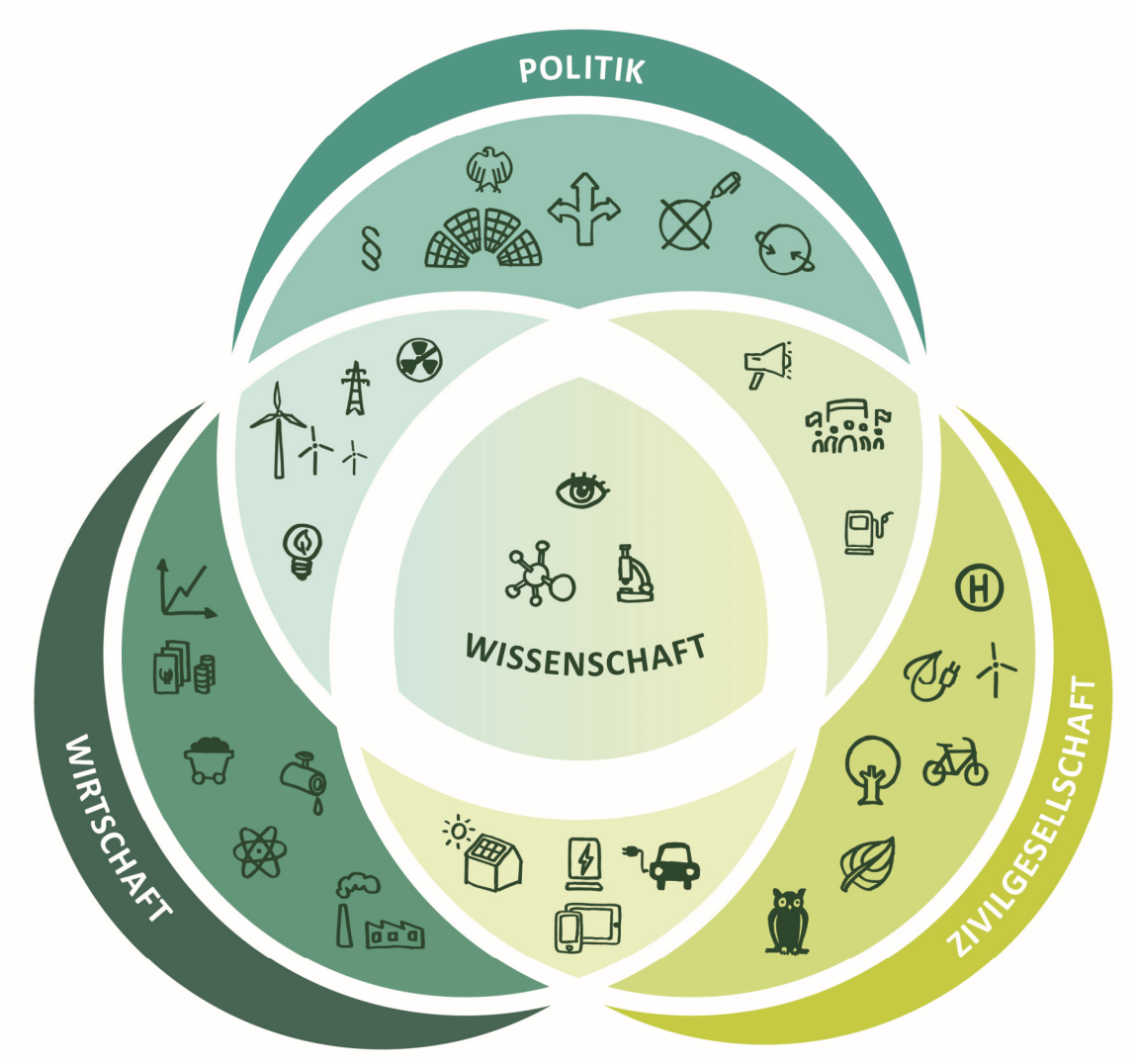
HUMBOLDT-VIADRINA
Governance Platform

Bericht ETR/01-2018

Risiken smart managen. Wie schaffen wir robuste digitale Energieinfrastrukturen?

Prof. Dr. Gesine Schwan, Katja Treichel und Sarah Schmauk



Bericht zum Trialog® am 14. Dezember 2017

Risiken smart managen.

Wie schaffen wir robuste digitale Energieinfrastrukturen?

Prof. Dr. Gesine Schwan, Katja Treichel und Sarah Schmauk

Die HUMBOLDT-VIADRINA Governance Platform gGmbH

Die HUMBOLDT-VIADRINA Governance Platform gGmbH ist eine gemeinnützige Gesellschaft, die sich für die Förderung von demokratischen Prozessen und durchdachten Governance-Strategien in Deutschland, Europa und der Welt einsetzt. Unser Beitrag zu Good Governance konzentriert sich insbesondere auf die Grundprinzipien Transparenz und Partizipation. Mit unseren Multi-Stakeholder-Initiativen und Trialogen entwickeln wir Verfahren mit dem Anspruch, möglichst viele Perspektiven zu integrieren und sie transparent zu machen. Denn nur über Transparenz und Partizipation sind die Berücksichtigung aller Stakeholdergruppen und die daraus resultierende Stärkung von Vertrauen in politische Entscheidungsprozesse möglich.

Über das Projekt

Im April 2013 haben acatech – Deutsche Akademie der Technikwissenschaften, die Nationale Akademie der Wissenschaften Leopoldina und die Union der deutschen Akademien der Wissenschaften das interdisziplinäre Projekt „Energiesysteme der Zukunft“ (ESYS) gestartet. Rund 100 Expertinnen und Experten aus Wissenschaft sowie unternehmensseitiger Forschung erarbeiten seitdem wissenschaftlich fundierte Handlungsoptionen für die Gestaltung einer sicheren, bezahlbaren und nachhaltigen Energieversorgung. Um die Positionen unterschiedlicher Stakeholder einbeziehen zu können, tauschen sich die ESYS-Arbeitsgruppen in verschiedenen Dialogformaten mit Vertreterinnen und Vertretern der Politik, Wirtschaft und organisierten Zivilgesellschaft aus. Die Trialoge der HUMBOLDT-VIADRINA Governance Platform werden dazu genutzt, neue Themen aus verschiedenen Perspektiven zu beleuchten und Fragestellungen im Hinblick auf ihre gesellschaftliche Anschlussfähigkeit zu schärfen.

Empfohlene Zitierweise: HUMBOLDT-VIADRINA Governance Platform (2018): „Risiken smart managen. Wie schaffen wir robuste digitale Energieinfrastrukturen?“ Bericht ETR/01-2018 von Schwan, Gesine; Treichel, Katja; Schmauk, Sarah zum Trialog vom 14.12.2017.

INHALTSVERZEICHNIS

EXECUTIVE SUMMARY

Thema und Hintergrund

Am 14. Dezember 2017 fand der siebte Trialog in Kooperation mit dem Projekt „Energiesysteme der Zukunft“ (ESYS) statt, der sich mit dem Thema „Risiken smart managen. Wie schaffen wir robuste digitale Energieinfrastrukturen?“ befasste.

