorschriften definieren und relevante Akteure identifizieren.
- Kleine Netzbetreiber gegen gleichzeitige Angriffe schützen.
- Sicherheitsvorschriften für relevante dritte Akteure anpassen.

266 Verordnung (EU) 2019/881.

267 Vgl. BSI 2018, S. 54.

Langfristiger Lösungsbeitrag: Neben dem bisherigen Fokus der Security-Maßnahmen auf die in der BSI-Kritis-Verordnung beschriebenen Akteure, muss die systemische Gefährdung durch Sicherheitsvorfälle stärker in den Blick rücken, die sowohl kleinere Akteure als auch branchenfremde Akteure und grenzübergreifende Vorfälle einschließt. Soweit möglich sollte dies europäisch harmonisiert geschehen, allein um im Krisenfall auch im europäischen Verbundnetz gleiche Begrifflichkeiten und Definitionen für Notfallmaßnahmen, Systemstatus oder Schranken für kritische Systemmesswerte zu haben. Zudem sollten die Standards als erster Schritt in nationales Recht umgesetzt werden, da die Umsetzung auf europäischer Ebene potenziell mehr Zeit in Anspruch nimmt.

Neben den Unternehmen der Wertschöpfungskette Energie haben weitere Akteure des Energiesektors einen unmittelbaren Einfluss auf die Resilienz. Diese sind bisher nicht von den gesetzlichen Regelungen (EnWG, Anschlussregeln, BSI Sicherheitsgesetz etc.) zur Resilienz betroffen. Auch die Verbraucherseite „hinter dem Zähler" gewinnt in Zukunft an Relevanz, für die es bisher wenige Regulierungen bezüglich der Cyber-Sicherheit gibt. Eine Einbeziehung etwa durch geeignete Verpflichtungen oder Sicherheitsauflagen ist daher sinnvoll. Die Umsetzung der Verpflichtungen sollte von einer dafür verantwortlichen Stelle überprüft werden.

Die notwendigen vorgeschriebenen Sicherheitsmaßnahmen sind jeweils so zu gestalten, dass Innovationen nicht ausgebremst oder unterbunden werden. Die Energiewende und das Erreichen der Klimaschutzziele der Bundesregierung benötigen viele Innovationen, gerade auch im Bereich der Netzdienlichkeit (siehe Basisursache 1, Abschnitt 4.1) und im Bereich der digitalen Geschäftsmodelle. Besonders Letztere müssen sich schnell durchsetzen können und benötigen kurze Veröffentlichungszyklen, sodass mit den Erfahrungen der Konsumentinnen und Konsumenten das Produkt sukzessive verbessert wird. Es sind also Verfahren zu verwenden, die hohe Datenschutzanforderungen und Transparenz der Datennutzung gewährleisten und gleichzeitig mit dem hohen Innovationstempo digitaler Innovationen mithalten können.

Was kann man heute tun?

Risikoszenarien als Grundlage für Standards definieren und relevante Akteure identifizieren. Um Maßnahmen zur Stärkung der Cyber-Sicherheit zu entwickeln, gilt es zunächst zu definieren, gegen welche Risiken man sich schützen will. Die Smart Grid Task Force Expert Group 2 schlägt hierfür vor, all jene Cyber-Risikoszenarien zu ermitteln, die auf der Incident Classification Scale[268] von ENTSO-E zu einem Notfallzustand (Level 2) oder Blackout (Level 3) führen können. Diese Szenarien beziehen sich jedoch nur auf ÜNB auf europäischer Ebene und sollten auch für VNB auf deutscher Ebene sowie weitere relevante Akteure (siehe S.112) definiert werden. Insbesondere sollten auch Szenarien mit spieltheoretischen Ansätzen betrachtet werden: Spieltheorie behandelt Entscheidungssituationen, bei denen sich die Beteiligten durch ihre Aktionen gegenseitig beeinflussen und daher immer die Aktionen des jeweiligen „Spielgegners" voraussehen müssen. Durch die vielen kleinen, steuerbaren Erzeugungs- und Verbrauchsanlagen kann ein Angreifer mit der Physik des Stromnetzes „spielen" und beispielsweise durch gezieltes An- und Ausschalten eine Störung bis hin zu einem Blackout verursachen. In den Risikoszenarien sind daher auch geeignete Richtwerte für eine „kritische Masse" zu ermitteln. Diese Szenarien können insbesondere dabei helfen,

268 ENTSO-E 2018.

„Security by Design“ zu realisieren, das heißt Cyber-Sicherheit bereits beim Design neuer Lösungen und Systeme zu berücksichtigen.

Bewertung: Da es sich bei der vorgeschlagenen Maßnahme um die Grundlage für sinnvoll definierte Standards handelt, sollte mit der Umsetzung zeitnah begonnen werden. So könnte eine schnellere, einheitliche, verbundnetzweite Standardisierung erzielt werden.

Die zukünftige Bedeutung kleiner Netzbetreiber bezüglich Cyber-Sicherheit berücksichtigen

In dem zukünftigen digitalisierten Energiesystem werden auch kleinere Netzbetreiber – sogar mit weniger als 100.000 angeschlossenen Kunden[269] – potenziell interessant für einen Cyber-Angriff. Dies ist insbesondere der Fall, wenn eine größere Anzahl dieser Netze zur gleichen Zeit manipuliert werden kann, da zum Beispiel vergleichbare Software, vergleichbare Infrastruktur und vergleichbare Verfahren der Cyber-Sicherheit eingesetzt werden. Daher sollte bei der Erstellung von Standards auch das Risiko berücksichtigt werden, dass durch die Übernahme gleicher Systeme von vielen kleinen Netzbetreibern ein großer Blackout herbeigeführt wird.

Eine Option wäre, die BSI-Kritis-Verordnung so anzupassen, dass auch kleinere Leistungsmengen berücksichtigt werden. Dadurch würden auch Anlagen im Besitz kleiner Netzbetreiber zur kritischen Infrastruktur zählen und wären dementsprechend zu technischen Mindeststandards für die Sicherheit sowie Meldung von Störungen verpflichtet. Dabei sind die Richtlinien und Zertifizierungsprozesse immer so anzupassen, dass deren Einhaltung beziehungsweise Umsetzung für diese kleinen Netzbetreiber handhabbar und effektiv ist. Die Umsetzung dieser Maßnahmen ist regelmäßig durch eine zentrale Stelle zu prüfen.

Bewertung: Die Umsetzung der Maßnahme ist mittelfristig möglich. Zertifizierungsprozesse geben immer nur den aktuellen Stand wieder und garantieren keine Fehlerfreiheit, weswegen die Effektivität regelmäßig evaluiert werden sollte. Es kann sich Widerstand seitens der kleinen Versorger gegen eine möglicherweise eingeschränkte Handlungsautonomie entwickeln, wenn diese nicht ausreichend in die Konzeption der Maßnahmen eingebunden werden. Im Zuge der Umsetzung der Maßnahme fallen Zertifizierungskosten an. Für ÜNB wurden Kosten bereits beziffert: Industrie- und Regulierungsempfehlungen für die Cyber-Sicherheit im europäischen Energiesektor wurden in einer von der Europäischen Kommission beauftragten Studie beschrieben und würden bei Umsetzung die Stromrechnung der Endverbraucherinnen und Endverbraucher im Durchschnitt um weniger als 0,2 Prozent erhöhen.[270]

Sicherheitsstandards für relevante dritte Akteure anpassen

In Zukunft müssen auch dritte Akteure in der Standardisierung berücksichtigt werden, die eine Kommunikationsverbindung zu Erzeugungsanlagen und Geräten haben.

Laut BSI-Kritis-Verordnung zählt auch eine „Anlage oder System zur Steuerung/Bündelung elektrischer Leistung“ ab einer Größe von 420 Megawatt zur KRITIS. Es muss geprüft werden, ob dieser Grenzwert herabgesetzt werden muss. Außerdem sollte geprüft werden, ob Plattformen in der BSI-Kritis-Verordnung berücksichtigt werden

269 Einteilung entsprechend dem EnWG 2020.

270 Fischer et al. 2019.

sollten – und wenn ja, welche. Ein Kriterium könnte sein, ob eine systemrelevante große Menge an Verbrauchs- oder Erzeugungsanlagen über die Plattform steuerbar ist. Beides kann mithilfe der Risikoszenarien geschehen.

Die Hersteller der zuvor genannten Erzeugungsanlagen und Geräte müssen ebenfalls über geeignete Standards eingebunden werden. Idealerweise gelangen Produkte mit gravierenden Sicherheitslücken gar nicht erst auf den Markt. Als organisatorischer Rahmen könnte hier die VDE-Standards-4100- und 4105-Reihe[271], die Netzanschlussregeln für Bezugs- und Erzeugungsanlagen im Niederspannungsnetz beschreibt, um Cyber-Sicherheitsaspekte ergänzt werden. Durch geschickte Wahl der Anlageneinstellungen (zum Beispiel Fernsteuerbefehle werden nur umgesetzt, wenn bestimmte elektrische Parameter innerhalb gewisser Grenzen liegen) kann ein preiswertes und äußerst robustes Gesamtsystem erreicht werden. Die tatsächliche Einhaltung der Standards sollte regelmäßig überprüft werden.

Bewertung: Die Umsetzung der vorgeschlagenen Maßnahme sollte mittelfristig erfolgen. Eine einheitliche Standardisierung kann jedoch aufgrund der großen Anzahl heterogener Betroffener schwierig werden und ist zudem zeitintensiv.

Die Maßnahme wird als sehr effektiv eingeschätzt, da die Angriffsfläche für Cyber-Angriffe verringert wird. Die Anlagen und Geräte werden nachhaltig robuster. Der Aufwand für die Umsetzung ist gering, falls es sich um Neuanlagen handelt. Im Fall von Bestandsanlagen wird die Umsetzung jedoch schwierig, da Bestandsschutz besteht: Bei nachträglicher Änderung der Rahmenbedingungen und Vorgaben müssen diese in den Geräten nicht umgesetzt werden.

Durch die Einheitlichkeit der Standardisierung können potenzielle Sicherheitslücken besser erkannt werden. Die Kosten werden eher gering bis mittelhoch ausfallen, da die Anforderungen recht einfach sind und entsprechende Standardbauelemente mit einer gesetzlichen Verpflichtung schnell verfügbar sein werden.

Einen sukzessiven, rollierenden Prozess zur Erstellung von Sicherheitsvorgaben aufbauen

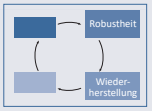
Innovationen würden durch einen sukzessiven, rollierenden Prozess nach dem jeweils aktuellen Sicherheitsstandard auf den Markt gehen, und Veränderungen an diesem Standard können in späteren Versionen verwirklicht werden. Zugleich müssen hohe Datenschutzanforderungen erfüllt werden. Zertifizierungen könnten an am Markt tätige Unternehmen delegiert werden, die dann als Prüfinstanzen zertifiziert würden (angelehnt an den Kraftwerkssektor). Die Einführung der Sicherheitsstandards und Zertifizierungen sollte zeitnah durch das BSI und in enger Zusammenarbeit mit der BNetzA durchgeführt werden, da nur diese die Bedeutung für die Resilienz einschätzen kann. Dabei ist es wichtig, Standards und Prozesse auf europäischer Ebene zu etablieren. Es ist für Hersteller in der Regel nicht attraktiv, Produkte nur auf den deutschen Markt zugeschnitten zu entwickeln. Ob Deutschland in bestimmten Fällen als Leitmarkt Vorreiter sein kann, ist genau zu prüfen und dann entsprechend zu berücksichtigen.

Bewertung: Die vorgeschlagene Maßnahme sollte kurzfristig umgesetzt werden. Da zunehmend digitale Geschäftsmodelle in den Markt gehen und Zertifizierungsprozesse eine Lernkurve brauchen, ist eine späte (in mehr als fünf Jahren) Einführung

271 Vgl. VDE|FNN 2019-3.

der Standards und Zertifizierungen risikoreich. Ein Vorteil wäre insbesondere, dass Zertifizierung und Regulierung mit Marktzyklen synchronisiert werden können. Die Maßnahme könnte bei den Regulierern beziehungsweise den verantwortlichen Ministerien auf Widerstand stoßen, da in einem rollierenden Prozess der aktuellste Sicherheitsstandard nicht immer – jedoch schnellstmöglich – umgesetzt sein muss. Die zeitliche Abfolge zwischen Erlassen eines neuen Sicherheitsstandards und dessen Umsetzung muss angemessen schnell ablaufen: Beispielsweise ist es nicht akzeptabel, einen Sicherheitspatch ein halbes Jahr wegen der Prozesse zu verzögern.

Handlungsoption 5:
Maßnahmen zum Umgang mit Sicherheitslücken definieren



Ergebnis: Es gibt möglichst wenige Blackout-relevante Cyber-Sicherheitslücken und auf Sicherheitsvorfälle kann schnell reagiert werden.

Dringlichkeit: ● ● **Wirksamkeit:** ● ● ●

Was kann man heute tun?

- Risiko aus staatlich gewollten Sicherheitslücken verringern.
- Risiko aus Sicherheitslücken in systemkritisch eingesetzten Produkten reduzieren.
- OT gegen IT-Fehler absichern.
- Europäisch organisierte Notfallteams zur Unterstützung im Fall von Cyber-Angriffen einsetzen.

Langfristiger Lösungsbeitrag: Oberstes Ziel sollte es stets sein, sichere Software zu produzieren und jede Sicherheitslücke so bald wie möglich nach ihrem Entdecken zu schließen. Auch mit ausreichender Standardisierung kann es zu Sicherheitslücken in der Software kommen, entweder durch Fehler in der Software oder aufgrund von Hintertüren. Daher braucht es im Angriffsfall Expertengruppen, die in der Lage sein müssen, schnell einzugreifen, um das System wiederaufzubauen.

Es ist unwahrscheinlich, dass der Trend der IT/OT-Konvergenz grundsätzlich verhindert werden kann. Stattdessen ist ein gemeinsamer Security-Ansatz notwendig, der beide Bereiche berücksichtigt. Ein wichtiges Designprinzip sollte zwar die klare Trennung zwischen IT, auf die über das Internet zugegriffen werden kann, und sicherheitskritischen Systemen sein, jedoch ist dies in einem zukünftigen Stromnetz nicht immer umsetzbar: Durch die zunehmende Vernetzung der Geräte (IoT, Smart Home, Cloud-Dienste) werden auch Bereiche potenziell sicherheitskritisch, die sich außerhalb der Kontrolle der Netzbetreiber befinden.

Was kann man heute tun?

Angriffsfläche aus Sicherheitslücken verringern

Sollten sich staatliche Stellen Zugangswege auf IKT-Komponenten offenhalten und Werkzeuge wie den „Staatstrojaner“ oder Software zur „aktiven Cyberabwehr“[272] herstellen, sollte dies immer auch ausführlich gegen die Gefahr für die KRITIS Energie abgewogen werden. Zwischen der Veröffentlichung der Sicherheitslücken und der

272 IKT-Werkzeuge, um in fremde Rechner einzudringen und dort Daten und Programme zu manipulieren und zu löschen. Solche Maßnahmen sind an sich hochumstritten. Die ethische, technische oder juristische Bewertung solcher Maßnahmen ist jedoch nicht Thema dieser Analyse.

vollständigen Geheimhaltung müssen Kompromisslinien gefunden werden. Der Abwägungsprozess sollte transparent sein. Eine Begleitung und Aufbereitung durch eine vom Innenministerium unabhängige Stelle würde die Qualität der Maßnahme voraussichtlich verbessern.

Um Sicherheitslücken in IKT-Komponenten einzelner Hersteller, die im Umfeld der Energieversorgung eingesetzt werden (dazu zählen sowohl eingebettete Systeme von Erzeugungsanlagen als auch Komponenten der Kommunikationsinfrastruktur), nicht zum Risiko werden zu lassen, gibt es verschiedene Möglichkeiten.

Zum Teil wird gefordert, Hersteller ganz aus der KRITIS auszuschließen, weil man annimmt, dass die Herstellerländer den Einbau von Hintertüren anordnen könnten. Die Bewertung einer solchen Option ist jedoch schwierig: Die politischen Auswirkungen solcher Maßnahmen, unter anderem auf das globale Handelssystem, sind schwer abschätzbar. Zudem ist die Effektivität eines solchen Ausschlusses aus technischer Sicht zweifelhaft: Bisher ist es hochspezialisierten, vom Staat finanziell gut ausgestatteten Teams immer gelungen, erfolgreich in komplexe IKT-Systeme einzudringen, auch ohne staatlich verordnete Schwachstellen. Außerdem sind die Lieferketten für IKT-Komponenten sehr komplex, sodass nicht immer genau definiert werden kann, was die nationale Herkunft einer Komponente ist. Doch gibt es andere Optionen:

Zum einen können die Hersteller verpflichtet werden, den Quellcode vertraulichen staatlichen Prüfstellen offenzulegen, wie es etwa in Großbritannien für den Hersteller Huawei bei der Errichtung des Mobilfunknetzes vorgeschrieben wurde.[273] Außerdem könnte die Ausrüstung besonders kritischer Kernbereiche der Kommunikationsnetze ausgewählten europäischen Herstellern vorbehalten bleiben. Denn die Wahrscheinlichkeit eines Angriffs auf sicherheitskritische Infrastrukturen innerhalb der EU durch ein heutiges EU-Mitglied gilt auch auf mittlere Sicht als extrem unwahrscheinlich.

Zum anderen sollte es nicht zu einer Abhängigkeit von einzelnen Herstellern kommen: Der Wechsel des Herstellers muss in überschaubarer Zeit möglich sein, falls anzunehmen ist, dass dieser ein Sicherheitsrisiko darstellt. Eine nach Herstellern diversifizierte Infrastruktur ist ebenfalls eine Möglichkeit, um Abhängigkeiten zu vermeiden und das Risiko durch einzelne Hersteller zu verringern. Hierfür müsste eine Vorschrift erlassen werden, dass Betreiber von KRITIS-IKT-Infrastrukturen jede kritische Funktion jeweils mit Komponenten verschiedener Hersteller ausführen müssen. Darüber hinaus könnten besonders kritische Komponenten durch unterschiedliche Hersteller redundant ausgelegt werden.

Bewertung: Bei der Umsetzung der vorgeschlagenen Maßnahmen handelt es sich um einen kontinuierlichen und langen Prozess, der die Angriffsfläche für Attacken erheblich reduzieren kann. Durch die Möglichkeit, Einblick in den Quellcode zu bekommen, kann eine hohe Qualität sichergestellt werden. Dennoch wird auch eine solche Prüfstelle nicht jede Sicherheitslücke finden können. Zudem besteht das Risiko, dass staatliche Stellen diese Informationen auf problematische Weise nutzen, ohne demokratischer Kontrolle zu unterliegen. Eine besondere Herausforderung für solche Stellen ist auch die Ausstattung mit geeigneten Expertinnen und Experten.

273 Katwala 2019.

Fraglich ist außerdem, welche unabhängige Stelle eine Überprüfung des Quellcodes vornehmen sollte. Eine Behörde, die dem Innenministerium unterstellt ist, hätte einen Interessenkonflikt mit Sicherheitsbehörden und Geheimdiensten. Die nötige Neutralität wäre deshalb zweifelhaft. Durch diese Behörde würden überdies hohe Kosten entstehen. Die Politik müsste diese Kosten also dem möglichen Schaden gegenüberstellen, aber auch dem Nutzen für die Resilienz, der durch diese Sicherheitsaudits entsteht.

Ein durch die Diversifizierung der Hersteller entstehender heterogener „Gerätezoo" ist zwar effektiv bezüglich der Resilienz des Stromnetzes, schafft jedoch auch wieder mehr Komplexität und dadurch neben erhöhten Kosten auch neue Vulnerabilitäten.

OT gegen IT-Fehler absichern

Da es nicht möglich ist, eine vollständige Absicherung der IT-Seite gegen Cyber-Angriffe oder auch Softwarefehler zu erreichen, muss die Absicherung auf OT-Seite stattfinden. Hier sind verschiedene Optionen denkbar. Beispielsweise könnte eine Systemarchitektur implementiert werden, bei der zwischen Grundfunktionalitäten, die systemstabilisierende Komponenten beinhalten, und erweiterten Funktionalitäten unterschieden wird. Während die Grundfunktionalitäten nicht von außen geändert werden sollten, wäre dies bei den erweiterten Funktionalitäten möglich. So bleiben systemkritische OT klar von IT getrennt und dadurch geschützt.

Eine weitere Möglichkeit wäre, im Normalbetrieb zwar die Vorteile der IT/OT-Konvergenz zu nutzen, jedoch Rückfalllösungen zu implementieren, die im Falle eines Problems auf IT-Seite eine Trennung der beiden Bereiche ermöglichen: Die OT muss so gestaltet sein, dass sie auch dann funktionstüchtig ist, wenn die IT ausfällt. Hier bedarf es risikobasierter Ansätze, die gemeinsam von Security- und Energieexpertinnen und -experten entwickelt werden. Es sind konkrete Umsetzungsmöglichkeiten zu entwickeln, zu erproben und zu bewerten.

Bewertung: Eine Umsetzung ist mittelfristig möglich, da IT/OT-Systeme momentan langsam zusammenwachsen und die Schnittstellen noch unklar sind. Es ist fraglich, ob die OT ohne die Marktkommunikation auf IT-Seite zukünftig überhaupt sinnvoll funktionieren kann. Die Kosten sind nicht unerheblich, denn der alleinige Betrieb der OT losgelöst von der IT müsste in jedem Umsetzungsszenario separat getestet werden. Zudem ist es möglich, dass das Umschalten auf den OT-Betrieb durch entsprechende Angriffe gezielt ausgelöst werden kann. Damit wäre es trotz der Trennung von IT und OT möglich, wirtschaftliche Schäden zu provozieren. Der Nachweis der Effektivität der Trennung kann nur durch Tests in den einzelnen Infrastrukturen selbst geführt werden. Man sollte sich aber im Klaren sein, dass nicht alle Angriffsszenarien abgedeckt werden können. Der erfolgreiche Stuxnet-Angriff im Jahr 2010 erfolgte etwa auf ein physikalisch abgetrenntes System.[274]

Schnelle Notfallteams für Cyber-Vorfälle initiieren

Um insbesondere bei gravierenden Cyber-Sicherheitsvorfällen schnell und richtig zu handeln, bedarf es eines Notfallteams – einer Gruppe aus europäisch organisierten Expertinnen und Experten speziell für das elektrische Energiesystem, die jederzeit zur Verfügung stehen und angegriffene Unternehmen mit Expertise unterstützen. Diese Sicherheitsspezialistinnen und -spezialisten müssen dementsprechend umfangreiches und detailliertes Wissen über das Stromversorgungssystem mitbringen und das System

274 Vgl. Langner 2011.

sowohl elektrotechnisch als auch informations- und kommunikationstechnisch verstehen. Eine zentrale Stelle, wie in Handlungsoption 14 beschrieben, sollte diese Teams unterstützen; sowohl in Echtzeit bei Vorfällen als auch zur späteren Analyse.

Ein Organ ähnlich CERT auf europäischer Ebene gibt es bisher nicht. Die EECSP-Expert Group empfiehlt hierfür ein Regelwerk für die regionale Zusammenarbeit der CERT-Gruppen im Energiebereich, das von der Europäischen Kommission in Zusammenarbeit mit den Mitgliedstaaten erstellt werden soll.[275]

Bewertung: Ein großer Vorteil wäre, dass schnell auf Cyber-Sicherheitsvorfälle in der Energieversorgung reagiert werden kann, um so gegebenenfalls großen Blackouts vorzubeugen. Andererseits sollte darauf geachtet werden, dass dabei keine „Wissensinseln" entstehen, sondern die Expertise und das Wissen geeignet verteilt werden. Auch müssen das Personal und der Nachwuchs gesichert werden. Um die Akzeptanz eines solchen Notfallteams zu erhöhen, sollte es sich um eine unabhängige Instanz handeln.

6.3 Handlungsfeld 3: Technische Resilienz durch Netzbetreiber und Netznutzer stärken

Problem 2040: Die Umbrüche im elektrischen Energiesystem, etwa durch dezentrale Erzeugungsanlagen und neue Akteure, sorgen potenziell für mehr Überraschungen im Betrieb der Netze, die die Resilienz bedrohen und sich von bisherigen Störereignissen sehr unterscheiden können.

Erläuterung: In einem technisch hochkomplexen System, wie es die Basisursache 3 (siehe Abschnitt 4.3) beschreibt, können die Netzbetreiber sehr viel schwerer als heute prognostizieren, was in ihren Netzen passieren wird. Die Netzbetreiber werden einen Teil ihrer „Gestaltungshoheit" verlieren: Es wird möglicherweise genossenschaftliche oder kommunale Strukturen geben, die eigene Energienetze mit lokalen Energiemanagementkonzepten jenseits der heutigen energiewirtschaftlichen Akteure realisieren. Zugleich haben die Netzbetreiber in einem von dezentraler Erzeugung geprägten System kaum noch die Möglichkeit, große Kraftwerke mit ihren rotierenden Massen zur Frequenzstabilisierung zu nutzen. Auch werden die Verteilnetze viel näher als heute an den physikalisch-technischen Belastungsgrenzen betrieben, in ihrer Komplexität zunehmend schwerer handhabbar und daher durch eine weit (pro-)aktivere und anspruchsvollere Netzführung und zunehmende Automatisierung geprägt sein.[276] Einerseits hat also der einzelne VNB in sehr viel höherer Frequenz als heute Maßnahmen zur Stabilisierung des eigenen Netzes durchzuführen und muss dabei auf eine deutlich erhöhte Kleinteiligkeit und Diversität neuer Akteure reagieren. Andererseits werden sich die Netzbetreiber viel häufiger als heute gegenseitig bei der Systemstabilisierung unterstützen müssen. Resilienz muss daher deutlich mehr von der technischen Unterstützung durch Betreiber kleiner Erzeugungsanlagen, Speicher und flexibler Verbrauchsanlagen profitieren und durch Netzbetreiber der unteren Spannungsebenen aufrechterhalten werden.

275 EECSP 2017.

276 So zählte der Netzbetreiber EWE Netz GmbH nach eigener Aussage im Jahr 2010 noch 100 Eingriffe in die Netzeinspeisung, im Jahr 2019 werden es voraussichtlich deutlich über 4.000 sein.

Zeithorizont des Problems: Es ist schwer zu bestimmen, wann neuartige Probleme auftreten. Daher seien hier einige Indikatoren angegeben, die die Dringlichkeit verdeutlichen, sich zügig auf mögliche Überraschungen vorzubereiten:

- Leistungsmenge und Anzahl der über das Internet steuerbaren Erzeugungs- und Verbrauchsanlagen nehmen zu.
- Es entwickeln sich digital basierte Geschäftsmodelle, die bei großer Durchdringung einen Einfluss auf Last-/Verbrauchskurven haben.
- Das große Engagement von Privatakteuren, durch eigene Beiträge direkt zur Energiewende beizutragen, führt zu Entwicklungen, die die Resilienz gefährden könnten (siehe auch Infobox Abschnitt 2.2 „Steckbare Solargeräte, Balkonkraftwerk, Solar-Rebell oder Guerilla-PV“).

Heute bereits bestehende Maßnahmen: Deutschland hat eine der sichersten Stromversorgungen der Welt. Dies liegt an einem umfangreichen Maßnahmenkatalog, der nicht nur die Pflichten und Rechte der Netzbetreiber, sondern auch die Pflichten weiterer Akteure wie der Betreiber von Einspeise- und Verbrauchsanlagen umfassend regelt. Zunehmend ergänzen Gesetzgeber diese Maßnahmen um Vorschriften für kleinere Erzeugungsanlagen, damit diese keine Gefahr für die Systemsicherheit darstellen. Auch auf europäischer Ebene verbessern die ÜNB permanent die Absicherung gegen große Stromausfälle.

Da das Geschehen auf Verteilnetzebene zunehmend eine Rolle für die Systemsicherheit spielt, ist die Zusammenarbeit der Netzbetreiber der verschiedenen Spannungsebenen mehr in den Vordergrund gerückt. Dazu wurde 2017 etwa vom VDE eine Anwendungsregel[277] veröffentlicht, die die Zusammenarbeit aller Netzbetreiber standardisiert und ein zehn Jahre älteres Regelwerk[278] ersetzt. Auch auf europäischer Ebene werden von ENTSO-E und den Verbänden der VNB Vorschläge und Maßnahmen erarbeitet, das Zusammenspiel der Netzbetreiber und weiterer Akteure neuen Gegebenheiten – insbesondere den Veränderungen auf der Marktseite und der dezentralen Erzeugung – anzupassen.

Durch das Gesetz zur Digitalisierung der Energiewende[279] wird durch das Ausrollen der Smart Meter in den Verteilnetzen eine Kommunikationsinfrastruktur errichtet werden, um mit dezentralen Erzeugungs- und Verbrauchsanlagen sicher Informationen austauschen zu können.

Die großen Netzbetreiber haben Krisenpläne für ausgewählte Szenarien (Cyber-Angriff, Sonnenfinsternis, Telekommunikationsausfall etc.) vorliegen und üben diese regelmäßig, um das operative Verhalten und die Prozesse in derlei Ausnahmefällen proben und entwickeln zu können. Ein bereits bestehendes Trainingscenter ist zum Beispiel das CyberRange-e von Westenergie,[280] in dem auch für andere Energieversorger und Netzbetreiber unter realen Bedingungen die Effektivität der vorhandenen Abwehrprozesse analysiert, getestet, trainiert und optimiert werden kann.

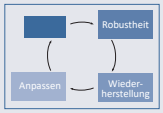
277 VDE-AR-N 4140 Anwendungsregel: 2017-02 „Kaskadierung von Maßnahmen für die Systemsicherheit von elektrischen Energieversorgungsnetzen“.

278 Vgl. VDN 2007.

279 Deutscher Bundestag 2016.

280 Trainingscenter CyberRange-e der Innogy SE, vgl. Westenergie 2020.

Handlungsoption 6: Digitalisierung der Stromnetze voranbringen



Ergebnis: Die Netzbetreiber haben deutlich mehr Möglichkeiten zur Systemstützung durch eine umfangreiche Digitalisierung, neue Prozesse sowie regelmäßige, resilienzorientierte Trainings.

Dringlichkeit: ● ● ● **Wirksamkeit:** ● ● ●

Was kann man heute tun?

- Kriterien für die technische Ausstattung – auch für kleine Netzbetreiber – und den Informationsaustausch für den proaktiven Systembetrieb festlegen.
- Einen Prozess zur Beobachtung und Bewertung der Digitalisierung der Netze aufsetzen.
- Verpflichtende Trainings zum Umgang mit überraschenden Ereignissen durchführen.

Langfristiger Lösungsbeitrag: Für die Behebung komplexer Störfälle benötigt der Netzbetreiber in Zukunft nicht nur ein umfassenderes Lagebild im eigenen Netz (siehe auch Handlungsoption 3 zum IKT-Lagebild), sondern auch das Wissen über die Netzgebiete anderer Netzbetreiber. Es wird nicht mehr ausreichen, Systemzustände zu erfassen und zu berechnen. Vielmehr müssen auch Kurzfristprognosen über die Systemdynamik erstellt werden, um die Auswirkungen von Schaltmaßnahmen und anderen Systemdienstleistungen abschätzen zu können. Ebenso ist das Wissen über und der Zugriff auf vorhandene Flexibilitäten wichtig. Damit die Netzbetreiber ein solches Lagebild erstellen, austauschen und geeignete Maßnahmenplanungen untereinander abstimmen können, ist eine umfangreiche Digitalisierung notwendig. Dafür ist ein neues Instrumentarium erforderlich:

- Durchgehende Digitalisierung der Verteilnetze und der angeschlossenen Erzeugungsanlagen und steuerbaren Verbrauchsanlagen sowie die weitgehende Automatisierung von Schalthandlungen.

- Ein umfangreicher, in Teilen schwarzfallfester (siehe Handlungsoption 2) Austausch von Echtzeitinformationen der Netzbetreiber untereinander, aber auch mit den Betreibern von Erzeugungsanlagen, um sowohl frühzeitig Bedrohungssituationen erkennen und abwenden zu können als auch den Systemwiederaufbau zu erleichtern.

- Werkzeuge der Systemführung, die in der Lage sind, das betriebsführende Personal bei den komplexeren Aufgaben zu unterstützen (KI und „Digitale Zwillinge“ werden hier wesentliche Beiträge leisten, siehe Abschnitt 3.1.4 und 3.2.1).

Bisher sind die Netzbetreiber zwar verpflichtet, die vorgelagerten Netzbetreiber auf Anforderung bei der Aufrechterhaltung der Systemsicherheit zu unterstützen, sie sind jedoch nicht verpflichtet, bereits bei der Ausstattung ihrer Infrastruktur die Belange der vorgelagerten Netzbetreiber zu berücksichtigen. Eine abgestimmte Weiterentwicklung der digitalen Ausstattung der Infrastruktur ist allerdings notwendig. Es wäre daher zu überprüfen, welche Ausstattung sich als technisch und ökonomisch effizient erweist, und entsprechende Maßnahmen wären in die Regulierung zu übernehmen. Wie der Regulator eine zukünftige Aufteilung der Verantwortung der Netzbetreiber

ausgestalten soll, ist anhand des heutigen Wissensstands nicht zu bestimmen oder sinnvoll festzulegen. Daher sollten möglichst keine Entscheidungen gefällt werden, die starke Pfadabhängigkeiten erzeugen.

Was kann man heute tun?
Kriterien für die technische Ausstattung und den Informationsaustausch für den proaktiven Systembetrieb festlegen und einen Prozess zu Beobachtung und Bewertung der Digitalisierung aufsetzen
Die Digitalisierung der Verteilnetze muss ausreichend schnell von den Netzbetreibern umgesetzt werden. Dazu gehört neben einer umfangreichen technischen Ausstattung für den automatisierten proaktiven Systembetrieb auch das Know-how, diese Techniken einzuführen und sicher und zuverlässig zu betreiben. Anders werden die VNB in Zukunft keinen größeren Teil der Verantwortung für die Systemsicherheit wahrnehmen können. Grundvoraussetzung dafür ist eine abgestimmte Weiterentwicklung der digitalen Infrastruktur: Bereits bei der Ausstattung der eigenen digitalen Infrastruktur eines Netzbetreibers sollten die Belange vorgelagerter Netzbetreiber berücksichtigt werden.

