Leopoldina
Nationale Akademie
der Wissenschaften

acatech
DEUTSCHE AKADEMIE DER
TECHNIKWISSENSCHAFTEN

UNION
DER DEUTSCHEN AKADEMIEN
DER WISSENSCHAFTEN

Februar 2021
Stellungnahme

Resilienz digitalisierter Energiesysteme

Wie können Blackout-Risiken begrenzt werden?

„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

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

Redaktion
Anja Lapac, acatech

Wissenschaftliche Koordination
Dr. Achim Eberspächer, acatech
Dr. Berit Erlach, acatech
Dr. Marita Blank-Babazadeh, OFFIS
Katharina Bähr, acatech
Sanja Stark, OFFIS

Produktionskoordinatorin und Satz
Annika Seiler, acatech

Gestaltung
aweberdesign.de . Büro für Gestaltung

Coverfoto
shutterstock.com/142043677/Gianluca Muscelli

Druck
Kern, Bexbach
Gedruckt auf säurefreiem Papier, Printed in EC

ISBN: 978-3-8047-4224-6

Bibliographische 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.

Resilienz digitalisierter Energiesysteme

Wie können Blackout-Risiken begrenzt werden?

Vorwort

Die Digitalisierung kann die Energieversorgung umweltfreundlicher, zuverlässiger und ökonomisch effizienter machen. Zugleich erwachsen aus ihr neue Fehlerquellen und Angriffsflächen. So schnitt am 14. August 2003 ein großflächiger Stromausfall 55 Millionen Menschen in der Nordost-Region der USA und in Teilen Kanadas von der Stromversorgung ab. Erst nach zwei Tagen waren wieder alle Verbraucher am Netz. Die Ursache war ein unerkannter Softwarefehler, der durch eine unglückliche Verkettung von Ereignissen schwerwiegende Folgen hatte. Und bereits 2015 gelang es Hackern in der Ukraine weltweit zum ersten Mal, einen Stromausfall auszulösen.

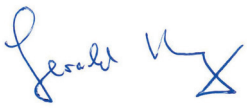
Blackouts sind besonders bedrohlich, weil das Stromsystem eine Sonderstellung unter den kritischen Infrastrukturen einnimmt. Wasserversorgung und -entsorgung, Transport, Gesundheitswesen sowie Informations- und Kommunikationstechnologien reagieren bereits nach kurzer Zeit empfindlich auf Störungen in der Stromversorgung.

Eine ESYS-Arbeitsgruppe untersuchte anhand möglicher Zukunftsszenarien für das Jahr 2040, wie sich Risikofaktoren für Blackouts entwickeln und welche neu entstehen könnten. Sowohl die Energiewende als auch die Digitalisierung sind jeweils dynamische Geschehen, deren Einflussfaktoren nicht immer gesteuert werden können. Unvorhergesehene und unvorhersehbare Ereignisse werden deshalb zukünftig häufiger eintreten, sodass bewährte Maßnahmen des Risikomanagements nicht mehr greifen.

Für solche ungewissen Situationen, so die Forscherinnen und Forscher, eignet sich das Konzept der Resilienz. Ein resilientes Energiesystem kann Störereignisse unbeschadet abfangen oder zumindest in kurzer Zeit mit möglichst geringem Schaden und mit vertretbaren Kosten wieder in den normalen Betriebszustand zurückkehren. Die Arbeitsgruppe skizziert 15 Handlungsoptionen, die als Bausteine einer Resilienzstrategie gegen große Blackouts dienen können.

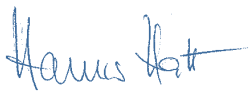
Es zeigt sich deutlich, dass die Verantwortung für eine zuverlässige Stromversorgung zukünftig nicht mehr ausschließlich bei den großen Akteuren der Energieversorgung liegt: auch kleinere Akteure der Energieversorgung, Bürgerinnen und Bürger sowie Akteure außerhalb des Stromsystems, wie etwa Plattformbetreiber, Betreiber öffentlicher Kommunikationsnetze und Gerätehersteller, müssen zur Sicherung der Resilienz beitragen.

Wir danken den Wissenschaftlerinnen und Wissenschaftlern sowie den Gutachterinnen und Gutachtern herzlich für Ihr Engagement.



Prof. (ETHZ) Dr. Gerald Haug
Präsident
Nationale Akademie der Wissenschaften Leopoldina

Prof. Dr. Dieter Spath
Präsident
acatech – Deutsche Akademie der Technikwissenschaften



Prof. Dr. Dr. Hanns Hatt
Präsident
Union der deutschen Akademien der Wissenschaften

Inhalt

Vorwort ... 3

Inhalt ... 5

Abkürzungen ... 6

Glossar ... 7

Zusammenfassung ... 11

1 Energiewende und Digitalisierung: Neuen Blackout-Risiken begegnen ... 17

1.1 Massive Schäden durch lang andauernde Blackouts ... 18
1.2 Wandel in der Energieversorgung ... 19
1.3 Umwälzungen durch Digitalisierung ... 20
1.4 Neue Risiken für Blackouts ... 21
1.5 Resilienz als Ansatz für die Ausfallsicherheit ... 25
1.6 Methodisches Vorgehen der Arbeitsgruppe ... 26

2 Handlungsoptionen ... 27

2.1 Handlungsfeld 1: Wechselwirkung IKT und Energie verstehen und lenken ... 30
2.2 Handlungsfeld 2: Cyber-Sicherheit systemisch entwickeln ... 34
2.3 Handlungsfeld 3: Technische Resilienz durch Netzbetreiber und Netznutzer stärken ... 39
2.4 Handlungsfeld 4: IKT-Integration kleiner Anlagen netzdienlich gestalten ... 42
2.5 Handlungsfeld 5: Anreize für Netzbetreiber zur Steigerung der Resilienz stärken ... 45
2.6 Handlungsfeld 6: Beteiligung von Privatakteuren bei der Gestaltung und Umsetzung von Resilienz sicherstellen ... 49
2.7 Handlungsfeld 7: Langfristige Risiko- und Resilienzbewertung institutionalisieren ... 53

3 Fazit ... 56

Literatur ... 58

Das Akademienprojekt ... 61

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
ENTSO-E	Verband Europäischer Übertragungsnetzbetreiber für elektrische Energie
IKT	Informations- und Kommunikationstechnik (auch: -technologie)
KRITIS	Kritische Infrastruktur
PV	Photovoltaik
StromNEV	Verordnung über die Entgelte für den Zugang zu Elektrizitätsversorgungsnetzen

Glossar

Aggregator	Ein Aggregator handelt und liefert Energie, ohne mit dem Versorger des Kunden verbunden zu sein. Er bündelt Erzeugungsanlagen, flexible Verbraucher und Speichersysteme, um sie zu vermarkten. Damit skaliert er kleine Anlagen auf ein handelbares Volumen.
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 des elektrischen Energiesystems	Die Digitalisierung des elektrischen Energiesystems beschreibt das anhaltendende 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.
Informations- und Kommunikationstechnik (IKT)	Informations- und Kommunikationstechnik (auch: -technologie) umfasst 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 und Kommunikationsnetze, aber auch Software.

1 BSI 2020 1.

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 ziehen in ihre Betrachtungen weitere Grundwerte mit ein.[2] Bedrohungen ergeben sich etwa aus höherer Gewalt, menschlichen oder technischen Fehlern oder vorsätzlichen Handlungen.
Internet der Dinge	Internet der Dinge (englisch Internet of Things) bedeutet, dass physikalische Objekte oder digitale, virtuelle Objekte mit IKT sowie Sensorik und Aktorik ausgestattet und darüber hinaus mit dem Internet verbunden sind.
Kaskadeneffekt	Eine Abfolge von Ereignissen oder Prozessen, die jeweils aufeinander aufbauen.
Last	Summe der Leistung, die einem Netz zu einem bestimmten Zeitpunkt entnommen wird.
Leitsystem	Leitsysteme haben zwei wesentlichen Aufgaben: die Überwachung von Prozessen oder Komponenten und deren Steuerung mittels sogenannter Fernwirktechnik.
Nachgelagertes Netz	Einem Netz nachgelagerte Netze sind Netze niedrigerer Spannungsebenen, die an dieses Netz angeschlossen sind: Ein Netz B ist einem Netz A nachgelagert, wenn es mit Netz A verbunden ist und Netz A selbst Übertragungsnetz ist oder die Stromübertragung vom Übertragungsnetz ins Netz B nur über Netz A erfolgt.
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.
Netzdienlich	Eine Anlage (Erzeugungs-, Verbrauchs- oder Speicheranlage) verhält sich netzdienlich, wenn sie in irgendeiner Form einen Beitrag zur Netzstabilisierung leistet, indem sie ihr Verhalten anpasst.
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.
Patch	Ein Patch ist die Verbesserung bestehender Versionen einer Software, etwa um neue Funktionen zu installieren oder Softwarefehler und Sicherheitslücken zu beheben.

2 BSI 2020 2.

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. In dieser Stellungnahme stehen allerdings nicht die nötigen Investitionen im Vordergrund, sondern vielmehr die lange Zeit, die für eine Umrüstung von Anlagen erforderlich wäre. Denn solange eine zur Beseitigung von Schwachstellen notwendige Umrüstung nicht abgeschlossen ist, wäre das System vulnerabel.
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 (zum Beispiel über Photovoltaik-Dachanlagen).
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 (häufig auch Sektorkopplung genannt) verbindet die Energiesektoren Strom, Wärme und 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).
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 technischen 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. Je nach Leistung der Entnahme oder Einspeisung werden Erzeugungs- beziehungsweise Verbrauchsanlagen an verschiedene Spannungsebenen angeschlossen.
Übertragungsnetz	Übertragungsnetze dienen der Energieübertragung über große Strecken (viele Hundert bis Tausende Kilometer) und dem großflächigen Ausgleich von Verbrauch und Erzeugung. Darüber hinaus ermöglichen sie den Anschluss sehr großer Kraftwerke oder Verbraucherbetriebe. Übertragungsnetze werden mit 220 bis 380 Kilovolt betrieben (Höchstspannung). Für die Übertragung über sehr große Entfernungen und für Seekabel kommt Hochspannungs-Gleichstrom-Übertragung (HGÜ) zum Einsatz.
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.
Verteilnetzbetreiber	Netzbetreiber, der für Verteilnetze verantwortlich ist (siehe Netzbetreiber und Verteilnetz).

Zusammenfassung

Durch die Energiewende und die zunehmende Digitalisierung werden in den nächsten zwei Jahrzehnten neue Risiken für die Stromversorgung entstehen. Um diese Risiken beherrschbar zu machen und Blackouts mitsamt ihren Folgeschäden für die Gesellschaft zuverlässig zu verhindern, ist eine Resilienzstrategie erforderlich. Die Arbeitsgruppe „Resilienz digitalisierter Energiesysteme“ des Akademienprojekts „Energiesysteme der Zukunft“ identifiziert dafür folgende Eckpfeiler:

- Die **Digitalisierung** bietet die Chance, dezentrale Erzeugungsstrukturen, Elektromobilität und neu auftretende Marktakteure effizient und sicher ins Energiesystem zu integrieren. Sie muss daher **aktiv gestaltet** und gefördert werden.

- **Kleine Akteure** der Energieversorgung, **Akteure außerhalb der Stromversorgung** (Gerätehersteller, Plattformbetreiber, Betreiber von öffentlichen Kommunikationsnetzen) und **Haushalte** haben zunehmend Einfluss auf die Sicherheit der Stromversorgung. Sie müssen daher stärker in die Resilienzsicherung einbezogen werden.

- Neue Angriffsflächen für Cyberkriminelle und Abhängigkeiten zwischen Strom- und IKT-System können zu **unvorhergesehenen oder sogar unvorhersehbaren Ereignissen** mit großem Bedrohungspotenzial führen. Die Netzbetreiber müssen mit diesen Risiken umgehen können.

- Die Politik sollte versuchen, zukünftige Entwicklungen rechtzeitig zu antizipieren und die hier geforderte Resilienzstrategie fortlaufend anpassen. Dafür ist ein **konsequentes Monitoring** erforderlich.

Digitalisierung und wachsende Komplexität führen zu neuen Bedrohungen

Eine zuverlässige Stromversorgung ist für eine moderne Industriegesellschaft unverzichtbar. Große Blackouts – **lang anhaltende und flächendeckende Stromausfälle** – würden in kürzester Zeit andere kritische Infrastrukturen wie Transportsysteme, Wasserversorgung und -entsorgung, Gesundheitswesen oder Informations- und Kommunikationssysteme empfindlich stören oder gar zusammenbrechen lassen.

Durch die Energiewende wird das Energiesystem komplexer: Immer mehr elektrische Energie wird wetter-, jahres- und tageszeitabhängig von Windenergie- und Solaranlagen bereitgestellt. Strom wird zunehmend auch für Elektrofahrzeuge und Wärmepumpen benötigt. Privatpersonen erzeugen Strom mit der eigenen Solaranlage, und neue Marktakteure mit neuen Geschäftsmodellen treten neben die klassischen Energieversorger. Großkraftwerke, die bisher für die Stabilisierung der Stromversorgung zuständig waren, gehen außer Betrieb.

Parallel dazu schreitet die **Digitalisierung** rasant voran. Es kommt zu einer starken Vernetzung, einer zunehmenden Automatisierung und dem Einsatz digitaler Technologien – nicht nur im Strombereich. Über das sogenannte **Internet der Dinge** werden viele Milliarden Geräte vernetzt – von Beleuchtung über Kühlschränke bis hin zu Industrieanlagen. Da diese Geräte auch an das Stromnetz angeschlossen sind, können sie in ihrer Summe die Stabilität der Stromversorgung beeinflussen.

Die **zunehmende Verknüpfung zwischen Stromversorgung und IKT** ist notwendiger Bestandteil einer sowohl zuverlässigen als auch ökonomisch effizienten Energieversorgung: **ohne Digitalisierung keine Energiewende**. Andererseits entstehen durch die zunehmende Komplexität in der Stromversorgung **neue Blackout-Risiken:**

1. Werden **viele kleine Erzeugungs- und Verbrauchsanlagen** gewollt oder zufällig gleichzeitig an- oder abgeschaltet, kann dies die Stromversorgung destabilisieren.

2. Die Stromversorgung wird anfälliger für **Fehlverhalten der IKT.** Besonders problematisch ist dabei, dass ein Teil der eingesetzten IKT im Fehlerfall nicht abgeschaltet werden kann, ohne die Stromversorgung empfindlich zu gefährden.

3. Die komplexen Abhängigkeiten zwischen dezentraler Erzeugung, Marktgeschehen und Änderungen im Verbrauch machen das Systemverhalten **schwerer vorhersehbar** und können zu **neuartigen komplexen Störfallabläufen** führen.

4. **Ungewissheit über zukünftige Entwicklungen erschwert ein optimales Systemdesign.** Eine zusätzliche Herausforderung stellt dabei die hohe Innovationsgeschwindigkeit im IKT-Bereich dar, die sich mit jahrzehntelangen Investitionszyklen in der Stromversorgung nur schwer verträgt.

Unvorhergesehene und unvorhersehbare Risiken erfordern eine Resilienzstrategie

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 (wie zum Beispiel Hacker-Angriffe) nicht mehr einfach bestimmbar. Die klassische Risikoanalyse, die auf diesem Prinzip beruht und auf deren Basis das System robust gestaltet wird, ist nicht mehr ausreichend. Zudem müssen sich die für die Systemsicherheit verantwortlichen Netzbetreiber zukünftig auf deutlich mehr Unsicherheit und Überraschungen einstellen. Daher wird es zunehmend wichtig, dass sie auch **auf unvorhergesehene und sogar unvorhersehbare Ereignisse reagieren,** diese beherrschen und auch im Falle eines Blackouts schnell wieder zum Normalbetrieb des Systems zurückkehren. Für solche Situationen hat sich das **Konzept der Resilienz** bewährt. Resilienz bedeutet, die Auswirkungen eines Störereignisses abzufangen – im schlimmsten Fall je nach Konstellation auch mit kurzzeitig abnehmender Versorgungsqualität –, ohne dass das System kollabiert, um anschließend zügig wieder in den normalen Betriebszustand zurückzukehren (siehe Abbildung 1).

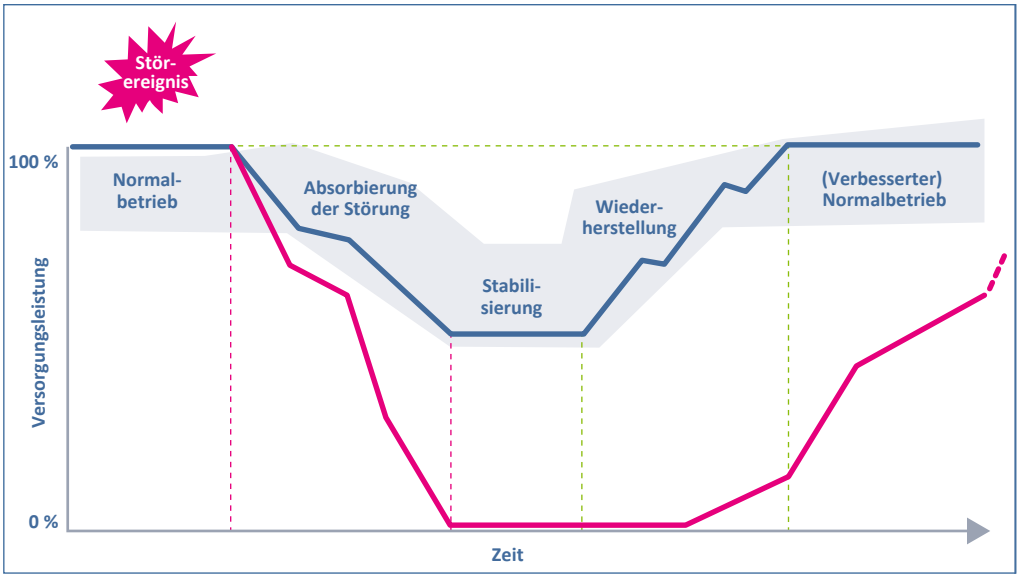


Abbildung 1: Wiederherstellung der Funktionsfähigkeit eines Systems: „die geeignete Reaktion auf ein Ereignis (Absorbieren der Störung), das Zurückfallen auf kritische Funktionen und Stabilisierung des Systems (Stabilisierung) und zuletzt das kontrollierte Zurückbringen zum Normalbetrieb des Systems (Wiederherstellung)."[3]

Eine **Resilienzstrategie** erfordert ein Portfolio an Maßnahmen – von der möglichst weitgehenden Identifikation von Schwachstellen und Risiken über Maßnahmen zur Unterstützung der Robustheit und Widerstands- und Anpassungsfähigkeit bis hin zu lernenden und das System verbessernden Maßnahmen einschließlich einer kosteneffizienten Notfallplanung.