Der Umbau des Energiesystems schreitet voran: immer mehr Erzeugungsanlagen speisen Strom aus erneuerbaren Energiequellen in das Netz. In 2016 wurden 31,7 Prozent des Stromverbrauchs durch erneuerbare Energiequellen gedeckt. Damit die wetterbedingt schwankenden Einspeisungen weiterhin mit dem Verbrauch koordiniert und auf verschiedene Netzebenen verteilt werden können, bedarf es verstärkt Informations- und Kommunikationstechnologien (IKT). Unter der Digitalisierung der Energiewende wird demnach der notwendige breite Einsatz von IKT verstanden, um Einspeisung, Verbrauch und Netze zu steuern sowie kritische Situationen zu erkennen und zu beheben. Gleichzeitig macht die IKT das Energiesystem aber auch verletzlicher, da durch die Vernetzung aller Komponenten ein gezielter Cyberangriff oder Störfall auch zu flächendeckenden Stromausfällen oder einem Blackout führen könnte.

Ziel des Trialogs war, zusammen mit den Stakeholdern aus Politik und Verwaltung, organisierter Zivilgesellschaft, Wirtschaft und Wissenschaft zu diskutieren, wie die Digitalisierung kritischer Energieinfrastrukturen gestaltet werden kann, um zum einen deren Vorteile nutzbar zu machen und zum anderen neue Risiken zu managen. Im Fokus standen dabei die Fragen, welche Chancen sich durch die zunehmende Vernetzung für Unternehmen sowie private Haushalte ergeben und welche Risiken und Herausforderungen entstehen können. Die Anregungen aus der Diskussion fließen in den weiteren Arbeitsprozess des Projekts „Energiesysteme der Zukunft“ wie bspw. das Fachgespräch im zweiten Quartal 2018.

Ausgangspunkt für die Diskussion bildeten ein Impulspapier der Mitglieder des Akademienprojekts „Energiesysteme der Zukunft“ (siehe Annex IV) sowie vier Leitfragen die hier zusammengefasst sind:

- Welche neuen Risiken entstehen durch die Digitalisierung kritischer Energieinfrastrukturen? Welche Rolle spielt dabei eine wachsende Bedrohungslage von außen, z. B. durch Cyberattacken?
- Welche Voraussetzungen müssen Gesetzgeber und Behörden schaffen, damit Energieinfrastrukturen wirksam und sicher digitalisiert werden können? Welche Regelungen und Gesetze, aber auch Instrumente wie ein Monitoring digitaler Risiken werden nötig?
- Welche Chancen für Unternehmen und deren Geschäftsmodelle entstehen durch die Digitalisierung von Energieinfrastrukturen, insbesondere in Bezug auf deren Sicherheit?
- Verändert die digitale Energiewende die Rolle und den Stellenwert privater Haushalte für das Gesamtsystem? Welche neuen

Verantwortlichkeiten können hier entstehen und wird z. B. ein „Cyber-Sicherheits-Führerschein“ nötig?

Teilnehmende

An der Trialog-Veranstaltung im Allianz Forum in Berlin nahmen insgesamt 49 Vertreterinnen und Vertreter aus Politik und Verwaltung, der Wirtschaft, der organisierten Zivilgesellschaft sowie der Wissenschaft und den Medien teil. Durch die Einbettung des Trialogs in das wissenschaftliche Projekt ESYS war die Wissenschaft mit 13 Personen vertreten. Teilnehmende Institutionen waren z.B. das Institut für ökologische Wirtschaftsforschung (IÖW), das Wissenschaftszentrum Berlin für Sozialforschung (WZB), das OFFIS-Institut für Informatik und die Stiftung Wissenschaft und Politik (SWP).

Einen etwas größeren Anteil (18 Personen) stellte bei diesem Trialog die Stakeholdergruppe Wirtschaft. Vertreten waren große Unternehmen aus den Bereichen Energieversorgung und -erzeugung (EnBW; Vattenfall, innogy se) sowie Beratung (Ecofys, Strategieberatung Neue Mobilitätssysteme). Ebenfalls nahmen diverse Organisationen und Verbände aus dem IT- und Digitalisierungsbereich, wie die STROMADAO UG, VHP Ready - Virtual Heat and Power, Webolution GmbH, Gnosis und der Digitalverband Bitkom sowie ein Vertreter der Siemens AG teil.

Die organisierte Zivilgesellschaft wurde u.a. durch die Verbraucherzentrale Bundesverband, den Chaos Computer Club (CCC) und den Deutschen Gewerkschaftsbund (DGB) mit insgesamt sieben Personen vertreten. Aus dem politischen Bereich kamen neun Vertreterinnen und Vertreter des Bundesministeriums für Wirtschaft und Energie, der Energie.Agentur.NRW, dem Deutschen Institut für Normung (DIN) und dem Umweltbundesamt (UBA). Die Medien waren durch eine Redakteurin des Tagesspiegels und das Fachmedium BIZZenergy vertreten.

Ergebnisse

Im Trialog wurde deutlich, dass die Digitalisierung des Energiesystems „janusköpfig“ ist: Sie hilft die Komplexität eines transformierten, stärker dezentralen und wetterabhängigen Stromsystems zu beherrschen; kann aber auch Risiken, bspw. durch Manipulation, Cyberangriffe oder fehlerhafte Anwendungen, steigern.

Nichtsdestotrotz sah die Mehrheit der Teilnehmenden die weitere Digitalisierung eines zunehmend dezentralen, erneuerbaren Energiesystems für wichtig an, um die Versorgungssicherheit aufrecht zu erhalten und die Erneuerbaren weiter auszubauen. Neben der Versorgungssicherheit spielen aber auch andere Dimensionen von Sicherheit eine Rolle: IT-Sicherheit, Daten- und Investitionssicherheit sowie Rohstoffsicherheit – sie müssen als Zielkanon im Blick behalten werden. Sicherheitskonzepte, die eine kurzfristige oder sektorielle Perspektive einnehmen und weder die Breitenwirkungen noch die Interdependenzen beachten, sind nicht zielführend. Für eine durchdachte und nachhaltige Sicherheit muss ein Sektor überschreitendes Verständnis, also ein integrierter

Ansatz entwickelt werden. Ebenfalls dürfen bei der Betrachtung des Gesamtsystems und der Möglichkeiten der Weiterentwicklung nicht die vorhandenen Pfadabhängigkeiten vernachlässigt werden, ebenso wie der internationale Kontext. Denn die gegenwärtige Transformation ist gekennzeichnet durch eine neue Generation an Technologien, die sich langsam durchsetzen sowie alten Technologien, die noch im System sind. Das hat zur Folge, dass es einen Konflikt zwischen dezentralen technischen Möglichkeiten und vorhandenen zentralen Systemverantwortungs- sowie Machtstrukturen gibt.

Im Rahmen der Diskussion wurde ein zunächst vorgestellter Demokratisierungsansatz durch die Dezentralisierung des Energiesystems weitestgehend verworfen, u.a. mit der Begründung, dass die Etablierung von dezentralen Erzeugungsanlagen nicht automisch zu dezentralen Entscheidungsstrukturen führt. Jedoch konnte ein „Aktivierungspotenzial“ der Dezentralisierung und Digitalisierung festgehalten werden: das Thema Energie wird weit in die Gesellschaft hineingetragen und es existieren viele neue Teilhabeoptionen für die Verbraucher, Prosumer und Unternehmen. Bezogen auf die Steuerung des Energiesystems wurde ein Mittelweg zwischen Dezentralität und Zentralität gefordert. Ein Vorschlag war, über Anreizstrukturen die wirtschaftlichen Entscheidungen zum Energiemanagement und zur Digitalisierung von Einheiten in der Größenordnung oberhalb privater Haushalte mit zu beeinflussen. Somit könnte ein Fundament von Versorgungssicherheit geschaffen werden, indem z.B. Stadtwerke durch Sektorkopplung selbstständig einen Minimalbetrieb aufrechterhalten können, ohne einen großen Austausch eingehen zu müssen. Auch spielt hier allgemeiner der Umgang mit Sicherheitsvorkehrungen hinein: was ist uns Sicherheit wert und wieviel sind wir bereit dafür zu zahlen?