Das wirtschaftliche Potenzial der Digitalisierung und Automatisierung wurde bereits in der Verteilernetzstudie im Auftrag des BMWI[281] und in Studien im Auftrag der Agora Verkehrswende[282] gezeigt: Die Nutzung von Flexibilität, die durch die Digitalisierung ermöglicht wird, und eine angepasste Regulierung in den nationalen Verteilnetzen können jährliche Kosteneinsparungen von mehreren Hundert Millionen Euro erbringen. Um dieses Potenzial in Gänze zu erschließen, müsste eine geeignete Regulierung geschaffen werden. Wenn dies nicht ausreicht, kann die Politik weitere Maßnahmen ergreifen, um die Netzbetreiber zur Digitalisierung zu bewegen. Da es in Deutschland sehr viele kleine Netzbetreiber gibt, sollte die Politik darauf achten, dass diese kleinen Akteure in die Lage versetzt werden, bei den technischen Änderungen Schritt zu halten und mit den geänderten Anforderungen umzugehen. Bereits heute zeigen einige Stadtwerke, dass sie willens und fähig sind, bei der Digitalisierung mitzuhalten, etwa durch Zusammenschlüsse mit anderen. Ähnliches gilt für Zusammenschlüsse regionaler Akteure, die ihre Energieversorgung in Teilen in die eigene Hand nehmen, etwa durch Quartierslösungen.[283] Da solche Konzepte oft bürgernah die Energiewende umsetzen, muss die Regulierung hier auch stark Akzeptanzthemen im Auge haben.[284]

Aufgabe der Regulierung kann es sein, sowohl Zukunftsoffenheit als auch Antizipation zukünftiger Entwicklungen anzureizen oder zu fordern. Diese Anforderungen könnten etwa in die Standardisierungsstrategie von BMWi und BSI[285] integriert werden. Allerdings konzentriert sich die Betrachtung der dort beschriebenen Roadmap bisher auf Themen, die direkt mit dem Smart Meter zu tun haben. Dies stellt jedoch nur einen Teil des Themas Netzdigitalisierung dar. Zu den weiteren Themen zählt etwa die Digitalisierung der netzeigenen Prozesse und Betriebsmittel selbst. Zur gesamthaften Betrachtung gehört auch die Begleitung der anderen beiden Themen, nämlich Austausch der Netzbetreiber untereinander und modernisierte Betriebsführung.

281 E-Bridge 2019.
282 Agora Verkehrswende et al. 2019.
283 Siehe zum Beispiel die Projekte Energetisches Nachbarschaftsquartier (www.enaq-fliegerhorst.de) und SmartQuart (www.smartquart.energy).
284 acatech/Leopoldina/Akademienunion 2020-1.
285 BSI/BMWi 2019.

Beim Informationsaustausch sind insbesondere gemeinsame Standards über die Austauschprozesse, ausgetauschte Informationen und deren Formate zu schaffen beziehungsweise bereits vorhandene Standards als verbindlich zu erklären. Diese können von einem Verband (zum Beispiel Bundesverband der Energie- und Wasserwirtschaft, FNN, oder einem entsprechenden Verband auf internationaler Ebene) festgelegt werden. Zusätzlichen Nutzen können gemeinsam definierte Softwareplattformen für den Austausch und auch Stammdatenbereitstellung schaffen. Bei der Betriebsführung und deren Modernisierung durch neue Möglichkeiten der Digitalisierung liegt die Verantwortung bei den jeweils verantwortlichen Netzbetreibern. Da die Betriebsführung aber zunehmend von der durchgängigen Digitalisierung der Netze und dem Austausch von Echtzeitinformationen abhängt, sollten diese Themen ebenfalls von der Politik begleitet werden. Ein möglicher Rahmen wäre der oben genannte Roadmap-Prozess. Gefördert werden kann die Modernisierung etwa durch entsprechende Forschungsprojekte hoher technischer Reife mit attraktiven Teilnahmebedingungen für die Netzbetreiber. Im nationalen 7. Energieforschungsprogramm könnten die Ministerien mit Einzelausschreibungen zum Thema „Resilienz und Digitalisierung“ die dafür notwendige Forschung vorantreiben.[286]

Es sollte zusätzlich ein Prozess eingeführt werden, in dem Digitalisierungsziele abgestimmt werden und deren planmäßige Umsetzung verfolgt und gegebenenfalls korrigiert wird. Die Digitalisierung der Netze sollte in diesem begleitenden Monitoringprozess beobachtet und bewertet werden. Aus den Ergebnissen sollten Empfehlungen oder verpflichtende Maßnahmen abgeleitet werden. Welche Reihenfolge der Digitalisierung die beste ist, hängt von vielen Faktoren ab und ist nicht im Vorhinein bestimmbar. Nicht zuletzt sind die lokalen Gegebenheiten in den Verteilnetzen ausschlaggebend. Die Verteilnetzbetreiber sollten daher weiterhin entsprechende Freiheiten bei der Ausgestaltung der Digitalisierung behalten.

Inwieweit und wie konkret die Politik für die genannten Themen regulatorische Vorgaben machen möchte, wäre unter dem Gesichtspunkt der langfristigen Resilienzsicherung zu prüfen.

Bewertung: Die Maßnahmen sollten kurzfristig angegangen werden, da die Umsetzung der Digitalisierung bereits begonnen hat und gestaltet werden muss. Der Zeitraum der Maßnahmen ist unbegrenzt, da immer wieder nachgesteuert werden muss. Darüber hinaus wird sich sowohl der zeitliche als auch der finanzielle Aufwand für Betrieb und Wartung erhöhen. Eine gelungene Umsetzung kann durch effizientere Integration vorhandener Flexibilitäten helfen, Netzausbau zu vermeiden, wenn außerdem die Abregelung dezentraler Anlagen gesetzlich geregelt wird.[287] Die Kosten für Netzausbau liegen meist um ein Vielfaches höher als die für IKT-Anpassungen, die für die Vermeidung des Netzausbaus nötig wären. Je nach Ausgestaltung wird in die unternehmerische Gestaltungsfreiheit der Netzbetreiber eingegriffen. Es entstehen Abhängigkeiten, die zur Reduzierung der eigenen Spielräume eines Netzbetreibers aufgrund des „Kompatibilitätszwangs“ (zusätzliche Schnittstellen sind aufzubauen und zu betreiben) führen können. Ein Informationsaustausch ist eine notwendige, aber nicht hinreichende Bedingung für effiziente Koordination; sie wird erst effizient, wenn auch die Anreize abgestimmt sind.

286 Zur Verbesserung des Datenaustauschs unter den Netzbetreibern siehe auch die Projekte Coordinet (www.coordinet-project.eu) und TDX Assist (www.tdx-assist.eu).

287 Büchner et al. 2014.

Verpflichtende Trainings zum Umgang mit überraschenden Ereignissen durchführen

Simulationen sind eine verbreitete Technik zum Testen von Systemen. Die Simulationen in Trainingscentern dienen dazu, auch systemische Auswirkungen von Störungen besser zu verstehen und besonders auch Störereignisse zu trainieren, die durch eine neue, durch Digitalisierung bedingte Systemdynamik entstehen könnten.

Aus der Risikobewertung sowie dem Wissen aus vorangegangenen Störereignissen, die in einer geeigneten Stelle erfasst und ausgewertet werden (siehe Handlungsoption 14), lassen sich repräsentative oder gar Worst-Case-Szenarien ableiten und in Übungen simulieren. Hier kann ebenfalls Wissen aus Risikoanalysen einfließen (siehe Handlungsoptionen 4 und 14). Solche Szenarien können durch Netzbetreiber als Training zum Üben des Verhaltens während eines Blackouts und anderer kritischer Situationen genutzt werden. Auch könnten in diesen Übungen neue IKT- und KI-gestützte Technologien und Werkzeuge getestet werden, die sich besser für die Reaktion auf unbekannte oder sehr ungewöhnliche Fehler eignen. Dies verbessert auch auf der Seite des Betriebspersonals die Bereitschaft, neue resilienzerhöhende Werkzeuge und Verfahren einzuführen. Die Politik sollte entscheiden und festlegen:

- Welchen Kriterien haben Szenarien und Übungen (Stresstests) zu folgen?
- Für wen sind diese Übungen verpflichtend, und wer verantwortet die Durchführung? Wie werden die Unternehmen danach zertifiziert?
- Wer verantwortet die Trainingscenter?
- Wer kommt für die anfallenden Kosten auf?

Mindestens die großen Netzbetreiber sollten diese Übungen regelmäßig abhalten und die verantwortlichen Personen an solchen Trainings teilnehmen. Sollte aus weiteren Analysen wie etwa in Handlungsoptionen 4 und 14 hervorgehen, dass auch weitere Akteure bei Auslösung und Behebung der Störung eine wesentliche Rolle spielen, sollten diese in angemessenem Umfang in diese Übungen einbezogen werden – z.B. Betreiber von Telekommunikationsnetzen und spezialisierte Cyber-Sicherheitsfachleute. Ein standardisierter Prozess für sowohl die Erarbeitung als auch die Durchführung der Übungen sollte verabschiedet werden, etwa durch eine Prüfstelle, Behörde oder einen Verband. Erarbeitung und Ausgestaltung des Prozesses sollten durch die Netzbetreiber geleistet werden. Die Übungen sollten regelmäßig überprüft und angepasst werden. Die Trainingscenter müssen daher so aufgebaut werden, dass sie einerseits die heutige und zukünftige Situation in den Netzen der Netzbetreiber gut abbilden, aber andererseits auch einfach konfigurier- und erweiterbar sind und von vornherein größte Flexibilität bei der Anlage von Übungsszenarien erlauben.

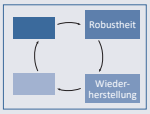
Für große Netzbetreiber mag sich ein eigenes Trainingscenter amortisieren. Jedoch sind diese Kosten weder für kleinere Betreiber sinnvoll oder tragbar, noch ermöglichen „kleine“ Trainingscenter in der Regel die Aufgabe, Übungen mit vielen Akteuren durchzuführen. Die Netzbetreiber sollten daher Konzepte für Kooperationsmöglichkeiten zum Betrieb solcher Center erstellen. Beispielsweise könnten bestehende Trainingscenter nicht nur den eigenen Mitarbeiterinnen und Mitarbeitern, sondern auch Externen zur Schulung zur Verfügung gestellt werden.

Die Kosten für die Netzbetreiber lassen sich voraussichtlich über die Netzentgelte umlegen. Auch könnten Kosten durch eine Nutzung Dritter solcher Zentren geteilt werden. Für die Kosten für andere Akteure gibt es bisher noch kein Modell. Ein solches Modell könnte etwa unter der Verantwortung der Bundesnetzagentur erarbeitet werden.

Bewertung: Die Optionen sollten kurzfristig angegangen werden, da der Aufbau dieser Trainingscenter einschließlich notwendiger Übungsszenarien und Klärung der damit zusammenhängenden Fragen zeitaufwendig ist. Hier kann auf Vorhandenem aufgesetzt werden. Die vorgeschlagenen Maßnahmen bieten den Vorteil, dass das Bewusstsein für neue Störereignisse deutlich erhöht würde. Das Betriebspersonal kann umfassender ausgebildet werden. Bestehende IT/OT-Infrastrukturen können simuliert und analysiert werden. Bei entsprechender Umsetzung können auch Einarbeitungszeiten verringert werden – ein großer Vorteil insbesondere bei zunehmendem Mangel an Fachkräften. Durch die Trainings entstehen jedoch zusätzliche Aufwände beim Betriebspersonal.

Auch wenn Erfahrungen mit Übungen vorliegen, stellen sich große technische Herausforderungen für diese Center. Es empfiehlt sich daher, in kleinen Schritten vorzugehen (wenige Akteure in Pilotprojekten, eingeschränkte Szenarienauswahl etc.). Jedoch sollte von Beginn an unbedingt nicht nur das elektrische Netz, sondern auch die involvierte IKT getestet und simuliert werden können.

Handlungsoption 7:
Regelwerk für Resilienz durch dezentrale Strukturen erarbeiten lassen



Ergebnis: Einzelne Netzabschnitte sind inselbetriebsfähig und können so einen Blackout überbrücken. Kritische Verbraucher werden bevorzugt mit Strom versorgt.

Dringlichkeit: ● ● **Wirksamkeit:** ● ● ●

Was kann man heute tun?

- Forschungs- und Entwicklungsprojekte zur Ausgestaltung und anschließende Feldtests durchführen.

Langfristiger Lösungsbeitrag: Im Fall eines großflächigen, längeren Blackouts kann bei geeigneter technischer und regulatorischer Ausgestaltung temporär eine lokale, in der Regel eingeschränkte Stromversorgung in einem Verteilnetz realisiert werden (sogenannter Inselbetrieb[288]), bis der übergeordnete Blackout behoben ist. Es wird auch an einem Wiederaufbau „von unten", also dem Zusammenschalten dieser Inseln, geforscht. Jedoch sind dazu noch sehr viele technische Fragen ungelöst. Ob ein solches Vorgehen irgendwann sinnvollerweise eingeführt werden sollte, ist derzeit daher nicht zu beantworten.

Der Inselbetrieb erfordert, dass im jeweiligen Netzgebiet Erzeugung und Verbrauch ausgeglichen sind. Um diesen Ausgleich zu unterstützen, können Speicher eingesetzt werden, und so eine wesentliche Rolle für den stabilen Inselbetrieb spielen. Wenn jedoch nicht genug Erzeugung zur Verfügung steht, um dieses Netzgebiet vollständig mit Strom zu versorgen, sollten kritische Verbraucher – wie Krankenhäuser oder Feuerwehr – bevorzugt mit Strom bedient werden. Dies kann auf verschiedenen Wegen realisiert werden:

Die technisch einfachere Möglichkeit besteht darin, jeweils die Netzabschnitte mit Strom zu versorgen, in denen sich kritische Verbraucher befinden. Hier ist heutzutage jedoch nur eine geringe Selektivität möglich.

- Alternativ können einzelne Verbraucher hinzugeschaltet beziehungsweise eingeschränkt werden. Hier gibt es zwei denkbare Umsetzungen:

288 Dieses wird bereits in einigen Ländern praktiziert – Inselnetze sind nichts an sich Neues.

- Durch die flächendeckende Ausbringung von Zählern mit Schalt- oder Regeleinrichtungen können einzelne Verbraucher technisch vom Netz getrennt werden.[289] Dies erfordert jedoch umfassende Änderungen an den technischen Anlagen.

- Durch Informationskampagnen werden Privatakteure motiviert, im Falle des Inselbetriebs ihren Verbrauch freiwillig einzuschränken. Vergleichbare Kampagnen waren bereits in anderen Ländern wie etwa Australien erfolgreich.

In jedem Fall erfordert ein selektiver Inselnetzbetrieb vor der regulatorischen und technischen Umsetzung eine intensive Einbeziehung der relevanten Akteure (Netzbetreiber, Anlagenbetreiber, Bürgerinnen und Bürger, Betriebe). Sonst wird es kaum möglich sein, ein Ergebnis zu erreichen, das auf allgemeine Akzeptanz trifft (siehe auch Handlungsfeld 6/Abschnitt 6.6).

Was kann man heute tun? Wesentliche Fragen, die einer Lösung bedürfen und zeitnah bearbeitet werden sollten, sind insbesondere:

- Welche Netzgebiete dürfen, müssen beziehungsweise können im Falle eines Blackouts technisch als Insel betrieben werden? Wie wird die nötige Mindestausstattung an Erzeuger-, Verbrauchs- und Speicherstrukturen in den jeweiligen Netzgebieten ermittelt (analog zu heutigen Last- und Erzeugungsscheiben)? Wie werden Inselnetze betrieben?

- Welche technischen Regeln für den Inselbetrieb müssen einheitlich, welche netzindividuell gestaltet werden?

- Gibt es Regeln, die vorzugsweise systemweit innerhalb des ENTSO-E-Verbunds normiert werden sollten?

- Welche technischen Voraussetzungen sind für den Schwarzstart eines Inselnetzes notwendig?

- Wie schafft man gesellschaftlich akzeptierte und diskriminierungsfreie Regeln für diesen Betrieb?

- Wie sind einheitliche Vorschriften und eine koordinierte Gestaltung des Inselbetriebs auszuarbeiten?

- Wie können Inselnetze in das allgemeine Wiederaufbaukonzept des Stromnetzes eingebunden werden?

- Wie sieht der regulatorische Rahmen aus? Welche neuen Pflichten, aber auch neue Rollen ergeben sich für die Netzbetreiber? Werden Netzbetreiber etwa im Inselbetrieb die Steuerung von Lasten und Erzeugung komplett übernehmen oder die Selbstorganisation von Aggregatoren oder dezentralen Erzeugungs- und Verbrauchsanlagen begleiten?

Als erste Umsetzungsmaßnahme empfiehlt es sich, im nationalen 7. Energieforschungsprogramm entsprechende Ausschreibungen vorzunehmen, um in Forschungs- und

289 Diese Lösung wurde zum Beispiel in Italien gewählt – unter anderem, um nicht zahlende Stromkunden vom Netz trennen zu können. In Deutschland ist sie hingegen nicht vorgesehen.

Entwicklungsprojekten die oben genannten Fragen zu beantworten. Auch erste Pilotprojekte könnten so ermöglicht werden, um die Lösungen im Feld unter Einbindung der relevanten Akteure zu erproben. Bereits heute werden in Projekten wie enera[290] oder Designetz[291] regionale Systemdienstleistungen entwickelt, die dabei helfen können, die oben genannten resilienten, dezentralen Versorgungsstrukturen zu schaffen. Die stabilisierende Funktion von Speichern im Energiesystem sollte ebenfalls bei der zukünftigen Forschung und Entwicklung von Speichertechnologien berücksichtigt werden.

Bewertung: Die Umsetzung der Maßnahmen wird einige Zeit in Anspruch nehmen und sollte daher zügig angegangen werden. Allein die Schaffung theoretischer Grundlagen und Untersuchungen in Pilotprojekten wird etwa zehn Jahre dauern. Technische Lösungen könnten in einzelnen Netzgebieten unabhängig von anderen eingeführt werden, weswegen eine Realisation schrittweise in wenigen Jahren erfolgen kann. Die Schaffung eines rechtlichen Rahmens wird jedoch weit mehr Zeit in Anspruch nehmen und sollte parallel vonstattengehen.

Die Wirkung größerer Blackouts kann durch das Abfangen einzelner betriebsfähiger Inseln reduziert werden. Der Wiederaufbau kann durch die Beiträge dezentraler Bereiche erleichtert werden. Beides verkürzt die Schwere und die Dauer eines großflächigen Versorgungsausfalls und kann damit die Resilienz des Gesamtsystems erhöhen. Allerdings erfordert diese Maßnahme einen enormen Abstimmungs- und Kommunikationsbedarf. Die Realisierung ist technisch sehr aufwendig. Zudem muss bei Änderungen der Verbraucherstruktur ständig nachprojektiert werden, um funktionsfähig zu bleiben. Auch mit Akzeptanzproblemen ist zu rechnen; für die zu erarbeitenden Kriterien für den Inselbetrieb wird ein großer gesellschaftlicher Konsens benötigt (siehe auch Handlungsoption 12). Als weitere Hürden für die Umsetzung werden neben der Schaffung eines konsistenten Regulierungsrahmens auch wirtschaftliche Anreize gesehen. Denn es muss erreicht werden, dass die Inselnetzfähigkeit vorhanden ist, auch wenn sie nur selten gebraucht wird.

Hohe Kosten werden für die Förderprogramme anfallen (schätzungsweise in der Größenordnung fünfzig Millionen Euro). Dabei ist zu beachten, dass auch Förderprogramme mit ausreichendem Volumen für Pilotierung aufgesetzt werden. Der Aufwand für die Schaffung der notwendigen Regelungstechnik von ausgewählten dezentralen Erzeugungsanlagen und der Selektionsinfrastruktur zum An- oder Abschalten einzelner Netzabschnitte oder Verbraucher (sofern dies nicht ohnehin über vorhandene Kommunikationsinfrastruktur der intelligenten Messsysteme möglich ist) wird als gering eingeschätzt. Andererseits können die Maßnahmen zu hohen Kosteneinsparungen führen – nicht nur, weil die Schadenskosten für große Blackouts vermieden werden, sondern auch, weil die Anforderungen an redundante Netzinfrastruktur gering gehalten werden. Wenn es möglich ist, einen teilautarken Betrieb während eines Blackouts herzustellen, zeigt die Maßnahme eine hohe Wirkung. Diese wird verstärkt durch einen möglichen Multiplikatoreffekt, der mit der Anzahl und der Flächenverteilung einsatzfähiger Inselnetze steigt.

290 www.projekt-enera.de
291 www.designetz.de

6.4 Handlungsfeld 4: IKT-Integration kleiner Anlagen netzdienlich gestalten

Problem 2040: In wenigen Jahren können sich annähernd alle neu auf den Markt gebrachten elektrischen Erzeugungsanlagen und Geräte mit dem Internet verbinden. Durch digitale Steuerbefehle kann es dadurch passieren, dass sehr viele Geräte gleichzeitig an- oder ausgeschaltet werden – im schlimmsten Fall so viele, dass dadurch die Systemsicherheit bedroht wird.

Erläuterung: Die Hersteller von elektrischen Geräten statten ihre Produkte mit Schnittstellen zum Internet aus. Diese soll den Verbraucherinnen und Verbrauchern einen höheren Nutzen bieten (zum Beispiel im Rahmen von intelligenten Heimautomatisierungssystemen) und dem Hersteller Informationen zur Verfügung stellen (etwa zu Wartungszwecken oder um seine Kundschaft besser zu verstehen).[292]

Durch Fehler in der Software, bösartige Absicht oder anderes nicht vorhersehbares Verhalten (zum Beispiel im Zusammenhang mit durch KI gesteuertem Verhalten oder nicht eingeplantem Nutzerverhalten) könnten die Geräte ihr An- oder Abschaltverhalten überraschend synchronisieren. Dieses synchrone Verhalten kann zusammen genommen eine so große und schnelle Leistungsänderung im Stromnetz verursachen, dass diese nicht mehr mithilfe von Regelleistung ausgeglichen werden kann, oder sogar kritisches Verhalten zeigen, das prinzipiell nicht durch Regelleistung auffangbar ist.

Neben Geräten wie Ladestationen für Elektrofahrzeuge oder Hausspeicher können auch kleine Erzeugungsanlagen – zum Beispiel Dach-PV oder KWK-Anlagen – kritisches simultanes Verhalten aufweisen. Hier kann unterschieden werden zwischen zwei Typen von Erzeugungsanlagen: zum einen solche, die über eine IKT-Schnittstelle verfügen, über die auf die Leistung direkt Einfluss genommen werden kann, und zum anderen solche, die zwar nicht direkt ansteuerbar sind, aber das gleiche Verhalten implementiert haben, wie es zum Beispiel bei PV-Anlagen der Fall war (siehe Infobox „50,2-Hertz-Problem“). Einer festen Implementierung von Regeln liegen also Annahmen über die Zukunft zugrunde, die Pfadabhängigkeiten erzeugen. Erweisen sich diese Annahmen als falsch, kann dies zu einer nur sehr aufwendig zu behebenden Vulnerabilität des Energiesystems führen. Dabei stehen nicht die Kosten im Vordergrund, die etwa durch eine Umrüstung verursacht würden. Vielmehr wirkt sich die lange Dauer für eine Umrüstung kritisch aus, da über diesen längeren Zeitraum Schadensereignisse über die Schwachstellen in der noch bestehenden Infrastruktur zu Blackouts führen könnten. Eine weitere Herausforderung für die Netzbetreiber wird es sein, mit dem Mix aus Alt- und Neugeräten umzugehen. Elektrotechnische Geräte und Betriebsmittel werden oftmals über Jahrzehnte in den Stromnetzen eingesetzt. Technische Neuerungen sind zum Teil schwer oder gar nicht zu integrieren, während sich ein Austausch der Geräte aus Kostengründen meistens verbietet. Auf der anderen Seite kann bewusst herbeigeführtes synchrones Verhalten von Erzeugungsanlagen und Speichern auch netzdienlich genutzt werden: In Zukunft werden weniger Großkraftwerke für die Bereitstellung von Regelleistung zur Verfügung stehen, weshalb dezentrale Anlagen diese Aufgabe übernehmen und einen Beitrag zur Systemstabilität leisten müssen. Zudem können sie im Falle eines Blackouts beim Aufbau eines Inselnetzes unterstützen (siehe Handlungsoption 7). In beiden Fällen ist eine kommunikationstechnische Anbindung kleiner Anlagen notwendig.

292 Auf die damit verbundenen enormen Datenschutzherausforderungen kann hier nicht eingegangen werden.

50,2-Hertz-Problem

In der Annahme, dass es zukünftig immer bei einem nur geringen PV-Ausbau bleiben würde, verabschiedete der verantwortliche Verband eine Regel, der zufolge sich PV-Anlagen bei einem Überangebot an Strom (gemessen an einem Frequenzanstieg über 50,2 Hertz) spontan abschalten müssen. Alle PV-Anlagen hatten dieses Verhalten fest implementiert. Schalten sich dabei jedoch viele Anlagen ab, führt dies zu einem Leistungsverlust, der die zu hohe Einspeisung massiv überkompensiert. In der Folge mussten in einem jahrelangen Prozess die PV-Anlagen umgerüstet werden. Zudem gab es in dieser Zeit das Risiko, dass die PV-Anlagen das System in speziellen Situationen destabilisieren.

Zeithorizont des Problems: Unerwünschtes simultanes Verhalten von Anlagen war bereits in der Vergangenheit relevant (siehe 50,2-Hertz-Problem). Das Thema bleibt aber dauerhaft aktuell: Es gibt etwa Anbieter, die auch für Privatkundinnen und -kunden einen stundenbasierten Strompreis anbieten, der auf den aktuellen Börsenpreisen basiert. Die ersten Privatakteure beginnen, ihre Elektroautoladestationen mit diesen Profilen zu programmieren. Daher ist davon auszugehen, dass in den nächsten Jahren entsprechende Produkte für den Massenmarkt verfügbar sein werden. Zeitbasiertes Laden ist im europäischen Ausland bereits gang und gäbe. Dies kann ohne steuernde Gegenmaßnahmen im Verteilnetz zu Engpässen führen. Ein mögliches Problem für die Systemstabilität ist eher mittel- bis langfristig zu erwarten.

Heute bereits bestehende Maßnahmen: Dezentrale Erzeugungsanlagen leisten bereits heute einen umfangreichen Beitrag zur Systemstabilisierung, etwa indem sie Blindleistungsregelung betreiben und zur Frequenzstützung beitragen. Dezentrale Erzeugungsanlagen ab einer Größe von dreißig Kilowatt im Niederspannungsnetz sollen gemäß § 9 EEG durch den Netzbetreiber ansteuerbar sein, um Engpässe zu vermeiden und die Anlagen in kritischen Situationen zu koordinieren. Die zu erbringenden Systemdienstleistungen wie die dynamische Netzstützung[293] werden in den VDE-Standards 4105 und 4100 (für Anlagen am Niederspannungsnetz beziehungsweise am Mittelspannungsnetz) beschrieben. Geräte im Haushalt „hinter dem Zähler“ unterliegen kaum Network Codes oder vergleichbaren Regelungen. Eine Ausnahme bildet hier der § 14a im EnWG, der VNB dazu verpflichtet, Letztverbrauchern in der Niederspannung ein reduziertes Netzentgelt anzubieten, wenn diese ihre Anlagen durch den Netzbetreiber dafür netzdienlich steuern lassen. In der Schweiz wurde bereits gezeigt, dass Geräte wie Wärmepumpen oder elektrische Heizungen tatsächlich Systemdienstleistungen unter zeitkritischen Bedingungen erbringen können: Dort wurden diese Geräte kommunikationstechnisch angebunden und im Verbund als Regelleistung vermarktet (siehe Infobox „Praxisbeispiel: Ein virtuelles Speichernetzwerk aus Privathaushalten“).

Praxisbeispiel: Ein virtuelles Speichernetzwerk aus Privathaushalten

Der Schweizer Energieversorger Swisscom Energy Solutions hat mit „tiko“[294] ein virtuelles Speichernetzwerk entwickelt und realisiert. tiko verbindet mehr als 10.000 elektrische Heizgeräte in der Schweiz. Dazu zählen Wärmepumpen und Warmwasserkessel. Die Flexibilität, die durch die Aggregation der verschiedenen Verbrauchsanlagen entsteht, wird für Regelleistung eingesetzt (Primär- und Sekundärregelleistung) für den ÜNB Swissgrid. Zu diesem Zweck kommuniziert ein zentrales System mit lokalen Messsystemen und Steuersystemen über ein mobiles Kommunikationssystem und Power Line Communication (Kommunikation über Stromleitungen). Die Anlagen werden so gesteuert, dass die Endverbraucher nicht in ihrem Komfort eingeschränkt sind.[295]

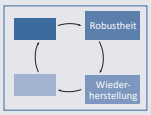
293 Neu installierte dezentrale Erzeugungsanlagen müssen künftig bei kurzzeitigen Spannungseinbrüchen oder erhöhungen am Netz bleiben und es so stützen, siehe VDE|FNN 2018-2.

294 https://tiko.ch/page/home/?lang=de

295 Vgl. Geidl et al. 2017.

Der VDE diskutiert außerdem derzeit, ob Ladestationen für Elektroautos ab 3,6 Kilowatt generell durch den Netzbetreiber steuerbar gemacht werden sollen.[296]

Handlungsoption 8:
Standardisierung zur Vermeidung problematischen simultanen Verhaltens initiieren



Ergebnis: Gerätestandards verringern die Wahrscheinlichkeit von stabilitätsgefährdenden Gleichzeitigkeiten und simultanen Verhaltens.

Dringlichkeit: ● ● ● **Wirksamkeit:** ● ●

Was kann man heute tun?

- Eine Richtlinie für Patchability erarbeiten, verabschieden und einführen.
- Analysen und Forschung für die Plausibilisierung von Schaltbefehlen anhand lokaler physikalischer Größen durchführen.

Langfristiger Lösungsbeitrag: Ungeplante, unvorhersehbare Gleichzeitigkeiten oder zeitgleiches Abschalten von Geräten und Erzeugungsanlagen müssen als potenzielles Risiko erkannt und dementsprechend in einer Resilienzstrategie berücksichtigt werden. Geräte sollten im Auslieferungszustand vom Hersteller so konfiguriert werden, dass die Systemstabilität gefährdendes simultanes Verhalten möglichst nicht auftreten kann. Es kann Käufern und erst recht privaten Haushalten nicht zugemutet werden, sich selbst um den Beitrag ihrer Geräte zur Resilienz des Stromnetzes zu kümmern. Dazu braucht es von Fachgremien entwickelte Mindeststandards. Diese Mindeststandards müssen so gehalten sein, dass sie einen großen Umfang möglicher Anlagen einschließen und auch die Verpflichtung zu bedarfsgerechten Updates enthalten. Eine internationale Standardisierung wäre vorteilhaft, da kritisches simultanes Verhalten überall im europäischen Verbundnetz dieselben negativen Auswirkungen hat. Das Schweizer Beispiel (siehe Infobox „Praxisbeispiel: Ein virtuelles Speichernetzwerk aus Privathaushalten“) zeigt dabei, dass es keine anwendungsfallunabhängigen Standards zum Verhalten der Geräte geben kann: Während für den Anwendungsfall der Regelleistung eine sehr kurze Reaktionszeit für Primär- und Sekundärregelleistung erforderlich ist, könnte zum Verringern von Gleichzeitigkeiten ein absichtlich verzögertes Schaltverhalten sinnvoll sein.

Die Resilienzmaßnahmen sollten entsprechend dem Akteur, der die zeitgleichen Schalthandlungen verursachen könnte, wie folgt angepasst werden:

1. Energiewirtschaftliche Akteure (zum Beispiel Aggregatoren): Diese werden über die Energiegesetzgebung direkt adressiert und über Anwendungsregeln beziehungsweise Network Codes eingebunden (siehe auch Handlungsoption 4).

2. Nicht energiewirtschaftliche Akteure (zum Beispiel Hersteller von Smart-Home-Plattformen, Gerätehersteller): Für diese müssen neue Standards erarbeitet werden. Diese schreiben kein konkret definiertes Verhalten vor, sondern sind flexibel, um sich an verschiedene Situationen anpassen zu können (etwa über Softwareupdates).

3. Bösartige Angreifer: Die Organisation von und Maßnahmen zu Cyber-Sicherheit (siehe auch Handlungsfeld 2/Abschnitt 6.2) sind das Mittel der Wahl.

296 Vgl. VDE|FNN 2018-3.

Was kann man heute tun?

Eine Richtlinie für Patchability erarbeiten, verabschieden und einführen

Ein Patch ist die Verbesserung bestehender Versionen einer Software, etwa um neue Funktionen zu installieren oder Softwarefehler und Sicherheitslücken zu beheben. Patchability beschreibt hier die Eigenschaft einer technischen Anlage, dass installierte Software im laufenden Betrieb und ohne viel Aufwand aus der Ferne durch das Einspielen von Patches verbessert werden kann. Dies kann automatisch durch die Hersteller erfolgen oder durch den Betreiber selbst, soweit dieser qualifiziert ist. Patchability ist sowohl für Erzeugungsanlagen als auch für Verbrauchsanlagen relevant und sollte folgende Bedingungen erfüllen:

- Es werden regelmäßige Updates durchgeführt.
- Diese Updates sind nicht durch andere als den Hersteller (oder autorisierte Stellen) durchführbar.
- Funktionen, die sich auf das elektrische Energiesystem auswirken, sind in der Software abgebildet (soweit die Anlage dies technisch unterstützt).
- Die Software wurde so entwickelt, dass Anpassungen der Funktionen, die das elektrische Verhalten bestimmen, unkompliziert durchzuführen sind.

Für die Patchability muss der Regulator mit den Herstellern noch einige Voraussetzungen klären, etwa Finanzierung, Haftungsfragen, Regeln bei Abkündigung eines Produkts und Verantwortungen für die geeignete Kommunikationsinfrastruktur. Alle Funktionen, die nicht durch ein Update angepasst werden können, stellen ein potenzielles Sicherheitsrisiko dar. Dieses manuell zu beheben, kann – je nach Anzahl der installierten Anlagen – viele Jahre dauern und hohe Kosten verursachen. Durch Patches kann dieses Verhalten jeweils angepasst werden, ohne dafür an den Anlagen vor Ort Anpassungsarbeiten verrichten zu müssen. Hier kommt den Komponentenherstellern eine besondere Rolle zu: Diese müssen die Updates der Firmware, also der Betriebssoftware, oder auch die Einstellung oder Konfiguration des Systems gemäß den Vorgaben der Anschlussregeln (verabschiedet vom Netzbetreiber oder vom VDE) durchführen können. Es muss dann schlussendlich durch Verordnungen gewährleistet werden, dass nur Anlagen verkauft werden dürfen, die die gewünschte Eigenschaft haben. Vermutlich ist die Regelung für in Deutschland verkaufte Anlagen ausreichend. Dies sollte jedoch geprüft werden.

Bewertung: Die Eigenschaft der Patchability ist langfristig sehr wirksam. Es ist heute unmöglich zu wissen, welchen technischen Anforderungen Anlagen in der Zukunft genügen müssen, um kein Risiko für die Systemstabilität darzustellen. Deshalb muss Patchability bereits heute in Anlagen und Geräten – die zum Teil Jahrzehnte lang genutzt werden – eingebaut werden. Beispielsweise könnten in zehn Jahren kommerzielle Quantencomputer zur Verfügung stehen, sodass die heute regulär verwendeten kryptografischen Verfahren zur Verschlüsselung nicht mehr sicher wären (siehe Kapitel 3.1.10). Hier muss also ein Update auf Verfahren der Post-Quanten-Kryptografie möglich sein. Auch bei Erzeugungsanlagen ist es unmöglich vorauszusehen, welchen Network Code beziehungsweise welches Verhalten sie in den kommenden Jahren oder Jahrzehnten haben müssen, um etwa geeignet auf Frequenzabweichungen zu reagieren.

Die Erarbeitung, Verabschiedung und Einführung einer Richtlinie für Patchability mit anschließender Umsetzung dauert einige Jahre, wobei der eigentliche Standardisierungsprozess nur einen kleinen zeitlichen Anteil ausmacht. Parallel wächst die Anzahl der Anlagen mit Internetanschluss exponentiell schnell. Daher muss dieser Prozess so früh wie möglich angestoßen werden.