Die Arbeitsgruppe hat **15 Handlungsoptionen** identifiziert (siehe nächste Seite), die als Bausteine einer Resilienzstrategie gegen große Blackouts dienen können. Diese Handlungsoptionen wurden so gewählt, dass sie den bereits **heute gegebenen Handlungsbedarf** adressieren, um die neu entstehenden Risiken **in einem langfristigen Zeithorizont bis 2040** abzufangen. Nur wenn die Resilienzstrategie mit der rasant voranschreitenden Energiewende und der Digitalisierung

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

Schritt hält, können die Potenziale für eine effiziente, sichere und nachhaltige Energieversorgung bestmöglich genutzt und die Blackout-Risiken in einer digitalisierten Welt beherrscht werden.

Wie können Blackout-Risiken begrenzt werden?

Als Bausteine einer umfassenden Resilienzstrategie für das digitalisierte Energiesystem bieten sich die folgenden Maßnahmen an, die in verschiedene Handlungsfelder gegliedert sind:

Handlungsfeld:
Wechselwirkung IKT und Energie verstehen und lenken

Die elektrische Energieversorgung wird zukünftig stärker von IKT-Systemen abhängig sein.
Die Gefahr, dass Störungen der IKT-Systeme zu Blackouts führen, ist zu vermeiden.

- **HO 1. Abhängigkeiten zwischen Stromversorgung und Kommunikationsnetzen analysieren lassen,** um das Risiko kaskadierender Ausfälle zu minimieren.
- **HO 2. Regeln für resiliente Kommunikationsnetze schaffen,** durch Vorgaben zu größerer Redundanz und Schwarzfallfestigkeit.
- **HO 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.

Handlungsfeld:
Cyber-Sicherheit systemisch entwickeln

Die Anforderungen an die Cyber-Sicherheit müssen bei allen Akteuren auf ein ausreichend hohes Niveau gebracht werden. Dies erfordert sowohl technisch als auch organisatorisch
neue Lösungen.

- **HO 4. Cyber-Sicherheitsstandards für alle Blackout-relevanten Akteure einführen,** unter anderem für kleine Netzbetreiber, branchenfremde Akteure und Geräte „hinter dem Zähler".
- **HO 5. Maßnahmen zum Umgang mit Sicherheitslücken definieren,** um Vulnerabilitäten aufgrund menschlichen Versagens im Sicherheitsmanagement, aufgrund von Softwarefehlern oder staatlich gewollten Hintertüren zu begegnen.

Handlungsfeld:
Technische Resilienz durch Netzbetreiber und Netznutzer stärken

Insbesondere in den Verteilnetzen wird die Netzführung zukünftig anspruchsvoller. Sowohl kleine Netzbetreiber als auch Betreiber kleiner Erzeugungsanlagen müssen deutlich mehr als heute üblich zur Resilienz beitragen.

- **HO 6. Digitalisierung der Stromnetze voranbringen,** durch entsprechende technische Ausstattung auch kleiner Netzbetreiber.
- **HO 7. Regelwerk für Resilienz durch dezentrale Strukturen erarbeiten lassen.** Sind einzelne Netzabschnitte inselbetriebsfähig, können sie im Falle eines Blackouts temporär die lokale Versorgung aufrechterhalten und beim Wiederaufbau der Versorgung helfen.

Handlungsfeld:
IKT-Integration kleiner Anlagen netzdienlich gestalten

Der Großteil der Anlagen und Kleingeräte wird zukünftig mit dem Internet verbunden sein und sich darüber digital steuern lassen. Unerwünschtes simultanes Verhalten – etwa hohe Leistungsspitzen durch Gleichzeitigkeiten – kann die Stabilität des elektrischen Energiesystems gefährden und muss vermieden werden. Auf der anderen Seite können diese Anlagen auch genutzt werden, um das Energiesystem aktiv zu stabilisieren.

- **HO 8. Standardisierung zur Vermeidung problematischen simultanen Verhaltens initiieren,** zum Beispiel durch Mindeststandards zur „Patchability" von Erzeugungsanlagen und Geräten. So kann die Software von Geräten im laufenden Betrieb an neue Anforderungen angepasst werden.
- **HO 9. Systemstabilisierung durch dezentrale Anlagen ausbauen** und die dafür erforderliche kommunikationstechnische Anbindung voranbringen.

Handlungsfeld:
Anreize für Netzbetreiber zur Steigerung der Resilienz stärken

Es fehlen weitgehend effektive und effiziente Anreize für die Netzbetreiber und Marktparteien, sich resilienzverbessernd zu verhalten. Dazu sollten marktliche Anreize geschaffen werden.

- **HO 10. Eine Resilienzkomponente in die Anreizregulierung integrieren,** damit Netzbetreiber in Resilienzmaßnahmen investieren.
- **HO 11. Resilienzverbessernde Netzentgelte und Anschlussgebühren einführen,** um die Standortwahl und die Betriebsweise für Erneuerbare-Energie-Anlagen zu beeinflussen.

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

Zur Systemstützung kann auch die Steuerung von Anlagen aufseiten privater Akteure notwendig werden. Zur Ausgestaltung sollte ein Stakeholder-Gremium geschaffen werden, das Lösungen entwickelt, die für verschiedene Nutzergruppen wählbar sind und Fragen der Akzeptabilität berücksichtigen.

- **HO 12. Ein Stakeholder-Gremium zur Berücksichtigung der Belange von Privatakteuren entwickeln** und alle relevanten Akteure in die Entscheidungsfindung für neue Regelungen einbeziehen.
- **HO 13. Bewusstsein für den Einfluss privater Akteure schaffen,** durch Informations- und Bildungskampagnen.

Handlungsfeld:
Langfristige Risiko- und Resilienzbewertung institutionalisieren

Es wird zukünftig unvorhersehbare Trends geben, die etwa aus der Digitalisierung und der Energiewende entstehen und die Gefahr von Blackouts erhöhen könnten. Es sollte ein geeigneter Organisationsrahmen geschaffen werden, der es ermöglicht, flexibel auf solche Trends
zu reagieren und mit ihnen umzugehen.

- **HO 14. Organisationsrahmen für die Meldung von Störfällen und die Resilienzbewertung schaffen** und geeignete Kenngrößen für Resilienz entwickeln.
- **HO 15. Einen übergeordneten Begleitprozess ins Leben rufen,** um die Resilienzstrategie regelmäßig zu evaluieren.

Tabelle 1: Übersicht über Handlungsfelder und Handlungsoptionen (HO)

Nur wenn zukünftig alle relevanten Akteure ihren Teil zur Resilienz beitragen, wird es gelingen, die gewohnt hohe Zuverlässigkeit der Stromversorgung aufrechtzuerhalten. Durch eine geeignete Resilienzstrategie kann die Politik hierfür den Rahmen setzen.

1 Energiewende und Digitalisierung: Neuen Blackout-Risiken begegnen

Das elektrische Energiesystem gehört zu den kritischen Infrastrukturen (KRITIS), von denen das Wohlergehen einer modernen Industriegesellschaft abhängt. Andere KRITIS sind etwa Wasserversorgung und -entsorgung, Transport, Gesundheitswesen oder Informations- und Kommunikationssysteme. Die **Stromversorgung nimmt unter den KRITIS eine Sonderrolle ein:** Alle anderen KRITIS sind nach kürzester Zeit empfindlich gestört, wenn die Stromversorgung unterbrochen ist.

Die europäische Stromversorgung ist im internationalen Vergleich sehr zuverlässig und robust gegenüber Störungen. Der **Wandel in der Energieversorgung** könnte aber dazu führen, dass diese gewohnt hohe Versorgungssicherheit gefährdet wird. Zum einen steigt der Anteil erneuerbarer Energien, die zum Teil von Wetter, Jahres- und Tageszeit abhängen, an der Stromerzeugung. Zum anderen steigt der Stromverbrauch und Verbrauchsmuster ändern sich, zum Beispiel durch Elektromobilität und eine weitere Umstellung auf den Energieträger Strom im Zuge der Dekarbonisierung. Nicht zuletzt verändert die **Digitalisierung** die Energieversorgung. Diese Systemtransition führt nicht nur dazu, dass die Mechanismen zur Systemstabilisierung, die den Netzbetreibern heute zur Verfügung stehen, im Verlauf der nächsten zwei Jahrzehnte zum Teil wegfallen. Sie bedingt auch **neue Arten von Störungen**, die derzeit noch keine große Rolle spielen oder sogar noch gänzlich unbekannt sind.[4] Auch Ereignisse ohne unmittelbaren Bezug zur Stromversorgung können Einfluss auf den sicheren Betrieb des elektrischen Energieversorgungssystems haben. Eine Pandemie könnte dazu führen, dass wesentliches Betriebs- und Wartungspersonal durch Krankheit ausfällt oder aufgrund von Erkrankungen in der Familie nicht zur Arbeit kommen wird. Dies war zum Glück während der Covid-19-Pandemie im Jahr 2020 noch nicht der Fall. Digitalisierung kann helfen, viele der so für die Stromversorgung entstehenden Schwierigkeiten deutlich abzumildern.

Diese Stellungnahme schlägt **Handlungsoptionen für die Politik** vor, um den mittelfristig entstehenden neuen Gefährdungen, die aus dem Zusammenwirken der Energiewende und der zunehmenden Digitalisierung resultieren, bereits heute zu begegnen. Eine besondere Herausforderung ist dabei der ständige Wandel, dem das elektrische Energiesystem selbst unterliegt – ein Ansatz „auf grüner Wiese“ ist nicht möglich. Im Fokus steht dabei, **große Stromausfälle zu verhindern** oder zumindest so gut wie möglich abzumildern. Im folgenden Text wird durchgängig die übliche Bezeichnung „Blackout“ für große, lang andauernde Stromausfälle in einer Region verwendet.

Das Restrisiko eines mehrtägigen überregionalen Blackouts bleibt trotz aller Vorkehrungen immer bestehen. Die Politik muss dafür sorgen, dass auch in diesem

4 Kröger 2017, S. 39–55.

Fall die allgemeine Katastrophenvorsorge greift. Dies liegt jedoch außerhalb des Untersuchungsrahmens dieser Stellungnahme.

Alle hier beschriebenen Ergebnisse, methodischen Vorgehensweisen und Handlungsoptionen werden ausführlich in der zugehörigen Analyse[5] abgeleitet und detailliert beschrieben.

1.1 Massive Schäden durch lang andauernde Blackouts

Eine anschauliche Darstellung der Folgen lang andauernder Blackouts liefert eine Analyse des Büros zur Technikfolgen-Abschätzung beim Deutschen Bundestag aus dem Jahr 2011.[6] Bereits direkt nach dem Stromausfall können ernsthafte Folgen auftreten, so zum Beispiel Verkehrsunglücke wegen fehlender Ampeln. Besonders gravierende Folgen ergeben sich im Gesundheitsbereich: Die unfallbedingten erhöhten Todes- und Verletztenzahlen werden durch eingeschränkte Rettungs- und Transportmöglichkeiten noch gesteigert. Festnetztelefonate sind nicht mehr möglich. Nach einigen Stunden ist auch die Mobiltelefonie stark eingeschränkt. Dadurch können in Notfällen keine Rettungsdienste oder die Polizei gerufen werden. Die Bevölkerung kann nicht ausreichend informiert werden. Nach einigen Tagen sterben Tiere in der Landwirtschaft. Menschen in Krankenhäusern geraten in kritische Zustände, wenn sie die Verschlechterung der Behandlungsbedingungen nicht verkraften. Die Lebensmittelversorgung ist gestört. Es kann zu Unruhen und zur Gefährdung der öffentlichen Ordnung kommen. Einbrüche, Vandalismus und weitere kriminelle Delikte nehmen dramatisch zu – die Polizei kann kaum noch eingreifen, da sie einerseits die Menge an Vorfällen nicht bearbeiten und andererseits oft gar nicht erst gerufen werden kann. Selbst wenn nach einigen Tagen die Stromversorgung wiederhergestellt würde, blieben viele Folgen lange oder dauerhaft bestehen. Das Vertrauen der Gesellschaft wäre nachhaltig gestört, sowohl in die Energieversorger, als auch den Staat und sich selbst als soziale Gemeinschaft.

Die ökonomischen Kosten eines lang anhaltenden Ausfalls wären enorm. Zwar gibt es für solch einen Fall keine genauen quantitativen Abschätzungen, Anhaltspunkte liefern aber die geschätzten Kosten eines einstündigen Stromausfalls um die Mittagszeit an einem Wochentag im Winter, die im Jahr 2010 für Deutschland mit 600 Millionen Euro beziffert wurden.[7] Für einen längeren Ausfall werden die Kosten pro Stunde voraussichtlich signifikant höher liegen.

Diese Stellungnahme konzentriert sich daher auf **große Stromausfälle (Blackouts)**, die im Zusammenhang mit dem Wandel des gesamten Energiesystems **in den nächsten zwei Dekaden** auftreten könnten. Der Zeithorizont bis 2040 wurde gewählt, um langfristige Entwicklungen miteinzubeziehen. Ein längerer Horizont als zwei Dekaden schien nicht geeignet, da die Entwicklung der Digitalisierung dafür zu unvorhersehbar ist. Ein Stromausfall wird als „groß“ verstanden, wenn ein Gebiet mit mindestens 500.000 Kunden betroffen ist und der Ausfall mehrere Stunden dauert.[8]

5 Mayer/Brunekreeft 2021.

6 Petermann et al. 2011.

7 Piasceck et al. 2013.

8 Angelehnt an Büchner et al. 2014, BSI-KritisV 2017, S. 7.

1.2 Wandel in der Energieversorgung

Im Zuge der Energiewende steigt der Anteil erneuerbarer Energien (Wind, Sonne, Wasserkraft und Biomasse) an der Stromerzeugung in Deutschland – im Jahr 2019 betrug er bereits über 46 Prozent der nationalen Nettostromerzeugung. Auch die Europäische Union hat 2019 mit dem „Green Deal“[9] das Ziel bekräftigt, die Energieerzeugung bis 2050 überwiegend auf erneuerbare Energien umzustellen – in einem voll integrierten und digital verbundenen europäischen Energiemarkt. Folgende Trends der Energieversorgung bedingen zukünftig eine Neubewertung der Risikosituation von Blackouts:

- **Diversität der Erzeugungsstruktur:** Ein großer Teil der elektrischen Energie stammt in Deutschland zukünftig aus kleinen Erneuerbare-Energie-Anlagen, während konventionelle Kraftwerke immer weniger elektrische Energie einspeisen. Die Stromerzeugung erfolgt dadurch nicht mehr nur verbrauchsgetrieben, sondern wetter-, jahres- und tageszeitabhängig.
- **Geografische Diversität:** Wasserkraft, Biomasse, Wind- und Solarkraft sind regional in Europa unterschiedlich verteilt. Die Stromerzeugung findet zunehmend nicht mehr in der Nähe großer industrieller Zentren mit hohem Verbrauch statt, sondern an guten Windenergie- und Solarstandorten – beispielsweise in den dünn besiedelten Regionen Nord- und Nordostdeutschlands. Dadurch muss der Strom über weitere Strecken transportiert werden.
- **Steigender Verbrauch und veränderte Verbrauchsmuster:** In Zukunft wird Strom auch verstärkt in den Sektoren Wärme und Verkehr eingesetzt werden. Die gesamte Energieversorgung wird dadurch noch stärker von elektrischer Energie abhängig. Durch die Zunahme von Elektrofahrzeugen, Wärmepumpen und anderen steuerbaren, flexiblen Verbrauchsanlagen in Haushalten und Industrie sowie von stationären Speichern ändern sich zudem die Verbrauchsmuster. Auch die IKT-Systeme tragen einen nicht unwesentlichen Anteil am Energiebedarf.
- **Steigende Belastung der Stromnetze:** Die Verteilnetzbetreiber müssen bereits heute aufgrund der zunehmenden Einspeisung von Wind- und Solarenergie immer häufiger in die Netze eingreifen, um durch Erzeugungsspitzen verursachte Netzengpässe zu vermeiden – ein Trend, der voraussichtlich massiv zunehmen wird. Auch die Übertragungsnetze werden häufiger nah an ihrer Belastungsgrenze betrieben.
- **Veränderte Rolle von Privatakteuren:** Auf lokaler Ebene können Erzeugung, Speicherung und Verbrauch zusammenfallen, wenn Privatakteure als sogenannte Prosumer nicht nur Strom verbrauchen, sondern diesen auch selbst produzieren, ins Netz einspeisen und gegebenenfalls speichern.
- **Volatilere Energiemärkte:** Energiemärkte ändern sich in Richtung kleinerer handelbarer Energiemengen, kürzerer Lieferzeiträume, jedoch geografisch größerer Ausdehnung der Märkte. Es entsteht zunehmend ein Bedarf an Preissignalen, die sich für verschiedene Gebiete unterscheiden.
- **Neue Geschäftsmodelle:** Es entstehen neue Geschäftsmodelle, einige bereits heute in den Bereichen Vermarktung erneuerbarer Energien oder auch Smart Home zur Vernetzung von Geräten innerhalb eines Haushalts.