Zum Thema Faktor Mensch und der Frage nach seiner zukünftigen Rolle im Energiesystem im Vergleich zu automatisierten Prozessen kamen die Teilnehmenden darüber ein, dass es in Zukunft beides geben wird: Menschliche Verantwortung und Algorithmen im Dienste des Menschen. Dabei wurde bemängelt, dass es bisher zu wenig gute Programmierer und zu wenige speziell auf die Digitalisierung ausgerichtete Berufe in der Energiewirtschaft gibt. Eine Empfehlung war daher, dass Ausbildungen in der Energiewirtschaft mit einer stärkeren digitalen Komponente ergänzt werden sollten. Zusätzlich sollte es weitaus mehr Schulungen und Fortbildungen für Personal geben, damit den neuen Herausforderungen der Verbindung von menschlicher Verantwortung und Algorithmen entsprechend begegnet werden kann.

Im Trialog wurde zudem festgehalten, dass Sicherheitsstandards helfen können, einen Großteil, jedoch nicht alle Probleme abzudecken. Gemeinsame Standards wurden als ökonomisch nützlich angesehen, da sie die Vernetzung untereinander erleichtern können (z.B. durch gleiche Komponenten, Plug-and-Play). Zum anderen können durch Standards Veränderungen flächendeckender an die Masse kommuniziert werden (z.B. durch Updates). Das grundlegende Spannungsverhältnis von Standards im Sinne von vorab definierten Strukturen versus flexiblen Anforderungen in besonderen Situationen konnte nicht aufgelöst werden.

Im Bereich der IT-Sicherheit wurden folgende Punkte als richtungsweisende Ansätze für eine resiliente digitale Energieinfrastruktur genannt:

- Es sollte mehr Austausch über Probleme, bemerkte Angriffe oder Schadsoftware geben.
- Im IT-Bereich können Risiken dadurch eingedämmt und Resilienz geschaffen werden, indem die Komplexität von Softwaresystemen (höhere Modularität und Nachvollziehbarkeit) verringert und mehr Qualitätssicherung betrieben wird.
- Daran anschließend sollte Dezentralität unterstützt werden: viele unterschiedliche Systemkomponenten, die einander vollständig kompensieren können und möglichst geringe gegenseitige Abhängigkeiten haben (Vermeidung von single-points-of-failures).
- Gestützt auf den IT-Security Lifecycle wurde ein Umdenken im Bereich des Risikomanagements gefordert. Systeme sollten unter der Annahme entwickelt werden, dass „etwas passieren“ könne.
- Trotz Komplexität von IT-Themen ist der Dialog mit der Gesellschaft wichtig, gerade im Energiebereich. Es muss eine gemeinsame Sprache gefunden werden, um nicht nur zu technologischen Entscheidungen zu gelangen, sondern auch zu gesellschaftlich und politisch tragfähigen.

Trialoge

Die Trialoge der HUMBOLDT-VIADRINA Governance Platform sind ganztägige Veranstaltungen. Sie organisieren eine gemeinwohlorientierte Verständigung von Stakeholdern aus Politik und Verwaltung, Unternehmen und organisierter Zivilgesellschaft begleitet von Wissenschaft und Medien zu aktuellen gesellschaftspolitischen Themen. Die Trialoge bringen ein möglichst breites Spektrum an kontroversen gesellschaftlichen Positionen und Ideen zusammen. Mit der Chatham House Rule und einer fairen Moderation schaffen sie eine vertrauliche und zugleich offene Atomsphäre zwischen den Teilnehmenden. So können eine Vielzahl von Standpunkten und Ideen Eingang in die Diskussion finden – unabhängig von divergierenden Machtpositionen. Diese Perspektivenvielfalt bietet die Chance, breit getragene Grundkonsense zu ermitteln.

In den transdisziplinären Trialogen rückt die Wissenschaft stärker in den Mittelpunkt, da ihre Forschungsarbeit und jeweilige Implikationen den Fokus der Diskussion bilden. Die Wissenschaft erhält durch den Austausch mit gesellschaftlichen Akteuren eine Rückkopplung zu ihrer Arbeit und die Teilnehmenden aus den verschiedenen Stakeholdergruppen gewinnen neue Einsichten und Perspektiven. So wird durch das Zusammenbringen von wissenschaftlich-analytischer Forschung, gesellschaftlichem Erfahrungswissen und gesellschaftspolitischen Entscheidungs- und Problemlösungsanforderungen eine breite Basis der Erkenntnisse hergestellt, die Perspektivenwechsel und breitere Verständigungsprozesse ermöglicht. Dieses transdisziplinäre Dialogformat trägt langfristig zu einer gesteigerten gesellschaftlichen Anschlussfähigkeit der Forschungsergebnisse, robustem Gesellschaftswissen sowie besser informierten politischen Entscheidungen bei.

1 Beschreibung der Trialog-Veranstaltung

1.1 Hintergrund

Im April 2013 haben acatech – Deutsche Akademie der Technikwissenschaften, die Nationale Akademie der Wissenschaften Leopoldina und die Union der deutschen Akademien der Wissenschaften das **interdisziplinäre Projekt „Energiesysteme der Zukunft" (ESYS)** gestartet. Rund 100 Expertinnen und Experten aus Wissenschaft sowie unternehmensseitiger Forschung erarbeiten seitdem wissenschaftlich fundierte Handlungsoptionen für die Gestaltung einer sicheren, bezahlbaren und nachhaltigen Energieversorgung. Um die Positionen unterschiedlicher Stakeholder einbeziehen zu können, tauschen sich die ESYS-Arbeitsgruppen in verschiedenen Dialogformaten mit Vertreterinnen und Vertretern der Politik, Wirtschaft und organisierten Zivilgesellschaft aus. Die Trialoge der HUMBOLDT-VIADRINA Governance Platform werden dazu genutzt, neue Themen aus verschiedenen Perspektiven zu beleuchten und Fragestellungen im Hinblick auf ihre gesellschaftliche Anschlussfähigkeit zu schärfen.

Anknüpfend an die ESYS-Arbeitsgruppe „Risiko und Resilienz", welche sich grundsätzlich mit Fragen einer gesicherten Versorgung im Energiesystem befasste[1], möchte sich das Projekt ESYS auch mit speziellen Fragen einer sicheren Digitalisierung des Energiesystems auseinandersetzen. Auftakt hierzu bildete der Trialog, dessen Ergebnisse in einem Fachgespräch vertieft werden.

Als inhaltliche Vorbereitung für den Trialog wurde allen Teilnehmenden ein Impulspapier der ESYS-Mitglieder Dr. Achim Eberspächer, Prof. Sebastian Lehnhoff und Dr. Christoph Mayer zur Verfügung gestellt, in dem die wichtigsten Entwicklungen sowie mögliche Handlungsbedarfe aufgezeigt wurden. Zusätzlich dienten vier Fragen als **Leitfaden für die Diskussion**:

- Welche neuen Risiken entstehen durch die Digitalisierung kritischer Energieinfrastrukturen? Welche Rolle spielt dabei eine wachsende Bedrohungslage von außen, z. B. durch Cyberattacken?
- Welche Voraussetzungen müssen Gesetzgeber und Behörden schaffen, damit Energieinfrastrukturen wirksam und sicher digitalisiert werden können? Welche Regelungen und Gesetze, aber auch Instrumente wie ein Monitoring digitaler Risiken werden nötig?
- Welche Chancen entstehen für Unternehmen und deren Geschäftsmodelle durch die Digitalisierung von Energieinfrastrukturen, insbesondere in Bezug auf deren Sicherheit?