Für Hersteller bedeutet diese Forderung zunächst einen erhöhten Aufwand, weswegen es auch zu Widerständen und Verzögerungen in der Umsetzung kommen kann. Gegebenenfalls fallen höhere Kosten in der Anschaffung von Anlagen an. Bevor die Politik entsprechende Verordnungen ausgestaltet, muss der Nutzen für die Resilienz gegen die gestiegenen Kosten für die Herstellung der Anlage abgewogen werden. Entscheidendes Kriterium ist, wie viel Leistung gleichartige Anlagen in ihrer Gesamtheit kurzfristig ändern können und wie wahrscheinlich dies ist – über die komplette Installationszeit der Anlagen. Im laufenden Betrieb und in der Nachrüstung von Funktionalität kann durch die vorgeschlagene Maßnahme jedoch mit erheblichen Einsparungen gerechnet werden. Allerdings ist zu beachten, dass eine vollständige Absicherung nie möglich ist und Patchability auch ein Einfallstor für Angreifer darstellen kann.

Analysen und Forschung für die Plausibilisierung von Schaltbefehlen anhand lokaler physikalischer Größen durchführen

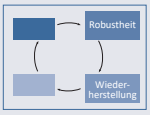
Das systemschädliche Verhalten kann nicht nur von den dezentralen Erzeugungsanlagen oder Verbrauchsanlagen direkt ausgelöst werden, sondern auch durch Fehler oder bösartiges Eindringen in deren IT-Systeme. Würden jedoch die Erzeugungsanlagen die Schaltbefehle anhand lokaler Parameter eigenständig auf Plausibilität prüfen – dies könnten etwa physikalische Größen wie Spannung und Frequenz sein –, könnte der Angriff auf die IT-Systeme weitgehend aufgefangen werden. Hierfür können insbesondere KI-Methoden zum Einsatz kommen.

Welche Art der Plausibilitätsprüfung feststellen kann, ob die durch den Netzbetreiber übermittelten Schalthandlungen in der aktuellen Netzsituation schädlich sind und daraus Anschlussregeln oder Network Codes abgeleitet werden können, lässt sich heute jedoch nicht beurteilen. Daher sind hier zunächst entsprechende Analysen und Forschungen notwendig, die durch den Netzbetreiber unter Einbindung der anderen relevanten Akteure durchgeführt werden sollten. Zudem muss eine zukünftige Anpassung dieser Plausibilisierung mittels Patch möglich sein.

Bewertung: Durch diese Maßnahme können Angriffe auf die Verbraucherseite erheblich erschwert werden. Die Umsetzung ist mittelfristig anzusetzen und sollte vor dem Ausrollen entsprechender Technologien erfolgen. Es ergäbe sich insgesamt eine robuste Lösung, die preiswert und manipulationssicher gestaltet werden kann. Der Aufwand für die Harmonisierung und Standardisierung unter Einbeziehung unterschiedlicher, teilweise internationaler Hersteller und Netzbetreiber ist voraussichtlich hoch.

Ein Zwang zur Umsetzung könnte Hersteller belasten. Ohne eine Verpflichtung der Hersteller bestünde jedoch die Gefahr, dass die vorgeschlagene Funktion nicht flächendeckend zur Verfügung steht.

Handlungsoption 9: Systemstabilisierung durch dezentrale Anlagen ausbauen



Ergebnis: Dezentrale Anlagen leisten einen wesentlichen Beitrag zur Stabilität des elektrischen Energiesystems.

Dringlichkeit: ● ● **Wirksamkeit:** ● ● ●

Was kann man heute tun?

- Maßnahmen zur Herstellung der notwendigen kommunikationstechnischen Anbindung erarbeiten und dabei relevante Akteure wie Netzbetreiber, Anlagenbetreiber oder Telekommunikationsunternehmen einbeziehen.
- Zum Einsatz von künstlicher Intelligenz forschen, um auch auf komplexe und unbekannte Störereignisse oder Angriffe angemessen reagieren zu können.

Langfristiger Lösungsbeitrag: Dezentrale Erzeugungs- und steuerbare Verbrauchsanlagen können und sollten in Zukunft viel mehr als heute zur Systemstabilität und Resilienz des Stromnetzes beitragen. Perspektivisch müssen auch die kleinen Anlagen verstärkt Systemdienstleistungen wie Frequenz- und Spannungshaltung sowie Kurzschlussleistung bereitstellen oder beim Wiederaufbau unterstützen. Damit das möglich wird, muss jedoch die Ausstattung der Anlagen entsprechend angepasst werden.

Was kann man heute tun? Um das Potenzial der vielen kleinen Energieanlagen für die Systemsicherheit nutzen zu können, braucht es neben der notwendigen leistungselektronischen Ausstattung insbesondere Konnektivität. Die Anlagen müssen kommunikationstechnisch angebunden sein und ihre Funktionen müssen über diese Anbindung vom Leitsystem des Netzbetreibers angesprochen werden können. Für die verantwortlichen Netzbetreiber muss es dazu kosteneffizient möglich sein, dezentrale Erzeugungsanlagen und steuerbare Verbrauchsanlagen mit all ihren Funktionalitäten in ihre Leitsysteme zu integrieren (siehe auch Handlungsoption 6). Dies sollte über große Plattformen geschehen, die zuvor vereinbarten (internationalen) Interoperabilitätsstandards folgen und in die KRITIS-Gesetzgebung einbezogen werden (siehe Handlungsoption 4). Aufgrund der Vielzahl an dezentralen Erzeugungsanlagen sollte eine geeignete, gegebenenfalls hierarchische Lösung entwickelt werden, die zum Beispiel auf Zwischeninstanzen – ähnlich Aggregatoren – beruht. Im Sommer 2019 wurde von ÜNB, den großen VNB und weiteren Versorgern dazu das Vorhaben CONNECT+ gestartet. Ziel ist es, den Datenaustausch für Engpassvermeidung durch Redispatchmaßnahmen unter Einbindung von Anlagen mit einer Anschlussleistung ab hundert Kilowatt zu gewährleisten. In diesem Vorhaben werden viele technische und regulatorische Fragen geklärt werden. Es bietet sich daher an, in diesem Projekt auch Fragen zu zukünftigen Resilienzmechanismen von den Beteiligten erarbeiten zu lassen. Fragen, etwa zur Steuerung und Sicherheitszertifizierung, sind ebenfalls zu klären. Eine Einbindung auch von kleineren Erzeugungsanlagen in die Plattformen ist perspektivisch technisch und regulatorisch vorzusehen.

Auch kleine Geräte wie Wärmepumpen können in der Gesamtheit einen nennenswerten Beitrag zur Systemsicherheit leisten (siehe Infobox Abschnitt 6.4 „Praxisbeispiel: Ein virtuelles Speichernetzwerk aus Privathaushalten“). Die deutschen Präqualifikationsregelungen der ÜNB für Regelleistung[297] erschweren derzeit jedoch

297 Vgl. Regelleistung 2019-2.

solche Modelle – unter anderem, weil die Anforderungen an die IKT-Anbindung von Regelleistung erbringenden Erzeugungsanlagen auf Voraussetzungen beruhen, die nur für größere Aggregate gelten. Es müsste also zunächst gezeigt werden, dass die notwendig hohen Anforderungen an die IKT-Anbindung auch mit kostengünstigeren Mitteln zu erreichen wären. Pilotprojekte mit ÜNB, Telekommunikationsunternehmen und Aggregatoren sollten diese Fragestellungen untersuchen.

Ein weiterer Ansatz zur Einbindung kleiner Erzeugungsanlagen und steuerbarer Verbrauchsanlagen ist es, die Anlagen mit Software für KI anzulernen, um auch auf komplexe und unbekannte Störereignisse oder Angriffe angemessen zu reagieren. Beispielsweise können mit dem sogenannten Adversarial Resilience Learning Instabilitäten und Angriffe abgewendet beziehungsweise abgewehrt werden, die bislang unbekannt sind beziehungsweise für die es derzeit noch keine Lösung gibt (siehe Abschnitt 3.2.1). Dies ist umso notwendiger, da man annehmen muss, dass potenzielle Angreifer bereits an ebensolchen Verfahren arbeiten, um Stromnetze angreifen zu können. Solche noch in den Kinderschuhen steckenden Verfahren der KI sollten intensiv erforscht werden.

Über die Umsetzung jeder resilienzsichernden Maßnahme, die die Einbindung von Haushalten benötigt, entscheidet jedoch voraussichtlich nicht die technische und ökonomische Machbarkeit, die bereits in vielen Forschungs- und Pilotprojekten untersucht wurde und wird; vielmehr ist die Akzeptanz durch Privatakteure ausschlaggebend (siehe Handlungsfeld 6/Abschnitt 6.6).

Bewertung: Durch die vorgeschlagenen Maßnahmen kann das Potenzial kleiner, verteilter Erzeugungs- und steuerbarer Verbrauchsanlagen zur Systemstabilisierung ausgeschöpft werden. Die Umsetzung sollte mittelfristig erfolgen. Jedoch sollten die nötigen Voruntersuchungen und Standardisierungsprozesse frühzeitig angegangen werden, da dies zeitaufwendig sein kann. Insbesondere der Einsatz neuer Technologien wie etwa KI sollte ausreichend erprobt sein, um Verständnis und Vertrauen zu schaffen. An den vorgeschlagenen Prozessen werden viele verschiedene Akteure beteiligt sein, die sich in ihren Interessen verletzt fühlen könnten (wie etwa Privatakteure). Zudem kann es zu Hürden in der Umsetzung kommen, da Netz- oder Anlagenbetreiber zu hohen Aufwand oder zu hohe Kosten befürchten. Dazu muss zunächst der Nutzen aufgezeigt werden.

6.5 Handlungsfeld 5: Anreize für Netzbetreiber zur Steigerung der Resilienz stärken

Problem 2040: Resilienz ist ein neues Phänomen in der Regulierungsdiskussion. Dementsprechend finden sich nur wenige Aspekte im energiewirtschaftlichen Regelrahmen, die explizit Resilienz berücksichtigen. Dies ist wenig verwunderlich, da das Thema Resilienz schlichtweg kein Teil der Diskussionen war, als die heute geltenden Gesetze und Verordnungen entwickelt wurden. Demzufolge fehlen weitgehend effektive und effiziente Anreize für die Netzbetreiber und Marktparteien, sich resilienzverbessernd zu verhalten.

Erläuterung: Resilienzverbessernde Anreize betreffen im Grunde die gesamte Wertschöpfungskette der Stromversorgung, vertikal sowie horizontal. Vertikal meint hier, dass alle Stufen der Stromwertschöpfungskette betroffen sind, von der Erzeugung bis hin zum Endverbraucher. Horizontal bezieht die Wertschöpfung nicht nur

die etablierten Energieversorgungsunternehmen mit ein, sondern auch solche Unternehmen, die nur mittelbar an der Stromversorgung beteiligt sind, wie zum Beispiel Gerätehersteller oder IT-Firmen. So ergibt sich eine komplexe Wertschöpfungskette, die hier nur angeschnitten werden kann. Allerdings ist zu beachten, dass sich nicht alle Herausforderungen durch die Anreizregulierung lösen lassen. So ist jeweils zu prüfen, ob sich eine gewünschte Wirkung auf die Resilienz durch die Anreizregulierung ökonomisch effizient realisieren lässt oder nur durch (ergänzende) ordnungsrechtliche Instrumente eine effektive Gefahrenabwehr (wie etwa im Umfeld der Cyber-Sicherheit, siehe Handlungsoptionen 4 und 5) erreicht werden kann.

Mindestens vier Themenbereiche gilt es zu betrachten, wenn man die Integration von Resilienz in den institutionellen Rahmen auf der Verteilnetzebene diskutiert:

- **Anreizregulierung**[298] für Netzbetreiber (siehe Handlungsoption 10): Den Netzbetreibern wird durch die Anreizregulierung eine Erlösobergrenze vorgegeben. Ob und wie die Anreizregulierung die Resilienzthematik effektiv berücksichtigt, hängt von der Art der Kosten ab, die durch die resilienzverbessernden Maßnahmen entstehen. Wir unterscheiden folgende Kostenarten und skizzieren kurz die Anreize der Netzbetreiber, wenn die resilienzverbessernde Maßnahme zu entsprechenden Kosten führt:

  - Ausgaben für resilienzverbessernde Maßnahmen können Kapitalausgaben (CAPEX) sein. Für die VNB werden diese bereits in der aktuellen Verordnung über die Anreizregulierung der Energieversorgungsnetze (kurz: Anreizregulierungsverordnung, ARegV) durch den Kapitalkostenabgleich jährlich abgegolten. Somit entsteht kein Nachteil für die VNB. Für die ÜNB hängt es davon ab, ob resilienzverbessernde Investitionsmaßnahmen (im Sinne von § 23 AregV) berücksichtigt werden. Falls ja, gehen die Ausgaben auch direkt in Erlösobergrenze; falls nicht, fallen die Ausgaben unter den Zeitverzug.[299]

  - Ausgaben für resilienzverbessernde Maßnahmen können Betriebskosten (OPEX) sein. In aller Regel fallen diese Ausgaben unter den Zeitverzug in der Anreizregulierung. Sofern die Ausgaben nicht in ein Basisjahr[300] fallen, sind sie für die Netzbetreiber nachteilig, und daher besteht hier ein Anreiz für die Netzbetreiber, diese zu vermeiden. Sofern darüber hinaus eine regulierungsbedingte CAPEX-Präferenz (CAPEX-bias) vorliegt, würden zusätzlich Anreize für die Netzbetreiber geschaffen, OPEX zu verringern.

  - Die Kosten eines Stromausfalls sind externe Kosten: Sie fallen nicht bei dem Netzbetreiber, sondern bei den Netzkunden an. Es wurde in der Literatur argumentiert, dass gerade unter einer Preis- oder Erlösobergrenzen-Regulierung die

298 Die Anreizregulierung ist ein Instrument, damit Netzbetreiber der „natürlichen Monopole“ Strom- und Gasnetz keine Monopolgewinne erzielen und ihre Netze sowohl möglichst kostensparend als auch qualitativ hochwertig betreiben. Durch die Erlösobergrenzen wird der Anreiz geschaffen, Kosten zu senken, um so höhere Gewinne zu erzielen.

299 Zeitverzug bezeichnet den Umstand, dass einige Kosten und Erlöse über die Regulierungsperiode hinweg zeitweise entkoppelt sind. Ergibt sich eine Abweichung der tatsächlichen Kosten in einem Jahr in der Regulierungsperiode von den Kosten im Basisjahr, wird diese Abweichung erst wieder im nächsten Basisjahr zu Beginn der neuen Regulierungsperiode erfasst.

300 Basisjahr bezeichnet das Geschäftsjahr, in dem die Kostenprüfung durchgeführt wird, aus der sich die Erlösobergrenze für die folgende Regulierungsperiode herleitet. Das Basisjahr liegt drei Jahre vor Beginn einer Regulierungsperiode.

Anreize für den Netzbetreiber, solche externen Kosten zu vermeiden, zu gering sind.[301] Infolgedessen sind zusätzliche Regulierungsinstrumente, wie etwa eine Q-Komponente (Q steht für Qualität) oder hier eine R-Komponente (R für Resilienz), erforderlich. Dieses Argument führt in die sogenannte Output-basierte Regulierung.

- Die resilienzverbessernden Ausgaben (insofern sie abgrenzbar sind) könnten außerhalb der Anreizregulierung gehalten werden und werden demnach als cost-pass-through behandelt. In dem Falle wären die Netzbetreiber indifferent, ob sie die Ausgaben tätigen oder nicht. Andererseits hätten sie keine Anreize, die Ausgaben effizient zu tätigen. Es verbleibt in diesem Fall eine Restunsicherheit, wie das Benchmarking mit den Kostenerhöhungen umgeht, die sich nicht unmittelbar in Output- oder Effizienzverbesserungen übertragen lassen.

- **Netznutzungsentgelte** (siehe Handlungsoption 11): Diese bestimmten Entgelte für den Zugang zu den Übertragungs- und Verteilernetzen (Netzentgelte) einschließlich der Ermittlung der Entgelte für dezentrale Einspeisungen.

- **Marktdesign**: Bei einem großflächigen, lang andauernden Blackout kann es passieren, dass der Betrieb des Übertragungsnetzes auseinanderfällt und in einen Inselbetrieb übergeht: Dieses Phänomen ist bekannt als sogenannter Network Split. Um einen Inselbetrieb und später eine schnelle Rückführung in die zentrale Betriebsführung zu ermöglichen, ist eine verteilte Struktur der Anlagen (vor allem steuerbare Erzeugung) erforderlich (siehe Handlungsoption 7). Derzeit aber folgen Investitionsentscheidungen für Anlagen den Marktgesetzen, wobei Resilienz keine Rolle spielt. Die Standortwahl bei Erzeugungsanlagen folgt der betriebswirtschaftlichen Effizienz. Eine räumliche Verteilung der Erzeugungsanlagen mit positiver Rückwirkung auf die Resilienz des Gesamtsystems erfordert demzufolge ein gezieltes Marktdesign, sodass die betriebswirtschaftliche Optimierung auch resilienzsteigernd wirkt. Über Netznutzungs- und -anschlussgebühren kann das Verhalten der Netznutzer entsprechend gelenkt werden (siehe Handlungsoption 11).

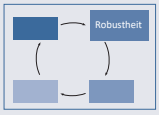
- **Governance**: Die Stromversorgung wird dezentraler. Von der früheren zentralen, Top-down-, Closed-Shop-Organisation mit wenigen, gut vernetzten Unternehmen wurde die Energieversorgung zu einer dezentralen, Bottom-up-, Open-World-Organisation mit vielen, zum Teil sehr heterogenen Akteuren. Es ist derzeit unklar, wer die Verantwortung für die Resilienz des Systems trägt und wer welche Investitionen plant. Es ist von zentraler Bedeutung, dass die Rollen und Verantwortlichkeiten klar zugeordnet und abgegrenzt sind, um eine effiziente Koordination und Kooperation sicherzustellen (siehe auch Abschnitt 2.3).

Zeithorizont des Problems: Bei Investitionsanreizen für resilienzsteigernde Maßnahmen durch den Netzbetreiber stehen zwar langfristige, präventive Maßnahmen im Fokus. Da die Netzbetreiber bereits jetzt resilienzverbessernde Maßnahmen ergreifen (zum Beispiel nicht kapitalbasierte IT-Ausgaben für Information-Security-Management-Systeme), wäre es gleichwohl wünschenswert, die ARegV bei nächster Gelegenheit derart anzupassen, dass solche Ausgaben regulatorisch adäquat anerkannt und resilienzverbessernde Maßnahmen gefördert werden.

301 Vgl. Spence 1975.

Bei Maßnahmen, die dem Netzbetreiber ein Instrument in die Hand geben, die Netznutzer resilienzverbessernd zu lenken, kann dies eine kurzfristige Lenkungswirkung auf das Verhalten der Netznutzer haben. Andererseits zielen solche Maßnahmen auf die Steuerung des Investitionsverhaltens der Netznutzer ab, mit zum Teil langfristigen Auswirkungen. Um diese langfristige Lenkungswirkung entfalten zu können, ist eine zeitnahe Umsetzung geboten.

Handlungsoption 10:
Eine Resilienzkomponente in die Anreizregulierung integrieren



Ergebnis: Die ARegV enthält Anreize für die Netzbetreiber, effektive resilienzverbessernde Maßnahmen durchzuführen.

Dringlichkeit: ● ● **Wirksamkeit:** ● ●

Was kann man heute tun?

- Eine R-Komponente in die ARegV als zusätzliche Regelung zur Verbesserung der Resilienz einführen.

Langfristiger Lösungsbeitrag: Wie oben beschrieben hängt es von der Art der Kosten einer resilienzverbessernden Maßnahme ab, ob und wie durch die aktuelle Regulierung Anreize für diese Maßnahme geschaffen werden. Insbesondere die externen Kosten eines Stromausfalls, die durch die resilienzverbessernde Maßnahme zumindest teilweise vermieden werden, haben keine Auswirkungen auf die Anreize der Netzbetreiber. Ein analoges Problem besteht bei der Qualität der Energieversorgung, die zu externem Nutzen führt, jedoch nicht zwangsläufig von der Anreizregulierung adressiert wird. Daher wurde in Deutschland die Q-Komponente in die Regulierung aufgenommen, um den externen Kosten/Nutzen der Qualität der Stromversorgung Rechnung zu tragen.

Die Versorgungssicherheit bezüglich der Stromnetze fließt unter dem Begriff „Qualität“ in die ARegV[302] ein, wobei die Begriffe Netzzuverlässigkeit und Netzleistungsfähigkeit unterschieden werden. Die Paragraphen §§ 18–20 der ARegV regeln die sogenannte Q-Komponente, wobei „Q“ für Qualität steht.

Das Thema Resilienz – wie oben definiert – ist von der Q-Komponente aus zwei Gründen nicht abgedeckt. Erstens sind die Indikatoren zur Bestimmung der Qualität nicht geeignet, um auch das Thema Resilienz mit abzudecken: Die Qualitätsindikatoren messen die Unterbrechung, nachdem sie stattgefunden hat, und zielen auf eine Vielzahl kleinerer Unterbrechungen. Im vorliegenden Kontext zielt Resilienz jedoch auf die Fähigkeit ab, das elektrische Energiesystem möglichst schnell nach großen und andauernden Versorgungsausfällen wieder betriebsfähig zu haben. Resilienz setzt daher an einem anderen Punkt an als die Qualität: Resilienz ist präventiv und vorausschauend. Zweitens liegen die Ursachen für die Ausfälle, die hier im Kontext der Resilienz im Fokus stehen, meist außerhalb der Kontrolle der Netzbetreiber, die demzufolge nicht haften. Folglich sind die monetären Konsequenzen ebenfalls außerhalb der ARegV gehalten.

Daher gilt es, in Ergänzung zur Qualität effektive resilienzverbessernde Anreize für die Netzbetreiber in die ARegV zu integrieren, ohne dass die Netzbetreiber in die

302 ARegV 2019.

Haftung genommen werden und das wirtschaftliche Risiko für die Netzbetreiber zu stark erhöht wird.

Was kann man heute tun? Auch wenn Netzbetreiber für die nicht kontrollierbaren Versorgungsausfälle nicht haften, haben sie durchaus Einfluss auf die Resilienz. Die Konsequenz eines Resilienzmanagements wird in aller Regel sein, dass Kosten entstehen und der Netzbetrieb kurzfristig nicht im Sinne der aktuellen ARegV betriebswirtschaftlich optimiert wird. So könnten etwa die folgenden Kosten entstehen, die die kurzfristige Effizienz der Netzbetreiber negativ beeinflussen würden:

- Ausgaben der Netzbetreiber, um die Resilienz bei den Netznutzern zu verbessern, etwa durch technische Maßnahmen am Netzanschlusspunkt.
- Ausgaben für bessere IT-Infrastruktur.
- Kosten für resilienzverbessernde Redundanzen im Netz.

Ohne flankierende Anreize wird der Netzbetreiber die externen Kosten (also all die Kosten, die bei einem länger andauernden Ausfall nicht bei ihm selbst anfallen) des Versorgungsausfalls nicht berücksichtigen; genau deshalb bräuchte die ARegV eine zusätzliche Regelung zur Verbesserung der Resilienz: eine R-Komponente, mit „R“ für Resilienz.

Folgende Fragen sind für die konkrete Umsetzung einer Resilienzkomponente zu beantworten:

- Was wären die geeigneten Indikatoren für eine Resilienzkomponente?
  - Insbesondere: Wie wäre der geeignete zeitliche Bezug? Die Maßnahmen sind präventiv, was von einem Indikator berücksichtigt werden muss.

  - Wichtig ist weiterhin, eine Doppeltrechnung von resilienzverbessernden Ausgaben, die anderweitig bereits abgedeckt sind, zu vermeiden.

- Was wären geeignete Instrumente, um die Anreize für die Netzbetreiber zu verbessern? Denkbare Optionen (wobei das geeignete Instrument auch vom gewählten Indikator abhängt) wären zum Beispiel:
  - Ein Bonus-Malus-System, ähnlich der Q-Komponente, das einen finanziellen Anreiz für resilienzverbessernde Maßnahmen setzt.

  - Ein Cost-pass-through-Mechanismus, wobei gilt, dass die resilienzverbessernden Ausgaben abgrenzbar sein müssen. Dieser Mechanismus hätte den Effekt, dass Kosten der resilienzverbessernden Maßnahmen aus Sicht der Netzbetreiber budgetneutral wären, da sie diese auf die Netznutzer (ohne Zu- oder Abschläge) umlegen könnten.

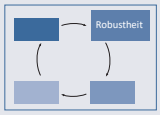
  - Der indirekte Weg durch das Benchmarking im Rahmen der ARegV, indem der Indikator als Output aufgenommen wird und Ausgaben in die normale Anreizwirkung fallen. Dies bedeutet zunächst, dass die Kosten für resilienzverbessernde Maßnahmen einem Kostendruck unterliegen würden, zugleich aber die Effizienz dieser Maßnahmen im Benchmarking (bei dem die Maßnahmen der Netzbetreiber verglichen werden) honoriert würde. Letztlich soll so sichergestellt werden, dass die resilienzverbessernden Maßnahmen möglichst kostengünstig und wirksam gestaltet werden.

Diese Auflistung ist nicht abschließend, und die Optionen sind hier nur angedeutet und müssten in einem ersten Schritt ausgearbeitet werden. Die Umsetzung braucht noch vertiefte Analyse. Alle Optionen haben Vor- und Nachteile, die in erheblichem Maße von den Details der jeweiligen Ausgestaltung abhängen. In Abhängigkeit des gewählten Instruments sollten die Parameter eine gute Balance zwischen Effektivität der Anreize und Risiko für die Netzbetreiber darstellen.

Bewertung: Die Umsetzung einer solchen Resilienzkomponente ab der vierten Regulierungsperiode (mit Start 2024) erscheint erreichbar. Da ein Branchendialog unter Leitung des BMWi zu einer weiteren Novelle der ARegV bereits läuft, wäre es grundsätzlich möglich, dieses Thema dort noch aufzunehmen. Diese Option wirkt indirekt und präventiv, denn die Resilienzkomponente verbessert die Anreize. Da die Resilienzkomponente indirekt und präventiv wirkt, hat sie keinen Einfluss auf die Anreize im Falle eines Blackouts. Die Wirkung entfaltet sich über Anreize, und somit liegen die Umsetzung und das Management beim Netzbetreiber und nicht beim Regulierer.

Eine Herausforderung dürfte insbesondere die Definition geeigneter Indikatoren und objektiv bestimmbarer Parameter sein. Hingegen dürften die Kosten der Maßnahme gering ausfallen. Da das System durch die Maßnahme einen Beitrag zur Vermeidung von großflächigen, lang andauernden Versorgungsausfällen leistet, können Kosten vermieden werden. Eine Kosten-Nutzen-Abschätzung hierzu muss allerdings noch erfolgen.

Handlungsoption 11:
Resilienzverbessernde Netzentgelte und Anschlussgebühren einführen



Ergebnis: Durch eine Novellierung der StromNEV wird es den Netzbetreibern ermöglicht, Netznutzungsentgelte effektiv resilienzverbessernd anzupassen.

Dringlichkeit: ● ● **Wirksamkeit:** ● ●

Was kann man heute tun?

- Smart Connection Agreements um eine Resilienzbetrachtung erweitern, sodass resilienzverbessernde Standortentscheidungen und Vermeidung von Gleichzeitigkeiten belohnt werden.

Langfristiger Lösungsbeitrag: Die Netznutzungsentgelte im weiteren Sinne werden in der Verordnung über die Entgelte für den Zugang zu Elektrizitätsversorgungsnetzen (§§ 15 ff. StromNEV) geregelt. Die StromNEV[303] klärt die Struktur der Netznutzungsentgelte, jedoch nicht deren Höhe. Vielmehr leitet sich die Höhe der Netznutzungsgebühren aus der Erlösobergrenze und damit aus der ARegV ab. Zwei Unterscheidungen bei den Netznutzungsgebühren sind für die Betrachtung im Kontext der Resilienz besonders wichtig:

- Die Tarifstruktur: Üblicherweise werden hier vier Komponenten unterschieden. 1. Arbeitspreis (Euro pro Kilowattstunde), 2. Kapazitätspreis (Euro pro Kilowatt), 3. Grundpreis (Euro pro Jahr) und 4. einmalige Anschlussgebühr.

- Die Kostenverteilung: Wer bezahlt? Nur der Abnehmer oder auch der Einspeiser (Erzeuger)?

303 StromNEV 2019.

Die Differenzierung der Netznutzungsentgelte kann darüber hinaus grundsätzlich verfeinert werden, insbesondere zeitlich und räumlich. Resilienz ist bislang kein Differenzierungskriterium. Die StromNEV regelt die Details der Kalkulation der Netzentgelte, sodass hier wenig Spielraum für Netzbetreiber verbleibt, um etwa resilienzförderndes Verhalten oder Maßnahmen der Netznutzer, die positiv auf die Resilienz des elektrischen Energiesystems wirken, über die Netzentgelte zu honorieren. Deshalb können die Netzbetreiber auch nicht selbstständig und auf eigene Initiative die Netznutzungsentgelte effektiv resilienzverbessernd anpassen. Eine solche Anpassung bedarf einer Novellierung der StromNEV.

Was kann man heute tun? Im Kontext der Resilienz des elektrischen Energiesystems erscheinen in Bezug auf die Netznutzung und deren Bepreisung insbesondere zwei Aspekte derzeit besonders relevant:

- Gleichzeitigkeitseffekte: Diese treten auf, wenn viele Anlagen oder Akteure wie zum Beispiel Händler gleichzeitig auf externe Impulse reagieren und damit große Schwankungen und Systeminstabilität verursachen. In einem digitalisierten elektrischen Energiesystem kann etwa die hohe Marktdurchdringung einer spezifischen Software ursächlich für Gleichzeitigkeiten sein. Alternativ können solche Überschneidungen im Nutzerverhalten auch dann auftreten, wenn verschiedene Softwarelösungen den gleichen externen Parameter nutzen, um automatisierte Handlungen zu initiieren (zum Beispiel analog zur 50,2-Hertz-Problematik, siehe Infobox „50,2-Hertz-Problem“), oder wenn viele Händler mit vergleichbarer Software arbeiten und es so zu extremen Schwankungen an den Märkten kommt, die dann die technischen Grenzen des Systems erreichen und so die Resilienz des elektrischen Energiesystems reduzieren.

- Netztopologie: Diese zielt auf resilienzverbessernde Standortentscheidungen (kurz- und langfristig) der Netznutzer. Die Resilienz des Gesamtsystems, insbesondere die Auswirkungen auf andere Netznutzer, ist derzeit nicht Teil der rationalen betriebswirtschaftlichen Überlegungen der Netznutzer; Standortentscheidungen werden aufgrund ganz anderer Überlegungen getroffen.

In beiden Fällen kann ein differenzierteres Netznutzungsentgelt lenkend wirken, um die Resilienz des elektrischen Energiesystems zu erhöhen. Derzeit wird viel über Smart Connection Agreements[304] diskutiert. Smart Connection Agreements sollen bereits bei der Netzanschlussgebühr, insbesondere bei erneuerbaren Energien, Netzknappheiten berücksichtigen. Unter Anwendung dieser Smart Connection Agreements kann ein Investor zwar durchaus an einem Standort investieren, an dem das Netz bereits überlastet ist oder durch die neu anzuschließenden Anlagen überlastet wird, muss dann aber damit rechnen, häufiger abgeregelt zu werden oder höhere Anschlusskostenbeiträge zu bezahlen (siehe dazu das Instrument „Netzausbauzuschuss“ im Referentenentwurf des Kohleausstiegsgesetzes). Die Details regeln die Smart Connection Agreements. Bei der Definition solcher Smart Connection Agreements stehen die Anschlusszeit und die Anschlusskosten im Vergleich zur möglichen Abregelung von Erzeugungskapazitäten im Fokus, um die dem Netzbetreiber im Rahmen des Engpassmanagements zugängliche Flexibilität im System zu erhöhen: Je schneller und kostengünstiger der Anschluss

304 Smart Connection Agreements bezeichnen flexible Netzanschlussbedingungen für Erzeuger, die dem Netzbetreiber die Möglichkeit der Abregelung (mit oder ohne Entschädigung für den Erzeuger) einräumen. Solche flexiblen Netzanschlussbedingungen befinden sich aktuell in Erprobung, etwa in Frankreich, Belgien und dem Vereinigten Königreich (Furusawa et al. 2019).

bereitgestellt wird, desto geringer die gesicherte Einspeisung (beziehungsweise desto höher die potenzielle Abregelung).

Es läge nahe, genau solche Smart Connection Agreements um eine Resilienzbetrachtung zu erweitern: Netznutzer mit resilienzverbessernden Standortentscheidungen und/oder mit Abbau von Gleichzeitigkeiten werden belohnt (zum Beispiel durch einen schnelleren und/oder günstigeren Netzanschluss) und umgekehrt. Die genaue Ausgestaltung wird sehr von den Details des Netzes bestimmt. Deshalb sollte die Umsetzung flexibel und fallabhängig beim Netzbetreiber liegen; die StromNEV kann nur den Rahmen abstecken, der den Netzbetreibern solche flexiblen Smart Connection Agreements erlaubt. Aber auch hier gilt, dass der Netzbetreiber das Instrument der Smart Connection Agreements erst dann zur Steuerung von resilienzverbessernden Maßnahmen einsetzen wird, wenn sich aus der ARegV ein entsprechender Anreiz für ihn ergibt (Vergleich Handlungsoption 10).

Bewertung: Die vorgeschlagenen Maßnahmen sollten zeitnah umgesetzt werden. Es würde sich zum Beispiel anbieten, das Thema Resilienz bei einer nächsten Novelle der StromNEV aufzunehmen. Die Umsetzung liegt bei den Netzbetreibern, die so die Möglichkeit haben, Netznutzer resilienzverbessernd zu lenken. Grundsätzlich gilt hier jedoch, dass diese Anpassungen der StromNEV bedingen, dass die Netzbetreiber zunächst durch eine Anpassung der ARegV entsprechende Anreize zur Steigerung der Resilienz erhalten, wie in der Handlungsoption 10 beschrieben. Als wie effektiv sich die Maßnahme erweist, ist fallabhängig: Manche Anreize dürften sehr wirksam sein, andere gar nicht. Dies muss entsprechend geprüft werden. Außerdem zieht eine Anpassung der Tarifstruktur an einer Stelle häufig Anpassungen an anderer Stelle nach sich. Darüber hinaus kann sich auch politischer Widerstand durch diejenigen entwickeln, die zusätzlich bezahlen müssen.

Die Umsetzungskosten werden als gering eingeschätzt. Zudem können Kosten vermieden werden, da das System einen Beitrag zur Vermeidung von großflächigen, lang andauernden Blackouts leistet.

6.6 Handlungsfeld 6: Beteiligung von Privatakteuren bei der Gestaltung und Umsetzung von Resilienz sicherstellen

Problem 2040: Durch die bestehende gute technische Vernetzung bergen die Erzeugungsanlagen von Privatakteuren großes Potenzial für die Stützung und Resilienz des Energiesystems. Um das Potenzial zu nutzen, sind jedoch Eingriffe in das private Umfeld der Akteure notwendig. Werden die Eingriffsoptionen den Privatakteuren nicht gut erklärt und transparent gehandhabt, besteht die Gefahr, dass Maßnahmen zur Erhöhung der Resilienz nicht greifen. Zudem haben Privatakteure einen wachsenden Einfluss auf die Systemstabilität. Zu wenig Bewusstsein darüber kann negative Effekte auf die Systemstabilität haben.