9 Europäische Kommission 2019.

1.3 Umwälzungen durch Digitalisierung

Digitalisierung prägt fast alle Bereiche in Wirtschaft und Gesellschaft und so auch die Energieversorgung. Anwendungen und Prozesse werden vernetzt und automatisiert, Objekte der physikalischen Welt werden mit dem Internet verbunden, soziale Netzwerke verändern das Zusammenleben, künstliche Intelligenz unterstützt Entscheidungen oder trifft sie gleich selbst. Viele Entwicklungen der Digitalisierung sind wegen der hohen Innovationsgeschwindigkeit, der schnellen Marktdurchdringung und des disruptiven Charakters **unvorhersehbar**.

In allen Bereichen der Energieversorgung kommt es zu einer **steigenden Vernetzung durch Informations- und Kommunikationstechnologien (IKT)**. Der Rollout der Smart-Meter-Infrastruktur stellt als sichere Infrastruktur für die Ansteuerung von dezentralen Anlagen ein großes Potenzial für die Digitalisierung der Energieversorgung dar. Die Umsetzung ist derzeit in intensiver Diskussion in den Standardisierungsgremien und dem BSI. Digitalisierung und IKT umfassen jedoch weitaus mehr: alle Technologien, Anwendungen und Prozesse, die für die elektronische Erfassung und Verarbeitung von Informationen und deren Kommunikation eingesetzt werden. Dazu zählen Hardware wie Server und Kommunikationsnetze, aber auch Software. Daten sind vermehrt verfügbar, und die Möglichkeiten, diese zu verarbeiten, oft in Echtzeit, werden stetig verbessert. Besonders die Verteilnetze müssen weitreichender automatisiert werden, um die wachsende Menge an variabler Erzeugung aus Erneuerbare-Energie-Anlagen effizient zu integrieren.

IT/OT-Konvergenz schafft Mehrwert: Früher waren die IKT-Systeme für die Abwicklung von geschäftlichen und administrativen Prozessen und Transaktionen („Information Technology“, IT) physikalisch strikt getrennt von den IKT-Systemen, die direkt Produktionsprozesse steuerten („Operational Technology“, OT). Heute nimmt die Interaktion zwischen diesen beiden Bereichen immer mehr zu. Beispielsweise werden Daten aus der OT genutzt, um zu entscheiden, wann eine Wartung erforderlich ist. Umgekehrt haben auch OT-Systeme Schnittstellen zu anderen Systemen, etwa um bei Schalthandlungen die Auswirkungen auf die Lebensdauer von Betriebsmitteln (also elektrische Bauteile wie Stromleitungen, Transformatoren und Schaltanlagen) zu berücksichtigen und so die ökonomische Effizienz zu erhöhen.

Durch die Digitalisierung werden **neue Akteure** in der Energieversorgung auftreten, die zum Beispiel digital basierte Produkte oder Plattformen für die Energieversorgung anbieten. Beispiele sind Plattformen für Smart-Home-Anwendungen oder Marktplattformen für den Energiehandel. Perspektivisch werden mehr oder weniger alle Konsumgeräte (von Beleuchtung über Fernseher bis hin zu Kühlschränken) mit dem Internet verbunden sein – das sogenannte Internet der Dinge. Branchenfremde Anbieter vertreiben Systeme, wie etwa Smart-Home-Lösungen, die automatisiert Geräte steuern können. Um die Wirkungen der Digitalisierung abzuschätzen, reicht es daher nicht aus, nur technische und betriebliche Prozesse zu betrachten; auch eine veränderte gesellschaftliche und ökonomische Dynamik muss berücksichtigt werden.

Der Betrieb des elektrischen Energiesystems erfordert den immer intensiveren Einsatz von IKT, um die neuen Komplexitäten effizient zu beherrschen. Daraus entstehen einerseits **neue Vulnerabilitäten** durch Lücken in der Cyber-Sicherheit, fehlerhafte Software oder deren fehlerhafte Nutzung. Zudem wird in einem verteilten

digitalisierten Energiesystem der Versorgungswiederaufbau komplexer werden. Andererseits ermöglicht Digitalisierung eine **viel schnellere Reaktion auf nicht erwartete Entwicklungen**. Denn Software kann in der Regel viel schneller angepasst werden, als physikalische Komponenten entwickelt und ausgetauscht werden können. **Die (unvermeidbare) Digitalisierung birgt sowohl große Chancen als auch Gefahren für die Sicherheit der Energieversorgung.**

Die Entwicklungen aus der Energiewende und der Digitalisierung führen also dazu, dass sich die verantwortlichen Akteure in eine Welt mit **deutlich mehr Unsicherheit und unerwarteten Ereignissen** hineinbegeben. Eine viel größere Anzahl an kleinen Störungen ist zu erwarten, die sich nicht zu großen Stromausfällen entwickeln dürfen und zügig behoben oder abgefangen werden müssen.

1.4 Neue Risiken für Blackouts

Die ESYS-Arbeitsgruppe untersuchte anhand möglicher Zukunftsszenarien für das Jahr 2040, wie sich Risikofaktoren für Blackouts entwickeln und welche neuen Risikofaktoren durch Veränderungen im System in den nächsten zwei Jahrzehnten entstehen könnten. Vier **Basisursachen für neue Risikofaktoren** wurden identifiziert. Die Basisursachen selbst sind durch politische Entscheidungen kaum abzuschwächen.

Basisursache 1: Die Vielzahl an **kleinen, aktiv steuerbaren Erzeugungs- und Verbrauchsanlagen** ist durch die Möglichkeit von simultanem Verhalten, das durch Digitalisierung induziert wird, 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. Wird eine große Anzahl kleiner Verbrauchsanlagen (beispielsweise Wärmepumpen, ladende Elektrofahrzeuge oder elektrische Hausspeicher) über das Internet gleichzeitig an- oder abgeschaltet, können dadurch Effekte auftreten, die zu destabilisierenden Frequenzschwankungen führen können. Ursachen für problematisches simultanes Verhalten können automatisierte Märkte sein, an denen die betroffenen Anlagen teilnehmen. Auch Schaltbefehle anderer Plattformen, die etwa vom Hersteller der Anlagen oder von unabhängigen, branchenfremden Akteuren betrieben werden, können zu unerwünschtem simultanem Verhalten führen. Nicht zuletzt können auch gezielte böswillige Manipulationen die Ursache des Problems sein. Bei kleinen, dezentralen Erzeugungsanlagen können vor allem fehlende Anreize für netzdienliches Verhalten zu Problemen führen. Eine weitere Schwierigkeit ist ein Mangel an Akzeptanz: Teilweise sind Privatpersonen skeptisch gegenüber technischen Lösungen, die in ihre Entscheidungshoheit eingreifen. Dies kann dem Einsatz möglicher stabilisierender Lösungen im Wege stehen. Zudem führen neue kommunale oder genossenschaftliche Strukturen zu veränderten Interessenverhältnissen.

Basisursache 2: Fehler der IKT können zu massiven Bedrohungen führen. Die bisherigen Maßnahmen zur Absicherung gegen digitale Störereignisse wie Softwarefehler oder Cyber-Angriffe reichen in einer zukünftig stark digitalisierten Welt bei Weitem nicht aus. Bisher zählen nur relativ große Anlagen und Infrastrukturen als kritische Infrastrukturen (siehe Infobox „kritische Infrastruktur elektrische Energieversorgung“), und dementsprechend müssen deren IKT-Systeme gegen digitale Störereignisse abgesichert sein. In Zukunft geht jedoch eine Gefahr von IKT-Systemen aus, die

bisher überhaupt nicht als Bestandteile des Energiesystems gesehen wurden. Vor allem die unter Basisursache 1 beschriebenen kleinen, kommunikativ angebundenen Geräte in Verbindung mit der Plattformökonomie stellen einen zentralen und weitreichenden Angriffspunkt dar: Gelingt es einem Angreifer, eine Plattform zu korrumpieren, kann er die angeschlossenen Geräte unter seine Kontrolle bringen. Weitere Entwicklungen im IKT-Bereich verstärken diese Risiken. Erstens können die kurzen Innovationszyklen und der Druck zur schnellen Markteinführung eines Softwareprodukts zu Kompromissen bei Sicherheitsstandards und Softwarequalität verleiten. Zweitens führt die Tendenz zur Bildung von Oligopolen und Monopolen bei den Geräteherstellern dazu, dass dieselben Sicherheitslücken potenziell eine sehr große Anzahl von Geräten betreffen, die in ihrer Summe dann systemkritisch sind. Drittens hat sich eine „Wachstumsbranche" für hochprofessionalisierte Produkte und Dienstleistungen für Cyber-Angriffe sowie für das Aufspüren von Sicherheitslücken herausgebildet. Zunehmend sind auch staatliche Akteure in Deutschland und anderswo daran beteiligt, indem sie Sicherheitslücken in Software verlangen und Werkzeuge für eigene Cyber-Angriffe erstellen lassen (beispielsweise „Staatstrojaner"). Erschwerend kommt hinzu: Fehlerhafte oder böswillig manipulierte IKT-Systeme können nicht einfach abgeschaltet werden, denn ohne sie ist die Kontrolle des Stromnetzes nicht möglich und es würde zum Blackout kommen. Das heißt, das System muss auch im fehlerhaften Zustand betrieben werden, ohne dass weitere Fehler oder Schäden entstehen. Dies ist jedoch in einem hoch verteilten System, in dem viele verschiedene Akteure verantwortlich sind und neue Arten von Fehlern auftreten können, sehr schwierig. Zusätzlich werden viele Akteure nicht das notwendige Wissen aufbauen können, um mit derartigen Sicherheitsvorfällen umzugehen.

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.[10] 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, Anlagen oder Systeme 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
- **Messstelle**, deren angeschlossene Verbrauchsstelle beziehungsweise Einspeisung eine Leistung von mehr als 420 Megawatt aufweist.

10 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[11]	Anzahl Anlagen, die 420 Megawatt entsprechen	Dies entspricht in etwa:[12]
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[13]			
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 2: Wie viele dezentrale Anlagen entsprechen zusammengerechnet der Größenordnung einer kritischen Infrastruktur?

Die Beispiele in der Tabelle 2 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).

11 Eigene Berechnung aus Netztransparenz 2019; BDEW 2017.

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

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

Basisursache 3: Die technische Systemkomplexität erschwert die Vorhersage von Auswirkungen im operativen Betrieb. Die tages-, wetter- und jahreszeitabhängige Stromerzeugung aus Photovoltaik(PV)- und Windenergieanlagen erfordert schnelle – häufig sofortige – Reaktionen. Gleichzeitig ergeben sich durch die zunehmende Anzahl dezentraler Stromerzeugungsanlagen und Speicher komplexere Abhängigkeiten der verschiedenen Systemkomponenten voneinander. Diese können zu unvorhergesehenen, sich gegenseitig verstärkenden Effekten führen. Auch der Einsatz von künstlicher Intelligenz zur autonomen Steuerung dezentraler Anlagen kann aufgrund emergenten Verhaltens die Vorhersage des Systemverhaltens erschweren. Nicht zuletzt können auch die zukünftigen Strommärkte eine schwer vorhersagbare Systemdynamik verursachen – etwa durch variable Tarife, bei denen der Preis für elektrische Energie zeitabhängig variiert werden kann, oder neue Marktformen wie Peer-to-Peer-Märkte, die ohne zentrale Instanz auskommen und über die der Handel zwischen zwei Parteien direkt abgewickelt wird.

Die zunehmende **gegenseitige Abhängigkeit zwischen Strom- und IKT-System** kann zudem Störfallabläufe komplexer gestalten. Einerseits wird die Stromversorgung der Zukunft noch viel stärker als heute vom Funktionieren verschiedener IKT-Komponenten sowohl innerhalb des Energiesystems (etwa Leitsysteme der Netzbetreiber) als auch außerhalb des Energiesystems (etwa Plattformen oder Smart-Home-Systeme) abhängig sein. Andererseits ist IKT empfindlich von der Stromversorgung abhängig. So kann ein Ausfall eines IKT-Systems zum Ausfall von Teilen der Stromversorgung führen und umgekehrt – im schlimmsten Fall können dadurch kaskadenartig immer mehr Teilsysteme ausfallen. Das heißt, dass sich selbst Ausfälle von kleinen Teilsystemen zu einem großen Blackout hochschaukeln können. Im Falle eines Blackouts können es diese Wechselwirkungen samt möglicher Rückkopplungen außerdem erschweren, ein Lagebild zu erstellen und das System wieder anzufahren.

Basisursache 4: Ungewissheit über zukünftige Entwicklungen erschwert ein optimales Systemdesign. Das Systemdesign des elektrischen Energiesystems – unter anderem technischer Aufbau und Prozesse, Richtlinien, Regulierung – basiert auf expliziten und impliziten Annahmen über die Zukunft. Aufgrund der oben genannten Ungewissheiten werden sich jedoch wahrscheinlich einige dieser Annahmen als falsch herausstellen. Dies ist umso problematischer, als implementierte Technologien und die aufgebauten Infrastrukturen eine Pfadabhängigkeit schaffen, die eine spätere Anpassung an neue, unerwartete Entwicklungen erschwert – etwa durch langwierige Umrüstungsprozesse. Eine zusätzliche Herausforderung ergibt sich dabei aus den verschiedenen Entwicklungsgeschwindigkeiten von energietechnischer Infrastruktur und IKT. So werden elektrotechnische Komponenten über Jahrzehnte eingesetzt, während manche Software mehrfach pro Jahr aktualisiert wird und Innovationszyklen in der IKT-Branche nur wenige Jahre dauern.

Risiken im regulatorischen Bereich können sich unter anderem durch nicht ausreichend definierte Verantwortlichkeiten zwischen verschiedenen Akteuren ergeben, aber auch durch fehlende Abstimmung zwischen verschiedenen Staaten. Auch die schwer absehbare Entwicklung gesellschaftlicher Einstellungen ist ein Unsicherheitsfaktor.

1.5 Resilienz als Ansatz für die Ausfallsicherheit

Warum reichen also die bisherigen Prinzipien zur Verhinderung von Blackouts nicht mehr aus?

Das klassische Risikomanagement legt den Fokus auf die Identifizierung und Beseitigung von Schwachstellen in der Systemauslegung und stützt sich dabei stark auf Erfahrungswissen und Lernen aus der Vergangenheit. Um Risiken zu messen und zu bewerten, werden die Wahrscheinlichkeit des Eintritts der Störereignisse und der Schaden durch diese Störereignisse abgeschätzt. Mit diesem Wissen werden dann Schwachstellen beseitigt, also die **Vulnerabilität** des Systems verringert, und das System damit robust gestaltet. **Robustheit** (als Gegensatz zu Vulnerabilität) bedeutet, dass einem Störereignis ohne Einbußen bei der Qualität der Leistungserbringung begegnet wird. Primär auslösende Störereignisse, die zu Blackouts führten, waren bisher meist der Ausfall einer großen Komponente – etwa eines Großkraftwerks oder einer Leitung im Übertragungsnetz infolge eines Kurzschlusses –, gefolgt von weiteren Fehlern. Durch geeignete Systemauslegung, insbesondere Redundanz[14] bei großen Betriebsmitteln, gelang es in Deutschland, die Wahrscheinlichkeit für einen Blackout extrem gering zu halten.

Aus den beschriebenen Basisursachen ergibt sich jedoch, dass für wesentliche zukünftige Risikofaktoren das Wissen und die Erfahrung für eine risikobasierte Abschätzung fehlen.[15] Die **erhöhte Komplexität der Stromversorgung** (Basisursachen 2, 3) macht eine vollständige Analyse aller möglichen Störereignisse unmöglich. Die **Unsicherheit** (Basisursache 4), wie sich die elektrische Energieversorgung in Zukunft entwickeln wird, führt dazu, dass nicht alle möglichen Entwicklungen in die Risikovorsorge einbezogen werden. Zudem ziehen die Akteure aus dem vorhandenen und allgemein geteilten Wissen über die zukünftige Stromversorgung unterschiedliche Schlüsse (**soziopolitische Ambiguität**) und bewerten daher etwa aufgrund verschiedener Werteeinstellungen die Akzeptanz von Risiken und deren Vermeidungsmaßnahmen unterschiedlich.

Für den Umgang mit Unsicherheiten in komplexen soziotechnischen Systemen hat sich das Konzept der **Resilienz** bewährt. Es zielt wesentlich auf die Zeit nach dem Störereignis ab („soft landing“)[16] und kann so besser mit unvorhergesehenen Störereignissen umgehen. Eine **resiliente Stromversorgung** besitzt die Fähigkeit, Störereignisse unbeschadet abzufangen oder, im Falle von Teilausfällen, zumindest in kurzer Zeit mit möglichst geringem Schaden und vertretbaren Kosten wieder in den normalen Betriebszustand zurückzukehren.[17] Ein resilientes System kann insbesondere mit neuen Gegebenheiten umgehen, die sich aus dem Systemwandel aufgrund von Energiewende und Digitalisierung ergeben. Maßnahmen, die das System physikalisch härten, um es robust und damit resilient zu machen, liegen nicht im Fokus dieser Stellungnahme. Auch Schalthandlungen, die automatisch auf physikalische Größen wie Spannung oder Frequenz reagieren, um Abweichungen vom Normalbetrieb abzufangen, werden nicht diskutiert.

14 Redundanz bedeutet, dass zusätzliche, im Normalbetrieb nicht benötigte Betriebsmittel vorgehalten werden, die die gleiche Funktion erfüllen. Bei Ausfall eines Betriebsmittels kann dessen Funktion dann durch diese übernommen werden.