[1] Renn, Ortwin (Hrsg.): Das Energiesystem resilient gestalten: Szenarien – Handlungsspielräume – Zielkonflikte (Schriftenreihe Energiesysteme der Zukunft), München 2017

- Verändert die digitale Energiewende die Rolle und den Stellenwert privater Haushalte für das Gesamtsystem? Welche neuen Verantwortlichkeiten können hier entstehen und wird z. B. ein „Cyber-Sicherheits-Führerschein“ nötig?

1.2 Ziele des Trialogs

Ziel des Trialogs war es, eine Diskussion über die Gestaltungsmöglichkeiten einer digitalen Energieinfrastruktur sowie die damit zusammenhängenden Chancen und Risiken zu führen. Der Trialog sollte einen Rahmen schaffen, im dem sich Akteure aus Wissenschaft und Gesellschaft auf Augenhöhe begegnen. All diese Akteure sind **Wissens- und Erfahrungsträger** und bringen zugleich ihre eigenen Logiken in die Diskussion ein. Die Wissenschaftlerinnen und Wissenschaftler des Akademienprojekts ESYS konnten im Trialog zu einem sehr frühen Zeitpunkt in ihrer Arbeitsphase einen Überblick über die verschiedenen gesellschaftlichen Perspektiven und den Stand der gesellschaftlichen Diskussionen erhalten. Die Teilnehmerinnen und Teilnehmer aus den Stakeholdergruppen Politik und Verwaltung, Wirtschaft, organisierte Zivilgesellschaft und Medien bekamen einen Überblick über die aktuellen Entwicklungen im Bereich der digitalen Energieinfrastrukturen und erhielten die Möglichkeit, Anliegen, Interessen und Erfahrungen in die wissenschaftliche Debatte einzubringen. Dabei werden die Teilnehmerinnen und Teilnehmer auch angehalten, nicht nur ihre Positionen vorzutragen, sondern diese auch zu begründen. Der **transdisziplinäre Austausch** soll den Teilnehmenden dazu verhelfen, andere Perspektiven anzunehmen, was für eine *echte* Verständigung notwendig ist. Ein wichtiges Element dabei ist, eine gemeinsame, für alle verständliche Sprache zu finden.

> *„Wir haben gelernt und wir lernen, dass es immer verschiedene Sichten auf eine Sache gibt und, dass die Vielfalt der Perspektiven die Chance bietet, nicht einseitig, nicht tunnelorientiert zu sein und auf diese Weise auch zu besseren Lösungen zu kommen, weil man mehr Dinge berücksichtigt hat.“*
> | ZIVILGESELLSCHAFT

Im Ergebnis soll der Trialog die gesellschaftliche Anschlussfähigkeit der wissenschaftlichen Arbeit stärken, insbesondere bei der Formulierung der Analysen und Stellungnahmen sowie zur Herausstellung relevanter Punkte innerhalb großer Themenkomplexe. Der Austausch und die Verständigung der verschiedenen Stakeholder kann so zur **Akzeptanz der Ergebnisse** beitragen. Weiterführende Informationen zum Konzept der Trialoge und zum Akademienprojekt Energiesysteme der Zukunft finden Sie im Annex I.

1.3 Auswahl der Inputgebenden

Dem Trialog-Format entsprechend wurden die Inputgebenden entlang der Stakeholder-Zuordnung eingeladen. Der Anspruch bestand nicht darin, dass die Inputgebenden alle vermeintlichen Gemeinwohlinteressen vertreten, sondern im Gegenteil, dass sie durchaus ihre Teilperspektiven vorstellen, die auch im Gegensatz zueinander oder zu den Positionen von Teilnehmerinnen und Teilnehmer aus anderen Stakeholder-Gruppen stehen können. Überschneidungen zwischen den Sektorenvertretern sind möglich und auch erwünscht, um zu Grundkonsenskorridoren zu gelangen. Diese sind wiederum essentiell, um das überparteiliche Ziel der Energiewende gemeinwohlorientiert und effektiv umzusetzen.

Die **inhaltliche Einführung** in das Thema gab Herr Prof. Sebastian Lehnhoff. Er ist Vorstand von OFFIS – Institut für Informatik und Professor für Energieinformatik an der Carl von Ossietzky Universität Oldenburg. Anschließend folgten Inputvorträge von Vertreterinnen und Vertretern der Stakeholdergruppen. Zu Beginn gab es einen Input aus der **Wirtschaft** von Frau Friederike Ernst, COO von Gnosis und Generalsekretärin des Blockchain Bundesverbands. Sie gab eine kurze Einführung in die Funktionsweise der Blockchain-Technologie und stellte den Bezug zum Energiesektor her. Als Vertreter der **organisierten Zivilgesellschaft** sprach Herr Linus Neumann vom Chaos Computer Club (CCC) über Sicherheit in kritischen Infrastrukturen, ihre Schwachstellen und Möglichkeiten, wie diese eingedämmt werden können. Zuletzt gab Herr Alexander Kleemann, der im Referat Netzregulierung im Bundesministerium für Wirtschaft und Energie tätig ist (**Politik und Verwaltung**), einen Einblick in die Entstehung und die Inhalte des Gesetzes zur Digitalisierung der Energiewende.

2 Analyse des Trialogs

2.1 Auswertung und Überblick

Die qualitative Auswertung der transkribierten Diskussion erfolgte angelehnt an die **dokumentarische Methode** nach Ralf Bohnsack[2], eine etablierte Methode der qualitativen Sozialforschung, die insbesondere für die Auswertung von Gesprächen mit mehreren Personen angewandt wird. Mit diesem Verfahren kann eine tiefergehende Interpretation des Materials erreicht werden, als bei einer Interpretation ausschließlich entlang des Diskussionsverlaufs. Die diskutierten Themen können schließlich gebündelt dargestellt und prägnante Aussagen zitiert werden.

[2] Bohnsack, Ralf (2008): Rekonstruktive Sozialforschung, Einführung in qualitative Methoden, Opladen/ Farmington Hills.

Die vorliegende Analyse trägt die verschiedenen Aspekte, Verständnisse und Diskurse der Trialog-Veranstaltung systematisch zusammen. Der **Aufbau des Berichts** orientiert sich an den in der Auswertung des Transkripts **identifizierten Themenbereichen**:

- Entwicklung und Herausforderungen des digitalen Energiesystems
- Dezentralität und Digitalisierung
- Dimensionen von Sicherheit
- Faktor Mensch im System
- Zusammenarbeit für mehr Sicherheit

Diese Themenbereiche werden mit den dazugehörigen Argumenten beleuchtet und ausgewertet. Aus den Ergebnissen kann ein Sachstand der Diskussion zwischen den vertretenen Stakeholdern erarbeitet werden. Daraus lässt sich ein gesellschaftlicher Grundkonsenskorridor ableiten, aber auch Fragen und Gesichtspunkte, die der weiteren Vertiefung durch die Wissenschaftlerinnen und Wissenschaftler bedürfen. Die Ergebnisse zeigen die wichtigsten Punkte der gesellschaftlichen Debatte auf, die in den politischen Handlungsempfehlungen der Wissenschaftlerinnen und Wissenschaftler zum Thema berücksichtigt werden sollten.