Erläuterung: Privatakteure nehmen auf der einen Seite eine zunehmend aktive Rolle ein und wirken bereits heute aktiv an der Gestaltung des Energiesystems mit, zum Beispiel als Prosumer oder Energiegenossenschaften, die Wind- und PV-Anlagen betreiben, Quartierslösungen, in denen sich private Haushalte selbst organisieren und lokal Energie austauschen können oder indem sie sogenannte Balkon-PV-Anlagen

installieren (siehe Infobox Abschnitt 2.2 „Steckbare Solargeräte, Balkonkraftwerk, SolarRebell oder Guerilla-PV“). Auf der anderen Seite liegen die Barrieren bei der Umsetzung der Energiewende zunehmend in gesellschaftlichen Konflikten.[305]

Das Potenzial der Digitalisierung und Vernetzung für die Resilienz kann durch die Netzbetreiber unter anderem wie folgt genutzt werden:

- Direkte Steuerung der Anlagen durch den Netzbetreiber, zum Beispiel um kritischen Systemzuständen vorzubeugen (siehe Handlungsoption 9). Hier ist zu unterscheiden zwischen zwei Arten von Eingriffen:
  - Die Privatakteur merkt selbst nichts von dem Eingriff, da nur solche Flexibilitäten genutzt werden, die der Akteur selbst nicht benötigt.
  - Die Privatakteur merkt den Eingriff durch Einschränkung seines Nutzungsverhaltens.
- Selektives An- oder Abschalten von Anlagen für den Inselbetrieb im Notfall (siehe Handlungsoption 7). Durch die Installation von intelligenten Schaltern auch auf Niederspannungsebene könnte Lastabwurf noch detaillierter erfolgen als bisher. Dies erleichtert umgekehrt auch den Aufbau von Inselnetzen, da Verbrauch und Erzeugung leichter ausbalanciert werden können (siehe Handlungsoption 7).
- Sammeln von Daten: Dadurch können Verbrauchsprofile verbessert werden, wodurch die Einsatzplanung optimiert werden kann und weniger Regelleistung notwendig wird.

Ob es in Zukunft notwendig sein wird, diese Maßnahmen durchzuführen, um das digitalisierte, dezentralisierte Stromnetz stabil zu halten, kann heute noch nicht abschließend beurteilt werden. Ein kategorisches Ausschließen dieser Maßnahmen würde jedoch Pfadabhängigkeiten erzeugen, die bei der ungewissen Zukunft ein Risiko darstellen. Daher ist es wichtig, heute schon zu betrachten, welche Anforderungen die Umsetzung dieser Maßnahmen mit sich bringen würde, insbesondere auch in Bezug auf die Akzeptanz von Privatakteuren (siehe Abschnitt 2.2). Letztendlich bedeuten all diese Maßnahmen immer einen Eingriff in das private Umfeld der Akteurinnen und Akteure. Dabei geht es sowohl um konkrete Rechte, die berücksichtigt werden müssen (beim Sammeln von Daten zum Beispiel der Schutz der Privatsphäre), als auch um Sorgen (zum Beispiel, dass Verbrauchs- und Nutzungsdaten Aufschluss über die Lebensführung geben könnten oder dass der Eingriff durch Netzbetreiber das eigene Handeln einschränkt, wenn zum Beispiel das Elektroauto nicht geladen ist), die adressiert werden müssen.

Die Umsetzung einer Maßnahme kann entweder auf freiwilliger Basis erfolgen oder durch den Gesetzgeber vorgegeben werden, abhängig davon, wie wichtig eine zeitnahe und vollständige Umsetzung für die Resilienz ist. In beiden Fällen können Probleme auftreten, von denen folgende hervorgehoben werden sollen:

- Freiwilliges System
  - **Fehlendes Verständnis:** Die Privatakteure sind sich ihres Einflusses auf das übergeordnete, recht komplexe System nicht bewusst; dadurch kann ihr Verhalten zu systemkritischen Zuständen beitragen (zum Beispiel Sicherheitsupdates von Geräten werden nicht durchgeführt etc.).

305 Wie etwa die Abstandsregeln für Windkraftanlagen oder der stockende Übertragungsnetzausbau.

- **Fehlende Akzeptanz:** Die technischen Voraussetzungen können nicht geschaffen werden, da die Akteure nicht bereit sind, etwa Zähler mit Schalt- und Regelvorrichtungen zu installieren. Technische Lösungen insgesamt können nicht umgesetzt werden oder Verbraucher reagieren nicht auf Anreize. In diesem Zusammenhang ist auch das Thema Datenschutz[306] relevant.

• Reguliertes System
  - **Verlust der Selbstbestimmung:** Die Akteure verlieren ihre Selbstbestimmung, da ihr Verbrauch oder ihre Erzeugung eingeschränkt wird oder sie – im Fall der direkten Steuerung durch den Netzbetreiber – keinen Einfluss mehr auf ihre eigenen Anlagen und Geräte haben. Dadurch kann Akzeptanz sinken.

  - **Vertrauensverlust:** Wenn in das System (etwa zum Wiederaufbau nach einem Blackout) eingegriffen werden kann und dies nach nicht nachvollziehbaren Kriterien in ungleicher Weise geschieht (etwa, dass der Strom in einem Straßenzug wiederhergestellt wird, während ein anderer warten muss), dann kann das als mangelnde Fairness erlebt werden, und Vertrauensverluste gegenüber den Systemverantwortlichen (in diesem Fall die Netzbetreiber) können auftreten.

Die angesprochenen Probleme können dazu führen, dass das Potenzial privater Anlagen zur verbesserten Resilienz nicht genutzt werden kann, Lösungen nicht umgesetzt werden können, neue Regelungen nicht greifen oder systemkritische Situationen erst auftreten. Alle Akteure müssen gleichermaßen berücksichtigt und erreicht werden. Es ist davon auszugehen, dass es unter den Privatakteuren einerseits solche mit hoher Informiertheit und Interesse gibt, andererseits aber auch Menschen, die sich damit nicht selbst befassen wollen, sondern erwarten, dass staatliche Kontrollinstanzen ihre Rechte schützen. Daneben wird es auch verunsicherte oder verunsicherbare Menschen geben, die technischen Innovationen oder relevanten Akteuren (Energieversorger, Kontrollinstanzen) nicht vertrauen, bis hin zur Unterstellung schädigender Absichten (Verschwörungstheorien). Privatakteure, die Interesse an den Zusammenhängen der digitalisierten Energieversorgung haben oder entwickeln, insbesondere die Prosumer, werden höhere Ansprüche an die Gestaltung und die Einbindung in Entscheidungsprozesse artikulieren.

Zeithorizont des Problems: Privatakteure müssen heute schon als für die Resilienz relevant angesehen und die verbesserte Einbindung dieser Akteure bezüglich der Eingriffsnotwendigkeit so schnell wie möglich angegangen werden. Die Digitalisierung schreitet mit hoher Geschwindigkeit voran und bringt ständig Neuerungen mit sich; die notwendigen begleitenden gesellschaftlichen Diskurse entwickeln sich erst langsam. Der Zeitdruck für den Einsatz neuer Technologien und Lösungen ist groß. Dies macht umfassende Bildung zum Thema Digitalisierung notwendig.[307]

Heute bereits bestehende Maßnahmen: Bereits heute wird der Weg beschritten, bei Entscheidungsprozessen durch die Bundesregierung gesellschaftliche Gruppen frühzeitig einzubeziehen und an der Gestaltung von Institutionen mitwirken zu lassen. Die geplanten Reallabore des BMWi im 7. Energieforschungsprogramm haben die Aufgabe, gesellschaftliche Fragestellungen zu untersuchen. Eine ausführliche

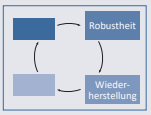
306 Datenschutz ist ein sehr wichtiges Thema, gerade um die Akzeptanz in der Bevölkerung zu fördern. Datenschutz wird hier nur am Rande betrachtet, da er nicht direkt für die Systemstabilität relevant ist.

307 WBGU 2019.

Analyse zu den soziotechnischen Fragestellungen eines Blackouts im Zusammenhang mit einer dezentral orientierten Stromversorgung wurde im Projekt SES erarbeitet.[308]

Im Zuge des IT-Sicherheitsgesetzes 2.0 plant das Bundesministerium des Innern die Einführung eines IT-Sicherheitskennzeichens. Damit sollten die Verbraucher über die Cyber-Resilienz eines Produkts informiert werden, was langfristig die Qualität der im Gebrauch befindlichen Produkte bezüglich der Cyber-Sicherheit verbessern könnte.

Handlungsoption 12: Ein Stakeholder-Gremium zur Berücksichtigung der Belange von Privatakteuren entwickeln



Ergebnis: Alle relevanten Akteure sind durch einen fortlaufenden und transparenten Prozess in Entscheidungsfindungen für neue Regelungen einbezogen.

Dringlichkeit: ● ● ● **Wirksamkeit:** ● ●

Was kann man heute tun?

- Ein Stakeholder-Gremium entwickeln, das akzeptable Lösungen für Privatakteure schafft und transparent handhabt.

Langfristiger Lösungsbeitrag: Ziel ist es, einen Prozess zu entwickeln, der alle relevanten Akteure in die Entscheidungsfindung für neue Regelungen, die Privatakteure betreffen, einbezieht. Neben dem Regulierer sowie den Privatakteuren selbst sind das vor allem Netzbetreiber, Aggregatoren, Verbände und Verbraucherzentralen. Hierbei sollte es sich um einen fortlaufenden, transparent gestalteten Prozess handeln, da es ständig technische Neuerungen und neu auftretende Akteure geben wird. Die Privatakteure sollten angemessen adressiert und als Partner mit eigenen Interessen und Befürchtungen etc. ernst genommen werden. Ziel des Stakeholder-Gremiums sollte es sein, möglichst gesellschaftlich konsensfähige Lösungen zu finden.

Zusätzlich sollte die Politik dazu Studien und Forschungsprojekte anregen, die im Schwerpunkt rechtliche, ethische und sozialwissenschaftliche Aspekte analysieren. Diese Studien und Projekte stehen unter anderem vor zwei großen Herausforderungen: Erstens lassen sich Erfahrungen und Daten, die in Studien aus anderen Ländern erfasst wurden, oft nicht übertragen, da sich gesellschaftliche Bedingungen und Einstellungen zu sehr unterscheiden. Zweitens ändern sich Wertvorstellungen, Einstellungen zu Datenschutz oder Bereitschaft zur Akzeptanz[309] rechtlicher Vorgaben über die Zeit, sodass Erfahrungen von heutigen Projekten schwerer in zukünftige Vorhaben zu übertragen sind.

Was kann man heute tun? Zunächst sollten für eine konkrete Fragestellung (wie etwa direkte Steuerung oder selektiver Lastabwurf) die relevanten Akteure bestimmt und ein Stakeholder-Gremium geschaffen werden, das Maßnahmen ableitet, die möglichst die Interessen aller Akteure berücksichtigen. Da eine Universallösung gesellschaftlich kaum akzeptabel sein wird, sollte hier zumindest eine Mehrzahl an Lösungen angedacht werden, die für verschiedene Nutzergruppen (Prosumer, Genossenschaft, Verbraucher etc.) wählbar sind. Besonders sensibel ist die Akzeptanz solcher

308 Burkart et al. 2014.

309 Beispiel ist etwa die Akzeptanz von Infrastrukturvorhaben (siehe zum Beispiel acatech 2011).

Regelungen durch die Privatakteure. Entstehende Fragen und Befürchtungen, die etwa Datenschutz und Eingriffe in die Privatsphäre betreffen, sollten frühzeitig aufgegriffen und berücksichtigt werden.

Zusätzlich müsste in diesem Stakeholder-Gremium auch entschieden werden, welche der Maßnahmen für die Resilienz kritisch sind und daher verpflichtend umgesetzt werden müssen und welche über geeignete Anreizsysteme umgesetzt werden können. Hierfür gibt es verschiedene Möglichkeiten, wie zum Beispiel:

- **Freiwillige Selbstbeschränkung:** Privatakteure schränken im Notfall ihren Verbrauch oder ihre Erzeugung freiwillig ein, um das System zu entlasten. Dazu sind jedoch ein geeignetes Informationssystem und Basiswissen über den Systemeinfluss von Privatakteuren notwendig (siehe Handlungsoption 13).

- **Finanzielle Anreize:** Über finanzielle Anreize können private Netznutzerinnen und -nutzer motiviert werden, ihre Erzeugungsanlage im sehr seltenen Krisenfall zur Systemstabilisierung freizugeben, das heißt zum Beispiel dem Netzbetreiber zu erlauben, die Anlagen abzuregeln.

- **Finanzielle AnrMarktliche Anreize:** Über marktliche Anreize wie etwa variable Tarife[310] kann eine indirekte Steuerung der Erzeugungsanlagen von Privatakteuren erzielt werden. Im Gegensatz zu den beiden vorgenannten Optionen, die im Krisenfall greifen, zielt diese auf eine Entlastung des Systems im Normalbetrieb ab.

- **Verpflichtende Beiträge:** Private Erzeugungsanlagen werden über die technischen Anschlussbedingungen zur Abschaltbarkeit oder Steuerbarkeit verpflichtet; eine sinnvolle Leistungsgrenze ist zu bestimmen.

Die ersten zwei der genannten Möglichkeiten könnten Teil der Energiedienstleistungen sein, die sich im Zuge der Dezentralisierung und Vernetzung entwickeln – wie zum Beispiel Heimenergiemanagementsysteme – oder aber auch als Teil der Versorgungsverträge umgesetzt werden. In diesem Fall haben sich die Privatakteure aktiv für die Abschaltbarkeit und Steuerbarkeit entschieden beziehungsweise diese akzeptiert. Für die Umsetzung dieser Anreizsysteme sind ebenfalls entsprechende technische Lösungen zu entwickeln. Hierbei ist zu beachten, dass es sich um sogenannte Plug-and-Play-Lösungen handeln sollte, das heißt, diese funktionieren, ohne umfangreiche Installationen oder Konfigurationen vornehmen zu müssen. Die Verantwortung dafür, dass solche Lösungen technisch funktionieren und wie gewünscht zur Resilienz beitragen, sollte nicht bei den Privatakteuren liegen, sondern durch Hersteller und Systembetreiber übernommen werden.

Es sollten zunächst geeignete Untersuchungen in Forschungsprojekten durchgeführt und neue Regelungen zunächst in Experimenten oder Reallaboren erprobt werden. Hierfür eignen sich zum Beispiel Quartierslösungen, in denen es bereits eine Beteiligung von Privatakteuren gibt. Die Untersuchungen sollten national und international angelegt sein. So können Lösungen entstehen, die für einen breiteren Markt geeignet und somit für Hersteller attraktiver sind.

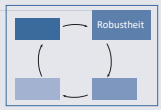
310 Tarife, in denen die Kilowattstunde Strom zu Spitzenlastzeiten verteuert wird und bei geringer Netzbelastung der Strom günstiger bezogen werden kann.

Die Effekte von Anreizsystemen und Regulierungen können auch immer Rückwirkungen – positive und negative – auf das elektrische Energiesystem haben. Anreize müssen daher so gestaltet werden, dass sie einerseits die gewünschte Wirkung entfalten und andererseits negative Rückwirkungen verhindert oder aufgefangen werden. Auch eine potenzielle Ablehnung durch die Akteure muss berücksichtigt werden.

Bewertung: Die Akzeptanz der Bevölkerung und der verschiedenen Akteursgruppen sowie deren aktive Mitgestaltung der Digitalisierung des Energiesystems und der dafür relevanten Regeln ist zentral für langfristige Resilienz. Die Optionen sollten kurzfristig angegangen werden, da sich die Ziele nur langfristig umsetzen lassen. Diese Handlungsoption hat den Vorteil, dass sie in einer aktiven Bürgerbeteiligung sowie einer verbesserten Ansteuerbarkeit von privaten Anlagen und Geräten zur Systemstabilisierung resultieren würde. Es ist allerdings fragwürdig, ob mit Freiwilligkeit genug Potenzial zur Systemstützung zur Verfügung stünde. Erfahrungen aus anderen Ländern lassen vermuten, dass finanzielle Anreize oft nicht ausreichen, sondern vielmehr Akzeptanz durch Einbeziehung und Verständnis erreicht wird. Im Fall von Regulierung besteht die Gefahr einer Einschränkung der Souveränität der Privatakteure.

Auf der einen Seite erfordern Beteiligungsprozesse Zeit und sind dadurch kostenintensiv. Andererseits können durch frühzeitige Einbeziehung der Akteure technologische Fehlentwicklungen vermieden werden, da direkt „legitime" Technologien und Umgangsweisen mit diesen implementiert werden können. Dies kann zu Kostenersparnissen führen.

Handlungsoption 13: Bewusstsein für den Einfluss privater Akteure schaffen



Ergebnis: Privatakteure haben eine Vorstellung von ihrem Einfluss auf die Stabilität des elektrischen Energiesystems und sind „digital mündig".

Dringlichkeit: ● ● ● **Wirksamkeit:** ● ●

Was kann man heute tun?

- Informations- und Bildungskampagnen zum Thema Resilienz für verschiedene Zielgruppen, die zielgruppenspezifische Informationsbedürfnisse berücksichtigen.

Langfristiger Lösungsbeitrag: Für die Privatakteure sollte besser nachvollziehbar gemacht werden, welchen Einfluss ihr Verhalten auf die Stabilität des elektrischen Energiesystems hat und welche Beiträge sie leisten können, um die Stabilität zu unterstützen, indem sie etwa zeitnah aktuelle Updates von ihren Geräten installieren oder im Inselnetzfall keine unnötigen Verbrauchsgeräte nutzen. Hier gilt es, ein Problembewusstsein, digitale Mündigkeit und ein minimales Verständnis für die komplexen Zusammenhänge im Energiesystem zu fördern. Das Verständnis der Privatakteure zu verbessern, kann auch dazu beitragen, dass technische Maßnahmen, wie das Abregeln von kleinen Erzeugungsanlagen im Notfall, besser akzeptiert werden (siehe Handlungsoption 12).

Es kann nicht der Anspruch bestehen, dass Privatakteure das System bis ins Detail verstehen. Dennoch müssen Betroffene die Möglichkeit der umfassenden Information haben, sofern ihre Rechte und Interessen berührt werden. Im Sinne der Transparenz und des Vertrauens ist es notwendig, Informationsangebote aufzubauen,

die den jeweiligen Informationsbedürfnissen entsprechen. Die Verantwortlichkeit für Cyber-Sicherheit liegt jedoch nicht bei den Verbrauchern, sondern bei Herstellern, Betreibern und weiteren Akteuren (siehe Handlungsfeld 2/Abschnitt 6.2).

Was kann man heute tun? Um den Einbezug der Privatakteure und deren Souveränität zu gewährleisten, sollten im ersten Schritt Informationsangebote wie Kampagnen entwickelt und realisiert sowie Bildungsangebote in Schule und Weiterbildung eingebunden werden. In den Informations- und Bildungsangeboten sollten mindestens die folgenden Aspekte Berücksichtigung finden:

- Welche Auswirkungen hat das eigene Verhalten auf das Netz, und wie kann vermieden werden, dass es zu Instabilitäten beiträgt?

- Warum ist es sinnvoll, im Falle eines Not- oder Inselbetriebs den eigenen Verbrauch freiwillig einzuschränken? Wie verhalte ich mich systemstabilisierend in einem Inselnetzfall?

- Wie kann ich mich im Falle eines Blackouts verhalten, damit das System möglichst bald wieder an- und hochgefahren werden kann?

- Warum ist es wichtig, aktuelle Softwareupdates für die eigenen Anlagen zeitnah zu installieren?

Die Informations- und Bildungskampagnen sollten flächendeckend Anwendung finden und alle Bevölkerungsgruppen ansprechen. Dabei ist es wichtig, Informationen an die unterschiedlichen Informationsbedürfnisse in transparenter Weise anzupassen, etwa durch ein Informationsportal für unterschiedliche Zielgruppen und mit unterschiedlichen Kommunikationsformaten, um die (digitale) Souveränität der Privatakteure zu stärken. Solche Maßnahmen könnten noch effektiver gestaltet werden, wenn sie auf einer verhaltensanalytischen Grundlage geplant werden, da so verschiedene Aspekte individuellen Verhaltens berücksichtigt und besser angesprochen werden können. Es können auch Konzepte wie das oben genannte IT-Sicherheitskennzeichen helfen, dass sich die Privatakteure beim Thema Cyber-Sicherheit informieren und beteiligen können. Der Diskurs um die Digitalisierung und Vernetzung und deren Chancen ist im Allgemeinen positiv besetzt, was auch für die Vermittlung der Chancen der Digitalisierung für die Energiewende genutzt werden sollte. Hier ergeben sich ebenfalls Schnittstellen mit der Bildung für Digitalisierung und Nachhaltigkeit.

Wichtig ist, dass die Anbieter der Bildungsangebote und insbesondere der Informationskampagnen nicht als interessengeleitet wahrgenommen werden. Insofern bieten sich Ministerien, Verbraucherschutzorganisationen oder Allianzen dieser Akteure als durchführende Organisationen an. Auch für die Vertrauensbildung gegenüber den Instanzen und Instrumenten, die erarbeitete Maßnahmen überwachen, ist das Einbeziehen relevanter Sachwalter der Privatakteure, hier insbesondere Verbraucherschutzorganisationen und Datenschutzinitiativen, zu berücksichtigen. Diese sollten sowohl an der Eingriffsausgestaltung als auch an der Kommunikation mitwirken.

Bewertung: Auch hier ist mit einer langen Umsetzungszeit von zehn bis zwanzig Jahren zu rechnen, da gesellschaftlicher Wandel langsam vonstattengeht und neue Praktiken und soziotechnische Innovationen nur über einen längeren Zeitraum die

gesamte Bevölkerung durchdringen. Im Grunde handelt es sich aber um einen kontinuierlichen Prozess, denn für den Bereich der Digitalisierung und Energiewende kann angenommen werden, dass neue Technologien zeitnah entwickelt werden, die derzeit nicht absehbar sind. Eine Kalibrierung gerade der Informationsstrategie und des Informationsangebots ist daher sinnvoll.

Durch die vorgeschlagenen Maßnahmen werden nicht nur Akzeptabilität und Akzeptanz gefördert. Es bilden sich auch Humankapital und digitale Souveränität. Ein langfristiger und stabiler Bildungsprozess kann entstehen. Allerdings sind Beteiligungswille und Bildungsinteresse nicht ohne Weiteres gegeben (eine Indoktrination kann nicht das Ziel sein). Gegebenenfalls werden Informationsangebote als Werbekampagne und interessengeleitet wahrgenommen. Dieser Gefahr kann aber durch Einbindung zivilgesellschaftlicher Akteure entgegengewirkt werden. Ein komplettes Verständnis ist für Privatakteure nicht möglich, da es nicht einmal für Expertinnen und Experten möglich ist, das zukünftige elektrische Energiesystem vollständig zu verstehen. Nichtsdestotrotz bedeutet dieses mangelnde Verständnis für die Privatakteure ein Stück weit „Entmündigung“. Das heißt, dass ein Vertrauensaufbau gegenüber den Urhebern der Information und den steuernden oder kontrollierenden Instanzen (sowohl technisch als auch regulatorisch) ebenso wichtig wird.

Die Umsetzung der Maßnahmen kann dadurch erschwert werden, dass Informationskampagnen und Bildungsangebote nie die gesamte Bevölkerung erreichen. Die Akteure sind zudem sehr heterogen, sodass nicht alle gleichermaßen abgeholt werden können. Maßgeschneiderte Angebote bieten hier aber Hilfe. Die Bildungsstrategie ist einzubetten in übergeordnete Bildungsstrategien zur Digitalisierung und Nachhaltigkeit. Diese Prozesse unterliegen aber gegebenenfalls auch wechselnden politischen Interessen.

Ähnlich wie bei Handlungsoption 12 können durch langfristiges Umdenken und Mitziehen aller Beteiligten dezentrale, kleine Lösungen erreicht und eingebunden werden. Wenn bei den Bürgerinnen und Bürgern ein gewisses Bewusstsein geschaffen werden kann, werden teure Ausnahmesituationen wie ein Blackout möglicherweise vermieden, was die Mehrkosten, die durch diese Handlungsoption entstehen, aufwiegt.

Bildung wirkt auf mehreren Ebenen und bereitet auch den Boden für weitere Resilienzmaßnahmen und beugt Ohnmachts- und Verschwörungsempfindungen vor. Die vorgeschlagenen Maßnahmen sind entscheidend, um Resilienz auf Dauer zu erreichen.

6.7 Handlungsfeld 7: Langfristige Risiko- und Resilienzbewertung institutionalisieren

Problem 2040: Fast alle Entscheidungen sowohl des Gesetzgebers als auch der für die Systemsicherheit verantwortlichen Netzbetreiber schaffen Pfadabhängigkeiten. Diese Entscheidungen basieren auf Erfahrungen, anerkannten Analysen und Regeln und Vermutungen über zukünftige Entwicklungen. Sie berücksichtigen jedoch bisher noch zu wenig, dass überraschende und unerwartete Entwicklungen die Systemsicherheit massiv beeinflussen können.

Erläuterung: Um die Systemsicherheit zu gewährleisten, werden auch in den nächsten zwei Jahrzehnten immer wieder Entscheidungen vom Regulator oder von den operativ tätigen Akteuren getroffen werden müssen. In Zukunft wird es vermutlich unvorhersehbare Trends geben, die etwa aus der Energiewende und der Digitalisierung (siehe Kapitel 2 und 3) entstehen und die sich als eine Bedrohung für die Systemsicherheit erweisen könnten. Bisher existieren eher wenige Ansätze, die gestatten, unerwartete und überraschende Entwicklungen zu antizipieren und Unsicherheiten zu begegnen. Dies ist sicherlich, wie die hohe Zuverlässigkeit und Qualität der Versorgung zeigen, kein Versäumnis von Politik oder Stromversorgern. Vielmehr waren bisher weitgehend evolutionär und linear verlaufende Entwicklungen sowohl leichter zu gestalten als auch besser vorhersehbar. Die Erfahrungen aus der Vergangenheit zusammen mit wohlbegründeten Annahmen über zukünftige Entwicklungen reichten bislang aus, um die richtigen Entscheidungen zu treffen. Dies wird in Zukunft so nicht mehr der Fall sein (siehe auch Kapitel 5). Zudem ändern sich in einem lang andauernden gesellschaftlichen Transformationsprozess Beurteilungen und Werteinstellungen, sodass die normativen Vorstellungen, unter denen Entscheidungen getroffen wurden, zu einem späteren Zeitpunkt nicht mehr gelten.

Diese Lücken waren und sind wesentliche Treiber, sich mit dem Konzept Resilienz auseinanderzusetzen. Maßnahmen lassen sich jedoch nur schwer nach ihrem Nutzen für die Resilienz bewerten, wenn einerseits Basisdaten aus vielen Störereignissen und deren Auswirkungen aus der Vergangenheit fehlen, andererseits auch Resilienzverbesserungen nicht ausreichend bewertbar und messbar sind. Dies führt zu Effektivitäts- und Effizienzverlusten bei der Sicherung der Resilienz.

Es stellt sich die Frage, wie die Politik Akteure zu Maßnahmen verpflichten und ihnen Kosten aufbürden kann, wenn es für die Resilienz eines Systems keine Standards, keine vereinbarten Kenngrößen und Verfahren gibt. Man kann zwar sowohl die Kosten der Maßnahmen als auch den Schaden eines vermiedenen Blackouts abschätzen, aber oft nicht, wie sehr sich das Blackout-Risiko durch eine Maßnahme (auch langfristig) ändert. Diese Situation ist in technischen Systemen nicht unbekannt und tritt beispielsweise auch bei der Cyber-Sicherheit auf. Im Laufe der Jahre haben sich daher viele Rahmenwerke und Ersatzmaße etabliert, mit denen erfolgreich gearbeitet wird, wie etwa Reifegradmodelle oder auch qualitative Risikomaße.

Zeithorizont des Problems: Aktuell sind Entwicklungen zur Digitalisierung und Energiewende, die bereits in wenigen Jahren massiven Einfluss auf die Systemsicherheit haben können und auf die innerhalb des Energiesystems planmäßig reagiert werden sollte, nicht zu erwarten. Sobald Digitalisierung jedoch einen größeren Einfluss auf die Energieversorgung gewinnt als heute, können überraschende Entwicklungen mit potenziellem großem Einfluss auf die Systemsicherheit deutlich schneller eintreten. Aus diesem Grund sollten Lösungen in den kommenden Jahren entwickelt und umgesetzt werden.

Heute bereits bestehende Maßnahmen: Derzeit wird auf EU-Ebene durch die Verordnung „Risikovorsorge im Elektrizitätssektor“[311] für die ÜNB eine umfangreiche und supranationale Risikobewertung institutionalisiert. Dazu gehört auch die

311 vgl. Verordnung (EU) 2019/941.

Benennung einer nationalen Krisenkoordinierungsstelle, die als Ansprechstelle im Fall einer Stromversorgungskrise fungieren soll. Die Verordnung konzentriert sich auf „Risikoszenarien“ als mögliche Ereignisse, die zu einem großen Blackout führen können, und fokussiert sich dabei auf die Übertragungsnetze, extreme Blackouts, einen mittleren Zeithorizont, absehbare Risiken und die dazu wirksamen Maßnahmen. Daher bleiben einige Lücken: So bleiben etwa langfristige Entwicklungen, überraschende Ereignisse und (aus Sicht des ENTSO-E-Gesamtnetzes) weniger gravierende Blackouts unberücksichtigt. Der Prozess der Szenarienerstellung unter Verantwortung der ÜNB bezieht nur wenig Expertise aus anderen Disziplinen ein. Dadurch kann ein Bias entstehen, da Menschen aus ähnlichen fachlichen Kontexten oftmals eine ähnliche Einschätzung zukünftiger Entwicklungen vornehmen.

Um Gefahren für Systemsicherheit bewerten zu können, existiert bereits heute – insbesondere auf der Ebene der Übertragungsnetze – eine große Anzahl an technischen Verfahren, die zudem stetig aufgrund neuer Erkenntnisse verbessert werden. Auch greift der Gesetzgeber beziehungsweise Regulierer immer wieder und meist schnell ein, wenn Ereignisse auftauchen, die das elektrische Energiesystem bedrohen.[312] Die hohe Versorgungsqualität in Deutschland ist wesentlich diesem Vorgehen zu verdanken. Es werden sehr wohl bekannte seltene Ereignisse und Ereigniskombinationen betrachtet, die große Stromausfälle verursachen könnten. Weniger im Fokus stehen jedoch Risikofaktoren, die sich kaum aus den bisherigen Erfahrungen erschließen, wie die Effekte einer zunehmenden Digitalisierung, die weit über die Systeme der Netzbetreiber hinausgeht. Die Lücke über die gesamte Branche und alle Akteure gesehen ist noch sehr groß. Es ist erkennbar, dass das bisher erfolgreich angewandte deterministische N-1-Prinzip ergänzt werden muss, um die Sicherheit zukünftiger, komplexerer Versorgungssysteme zu gewährleisten.

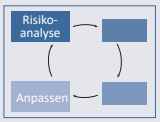
Das BSI ist heute die zentrale Meldestelle für Betreiber kritischer Infrastrukturen in Angelegenheiten der Sicherheit in der Informationstechnik.[313] Das dortige IT-Lagezentrum identifiziert, dokumentiert und analysiert Sicherheitsvorfälle und erstellt daraufhin Informationen und Warnungen. Es reagiert zeitnah auf Schwachstellen und Sicherheitsvorfälle. Zu diesem Zweck benötigt das IT-Lagezentrum stets ein Lagebild der Sicherheitslage in Deutschland. Außerdem fungiert das IT-Lagezentrum „als zentrale Meldestelle für IT-Sicherheitsvorfälle u.a. in der Bundes- und Landesverwaltung sowie den Kritischen Infrastrukturen“[314] und erstellt Lageberichte an das nationale Cyber-Abwehrzentrum (NCAZ). Im NCAZ arbeiten das Bundeskriminalamt (BKA), das BSI, der Bundesnachrichtendienst, das Bundesamt für Verfassungsschutz und die Polizeibehörden der Bundesländer zusammen und bewerten Cyber-Angriffe jeweils entsprechend ihrer Expertise aus informationstechnischer, nachrichtendienstlicher und polizeilicher Sicht. Dadurch kommt es zu einer Überschneidung zwischen Behörden, die rein für die Abwehr zuständig sind, und solchen, die sich auch mit Cyber-Angriffen beschäftigen, was zu Interessenkonflikten führen kann.

312 Mihm 2019.

313 Vgl. BSIG 2019 § 8b.

314 BSI 2018, S. 54.

Handlungsoption 14: Organisationsrahmen für die Meldung von Störfällen und die Resilienzbewertung schaffen



Ergebnis: Es gibt geeignete Organisationsstrukturen, um Störfälle zu erfassen und auszuwerten. Mögliche Risiken werden auf Grundlage objektiver Kenngrößen zur Resilienzbewertung systematisch bewertet und von Netzbetreibern und anderen relevanten Akteuren berücksichtigt.

Dringlichkeit: ● ● ● **Wirksamkeit:** ● ● ●

Was kann man heute tun?

- Eine zentrale und unabhängige Informations- und Meldestelle für Störereignisse aufbauen.
- Eine behördliche oder behördlich beaufsichtigte Institution aufbauen, die regelmäßig eine Risikobewertung durchführt.
- Geeignete Kenngrößen für Resilienz entwickeln und entsprechende Vorgaben schaffen.

Langfristiger Lösungsbeitrag: Es muss ein geeigneter institutioneller Organisationsrahmen geschaffen werden, um stärker auf den Umgang mit Unsicherheiten und unerwarteten Entwicklungen achten zu können. Dafür sollte das Konzept der Resilienz stärker in der Risikobewertung und in politischen Maßnahmen zur Bewahrung der Versorgungssicherheit verankert werden.

In einer zentralen europäischen Informations- und Meldestelle sollte bestehendes Wissen über Risiken, Störereignisse, relevante Cyber-Sicherheitslücken und mögliche Gegenmaßnahmen für den Netzbetrieb mehrsprachig verfügbar gemacht und stetig aktualisiert werden. Dabei sollen der Vertrauensschutz sowie die nationale Sicherheit der Mitgliedstaaten gewährleistet bleiben. Dies erfordert Meldepflichten im Energie- und Cyberbereich insbesondere für die Betreiber von Strom- und Kommunikationsnetzen sowie weitere Recherche und Aufbereitung von für die Resilienz relevanten Störereignissen und deren Behebung. Recherche und Aufbereitung könnten durch die Meldestelle geleistet werden; zudem könnten Empfehlungen formuliert werden. Es sollten nicht nur Störungen im Übertragungsnetz, sondern auch in den Verteilnetzen betrachtet werden, sofern diese als relevant für Blackouts eingeschätzt werden. Dazu ist einerseits eine enge und vertrauensvolle Zusammenarbeit mit den Netzbetreibern notwendig, andererseits muss die Institution weitgehend unbeeinflusst von den Netzbetreibern arbeiten können, um dem Gemeinwohl zu dienen.