15 Nach Aven/Renn 2009.

16 Vgl. Kröger 2019, S. 291 und Thoma 2014, S. 14.

17 Nach acatech/Leopoldina/Akademienunion 2017, S. 10.

Abbildung 1 illustriert das Konzept der Resilienz und zeigt die Vorteile eines resilienten Systems gegenüber einem nicht resilienten System: Das Störereignis kann absorbiert werden, sodass die Versorgungsleistung zum Teil erhalten bleiben kann und der Wiederaufbau deutlich schneller erfolgt.

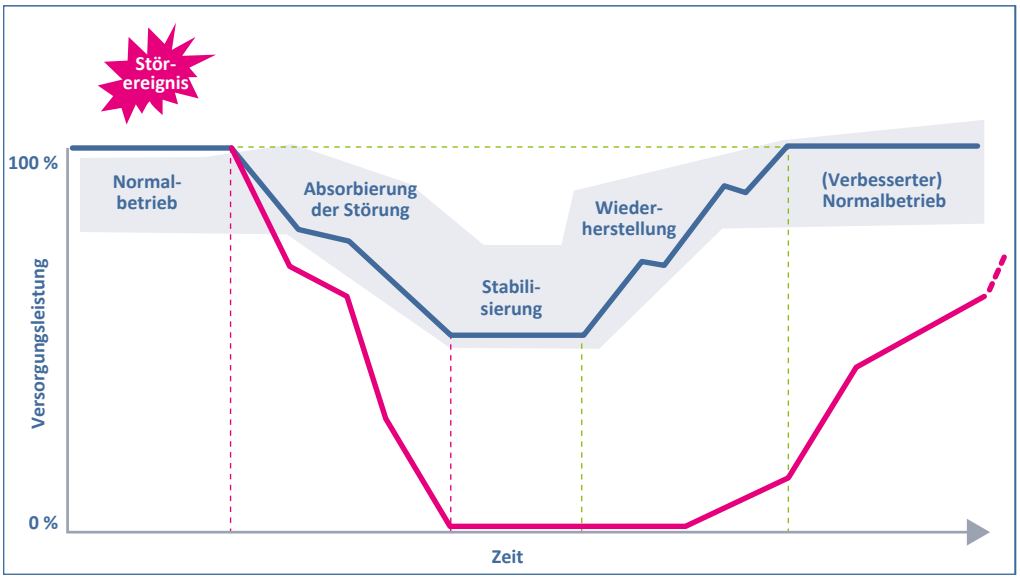


Abbildung 1: Wiederherstellung der Funktionsfähigkeit eines Systems: „die geeignete Reaktion auf ein Ereignis (Absorbieren der Störung), das Zurückfallen auf kritische Funktionen und Stabilisierung des Systems (Stabilisierung) und zuletzt das kontrollierte Zurückbringen zum Normalbetrieb des Systems (Wiederherstellung)“[18]

1.6 Methodisches Vorgehen der Arbeitsgruppe

Angelehnt an die Methodik der Risiko-Governance[19] wurde zunächst in mehreren interdisziplinären Workshops und unterstützt durch wissenschaftliche Recherchen eine umfassende Umfeldanalyse einer zukünftigen Stromversorgung mit besonderer Berücksichtigung der Digitalisierung durchgeführt. Schwerpunkt waren Entwicklungen der nächsten zwanzig Jahre mit Relevanz für Blackouts. Um mögliche zukünftige Entwicklungen abzuschätzen, wurde im zweiten Schritt eine Szenario-Analyse durchgeführt: In vier Szenarien wurden mögliche Energiezukünfte für das Jahr 2040 beschrieben. Für jedes Szenario wurde analysiert, welche neuen Bedrohungen sich entwickeln, die zu Blackouts führen können. Es zeigt sich, dass sich die Ursachen für diese Bedrohungen auf die vier oben genannten Basisursachen zurückführen lassen.

Im nächsten Schritt wurden Möglichkeiten ermittelt, wie den neuen Bedrohungen begegnet werden kann. Zur Umsetzung dieser Möglichkeiten wurden Handlungsoptionen für die Politik beschrieben, Akteuren zugeordnet und interdisziplinär bewertet. Der Fokus liegt dabei auf dem heutigen Handlungsbedarf. Denn zum einen brauchen einige Maßnahmen mehrere Jahre in der Umsetzung (beispielsweise, wenn Forschung und Entwicklung erforderlich sind). Zum anderen muss aufgrund von langlebigen Investitionen im Energiesystem die Weiterentwicklung des Energiesystems vorausschauend geplant werden.

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

19 IRGC 2018.

2 Handlungsoptionen

Um den Risiken wirksam zu begegnen, die sich aus den Veränderungen der Stromversorgung ergeben, und unsere Versorgungssicherheit auch zukünftig sicherzustellen, sind neue Denkansätze erforderlich.

Die ESYS-Arbeitsgruppe hat dazu sieben problemorientierte **Handlungsfelder** identifiziert und hierfür jeweils politische Handlungsoptionen erarbeitet. Diese können, wenn sie zeitnah umgesetzt werden, mittel- und langfristig bis 2040 zur Lösung des jeweils adressierten Problems beitragen. Es wird aufgezeigt, wie die Politik die verantwortlichen Akteure zur Umsetzung dieser Maßnahmen bewegen und darin unterstützen kann. Die Maßnahmen zielen darauf, die Voraussetzungen für Resilienz zu verbessern und so große Blackouts zu vermeiden beziehungsweise die Versorgung nach einem Blackout möglichst schnell wiederherzustellen und somit auch die sozialen, ökonomischen und ökologischen Auswirkungen zu minimieren.

Die Kurzübersicht der Handlungsfelder und Handlungsoptionen stellt zunächst die Probleme dar, die sich aus den Basisursachen (siehe Kapitel 1.4) ergeben und die in dem jeweiligen Handlungsfeld angegangen werden, und zeigt auf, welche Handlungsoptionen konkret dazu vorgeschlagen werden:

Handlungsfeld:
Wechselwirkung IKT und Energie verstehen und lenken

Die elektrische Energieversorgung wird zukünftig stärker von IKT-Systemen abhängig sein.
Die Gefahr, dass Störungen der IKT-Systeme zu Blackouts führen, ist zu vermeiden.

- Handlungsoption 1 – Abhängigkeiten zwischen Stromversorgung und Kommunikationsnetzen analysieren lassen.
- Handlungsoption 2 – Regeln für resiliente Kommunikationsnetze schaffen.
- Handlungsoption 3 – Akteure zu einer integrierten Betriebsführung der IKT- und Stromversorgung hinleiten.

Handlungsfeld:
Cyber-Sicherheit systemisch entwickeln

Die Anforderungen an die Cyber-Sicherheit müssen bei allen Akteuren auf ein ausreichend hohes Niveau gebracht werden. Dies erfordert sowohl technisch als auch organisatorisch neue Lösungen.

- Handlungsoption 4 – Cyber-Sicherheitsstandards für alle relevanten Akteure einführen.
- Handlungsoption 5 – Maßnahmen zum Umgang mit Sicherheitslücken definieren.

Handlungsfeld:
Technische Resilienz durch Netzbetreiber und Netznutzer stärken

Insbesondere in den Verteilnetzen wird die Netzführung zukünftig anspruchsvoller. Sowohl kleine Netzbetreiber als auch Betreiber kleiner Erzeugungsanlagen müssen deutlich mehr als heute üblich zur Resilienz beitragen.

- Handlungsoption 6 – Digitalisierung der Stromnetze voranbringen.
- Handlungsoption 7 – Regelwerk für Resilienz durch dezentrale Strukturen erarbeiten lassen.

Handlungsfeld:
IKT-Integration kleiner Anlagen netzdienlich gestalten

Der Großteil der Anlagen und Kleingeräte wird zukünftig mit dem Internet verbunden sein und sich darüber digital steuern lassen. Der daraus entstehenden Gefahr simultanen Verhaltens, das die Stabilität des Energiesystems bedrohen kann, ist zu begegnen. Auf der anderen Seite können diese Anlagen auch genutzt werden, um das Energiesystem aktiv zu stabilisieren.

- Handlungsoption 8 – Standardisierung zur Vermeidung problematischen simultanen Verhaltens initiieren.
- Handlungsoption 9 – Systemstabilisierung durch dezentrale Anlagen ausbauen.

Handlungsfeld:
Anreize für Netzbetreiber zur Steigerung der Resilienz stärken

Es fehlen weitgehend effektive und effiziente Anreize für die Netzbetreiber und Marktparteien, sich resilienzverbessernd zu verhalten. Dazu sollten marktliche Anreize geschaffen werden.

- Handlungsoption 10 – Eine Resilienzkomponente in die Anreizregulierung integrieren.
- Handlungsoption 11 – Resilienzverbessernde Netzentgelte und Anschlussgebühren einführen

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

Zur Systemstützung kann auch die Steuerung von Anlagen privater Akteure notwendig werden. Zur Ausgestaltung sollte ein Stakeholder-Gremium geschaffen werden, das Lösungen entwickelt, die für verschiedene Nutzergruppen wählbar sind und Fragen der Akzeptabilität berücksichtigen.

- Handlungsoption 12 – Ein Stakeholder-Gremium zur Berücksichtigung der Belange von Privatakteuren entwickeln.
- Handlungsoption 13 – Bewusstsein für den Einfluss privater Akteure schaffen.

Handlungsfeld:
Langfristige Risiko- und Resilienzbewertung institutionalisieren

Es wird zukünftig unvorhersehbare Trends geben, die etwa aus der Digitalisierung und der Energiewende entstehen und die Gefahr von Blackouts erhöhen könnten. Es sollte ein geeigneter Organisationsrahmen geschaffen werden, der es ermöglicht, flexibel auf solche Trends reagieren und mit ihnen umgehen zu können.

- Handlungsoption 14 – Organisationsrahmen für die Meldung von Störfällen und die Resilienzbewertung schaffen.
- Handlungsoption 15 – Einen übergeordneten Begleitprozess ins Leben rufen.

Tabelle 3: Kurzübersicht der Handlungsfelder und Handlungsoptionen

Wirkungsbereiche für die Umsetzung der Handlungsoptionen

Der Weg ins Unbekannte ist ein stetiger Lernprozess, in dessen Verlauf kontinuierlich Maßnahmen getroffen und Pfadabhängigkeiten berücksichtigt werden müssen. Bereits in den nächsten Jahren könnten einige der skizzierten Bedrohungen Realität werden. Die Politik muss deshalb bereits heute handeln, um auf diese Entwicklungen reagieren zu können. Sie kann 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 können, sind dann angebracht, wenn heute schon bekannt ist, dass ein Problem für die Resilienz besteht und bewertbare Lösungen 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 akzeptierbare Maßnahmen gefunden werden und das Vertrauen in die Angemessenheit von Entscheidungen wächst.

Es folgen sieben Unterkapitel zur Vorstellung und Diskussion der einzelnen Handlungsfelder und -optionen. Zu jedem Handlungsfeld werden zunächst das Kernproblem und die daraus resultierenden Gefahren erläutert, die in den nächsten Dekaden zu einem Blackout führen könnten. Im Anschluss werden jeweils die wichtigen heutigen Handlungsoptionen für die Politik erörtert und aufgeführt, mit welcher Dringlichkeit deren Umsetzung in Angriff genommen werden sollte (● ● ● in den nächsten zwei Jahren, ● ● in zwei bis vier Jahren, ● in fünf bis zehn Jahren). Zudem wird angegeben, wie wirksam die Handlungsoption zur Steigerung der Resilienz ist (● ● ● erhöht die Resilienz deutlich, ● ● trägt wesentlich bei, ● geringerer Beitrag).

Die Umsetzung der dargestellten Handlungsoptionen durch die Politik kann auf verschiedenem Wege erfolgen. In einem nächsten Schritt müssten basierend auf den hier dargestellten Ergebnissen verschiedene Möglichkeiten der konkreten Implementierung analysiert werden. So müssten unter anderem für jede Handlungsoption die Vor- und Nachteile von ordnungsrechtlichen Lösungen gegenüber finanzieller Anreizsteuerung und von staatlicher Regulierung gegenüber Selbstregulierung gegeneinander abgewogen werden. Auch die Frage, ob eine einheitliche europäische Vorgehensweise angestrebt wird oder (zunächst) eine nationale Lösung praktikabler ist, sollte in die Überlegungen einbezogen werden. Die Antworten auf diese Fragen sind fallabhängig und

müssten daher für jede einzelne Handlungsoption analysiert werden. Eine umfassende Diskussion verschiedener Implementierungspfade der 15 Handlungsoptionen würde den Rahmen dieser Stellungnahme sprengen und dem Ziel, einen überschaubaren Überblick über die wichtigsten Risiken, Handlungsfelder und Lösungsansätze zu liefern, entgegenstehen. Diese Stellungnahme ist daher auch als Impuls zu verstehen, um die gesellschaftliche und politische Diskussion zur konkreten Ausgestaltung der Handlungsoptionen in Gang zu setzen.

2.1 Handlungsfeld 1: Wechselwirkung IKT und Energie verstehen und lenken

Die Sicherheit der Stromversorgung wird in der Zukunft weit mehr als heute von IKT abhängen. Dies betrifft bei Weitem nicht nur die Netzbetreiber, sondern auch weitere Energieakteure wie etwa Stromhändler und Vertriebe. Aber auch Akteure, die ursprünglich nicht in der Energiewirtschaft tätig sind, werden maßgeblichen Einfluss auf die Sicherheit der Energieversorgung haben. Dazu zählen beispielsweise die Betreiber öffentlicher Kommunikationsnetze, auf denen auch das Internet basiert. Die gegenseitige Abhängigkeit von Stromversorgung und IKT birgt die Gefahr kaskadierender Ausfälle: So kann etwa ein Kommunikationsausfall einen Stromausfall verursachen, der weitere Kommunikationsstörungen auslöst, was zu weiteren Stromausfällen führt und so weiter. Besonders kritisch sind IKT-Ausfälle, die zu einem gleichzeitigen Ausfall vieler IKT-Komponenten führen.

Strom- und IKT-Systeme bilden zukünftig ein kombiniertes Gesamtsystem mit wechselseitigen Abhängigkeiten, ein komplexes sogenanntes cyber-physisches Energiesystem. Dabei können digitale Technologien zur Komplexitätsbewältigung und zur besseren Vorhersehbarkeit und Stabilität beitragen. Andererseits können aber fehlende situationsadäquate Informationen über mögliche Störungen der IKT-Systeme jederzeit zu Fehlern in der Betriebsführung des Stromnetzes führen. Der Einfluss fehlerhafter oder unsicherer IKT kann bereits durch geeignete Maßnahmen zu Cyber-Sicherheit entschärft werden (siehe Handlungsfeld 2). Dennoch spiegelt die heute übliche Sicht, die zur Planung, Überwachung und Steuerung der notwendigen IKT-Anwendungen inklusive des verwendeten Kommunikationssystems als externe Systeme „neben“ dem physikalischen elektrischen Energieversorgungssystem im engeren Sinne anzusehen, die Realität nicht mehr ausreichend wider. Sie muss durch einen Ansatz ersetzt werden, der das Verschmelzen der beiden Systeme anerkennt.

Auch für den schnellen Netzaufbau nach einem möglichen Blackout sind in besonderem Maße IKT-Systeme gefordert: Die Netzbetreiber müssen das Wiederanfahren des Netzes untereinander technisch koordinieren, Kraftwerke müssen kommunikativ angesteuert und zugeschaltet werden, Informationen über den während des Hochfahrens noch fragilen Netzzustand und das Gleichgewicht zwischen Last (Stromverbrauch) und Einspeisung müssen laufend ausgewertet werden. IKT-Systeme, die nicht gegen Stromausfälle gewappnet sind, würden einen Wiederaufbau der Stromversorgung sehr erschweren.

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.

Die gegenseitigen Abhängigkeiten zwischen dem energietechnischen Teil der Stromversorgung und den Kommunikationsnetzen müssen so gestaltet werden, dass kaskadierende Ausfälle unmöglich oder zumindest extrem unwahrscheinlich werden. Dies kann perspektivisch gelingen, indem die Abhängigkeit von systemrelevanten IKT-Systemen in einem Netzgebiet von der Stromversorgung in anderen Netzgebieten verringert wird: 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 in anderen Netzgebieten keine Störungen der IKT-Systeme auftreten. Wie vollständig dies gelingen kann, ist allerdings unklar: Vielfach vernetzte IKT-Systeme und nicht vorhandene geografische Kongruenz zwischen Kommunikations- und Stromnetzen erschweren diese Aufgabe.

Bevor ein solcher Lösungsansatz erarbeitet und ausgestaltet werden kann, gilt es zunächst, überhaupt zu verstehen, welche Abhängigkeiten zwischen Kommunikationsnetzen und Stromversorgung bestehen und mit welchen Mitteln sie entschärft werden können, damit auch im Fall gestörter Kommunikation eine grundlegende Stromversorgung gegeben ist. Im Zuge dessen sollten auch mögliche Cyber-Sicherheitslücken identifiziert werden, die sich aus den Abhängigkeiten ergeben. Dazu sind seitens der Politik entsprechende Studien und Forschungsprogramme zu initiieren. Die Ergebnisse der Studien und Projekte sollten auf europäischer Ebene diskutiert und in Verfahren und Regeln überführt werden. Neben der Politik sollten insbesondere ENTSO-E, der Verband der europäischen ÜNB, der von der Europäischen Union zwar geforderte, aber noch nicht realisierte Verband der europäischen VNB[20] sowie Standardisierungsverbände beteiligt werden.

20 Verordnung (EU) 2019/943, Art. 52–56.

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.

Es muss größere Redundanz in den Kommunikationsnetzen vorgesehen werden, um das Risiko eines für die Stromversorgung bedrohlichen Ausfalls von Kommunikationsnetzen deutlich zu vermindern. Ausfälle aufgrund einer gemeinsamen Ursache (sogenannte Common Cause Failures) müssen berücksichtigt werden, damit nicht dieselbe Ursache auch die redundanten Systeme ausfallen lässt.