2.2 Hintergrund zum digitalen Energiesystem

Das Energiesystem befindet sich im Wandel – nicht nur hinsichtlich der Erzeugung und der Energiequellen, sondern auch in Bezug auf dessen Steuerung, die zunehmend digitalisiert wird. Auf dem Trialog wurden die derzeitigen Entwicklungen des digitalen Energiesystems aufgezeigt sowie mögliche Handlungsbedarfe skizziert.[3] Dabei waren zwei Aussagen zentral als Grundannahme für die Diskussion. Zum einen wurde festgestellt, dass die Digitalisierung alle betrifft, besonders im Rahmen der Energiewende. Strom und Digitalisierung verhalten sich dabei wie Siamesische Zwillinge: **Ohne Strom keine Digitalisierung und ohne Digitalisierung kein Strom**. Zum anderen wurde konstatiert, dass die Digitalisierung für das Energiesystem "janusköpfig" ist. Sie hilft die Komplexität eines transformierten, stärker dezentralen und wetterabhängigen Stromsystems zu beherrschen, kann aber auch Risiken, bspw. durch Manipulation, Cyberangriffe oder fehlerhafte Anwendungen, steigern.

Die gegenwärtige Transformation ist gekennzeichnet durch eine neue Generation an Technologien, die sich langsam durchsetzen sowie alten Technologien, die noch im System sind. Die alten Technologien beruhen auf Makrophänomenen, die große Kraftwerke mit Skaleneffekten hervorgebracht haben sowie zentrale ökonomische Strukturen und Entscheidungssysteme. Auf diese eher zentralen Strukturen wurde eine IT-Struktur aufgesetzt, über

[3] Für weitere Informationen siehe: Eberspächer, Achim/Lehnhoff, Sebastian/Mayer, Christoph (2017): Risiken smart managen. Wie schaffen wir robuste digitale Energieinfrastrukturen? (Impulspapier für den Trialog).

die jetzt immer mehr dezentrale Erzeugungspunkte eingebunden werden. Am Beispiel Photovoltaik lässt sich das gut veranschaulichen: die produzierende Einheit ist kein großes Kraftwerk mehr, sondern auf einer vergleichsweise mikroskopischen Ebene. Das Gleiche gilt für den Übergang von der Elektromechanik hin zur halbleiterbasierten Leistungselektronik, die die Basis für die komplette neuere Steuerungstechnik in den Netzen ist. **Das hat zur Folge, dass es technologische Möglichkeiten gibt, die dezentrale technische Lösungen ermöglichen, die sich jedoch an Systemverantwortungs- und Machtstrukturen stoßen, die mit den alten Technologien gewachsen sind**.

Es ist folglich wichtig zu unterscheiden, was konkret zentral oder dezentral ist bzw. werden soll und, wo die jeweiligen **Verantwortlichkeiten und Entscheidungsstrukturen** liegen. Die Erzeugung findet zunehmend dezentral statt und es existieren teilweise neue Besitzstrukturen. Das bedeutet jedoch nicht und hat auch nicht zwangsläufig zur Folge, dass dadurch auch die Verantwortlichkeiten, z.B. für die Versorgungssicherheit, dezentral organisiert sind oder, dass dezentrale Technologien dominieren. Im Trialog wurde der Vergleich von Smartphones angebracht, die nur auf wenigen Betriebssystemen basieren, obwohl fast jeder ein Smartphone besitzt. Auch bei der Digitalisierung des Energiesystems ist es vorstellbar, dass es nur zwei, drei große Hersteller gibt, die die Kommunikation und Sicherheit der Anlagen gestalten.

Hervorgehoben wurde hierbei nochmals die Schwierigkeit, dass sowohl die Erzeugung als auch die Verteilung und der Verbrauch derzeit neu organisiert werden. Dies stellt neue Herausforderungen an die IT-basierten Managementsysteme des Stromsystems, die größtenteils noch nicht erfüllt werden (z.B. beim Thema Cyber-Sicherheit). Trotz dieser Veränderungen müssen aber Netzstabilität und Versorgungssicherheit gewährleistet werden.

Eine weitere Herausforderung der Transformation ist die **Geschwindigkeit, mit der die Digitalisierung voranschreitet**. Diese bringt zwar viele neue Optionen mit sich. Aber selbst diejenigen, die sich tagtäglich mit diesen neuen Technologien befassen, haben Schwierigkeiten den Überblick über die Anwendungsbereiche und Sicherheitsanforderungen zu behalten. Es existieren unzählige Gabelungen, an denen weitergeforscht, aber auch reguliert werden kann oder müsste. Hinzu kommt, dass sich der Großteil der Gesellschaft nur wenig unter der digitalisierten Energiewende vorstellen kann. Während alle Menschen mehr oder weniger auf Energie und Digitalisierung angewiesen sind, kennen sich die wenigsten damit aus. Für viele Generationen kam der Strom „einfach nur aus der Steckdose“.

Die **Entwicklung hin zum aktiven Konsumenten**[4] **oder gar Prosumer**[5] **sowie zu einer vermehrten Nutzung smarter Geräte steht noch am Anfang**. Jedoch wurde während der Diskussion unterstrichen, dass trotz der vergleichsweise geringen Zahl von Prosumern (in Deutschland eine Million von etwa 40 Millionen Haushalten), die etwa 1 % zur Energieerzeugung beitragen, ihre Vorreiterrolle durchaus bedeutsam ist. Durch sie werden neue Konzepte ausprobiert und entwickelt, welche wichtige Implikationen für die Gesellschaft mit sich bringen.

Prosumer

Ein Prosumer ist ein „Konsument, der gleichzeitig einen Teil der konsumierten Produkte oder Dienstleistungen selber produziert". Im Energiesystem produzieren Prosumer einen Teil ihrer konsumierten Energie selbst. Zu den Prosumern gehören z. B. Hausbesitzer mit einem Solarpanel auf dem eigenen Dach, Mieter, die den Mieterstrom einer Solaranlage verbrauchen oder auch die BürgerInnen, die an Windkraftanlagen beteiligt sind (vgl. Fußnote 5).

Aktive Konsumenten

Neben den Prosumern (oder Prosumenten) ermöglichen digitale Technologien aber auch allen nicht produzierenden Konsumenten, eine aktivere Rolle im Energiesektor einzunehmen bspw. durch Car-Sharing, Stromtarifwahl, Smart-Metering und intelligente Haushaltgeräte. Das Gesetzespaket der Europäischen Kommission „Saubere Energie für alle Europäer" möchte die aktive Rolle der Verbraucher stärker unterstützen.

Allerdings reicht es nicht aus, den Sachstand und die Diskussion um die Digitalisierung des Energiesystems alleine in Deutschland zu verfolgen. Neben den Übergängen von der alten zur neuen Energiewelt in Deutschland bestehen in Europa ganz unterschiedliche Strukturen in den einzelnen Mitgliedstaaten. Langfristig müssen diese jedoch alle **im europäischen Verbundnetz durch entsprechende Technologien sicher miteinander kommunizieren**. Neben dem Wunsch einen gemeinsamen Binnenmarkt für Strom wirtschaftlich zu ermöglichen, muss der Sicherheitsgedanke im Rahmen der fortschreitenden Digitalisierung eine wichtige Rolle in der Weiterentwicklung des Binnenmarkts spielen. Dazu zählen Standards, die nicht nur den Smart-Meter-Roll-Out betreffen, hier jedoch bereits ihren wichtigen Anfang haben. Gerade durch seine Größe, Komplexität und die Dynamik der Ausbreitungseffekte zählt das europäische Stromsystem zu einer der herausforderndsten kritischen Infrastrukturen.