Zudem sollte es eine behördliche oder behördlich beaufsichtigte Institution geben, die regelmäßig eine langfristig orientierte Risikobewertung durchführt. Diese Institution würde abschätzen, ob mögliche Entwicklungen erkennbar sind, die die mittel- und langfristige Bedrohungslage für Blackouts verändern könnten, und dazu jeweils Handlungsvorschläge für die Politik entwickeln. Im Rahmen einer Risikobewertung sollten Indikatoren zur Früherkennung von Bedrohungen erarbeitet und regelmäßig aktualisiert werden. Auch für den Umgang mit unbekannten, überraschenden Bedrohungen und Entwicklungen sollten Maßnahmen vorgeschlagen werden.

Derzeit existiert kein ausgearbeitetes gemeinsames Verständnis von Resilienz, das es erlauben würde, anhand von Standards, Kennzahlen und Bewertungsverfahren Maßnahmen zur Resilienzverbesserung bewerten zu können. Ein solches Verständnis

wird benötigt, um seitens der Politik Vorgaben zur Resilienzsicherung für die Akteure zu schaffen und zu bewerten.

Was kann man heute tun?
Eine zentrale, unabhängige Informations- und Meldestelle für Störereignisse aufbauen
Da nicht abschätzbar ist, wie schnell diese europäische Informationsstelle für den Energiebereich aufgebaut werden kann, kann die Politik im ersten Schritt eine nationale Stelle einrichten. Die Erfahrungen aus der nationalen Institution könnten später helfen, eine entsprechende europäische Stelle ins Leben zu rufen und zu gestalten. Unter Einbeziehung der relevanten Akteure und Netzbetreiber sollte ein Vorschlag zu den notwendigen Aufgaben und Prozessen einer nationalen Meldestelle erarbeitet werden. Dazu sind besonders die folgenden Fragen zu beantworten:

- Wer baut diese Stelle auf, und wie ist sie an andere Behörden angeschlossen oder in diese eingebettet?
- Welche Richtlinien werden dieser Institution vorgegeben, und wer setzt diese Richtlinien?
- Was wird in Ergänzung zu den heutigen Vorfällen meldepflichtig, und was wird wie ausgewertet?
- Wie ist die technische und personelle Ausstattung dieser Institution?
- Wie ist die Zusammenarbeit mit der nach der EU-Verordnung „Risikovorsorge im Elektrizitätssektor“ vorgesehenen Krisenkoordinierungsstelle[315]?
- Welche Verpflichtungen zur Meldung und auch zum Nutzen der vorgehaltenen Informationen werden den Netzbetreibern (und weiteren Akteuren der Energieversorgung) auferlegt?

Ein wesentlicher Aufgabenteil der vorgeschlagenen Stelle ist die Beschäftigung mit Cyber-Sicherheit, mindestens soweit diese in Beziehung zu dem sicheren Betrieb des elektrischen Energiesystems steht. Hierzu ist zu klären, wie eine Unabhängigkeit insbesondere von Behörden oder Ministerien erreicht werden kann, die, etwa zum Zweck der Verbrechensbekämpfung, Sicherheitslücken nutzen möchten. Die Informations- und Meldestelle sollte so transparent gestaltet sein, dass auch nationale Behörden und Notfallteams zeitnah über Vorfälle informiert werden. Zur Untersuchung der Gefahren sind unter anderem unabhängige Expertinnen und Experten einzubeziehen, etwa unter Leitung der BNetzA und des BSI. Um die Neutralität dieser Untersuchung zu gewährleisten, ist es notwendig, dass die Untersuchung von zusätzlichen politischen Vorgaben unabhängig ist.

Die neue Stelle sollte im engen Kontakt mit den Herstellern stehen und auch mit Sanktionsmöglichkeiten ausgestattet werden. Wird nach einer möglichst obligatorischen Prüfung festgestellt, dass eine Sicherheitslücke zur Gefährdung des Energiesystems führt, sollte die Energieregulierung benachrichtigt werden. Im nächsten Schritt könnten betroffene Akteure benachrichtigt und verpflichtende oder empfehlende Maßnahmen eingeleitet werden. Bezüglich der „Staatstrojaner“ sollten von vornherein technische und organisatorische Mechanismen vorgehalten werden, um diese Zugangswege zu schließen, sollten sie bekannt und damit für Dritte nutzbar werden.

315 Diese nationale Stelle ist „eine Person, eine Gruppe von Personen, ein Team aus den maßgeblichen nationalen Managern von Stromversorgungskrisen oder eine Einrichtung, die bzw. das als Ansprechstelle eingesetzt und damit beauftragt wurde, den Informationsfluss während einer Stromversorgungskrise zu koordinieren.“ Verordnung (EU) 2019/941

Bewertung: Die verantwortlichen Akteure, insbesondere die Netzbetreiber, hätten durch die vorgeschlagenen Maßnahmen besseren Zugang zu Informationen und Möglichkeiten, Maßnahmen zur Resilienz aufzusetzen. Nachteilig ist, dass bei sehr großer Transparenz auch Angriffe begünstigt werden könnten. Zudem könnte dies zu Misstrauen bei den Netzbetreibern führen.

Die unabhängige Stelle sollte in den kommenden Jahren etabliert werden. So wird sie Nutzen stiften, sobald sich Störereignisse häufen, die sich in ihrer Charakteristik von den heute für einen Blackout relevanten Störereignissen unterscheiden.

Eine Umsetzung könnte allerdings dadurch erschwert werden, dass es Zielkonflikte aus staatlicher Sicht gibt: das Ziel nach Geheimhaltung von Sicherheitslücken, um sie nicht potenziellen Angreifern offenzulegen, auf der einen Seite und das Ziel nach Transparenz, damit Effekte der Sicherheitslücke im Strombetrieb berücksichtigt werden können, auf der anderen Seite. Erfahrungen zeigen außerdem, dass es häufig an der „Meldemoral“ hapert: Vorfälle werden von den Akteuren oft nicht gemeldet, wenn die Konsequenzen der Vorfälle nach außen hin nicht sichtbar wurden. Je nach Definition der relevanten Störereignisse kann die Komplexität aufgrund der Menge der auszuwertenden Ereignisse sehr groß werden.

Eine behördliche oder behördlich beaufsichtigte Institution aufbauen, die regelmäßig eine Risikobewertung durchführt

Eine Institution zur Risikobewertung möglicherweise bedrohlicher Entwicklungen im elektrischen Energiesystem sollte eine Risikobewertung, wie sie die EU-Verordnung zur „Risikovorsorge im Elektrizitätssektor“[316] vorschlägt, um folgende Punkte erweitern:

- Ausarbeitung von Frühwarnsystemen und -indikatoren: Das könnten etwa Risikoindikatoren zu Marktrisiken, technische Disruptionen, politische Verwerfungen oder Veränderungen der gesellschaftlichen Einstellungen sein.

- Beobachtung langfristiger Entwicklungen und Erarbeitung von Anpassungsstrategien: Aus den Anpassungsstrategien lassen sich insbesondere auch die Handlungsoptionen für die Politik ableiten.

- Einbeziehung von Expertise auch außerhalb der Energieversorgung: Werden Expertinnen und Experten aus den verschiedenen Bereichen, mindestens auch aus der IKT-Domäne, der Risikoforschung und den Gesellschaftswissenschaften eingebunden, verringert dies das Risiko, Bedrohungen zu übersehen, die nicht direkt aus dem Elektrizitätssektor resultieren. Es ist jeweils abzuwägen zwischen der Ergebnisqualität, der Akzeptanz eines solchen Gremiums und dem Aufwand, der betrieben werden soll. Ein Fokus sollte auf systemischen Risiken liegen, die die Funktionsfähigkeit und Stabilität des gesamten elektrischen Energiesystems gefährden. Ebenso müssen Risiken betrachtet werden, die sich aus der Kopplung mit anderen Sektoren wie etwa dem Gassektor[317] ergeben.

316 Vgl. Verordnung (EU) 2019/941.

317 So werden beispielsweise zunehmend Gasverdichter elektrisch betrieben und an Kommunikationsnetze angeschlossen. Dies bedeutet neue Flexibilitäten für das Energiesystem, aber auch erhöhten Sicherungsaufwand für die IKT, da durch Fehler die Gasversorgung ausfallen könnte.

Eine Umsetzungsmöglichkeit wäre die Beauftragung der BNetzA, da diese ohnehin in den durch die EU-Verordnung vorgegebenen Prozess eingebunden ist. Außerdem hat sie langjährige Erfahrung, die Möglichkeit, die Ergebnisse in Verordnungen einfließen zu lassen und Synergien zwischen den Sektoren Energie und Telekommunikation herzustellen. Alternativ ließe sich auch eine nicht behördliche Lösung etablieren. Diese könnte vermutlich einerseits freier agieren, würde andererseits aber weniger Verbindlichkeit erzeugen. Zudem sollte die Entwicklung neuer methodischer Ansätze gefördert werden, die helfen, die Vorhersagemöglichkeiten zu stärken.

Bewertung: Durch eine institutionalisierte Risikobewertung würde eine wesentliche Lücke im Hinblick auf Resilienz geschlossen werden. Zwar besteht kein besonderer Zeitdruck für die Umsetzung, es bietet sich jedoch an, diese Maßnahmen in die EU-Verordnung (EU) 2019/941 einzubinden.

Ein Vorteil ist, dass sowohl viele neue Risikofaktoren als auch überraschende Entwicklungen einbezogen werden. Eine Umsetzung könnte sich allerdings verzögern, solange das Netz zuverlässig und sicher funktioniert – von den Verantwortlichen also noch kein Handlungsbedarf gesehen wird. Außerdem gibt es bisher verhältnismäßig wenig Übung mit solchen Gremien.

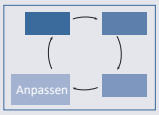
Geeignete Kenngrößen für Resilienz entwickeln und entsprechende Vorgaben schaffen

Es sind geeignete qualitative und quantitative Kenngrößen für Resilienz zu entwickeln. Diese erleichtern die Beurteilung, welche Maßnahmen zur Vermeidung von Blackouts oder zum verbesserten Wiederaufbau geeignet sind. Es bietet sich an, dass das BMWi eine Studie zur Ausarbeitung einer geeigneten Methodik und Metrik sowie zu Lösungsvorschlägen beauftragt. Den Kenngrößen entsprechende Vorgaben und Standards können national (etwa vom VDE) oder europäisch (etwa im Rahmen eines EU-Mandats) erarbeitet werden; die großen Verbände (national etwa VDE) und Standardisierungsgremien (etwa CEN/CENELEC beziehungsweise IEC) sind dafür geeignet. Internationale Standardisierung sorgt in der Regel für Kostenvorteile und mehr Innovationen. Die Zertifizierung oder sonstige Überprüfung der Einhaltung dieser Vorgaben ist möglichst so sicherzustellen, dass Innovationen nicht behindert werden (siehe Handlungsoption 4). Die Verpflichtung zur Einhaltung der nationalen Vorgaben wird sinnvollerweise von der BNetzA in Zusammenarbeit mit dem BSI vorgenommen.

Bewertung: Die Umsetzung sollte in den nächsten Jahren beginnen. Durch klare Standards zur Bewertung wird „Resilience by Design“, also die Berücksichtigung von resilientem Verhalten bereits in der Designphase von Lösungen, ermöglicht. Netzinvestitionen in IKT erhalten eine fundierte Begründung und Berechtigung; ein klares, transparentes Vorgehen wird gefördert.

Es ist schwer abzusehen, wie gut sich Resilienz im hier vorgestellten Sinne in Kenngrößen objektivieren lässt. Die Kosten sind gering, da die Arbeit überwiegend methodisch und konzeptionell ist. Höhere Kosten entstehen erst durch die Umsetzung. Ein genaueres Wissen um den richtigen Mitteleinsatz für Resilienz vermeidet ineffiziente Maßnahmen und damit Kosten.

Handlungsoption 15:
Einen übergeordneten Begleitprozess ins Leben rufen



Ergebnis: Die Resilienzstrategie für die Stromversorgung wird in ihrer Gesamtheit regelmäßig neutral evaluiert.

Dringlichkeit: ● ● ● **Wirksamkeit:** ● ● ●

Was kann man heute tun?

- Einen übergeordneten Begleitprozess gestalten und eine Institution aufbauen, die den Begleitprozess durchführt.

Langfristiger Lösungsbeitrag: Eine unabhängige Institution evaluiert im Auftrag der Politik in einem begleitenden Monitoring, ob die bisherige Resilienzstrategie, die sich in politischen Entscheidungen zu Resilienzmaßnahmen und deren Umsetzung äußert, effektiv, effizient und – nach dem Stand des verfügbaren Wissens – ausreichend sein wird.

Was kann man heute tun: In Abgrenzung zur Risikobewertung, die in Handlungsoption 14 vorgeschlagen wird und die die Erarbeitung konkreter Risikoinstrumente und neuer Resilienzmaßnahmen zum Ziel hat, ist der Fokus der hier vorgeschlagenen Option, die Resilienzstrategie und deren Umsetzung in Gänze regelmäßig auf ihre Wirkungsweise hin neu zu beleuchten. Die wesentliche Aufgabe eines solchen übergeordneten Begleitprozesses ist die periodische Bewertung getroffener politischer Entscheidungen und deren Umsetzung. Insbesondere sollten folgende Fragen beantwortet werden:

- Wurde die beabsichtigte Wirkung erreicht?
- Sind unvorhergesehene negative Effekte zu erwarten oder bereits eingetreten?
- Gibt es Wechselwirkungen zwischen verschiedenen Maßnahmen, die mögliche negative Effekte zur Folge haben?
- Sind die eingesetzten Mittel zur Zielerreichung noch adäquat?
- Ist die ursprünglich intendierte Wirkung auch heute und in Zukunft noch gewünscht?

Nicht zuletzt wäre in diesem Prozess regelmäßig zu prüfen, ob durch die Entscheidungen und Umsetzungsmaßnahmen zur Energiewende Pfadabhängigkeiten erzeugt werden, die einen Einfluss auf die Resilienz haben können, und wie auf diese Pfadabhängigkeiten reagiert werden kann. Dabei stellen sich besondere Herausforderungen, mit denen sich die Ausführenden des Prozesses beschäftigen müssen: Das Ergebnis der Entscheidungen ist ex post nicht messbar: wenn kein großer Blackout stattgefunden hat, sagt das wenig darüber aus, ob durch Entscheidungen die Wahrscheinlichkeit für Blackouts reduziert werden konnte. Daher wird dieser Monitoringprozess nur ausführbar, wenn die Schritte zur Risikobewertung und zur Resilienzmessung der Handlungsoption 14 durchgeführt werden.

Das Zusammentragen der notwendigen Informationen kann durch ein Ministerium (zum Beispiel BMWi) oder eine Behörde (zum Beispiel BNetzA) geschehen, unter Beteiligung anderer relevanter politischer Gremien wie etwa des BMI. Zur Bewertung der Entscheidungen stehen mehrere sich ergänzende Optionen zur Auswahl, beispielsweise:

- Eine eigenständige, unabhängige, wissenschaftliche Durchführung der Bewertung,

um politische Unabhängigkeit zu gewährleisten, etwa analog dem Sachverständigenrat zur Begutachtung der gesamtwirtschaftlichen Entwicklung. Dies erforderte ein eigenes Gesetz.

- Eine wissenschaftliche Bewertung der von der Exekutive erfassten, verdichteten und analysierten Informationen. Einen vergleichbaren Prozess stellt etwa der Monitoringprozess „Energie der Zukunft“ der Bundesregierung dar.

- Eine Mitarbeit der Stakeholder unter Einschluss der Zivilgesellschaft, um Akzeptanz zu schaffen und Zielvorstellungen explizit zu machen. Die direkte Einbindung von Bürgerinnen und Bürgern ist ebenfalls möglich, erhöht den Aufwand aber deutlich. Dies gilt insbesondere, wenn die Teilnehmerinnen und Teilnehmer einen repräsentativen Ausschnitt der Gesellschaft bilden sollen.

- Studien zu Einzelaspekten.

Der Bewertung schließen sich – je nach Ergebnis – verschiedene Handlungsmöglichkeiten an, über die dann in den jeweiligen politischen Entscheidungsgremien entschieden wird:

- Anpassen von Maßnahmen: Maßnahmen sollten generell so gestaltet sein, dass die Möglichkeit besteht, bei Unwirksamkeit frühzeitig nachzujustieren und im Zuge dessen etwa Anreizsysteme zu verbessern oder Regulierungen anzupassen.

- Streichen von Maßnahmen: Wenn Maßnahmen sich als zu unwirksam oder ineffizient erweisen oder gar überwiegend negative Effekte zur Folge haben, sollten sie gestoppt werden können. Ein Beispiel hierfür ist die sogenannte Sunset-Gesetzgebung aus den USA. Diese ermöglicht es, dass Gesetze außer Kraft treten, falls sie nicht explizit verlängert oder neu beschlossen werden.

- Beschluss von neuen Maßnahmen: Wenn die bisherigen Maßnahmen nicht ausreichen, sollte geprüft werden, ob neue, zusätzliche Maßnahmen sinnvoll sind und wie diese zu gestalten wären. Dies kann es unter anderem ermöglichen, technische Neuerungen zu integrieren.

Bewertung: Der hier vorgestellte Vorschlag ermöglicht es, die Wirkung von durch die Politik auf den Weg gebrachten resilienzsichernden Maßnahmen regelmäßig zu überprüfen. Er stellt die notwendigen Informationen bereit, die die Politik benötigt, um Anpassungen an der Umsetzung der Resilienzstrategie vorzunehmen. Daher wird der Vorschlag als effektiv eingeschätzt. Mit der Umsetzung sollte begonnen werden, sobald Maßnahmen, etwa aus dieser Analyse, eingeleitet wurden und erste Ergebnisse zur Bewertung ihres Effekts zur Verfügung stehen. Diese können als Blaupause dienen, anhand deren das Gremium konkret ausgestaltet und der Beratungsprozess entwickelt und erprobt werden kann.

Eine Mitarbeit der wesentlichen Akteure (Energieversorger, Hersteller, Dienstleister beziehungsweise deren Verbände, Bürgerinnen und Bürger) erhöht die Akzeptanz, was die spätere politische Umsetzung erleichtert. Die direkte Einbindung von Bürgerinnen und Bürgern erhöht den Mobilisierungsaufwand deutlich – insbesondere dann, wenn diese repräsentativ vertreten sein sollen. Ersatzweise bieten sich zur Einbindung daher zivilgesellschaftliche Vereine/NGOs an.

7 Fazit

Durch die Energiewende in einer digitalisierten Welt werden in den nächsten zwei Jahrzehnten zwar neue Risiken für die Stromversorgung entstehen – aber auch vielfältige neue Möglichkeiten bereitgestellt, die Energieversorgung sicher zu gestalten. So wird das durch Digitalisierung beeinflusste Verhalten einer großen Anzahl kleiner, aktiv steuerbarer Erzeugungs- und Verbrauchsanlagen zunehmend systembeeinflussend werden. Denn wenn viele kleine Anlagen gleichzeitig an- oder abgeschaltet werden, hat dies einen großen Einfluss. Dieser Effekt kann bewusst zur Stabilisierung in kritischen Situationen genutzt werden, er kann aber auch destabilisierend wirken, wenn er im falschen Moment auftritt. Auch die Risiken durch Softwarefehler und Cyber-Angriffe steigen mit zunehmender Digitalisierung. Dabei sind nicht nur die eigentlichen Energieanlagen relevant, sondern auch Millionen von an das Internet angeschlossenen Haushaltsgeräte von der Heizungsanlage bis zum elektrischen Hausspeicher. Durch die fluktuierende Einspeisung aus Windenergie- und Solaranlagen, die Vielzahl dezentraler Anlagen und die zunehmende Akteursvielfalt wird das Energiesystem komplexer und im Betrieb schwerer vorhersehbar. Dazu trägt auch die steigende gegenseitige Abhängigkeit zwischen Energiesystem und IKT-System bei. Nicht zuletzt erschweren die Ungewissheit über zukünftige technische Entwicklungen, nicht definierte Verantwortlichkeiten und die schwer absehbare Entwicklung gesellschaftlicher Einstellungen ein optimales Systemdesign.

Die Politik muss geeignete Rahmenbedingungen setzen, die diese Risiken gerade auch durch die Nutzung der Möglichkeiten der Digitalisierung beherrschbar machen und Blackouts mit ihren verheerenden Folgen für die Gesellschaft zuverlässig verhindern. Insbesondere für den Umgang mit unvorhergesehenen und unvorhersehbaren Risiken eignet sich das Konzept der Resilienz. Eine Resilienzstrategie umfasst die vier Schritte

1. Risiken und Schwachstellen identifizieren,
2. System robust und vorsorgend gestalten,
3. Ausfälle überbrücken/Funktionen wiederherstellen sowie
4. lernende und adaptive Systeme aufbauen.

Ein wirksames Maßnahmenpaket sollte darauf abzielen, in allen vier Bereichen umfassende Verbesserungen zu erzielen. Dafür schlägt die ESYS-Arbeitsgruppe 15 Handlungsoptionen vor, die in 7 Handlungsfelder aufgeteilt sind.

Handlungsfeld	Handlungsoptionen
Wechselwirkung IKT und Energie verstehen und lenken	
	**1. Abhängigkeiten zwischen Stromversorgung und Kommunikationsnetzen analysieren lassen,** um das Risiko kaskadierender Ausfälle zu minimieren.
	2. Regeln für resiliente Kommunikationsnetze schaffen, durch Vorgaben zu größerer Redundanz und Schwarzfallfestigkeit.
	3. Akteure zu einer integrierten Betriebsführung der IKT-Systeme und elektrischen Netze hinleiten mit dem Ziel der Integration der IKT-Überwachung in die Netzleittechnik und der Erstellung eines integrierten Lagebilds.
Cyber-Sicherheit systemisch entwickeln	
	**4. Cyber-Sicherheitsstandards für alle Blackout-relevanten Akteure einführen,** unter anderem für kleine Netzbetreiber, branchenfremde Akteure und Geräte „hinter dem Zähler“.
	5. Maßnahmen zum Umgang mit Sicherheitslücken definieren, um Vulnerabilitäten aufgrund menschlichen Versagens im Sicherheitsmanagement, aufgrund von Softwarefehlern oder staatlich gewollten Hintertüren zu begegnen.
Technische Resilienz durch Netzbetreiber und Netznutzer stärken	
	**6. Digitalisierung der Stromnetze voranbringen,** durch entsprechende technische Ausstattung auch kleiner Netzbetreiber.
	7. Regelwerk für Resilienz durch dezentrale Strukturen erarbeiten lassen für temporäre lokale Versorgungsmöglichkeiten in Verteilnetzen im Inselbetrieb.
IKT-Integration kleiner Anlagen netzdienlich gestalten	
	**8. Standardisierung zur Vermeidung problematischen simultanen Verhaltens,** zum Beispiel durch Mindeststandards zur „Patchability“ von Erzeugungsanlagen und Geräten.
	9. Systemstabilisierung durch dezentrale Anlagen ausbauen und die dafür erforderliche kommunikationstechnische Anbindung schaffen.
Anreize für Netzbetreiber zur Steigerung der Resilienz stärken	
	**10. Eine Resilienzkomponente in die Anreizregulierung integrieren,** damit Netzbetreiber in Resilienzmaßnahmen investieren.
	11. Resilienzverbessernde Netzentgelte und Anschlussgebühren einführen, um die Standortwahl und die Betriebsweise für Erneuerbare-Energie-Anlagen zu beeinflussen.
Beteiligung von Privatakteuren bei der Gestaltung und Umsetzung von Resilienz sicherstellen	
	**12. Ein Stakeholder-Gremium zur Berücksichtigung der Belange von Privatakteuren entwickeln** und alle relevanten Akteure in die Entscheidungsfindung für neue Regelungen einbeziehen.
	13. Bewusstsein für den Einfluss privater Akteure schaffen, durch Informations- und Bildungskampagnen.
Langfristige Risiko- und Resilienzbewertung institutionalisieren	
	**14. Organisationsrahmen für die Meldung von Störfällen und die Resilienzbewertung schaffen** und geeignete Kenngrößen für Resilienz entwickeln.
	15. Einen übergeordneten Begleitprozess ins Leben rufen, um die Resilienzstrategie regelmäßig zu evaluieren.

Tabelle 3: Übersicht über Handlungsfelder und Handlungsoptionen

Neben den großen Energieversorgern und ÜNB werden zunehmend auch weitere Akteure relevant für die Resilienz gegen Blackouts – etwa kleine Stadtwerke, VNB, Prosumer, Privathaushalte, Gerätehersteller, Plattformbetreiber und Betreiber von öffentlichen Kommunikationsnetzen. Sie alle gilt es im Rahmen der Resilienzstrategie angemessen zu adressieren.

Auch wenn einige der Risiken erst mittel- bis langfristig zum Tragen kommen, ist die Weiterentwicklung der Resilienzstrategie zeitnah erforderlich. Denn viele der vorgestellten Maßnahmen nehmen in der Umsetzung viel Zeit in Anspruch. Auch die langlebigen Investitionen in Stromnetze und -erzeugungsanlagen schaffen Pfadabhängigkeiten und erfordern vorausschauendes und zeitnahes Handeln.

8 Anhang: Szenarien als Beschreibung möglicher Entwicklungen bis 2040

Ein Szenario beschreibt eine nach heutigem Wissen für möglich gehaltene zukünftige Entwicklung – also weder deterministische Prognosen noch Wahrscheinlichkeitsprognosen. Sie dienen als Mittel, um über die Zukunft – oder besser: mögliche „Zukünfte" – zu diskutieren. In der Regel sollen Szenarien helfen, heutige Handlungsmöglichkeiten mit den zukünftig möglichen Entwicklungen in Beziehung zu setzen. Szenarien können somit auch helfen, politische Handlungsalternativen zu bewerten.[318] Dies gilt umso mehr, als die Szenariomethodik Sichtweisen aus vielen Disziplinen und von vielen Akteuren integrieren kann. Ist ein Unsicherheitskontext zu berücksichtigen – etwa weil die Szenarien weit in der Zukunft liegen –, haben sich explorative Verfahren bewährt, bei denen prinzipielle Unsicherheiten bereits in der Methodik berücksichtigt werden.[319] Explorative Verfahren liegen auch dieser Analyse zugrunde. Im üblichen Vorgehen wird nach der Identifikation der Fragestellung, auf denen die Szenarien beruhen liegt, eine Umfeldanalyse durchgeführt. Aus der Umfeldanalyse werden zunächst die relevanten Einflussfaktoren ermittelt, welche die Zukunftsentwicklung maßgeblich prägen (sogenannte Schlüsselfaktoren). Aus diesen wurden dann konsistente Szenarien entwickelt (siehe Abschnitt 8.6 und 8.7)

In dieser Analyse wurden zudem auch einige Grundannahmen getroffen, die für alle Szenarien gleich sind, da sie aus heutiger Sicht als sehr wahrscheinlich angesehen werden können – wie etwa Annahmen zum zukünftigen Strommix oder zur Digitalisierung. Disruptionen wie etwa ein Zerfall der EU mit gleichzeitigem Aufbrechen des gemeinsamen elektrischen Energiesystems, ausgewachsene militärische Konflikte oder Naturereignisse auf deutschem Boden, die die Auswirkungen des Fukushima-Vorfalls 2011 in Japan um Größenordnungen übertreffen, werden in dieser Analyse nicht betrachtet, da diese Disruptionen die Spielregeln und Rahmenbedingungen so grundsätzlich ändern würden, dass die Fragestellungen dieser Analyse dann in den Hintergrund rücken würden.

Es wurden vier Szenarien für das Jahr 2040 erarbeitet und als sogenannte **Narrative aus Sicht des Jahres 2040** beschrieben. Zur Charakterisierung der szenariotypischen Bedrohungssituation wurde jedes Szenario um zwei szenariotypische Blackout-Narrative ergänzt – also eine Entwicklung, in der szenariotypische Risiken zusammen mit einem Störereignis zu einem Blackout führen. Durch diese Beispiele der Entstehung eines zukünftigen Blackouts wird konkret gezeigt, wie sich Digitalisierung auf die Bedrohungssituation im zukünftigen elektrischen Energiesystem auswirken könnte – sowohl als mitursächlich für einen Blackout als auch als Mittel, den Blackout

318 Vgl. Dieckhoff et al. 2014, S. 4.
319 Weimer-Jehle/Kosow 2011.

zu vermeiden oder die Auswirkungen zu begrenzen. Die Analyse der Narrative hilft also, eine Vorstellung davon zu gewinnen, wie Digitalisierung sowohl sicher (also möglichst nicht mitursächlich) als auch sichernd, nämlich gezielt zur Erhöhung der Resilienz, eingesetzt werden sollte.

8.1 Szenarioübergreifende Grundannahmen für 2040

Sowohl der nationale als auch der **europäische Strommix** haben sich durch die weiterhin fallenden Energiepreise für die Energiegestehungskosten, flankiert durch staatliche Maßnahmen, deutlich geändert. Die nationale Stromerzeugung beruht inzwischen zu über drei Vierteln auf **erneuerbaren Energien**, davon mehr als achtzig Prozent Windenergie- und PV-Anlagen.[320] Um diese Durchdringung zu erreichen, mussten sowohl dezentrale Optionen (Wind in der Mittelspannung, PV in der Nieder- und Mittelspannung) als auch zentrale Optionen genutzt werden (große Anlagenparks in der Höchst- und Hochspannung). Auch europaweit wurde der Ausbau der erneuerbaren Energien in den meisten Ländern ähnlich stark vorangetrieben. Reservekapazitäten für Dunkelflauten sind in ausreichendem Maße vorhanden. Für das europäische Energieversorgungssystem sind dazu mehrere Optionen denkbar; insbesondere werden im Szenariohorizont einige Atomkraftwerke voraussichtlich noch ans Netz angeschlossen sein.[321]

Der **Stromverbrauch** hat sich durch die Sektorenkopplung annähernd verdoppelt,[322] da der Energiebedarf in anderen Sektoren wie Mobilität/Verkehr und Wärmeverbrauch nun auch zu einem großen Teil aus elektrischer Energie gedeckt wird. Die dazu notwendige Menge an elektrischer Energie übersteigt den Minderbedarf durch Effizienzgewinne. Aufgrund der hohen Durchdringung mit PV und Elektrofahrzeugen sind kleine Hausspeicher wirtschaftlich, etwa um den Eigenverbrauch des im Haus erzeugten Stroms aus PV zu erhöhen oder Elektrofahrzeuge zu Hause ohne Netzrestriktionen schnell laden zu können. Dies gilt umso mehr, als sich die Kosten im Vergleich zum Jahr 2020 deutlich verringert haben. Deutschlandweit liegt die installierte Leistung kleiner in Haushalten installierter Speicher in einer Größenordnung von fünfzig Gigawatt,[323] europaweit um ein Vielfaches höher.

Weitgehend alle Energieanlagen sind technisch in der Lage, ihre Erzeugung beziehungsweise ihren Verbrauch **flexibel anzupassen**. Dies trifft auf Erzeugungsanlagen wie Kraft-Wärme-Kopplung und Wind- und PV-Anlagen zu, die abgeregelt werden, aber auch bei der Spannungshaltung unterstützen können. Auch Verbrauchsanlagen wie Wärmepumpen und Speicheranlagen können durch Lastverschiebung Flexibilität bereitstellen. Industrieprozesse nehmen, soweit sie ihren Bedarf an elektrischer Energie über das Stromnetz decken, in hohem Maße am Lastmanagement teil – entweder durch direkte Teilnahme am Strommarkt oder über entsprechende Tarife der Versorger.

Der **Handel von Energie** wird kleinteiliger: Es können an den Börsen kleinere Energiemengen in kleineren Zeiteinheiten gehandelt werden. Auch die Zeitspanne

320 In den meisten Studien sind nur Daten für 2030 und 2050 direkt angegeben. Deshalb werden hier Zwischenwerte angenommen. Vgl. acatech/Leopoldina/Akademienunion 2020-1 und WWF 2018.

321 ESYS 2019.

322 Abschätzungen für 2050 werden hier zugrunde gelegt, vgl. Ausfelder et al. 2017.

323 Szenarien rechnen beispielsweise mit einer installierten Leistung von 50 bis 100 Gigawatt an PV-Batteriespeicher-Haussystemen im Jahr 2050 (WWF 2018).

vom Abschluss des Handels über ein Produkt und gegebenenfalls Meldung an den/die Netzbetreiber bis zur physikalischen Lieferung ist deutlich geringer als heute. Hingegen vergrößert sich der Austausch geografisch: Der grenzübergreifende Handel hat über ganz Europa deutlich zugenommen.

Die **Verteilnetze** wurden überwiegend nach heutigen Regeln (Netzgrenzwerte, Einspeisekappung[324] etc.) entsprechend dem lokalen Zuwachs an dezentraler Erzeugung und neuen Verbrauchern wie Elektrofahrzeugen ausgebaut[325] sowie um eine Engpassbewirtschaftung erweitert. Die Netze wurden insbesondere so ausgelegt, dass sie mehr als heute Rückspeisung aufnehmen und aktives Verbrauchsverhalten ermöglichen können. **Netzanschlussregeln** wurden so angepasst, dass das technische Potenzial der flexiblen Anlagen verfügbar ist. **Europäische Entwicklungen** sind weitgehend an diese Entwicklungen angepasst verlaufen, das heißt, dass die für das europäische elektrische Energieversorgungssystem relevanten Länder ähnliche Entwicklungen hinsichtlich EE-Ausbau und Digitalisierung durchlaufen haben.

Die **Digitalisierung** wurde weiterhin vorangetrieben. Die **IKT-Durchdringung und Vernetzung** betrifft alle Bereiche der Energieversorgung. Smart Meter sind flächendeckend ausgerollt. Fast alle Erzeuger und viele Betriebsmittel der elektrischen Netze (Transformatoren, Schalter, Sensoren etc.) sind bis in die Niederspannung kommunikativ angebunden. Mobile Kommunikation ist zuverlässig und breitbandig überall zu garantierter Mindestqualität verfügbar. Das **Internet der Dinge** ist Standard: Mehr oder weniger alle Geräte sind mit dem Internet verbunden (Beleuchtung, Kühlschränke, Fernseher, Zahnbürsten, Heizungen, Rollläden usw.). Für Geräte mit hohen Sicherheitsanforderungen gibt es angemessen geschützte Kommunikationsanbindungen (etwa medizinische Versorgung). Die Umsetzung der **IT-Sicherheit** mit den Schutzzielen Datenvertraulichkeit, Integrität und Verfügbarkeit ist weit vorangeschritten, da dies gesellschaftlich gefordert wird. Dennoch gelingt es aufgrund der hohen Komplexität der IKT-Systeme und der eigenen Dynamik der IKT-Branche nicht, alle Sicherheitslücken zu schließen. **Künstliche Intelligenz** spielt in vielen Bereichen eine große Rolle, oft als lernende Systeme. Neben technischer Unterstützung (autonome Fahrzeuge, Netzsteuerung, vollautomatisiere Industrieprozesse) prägt KI auch das soziale Umfeld in vielen Bereichen mehr als heute, wie bei der Partnerwahl, bei Kaufentscheidungen oder bei Medienberichten, die vollständig automatisiert und personalisiert erstellt werden. Einerseits prägen sowohl in der Hardware- als auch in der Softwareherstellung **Monopole** und Oligopole die Digitalisierung; andererseits haben sich insbesondere im Software- und Dienstleistungsbereich verschiedene spezialisierte Unternehmen erfolgreich etabliert. Dieser Erfolg wird – ähnlich wie heute – unter anderem dadurch technologisch ermöglicht, dass viele Komponenten keine größeren Investitionen mehr benötigen, sondern über Plattformen bezogen werden können.