Zusätzlich sollten die Betreiber einen bestimmten Teil des Kommunikationsnetzes schwarzfallfest aufbauen, also durch eine eigene unabhängige Stromversorgung etwa auf Basis von Batterien versorgen, die auch während eines Stromausfalls ihre Funktion noch erfüllen können. Dies wird unter anderem nötig sein, um im Falle eines Blackouts den Systemwiederaufbau durch die Netzbetreiber oder auch einen Inselbetrieb zu unterstützen.

Die Netzbetreiber sollten technisch bestimmen, welche Teile der Kommunikationsnetze schwarzfallfest sein müssen, welche Zeitintervalle im Stromausfall überbrückt werden müssen und welcher Technologiemix sich am besten technisch und ökonomisch dafür eignet. Aus diesen Bestimmungen sollte ein verbindlicher Leitfaden aufgestellt werden, anhand dessen die Netzbetreiber das Vorgehen in der Praxis umsetzen können.

Neben dem aktuell diskutierten Mobilfunkstandard CDMA 450 sollten auch weitere zusätzliche Technologieoptionen überprüft werden, etwa eine Priorisierung von Teilen des öffentlichen Mobilfunknetzes für kritische Dienste oder auch Satellitenkommunikation, die zunehmend kostengünstig wird und unbeeinflusst von Stromausfällen ist.

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.

Zukünftig sollten neben den elektrotechnischen Kenngrößen auch die Informationen über die Systemzustände der relevanten IKT-Komponenten beziehungsweise Kommunikationsnetze in ein übergreifendes Lagebild integriert werden. So kann etwa falsche oder fehlende Übertragung von Messwerten in der Betriebsführung berücksichtigt werden. Die Betriebsführungssysteme der Netzbetreiber und weiterer Akteure, die für die Systemstabilität eine Rolle spielen, müssen also potenzielles Fehlverhalten der IKT-Systeme möglichst frühzeitig erkennen, bewerten und in nachfolgenden Aktionen angemessen berücksichtigen.

Die ÜNB sollten die heute bereits vorhandenen Informationen über ihre Kommunikationssysteme in die Leitsysteme für das Stromnetz integrieren. Diese Informationen sind in der Regel aus den Monitoringsystemen für die Kommunikationsüberwachung extrahierbar. In Trainings kann dann geübt werden, wie diese Informationen im Störfall genutzt werden können (siehe Handlungsoption 6). Dazu könnten etwa Netzbetreiber anhand definierter Anwendungsfälle in Pilotprojekten die Wirksamkeit der integrierten Leitsysteme erproben. Die verantwortlichen nationalen beziehungsweise europäischen Verbände sollten drei Richtungen verfolgen und priorisieren:

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

2. Von Netzbetreibern zu weiteren Akteuren: Werden Maßnahmen zur Systemsicherung zunehmend von IKT-Systemen abhängig, die nicht der Kontrolle der Netzbetreiber unterliegen, wie beispielsweise die Steuerung von Windparks, so müssen die Netzbetreiber den Zustand dieser Systeme ebenfalls kennen und berücksichtigen.

3. Vom einzelnen Netzbetreiber zur Kaskade: Für eine Lagebeurteilung seines Netzes benötigt der Netzbetreiber Informationen, inwieweit nachgelagerte Netze, das heißt Netze niedrigerer Spannungsebene, die an dieses Netz angeschlossen sind, seine Anweisungen ausführen können.

Jeder Aktionspunkt muss verbindliche Regeln hervorbringen, in denen der Austausch der relevanten IKT-Kenngrößen festgelegt wird. Die Regeln würden etwa Datenformate und Austauschhäufigkeit von operativen Bewegungsdaten bestimmen. Für die ÜNB regelt bereits heute der Verband ENTSO-E den Datenaustausch.

2.2 Handlungsfeld 2: Cyber-Sicherheit systemisch entwickeln

Cyber-Angriffe sind eine neue Form der Bedrohung der Stromversorgung, die insbesondere durch die auf bewusste Sabotage zurückzuführenden Stromausfälle in der Ukraine 2015 und 2016 an Sichtbarkeit gewonnen haben.[21] Auch Fehler in der IKT haben bereits größere Stromausfälle mitverursacht. Die Sicherheitslage wird sich in den nächsten Jahren und Jahrzehnten noch weiter verschärfen: Bisher fordert die Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik[22] lediglich von den Betreibern besonders „großer“ energietechnischer Infrastrukturen, zum Beispiel Großkraftwerke (siehe Infobox "kritische Infrastruktur elektrische Energieversorgung" , dedizierte Maßnahmen zur Cyber-Sicherheit ein. Doch ein Blackout könnte zukünftig auch durch einen Cyber-Angriff auf einen großen Schwarm „kleinerer“ Systeme verursacht werden, die in Massen im Energiesystem verbaut sind. Hierzu zählen unter anderem Standard-Baugruppen zur Verteilnetzautomatisierung, Steuerungsboxen für Photovoltaik-Anlagen, aber auch Elektrogeräte in privaten Haushalten, auf die alle in zunehmendem Maße über das Internet zugegriffen werden kann. Cyber-Angriffe werden in diesem Fall dadurch begünstigt, dass auf sehr vielen Geräten dieselbe Software läuft, sodass über dieselbe Sicherheitslücke in der Software gleichzeitig sehr viele Geräte attackiert werden können. In Summe können dadurch Effekte ausgelöst werden, die den eines ausgefallenen Großkraftwerks übersteigen und zu einem Blackout führen können. Doch auch IKT-Systeme außerhalb der Energieinfrastruktur, etwa zentrale Serviceplattformen, Smart-Home-Dienste oder Fernwartungsleitstellen von Herstellern, können in der Gesamtheit systemkritisch sein, da über sie sehr viele Geräte angesteuert und somit auch fehlerbedingt lahmgelegt oder sabotiert werden können. Aufgrund der Vielzahl und Vielfalt dieser Systeme und IKT-Komponenten, die zukünftig Einfluss auf die Stromversorgung haben werden, 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.

Doch nicht nur unbeabsichtigte Fehler und kriminelle Akteure können die Cyber-Sicherheit schwächen. Auch der Staat verordnet gegebenenfalls Cyber-Sicherheitslücken, die einen Zugriff auf IKT-Systeme auch ohne die normalen Zugriffsrechte ermöglichen – sogenannte Hintertüren – und entwickelt eigene Angriffswerkzeuge, von denen er sich eine verbesserte Verbrechensbekämpfung erhofft. Geraten Informationen über diese versteckten Sicherheitslücken in falsche Hände, können davon potenziell Gefährdungen für alle KRITIS ausgehen.

Eine weitere Herausforderung stellt die hohe Innovationsgeschwindigkeit im Bereich der IKT dar. Zertifizierungsprozesse für die Sicherheitsstandards sollten Innovationen nicht durch zu große Trägheit ausbremsen. Dass dies zu Schwierigkeiten führen kann, zeigt sich am Beispiel des Smart Meter Rollouts: Die Verzögerungen im Zertifizierungsprozess haben zu Verunsicherungen am Markt und Schwierigkeiten bei der Umsetzung weiterer Dienste (Gateway-Administration und Mehrwertdienste) geführt. Die Verzögerungen können ebenfalls dazu führen, dass Lösungen außerhalb der

21 Whitehead et al. 2017.

22 BSI-KritisV 2017.

sicheren Smart-Meter-Infrastruktur entstehen. Umständliche Verfahren bergen nicht nur die Gefahr von Effizienzverlusten, sondern auch von verringerter Sicherheit.

Cyber-Sicherheit kann niemals allein durch die Einführung technischer 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. Es reicht nicht, sich nur um die Abwehr von Cyber-Störungen zu kümmern. Auch der Betrieb während einer Störung, die Behebung und die nachfolgende Analyse müssen beherrscht werden. Dies ist für viele Akteure aufgrund fehlenden Wissens oder Personals nicht möglich.

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.

Um eine Grundlage für neue Sicherheitsvorschriften zu schaffen, muss zunächst anhand von Risikoszenarien definiert werden, welche bisher zu wenig betrachteten Ursachen aus dem Cyber-Sicherheitsumfeld Blackouts hervorrufen können. Diese Risikoszenarien sollten neben Angriffen auf Übertragungs- und große Verteilnetze auch andere Arten von Angriffen und Fehlern berücksichtigen. Dazu zählen insbesondere Angriffe und Fehler, die eine große Anzahl kleiner Einheiten oder relevante IKT-Systeme von Akteuren außerhalb der Energiewertschöpfungskette – beispielsweise Herstellerplattformen oder zentral verwaltete Smart-Home-Systeme – betreffen. Die Risikoszenarien sind regelmäßig anzupassen, da die schnellen Entwicklungen der Digitalisierung unvorhersehbar sind. Diese Szenarien können insbesondere dabei helfen, „Security by Design“ zu realisieren, das heißt Cyber-Sicherheit bereits beim Design neuer Lösungen und Systeme zu berücksichtigen.

Die daraus abzuleitenden verbindlichen Cyber-Sicherheitsstandards zur Absicherung der Stromversorgung sollten mittelfristig EU-weit harmonisiert und standardisiert werden. Dabei sollten Richtlinien und Zertifizierungsprozesse der Größe der Akteure angemessen sein.

Verbindliche Sicherheitsstandards auch für Kleingeräte „hinter dem Zähler“ können verhindern, dass durch Endverbraucher Produkte mit Sicherheitslücken in einer Zahl eingesetzt werden, die ein Bedrohungspotenzial für die Stromversorgung darstellt. Zusätzlich sollten die Netzanschlussregeln für Bezugs- und Erzeugungsanlagen im Verteilnetz mindestens um Cyber-Sicherheitsaspekte erweitert werden, die gleichzeitige Angriffe auf eine große Anzahl dieser Anlagen erschweren.

Der Standardisierungsprozess sollte dem Innovationstempo digitaler Innovationen angepasst werden, sodass die für die Energiewende notwendigen Innovationen nicht ausgebremst oder unterbunden werden. Zugleich müssen hohe Datenschutzanforderungen erfüllt werden. Hierfür sollte ein Prozess zur Erstellung von Sicherheitsvorgaben etabliert werden, der regelmäßig die Wirksamkeit der Sicherheitsstandards evaluiert und bei Bedarf eine spätere Anpassung ermöglicht. Die Ausgestaltung der Standards nach behördlichen Vorgaben könnte von Verbänden und die Zertifizierung von qualifizierten Marktakteuren durchgeführt werden. Besonders Letzteres ließe Kosteneffizienz und zügige Zertifizierungen erwarten, im Gegensatz zu einer staatlich geleisteten Zertifizierung.

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.

Auch die besten Sicherheitsmaßnahmen bieten keinen allumfassenden Schutz vor IKT-verursachten Vulnerabilitäten, etwa aufgrund von Softwarefehlern, menschlichem Versagen im Sicherheitsmanagement oder staatlich gewollten Hintertüren.

Im Falle staatlich gewollter Hintertüren halten sich staatliche Stellen Zugangswege auf IKT-Komponenten offen oder stellen IKT-Werkzeuge her, um in fremde Rechner eindringen und dort Daten und Programme manipulieren oder löschen zu können. Beispiel hierfür sind sogenannte „Staatstrojaner“ und Software zur „aktiven Cyberabwehr“.[23] Solche Maßnahmen stellen ein hohes Risiko für die Versorgungssicherheit dar. Eine ausführliche Risikoabwägung (auch für weitere KRITIS) ist daher unumgänglich. Der Abwägungsprozess sollte so weit wie möglich transparent sein, wobei allerdings das notwendige Maß an Geheimhaltung gewahrt bleiben muss. Eine Kontrolle des Abwägungsprozesses durch eine vom Innenministerium unabhängige Stelle würde die Qualität der Maßnahme verbessern.

Verordnen andere Staaten ihren Herstellern, Sicherheitslücken in Software einzubauen, können sie gegebenenfalls darüber auf systemkritisch eingesetzte IKT-Komponenten auch in anderen Ländern zugreifen. Um dem entgegenzuwirken, besteht die Option, Hersteller zu verpflichten, den Quellcode staatlichen Prüfstellen offenzulegen. Dies wurde zum Beispiel in Großbritannien für den Hersteller Huawei bei der Errichtung des Mobilfunknetzes vorgeschrieben.[24] Es muss jedoch geklärt werden, wie eine solche Prüfung durchführbar ist. Zudem wird diskutiert, ob es nur ausgewählten europäischen Herstellern vorbehalten sein sollte, besonders kritische Kernbereiche der Stromversorgung mit IKT auszurüsten. Darüber hinaus könnte man die Abhängigkeit von einzelnen Herstellern verringern, indem Betreiber von KRITIS verpflichtet werden, Produkte verschiedener Hersteller nebeneinander zu betreiben und auf eine angemessen schnelle Austauschbarkeit von Produkten zu achten oder Produkte zyklisch auszutauschen.

Es sollte ein gemeinsamer Sicherheitsansatz für IT/OT-Systeme entwickelt und wo nötig eine klare Trennung zur Absicherung der OT-Seite ermöglicht werden. IT-Probleme sollten möglichst nicht zu kritischen Störungen der OT-Systeme führen. Dazu ist zu klären, welche Rückfall-Lösungen geeignet sind.

23 Maßnahmen wie der „Staatstrojaner“ sind an sich hochumstritten – die ethische, technische oder juristische Bewertung solcher Maßnahmen ist jedoch nicht Thema dieser Stellungnahme.

24 Katwala 2019.

Das notwendige Knowhow zur Abwehr und Analyse eines komplexen Cyber-Angriffs mit dem Ziel eines Blackouts können viele Betreiber relevanter Infrastrukturen personell nicht vorhalten. Hier könnten (am besten europäisch organisierte) Notfallteams aus Expertinnen und Experten unterstützen.

IT/OT-Konvergenz

Die IT/OT-Konvergenz ist ein Teilaspekt der Digitalisierung. „Operation Technologies“ (OT) bezeichnen IKT-Systeme, die direkt mit physikalischen Geräten oder technischen Prozessen interagieren. „Information Technologies“ (IT) umfassen in diesem Zusammenhang die IKT-Systeme für die Abwicklung von geschäftlichen oder administrativen Prozessen und Transaktionen wie Rechnungswesen, Vertragswesen oder Kundenmanagement.

Ursprünglich waren „OT“-Systeme aus Sicherheitsgründen von den „IT“-Systemen physikalisch getrennt, sodass keinerlei direkter Datenverkehr zwischen den beiden Systemwelten möglich war. IT/OT-Konvergenz bedeutet eine Abkehr von dieser strikten Trennung durch die vermehrte Integration von IT und OT und die gemeinsame Nutzung von Daten. Die Motivation ist eine Kostensenkung durch Vermeidung von Parallelinfrastrukturen oder die reibungslosere Integration von Workflows. Die IT/OT-Konvergenz findet in vielen Branchen statt – so auch in der Energieversorgung.

Eine mögliche sicherheitskritische negative Auswirkung der IT/OT-Konvergenz zeigte sich am Beispiel des Betankens eines Rettungsfahrzeugs in einem Feldversuch zur Simulation eines lokalen Blackouts. Zwar gab es eine unabhängige Notstromversorgung der Tankstelle, die den Blackout überbrücken konnte, jedoch stellte die Pumpanlage („OT“) vor jeder Betankung eine kommunikative Verbindung mit dem Kassensystem („IT“) her – und das Kassensystem wies die Betankung ab, da keine Verbindung mit dem Finanzamt für steuerliche Transaktionen aufgebaut werden konnte. In diesem Fall gab es also eine im Tagesgeschäft gewollte, aber in der Blackout-Situation ungewollte Rückkopplung der IT auf die OT, die ein Betanken des Rettungsfahrzeugs verhinderte.

Es zeigt sich, dass Fehler außerhalb der OT-Systeme wie hier die Störung der Finanzamts-IT zu unerwünschtem Verhalten auf der OT-Seite (im Notbetrieb nicht anschaltbare Pumpanlage) führen können. Dies ist umso problematischer, je systemrelevanter das OT-System ist, beispielsweise bei Kraftwerks- oder Netzleitsystemen. Im KRITIS-Bereich ist IT/OT-Konvergenz daher mit großer Vorsicht zu gestalten.

2.3 Handlungsfeld 3: Technische Resilienz durch Netzbetreiber und Netznutzer stärken

Die Umbrüche der elektrischen Energieversorgung, die sich aus der zunehmend variablen Erzeugung, Dezentralisierung und Digitalisierung der Stromversorgung ergeben, erhöhen von Jahr zu Jahr die Gefahr von „mehr Überraschungen" im Betrieb der Netze. Mit der wachsenden Komplexität in den nächsten beiden Dekaden können die Netzbetreiber immer schwerer prognostizieren, was in ihren Netzen passieren wird. Zudem können sich zukünftige Störereignisse von bisherigen Störereignissen sehr unterscheiden: Schnelle, unerwartete Leistungsschwankungen können aus dem Zusammenwirken jahreszeit-, tageszeit- und wetterabhängiger Erzeugung, der Vielzahl der über das Internet steuerbaren Anlagen und digital basierter Geschäftsmodelle entstehen. Die Verteilnetze werden zunehmend an den physikalisch-technischen Belastungsgrenzen betrieben werden und durch eine weit komplexere, (pro)aktivere und anspruchsvollere Netzführung und durchgängige Automatisierung geprägt sein – Fehler können sich dadurch stärker auswirken. Viele VNB werden in sehr viel höherer Frequenz als heute Maßnahmen zur Stabilisierung des eigenen Netzes durchführen und dabei auf eine deutlich erhöhte Kleinteiligkeit und Diversität neuer Akteure reagieren müssen.

Resilienz muss daher deutlich mehr von der technischen Unterstützung durch Betreiber kleiner Erzeugungsanlagen profitieren und durch Netzbetreiber der unteren Spannungsebenen unterstützt werden.