[4] Siehe z.B. Europäische Kommission (2016): Anhang. Maßnahmen zur Beschleunigung der Umstellung auf saubere Energie. COM(2016) 860 final, abrufbar unter: http://eur-lex.europa.eu/resource.html?uri=cellar:fa6ea15b-b7b0-11e6-9e3c-01aa75ed71a1.0003.02/DOC_3&format=PDF

[5] Zum Thema Prosumer siehe Flaute, Markus/Großmann, Anett/Lutz, Christian (2016): Gesamtwirtschaftliche Effekte von Prosumer-Haushalten in Deutschland (GWS Discussion Paper 2016/5), abrufbar unter http://www.gws-os.com/discussionpapers/gws-paper16-5.pdf

2.2.1 Begriffe im Wandel: Robustheit und Resilienz als Leitbilder

Neben Umweltverträglichkeit und Wirtschaftlichkeit stellt die Versorgungssicherheit eines der drei wichtigsten energiepolitischen Ziele Deutschlands dar. Die Versorgungssicherheit in Deutschland ist bisher eine der besten in Europa mit einem SAIDI-Wert[6] im Strombereich von 12,8 Minuten/Jahr.[7]

Robustheit

Der Begriff Robustheit kommt aus dem Lateinischen (robustus, von robur Hart-, Eichenholz) und wird verwendet als „standhaltend gegenüber Einwänden und neuen Ereignissen". Robustheit ist im Wesentlichen die Fähigkeit, einer Aufgabe oder Versorgung nachzukommen oder die Qualität dieser Aufgabe zu erhalten, auch bei veränderten Umgebungs- und Eingangsparameter. Im elektrischen Energieversorgungssystem bedeutet das, dass die **Frequenz des Stromnetzes erhalten bleibt** und der Verbraucher Strom mit definierter Spannung aus der Steckdose bekommt, **unabhängig davon wie stark der Wind weht oder wie kräftig die Sonne scheint**. Hierbei kommt dem sog. N-1-Prinzip eine wichtige Rolle zu: das System muss so aufgebaut sein, dass wesentliche Elemente im System einmal ausfallen dürfen, ohne dass dies zu Versorgungsunterbrechungen führt. So kann die Versorgungsqualität aufrechterhalten werden, sollte eine wesentliche Komponente (Kraftwerk, Leitung, Transformator) ausfallen.

System Average Interruption Duration Index (SAIDI-Index)

Der SAIDI-Index wird als Indikator für die Zuverlässigkeit von Energienetzen verwendet. Er stellt die durchschnittliche Ausfalldauer je versorgtem Verbraucher da und wir in Zeiteinheiten gemessen.

Berechnet wird der Index indem die Summe aller Versorgungsunterbrechungen durch die Gesamtzahl aller Verbraucher geteilt wird:

$$\mathrm{SAIDI} = \frac{\sum U_i N_i}{N}$$

N_i stellt dabei die Anzahl der von der Unterbrechung betroffenen Verbraucher in einem Gebiet (Ortsteil, Stadt) und U_i die Dauer der Unterbrechungen dar (vgl. Fußnote 6).

Mit den neuen Risiken eines digitalisierten Stromsystems, wie Hackerangriffe, ist das N-1-Kriterium als ein klassischer Robustheitsmechanismus nur noch bedingt haltbar, weil es nicht auf vernetzte IT-Systeme übertragbar ist. Es müssen neue Ansätze überlegt werden und auch die Möglichkeit, ob ggf. Qualitätsengpässe kurzfristig hingenommen werden können, um bspw. wichtige Infrastrukturen zu schützen und so das Gesamtsystem dennoch resilient zu gestalten.

[6] Für weitere Informationen siehe https://de.wikipedia.org/wiki/System_Average_Interruption_Duration_Index

[7] Bundesnetzagentur (2018): Kennzahlen der Versorgungsunterbrechungen Strom, abrufbar unter https://www.bundesnetzagentur.de/DE/Sachgebiete/ElektrizitaetundGas/Unternehmen_Institutionen/Versorgungssicherheit/Versorgungsunterbrechungen/Auswertung_Strom/Versorgungsunterbrech_Strom_node.html

Resilienz

Der Begriff Resilienz kommt aus der ersten Hälfte des 19. Jahrhunderts und wurde in der Werkzeugmechanik das erste Mal verwendet. Er beschreibt die Anforderung an Werkzeuge und Materialien nicht spröde, sondern stabil zu sein, aber auch nicht zu fest, sondern rückfedernd, so dass sie bei einem härteren Schlag weder zerbröseln noch kaputtgehen. Übertragen auf das Energiesystem bedeutet das, dass die **Versorgungsqualität kurzfristig beeinträchtigt sein darf, aber dann auch sehr schnell – wenn das eigentliche Störereignis vorbei ist und behoben wurde – das System wieder die ursprüngliche Qualität der Versorgungssicherheit liefert**. Damit geht Resilienz über den Robustheitsbegriff hinaus und bietet die Möglichkeit, Systeme unter den neuartigen Einflüssen der Digitalisierung zu steuern.

Resilienz ist die Fähigkeit eines Systems, seine Funktionsfähigkeit unter Belastung aufrechtzuerhalten beziehungsweise kurzfristig wiederherzustellen.

Zu beachten ist jedoch, dass sich **Resilienz auf das Gesamtsystem bezieht**: die Digitalisierung ist nur ein Aspekt. Neben dem Energiesystem als Primärsystem als solchem gibt es das IKT-System und die Märkte. Gibt es Probleme bei einem dieser Teile, muss das Gesamtsystem dennoch funktionieren. In der Diskussion wurde u.a. die Frage aufgeworfen, ob sowohl die globale System-Resilienz als auch die lokale Resilienz immer bestehen muss oder, ob es denkbar wäre, dass manche Regionen „vom System genommen werden", um das Gesamtsystem oder wichtige Regionen stabil zu halten. Unstrittig war hingegen, dass Digitalisierung durch intelligente Algorithmen und hochautomatisierte Entscheidungsprozesse das Potenzial hat, Resilienz in sehr kurzen Zeitbereichen zu realisieren, um bestimmte Ereignisse abzufedern.

2.2.2 Cyberangriffe und Stromausfälle

„Krisenmanagement beginnt, wenn das Kind am Rand des Brunnens turnt, und nicht erst, wenn es im Brunnen liegt."
| ZIVILGESELLSCHAFT

In der Vergangenheit gab es bereits Probleme aufgrund von Schadsoftware und Cyber-Angriffen auf diverse digitalisierte Infrastrukturen. Im Trialog wurden Beispiele aus verschiedenen Ländern genannt:

Deutschland 2015

Im Mai 2015 wurden mehrere Angriffe auf den Deutschen Bundestag entdeckt. Betroffen waren mindestens 16 Abgeordnetenbüros sowie das Büro der Bundeskanzlerin. Es wurden Postfächer kopiert, Festplatten ausspioniert und es wurden interne sowie vermutlich auch

vertrauliche Daten entwendet. Zurückzuführen waren die Angriffe höchstwahrscheinlich auf eine Einheit des russischen Militärgeheimdienstes, genannt „Fancy Bear“.[8]

Von einem Teilnehmenden wurde darauf hingewiesen, dass der Angriff auf den deutschen Bundestag wie auch häufig bei andere Cyber-Attacken durch **Social Engineering** erfolgt ist. Das bedeutet, das hinter einer augenscheinlich offiziellen E-Mail mit Anhang Schadsoftware in das System gelangt, sobald der Anhang von dem Empfänger geöffnet wird. Durch das Öffnen des E-Mail-Anhangs gelangt dann die Schadsoftware in das System.