Es existiert ein globales, umfangreiches Wertschöpfungsnetzwerk aus staatlichen, illegalen oder legalen privaten Akteuren, die – oft in einem **Graubereich des IKT-Markts** – an der Produkterstellung und Dienstleistungen oder deren Finanzierung beteiligt sind, mit dem einzigen Ziel, in die IKT-Systeme von Unternehmen, Behörden und Privatpersonen einzudringen – sie zu **hacken** –, ohne dass diese einen

324 Das heißt, die Netze wurden auf einen bestimmten Prozentsatz der Spitzeneinspeisung aus EE ausgebaut.

325 Dies bedeutet nicht, dass alle Elektrofahrzeuge in einem Niederspannungsstrang gleichzeitig per Schnellladung geladen werden können.

solchen Eingriff autorisiert haben. Die Gründe reichen von Kriminalitätsbekämpfung („Staatstrojaner“) bis hin zur politisch motivierten Sabotage wie in der Ukraine 2015. Da es, um diese Optionen sinnvoll nutzen zu können, jahrelanger Vorbereitungen bedarf, sind bereits viele IKT-Systeme von diesen Akteuren prophylaktisch mit hochspezialisierter Schadsoftware infiltriert, oder es werden bewusst Hintertüren beziehungsweise Backdoors in einem IKT-System belassen oder angeordnet, das heißt Sicherheitslücken, die einen Zugriff auf dieses System auch ohne die normalen Zugriffsrechte ermöglichen.

Die **Auswirkungen des Klimawandels** sind deutlich zu spüren und beeinflussen die Stromversorgung: Durch häufigere und heftigere Stürme oder Starkregen werden Leitungen häufiger beschädigt, Hitze verringert die Übertragungskapazität elektrischer Komponenten,[326] Hitzewellen und Dürren führen zur Abschaltung von Atomkraftwerken[327] und fehlendem Wasser in Wasserkraftwerken, Überschwemmungen schädigen das elektrische Energiesystem. Das Wetter wird chaotischer und daher schwerer zu prognostizieren.[328]

8.2 Szenario 1 – „Business as usual“

Die heutigen Entwicklungen wurden moderat fortgeschrieben. Die heutigen wesentlichen Akteure bleiben in Aufgaben und Strukturen weitgehend unverändert.

Der **Netzbetrieb** unterscheidet sich im Wesentlichen kaum vom heutigen: Große ÜNB sind für den sicheren Betrieb in der gesamten von ihnen verantworteten Regelzone verantwortlich. Die Netzbetreiber vertrauen mit den heutigen Mechanismen auf die vier Systemdienstleistungen. Diese wurden jedoch um einige neue Möglichkeiten und Maßnahmen erweitert, etwa durch Beiträge der verteilten EE-Anlagen zur Frequenzhaltung und zur Systemwiederherstellung aus den Verteilnetzen. Der Netzbetrieb ist zwar für Übertragungsnetze stark automatisiert; ein weitgehend autonomer Betrieb in Problemsituationen ist aber kaum möglich. Hochautomatisierte Prozesse zum Wiederanfahren des Systems nach einem Stromausfall existieren nur in geringem Umfang. Die vielen Kleinerzeuger werden in der Regel auch von kleinen Akteuren betrieben, die jedoch Softwaresysteme von wenigen, großen Herstellern verwenden und jene oft nicht selbst betreiben.

Auch die kleinteilige Struktur deutscher Stadtwerke und VNB hat sich kaum verändert. Aufgrund der komplexeren Betriebsführung und einer erhöhten Digitalisierung und Automatisierung des Netzbetriebs ist dieser jedoch an wenige Unternehmen ausgelagert, die zum Teil im gemeinsamen Besitz der beteiligten Stadtwerke liegen und zum Teil Dritten gehören. Dies ist ein Unterschied zu den meisten anderen europäischen Ländern, in denen weit weniger und daher größere VNB die Verantwortung für die Netze haben.

326 So musste im Herbst 2019 in Kalifornien für fast eine Million Kunden der Strom abgestellt werden, weil aufgrund des außergewöhnlich trockenen und windigen Wetters die Gefahr von Leitungsschäden zu groß wurde. Gorman 2019.

327 Spiegel 2019.

328 Siehe etwa Mann et al. 2018.

Auch die **Energiemärkte** haben ähnliche Strukturen wie heute, wenn auch der Handel schneller und kleinteiliger ist. Es gibt kaum ganz neue Marktformen, jedoch gibt es auch im Verteilnetz ein preisbasiertes Engpassmanagement. Speicher spielen für die Netzstabilisierung kaum eine Rolle. Die existierenden **IKT-Schnittstellen** der Anlagen sind zumeist stark herstellergebunden und deshalb uneinheitlich. Dadurch gibt es kaum Anbieter, die effiziente Lösungen für alle Schnittstellen bedienen können. Daher unterbleiben bei Kleinanlagen eine weitgehend flexible Bewirtschaftung für Netzdienstleistungen sowie eine effiziente Vermarktung. Jedoch können auch kleine Aggregatoren mit KI-gestützten Standardprodukten eine gut prognostizierbare Einspeisung aus Wind und PV an den Markt bringen.

Die Gesellschaftsstruktur ist eher individualistisch geprägt. Zugleich wird der Staat als Fürsorgeinstanz für die Bürgerinnen und Bürger wahrgenommen. Die Menschen sind zurückhaltend bei der Weitergabe privater Verbrauchs- und Haushaltsdaten. Der Gesetzgeber unterstützt diese Haltung durch strengen **Datenschutz**. Dieser schränkt die datenbasierten Geschäftsmodelle stark ein, soweit sie auf intransparentem Umgang mit Kundendaten basieren. Der Umgang mit Cyber-Störungen, das heißt Ereignissen, die im IKT-System entstehen (zum Beispiel Programmierfehler oder Hackerangriffe) und Störungen im Betrieb des Stromnetzes auslösen, ist überwiegend national geregelt. Es gibt wenig europaweiten Austausch über Sicherheitsvorfälle, Fehler und Angriffe und auch keine entsprechenden europäischen Institutionen, die im Krisenfall unterstützen können.

Blackout-Narrative
Digitaler Ursprung
Es gibt staatliche Werkzeuge für Cyber-Spionage und Angriffe und viele Hintertüren in Software wurden wissentlich nicht geschlossen. Aufgrund dessen konnte der Geheimdienst eines anderen Landes vor einiger Zeit in SCADA-Systeme eines marktführenden Herstellers eindringen, die von mehreren großen VNB verwendet werden. Mit einer Schadsoftware wurde so der Zugang aus dem Internet auf das SCADA-System ermöglicht. Ein gezieltes Abschalten an Knotenpunkten und begleitende Attacken auf Betriebsmittel im Stromnetz lassen mehrere Millionen Menschen in mehreren Ländern ohne Strom.[329] Die Fehlerbehebung ist langwierig, da die Energieversorger nicht auf das Ereignis vorbereitet waren. Zudem stehen keine Expertinnen und Experten für das System zeitnah zur Verfügung, und Informationen über die eingesetzten Angriffswerkzeuge sind schwer beschaffbar. Die Batterien der elektrisch betriebenen Wartungsfahrzeuge sowie die Batterien einiger Kommunikationseinrichtungen der Netzbetreiber sind vorab gezielt entleert oder Ladevorgänge gestoppt worden, sodass sie für den Wiederaufbau nicht genutzt werden können. Während der Fehlerbehebungsphase werden zudem weitere Angriffe aus ebenfalls vorher angegriffenen IKT-Systemen gefahren, die geplante Wiederanfahrmaßnahmen erschweren, wie zum Beispiel die Software von Ladesäulen, die das Laden von Elektrofahrzeugen mit zusammen einigen Gigawatt auslöst. Die Gesellschaft ist verunsichert, da es keine vertrauensvolle Lösungsinstanz gibt und die Koordinationsstruktur – auch zwischen den Bürgerinnen und Bürgern – schwach ist. Der Angriff wurde genau geplant und auf die Gegebenheiten in den betroffenen Regionen angepasst. Dies konnte unter anderem dadurch gelingen, dass der Angriff in mehreren Netzen in anderen Ländern vorher geprobt wurde. Allerdings wurden die technischen Details der Angriffe und mögliche Schutzmaßnahmen nicht an andere Staaten weitergegeben.
Nicht-digitaler Ursprung[330]
Eine heftige Sturmfront zieht während einer Starklastlage über das Land. Ein Strommast bricht und kappt eine wichtige Übertragungsleitung. Eine weitere Leitung wird durch einen Blitzeinschlag zerstört. Durch den starken Sturm schalten viele Windräder aus Sicherheitsgründen automatisch ab. Ein Gleichgewicht zwischen Erzeugung und Verbrauch kann nicht mehr hergestellt werden, und das europäische Verbundnetz zerfällt in die einzelnen Regelzonen. Die Reservekraftwerke in den betroffenen Regelzonen können nicht schnell genug angefahren werden, da der plötzliche Ausfall der Windkraft nicht prognostiziert wurde. Hilfe zum Wiederaufbau durch die europäischen Verbundpartner ist nicht möglich. Der Wiederaufbau aus den Verteilnetzen ist ebenfalls nicht möglich, da die entsprechende Aktorik und die Funktionen in den Steuersystemen fehlen. Außerdem stehen keine Speicher zur Verfügung, um beim Netzwiederaufbau zu unterstützen. Kaskadierende Fehler verschlimmern das Problem.

Tabelle 4: Blackout-Narrative in Szenario 1 – „Business as usual“

329 Vgl. dazu den Stromausfall in der Ukraine am 23. Dezember 2015, der durch einen koordinierten Angriff unbekannter Hacker ausgelöst wurde, die über manipulierte Standardsoftware Malware in das System eines regionalen Energieversorgers einschleusen konnten und somit Zugriff auf das System hatten.

330 Ursachen, die nicht direkt aus der Digitalisierung des Energiesystems kommen.

8.3 Szenario 2 – „Automatisiert und modular“

Die Energieversorgung bewegte sich schnell von der heutigen weg. Kleine, voll automatisierte Strukturen prägen das System.

Der **Netzbetrieb** wurde durchgehend automatisiert. Auf viele Ereignisse und Störereignisse reagiert das Netz autonom, oft mit Unterstützung durch KI. Im Fall von Stromausfällen können sich viele Netzabschnitte durch Inselbetrieb autark versorgen. Im Fall unerwarteter und komplexer Störungen gibt es gut ausgebildetes Personal, das auf diese Störungen adäquat reagieren kann. Der Betrieb der erneuerbaren Energien liegt überwiegend in der Hand kleinerer Unternehmen, Privatpersonen und Genossenschaften. Dies wird durch Produkte unterstützt, die einen Normalbetrieb ohne große Expertenkenntnis ermöglichen. **Offene IT-Standards** haben sich durchgesetzt, sodass Systeme verschiedener Hersteller gut zusammenarbeiten können – eine Notwendigkeit für eine komplette Automatisierung des Betriebs. Der Ausbau von Speichern sorgt für einen hohen Grad an Flexibilität für die Systemstützung. Die Besitzer von Anlagen wie Wärmepumpen, Speicher oder KWK-Anlagen stellen diese zu geringen Kosten dem Netzbetreiber zur Verfügung, sodass die Flexibilität der Anlagen netzdienlich genutzt werden kann.

Intelligente Geräte werden auf Kundenseite nicht nur stark genutzt, sondern es besteht auch eine große Bereitschaft, die eigenen Verbrauchs- und Erzeugungsdaten zeitlich aufgelöst an Dritte weiterzugeben. Dies gilt für Privathaushalte und eingeschränkt auch für Unternehmen. Der von der Politik regulierte Datenschutz trägt dem Rechnung und ermöglicht entsprechende Freiräume bei der Verwendung der Daten. Außerdem werden Verbraucher oft selbst aktiv und organisieren sich in unabhängigen energetischen Nachbarschaften zum lokalen Austausch von Energie. Die Gesellschaft hat Vertrauen in die Politik und in die Versorger, ist stärker vernetzt und von Kollektivdenken geprägt.

Darüber hinaus haben sich **Märkte zur Beschaffung von Netzdienstleistungen** in vielen Bereichen durchgesetzt, sodass insbesondere auch Netzkapazitäten an den Märkten berücksichtigt werden. Die **europäischen Staaten sind gut organisiert** und haben gemeinsam Pläne ausgearbeitet, wie im Fall von Cyber-Störungen zu reagieren und zu handeln ist. Die Bundesregierung ist darauf bedacht, ähnlich wie die anderen europäischen Staaten, dass alle Geräte und Computer **Backdoors** haben: Sie haben eine ganze Bandbreite an Möglichkeiten, Schadsoftware auf Rechner zu spielen, um Informationen über Aktivitäten verdächtiger Personen oder Organisationen erlangen zu können.

Blackout-Narrative
Digitaler Ursprung
Deutschland besitzt zwar eine hochsichere Smart-Meter-Infrastruktur, da Sicherheitsvorschriften und Interoperabilitätsstandards durch eine spezialisierte Behörde erarbeitet wurden. Prinzipiell wären über die Smart Meter „smarte“ Dienstleistungen möglich. Allerdings führten langwierige Zertifizierungs- und Genehmigungsverfahren dazu, dass die für die Energiewende notwendigen Innovationen ausgebremst wurden. Innovative, digital basierte Geschäftsmodelle wurden deshalb so entwickelt, dass notwendige technische Prozesse über das offene Internet gesteuert werden. Einige dieser innovativen Dienstleister waren so erfolgreich, dass sie mehrere Hundert Megawatt steuern können – zum Teil aus dem Ausland außerhalb der deutschen Gesetzgebung. Einem mit großen finanziellen und technischen Ressourcen ausgestatteten Hackerkollektiv ist es in kurzer Zeit gelungen, in wenige dieser Unternehmen einzudringen und so in mehrere Millionen kleine Energieanlagen weniger Hersteller spezialisierte Schadsoftware einzuschleusen. Sie haben dazu Vulnerabilitäten in den Systemen genutzt, die aufgrund staatlicher Vorgaben eingerichtet oder nicht behoben waren. Parallel haben sie Informationen aus einem Rechenzentrum abgezapft, in welchem verschiedene Cloud-Dienste laufen, aus denen sich Informationen über das elektrische Energiesystem gewinnen lassen. Diese wurden von Expertinnen und Experten des Kollektivs mittels künstlicher Intelligenz ausgewertet, um einen maximal wirksamen Angriffsplan zu ermitteln, der Netzkonfiguration, Wetter, Verbrauch, Markt und weitere Parameter berücksichtigt. Zu einem geeigneten Zeitpunkt werden die Geräte unter Kontrolle der Angreifer so koordiniert, dass die Frequenzschwankungen zu einem Blackout führen. Der Wiederaufbau durch die Netzbetreiber wird immer wieder durch koordinierte Aktionen gestört. Dazu werden zum Beispiel weitere Vulnerabilitäten in bestehenden Systemen genutzt, etwa fehlende Sicherheitsupdates oder veraltete Betriebssysteme.
Nicht-digitaler Ursprung
In ganz Europa herrscht eine Hitzewelle, die über mehrere Wochen andauert. Durch die lange Belastung bei sehr hohen Temperaturen überlasten Übertragungsleitungen und Transformatoren immer wieder in kürzester Zeit. Aufgrund der Dauerbelastung kommt es schließlich zum Ausfall von zwei Übertragungsleitungen. Das Netz zerfällt in kleine Inseln: Netzgebiete, die in der Lage sind, sich vorübergehend selbst zu versorgen, koppeln (teilweise autonom) ab, um lokale Versorgungsqualität zu gewährleisten. In diesen Inselnetzen kann dadurch eine ausreichende Basisversorgung aufrechterhalten werden. Die Zusammenarbeit von ÜNB und VNB für diesen spezifischen Fall ist ungeklärt. Die Inselnetze verweigern eine Mithilfe am Wiederaufbau, da diese das Serviceniveau in ihrem Netzgebiet weiter beeinträchtigen würde. Der Schwarzstart, das heißt das Wiederanfahren des Systems nach einem Blackout, in den betroffenen Gebieten gestaltet sich äußerst schwierig, da die geltenden Routinen diesen Fall nicht vorsehen.

Tabelle 5: Blackout-Narrative in Szenario 2 – „Automatisiert und modular“

8.4 Szenario 3 – „Integriertes Europa“

Die Staaten der EU arbeiten industriepolitisch und energiepolitisch intensiv zusammen. Energieregulierungen – insbesondere für Verteilnetze – werden gemeinsam vorangetrieben und homogenisiert.

Die Struktur der **Netzbetreiber** ist ähnlich wie heutzutage. Der Automatisierungsgrad ist zwar deutlich höher als heute, jedoch werden autonome Elemente und Funktionen nur in wenigen Bereichen verwendet. Die Netzführung wird ebenfalls nur an wenigen Stellen von KI-gestützten, autonomen Systemen unterstützt, sodass die Beherrschung komplexer Situationen durch das menschliche Leistungsvermögen begrenzt wird. Dieser Mangel wirkt jedoch in der Regel nicht so schwer, da in hohem Maße **gut ausgebildetes Fachpersonal**, insbesondere Ingenieurinnen und Ingenieure, zur Verfügung stehen. Sie besitzen das technische Können, um auch ausgefallene Stresssituationen des Netzes einschätzen zu können. Dies wurde europaweit durch Bildungsinitiativen und Förderung von Zuwanderung erreicht. Verschiedene europaweit koordinierte Maßnahmen der Forschungs- und Industriepolitik haben dazu geführt, dass **kostengünstig (chemische) Speichersysteme** wie Batterien und Power-to-Gas-Anlagen zur Umwandlung von Strom in gasförmige Energieträger produziert werden. Diese Speichersysteme und -infrastrukturen werden umfangreich in der Stromversorgung eingesetzt. So konnte der größte Teil der Wertschöpfung in Europa belassen werden.

Das **Marktdesign** wurde so angepasst, dass Netzkapazitäten möglichst gut berücksichtigt werden können. Steuereingriffe durch Netzbetreiber auf fremde Anlagen (zum Beispiel KWK-Anlagen und Speicher) sind daher gängige Praxis im Normalbetrieb. Der Betrieb der dezentralen Anlagen wurde von wenigen großen internationalen Unternehmen übernommen, sodass sich in Europa ein **Oligopol** gebildet hat. Die Umsetzung **offener IKT-Standards** wurde vorangetrieben, sodass Energieanlagen verschiedener Hersteller gut in übergeordnete Systeme eingebunden werden können. Intelligente Geräte werden auf Kundenseite nicht nur stark genutzt, sondern es besteht auch eine große Bereitschaft, **Daten an Dritte weiterzugeben**. Der Wille, alle **Sicherheitslücken zu schließen**, ist groß und wird gefördert. Die Kriminalitätsbekämpfung wird dadurch kaum behindert, da dafür andere IT-gestützte Methoden entwickelt wurden.

Es gibt eine **europäische Organisation** der EU-Mitgliedstaaten, deren Vertreter sich in Fragen der Energieversorgung enger als heute abstimmen. Der europäische Regulierungsrahmen vereinheitlicht nationale Regulierungen. Insgesamt hat die Gesellschaft großes Vertrauen in die Behörden, die die Verantwortung für die Sicherheit der Energieversorgung tragen.

Blackout-Narrative
Digitaler Ursprung
Durch das vorherrschende Oligopol weniger Aggregatoren bietet ein Angriff auf eines dieser Großunternehmen bereits die Möglichkeit, die Versorgung eines großen Teils von Endkunden zu beeinflussen. Einer Gruppe von Hackern ist es gelungen, Schadsoftware in das IT-System eines marktführenden Aggregators einzuschleusen. Über Wochen können so mehr und mehr IKT-Systeme des Aggregators infiltriert werden. So können Vulnerabilitäten im Betrieb des Aggregators ausgespäht werden. Dadurch dass Prognosen des Betriebszustands aus dem IT-System in dem SCADA-System für die Optimierung des Betriebs verwendet werden, können fehlerhafte Daten eingespielt werden. Auf diese Weise gelingt es, die Aktivierung von Flexibilitäten zur Erbringung von Systemdienstleistung zu manipulieren. Bei einer Netzüberlastung in Europa stehen somit keine Kapazitäten für den Abruf von Regelleistung oder anderer Flexibilität zur Verfügung, und es kommt zum Blackout. Batteriespeicher sind Teil der virtuellen Kraftwerke des angegriffenen Unternehmens und können nicht für den Wiederaufbau genutzt werden.
Nicht-digitaler Ursprung
Eine Pandemie mit hoher Prävalenz führt dazu, dass die Gesellschaft große Unsicherheit ergreift. Menschen bringen sich in Sicherheit beziehungsweise bleiben bei ihren Familien, um sie in der Situation zu unterstützen, statt zur Arbeit zu gehen. Auch das bereits durch die Pandemie sehr knappe Personal in den Leitwarten und den IT-Abteilungen verlässt zum Teil den Arbeitsplatz. Die Stromversorgung gerät aufgrund fehlender Automatisierung, IT-Fehlern und mangelnden Personals in einen kritischen Zustand, der nicht mehr beherrschbar ist, da die Eingriffe in das Netzgeschehen durch das Betriebspersonal nicht mehr ausreichen. Es kommt zu einem Blackout. Die europäische Unterstützung beim Wiederaufbau greift nur schleppend, da Maßnahmen unterschiedlich schnell und intensiv umgesetzt wurden. In der Gesellschaft kommt es zu Unruhen, und das Vertrauen in die Verantwortlichen wird nachhaltig gestört.

Tabelle 6: Blackout-Narrative in Szenario 3 – „Integriertes Europa“

8.5 Szenario 4 – „Laissez-faire“

Sehr viel mehr als heute wird auf den freien Markt gesetzt.

Die Struktur der **Netzbetreiber** hat sich im Vergleich zu heute kaum verändert. Es herrscht ein hoher Autonomiegrad in den Netzen vor: Viele der heute manuell auszuführenden Funktionen werden automatisch ausgelöst – auch in kritischen Situationen. Die dezentralen Anlagen sind jedoch nur eingeschränkt für den Netzbetreiber direkt ansteuerbar, da die Hersteller der Anlagen **keine gemeinsam standardisierten Schnittstellen** verwenden.

Marktdesign sowie Produkte und Dienstleistungen haben sich so entwickelt, dass diese flexibel sind und Netzkapazitäten möglichst gut berücksichtigt werden können. Es gibt im Verteilnetz eine intensive Flexibilitätsbewirtschaftung. Zudem gibt es viele neue, auch branchenfremde Anbieter, Produkte und Dienstleistungen im Energieumfeld. Die Vermarktung von EE-Strom dominieren wenige große internationale Unternehmen, sodass sich in Europa ein **Oligopol** gebildet hat. Die meisten technischen Prozesse der Energieversorgung laufen automatisch und ohne menschliche Eingriffe ab. Da der **freie Markt** Innovationen befeuerte, werden modernste IKT-Technologien eingesetzt, etwa KI einer ganz neuen Generation.

Die demografische Entwicklung, mangelndes Technikinteresse verbunden mit einer fehlenden gesellschaftlich getragenen Internationalisierungsstrategie, um Studierende und Fachkräfte aus dem Ausland anzuwerben, haben zu einem gravierenden **Mangel an Ingenieurinnen und Ingenieuren** in Deutschland geführt. Daher wurden viele der Technologien im Ausland entwickelt. Das Fachpersonal ist nur bedingt in der Lage, in unbekannten Situationen die richtigen Entscheidungen zu treffen. Beim Auftreten von Störungen, Fehlern oder dem Wunsch nach geänderten Einstellungen muss eine Spezialistin beziehungsweise ein Spezialist aus dem Herstellerland hinzugezogen werden. Der Technologiefortschritt bei **Power-To-Gas-Speichern** setzt erst spät ein, da es lange keine Geschäftsmodelle gab. **Batteriespeicher** sind weitgehend auf Anwendungen beschränkt, bei denen sich die sehr hohen Kosten amortisieren, wie zum Beispiel Eigenverbrauchsoptimierung, Elektrofahrzeuge und Netzanwendungen.

Die Menschen sind zurückhaltend bei der Weitergabe ihrer Verbrauchs- und Haushaltsdaten. Der Gesetzgeber unterstützt diese Haltung durch **strengen Datenschutz**. Intelligente Geräte geben nur wenige Daten an Dritte weiter. Die europäische Zusammenarbeit im Hinblick auf gemeinsame Strukturen zur Lösung von Cyber Security ist gering. Der Staat nutzt intensiv **Angriffswerkzeuge und Backdoors** für Cyber-Angriffe, um Kriminalität zu bekämpfen. Auch das Militär entwickelt sein Potenzial zu Cyber-Angriffen stetig fort. Gesellschaftlicher Individualismus, geringes Politikvertrauen und starke Ökonomisierung der Lebensbereiche prägen die Gesellschaft. Gesellschaftliche Bereiche greifen nicht optimal ineinander. So könnte einerseits die Förderung von Immigration helfen, dem allgemein empfundenen Mangel an Ingenieurinnen und Ingenieuren abzuhelfen. Andererseits steht eine gesellschaftliche Skepsis gegenüber Immigration dem entgegen.

Blackout-Narrative
Digitaler Ursprung
Der Kraftwerkseinsatz wird hauptsächlich durch den Markt vorgegeben. Dies führt dazu, dass das Netz zeitweise an seinen Grenzen betrieben wird. Die Netzsteuerung wird hauptsächlich durch künstliche Intelligenz ausgeführt. Diese schätzt die Situation jedoch falsch ein und geht davon aus, dass die Situation beherrschbar ist. Dies wäre an sich kein Problem, doch muss sich das Betriebspersonal zu sehr auf die KI-Systeme verlassen. Es kommt zu ersten Teilausfällen, weiteren Fehlentscheidungen und schließlich zum Blackout. Der Wiederaufbau ist schwierig, da das System durch die hohe Komplexität schwer überschaubar ist und es an Fachkräften mangelt. Da die Situation für die KI unbekannt ist, muss das System manuell wiederaufgebaut werden, was wegen der Kleinteiligkeit des Systems und mangelnder Expertise schwierig und zeitaufwendig ist. Außerdem stehen kaum Daten von Anlagen zur Verfügung, die für den Wiederaufbau genutzt werden können, sodass verschiedene Einstellungen getestet werden müssen. Ein gezieltes Anfahren ist nicht möglich.
Nicht-digitaler Ursprung
Über soziale Netzwerke wird spontan ein europaweiter Flashmob organisiert. Ähnlich der Earth-Hour, einer jährlich wiederkehrenden Klima- und Umweltschutzaktion, bei der viele Menschen, Städte und Unternehmen freiwillig für eine bestimmte Stunde das Licht ausschalten, reduzieren viele Menschen gleichzeitig ihren Stromverbrauch drastisch. Den Menschen fehlt jedoch das Bewusstsein dafür, dass dies schwerwiegendes simultanes Verhalten hervorruft. Dieses wird vom digitalisierten Real-time-Handel verschlimmert und führen zu chaotischen Effekten.[331] Die Netzbetreiber sind auf diese Ereigniskette nicht vorbereitet und haben keine Vorkehrungen getroffen. Die Erzeugungsanlagen können nicht schnell genug reagieren, und es kommt zum Blackout. Der Wiederaufbau ist schwierig und langwierig, da es an Fachkräften mangelt und Daten aus dem System und den Anlagen nur in geringem Maße zur Verfügung stehen.

Tabelle 7: Blackout-Narrative in Szenario 4 – „Laissez-faire“

8.6 Schüsselfaktoren

Schlüsselfaktoren sind relevante Einflussfaktoren, welche die Unterschiede zukünftiger Entwicklungen maßgeblich prägen. Für die Szenarien sind strategisch relevante, charakteristische und qualitative Entwicklungsalternativen der Schlüsselfaktoren, sogenannte Projektionen, von Bedeutung. Diese stellen somit verschiedene, zukünftig mögliche Ausprägungen der Schlüsselfaktoren dar. Für einen Schlüsselfaktor wählt man häufig zwei bis vier Projektionen. In dieser Analyse wurde der Einfachheit halber die Entwicklung eines Schlüsselfaktors in jeweils nur zwei Projektionen beschrieben.

Die den obigen Szenarien zugrundeliegenden Schlüsselfaktoren (siehe Tabelle 8) mit ihren qualitativen Extremprojektionen wurden aus Literaturstudien[332] abgeleitet und in einem Workshop ergänzt. Die Schlüsselfaktoren sind nach verschiedenen fachlichen Bereichen gegliedert.

331 Dass Klimaaktivismus aber auch drastischere Maßnahmen ergreift, zeigt etwa Green 2019.

332 Basierend insbesondere auf Hirschl et al. 2018, Appelrath et al. 2012, acatech/Leopoldina/Akademienunion 2020-1, sowie einem internen Workshop des Projekts NEDS, NEDS 2015.

Schlüsselfaktor	Projektion	Erläuterung
Technik: Netz und Speicherung		
Speicherausbau		Ausbau von Speichern verschiedener Technologien
	Niedrig	Es wurden wenig vorhandene Speicher in die Netzführung integriert.
	Hoch	Es wurden sehr viele Speicher in die Netze integriert. Dies sind sowohl kleine als auch große Speicher und für verschiedene Anwendungsfälle wie etwa zur kurzfristigen und langfristigen Speicherung entsprechend der Anforderungen durch fluktuierende EE-Einspeisung.
Inselgröße		Größe der im Netz vorhandenen Netzabschnitte, die, soweit ausreichend Speicher und Einspeisung vorhanden, im Notbetrieb autonom betrieben werden können.
	Klein	Technisch ist es möglich, auch geeignete Niederspannungsabschnitte über einen gewissen Zeitraum als Insel zu betreiben.
	Groß	Netze in der Größordnung von (heutigen) Regelzonen aber auch große Verteilernetze der Hochspannung können teilweise als „Insel“ betrieben.werden.
Technik: IKT		
Offene Standards und Interoperabilität		Verfügbarkeit von Standards und die Umsetzung der Interoperabilität, das heißt, die Fähigkeit unterschiedlicher Systeme, möglichst problemlos zusammenzuarbeiten.
	Niedrig	Die existierenden Standards sind zumeist stark herstellergebunden. Es existieren viele verschiedene Standards, die oft nicht frei zugänglich sind. Eine Zusammenarbeit von Geräten verschiedener Hersteller ist häufig nur mit großem wirtschaftlichem und technischem Aufwand möglich.
	Hoch	Offene Standards haben sich durchgesetzt, so dass Systeme verschiedener Hersteller gut zusammen arbeiten können.
Autonomiegrad		Grad der Automatisierung gemessen an der Menge der Funktionen zur Überwachung und Steuerung von Netzen und Anlagen, die von IKT und nicht von Menschen übernommen werden
	Niedrig	Der Autonomiegrad hat sich im Vergleich zu heute qualitativ wenig verändert.
	Hoch	Es herrscht ein hoher Autonomiegrad. Die meisten Prozesse laufen automatisch und ohne menschliche Eingriffe ab.

Ökonomie		
Marktformern		Grad der Verfügbarkeit und Menge verschiedener Marktformen oder -mechanismen (zum Beispiel kleinere Produkte und Produktzeiträume oder lokale Märkte).
	Niedrig	Die Märkte haben sich im Vergleich zu heute kaum verändert, nur sehr wenige Systemdienstleistungen der Verteilnetze nutzen diese.
	Hoch	Smart Markets[333] haben sich in vielen Bereichen durchgesetzt. Dadurch werden Energiemengen und Dienstleistungen so genutzt, dass Netzkapazitäten möglichst gut berücksichtigt werden.
Quartierslösungen		Verfügbarkeit und Grad der Nutzung von Quartierslösungen, in denen sich private Haushalte selbst organisieren und lokal Energie austauschen können ohne dabei von zentralen Marktinstanzen abzuhängen.
	Niedrig	Quartierslösungen haben sich nicht durchgesetzt. Der Energiehandel findet über zentrale Marktformen statt.
	Hoch	Quartierslösungen werden stark genutzt und Energie wird über Peer-to-Peer-Plattformen direkt zwischen den Teilnehmern gehandelt.
Betreiberstruktur		Größe und Struktur der Anlagenbetreiber
	Klein	Es gibt überwiegend viele kleine Betreiber in lokalen Netzen, die zum Beispiel heutigen Stadtwerken oder Energiegenossenschaften ähneln.
	Groß	Es gibt überwiegend wenige, große Betreiber, die als Oligopole auftreten und verteilt agieren – ähnlich heutigen großen Betreibern virtueller Kraftwerke.
Werte und Einstellungen		
Bereitschaft zur Mitwirkung bei Haushalten		Grad der Nutzung intelligenter Geräte[334] und Bereitschaft, die eigenen Daten Dritten zur Verfügung zu stellen sowie Anlagen direkt (über Eingriffe des Netzbetreibers) oder indirekt (zum Beispielüber Stromtarife) zu steuern
	Niedrig	Intelligente Geräte werden nur vereinzelt durch Betreiber angesprochen. Kunden stellen ihre Daten etwa für Mehrwertdienste nur zurückhaltend zur Verfügung.
	Hoch	Der Einsatz intelligenter Geräte hat sich durchgesetzt. Diese werden auf Kundenseite stark genutzt und sind miteinander und mit dem Internet vernetzt. Die Bereitschaft Daten an Dritte weiter zu geben ist hoch und wird oft umgesetzt. Auch eigene Geräte wie etwa Wärmepumpen werden den Netzbetreibern von Verbrauchern zur Steuerung zur Verfügung gestellt.

333 Vgl. BNetzA 2011.

334 Geräte, die mit IKT ausgestattet sind und mit dem Internet verbunden werden können.

Akzeptanz bei den Netzbetreibern		Verfügbarkeit von ausgebildetem Personal mit der Fähigkeit, Änderungen an Einstellungen an digitalen Technologien vorzunehmen oder Fehler zu beheben, sowie gutem Wissen und Aufgeschlossenheit zu neuen Entwicklungen (Dies bedeutet insbesondere, wie gut der Automatisierungsgrad beherrschbar ist).
	Niedrig	Das Fachpersonal reagiert hervorragend auf Standardsituationen. Besteht Notwendigkeit zu flexiblen Reaktionen mit neuen Technologien, etwa um mit neuartigen Störungen umzugehen, muss Expertise eingekauft werden.
	Hoch	Das Wissen und die Akzeptanz sind hoch. Das Fachpersonal kann auch in neuartigen Extrem- und Ausnahmesituationen nicht zuletzt aufgrund der Verwendung digital basierter Innovationen sicher und flexibel reagieren.
Politik		
Datenschutzbestreben		Grad der Umsetzung von Datenschutzbestimmungen durch den Gesetzgeber
	Niedrig	Datenschutz ist in der Politik kein hochpriorisiertes Thema weswegen es nur wenige Bestimmungen dazu gibt.
	Hoch	Es gelten strenge Datenschutzbestimmungen.
Europäischer Zusammenhalt		Grad der innereuropäischen Abstimmungen, um auf Cyber-Störungen[335] reagieren und sich gegenseitig unterstützen zu können.
	Niedrig	Es gibt keine Organisation oder Mechanismen, die eine gegenseitige Unterstützung koordinieren oder Handlungsabläufe definieren.
	Hoch	Es gibt eine verantwortliche Organisation und gut ausgearbeitet Pläne, wie im Fall von Cyber-Störungen zu reagieren ist.
Nationale Schutzmaßnahmen zur IT-Sicherheit		Grad der Bestrebung der Bundesregierung, möglichst vollständige IT-Sicherheit zu fördern
	Niedrig	Der Staat gibt Kriminalitätsbekämpfung Vorrang, so dass zum Beispiel die Erstellung von Angriffswerkzeugen und Hintertüren geduldet oder sogar gewollt sind.
	Hoch	IT Sicherheit hat hohe Priorität, weswegen möglichst alle bekannten Sicherheitslücken schnell veröffentlicht werden. Angriffswerkzeuge werden nur sehr eingeschränkt von staatlichen Stellen aufgebaut.