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.

In Zukunft benötigen die Netzbetreiber für die Behebung komplexer Störfälle ein umfassendes Lagebild zum Systemzustand mit Informationen über nachgelagerte Netze, verfügbare Flexibilitäten und Kurzfristprognosen zur Systemdynamik. Damit die Netzbetreiber ein solches Lagebild erstellen, austauschen und nötige Maßnahmen untereinander abstimmen können, ist eine umfassende Digitalisierung der Verteilnetze und der angeschlossenen Erzeugungsanlagen, Speicher und steuerbaren Verbrauchsanlagen erforderlich. Grundvoraussetzungen dafür sind eine abgestimmte Weiterentwicklung der digitalen Infrastruktur sowie die Definition von Standards zum Informationsaustausch aller Akteure. Bereits bei der Ausstattung der eigenen digitalen Infrastruktur eines Netzbetreibers sollten die Belange vorgelagerter Netzbetreiber berücksichtigt werden. Regulator und Netzbetreiber sollten dabei darauf achten, die Digitalisierung so zu gestalten, dass auch kleine Netzbetreiber und Zusammenschlüsse regionaler oder lokaler Akteure mit geänderten Anforderungen umgehen können. Dafür könnte etwa die Standardisierungsstrategie von BMWi und BSI[25] entsprechend erweitert werden. Zudem könnten im nationalen 7. Energieforschungsprogramm die Ministerien mit Einzelausschreibungen zum Thema „Resilienz und Digitalisierung“ die dafür notwendige Forschung vorantreiben.[26]

Es sollte ein Prozess eingeführt werden, in dem Digitalisierungsziele abgestimmt werden und die planmäßige Umsetzung verfolgt und gegebenenfalls korrigiert wird: Die Digitalisierung der Netze sollte in diesem begleitenden Monitoringprozess beobachtet und bewertet und aus den Ergebnissen sollten Empfehlungen oder verpflichtende Maßnahmen abgeleitet werden. Insbesondere muss die Digitalisierung weit über den Smart Meter Rollout hinausgehen. Nicht zuletzt sind die lokalen Gegebenheiten in den Verteilnetzen ausschlaggebend. Die Verteilnetzbetreiber sollten daher weiterhin entsprechende Freiheiten bei der Ausgestaltung der Digitalisierung behalten.

Zudem sollten Trainings für alle Netzbetreiber verpflichtend werden, um den Umgang mit überraschenden und neuartigen Blackout-relevanten Störereignissen zu üben sowie neue IKT- und durch künstliche Intelligenz gestützte Technologien und Werkzeuge zu testen. Dabei sollten zusätzliche Akteure, die bei der Behebung der Störung eine wesentliche Rolle spielen – wie etwa die Betreiber von Telekommunikationsnetzen – miteinbezogen werden. Ein standardisierter Prozess und klare Kriterien für Erarbeitung und Durchführung der Übungen sollten verabschiedet werden.

25 BSI/BMWI 2020.

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

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.

Im Fall eines Blackouts kann bei geeigneter technischer und regulatorischer Ausgestaltung temporär ein sogenannter Inselbetrieb – eine lokale, in der Regel eingeschränkte Stromversorgung – in einem Verteilnetz realisiert werden. Sobald der übergeordnete Stromausfall behoben ist, wird das Inselnetz wieder mit dem übergeordneten Netz verbunden. So kann die Wirkung von Blackouts reduziert und der Wiederaufbau erleichtert werden.

Wenn innerhalb einer Netzinsel nicht genug Erzeugungskapazität zur Verfügung steht, um die Insel vollständig zu versorgen, sollten kritische Verbraucher – wie etwa Krankenhäuser oder die Feuerwehr – bevorzugt mit Strom versorgt werden. Ein solcher selektiver Inselnetzbetrieb sollte regulatorisch ausgestaltet und technisch vorbereitet werden. Hierzu sollten die relevanten Akteure (Netzbetreiber, Anlagenbetreiber, Bürgerinnen und Bürger, Betriebe) in einem Partizipationsprozess intensiv einbezogen werden.

Neben der Frage, wie gesellschaftlich akzeptierte und diskriminierungsfreie Regeln für diesen Betrieb geschaffen werden können, sollte ebenfalls geklärt werden, welche Netzgebiete als Inselnetz betrieben werden sollten und wie Mindestanforderungen an Erzeuger-, Verbrauchs- und Speicherstrukturen ermittelt werden. Insbesondere Speicher können eine wesentliche Rolle für den stabilen Inselbetrieb spielen.[27] Diese mögliche Funktion von Speichern im Energiesystem sollte auch bei der zukünftigen Forschung und Entwicklung von Speichertechnologien berücksichtigt werden. Es sollten auch Anforderungen an die IKT berücksichtigt (siehe auch Handlungsoption 2) und Rückfalllösungen erarbeitet werden, die auch Störungen der IKT-Bestandteile verkraften können. Zudem ist zu klären, wie einheitliche Vorschriften und eine koordinierte Gestaltung des Inselbetriebs ausgearbeitet werden können. Insbesondere ist zu klären, welche Regeln innerhalb des ENTSO-E-Verbunds normiert und damit als europäischer Standard vorgegeben werden sollten. Auch neue Rollen und Pflichten, die sich für Netzbetreiber ergeben könnten, sind zu klären. Zum Beispiel könnte der Netzbetreiber im Inselbetrieb die Steuerung von Lasten und Erzeugung komplett übernehmen oder die Selbstorganisation von Aggregatoren oder dezentralen Erzeugungs- und Verbrauchsanlagen begleiten.

Diese Fragen sollten in Forschungs- und Entwicklungsprojekten beantwortet und Lösungen in Pilotprojekten im Feld unter realen Bedingungen erprobt werden. Dazu können etwa im nationalen 7. Energieforschungsprogramm entsprechende Ausschreibungen vorgenommen werden. Die Umsetzung der Maßnahmen ist langwierig und sollte daher zügig angegangen werden. Die Schaffung eines rechtlichen Rahmens wird weit mehr Zeit in Anspruch nehmen und sollte parallel vonstattengehen.

27 Eine vertiefte Darstellung der Nutzung von Batteriespeichern findet sich in acatech/Leopoldina/Akademienunion 2020-1.

2.4 Handlungsfeld 4: IKT-Integration kleiner Anlagen netzdienlich gestalten

In wenigen Jahren werden sich annähernd alle neu auf den Markt gebrachten elektrischen Erzeugungsanlagen (Dach-Solaranlagen, Kraft-Wärme-Kopplungsanlagen etc.) und Geräte[28] mit dem Internet verbinden können. Sobald die gemeinsame Leistungsmenge dieser Geräte hinreichend groß ist, kann massenhaftes synchrones Verhalten (ausgelöst durch Softwarefehler, bösartige Absicht oder synchrones Nutzerverhalten) das Blackout-Risiko erhöhen, indem so große und schnelle Leistungsänderungen im Stromnetz verursacht werden, dass diese nicht mehr mit bisherigen Maßnahmen abgefangen werden können.

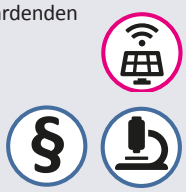
Auch Anlagen, die zwar nicht direkt durch das Internet ansteuerbar sind, aber gleiches Verhalten zur Netzstützung fest implementiert haben, können kritisches simultanes Verhalten aufweisen. Dies hat sich bereits in der Vergangenheit bei dem 50,2-Hertz-Problem gezeigt: In der Annahme, dass es zukünftig bei einem nur geringen Ausbau von PV bleiben würde, verabschiedete der damalige Verband der Netzbetreiber (VDN) in den Jahren 2005/2006 eine Regel, der zufolge sich PV-Anlagen bei einem Überangebot an Strom (gemessen an einem Frequenzanstieg über 50,2 Hertz) spontan abschalten müssen. Im Zuge der Energiewende hatte sich der Anteil an PV-Anlagen jedoch so vergrößert, dass eine gleichzeitige Abschaltung dieser Anlagen die zu hohe Einspeisung massiv überkompensieren und das System destabilisieren würde. In der Folge mussten in einem jahrelangen Prozess etwa 300.000 PV-Anlagen umgerüstet werden. Einer festen Implementierung von Regeln liegen also Annahmen über die Zukunft zugrunde. Erweisen sich diese Annahmen als falsch, kann dies zu einer nur sehr aufwendig zu behebenden Vulnerabilität des Energiesystems führen. Dabei stehen hier 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. Auf Altgeräte mit Bestandsschutz kann sich diese Problematik noch gravierender auswirken, da nachträgliche Änderungen rechtlich schwerer zu regeln sind.

Auf der anderen Seite kann bewusst herbeigeführtes synchrones Verhalten von Erzeugungsanlagen und Speichern auch netzdienlich genutzt werden. So kann dadurch zum Beispiel der Bedarf an Regelleistung aus Großkraftwerken reduziert oder im Falle eines Blackouts ein Inselnetz (siehe Handlungsoption 7) unterstützt werden. Dezentrale Erzeugungsanlagen leisten bereits heute Beiträge zur Systemstabilisierung, etwa indem sie sich an der Spannungshaltung beteiligen und zur Regelleistung beitragen.

28 Mit dem Begriff Gerät sind hier elektrische Geräte „hinter dem Zähler“ gemeint, also beispielsweise Wärmepumpen, elektrische Heizungen, Haushaltsgeräte, Ladestationen eines Haushalts oder elektrische Hausspeicher.

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.

Ungeplante, unvorhersehbare Gleichzeitigkeiten oder zeitgleiches Abschalten von Geräten und Erzeugungsanlagen müssen als potenzielles Risiko erkannt und dementsprechend in einer Resilienzstrategie berücksichtigt werden. Dazu braucht es von Fachgremien entwickelte, anwendungsfallspezifische Mindeststandards. Diese müssen so gehalten sein, dass sie einen großen Umfang möglicher Anlagen einschließen und zukunftssicher sind. Eine internationale Standardisierung wäre vorteilhaft, da kritisches simultanes Verhalten überall im europäischen Verbundnetz dieselben negativen Auswirkungen hat.

Ein wichtiger Teil dieser Standards für Erzeugungsanlagen und Geräte ist die Gewährleistung von „Patchability“: Das heißt, dass die Software einer technischen Anlage im laufenden Betrieb und ohne viel Aufwand aus der Ferne durch das Einspielen von Patches verbessert werden kann, entweder durch die Hersteller oder auch durch den Betreiber. Die Implementierung von Patchability muss bereits heute durchgeführt werden, da Anlagen und Geräte zum Teil Jahrzehnte lang genutzt werden und nicht vorhersehbar ist, welchen technischen Anforderungen sie in Zukunft entsprechen müssen. Hierfür sind Abstimmungen zwischen Regulator und Hersteller und weiteren betroffenen Akteuren wie etwa den Betreibern der Anlagen notwendig. Zu klären sind insbesondere Finanzierung, Haftungsfragen, Regeln bei Abkündigung eines Produkts und Verantwortlichkeiten für die Kommunikationsanbindung.

Zum Schutz vor systemschädlichem Verhalten kann zusätzlich lokale Plausibilisierung eingesetzt werden. Erzeugungsanlagen oder Geräte prüfen eigenständig – zum Beispiel anhand physikalischer Größen wie Spannung und Frequenz – die Plausibilität der Schaltbefehle und reagieren entsprechend. Hierfür können insbesondere Methoden der künstlichen Intelligenz zum Einsatz kommen. Welche Art der Plausibilitätsprüfung feststellen kann, ob die durch den Netzbetreiber übermittelten Schalthandlungen in der aktuellen Netzsituation schädlich sind, lässt sich heute nicht beurteilen. Daher sind hier zunächst entsprechende Analysen und Forschungen notwendig, die durch den Netzbetreiber – mit Einbindung der anderen relevanten Akteure (wie Anlagenhersteller und -betreiber) – durchgeführt werden sollten. Zudem muss eine zukünftige Anpassung dieser Plausibilitäten mittels Patch möglich sein.

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.

Die Systemrelevanz der kleinen Anlagen und Geräte lässt sich auch positiv gestalten: Dezentrale Erzeugungsanlagen und steuerbare Geräte können und sollten in Zukunft viel mehr als heute zur Resilienz des Energiesystems beitragen. Zum Beispiel können sie Systemdienstleistungen bereitstellen und so einen sicheren und zuverlässigen Systembetrieb gewährleisten oder nach einem Blackout den Wiederaufbau der Versorgung unterstützen. Dafür braucht es neben der notwendigen leistungselektronischen Ausstattung insbesondere eine – kosteneffizient umsetzbare – kommunikationstechnische Integration der Anlagen in das Leitsystem des Netzbetreibers, die über das reine Abregeln von Anlagen hinausgeht.

Im Rahmen des Smart Meter Rollouts ist zwar die Anbindung dezentraler Anlagen vorgeschrieben, der Fokus liegt aber eher auf Abrechnungsprozessen und variabler Tarifierung als auf einer möglichen Unterstützung der Systemstabilität durch die Ansteuerung angeschlossener Anlagen oder Mehrwertdiensten für Kunden. Um die gewünschte Konnektivität sicherzustellen, sollten die Regelungen um (internationale) Vereinbarungen zu Standards zur Interoperabilität sowie für die Einbindung dezentraler Anlagen in große Plattformen erweitert werden. Im Rahmen des Projekts CONNECT+ haben sich Netz- und Anlagenbetreiber im Sommer 2019 zusammengeschlossen, um technische und regulatorische Fragen bezüglich des Datenaustauschs zu klären. In Pilotprojekten mit Netzbetreibern, Telekommunikationsunternehmen und Aggregatoren soll unter anderem gezeigt werden, dass die hohen Anforderungen an die IKT-Anbindung zur Einbindung der kleinen Anlagen in einen Regelleistungspool auch mit kostengünstigen Mitteln zu erreichen wären.

Ein noch weitreichenderer Ansatz zur Einbindung kleiner Erzeugungsanlagen und steuerbarer Verbrauchsanlagen sieht vor, zur Steuerung dieser Anlagen künstliche Intelligenz zu nutzen und entsprechende Algorithmen direkt in die Anlagen zu integrieren. So kann auch auf komplexe und unbekannte Störereignisse oder Angriffe angemessen reagiert werden. Solche Verfahren der künstlichen Intelligenz stecken noch in den Kinderschuhen und sollten intensiv erforscht werden.

Über die Nutzung kleiner Anlagen und Geräte zur Systemstabilisierung entscheidet jedoch letztendlich nicht nur die technische und ökonomische Machbarkeit – die bereits in vielen Forschungs- und Pilotprojekten untersucht wurde und wird –, sondern auch die Akzeptanz durch Privatakteure. Diese sollte daher ebenfalls in entsprechenden Maßnahmen berücksichtigt werden (siehe Abschnitt 2.6).

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

Je höher der Anteil der dezentralen und digital vernetzten Anlagen im zukünftigen Stromnetz, desto höher der Bedarf an resilienzverbessernden Maßnahmen auch durch die Netzbetreiber. Im energiewirtschaftlichen Regelrahmen finden sich jedoch nur wenige Aspekte, die explizit Resilienz berücksichtigen. Dabei kann gerade der Netzbetreiber durch seine Investitionsentscheidungen die Resilienz des elektrischen Energiesystems maßgeblich beeinflussen. Die Netzbetreiber haben aktuell aber keinen Anreiz, die externen Kosten beziehungsweise deren Vermeidung in ihre Investitionsentscheidungen einzubeziehen: Sie tragen zwar die Kosten der Resilienzmaßnahmen, diese kommen aber den Netznutzern zugute. Die Kosten für resilienzverbessernde Maßnahmen finden bisher keine Anerkennung in der Verordnung über die Anreizregulierung der Energieversorgungsnetze (kurz: Anreizregulierungsverordnung, ARegV). Die Anreizregulierung ist ein Instrument, das dazu beitragen soll, dass Netzbetreiber der „natürlichen Monopole“ Strom- und Gasnetz keine Monopolgewinne erzielen und ihre Netze möglichst kosteneffizient betreiben. Durch die Erlösobergrenzen wird der Anreiz geschaffen, bei gegebener und messbarer Aufgabe Kosten zu senken, um so höhere Gewinne zu erzielen. 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 beschrieben) erreicht werden kann.

Im Folgenden werden zwei Themenbereiche zur Adressierung des beschriebenen Problems adressiert, die jedoch nur einen (prioritären) Ausschnitt aus einer Vielzahl von Regulierungsthemen in diesem Kontext darstellen:

Anreizregulierung (siehe Handlungsoption 10): Den Netzbetreibern wird durch die ARegV eine Erlösobergrenze vorgegeben, die maßgeblich die Anreize der Netzbetreiber bestimmt. Ob und wie die Anreizregulierung die Resilienzthematik effektiv berücksichtigt, hängt einerseits von der Art der Kosten ab, die durch die resilienzverbessernden Maßnahmen entstehen, und andererseits von bereits bestehenden Maßnahmen in der ARegV (zum Beispiel Q-Komponente). Die Abgrenzung der Qualitätsregulierung von der Resilienzthematik ist aufgrund der inhaltlichen Nähe der beiden Themen nicht ganz trennscharf. Wir argumentieren aber, dass für Resilienz, wie sie in diesem Dokument verstanden wird, durch die derzeitige ARegV keine ausreichenden Anreize geschaffen werden und ein zusätzliches Instrument erforderlich ist. Zwar verfügen die Netzbetreiber heute schon über Möglichkeiten, einen Teil der Ausgaben für resilienzverbessernde Maßnahmen geltend zu machen. Im Fokus steht hier jedoch die Frage, ob die Netzbetreiber auch hinreichend Anreize haben, diese Instrumente tatsächlich zu nutzen. Hier setzen wir mit dem Vorschlag einer Resilienzkomponente an.