Ukraine 2015

Im Dezember 2015 kam es in der Ukraine zu einem Stromausfall, von dem 700.000 Haushalte betroffen waren. Auch hier kamen sog. **SpearPhishing-E-Mails** zum Einsatz, die Mitarbeiter der ukrainischen Stromverteilnetzbetreiber dazu bewegten, schadhafte E-Mail-Anhänge zu öffnen, wodurch Schadsoftware in die Systeme gelangen konnte. Durch die schädliche Fernwartungssoftware wurden die Hochspannungsleiter der Umspannwerke und Schaltanlagen geöffnet, was unmittelbar zum Ausfall der Stromversorgung bei den Betroffenen geführt hat. Gleichzeitig wurden die Überwachungssysteme der Netzstellen abgeschaltet, so dass die Störung nicht feststellbar war. Weitere Elemente verdeutlichen das Ausmaß der Risiken: Auch die Telefonanlage wurde konzernweit lahmgelegt, so dass Störungsmeldungen, die zu einer raschen Fehlerklärung hätten führen können, verhindert wurden. Schließlich wurden Daten auf den Rechnern gelöscht und das Betriebssystem unbrauchbar gemacht sowie die Firmware überschrieben, so dass ein Wiederherstellen der Funktionsbereitschaft erheblich erschwert und verzögert wurde. D.h. es gab einen kombinierten Angriff auf das elektrische Energieversorgungssystem und auf Informations- und Kommunikationsstrukturen, so dass die Versorgung für mehrere Stunden unterbrochen war und eine Wiederherstellung nur unter erschwerten Bedingungen möglich war.[9]

Im Trialog wurde angemerkt, dass die Berichterstattung zu dieser Cyberattacke sehr überzogen gewesen sei. Aus Sicht eines Programmierers war nicht die Cyberwaffe kompliziert, sondern nur gut versteckt und der Angriff gut koordiniert.

Deutschland 2016

Nur wenig später machte ein Computervirus im schwäbischen Atomkraftwerk Gundremmingen Schlagzeilen. Der Virus fiel bei den Vorbereitungen von Revisionen in Block B des

[8] Für weitere Informationen siehe z.B. Patrick Beuth et.al (2017): Bundestags-Hack. Merkel und der schicke Bär auf Zeit-Online, abrufbar unter: http://www.zeit.de/2017/20/cyberangriff-bundestag-fancy-bear-angela-merkel-hacker-russland

[9] Für weitere Informationen siehe z.B. Bundesamt für Sicherheit in der Informationstechnik (2016): Die Lage der IT-Sicherheit in Deutschland 2016, Bonn, abzurufen unter https://www.bsi-fuer-buerger.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2016.pdf?__blob=publicationFile&v=5 oder Piotr Heller (2016): Die Hackerdämmerung, abrufbar unter http://www.faz.net/aktuell/wissen/physik-mehr/ukrainischer-stromausfall-war-ein-hacker-angriff-14005472.html

Atomkraftwerks auf und es gab diverse Spekulationen, wie der Virus in das System geraten war, da der betroffene Computer nicht mit dem Internet verbunden war. Betroffen war ein IT-System, das zu einer Brennelement-Lademaschine gehört. Diese Maschinen werden eingesetzt, um verbrauchte Brennelemente zwischen dem Reaktor und einem Lagerbecken zu transportieren. Später stellte sich heraus, dass die Schadsoftware über einen USB-Stick in das System gelangt sein muss.

Zwar gab es bei dem Fall kein bedeutendes Sicherheitsrisiko, er zeige aber laut einem Teilnehmenden besonders gut, dass **das Konzept von Sicherheit nicht einzig darauf ausgelegt sein sollte, dass nichts und niemand in ein System eindringen kann**.

Ukraine 2016

Im Dezember 2016 fiel in Teilen der ukrainischen Hauptstadt Kiew für knapp 75 Minuten der Strom aus. IT-Sicherheitsexperten sind sich einig, dass der Stromausfall durch Hacker herbeigeführt wurde, die monatelang Zugriff auf das Netzwerk eines Umspannwerkes hatten. Die **Schadsoftware war demnach spezifisch auf Industrieanlagen ausgerichtet** und konnte die Stromzufuhr aus der Ferne kappen. Sie nennen die Schadsoftware "Industroyer", eine Wortschöpfung aus "Industrie" und "Destroyer", dem englischen Wort für Zerstörer. Das Besondere an der Schadsoftware ist, dass sie nicht der Spionage dient. Sie wurde speziell dafür programmiert, Arbeitsprozesse von industriellen Kontrollsystemen, in diesem Fall das Steuerungssystem des Umspannwerkes, zu unterbrechen.[10]

Weltweit 2017

Es begann am Abend des 12. Mai 2017 mit Meldungen aus Großbritannien, dass zahlreiche Rechner des National Health Service von WannaCry[11] befallen sind. Im Anschluss daran folgten weltweit Meldungen über weitere Angriffe. So stoppte Renault den Betrieb in einigen Werken in Frankreich, in Spanien und Portugal waren die großen

WannaCry

ist eine Ransomware, die Daten auf den infizierten Computern verschlüsselt. Um den Code für die Entschlüsselung zu erhalten, sind die Betroffenen aufgefordert eine Lösegeldsumme in Bitcoin zu bezahlen. Ansonsten sei die Löschung der Daten veranlasst (siehe Fußnote 11).

[10] Für weitere Informationen siehe ESET (2017): WIN32/INDUSTROYER. A new threat for industrial control systems, abrufbar unter https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf oder Uli Ries (2017): Industroyer. Diese Malware soll Stromnetze angreifen. http://www.spiegel.de/netzwelt/web/industroyer-diese-malware-soll-stromnetze-angreifen-a-1151774.html

[11] Bundesamt für Sicherheit in der Informationstechnik (2016): Die Lage der IT-Sicherheit in Deutschland 2017, S. 23, abzurufen unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.pdf;jsessionid=2A139EB5ABA56F61F67327E266CD2AB5.2_cid369?__blob=publicationFile&v=4

Netzbetreiber Telefónica und Telecom betroffen, in den USA das Logistikunternehmen FedEx und in Deutschland fielen die Anzeigesysteme der Deutschen Bahn aus. WannaCry verbreitete sich via E-Mail (Social Engineering) und versuchte, sobald er ein System infiziert hatte wie ein Wurm andere Rechner im gleichen Netz zu kompromittieren.[12] Besonders anfällig für WannaCry waren veraltete Rechner mit Windows-Versionen, die keine aktuellen Sicherheitsupdates hatten.

Deutschland 2018

Der neuste zu verzeichnende Angriff wurde im Februar 2018 öffentlich, nachdem er intern bereits seit Dezember 2017 bekannt war. Erneut haben es Hacker auf die politischen Institutionen Deutschlands abgesehen. Konkretes Ziel des Hacker-Angriffs war das Datennetz der Bundesverwaltung, der Informationsverbund Berlin-Bonn (IVBB). Der IVBB gilt als stärker gesichert als das Netzwerk des Bundestages (vgl. Angriff Deutschland 2015).[13] Es wurde erneut eine Schadsoftware eingeschleust, durch welche wiederum Daten erbeutet wurden. Der Angriff konnte nach Aussagen des Bundesinnenministeriums isoliert und unter Kontrolle gebracht werden. Aller Wahrscheinlichkeit nach lag der Angriff schon ein ganzes Jahr zurück, bis er im Dezember 2017 entdeckt wurde.[14] Laut des früheren Bundesinnenministers de Maizière ändert jedoch auch der aktuelle Angriff nichts an der Tatsache, dass Deutschland mit dem IVBB „eines der sichersten Regierungsnetzwerke der Welt“[15] besitzt.