Tabelle 8: Schlüsselfaktoren und Zukunftsprojektionen

335 Hiermit sind Ereignisse gemeint, die im IKT-System entstehen (z. B. Programmierfehler oder Hackerangriff) und Störungen im Betrieb des Stromnetzes auslösen.

8.7 Rohszenarien

Ein Szenario ist eine prägnante Darstellung einer möglichen Zukunft, die auf widerspruchsfreien beziehungsweise konsistenten Kombinationen verschiedener Projektionen aufbaut. Eine Kombination alternativer Zukunftsprojektionen wird Rohszenario genannt. Unter Rohszenarien versteht man also konsistente Projektionsbündel[336]. Konsistent heißt dabei, dass sich einzelne Entwicklungen verschiedener Faktoren nicht gegenseitig ausschließen.

Bei der Erstellung der Szenarien war es wichtig, den Möglichkeitsraum gut abzudecken. Das heißt die Szenarien stellen möglichst verschiedene zukünftige Entwicklungen dar. Dies wurde über eine Abstandsanalyse sichergestellt: Zunächst wurde das Rohszenario Projektionsbündel „Business-as-Usual“ als linear-konservative Weiterentwicklung des heutigen Zustandes konstruiert. Als kontrastierendes Szenario wurde ein davon maximal abweichendes, gemessen an der Anzahl Unterschiede der Projektionen, konsistentes Rohszenario konstruiert. Zwei zusätzliche konsistente Rohszenarien wurden dann so konstruiert, dass der Abstand der Szenarien untereinander maximal war. Abschließend wurden allen Rohszenarien prägnante Bezeichnungen gegeben (siehe Tabelle 9).

Die Ausarbeitung des Rohszenarios als ein Narrativ rundet das Szenario ab und klärt zudem mögliche Entwicklungen (siehe Abschnitte 8.2 - 8.5). Die Szenarienauswahl und die Narrative wurden in Workshops der Arbeitsgruppe überprüft und weiterentwickelt.

	Ausprägungen			
Schlüsselfaktor \ Szenario	**Szenario 1: Business as Usual**	**Szenario 2: Automatisiert und modular**	**Szenario 3: Integriertes Europa**	**Szenario 4: Laissez-faire**
Speicherausbau	Niedrig	Hoch	Hoch	Niedrig
Inselgröße	Groß	Klein	Groß	Groß
Offene Standards und Interoperabilität	Niedrig	Hoch	Hoch	Niedrig
Autonomiegrad	Niedrig	Hoch	Niedrig	Hoch
Marktformen	Niedrig	Hoch	Hoch	Hoch
Quartierslösungen	Niedrig	Hoch	Niedrig	Niedrig
Betreiberstruktur	Klein	Klein	Groß	Groß
Bereitschaft zur Mitwirkung bei Haushalten	Niedrig	Hoch	Hoch	Niedrig
Akzeptanz bei den Netzbetreibern	Niedrig	Hoch	Hoch	Niedrig
Datenschutzbestreben	Hoch	Niedrig	Hoch	Hoch
Europäischer Zusammenhalt	Niedrig	Hoch	Hoch	Niedrig
Nationale Schutzmaßnahmen zur IT-Sicherheit	Niedrig	Niedrig	Hoch	Niedrig

Tabelle 9: Rohszenarien

336 Appelrath et al. 2012

Literatur

acatech 2011
acatech – Deutsche Akademie der Technikwissenschaften (Hrsg.): *Akzeptanz von Technik und Infrastrukturen* (acatech BEZIEHT POSITION), Heidelberg u. a.: Springer Verlag 2011.

acatech 2014-1
acatech – Deutsche Akademie der Technikwissenschaften (Hrsg.): *Future Business Clouds. Cloud Computing am Standort Deutschland zwischen Anforderungen, nationalen Aktivitäten und internationalem Wettbewerb* (acatech POSITION), 2014.

acatech 2014-2
acatech – Deutsche Akademie der Technikwissenschaften (Hrsg.): *Resilien-Tech. ‚Resilience-by-Design': Strategie für die technologischen Zukunftsthemen* (acatech POSITION), 2014.

acatech/Leopoldina/Akademienunion 2017-1
acatech – Deutsche Akademie der Technikwissenschaften, Nationale Akademie der Wissenschaften Leopoldina, Union der deutschen Akademien der Wissenschaften (Hrsg.): »*Sektorenkopplung*« – Optionen für die nächste Phase der Energiewende (Schriftenreihe zur wissenschaftsbasierten Politikberatung), 2017.

acatech/Leopoldina/Akademienunion 2017-2
acatech – Deutsche Akademie der Technikwissenschaften, Nationale Akademie der Wissenschaften Leopoldina, Union der deutschen Akademien der Wissenschaften (Hrsg.): *Das Energiesystem resilient gestalten: Maßnahmen für eine gesicherte Versorgung* (Schriftenreihe zur wissenschaftsbasierten Politikberatung), 2017.

acatech/Leopoldina/Akademienunion 2020-1
acatech – Deutsche Akademie der Technikwissenschaften, Nationale Akademie der Wissenschaften Leopoldina, Union der deutschen Akademien der Wissenschaften (Hrsg.): *Zentrale und dezentrale Elemente im Energiesystem: Der richtige Mix für eine stabile und nachhaltige Versorgung* (Schriftenreihe zur wissenschaftsbasierten Politikberatung), 2020.

acatech/Leopoldina/Akademienunion 2020-2
acatech – Deutsche Akademie der Technikwissenschaften, Nationale Akademie der Wissenschaften Leopoldina, Union der deutschen Akademien der Wissenschaften (Hrsg.): *Netzengpässe als Herausforderung für das Stromversorgungssystem. Optionen zur Weiterentwicklung des Marktdesigns* (Schriftenreihe zur wissenschaftsbasierten Politikberatung), 2020.

Agora Energiewende 2019
Agora Energiewende: *Stromspeicher in der Energiewende* (Studie), 2014. URL: https://www.hannover.ihk.de/fileadmin/data/Dokumente/Themen/Energie/Agora_Speicherstudie.pdf [Stand: 22.07.2020].

Agora Verkehrswende et al. 2019
Agora Verkehrswende/Agora Energiewende/Regulatory Assistance Projekt (RAP): Verteilnetzausbau für die Energiewende – Elektromobilität im Fokus (Studie), 2019.

Agora Energiewende/Wuppertal Institut 2020
Agora Energiewende/Wuppertal Institut: Klimaneutrale Industrie - Schlüsseltechnologien und Politikoptionen für Stahl, Chemie und Zement (Studie), Berlin 2020. URL: https://www.agora-energiewende.de/fileadmin2/Projekte/2018/Dekarbonisierung_Industrie/164_A-EW_Klimaneutrale-Industrie_Studie_WEB.pdf [Stand: 17.11.2020].

Appelrath et al. 2012
Appelrath, H.-J./Kagermann, H./Mayer, C. (Hrsg.):"*Future Energy Grid, Migrationspfade ins Internet der Energie*", acatech – Deutsche Akademie der Technikwissenschaften 2012

ARegV 2019
Anreizregulierungsverordnung vom 29. Oktober 2007 (BGBl. I S. 2529), die zuletzt durch Artikel 3 der Verordnung vom 23. Dezember 2019 (BGBl. I S. 2935) geändert worden ist.

Ausfelder et al. 2017
Ausfelder, F./Fischedick, M./Münch, W. et al. (Hrsg.): *Sektorenkopplung – Untersuchungen und Überlegungen zur Entwicklung eines integrierten Energiesystems* (Schriftenreihe Energiesysteme der Zukunft), München 2017.

Aven/Renn 2009
Aven, T./Renn, O.: „The role of quantitative risk assessment for characterizing risk and uncertainty and delineating appropriate risk management options, with special emphasis on terrorism". In: *Risk Analysis*, 29: 4, 2009, S. 587–600.

Babazadeh et al. 2018
Babazadeh, D./Mayer, C./Lehnhoff, S.: „Cyber-Resilienz". In: *bulletin.ch*, 5, 2018, S. 32–34.

Bacquet et al. 2018
Bacquet, J./Riemenschneider, R./Wintlev-Jensen, P.: „Future Trends in IoT". In: Vermesan, O./Bacquet, J. (Hrsg.): *Next Generation Internet of Things, Distributed Intelligence at the Edge and Human Machine-to-Machine Cooperation*, River Publishers 2018, S. 9–17.

Barwise/Watkins 2018
Barwise, T. P./Watkins, L.: „The evolution of digital dominance: how and why we got to GAFA". In: Moore, M./Tambini, D. (Hrsg.): *Digital Dominance: The Power of Google, Amazon, Facebook, and Apple*, New York u. a.: Oxford University Press 2018.

BBH 2017
Becker Büttner Held (BBH, Hrsg.): Studie zur *Digitalisierung der Energiewirtschaft*, 2017.

BBK/BSI 2019
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)/Bundesamt für Sicherheit in der Informationstechnik (BSI): Zusammenarbeit im Rahmen des UP KRITIS, 2020. URL: https://www.kritis.bund.de/SubSites/Kritis/DE/Aktivitaeten/Nationales/UPK/upk_node.html [Stand: 28.08.2019].

BBK/BSI 2020
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)/Bundesamt für Sicherheit in der Informationstechnik (BSI): Sektor: Informationstechnik und Telekommunikation. URL: https://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/Sektoren/ITK/ITK_node.html [Stand: 20.02.2020].

BCG 2018
The Boston Consulting Group (BCG): *The Electric Car Tipping Point - The Future of Powertrains for Owned and Shared Mobility*, 2018.

BDEW 2016
Bundesverband der Energie- und Wasserwirtschaft (BDEW, Hrsg.): *Die digitale Energiewirtschaft: Agenda für Unternehmen und Politik*, 2016.

BDEW 2017
Bundesverband der Energie- und Wasserwirtschaft (BDEW, Hrsg.): *Konkretisierung des Ampelkonzepts im Verteilungsnetz*, 2017.

BDEW 2019
Bundesverband der Energie- und Wasserwirtschaft (BDEW): *Branchenspezifischer Sicherheitsstandard für Anlagen oder Systeme zur Steuerung / Bündelung elektrischer Leistung (B3S Aggregatoren), nach § 8a Absatz 2 BSI-Gesetz*, 2019.

BDI 2019
Bundesverband der Deutschen Industrie e. V. (BDI, Hrsg.): *Deutsche digitale B2B-Plattformen, auf Deutschlands industrieller Stärke aufbauen. Ein Ökosystem für B2B-Plattformen fördern*, Berlin 2019.

Beuth 2019
Beuth, P.: Justizminister wollen, dass Mobilfunk-Überwachung bei 5G möglich ist, Spiegel online 03.06.2019. URL: https://www.spiegel.de/netzwelt/gadgets/5g-justizminister-wollen-zu-viel-sicherheit-verhindern-a-1270576.html [Stand: 25.06.2020].

Biselli 2020
Biselli, A.: Seehofer wollte den digitalen Gegenangriff starten (Update), Netzpolitik.org, 29.01.2020. URL: https://netzpolitik.org/2020/hackback-bundespolizei-seehofer-will-den-digitalen-gegenangriff-starten/ [Stand: 02.04.2020].

Bitkom 2017
Bitkom e. V.: Empfehlungen für das 7. Energieforschungsproramm der Bundesregierung – Mit der Digitalisierung in die nächste Phase der Energiewende starten, 2017. URL: https://www.bitkom.org/Bitkom/Publikationen/Empfehlungen-fuer-das-7-Energieforschungsproramm-der-Bundesregierung-Mit-der-Digitalisierung-in-die-naechste-Phase-der-Energiewende-starten.html [Stand: 23.06.2020].

BMWi 2015
Bundesministerium für Wirtschaft und Energie (BMWi, Hrsg.): *Strategie Intelligente Vernetzung*, 2015.

BMWi 2016
Bundesministerium für Wirtschaft und Energie (BMWi, Hrsg.): *Strom 2030, Langfristige Trends – Aufgaben für kommende Jahre* (Impulspapier), 2016.

BMWi 2019
Bundesministerium für Wirtschaft und Energie (BMWi): Rollout rückt näher: Drittes Zertifikat für Smart-Meter Gateway übergeben, Pressemitteilung 19.12.2019. URL: https://www.bmwi.de/Redaktion/DE/Pressemitteilungen/2019/20191219-rollout-rueckt-naeher-drittes-zertifikat-fuer-smart-meter-gateway-uebergeben.html [Stand: 21.02.2020].

BMWi 2020-1
Bundesministerium für Wirtschaft und Energie (BMWi, Hrsg.): *Die Nationale Wasserstoffstrategie*, Berlin 2020.

BMWi 2020-2
Bundesministerium für Wirtschaft und Energie (BMWi): Startschuss für den Einbau intelligenter Messsysteme – Rollout beginnt, Pressemitteilung 31.01.2020. URL: https://www.bmwi.de/Redaktion/DE/Pressemitteilungen/2020/20200131-startschuss-fuer-den-einbau-intelligenter-messsysteme-rollout-beginnt.html [Stand: 17.11.2020].

BNEF 2017
Bloomberg New Energy Finance (BNEF, Hrsg.): *Digitalization of Energy Systems* (Whitepaper), 2017.

BNetzA 2011
Bundesnetzagentur (BNetzA, Hrsg.): *„Smart Grid" und „Smart Market", Eckpunktpapier der Bundesnetzagentur zu den Aspekten des sich verändernden Energieversorgungssystems*, 2011.

BNetzA 2017
Bundesnetzagentur (BNetzA): Frequenzbedarfsabfrage für die zukünftige Nutzung der Frequenzen im Frequenzbereich 450 MHz, 2017. URL: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Frequenzen/Firmennetze/B%C3%BCndelfunk/20171220_Frequenzbedarfsabfrage450MHz.pdf?__blob=publicationFile&v=2 [Stand: 25.06.2020].

BNetzA 2019
Bundesnetzagentur (BNetzA): Moderne Messeinrichtungen / Intelligente Messsysteme, 2019. URL: https://www.bundesnetzagentur.de/DE/Sachgebiete/ElektrizitaetundGas/Verbraucher/Metering/SmartMeter_node.html [Stand: 06.03.2019].

BNetzA 2020-1
BNetzA: Covid-19-Pandemie: Netzauslastung in Deutschland, 2020. URL: https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Netzneutralitaet/Corona_Ma%C3%9Fnahmen/Corona_Ma%C3%9Fnahmen-node.html [Stand: 13.07.2020].

BNetzA 2020-2
Bundesnetzagentur (BNetzA): Kopplung der europäischen Stromgroßhandelsmärkte (Market Coupling) / Berechnung gebotszonenübergreifender Übertragungskapazitäten, 2020. URL: https://www.bundesnetzagentur.de/DE/Sachgebiete/ElektrizitaetundGas/Unternehmen_Institutionen/HandelundVertrieb/EuropMarktkopplung/MarketCoupling.html [Stand: 05.03.2020].

BNetzA/BKartA 2020
Bundesnetzagentur (BNetzA)/Bundeskartellamt (BKartA) (Hrsg.): *Monitoringbericht 2019*, 2020.

Brunekreeft et al. 2015
Brunekreeft, G./Luhmann, T./Menz, T./Müller, S.-U./Recknagel, P. (Hrsg.): *Regulatory Pathways for Smart Grid Development in China*, Springer Vieweg 2015.

Brunekreeft et al. 2016
Brunekreeft, G./Buchmann, M./Meyer, R.: „The Rise of Third Parties and the Fall of Incumbents Driven by Large-Scale Integration of Renewable Energies: The Case of Germany". In: *The Energy Journal*, 37: 2, 2016, S. 243–262.

Brühl et al. 2019
Brühl, J./Eckert, S./Tanriverdi, H./Wormer, V.: Staatsanwaltschaft ermittelt gegen deutschen Hersteller von Spähsoftware, Süddeutsche Zeitung online, 04.09.2019. URL: https://www.sueddeutsche.de/digital/finfisher-tuerkei-ermittlung-chp-spyware-handy-software-1.4587473 [Stand: 09.12.2019].

BSI 2015
Bundesamt für Sicherheit in der Informationstechnik (BSI, Hrsg.): *KRITIS-Sektorstudie, Informationstechnik und Telekommunikation (IKT)*, 2015. URL: https://www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/Sektorstudie_IKT.pdf [Stand: 12.06.2020].

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

BSI 2017-2
Bundesamt für Sicherheit in der Informationstechnik (BSI): *BSI-Standard 200-2: IT-Grundschutz-Methodik*, 2017.

BSI 2017-3
Bundesamt für Sicherheit in der Informationstechnik (BSI): *BSI-Standard 200-3: Risikoanalyse auf der Basis von IT-Grundschutz,* 2017.

BSI 2018
Bundesamt für Sicherheit in der Informationstechnik (BSI, Hrsg.): *Die Lage der IT-Sicherheit in Deutschland 2018*, Bonn 2018.

BSI 20191
Bundesamt für Sicherheit in der Informationstechnik (BSI, Hrsg.): *Die Lage der IT-Sicherheit in Deutschland 2019*, Bonn 2019.

BSI 2019-2
Bundesamt für Sicherheit in der Informationstechnik (BSI): Schutzprofil Smart Meter Gateway (BSI-CC-PP-0073), 2019. URL: https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/SmartMeter/SmartMeterGateway/Schutzprofil_Gateway/schutzprofil_smartmetergateway_node.html;jsessionid=083EF1CF6BC52A9031ED12B29C475407.1_cid341 [Stand: 03.04.2019].

BSI 20201
Bundesamt für Sicherheit in der Informationstechnik (BSI): Glossar der Cyber-Sicherheit, C, 2020. URL: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/cyberglossar/Functions/glossar.html?cms_lv2=9817276 [Stand: 12.05.2020].

BSI 2020-2
Bundesamt für Sicherheit in der Informationstechnik (BSI): Glossar der Cyber-Sicherheit, I, 2020. URL: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/cyberglossar/Functions/glossar.html?cms_lv2=9817288 [Stand: 12.05.2020].

BSIG 2019
BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 13 des Gesetzes vom 20. November 2019 (BGBl. I S. 1626) geändert worden ist.

BSI/BMWi 2019
Bundesamt für Sicherheit in der Informationstechnik (BSI)/Bundesministerium für Wirtschaft und Energie (BMWi): *Standardisierungsstrategie zur sektorübergreifenden Digitalisierung nach dem Gesetz zur Digitalisierung der Energiewende, Roadmap für die Weiterentwicklung der technischen BSI-Standards in Form von Schutzprofilen und Technischen Richtlinien*, 2019. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/SmartMeter/standardisierungsstrategie.pdf;jsessionid=1CC3BDDCACDA723CE15B04AA0D8F4D66.1_cid503?__blob=publiationFile&v=3 [Stand: 17.11.2020].

BSI-KritisV 2017
BSI-Kritisverordnung vom 22. April 2016 (BGBl. I S. 958), die durch Artikel 1 der Verordnung vom 21. Juni 2017 (BGBl. I S. 1903) geändert worden ist.

Büchner et al. 2014
Büchner, J./Katzfey, J./Flörcken, O./Moser, A./Schuster, H./Dierkes, S./van Leeuwen, T./Verheggen, L./Uslar, M./van Amelsvoort, M.: *„Moderne Verteilnetze für Deutschland"* (Verteilernetzstudie), Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi), 2014.

Burkart et al. 2014
Burkart, G./Maischatz, K./Müller, T (Hrsg.).: *Abschlussbericht zum Teilvorhaben: Soziologische Begleitforschung zum Smart Emergency Supply System*, 2014. URL: http://edok01.tib.uni-hannover.de/edoks/e01fb15/82106360X.pdf [Stand: 25.06.2020].

Chesney 2020
Chesney, R.: *The Domestic Legal Framework for U.S. Military Cyber Operations*, Hoover Institution Aegis Paper Series No. 2003, 2020.

Congress Gov 2018
Congress Gov: H.R.5515 – John S. McCain National Defense Authorization Act for Fiscal Year 2019. 132 STAT. 1636 Public Law 115-232-AUG. 13, 2018. URL: https://www.congress.gov/bill/115th-congress/house-bill/5515/text [Stand: 25.06.2020].

Connect+ 2020
Connect+ Ein Netzbetreiberprojekt: Wir machen Energiedatenaustausch möglich!, 2020. URL: https://netz-connectplus.de/ [Stand: 26.06.2020].

CRO 2020
Chief Risk Office (CRO)-Forum: Emerging Risk Initiative – Major Trends and Emerging Risk Radar – 2020 update, 2020. URL: https://www.thecroforum.org/2020/06/30/emerging-risk-initiative-major-trends-and-emerging-risk-radar-2020-update/ [Strand: 17.11.2020].

dena 2012
Deutsche Energie-Agentur GmbH (dena, Hrsg.): *Ausbau- und Innovationsbedarf der Stromverteilnetze in Deutschland bis 2030* (dena-Verteilnetzstudie), Berlin 2012.

dena 2015
Deutsche Energie-Agentur (dena, Hrsg.).: *Analyse der mit erhöhtem IT-Einsatz verbundenen Energieverbräuche infolge der zunehmenden Digitalisierung* (dena-METASTUDIE), 2015. https://www.dena.de/fileadmin/dena/Dokumente/Pdf/9232_dena-Metastudie_Analyse_IT-Einsatz_Energieverbraeuche_Digitalisierung.pdf [Stand: 03.07.2020].

dena 2019
Deutsche Energie-Agentur GmbH (dena, Hrsg.): *Künstliche Intelligenz für die integrierte Energiewende* (dena-ANALYSE), 2019. URL: https://www.dena.de/fileadmin/dena/Publikationen/PDFs/2019/dena-ANALYSE_Kuenstliche_Intelligenz_fuer_die_integrierte_Energiewende.pdf [Stand: 03.11.2020].

Deutscher Bundestag 2016
Deutscher Bundestag: „Gesetz zur Digitalisierung der Energiewende vom 29. August 2016". In: *Bundesgesetzblatt*, Teil I Nr. 43, 2016, S. 2034–2064.

Dieckhoff et al. 2014
Dieckhoff, C./Appelrath, H.-J./Fischedick, M./Grunwald, A./Höffler, F./Mayer, C./Weimer-Jehle, W.: *Zur Interpretation von Energieszenarien* (Schriftenreihe Energiesysteme der Zukunft), München 2014.

DGS/Greenpeace Energy 2019
Deutsche Gesellschaft für Sonnenenergie e. V./Greenpeace Energy: Nächster Fortschritt für Sonnenenergie vom eigenen Balkon: Mieter dürfen Steckdosen-Solargeräte jetzt selbst anmelden, 2019. URL: https://www.dgs.de/fileadmin/newsletter/2019/190423_PM%20zu%20Stecker-PV_4105.v09_final.pdf [Stand: 12.06.2020].

Duden 2019
Duden Online: digitalisieren, 2019. URL: https://www.duden.de/rechtschreibung/digitalisieren, [Stand: 28.02.2019].

Dumitrescu et al. 2018
Dumitrescu, R. et al.: *Studie „Autonome Systeme"*, 2018. URL: https://www.e-fi.de/fileadmin/Innovationsstudien_2018/StuDIS_13_2018.pdf [Stand: 03.11.2020].

E-Bridge 2019
E-Bridge (Hrsg.): *Wirtschaftlicher Vorteil der netzdienlichen Nutzung von Flexibilität in Verteilnetzen*, Kurzstudie im Auftrag von innogy SE, EWE NETZ GmbH, Stadtwerke München Infrastruktur GmbH, 2019. URL: https://www.e-bridge.de/wp-content/uploads/2019/02/20190212_Studie-E-Bridge_Vorteil_netzdienlicher-Flexibilit%C3%A4t_final.pdf [Stand: 02.07.2020].

Ecofys 2016
Ecofys: *Flex-Efficiency - Ein Konzept zur Integration von Effizienz und Flexibilität bei industriellen Verbrauchern* (Impulse), Studie im Auftrag von Agora Energiewende, 2016. URL: https://www.agora-energiewende.de/veroeffentlichungen/flex-efficiency/ [Stand: 17.11.2020].

EECSP 2017
Energy Expert Cyber Security Platform (EECSP, Hrsg.): *Cyber Security in the Energy Sector, Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector*, 2017. URL: https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf [Stand: 09.12.2019].

EEG 2020
Erneuerbare-Energien-Gesetz vom 21. Juli 2014 (BGBl. I S. 1066), das zuletzt durch Artikel 1 des Gesetzes vom 25. Mai 2020 (BGBl. I S. 1070) geändert worden ist.

EPRI 2020
Electric Power Research Institute (EPRI): Powering Through Together: Identifying COVID-19 Transmission and Distribution Operations Practices, 2020. URL: https://www.epri.com/research/products/000000003002019435 [Stand: 13.07.2020].

EEX 2019
European Energy Exchange AG (EEX): Market Operations, 2019. URL: https://www.eex.com/de/handel/market-operations [Stand: 08.03.2019].

ENaQ 2019
Energetisches Nachbarschaftsquartier Fliegerhorst Oldenburg (ENaQ): Digitale Plattform, 2019. URL: https://www.enaq-fliegerhorst.de/digitale-plattform/ [Stand: 30.04.2019].

EnBW 2019
Energie Baden-Württemberg AG: Netzsteuerung, 2019. URL: https://www.enbw.com/energie-entdecken/verteilung-und-transport/netzsteuerung/ [Stand: 02.07.2019].

Enkhardt 2019
Enkhardt, S.: Trianel stellt Smart-Meter-Aktivitäten ein, pv magazine, 03.05.2019. URL: https://www.pv-magazine.de/2019/05/03/trianel-stellt-smart-meter-aktivitaeten-ein/ [Stand: 06.05.2019].

ENTSOE 2018
European Network of Transmission System Operators for Electricity (ENTSO-E, Hrsg.): *Incident Classification Scale*, Brüssel 2018. URL: https://eepublicdownloads.blob.core.windows.net/public-cdn-container/clean-documents/SOC%20documents/Incident_Classification_Scale/180411_Incident_Classification_Scale.pdf [Stand: 09.12.2019].

ENTSO-E 2019-1
European Network of Transmission System Operators for Electricity (ENTSO-E): Imbalance Netting, 2019. URL: https://www.entsoe.eu/network_codes/eb/imbalance-netting/ [Stand: 28.03.2019].

ENTSO-E 2019-2
European Network of Transmission System Operators for Electricity (ENTSO-E): Who is ENTSO-E, 2019. URL: https://www.entsoe.eu/about/inside-entsoe/objectives/ [Stand: 20.02.2019].

ENTSO-E 2019-3
European Network of Transmission System Operators for Electricity (ENTSO-E): Day-Ahead Joint Steering Committee meeting, Decoupling on 7th June, 2019. URL: https://eepublicdownloads.entsoe.eu/clean-documents/Network%20codes%20documents/Implementation/stakeholder_committees/MESC/2019-07-02/Decouling_EPEX.pdf?Web=1.

ENTSO-E 2020
European Network of Transmission System Operators for Electricity (ENTSO-E): Response to the European Commission's public consultation to establish the priority list of Network Codes, 2020. URL: https://www.entsoe.eu/news/2020/05/26/response-to-the-european-commission-s-public-consultation-to-establish-the-priority-list-of-network-codes/ [Stand: 26.06.2020].

EnWG 2020
Energiewirtschaftsgesetz vom 7. Juli 2005 (BGBl. I S. 1970, 3621), das zuletzt durch Artikel 5 des Gesetzes vom 25. Mai 2020 (BGBl. I S. 1070) geändert worden ist.

EPEX SPOT 2017
The European Power Exchange (EPEX SPOT): Press Release „Exchange Council approves the introduction of 15-minute contracts on the Belgian and Dutch market", 2017. URL: https://www.epexspot.com/document/37626/170612_EPEX%20SPOT_Exchange%20Council.pdf [Stand: 29.03.2019].

EPEX SPOT 2019-1
The European Power Exchange (EPEX SPOT): Negative Preise, 2019. URL: https://www.epexspot.com/de/Unternehmen/grundlagen_des_stromhandels/negative_preise [Stand: 01.04.2019].

EPEX SPOT 2019-2
The European Power Exchange (EPEX SPOT): Liste der IVS, 2019. URL: https://www.epexspot.com/de/mitglied-werden/isv [Stand: 08.03.2019].

EPEX SPOT 2020
The European Power Exchange (EPEX SPOT): *Annual Report 2019*, 2020. URL: https://www.epexspot.com/sites/default/files/sites/catalogue/ [Stand: 17.11.2020].

ESYS 2019
Akademienprojekt ESYS: *Welche Bedeutung hat die Kernenergie für die künftige Weltstromerzeugung?* (Kurz erklärt!), 2019.

European Commission 2006
European Commission: *European Technology Platform SmartGrid, Vision and Strategy for Europe's Electricity Networks of the Future*, Luxembourg 2006.

European Commission 2016
European Commission (EC): Review of current national rules and practices relating to risk preparedness in the area of security of electricity supply, final report, 2016. URL: https://ec.europa.eu/energy/studies/review-current-national-rules-and-practices-relating-risk-preparedness-area-security_en [Stand: 29.06.2020].

European Commission 2019
European Commission: Commission Recommendation of 3.4.2019 on cybersecurity in the energy sector, 2019. URL: https://ec.europa.eu/energy/sites/ener/files/commission_recommendation_on_cybersecurity_in_the_energy_sector_c2019_2400_final.pdf [Stand: 23.06.2020].

Europäisches Parlament 2019
Europäisches Parlament Verbindungsbüro in Deutschland: Die Gesetzgebungsverfahren, 2019. URL: http://www.europarl.europa.eu/germany/de/europa-und-europawahlen/gesetzgebungsverfahren [Stand: 18.03.2019].

EY et al. 2018
Ernst & Young GmbH Wirtschaftsprüfungsstelle (EY)/ BET Büro für Energiewirtschaft und technische Planung GmbH/WIK Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste GmbH: *Digitalisierung der Energiewende – Topthema 3: TK-Netzinfrastruktur und TK-Regulierung*, Gutachten im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi), 2018.

EY et al. 2019
Ernst & Young GmbH Wirtschaftsprüfungsstelle (EY)/ BET Büro für Energiewirtschaft und technische Planung GmbH/WIK Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste GmbH: *Digitalisierung der Energiewende – Topthema 1: Verbraucher, Digitalisierung und Geschäftsmodelle*, Gutachten im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi), 2019.

Fischedick/Grunwald 2017
Fischedick, M./Grunwald, A.: *Pfadabhängigkeiten in der Energiewende: Das Beispiel Mobilität* (Schriftenreihe Energiesysteme der Zukunft), München 2017.

Fischer et al. 2019
Fischer, L./Memmen, J.-M./Veith, E. MSP/Tröschel, M..: „Adversarial Resilience Learning – Towards Systematic Vulnerability Analysis for Large and Complex Systems". In: International Academy, Research, and Industry Association (IARIA): *ENERGY 2019, The Ninth International Conference on Smart Grids, Green Communications and IT Energy-aware Technologies*, 2019, S. 24-32.

Fraunhofer ISE 2018
Fraunhofer-Institut für Solare Energiesysteme (ISE): Energy Charts, Nettostromerzeugung in Deutschland in 2017, 2018. URL: https://www.energy-charts.de/energy_pie_de.htm?year=2017 [Stand: 12.03.2019].

Fraunhofer ISI 2015
Fraunhofer-Institut für System- und Innovationsforschung (ISI, Hrsg.): *Gesamt-Roadmap, Stationäre Energiespeicher 2030*, Karlsruhe 2015.

Fraunhofer IOSB 2019
Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung (IOSB): Fehler in Stromnetzen mit Künstlicher Intelligenz automatisiert erkennen, 2019. URL: https://www.fraunhofer.de/content/dam/zv/de/presse-medien/2019/April/ForschungKompakt/iosb-ast-fehler-in-stromnetzen-mit-kuenstlicher-intelligenz-automatisiert-erkennen.pdf [Stand: 05.11.2020].

Fredersdorf et al. 2015
Fredersdorf, F./Schwarzer, J./Engel, D.: „Die Sicht der Endanwender im Smart Meter Datenschutz". In: *Datenschutz und Datensicherheit - DuD*, 39: 6, 2015, S. 682–686.

Furusawa et al. 2019
Furusawa, K./Brunekreeft, G./Hattori, T.: *Constrained Connection for Distributed Generation by DSOs in European Countries* (Bremen Energy Working Papers, No. 28), Jacobs University Bremen 2019.

Fünfschilling 2014
Fünfschilling, L.: *A dynamic model of socio-technical change: Institutions, actors and technologies in interaction* (Doctoral Thesis), University of Basel, Faculty of Humanities and Social Sciences, Zürich 2014.

Gasser et al. 2020
Gasser, P./Suterabc, J./Cinellia, M./Spadac, M./Burgherr, P./Hirschberg, S./Kadziński, M./Stojadinoviće, B.: „Comprehensive resilience assessment of electricity supply security for 140 countries". In: *Ecological Indicators*, 110, 2020, 105731.

Gast 2019
Gast, R.: Nein, der Quantencomputer ist noch nicht marktreif, Spektrum der Wissenschaft Verlagsgesellschaft, 09.01.2019. URL: https://www.spektrum.de/kolumne/ibm-bekanntgabe-wann-kommt-die-naechste-generation-der-supercomputer/1617490 [Stand: 25.06.2020].

Geels 2004
Geels, F. W.: „From sectoral systems of innovation to socio-technical systems Insights about dynamics and change form sociology and institutional theory". In: *Research Policy*, 33: 6-7, 2004, S. 897–929.

Geidl et al. 2017
Geidl, M./Arnoux, B./Plaisted, T./Dufour, S.: A fully operational virtual energy storage network providing flexibility for the power system, 12th IEA Heat Pump Conference 2017. URL: https://hpc2017.org/wp-content/uploads/2017/05/O.2.4.4-A-fully-operational-virtual-energy-storage-network-providing-flexibility-for-the-power-system.pdf [Stand: 09.12.2019].

GeSI/Accenture 2015
Global e-Sustainability Initiative (GeSI)/Accenture: Information and Communications Technologies Can Fast-Track Solutions to Global Warming and Social Issues While Driving Economic Growth, Finds Study by GeSI and Accenture, 2015. URL: https://newsroom.accenture.com/news/information-and-communications-technologies-can-fast-track-solutions-to-global-warming-and-social-issues-while-driving-economic-growth-finds-study-by-gesi-and-accenture.htm [Stand: 26.06.2020].

Gorman 2019
Gorman, S.: California's PG&E customers face new round of mass outages, Reuters 20.11.2019. URL: https://www.reuters.com/article/us-california-wildfire-pg-e-idUSKBN1XU07S [Stand: 26.06.2020].