Netznutzungsentgelte (siehe Handlungsoption 11): Diese Entgelte bestimmen die Kosten für den Zugang zu den Übertragungs- und Verteilernetzen (Netzentgelte), und die entsprechenden Regelungen umfassen auch die Ermittlung der Entgelte für dezentrale Einspeisungen. Wir integrieren die Thematik der Resilienz in die neuere Diskussion um Netzanschlussgebühren (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.

Letztlich versucht der aktuelle Umgang mit abschaltbaren Lasten[29] bereits, über einen freiwilligen und kurativen Prozess im Bereich der Lasten einen ähnlichen Effekt zu erreichen, wie dies bei Smart Connection Agreements für Lasten der Fall wäre. Der wesentliche Unterschied bei diesen beiden Instrumenten liegt jedoch in der Freiwilligkeit: Während abschaltbare Lasten frei entscheiden können, wann, in welchem Umfang und zu welchem (variierenden) Preis das Instrument genutzt wird, regelt das Smart Connection Agreement all dies vorab und ist ab dann bindend. Freiwillig ist dann nur noch die Zustimmung zum Smart Connection Agreement.

29 Geregelt in AbLaV 2016.

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.

Die Versorgungssicherheit des elektrischen Energiesystems fließt unter dem Begriff „Qualität“ in die ARegV[30] ein, wobei die Begriffe Netzzuverlässigkeit und Netzleistungsfähigkeit zur Bestimmung der Qualität 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. Resilienz setzt 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 liegen die monetären Konsequenzen ebenfalls außerhalb der ARegV und können so auch keine Anreizwirkung auf den Netzbetreiber ausüben.

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 bei seiner Investitionsentscheidung bezüglich Resilienzmaßnahmen berücksichtigen – genau deshalb bräuchte die ARegV eine zusätzliche Regelung zur Verbesserung der Resilienz: eine R-Komponente, mit „R“ für Resilienz.

Die wesentlichen Fragen, die für eine konkrete Umsetzung einer Resilienzkomponente zu beantworten sind, lauten:

- Was wären die geeigneten Indikatoren für eine Resilienzkomponente?
- Was wären geeignete Instrumente, um die Anreize für die Netzbetreiber zu verbessern?

Die konkrete Umsetzung ist komplex und sollte vertiefend analysiert werden. In Abhängigkeit des gewählten Instruments sollten die Parameter eine gute Balance zwischen Effektivität der Anreize und finanziellem Risiko für die Netzbetreiber darstellen.

30 ARegV 2019.

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.

Die Struktur der Netznutzungsentgelte wird in der Verordnung über die Entgelte für den Zugang zu Elektrizitätsversorgungsnetzen (kurz: Stromnetzentgeltverordnung, StromNEV) geregelt.[31] Deren Höhe hingegen ergibt sich aus der Erlösobergrenze und damit aus der ARegV. Wesentlich bei der Gestaltung der Netznutzungsgebühren sind die Tarifstruktur und die Kostenallokation. Die Netznutzungsentgelte könnten darüber hinaus weiter differenziert werden, insbesondere zeitlich und räumlich. Resilienz ist bislang kein Differenzierungskriterium.

Für die Resilienz des elektrischen Energiesystems erscheinen in Bezug auf die Netznutzung und deren Bepreisung insbesondere zwei Aspekte besonders relevant: erstens Gleichzeitigkeitseffekte und zweitens Netztopologie. In beiden Fällen kann ein differenzierteres Netznutzungsentgelt lenkend wirken, um die Resilienz des elektrischen Energiesystems zu erhöhen. Einen Ansatzpunkt liefern hier Smart Connection Agreements. Solche flexiblen Netzanschlussbedingungen befinden sich aktuell in Erprobung, etwa in Frankreich, Belgien und UK.[32] Smart Connection Agreements sollen bereits bei der Netzanschlussgebühr, insbesondere bei erneuerbaren Energien, Netzknappheiten berücksichtigen (analog zum Netzausbauzuschuss). Es läge nahe, ebensolche Smart Connection Agreements um eine Resilienzbetrachtung zu erweitern: Netznutzer mit resilienzverbessernden Standortentscheidungen und/oder mit Abbau von Gleichzeitigkeiten werden belohnt – und umgekehrt.

Die genaue Ausgestaltung wird sehr von den Details der jeweiligen Netztopologie bestimmt. Deshalb sollte die Umsetzung flexibel und fallabhängig beim Netzbetreiber liegen, und entsprechende Anreize sollten über die ARegV geschaffen werden (vgl. Handlungsoption 10).

31 StromNEV 2019, §§ 15 ff.

32 Vgl. Furusawa et al. 2019.

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

Bei dem digitalisierten und vernetzten Energiesystem handelt es sich um ein komplexes soziotechnisches System, in dem Technik und Gesellschaft gleichermaßen betrachtet werden müssen. Hierbei findet eine Koevolution von Technologie und Gesellschaft statt: Das technische System hat nicht nur Rückwirkungen auf die Lebensumstände in der Gesellschaft, es entwickelt sich auch auf Grundlage von gesellschaftlichen Erkenntnissen und Strömungen. So bedient etwa der Markt das gewachsene Bewusstsein für Energieeffizienz mit neuen technischen Produkten, die dann wiederum durch Marketing oder Energiesiegel auf das Bewusstsein zurückwirken.

Durch die zukünftig gute technische Vernetzung bergen die Anlagen und Geräte von Privatakteuren großes Potenzial für die Stützung des Energiesystems und eine Erhöhung der Resilienz. Dadurch wird aber auch das Verhalten von Privatakteuren zunehmend relevant, da die Erzeugungsanlagen und Geräte, die sie benutzen, einen systemkritischen Einfluss haben können (siehe Kapitel 2.4). Dieses Einflusses sind sich Privatakteure zumeist nicht bewusst.

Privatakteure nehmen bereits heute eine zunehmend aktive Rolle ein und wirken an der Gestaltung des Energiesystems mit, zum Beispiel als Prosumer. Darüber hinaus gibt es zum Beispiel Energiegenossenschaften, die Wind- und PV-Anlagen betreiben, oder erste Quartierslösungen, in denen sich private Haushalte selbst organisieren und lokal Energie austauschen können – eine Entwicklung, die sich durch Digitalisierung, elektrische Hausspeicher und Elektrofahrzeuge noch verstärken könnte.

Das Resilienzpotenzial durch die Digitalisierung der Haushalte kann zukünftig durch die Netzbetreiber unter anderem für das Sammeln von Daten für bessere Verbrauchsprognosen, für die direkte Steuerung der Anlagen wie etwa selektives An- oder Abschalten einer PV-Anlage oder für die Organisation des Inselbetriebs genutzt werden. Letztendlich bedeuten all diese Maßnahmen jedoch einen Eingriff in das private Umfeld der Akteure und erfordern deshalb auch ein gewisses Maß an Akzeptanz.

Bei der Umsetzung der Maßnahmen können daher Probleme auftreten, etwa ein Verlust an Selbstbestimmung und Vertrauen. Es besteht auch ein Risiko, dass Maßnahmen nicht greifen, beispielsweise, weil sie die Zielgruppe nicht ansprechen. Diese Probleme können dazu führen, dass das Potenzial privater Anlagen zur verbesserten Resilienz nicht genutzt wird, Lösungen nicht umgesetzt werden, neue Regelungen nicht greifen und so systemkritische Situationen begünstigt werden.

Rolle der Industrie

Auch **industrielle** Akteure müssen einen Beitrag zur Resilienz leisten. Der Beitrag kann indirekt sein, indem sichergestellt wird, dass Geräte und Anlagen, die im elektrischen Energiesystem zum Einsatz kommen, verschiedene resilienzverbessernde Anforderungen erfüllen. Dazu zählen:

- Sicherheitsvorschriften für IKT-Systeme (zum Beispiel Plattformen) werden eingehalten (siehe Handlungsoption 4),
- Sicherheitsstandards für Kleingeräte „hinter dem Zähler" werden eingehalten (siehe Handlungsoption 4)
- Der Quellcode wird staatlichen Stellen zur Prüfung auf mögliche Sicherheitslücken offengelegt (Handlungsoption 5)
- Flexible Konfiguration der Software technischer Anlagen wird ermöglicht (Handlungsoption 8)

Die industriellen Akteure, die von diesen Maßnahmen betroffen wären, sind:

- **Hersteller von Energietechnik** und deren OT-Systeme (zum Beispiel intelligenter Betriebsmittel, Erzeugungs- und Speicheranlagen)
- **Hersteller von IKT-Systemen** für die Stromversorgung (zum Beispiel IKT-Komponenten und Ausrüstung von Kommunikationsnetzen)
- **Betreiber von IKT-Systemen,** die im Zusammenhang mit der Stromversorgung stehen (zum Beispiel Rechenzentren, Plattformen, Kommunikationsnetze)

Darüber hinaus leisten industrielle Akteure auch heute schon einen aktiven Beitrag zur Resilienz des elektrischen Energiesystems, indem sie einen Teil ihrer Verbrauchsflexibilitäten den Netzbetreibern zur Verfügung stellen. Die Flexibilitäten dieser Prozesse können vermarktet und für die Systemstabilisierung genutzt werden, zum Beispiel in Form von Regelleistung oder als abschaltbare Lasten.[33] Für die zukünftige Energieversorgung ist es jedoch wichtig, Flexibilitäten von industriellen und gewerblichen Stromverbrauchern noch viel stärker zu erschließen.[34] Wesentliche Synergien entstehen hier durch **Industrie 4.0** – der durch Digitalisierung der Industrie geleisteten stärkeren Vernetzung von Maschinen und industriellen sowie kaufmännischen Abläufen. Die Unternehmen flexibilisieren so den Stromverbrauch ihrer Prozesse, um, durch die Preise an der Strombörse angereizt, flexibel auf das Dargebot von Wind- und Solarstrom reagieren zu können.[35] Überdies leistet Digitalisierung auch Beiträge zu einer **ressourcenschonenden Produktion.**[36]

Produktionsprozesse werden zukünftig klimaschonend oder sogar klimaneutral gestaltet. Dazu gehört nicht nur der Ersatz von Erdgas, Erdöl und Kohle durch Erneuerbare Energien, sondern auch teilweise eine völlige Umgestaltung der Produktionsverfahren (beispielsweise Direktreduktion mit Wasserstoff statt Hochofenverfahren in der Stahlerzeugung[37]). Dadurch können sich jedoch Verbrauchsmuster ändern, die im Netzbetrieb berücksichtigt werden müssen (siehe Kapitel 1.2).

33 Vgl. Umweltbundesamt 2015.
34 Vgl. acatech/Leopoldina/Akademienunion 2020-2.
35 Beispiele siehe: Agora 2016.
36 Vgl. Plattform Industrie 4.0 2020.
37 Vgl. Agora 2020.

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.

Durch den Aufbau eines Stakeholder-Gremiums sollen alle relevanten Akteure in die Entscheidungsfindung für neue Regelungen, die Privatakteure betreffen, einbezogen werden. Neben dem Regulierer sowie den privaten Akteuren 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. Ziel sollte sein, dass die Ergebnisse des Prozesses von allen Beteiligten akzeptiert werden können.

Besonders sensibel ist die Akzeptanz solcher Regelungen durch die Privatakteure. Entstehende Fragen und Befürchtungen, die etwa Datenschutz und Eingriffe in die Privatsphäre betreffen, sollten frühzeitig aufgegriffen und berücksichtigt werden. Gleichzeitig muss 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 (zum Beispiel freiwillige Selbstbeschränkung, finanzielle Anreize) umgesetzt werden können.

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 die gewünschte Wirkung entfalten und gleichzeitig negative Rückwirkungen verhindern oder auffangen. Auch eine potenzielle Ablehnung durch die Akteure muss berücksichtigt werden. Geeignete Untersuchungen in Forschungsprojekten zu diesen Anreizsystemen und deren Wirkung sollten durchgeführt und in Experimenten oder Reallaboren erprobt werden.

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.

Für die Privatakteure muss nachvollziehbar sein, welchen Einfluss ihr Verhalten auf die Stabilität des elektrischen Energiesystems hat und welche Beiträge sie leisten können, um die Stabilität zu unterstützen. Hier gilt es, ein Problembewusstsein, ein minimales Verständnis für Komplexität sowie digitale Mündigkeit zu fördern.

Privatakteure sind nicht unmittelbar verantwortlich für die Resilienz des Systems. Dennoch müssen umfassende Informationen für sie zugänglich sein, sofern ihre Rechte und Interessen berührt werden. Im Sinne von Transparenz und Vertrauen ist es notwendig, Informationsangebote aufzubauen, die den jeweiligen Informationsbedürfnissen entsprechen und den Einbezug der privaten Akteure und deren Souveränität gewährleisten.

Im ersten Schritt sollten dazu Informationsangebote – etwa Kampagnen – entwickelt und realisiert werden. Unter anderem sollten Bildungsangebote in Schule und Weiterbildung eingebunden werden. Dabei ist es wichtig, Informationen in transparenter Weise an die unterschiedlichen Informationsbedürfnisse anzupassen, etwa durch ein Informationsportal für unterschiedliche Zielgruppen und mit unterschiedlichen Kommunikationsformaten, um die (digitale) Souveränität der privaten Akteure 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.

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 Urheber an. Auch für den Aufbau von Vertrauen in die überwachenden Instanzen und Instrumente sind relevante Sachwalter der Privatakteure, hier insbesondere Verbraucherschutzorganisationen und Datenschutzinitiativen, einzubeziehen. Diese sollten sowohl an der Eingriffsausgestaltung als auch an der Kommunikation mitwirken.

2.7 Handlungsfeld 7: Langfristige Risiko- und Resilienzbewertung institutionalisieren

Entscheidungen von Regulierungsbehörden und operativ tätigen Akteuren wie Netzbetreibern beruhen oft auf Erfahrungen aus der Vergangenheit sowie auf Analysen bereits absehbarer zukünftiger Entwicklungen. Wie die hohe Zuverlässigkeit und Qualität der Versorgung zeigen, war dies bisher völlig ausreichend, um die richtigen Entscheidungen zu treffen. Das wird in Zukunft jedoch so nicht mehr der Fall sein. Denn durch den rapide zunehmenden Einfluss der Digitalisierung auf die Energieversorgung – etwa durch das „Internet der Dinge", digital basierte Geschäftsmodelle, digitalisierte oder automatisierte betriebliche Prozesse, künstliche Intelligenz und die Plattformökonomie – wird das System unüberschaubar und schlechter vorhersehbar. Überraschende Entwicklungen, die sich als Bedrohung für das elektrische Energiesystem erweisen könnten, können deutlich schneller als bisher eintreten.

Bei zukünftigen Risikobewertungen und Maßnahmen muss daher stärker auf den Umgang mit Unsicherheiten und unerwarteten Entwicklungen geachtet werden. Es müssen Risikofaktoren einbezogen werden, die sich kaum aus den bisherigen Erfahrungen erschließen lassen. Um zukünftig auch mit überraschenden Ereignissen besser umgehen zu können, sollte das Konzept der Resilienz stärker in der Risikobewertung und in politischen Maßnahmen zur Bewahrung der Versorgungssicherheit verankert werden. Dafür muss ein geeigneterer institutioneller Organisationsrahmen geschaffen werden.

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 und andererseits Resilienz der Stromversorgung bisher noch nicht ausreichend messbar und bewertbar ist. Dies führt zu Effektivitäts- und Effizienzverlusten bei der Sicherung der Resilienz.

Derzeit wird auf EU-Ebene durch die Verordnung „Risikovorsorge im Elektrizitätssektor"[38] für die ÜNB bereits eine detaillierte und supranationale Risikobewertung institutionalisiert. Dazu gehört auch die Benennung einer nationalen Krisenkoordinierungsstelle, die als Ansprechstelle im Fall einer Stromversorgungskrise fungieren soll. Die Verordnung konzentriert sich jedoch auf die Übertragungsnetze, extreme Blackouts, einen mittleren Zeithorizont und absehbare Risiken. Überraschende Ereignisse und langfristige Entwicklungen sollten jedoch ergänzend aufgenommen und stärker in das Blickfeld gerückt werden. Dabei sollte der Fokus nicht nur auf technischen Aspekten liegen. So können sich in einem lang andauernden gesellschaftlichen Transformationsprozess wie der Energiewende normative Vorstellungen und Beurteilungen ändern – ein prägnantes Beispiel hierfür ist die Einstellung zur Kernenergie in Deutschland. Da Entscheidungen des Gesetzgebers und auch der Netzbetreiber häufig Pfadabhängigkeiten schaffen, da sie zur Errichtung von Infrastrukturen führen, sollte eine Resilienzstrategie auch verschiedene mögliche gesellschaftliche Entwicklungen bis hin zu Instabilitäten berücksichtigen.

38 EU-Verordnung (EU) 2019/941 „Risikovorsorge im Elektrizitätssektor", vgl. Verordnung (EU) 2019/941.

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.

Eine zentrale und unabhängige europäische Informations- und Meldestelle für Störereignisse sollte stetig aktualisiertes Wissen über Blackout-relevante Risiken, Störereignisse, Cyber-Sicherheitslücken und mögliche Gegenmaßnahmen für den Netzbetrieb bündeln, aufbereiten und mehrsprachig verfügbar machen. Basierend auf den ausgewerteten Informationen könnte diese Stelle auch Empfehlungen formulieren. Sie sollte nationale Behörden und Notfallteams zeitnah über Vorfälle informieren und ebenfalls im engen Austausch mit den relevanten Akteuren (Netzbetreibern, gegebenenfalls Herstellern) stehen. Es ist auch zu klären, wie sie mit der Krisenkoordinierungsstelle der EU-Verordnung „Risikovorsorge im Elektrizitätssektor“ zusammenarbeitet. In einem ersten Schritt sollte die Stelle auf nationaler Ebene eingerichtet werden. Die so gewonnenen Erfahrungen können später helfen, eine entsprechende europäische Institution aufzubauen und zu gestalten.