Göring et al. 2016
Göring, A./Meister, J./Lehnhoff, S./Jung, M./Rohr, M./Herdt, H.: „Architecture and Quality Standards for the Joint Development of Modular Open Source Software for Power Grid Distribution Management Systems". In: Kupzog, F. (Hrsg.): *Proceedings from 5th D-A-CH+ Energy Informatics Conference in conjunction with 7th Symposium on Communications for Energy Systems (ComForEn)*, Wien: Eigenverlag des Österreichischen Verbandes für Elektrotechnik 2016, S. 36–39.

Green 2019
Green, M.: Extinction Rebellion considers using drones to shut London's Heathrow Airport, Reuters 31.05.2019. URL: https://www.reuters.com/article/us-britain-protests-climate-change/extinction-rebellion-considers-using-drones-to-shut-londons-heathrow-airport-idUSKCN1T02RF [Stand: 10.07.2020].

Gutheil et al. 2017
Gutheil, M./Liger, Q./Hettman, A./Eager, J./Crawford M.: *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, Directorate for internal policies*, 2017. URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU%282017%29583137_EN.pdf [Stand: 03.07.2020].

Haaß 1997
Haaß, W-D.: *Handbuch der Kommunikationsnetze, Einführung in die Grundlagen der Methoden der Kommunikationsnetze*, Berlin Heidelberg: Springer-Verlag 1997.

Hall 2019
Hall, M.: BNEF revidiert Erwartungen: Großspeicher werden Markt bis 2040 treiben, pv magazine 01.08.2019. URL: https://www.pv-magazine.de/2019/08/01/bnef-revidiert-erwartungen-grosspeicher-werden-markt-bis-2040-treiben/ [Stand: 03.03.2020].

Hannen 2019
Hannen, P.: Verbraucher können Balkonmodule jetzt selbst beim Netzbetreiber anmelden, 2019. URL: https://www.pv-magazine.de/2019/04/26/verbraucher-koennen-balkonmodule-jetzt-selbst-beim-netzbetreiber-anmelden/ [Stand: 26.06.2020].

haustec 2018
haustec.de: So entwickelt sich der Heimspeicher-Markt bis 2022, 2018. URL: https://www.haustec.de/energie/batteriespeicher/so-entwickelt-sich-der-heimspeicher-markt-bis-2022 [Stand: 03.03.2020].

Henry/RamirezMarquez 2016
Henry, D./Ramirez-Marquez, J. E.: „On the Impacts of Power Outages During Hurricane Sandy – A Resilience-based Approach". In: *Systems Engineering*, 19: 1, 2016, S. 59–75.

Hern 2017
Hern, A.: State hackers 'probably compromised' energy sector, says leaked GCHQ memo, 2017. URL: https://www.theguardian.com/technology/2017/jul/18/energy-sector-compromised-state-hackers-leaked-gchq-memo-uk-national-cybersecurity-centre [Stand: 25.06.2020].

Heesen et al. 2020
Heesen, J./AG IT-Sicherheit, Privacy/Recht und Ethik/ AG Technologische Wegbereiter/Data Science: *Zertifizierung von KI-Systemen* (Impulspapier Plattform Lernende Systeme), 2020. URL: https://www.plattform-lernende-systeme.de/files/Downloads/Publikationen/AG3_Impulspapier_290420.pdf [Stand: 03.11.2020].

Hirschl et al. 2018
Hirschl, B./Aretz, A./Bost, M./Tapia, M./Gößling-Reisemann, S. (Hrsg.): *Vulnerabilität und Resilienz des digitalen Elektrischen Energiesystems, Endbericht des Projekts „Strom-Resilienz"*, Berlin, Bremen 2018. URL: https://www.ioew.de/fileadmin/user_upload/BILDER_und_Downloaddateien/Publikationen/2018/Schlussbericht_Strom-Resilienz.pdf [Stand: 16.06.2020].

Hofmann/Sonnenschein 2015
Hofmann, L./Sonnenschein, M. (Hrsg.): *Smart Nord – Final Report*, Hannover 2015.

IEA 2011
International Energy Agency (IEA, Hrsg.): *Technology Roadmap – Smart Grids*, 2011.

IEEE 1991
Institute of Electrical and Electronics Engineers (IEEE, Hrsg.): *610-1990 – IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries*, New York 1991.

IEEE PES 2020
Institute of Electrical and Electronics Engineers (IEEE) Power & Energy Society (PES): *Sharing Knowledge on Electrical Energy Industry's First Response to COVID-19* (White Paper), 2020. URL: https://resourcecenter.ieee-pes.org/technical-publications/white-paper/PES_TP_COVID19_050120.html [Stand: 02.07.2020].

Illinois Tech 2020
Illinois Tech: COVID-19 Pandemic Highlights Challenges for Power System Operation, 2020. URL: https://www.iit.edu/news/covid-19-pandemic-highlights-challenges-power-system-operation-planning [Stand: 13.07.2020].

IRGC 2018
International Risk Governance Center (IRGC, Hrsg.): *Guidelines for the Governance of Systemic Risks*, Lausanne 2018.

ITU 2020
International Telecommunication Union (ITU): ITU Guidelines for national emergency telecommunication plans, 2020. URL: https://www.itu.int/en/ITU-D/Emergency-Telecommunications/Pages/Publications/Guidelines-for-NETPs.aspx [Stand: 13.07.2020].

Jacoby 2018
Jacoby, W. (Hrsg.): *Das Internet der Dinge als Basis der digitalen Automation*, BoD – Books on Demand 2018.

Jones/Mendelson 2011
Jones, R./Mendelson, H.: „Information Goods vs. Industrial Goods: Cost Structure and Competition". In: *Management Science*, 57: 1, 2011, S. 146-176.

Jones/Wagner 2018
Jones, B./Wagner, J.: IBM's blockchain-ready CPU is smaller than a grain of salt, costs just 10 cents, digitaltrends.com, 22.03.2018. URL: https://www.digitaltrends.com/computing/ibm-blockchain-computer-salt/ [Stand: 03.04.2020].

Katwala 2019
Katwala, A.: Here's how GCHQ scours Huawei hardware for malicious code, Wired, 22.02.2019. URL: https://www.wired.co.uk/article/huawei-gchq-security-evaluation-uk [Stand: 26.06.2020].

Kersting/Tresp 2019
Kersting, K./Tresp, V.: *Maschinelles und Tiefes Lernen* (Whitepaper Plattform Lernende Systeme) 2019. URL: https://www.plattform-lernende-systeme.de/publikationen-details/maschinelles-und-tiefes-lernen-der-motor-fuer-ki-made-in-germany.html?file=files/Downloads/Publikationen/AG1_Whitepaper_280619.pdf [Stand: 03.11.2020]

Kreuzburg 2018
Kreuzburg, M. (Hrsg.): *Rechtliche und marktorganisatorische Anforderungen an den P2P-Stromhandel* (FSBC Working Paper), 2018. URL: http://www.explore-ip.com/2018_P2P-Stromhandel.pdf [Stand: 16.06.2020].

Kröger 2017
Kröger, W.: „Securing the Operation of Socially Critical Systems from an Engineering Perspective: New Challenges, Enhanced Tools and Novel Concepts". In: *European Journal for Security Research*, 2, 2017, S. 39–55.

Kröger 2019
Kröger, W.: „Achieving Resilience of Large-Scale Engineered Infrastructure Systems". In: Noroozinejad Farsangi, E./Takewaki, I./Yang, T./Astaneh-Asl, A./Gardoni, P. (Hrsg.): *Resilient Structures and Infrastructure*, Singapore: Springer 2019, S. 289–313.

KWKG 2019
Kraft-Wärme-Kopplungsgesetz vom 21. Dezember 2015 (BGBl. I S. 2498), das zuletzt durch Artikel 4 des Gesetzes vom 20. November 2019 (BGBl. I S. 1719) geändert worden ist.

Langner 2011
Langner, R.: „Stuxnet: Dissecting a Cyberwarfare Weapon". In: *IEEE Security & Privacy*, 9: 3, 2011, S. 49-51.

Liang et al. 2017
Liang, G./Weller, S. R./Zhao, J./Luo, F./Dong, Z. Y.: „The 2015 Ukraine Blackout: Implications for False Data Injection Attacks". In: *IEEE Transactions on Power Systems*, 32: 4, 2017, S. 3317-3318.

Loleski 2018
Loleski, L.: „From cold to cyber warriors: the origins and expansion of NSA's Tailored Access Operations (TAO) to Shadow Brokers". In: *Intelligence and National Security*, 34: 1, 2018, S. 112-128.

London Business School 2020
London Business School: Nine reasons why tech markets are winner-take-all, 2020. URL: https://www.london.edu/think/nine-reasons-why-tech-markets-are-winner-take-all [Stand: 23.07.2020].

Mann et al. 2018
Mann, M./Rahmstorf, S./Kornhuber, K./Steinman, B. A./Miller, S. K./Petri, S./Coumou, D.: „Projected changes in persistent extreme summer weather events: The role of quasi-resonant amplification". In: *Science Advances*, 4: 10, 2018.

Mattern/Flörkemeier 2010
Mattern, F./Flörkemeier, C.: „Vom Internet der Computer zum Internet der Dinge". In: *Informatik-Spektrum*, 33: 2, 2010, S. 107–121.

McGraw 2013
McGraw, G.: „Cyber War is Inevitable (Unless We Build Security In)". In: *Journal of Strategic Studies*, 36: 1; 2013, S. 109-119.

Meinel/Sack 2009
Meinel, C./Sack, H.: *Digitale Kommunikation: Vernetzen, Multimedia, Sicherheit*, Berlin Heidelberg: Springer-Verlag 2009.

Metzger 2018
Metzger, J.: Distributed Ledger Technologie (DLT), Revision vom 19.02.2018, 14:40. In: *Gabler Wirtschaftslexikon (online)*. URL: https://wirtschaftslexikon.gabler.de/definition/distributed-ledger-technologie-dlt-54410/version-277444 [Stand: 11.02.2020].

Mihm 2019
Mihm, A.: So will die Netzagentur weitere Chaostage verhindern, Frankfurter Allgemiene Zeitung (online), 18.07.2019, URL: https://www.faz.net/aktuell/wirtschaft/deutsches-stromnetz-netzagentur-will-harte-strafen-fuer-haendler-16291655.html [Stand: 09.12.2019].

MsbG 2019
Messstellenbetriebsgesetz vom 29. August 2016 (BGBl. I S. 2034), das zuletzt durch Artikel 90 des Gesetzes vom 20. November 2019 (BGBl. I S. 1626) geändert worden ist.

NEDS 2015
Nachhaltige Energieversorgung Niedersachsen (NEDS): Projekt NEDS, 2015. URL: https://www.neds-niedersachsen.de/183.html [Stand: 26.06.2020].

Hermann et al. 2018
Hermann, A./Börries, S./Ott, R./Steiner, S./Höckner, J.: „enera: Flexibilitätsmärkte für die netzdienliche Nutzung", 2018. In: *netzpraxis*, 57: 11–12, 2018, S. 51-53.

Müller-Quade et al. 2019
Müller-Quade, J. et al.: *Neue Geschäftsmodelle mit Künstlicher Intelligenz – Bericht der Arbeitsgruppe Geschäftsmodellinnovationen* (Whitepaper Plattform Lernende Systeme), 2019. URL: https://www.plattform-lernende-systeme.de/files/Downloads/Publikationen/20190403_Whitepaper_AG3_final.pdf [Stand: 05.11.2020].

Netztransparenz 2019
Netztransparenz.de: EEG-Anlagenstammdaten zur Jahresberechnung 2017, 2019. URL: https://www.netztransparenz.de/EEG/Anlagenstammdaten [Stand: 13.02.2019].

Nieles et al. 2017
Nieles, M./Dempsy, K. L./Pillitteri, V. Y.: *An Introduction to Information Security* (NIST Special Publication 800-12), National Institute of Standards and Technology (NIST) 2017.

Nordpool 2020
Nordpool: COVID-19 Outbreak 2020; Nord Pool Business Continuity Management, 2020. URL: https://www.nordpoolgroup.com/About-us/covid-19-outbreak-2020-nord-pool-business-continuity-management/ [Stand: 13.07.2020].

Paaso et al. 2020
Paaso, A./Bahramirad, S./Beerten, J./Bernabeu, E./Chiu. B./Enayati, B./Hederman, B./Jones, L./Jun, Y./Koch, H./Montero, J. C./Nair, N./Novosel, D./Pierpoint, T./Rahmatian, F./Aguero J. R./Root, C./Sharafi, D./Tejera, E./Vittal, V.: *Sharing Knowledge on Electrical Energy Industry's First Response to COVID-19* (Whitepaper), IEEE 2020, https://resourcecenter.ieee-pes.org/technical-publications/white-paper/PES_TP_COVID19_050120.html [Stand: 30.06.2020].

Petermann et al. 2011
Petermann, T./Bradke, H./Lüllman, A./Poetzsch, M./Riehm, U.: *Was bei einem Blackout geschieht: Folgen eines langandauernden und großräumigen Stromausfalls* (Studien des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag – 33), Berlin: edition sigma 2011.

Piaszeck et al. 2013
Piaszeck, S./Wenzel, L./Wolf, A.: *Regional Diversity in the Costs of Electricity Outages: Results for German Counties* (HWWI Research Paper 142), Hamburg Institute of International Economics (HWWI) 2013.

Plattform Industrie 4.0 2020
Plattform Industrie 4.0: Was ist Industrie 4.0?, 2020. URL: https://www.plattform-i40.de/PI40/Navigation/DE/Industrie40/WasIndustrie40/was-ist-industrie-40.html, [Stand: 15.10.2020]

Plattform Lernende Systeme 2020
Plattform Lernende Systeme: Glossar, 2020. URL: https://www.plattform-lernende-systeme.de/glossar.html, [Stand: 16.07.2020].

PSOTF 2004
U.S.-Canada Power System Outage Task Force (PSOTF): *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, 2004.

Quark 2014
Quark, N.: Markttag – Wie kommt eigentlich der Strom aus einem virtuellen Kraftwerk an die Börse? Teil 3, 2014. URL: https://www.next-kraftwerke.de/energie-blog/stromhandel-regelenergie [Stand: 24.02.2020].

Regelleistung 2019-1
Regelleistung.net: Markt für Regelleistung in Deutschland, 2019. URL: https://www.regelleistung.net/ext/static/market-information [Stand: 10.03.2019].

Regelleistung 2019-2
Regelleistung.net: Präqualifikation für die Vorhaltung und Erbringung von Regelreserve, 2019. URL: https://www.regelleistung.net/ext/static/prequalification [Stand: 09.12.2019].

Regulation (EC) No 714/2009
Regulation (EC) No 714/2009 of the European Parliament and the Council of 13 July 2009 on conditions for access to the network for cross-border exchanges in electricity and repealing Regulation (EC) No 1228/2003.

Rid 2012
Rid, T.: „Cyber War Will Not Take Place". In: *Journal of Strategic Studies*, 35: 1, 2012, S. 5-32.

Rosinger/Uslar 2017
Rosinger, C./Uslar, M.: „§ 24: Zertifizierung des Smart Meter Gateway". In: v. Steinbach, A./Weise, M. (Hrsg.): *Messstellenbetriebsgesetz*, Berlin/Boston: Walter de Gruyter GmbH 2017, S. 183–191.

Russel/Norvig 2010
Russel, S./Norvig, P.: *Artificial Intelligence: A Modern Approach,* 3. Auflage, Upper Sassle River, New Jersey: Pearson Education 2010.

Sanger/Perlroth 2019
Sanger, D. E./Perlroth, N.: U.S. Escalates Online Attacks on Russia's Power Grid, 2019. URL: https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html [Stand: 25.06.2020].

Schittekatte et al. 2019
Schittekatte, T./Reif, V./Meeus, L.: *The EU Electricity Network Codes* (Technological Report), European University Institute 2019.

Schnabel 2015
Schnabel, P.: *Kommunikationstechnik-Fibel*, 2015.

Schröder/Kuckshinrichs 2015
Schröder, T./Kuckshinrichs, W.: „Value of Lost Load: An Efficient Economic Indicator for Power Supply Security? A Literature Review". In: *Frontiers in Energy Research*, 3: 55, 2015.

Schwab 2012
Schwab, A. J.: *Elektroenergiesysteme – Erzeugung, Transport, Übertragung und Verteilung elektrischer Energie*, Berlin Heidelberg: Springer-Verlag 2012.

Scott 2001
Scott, W. R.: *Institutions and Organization*, SAGE Publications 2001.

SGTF EG2 2019
Smart Grid Task Force Expert Group 2 on cybersecurity (SGTF EG2, Hrsg.): *Recommendations to the European Commission for the Implementation of Sector-Specific Rules for Cybersecurity Aspects of Cross-Border Electricity Flows, on Common Minimum Requirements, Planning, Monitoring, Reporting and Crisis Management*, 2019. URL: https://ec.europa.eu/energy/sites/ener/files/sgtf_eg2_report_final_report_2019.pdf [Stand: 16.06.2020].

smart-me 2020
smart-me: smart-me Technologie: Energiemessgeräte und Cloud-Software, 2020. URL: https://web.smart-me.com/technologie/ [Stand: 19.05.2020].

Spence 1975
Spence, A. M.: „Monopoly, quality and regulation". In: *Bell Journal of Economics*, 6: 2, 1975, S. 417–429.

Spiegel 2019
Der Spiegel: Weser zu warm – AKW Grohnde wird abgeschaltet, 2019. URL: https://www.spiegel.de/wissenschaft/technik/niedersachsen-weser-zu-warm-atomkraftwerk-grohnde-wird-abgeschaltet-a-1278987.html [Stand: 26.06.2020].

Statista 2019
Statista: Anzahl der Stromanbieterwechsel durch Haushaltskunden in Deutschland in den Jahren 2008 bis 2018, 2019. URL: https://de.statista.com/statistik/daten/studie/155539/umfrage/anzahl-der-versorgerwechsel-in-der-stromversorgung-seit-2005/ [Stand: 01.06.2020].

Steetskamp/van Wijk 1994
Steetskamp, I./van Wijk, D.: *Stromausfall: Die Verletzlichkeit der Gesellschaft; die Folgen von Störungen der Elektrizitätsversorgung* (Eine Studie des Rathenau-Instituts), Den Haag 1994.

Stolle et al. 2019
Stolle, C./Klaaßen, L./Gallersdörfer, U.: „The Carbon Footprint of Bitcoin". In: *Joule*, 3: 7, 2019, S. 1647-1661.

StromNEV 2019
Stromnetzentgeltverordnung vom 25. Juli 2005 (BGBl. I S. 2225), die zuletzt durch Artikel 1 der Verordnung vom 23. Dezember 2019 (BGBl. I S. 2935) geändert worden ist.

Stromnetze 2019
Forschungsinitiative Zukunftsfähige Stromnetze: Struktur des Stromnetzes, 2019. URL: https://forschung-stromnetze.info/basisinformationen/struktur-des-stromnetzes/verteilnetz/ [Stand: 20.02.2019].

Tagesspiegel 2019
Tagesspiegel Online: Nato rüstet sich für den Cyberkrieg, 2019. URL: https://www.tagesspiegel.de/politik/manoever-locked-shield-nato-ruestet-sich-fuer-den-cyberkrieg/24257218.html [Stand: 23.06.2020].

Taylor 2012
Taylor, T.: „Konvergenz von IT und OT, Steigerung der Leistungsfähigkeit von Verteilnetzen durch das Zusammenwachsen von IT und OT". In: *ABB technik*, 3, 2012, S. 23–27.

The Economist 2019-1
The Economist: What NATO is doing to keep abreast of new challenges, 2019. URL: https://www.economist.com/special-report/2019/03/14/what-nato-is-doing-to-keep-abreast-of-new-challenges?frsc=dg%7Ce [Stand: 23.06.2020].

The Economist 2019-2
The Economist: Offering software for snooping to governments is a booming business, 2019. URL: https://www.economist.com/business/2019/12/12/offering-software-for-snooping-to-governments-is-a-booming-business [Stand: 26.06.2020].

Thoma 2014
Thoma, K. (Hrsg.): *Resilien-Tech – "Resilience by Design": a strategy for the technology issues of the future* (acatech STUDY), München 2014.

Thomas/McDonald 2015
Thomas, M. S./McDonald, J. D (Hrsg.): *Power System SCADA and Smart Grids*, CRC Press 2015.

Thunnissen 2003
Thunnissen, D. T.: Uncertainty Classification for the Design and Development of Complex Systems, 3rd Annual Predictive Methods Conference, Newport Beach, California, 2003. URL: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.128.133&rep=rep1&type=pdf [Stand: 5.11.2020]

Tondel et al. 2018
Tøndel, I. A./Foros, J./Kilskar, S. S./Hokstad, P./Jaatun, M. G.: „Interdependencies and reliability in the combined ICT and power system: An overview of current research". In: *Applied Computing and Informatics*, 14: 1, 2018, S. 17–27.

Top 2018
Top Magazin Frankfurt (top): DE-CIX – Der größte Internetknoten der Welt, 2018. URL: https://www.top-magazin-frankfurt.de/redaktion/business-finance/de-cix-der-groesste-internetknoten-der-welt/ [Stand: 03.07.2019].

UCTE 2004-1
Union for the Co-ordination of the Transmission of Electricity (UCTE, Hrsg.): *Final Report of the Investigation Committee on the 28 September 2003 Blackout in Italy*, 2004.

UCTE 2004-2
Union for the Co-ordination of the Transmission of Electricity (UCTE, Hrsg.): *Policy 3: Operational Security v1.3/20.07.04*, 2004.

UCTE 2006
Union for the Co-ordination of the Transmission of Electricity (UCTE, Hrsg.): *Final Report – System Disturbance on 4 November 2006*, 2006.

Van der Aalst et al. 2019
Van der Aalst, W./Hinz, O./Weinhardt, C.: „Big Digital Platforms: Growth, Impact, and Challenges". In: *Business & Information Systems Engineering*, 61: 2, 2019, S. 645–648.

Vardi 2018
Vardi, M. Y.: „Move Fast and Break Things". In: *Communications of the ACM*, 61: 9, 2018, S. 7.

VDE 2019
Verband der Elektrotechnik, Elektronik und Informationstechnik (VDE): *E DIN VDE 0175-110 Richtlinien zur IT-Sicherheit und Resilienz für die Smart-Energy-Einsatzumgebung*, VDE Verlag 2019.

VDE|FNN 2018-1
Forum Netztechnik/Netzbetrieb im VDE (VDE|FNN): Allgemeines und Übersicht zu Technischen Anschlussregeln, 2018. URL: https://www.vde.com/de/fnn/arbeitsgebiete/tar/uebersicht [Stand: 27.02.2020].

VDE|FNN 2018-2
Forum Netztechnik/Netzbetrieb im VDE (VDE|FNN): Erzeugungsanlagen am Niederspannungsnetz (VDE-AR-N 4105), 2018. URL: https://www.vde.com/de/fnn/arbeitsgebiete/tar/tar-niederspannung/erzeugungsanlagen-am-niederspannungsnetz-vde-ar-n-4105-2018 [Stand: 09.12.2019].

VDE|FNN 2018-3
Forum Netztechnik/Netzbetrieb im VDE (VDE|FNN): Elektromobilität flächendeckend ermöglichen mit dem Stromnetz als Backbone, 2018. URL: https://www.vde.com/de/fnn/aktuelles/20181108-e-mobilitaet-backbone-stromnetz [Stand: 09.12.2019].

VDE|FNN 2019-1
Forum Netztechnik/Netzbetrieb im VDE (VDE|FNN): Systemdienstleistungen, 2019. URL: https://www.vde.com/de/fnn/arbeitsgebiete/vom-netz-zum-system/systemdienstleistungen [Stand: 26.05.2020].

VDE|FNN 2019-2
Forum Netztechnik/Netzbetrieb im VDE (VDE|FNN): Erstellung und Verhältnis zu Anwendungsregeln, 2019. URL: https://www.vde.com/de/fnn/arbeitsgebiete/europaeische-network-codes/erstellung-und-nationales-regelwerk [Stand: 27.02.2020].

VDE|FNN 2019-3
Forum Netztechnik/Netzbetrieb im VDE (VDE|FNN): Technische Anschlussregeln Niederspannung (VDE-AR-N 4100), 2019, URL: https://www.vde.com/de/fnn/arbeitsgebiete/tar/tar-niederspannung/tar-niederspannung-vde-ar-n-4100 [Stand: 09.12.2019].

VDN 2007
Verband der Netzbetreiber e. V. (VDN, Hrsg.) beim VDEW: *TransmissionCode 2007 – Netz- und Systemregeln der deutschen Übertragungsnetzbetreiber*, 2007. URL: https://www.vde.com/resource/blob/937758/14f1b92ea821e9e19ee13fc798c1ee0e/transmissioncode-2007--netz--und-systemregeln-der-deutschen-uebertragungsnetzbetreiber-data.pdf [Stand: 09.12.2019].

Vermesan et al. 2018
Vermesan, O./Eisenhauer, M./Serrano, M./Guillemin, P./Sundmaeker, H./Tragos, E. Z./Valino, J./Copigneaux, B./Presser, M./Aagaard, A./Bahr, R./Darmois, E. C.: „The Next Generation Internet of Things – Hyperconnectivity and Embedded Intelligence at the Edge". In: Vermesan, O./Bacquet, J. (Hrsg.): *Next Generation Internet of Things, Distributed Intelligence at the Edge and Human Machine-to-Machine Cooperation*, River Publishers 2018, S. 19-102.

Verordnung (EU) 2015/1222
Verordnung (EU) 2015/1222 der Kommission vom 24. Juli 2015 zur Festlegung einer Leitlinie für die Kapazitätsvergabe und das Engpassmanagement.

Verordnung (EU) 2016/631
Verordnung (EU) 2016/631 der Kommission vom 14. April 2016 zur Festlegung eines Netzkodex mit Netzanschlussbestimmungen für Stromerzeuger.

Verordnung (EU) 2016/1388
Verordnung (EU) 2016/1388 Der Komission vom 17. August 2016 zur Festlegung eines Netzkodex für den Lastanschluss.

Verordnung (EU) 2017/1485
Verordnung (EU) 2017/1485 der Kommission vom 2. August 2017 zur Festlegung einer Leitlinie für den Übertragungsnetzbetrieb.

Verordnung (EU) 2017/2196
Verordnung (EU) 2017/2196 der Kommission vom 24. November 2017 zur Festlegung eines Netzkodex über den Notzustand und den Netzwiederaufbau des Übertragungsnetzes.

Verordnung (EU) 2019/881
Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit).

Verordnung (EU) 2019/941
Verordnung (EU) 2019/941 des Europäischen Parlaments und des Rates vom 5. Juni 2019 über die Risikovorsorge im Elektrizitätssektor und zur Aufhebung der Richtlinie 2005/89/EG.

Verordnung (EU) 2019/943
Verordnung (EU) 2019/943 des Europäischen Parlaments und des Rates vom 5. Juni 2019 über den Elektrizitätsbinnenmarkt (Neufassung).

WBGU 2019
Wissenschaftlicher Beirat der Bundesregierung Globale Umweltveränderungen (WBGU): *Unsere gemeinsame digitale Zukunft*, Berlin: WBGU 2019. URL: https://www.wbgu.de/fileadmin/user_upload/wbgu/publikationen/hauptgutachten/hg2019/pdf/wbgu_hg2019.pdf [Stand: 17.11.2020].

Weijen/Bouwmans 2006
Weijnen, M./Bouwmans, I: „Innovation in Networked Infrastructures Coping with Complexity". In: *International Journal of Critical Infrastructures*, 2: 2/3, 2006, S. 121–132.

Weimer-Jehle/Kosow 2011
Weimer-Jehle, W./Kosow, H.: „Gesellschaftliche Kontextszenarien als Ausgangspunkt für modellgestützte Energieszenarien". In: Dieckhoff, C./Fichtner, W./Grunwald, A. et al. (Hrsg.): *Energieszenarien: Konstruktion, Bewertung und Wirkung – Anbieter und „Nachfrager" im Dialog*, Karlsruhe: KIT Scientific Publishing 2011, S. 53–65.

Westenergie 2020
Westenergie: CyberRange-e: Digitale Angriffe abwehren, 2020. URL: https://www.westenergie.de/unternehmen/netzservice/produkte/cyberrange-e [Stand: 17.11.2020].

Whitehead et al. 2017
Whitehead, D./Owens, K./Gammel, D./Smith, J.: „Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies". In: *70th Annual Conference for Protective Relay Engineers (CPRE)*, 2017.

Wooldridge/Jennings 1995
Wooldridge, M./Jennings, N. R.: „Intelligent agents: theory and practice". In: *The Knowledge Engineering Review*, 10: 2, 1995, S. 115–152.

Wüstenhagen et al. 2007
Wüstenhagen, R./Wolsink, M./Bürer, M. J.: „Social acceptance of renewable energy innovation: An introduction to the concept". In: *Energy Policy*, 35: 5, 2007, S. 2683–2691.

WWF 2018
WWF Deutschland (Hrsg.): *Zukunft Stromsystem II – Regionalisierung der erneuerbaren Stromerzeugung*, 2018.

Das Akademienprojekt

Mit der Initiative „Energiesysteme der Zukunft“ geben acatech – Deutsche Akademie der Technikwissenschaften, die Nationale Akademie der Wissenschaften Leopoldina und die Union der deutschen Akademien der Wissenschaften Impulse für eine faktenbasierte Debatte über Herausforderungen und Chancen der Energiewende in Deutschland. In interdisziplinären Arbeitsgruppen erarbeiten rund 100 Expertinnen und Experten Handlungsoptionen für den Weg zu einer umweltverträglichen, sicheren und bezahlbaren und Energieversorgung.

Die Arbeitsgruppe „Resilienz digitalisierter Energiesysteme“

Die Digitalisierung ist für die Energiewende unerlässlich, denn die Steuerung eines Energiesystems mit vielen kleinen Stromerzeugern und Speichern, volatiler Stromeinspeisung und zunehmender Sektorenkopplung erfordert ein hohes Maß an Automatisierung. Gleichzeitig bringt die Digitalisierung neue Risiken mit sich wie Cyberangriffe oder fehlerhafte IKT-Anwendungen. Die interdisziplinär zusammengesetzte Arbeitsgruppe hat untersucht, wie Blackouts im zukünftigen, digitalisierten Energiesystem verhindert werden können.

Die Ergebnisse der Arbeitsgruppe wurden in zwei Formaten aufbereitet:

1. Die **Analyse** *„Resilienz digitalisierter Energiesysteme. Blackout-Risiken verstehen, Stromversorgung sicher gestalten“* dokumentiert in umfassender Form den wissenschaftlichen Kenntnisstand zu den Risiken eines digitalisierten Energiesystems und der Anwendung des Resilienzkonzeptes in der Stromversorgung und erläutert die von der Arbeitsgruppe vorgeschlagenen Handlungsoptionen zu den Risiken eines digitalisierten Energiesystems und der Anwendung des Resilienzkonzeptes in der Stromversorgung im Detail.

2. Die **Stellungnahme** *„Resilienz digitalisierter Energiesysteme. Wie können Blackout-Risiken begrenzt werden?“* stellt die Ergebnisse in kompakter Form dar.

Mitwirkende des Projekts

Mitglieder der Arbeitsgruppe

Dr. Christoph Mayer (Leitung)	OFFIS, Oldenburg
Prof. Dr. Gert Brunekreeft (Leitung)	Jacobs University Bremen
Dr. Marius Buchmann	Jacobs University Bremen
Mathias Dalheimer	Fraunhofer ITWM
Dr. Volker Distelrath	Siemens AG
Prof. Dr. Bernd Hirschl	IÖW/BTU Cottbus
Prof. Dr. Jochen Kreusel	Hitachi ABB Power Grids
Prof. Dr. Wolfgang Kröger	ETH Zürich
Prof. Dr. Sebastian Lehnhoff	OFFIS, Oldenburg
Dr. Till Luhmann	BTC AG
Prof. Dr. Jannika Mattes	Universität Oldenburg
Prof. Dr. Ellen Matthies	Universität Magdeburg
Dr. Philipp Werdelmann	Westnetz GmbH
Prof. Dr.-Ing. Christof Wittwer	Fraunhofer ISE

Wissenschaftliche Referentinnen

Katharina Bähr	acatech
Dr. Marita Blank-Babazadeh	OFFIS, Oldenburg
Dr. Achim Eberspächer	acatech
Dr. Berit Erlach	acatech
Sanja Stark	OFFIS, Oldenburg

Institutionen und Gremien

Beteiligte Institutionen

acatech – Deutsche Akademie der Technikwissenschaften (Federführung)
Nationale Akademie der Wissenschaften Leopoldina
Union der deutschen Akademien der Wissenschaften

Direktorium

Das Direktorium leitet die Projektarbeit und vertritt das Projekt nach außen.

Prof. Dr. Dirk Uwe Sauer (Vorsitzender)	RWTH Aachen
Prof. Dr. Christoph M. Schmidt (Stellvertreter)	RWI – Leibniz-Institut für Wirtschaftsforschung
Prof. Dr. Hans-Martin Henning	Fraunhofer-Institut für Solare Energiesysteme ISE
Prof. Dr. Karen Pittel	ifo Institut
Prof. Dr. Jürgen Renn	Max-Planck-Institut für Wissenschaftsgeschichte
Prof. Dr. Indra Spiecker genannt Döhmann	Goethe-Universität Frankfurt am Main

Kuratorium

Das Kuratorium verantwortet die strategische Ausrichtung der Projektarbeit.

Prof. Dr. Reinhard F. Hüttl (Vorsitzender)	acatech Vizepräsident (Amt ruht derzeit)
Prof. Dr.-Ing. Dieter Spath	acatech Präsident
Prof. (ETHZ) Dr. Gerald Haug	Präsident Leopoldina
Prof. Dr. Dr. Hanns Hatt	Präsident Union der deutschen Akademien der Wissenschaften
Prof. Dr. Bärbel Friedrich	Altpräsidialmitglied Leopoldina
Prof. Dr.-Ing. Edwin J. Kreuzer	Präsident Akademie der Wissenschaften in Hamburg
Prof. Dr. Andreas Löschel	Universität Münster, Vorsitzender der Expertenkommission zum Monitoring-Prozess „Energie der Zukunft“
Prof. Dr. Robert Schlögl	Direktor Fritz-Haber-Institut der Max-Planck-Gesellschaft und Max-Planck-Institut für Chemische Energiekonversion
Oda Keppler (Gast)	Ministerialdirigentin BMBF
Dr. Rodoula Tryfonidou (Gast)	Referatsleiterin Energieforschung BMWi

Projektkoordination

Dr. Ulrich Glotzbach	Leiter der Koordinierungsstelle „Energiesysteme der Zukunft“, acatech

Rahmendaten

Projektlaufzeit
03/2016 bis 02/2022

Finanzierung
Das Projekt wird vom Bundesministerium für Bildung und Forschung (Förderkennzeichen 03EDZ2016) gefördert.

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

Hauptstadtbüro:
Dr. Ulrich Glotzbach
Leiter der Koordinierungsstelle „Energiesysteme der Zukunft“
Pariser Platz 4a, 10117 Berlin
Tel.: +49 (0)30 206 30 96 - 0
E-Mail: glotzbach@acatech.de

Schriftenreihe Energiesysteme der Zukunft

ISBN: 978-3-9820053-3-1