Auch die Risikobewertung sollte stärker institutionalisiert werden. Eine behördliche oder behördlich beaufsichtigte Institution sollte eingerichtet werden, die potenziell bedrohliche Entwicklungen für das Energiesystem frühzeitig identifiziert und Maßnahmen für die Politik vorschlägt. Dafür kann die EU-Verordnung zur Risikovorsorge im Elektrizitätssektor als Vorlage dienen. So kann die Ausarbeitung von Frühwarnsystemen und -indikatoren (etwa zu Marktrisiken, technische Disruptionen oder politische Verwerfungen) miteinbezogen werden. Auch die Beobachtung langfristiger Entwicklungen und die Erarbeitung von Anpassungsstrategien wären sinnvolle zusätzliche Maßnahmen, aus denen sich Handlungsoptionen für die Politik ableiten ließen. Neben Blackouts sollten auch kleinere Stromausfälle und „Beinaheausfälle“ in die Risikobewertung miteinbezogen werden, ebenso wie Sektoren, die durch ihren Anschluss an Kommunikationsnetze indirekte Rückwirkungen auf das Energiesystem haben können. Zudem sollte die Entwicklung neuer methodischer Ansätze gefördert werden, die helfen, die Vorhersagemöglichkeiten zu stärken. Dabei sollten Fachleute aus der Energieversorgung, der IKT-Domäne, der Risikoforschung und den Gesellschaftswissenschaften eingebunden werden.

Darüber hinaus sollte ein Rahmen geschaffen werden, mit dessen Hilfe Maßnahmen bezüglich ihrer Wirksamkeit überhaupt bewertet werden können. Dazu sind zunächst geeignete qualitative und quantitative Kenngrößen zu entwickeln. Den Kenngrößen entsprechende Vorgaben und Standards können national oder europäisch (etwa im Rahmen eines EU-Mandats) erarbeitet werden. Durch klare Standards zur Bewertung wird „Resilience by Design“, also die Berücksichtigung von resilientem Verhalten, bereits in der Design-Phase von Lösungen, ermöglicht. Netzinvestitionen in IKT erhalten eine fundierte Begründung und Berechtigung; ein klares, transparentes Vorgehen wird gefördert.

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.

Eine unabhängige Institution evaluiert im Auftrag der Politik in einem begleitenden Monitoring, ob die verfolgte Resilienzstrategie heute und in absehbarer Zukunft effektiv, effizient und ausreichend ist. Während die in Handlungsoption 14 vorgeschlagene Institution zur Risikobewertung die Erarbeitung konkreter Risikoinstrumente und neuer Resilienzmaßnahmen zum Ziel hat, liegt der Fokus also hier auf der Bewertung der Resilienzstrategie und ihrer Umsetzung in Gänze. Auf dem Prüfstand stehen politische Entscheidungen mit Auswirkungen auf die Resilienz des digitalisierten Energiesystems. Unter anderem dient der Prozess dazu, Pfadabhängigkeiten rechtzeitig zu erkennen und auf sie zu reagieren. Außerdem sollten auch Wechselwirkungen zwischen verschiedenen Maßnahmen in den Blick genommen werden, um mögliche negative Effekte zu antizipieren.

Die institutionalisierte Risikobewertung und die Entwicklung von Kenngrößen und Standards zur Resilienzbewertung (Handlungsoption 14) bilden eine wichtige Informationsgrundlage für den übergeordneten Monitoringprozess. Sie sollten daher vor oder zeitgleich mit dem Begleitprozess etabliert werden.

Für die Umsetzung des Begleitprozesses bieten sich verschiedene Modelle an:

- 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 Einbeziehung 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.

Basierend auf den Ergebnissen des Monitorings passen die jeweiligen politischen Entscheidungsgremien die Resilienzstrategie an, indem sie etwa Maßnahmen nachjustieren, ineffektive oder ineffiziente Maßnahmen abschaffen und neue Maßnahmen einführen.

3 Fazit

Die Digitalisierung und die damit einhergehende Transformation des Energiesystems schreiten stetig voran. Zum einen wird Digitalisierung benötigt, um mit den Änderungen im elektrischen Energiesystem durch die fluktuierende Einspeisung aus Windenergie- und Solaranlagen, dezentralen Erzeugungsstrukturen, Elektromobilität sowie neu auftretenden Marktakteuren umzugehen. Andererseits erhöht sich dadurch auch die Komplexität im System. Es treten neue Akteure – auch außerhalb des Systems – auf, die Einfluss auf die Sicherheit des Systems haben können, und es entstehen neue Angriffsflächen und Abhängigkeiten zwischen Strom- und IKT-System. Unvorhergesehene oder sogar unvorhersehbare Ereignisse und Entwicklungen können das elektrische Energiesystem destabilisieren und zu Blackouts führen, mit verheerenden Folgen für die Gesellschaft. Durch eine geeignete Resilienzstrategie kann die Politik den Rahmen setzen, um die gewohnte Zuverlässigkeit der Stromversorgung auch in einem digitalisierten und hochgradig vernetzten, klimafreundlichen Energiesystem weiterhin zu gewährleisten. Dabei sollte insbesondere – wo möglich – das Prinzip „Resilience by Design" angewendet werden, damit Lösungen so konzipiert werden, dass sie die Resilienz erhöhen. So soll Resilienz zur Grundvoraussetzung für technologische oder gesellschaftliche Sicherheitslösungen gemacht werden.[39]

Die hier vorgestellten 15 Handlungsoptionen für eine Resilienzstrategie adressieren Risiken, die durch die fortschreitende Digitalisierung im Zusammenhang mit der Energiewende in den nächsten zwanzig Jahren zu erwarten sind. Da die Umsetzung der Maßnahmen teilweise viel Zeit in Anspruch nimmt – so muss zum Teil zunächst das notwendige Wissen erarbeitet werden –, sollte sie zeitnah angegangen werden. Auch die langlebigen Investitionen in Stromnetze und Erzeugungsanlagen schaffen Pfadabhängigkeiten und erfordern vorausschauendes Handeln. Es sei angemerkt, dass Maßnahmen zur Erhöhung der Resilienz zunächst mit höheren Kosten verbunden sind. Diese Kosten sollten gegen die Kosten aufgewogen werden, die durch große Blackouts entstehen. Für eine konkrete Risikoabschätzung, die eine Maßnahme ins Verhältnis setzt mit der Wahrscheinlichkeit und den Kosten eines vermiedenen Schadens, fehlen Methoden und Daten. Diese Art der Berechnung ist jedoch in der Stromversorgung für die hier betrachteten Fälle auch nicht nötig, da die Kosten der vorgeschlagenen Maßnahmen sehr gering im Verhältnis zu den Schäden eines Blackouts ausfallen. Letztere werden als sehr hoch eingeschätzt, da neben ökonomischen Folgen auch schwerwiegende soziale und ökologische Konsequenzen auftreten können.

Die Maßnahmen adressieren überwiegend Akteure der Energieversorgung. Dabei rücken für die zukünftige Resilienz die heute – in Bezug auf große Blackouts – noch als weniger relevant angesehenen kleinen Akteure, so zum Beispiel Stadtwerke oder Betreiber kleiner Anlagen, gegenüber großen Energieversorgern und ÜNB stärker ins

39 Vgl. acatech 2014, S. 20 und 25.

Blickfeld. Zusätzlich wird für die zukünftige Resilienz die Einbeziehung von Akteuren nötig, die bisher gar nicht oder wenig im Zusammenhang mit der Verursachung, Vermeidung oder Abschwächung von Blackouts in Beziehung gesetzt wurden – etwa Gerätehersteller, Plattformbetreiber, Betreiber von öffentlichen Kommunikationsnetzen, Privathaushalte oder Innenministerien und Polizeibehörden. Für eine effektive Umsetzung vorgeschlagener Handlungsoptionen kann eine Interessenlagenanalyse der jeweils betroffenen und beteiligten Akteure hilfreich sein. Denn diese zukünftig hochrelevanten Akteure wirken auf verschiedenste Weise auf die Resilienz des elektrischen Energiesystems ein. Durch ihre neue Bedeutung für den Betrieb und die Zuverlässigkeit des Systems, durch Schwächung der Cyber-Sicherheit oder durch Veränderungen von simultanem Verhalten: Wenn viele kleine Anlagen gleichzeitig ab- oder zugeschaltet werden, kann das die Stromversorgung destabilisieren.

Die im Zuge der Digitalisierung verstärkte Vernetzung privater Haushalte und die in dieser Stellungnahme thematisierten möglichen Eingriffe der Netzbetreiber zur Systemstabilisierung werfen grundlegende Fragen des **Datenschutzes** auf, die aus rechts- und sozialwissenschaftlicher Sicht kontinuierlich weiterdiskutiert werden müssen. Da diese Fragen die Resilienz nicht direkt betreffen, werden sie in dieser Stellungnahme nicht weiter untersucht, es kommt ihnen aber dennoch eine hohe Relevanz zu.

Die Digitalisierung unserer Lebenswelt verbunden mit einer Energieversorgung im Umbruch erfordert also neue Maßnahmen, um den enormen gesellschaftlichen Schaden durch Blackouts zu vermeiden. Teile der Digitalisierung müssen aktiver gestaltet, neue Akteure müssen zu Beiträgen zur Resilienz verpflichtet, mögliche zukünftige Entwicklungen oder auch Disruptionen müssen rechtzeitig von der Politik antizipiert werden. Hierzu hat die vorliegende Stellungnahme Wege und Strategien aufgezeigt. In welchen Intervallen und mit welcher Geschwindigkeit Maßnahmen künftig angepasst werden müssen, lässt sich heute nicht überall absehen und bleibt daher Aufgabe eines konsequenten Monitorings und Lernens.

Literatur

AbLaV 2016
Verordnung zu abschaltbaren Lasten vom 16. August 2016 (BGBl. I S. 1984), die zuletzt durch Artikel 9 des Gesetzes vom 22. Dezember 2016 (BGBl. I S. 3106) geändert worden ist.

acatech 2014
acatech – Deutsche Akademie der Technikwissenschaften (Hrsg.): *Resilien-Tech. ‚Resilience-by-Design': Strategie für die technologischen Zukunftsthemen* (acatech POSITION), 2014.

acatech/Leopoldina/Akademienunion 2017
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 2016
Agora Energiewende: *Flex-Efficiency - Ein Konzept zur Integration von Effizienz und Flexibilität bei industriellen Verbrauchern*, 2016, URL: https://www.agora-energiewende.de/veroeffentlichungen/flex-efficiency/ [Stand: 15.10.2020]

Agora 2020
Agora Energiewende: *Klimaneutrale Industrie - Schlüsseltechnologien und Politikoptionen für Stahl, Chemie und Zement*, 2020. URL: https://www.agora-energiewende.de/fileadmin2/Projekte/2018/Dekarbonisierung_Industrie/164_A-EW_Klimaneutrale-Industrie_Studie_WEB.pdf [Stand: 15.10.2020]

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.

Aven/Renn 2009
Aven, T./Renn, O.: „The role of quantitative risk assessments 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.

Statistisches Landesamt Baden-Württemberg 2020
Statistisches Landesamt Baden-Württemberg: Gebäude und Wohnungen, 2020. URL: https://www.statistik-bw.de/Wohnen/GebaeudeWohnungen/BW-BT_einfamilienhaeuser.jsp [Stand: 25.09.2020].

BDEW 2017
Bundesverband der Energie- und Wasserwirtschaft (BDEW): Standardlastprofile Strom, 2017. URL: https://www.bdew.de/energie/standardlastprofile-strom/. [Stand: 25.09.2020].

Statistik Berlin Brandenburg 2020
Statistik Berlin Brandenburg: Basisdaten, 2020. URL: https://www.statistik-berlin-brandenburg.de/BasisZeitreiheGrafik/Bas-Mikrozensus.asp?Ptyp=300&Sageb=12011&creg=BBB&anzwer=5, [Stand: 25.09.2020].

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.

BSI 2020-1
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].

BSI/BMWI 2020
Bundesamt für Sicherheit in der Informationstechnik (BSI) und 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, 2020. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/SmartMeter/standardisierungsstrategie.pdf;jsessionid=1CC3BDDCACDA723CE15B04AA0D8F4D66.1_cid503?__blob=publicationFile&v=3 [Stand: 09.07.2020].

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 Verteilernetze für Deutschland (Verteilernetzstudie)*, Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi), 2014.

Europäische Kommission 2019
Europäische Kommission: Communication on The European Green Deal, 2019. URL: https://ec.europa.eu/info/publications/communication-european-green-deal_de [Stand: 03.04.2020].

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.

Statistisches Amt für Hamburg und Schleswig-Holstein 2020
Statistisches Amt für Hamburg und Schleswig-Holstein: *Statistisches Jahrbuch 2019/2020*, 2020, Hamburg 2020. URL: https://www.hamburg.de/contentblob/1005676/e93bee7f01624bcadfd70efe661d6e28/data/statistisches-jahrbuch-hamburg.pdf [Stand: 25.09.2020].

IRGC 2018
International Risk Governance Center (IRGC, Hrsg.): *Guidelines for the Governance of Systemic Risks*, Lausanne: International Risk Governance Center (IRGC) 2018.

Katwala 2019
Katwala, A.: Here's how GCHQ scours Huawei hardware for malicious code, 2019. URL: https://www.wired.co.uk/article/huawei-gchq-security-evaluation-uk [Stand: 26.06.2020].

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.

Mayer/Brunekreeft 2021
Mayer, C./ Brunekreeft, G. (Hrsg.): *Resilienz digitalisierter Energiesysteme. Blackout-Risiken verstehen, Stromversorgung sicher gestalten* (Schriftenreihe Energiesysteme der Zukunft), München, 2021.

Netztransparenz 2019
Netztransparenz: EEG-Anlagenstammdaten 2017, 2019. URL: https://www.netztransparenz.de/EEG/Anlagenstammdaten, [Stand: 19.02.2019].

Petermann et al. 2011
Petermann, T./Bradke, H./Lüllman, A./Poetzsch M./Riehm, U.: *Was bei einem Blackout geschieht: Folgen eines langandauernden und großräumigen Stromausfall*, Berlin: edition sigma 2011.

Piasceck 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]

SmartQuart 2020
SmartQuart: Bredburg – Das elektrische Quartier, 2020. URL: https://smartquart.energy/about/bedburg/ [Stand: 25.09.2020].

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.

Thoma 2014
Thoma, K. (Hrsg.): *Resilien-Tech – "Resilience by Design": a strategy for the technology issues of the future. Acatech STUDY*. Reihenherausgeber: acatech – Deutsche Akademie der Technikwissenschaften, München 2014.

Umweltbundesamt 2015
Umweltbundesamt (Hrsg.): *Potentiale regelbaren Lasten in einem Energieversorgungssystem mit wachsendem Anteil erneuerbarer Energien*, 2015.

Verordnung (EU) 2019/943
Verordnung (EU) 2019/943 des Europäischen Parlaments und des Rates vom 5. Juni 2019 über den Elektrizitätsbinnenmarkt (Neufassung).

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.

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, S. 1–8.

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.

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 und Referenten

Dr. Achim Eberspächer	acatech
Dr. Berit Erlach	acatech
Katharina Bähr	acatech
Dr. Marita Blank-Babazadeh	OFFIS, Oldenburg
Sanja Stark	OFFIS, Oldenburg

Gutachterinnen und Gutachter

Prof. Dr. Frank Eggert	TU Braunschweig
Prof. Dr. Michael Fehling	Bucerius Law School
Prof. Dr. Georg Götz	Justus-Liebig-Universität Gießen
Prof. Dr. Matthias Jarke	RWTH Aachen
Prof. Dr. Johanna Myrzik	Universität Bremen

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.

Die Stellungnahme wurde am 06.11.2020 vom Kuratorium des Akademienprojekts verabschiedet.

Die Akademien danken allen Autorinnen und Autoren sowie den Gutachtern für ihre Beiträge. Die Inhalte der Stellungnahme liegen in alleiniger Verantwortung der Akademien.

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

Deutsche Akademie der Naturforscher Leopoldina e.V. Nationale Akademie der Wissenschaften

Jägerberg 1
06108 Halle (Saale)
Tel.: 0345 47239-867
Fax: 0345 47239-839
E-Mail: leopoldina@leopoldina.org

Berliner Büro:
Reinhardtstraße 14
10117 Berlin

acatech–Deutsche Akademie der Technikwissenschaften e.V.

Karolinenplatz 4
80333 München
Tel.: 089 520309-0
Fax: 089 520309-9
E-Mail: info@acatech.de

Hauptstadtbüro:
Pariser Platz 4a
10117 Berlin

Union der deutschen Akademien der Wissenschaften e.V.

Geschwister-Scholl-Straße 2
55131 Mainz
Tel.: 06131 218528-10
Fax: 06131 218528-11
E-Mail: info@akademienunion.de

Berliner Büro:
Jägerstraße 22/23
10117 Berlin

Die Nationale Akademie der Wissenschaften Leopoldina, acatech – Deutsche Akademie der Technikwissenschaften und die Union der deutschen Akademien der Wissenschaften unterstützen Politik und Gesellschaft unabhängig und wissenschaftsbasiert bei der Beantwortung von Zukunftsfragen zu aktuellen Themen. Die Akademiemitglieder und weitere Experten sind hervorragende Wissenschaftlerinnen und Wissenschaftler aus dem In- und Ausland. In interdisziplinären Arbeitsgruppen erarbeiten sie Stellungnahmen, die nach externer Begutachtung vom Ständigen Ausschuss der Nationalen Akademie der Wissenschaften Leopoldina verabschiedet und anschließend in der *Schriftenreihe zur wissenschaftsbasierten Politikberatung* veröffentlicht werden.

Schriftenreihe zur wissenschaftsbasierten Politikberatung
ISBN: 978-3-8047-4224-6