Stromausfälle im Energiebereich

Die Digitalisierung bringt, wie oben beispielhaft ausgeführt, neue Risiken mit sich. Im Mittelpunkt der Diskussion stehen mögliche Cyberangriffe auf digitalisierte Energieinfrastrukturen und die daraus resultierende Gefahr eines großflächigen Blackouts. Doch auch vor der zunehmenden Digitalisierung gab es bereits eine Reihe von Stromausfällen weltweit, die mitunter durch intelligente Kommunikationsinfrastrukturen hätten verhindert werden können (siehe Tabelle). Der **Stromausfall in Europa 2006 wurde von den Teilnehmenden als ein wichtiges Beispiel dafür hervorgehoben.**

[12] Für weitere Informationen siehe Bundesamt für Sicherheit in der Informationstechnik (2017): Die Lage der IT-Sicherheit in Deutschland 2017, S.26, abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.pdf?__blob=publicationFile&v=4

[13] Siehe auch Ferdinand Otto et. al (2018): Angriff unter Kontrolle, Angreifer unbekannt, auf Zeit-Online, abrufbar unter http://www.zeit.de/digital/datenschutz/2018-03/bundesregierung-hackerangriff-kontrolle-sofacy-group-it-sicherheit

[14] Für weitere Informationen siehe Bundeswehr Journal (2018): Lange geplant: Hacker-Angriff auf das Datennetz des Bundes, abrufbar unter http://www.bundeswehr-journal.de/2018/lange-geplant-hacker-angriff-auf-das-datennetz-des-bundes/#more-8752

[15] Vgl. Bundesministerium des Inneren, für Bau und Heimat (2018): „Deutschland hat mit dem IVBB eines der sichersten Regierungsnetzwerke der Welt!“, abrufbar unter https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2018/03/statement-cyberangriff-ivbb.html

Tabelle 1: Größere Stromausfälle in Europe

Wann?	Wo?	Was ist passiert?	Grund
2003	Schweden/ Dänemark	In Südschweden und Dänemark fiel im September 2003 der Strom aus. 3,5-5 Millionen Menschen hatten ca.7 Stunden keinen Strom. Es gab zahlreiche Unfälle infolge ausgefallener Ampelanlagen, Eisenbahnen standen still und Telefone waren außer Betrieb. Ausgelöst wurde der Stromausfall durch zwei Kraftwerksdefekte, die eine Kettenreaktion auslösten	Kraftwerksdefekte
2004	Athen	In Athen und Umgebung kam es im Juli 2004 zu einem stundenlangen Stromausfall. Die Ursache für den Stromausfall war ein sogenannter Spannungskollaps. Grund für diese Entwicklung dürfte die steigende elektrische Last durch die zunehmende Klimatisierung sein. Kleinklimaanlagen sind dadurch gekennzeichnet, dass sie einen hohen Bedarf an Blindleistung aufweisen.	Spannungskollaps aufgrund zu geringer Blindleistungseinspeisung
2005	Schweiz	Aufgrund von Bauarbeiten musste die der Schweizerischen Bundesbahnen (SBB) zwei Stromleitungen abschalten. Dabei ging man bei der SBB davon aus, dass die noch zur Verfügung stehende Leitung mehr belastet werden könnte, als tatsächlich der Fall war. Doch aufgrund von Überbelastung setzte eine Schutzabschaltung ein. Damit war der Stromtransport Richtung Norden komplett abgeschnitten. Im Tessin entstand eine Überbelastung, weil der Strom nicht mehr weitergeleitet werden konnte. Dadurch wurde das Netz in zwei Teile geteilt: Während sich im Süden die Kraftwerke wegen fehlender Last abschalteten, fehlten in der restlichen Schweiz rund 200 MW. Die beiden Leitungen aus Deutschland konnten die fehlende Leistung nicht ausgleichen, so dass sich auch die restlichen Kraftwerke wegen Überlast abschalteten.	Überlast, falsches Leistungsmanagement
2006	Europa	Um 22:09 Uhr kam es zu einem größeren Stromausfall in Europa. Teile von Deutschland, Frankreich, Belgien, Italien, Österreich, Spanien waren teilweise bis zu 120 Minuten ohne Strom. Auslöser war die planmäßige zeitweilige Abschaltung einer von E.ON betriebenen 380-kV-Hochspannungsleitung am Abend des 4. November 2006 für die Ausschiffung des Kreuzfahrtschiffs Norwegian Pearl.	Geplante Abschaltung einer Hochspannungsleitung
2015	Niederlande	Nach einer Überlastung kam es im Umspannwerk Diemen südöstlich von Amsterdam zu einer Überlastung. Weite Teile der Stadt sowie der Flughafen Schiphol blieben in der Folge für etwas mehr als eine Stunde ohne Strom.	Technischen Fehler in Hochspannungsstation
2015	Türkei	Wegen starker Schwankungen durch den Ausfall mehrerer Kraftwerke im Stromnetz des Landes wurde die Netzkopplung mit dem europäischen Verbundsystem getrennt. In der Folge konnten 80 von 81 Provinzen des Landes nicht mehr mit elektrischer Energie versorgt werden. 76 Millionen Menschen blieben für neun Stunden ohne Strom.	Ausfall mehrerer Kraftwerke

2.2.3 Digitalisierung eines bestehenden Energiesystems – Chancen und Grenzen

Die Energiewende mit ihren vielen dezentralen Erzeugungs- und Verbrauchsanlagen, von denen ein Großteil abhängig von der Wetterlage in das System einspeist, ist ohne Digitalisierung nicht mehr machbar. Bis vor einigen Jahren gab es knapp hundert Kraftwerke in Europa, die aktiv geregelt wurden und die Versorgungsqualität und -sicherheit gewährleistet haben. In Zukunft wird es eine **Anzahl von aktiven Anlagen im mehrstelligen Millionenbereich allein in Deutschland geben, die einen direkten Einfluss auf die Versorgungsqualität haben werden**. Das sind Zahlen, Steigerungen, Größenordnungen, die jenseits der Skalierbarkeit konventioneller Technologien in diesem Bereich sind. Das bedeutet wiederum, dass mit anderen digitalen, intelligenten Systemen gearbeitet werden muss, die den menschlichen Bediener und die Systeme sowie die Systemführung unterstützen. Von den Teilnehmenden wurde mehrfach betont, dass **die zukünftigen Systeme so komplex sein werden, dass sie die Möglichkeiten eines Menschen, kurzfristige und systemrelevante Entscheidungen zu treffen, übersteigen**.

Die Energiewende gekoppelt mit der Digitalisierung ermöglicht nicht nur neue Erzeugungsstrukturen, sondern über die Sektorkopplung auch neue Verbrauchs- und Verteilungsstrukturen. Das ist auch für größere Betriebe interessant, da es verschiedene Strategien gibt, sich am Markt zu bewegen – wann biete ich am Markt etwas an, wann speichere den Strom? Die Digitalisierung ermöglicht eine dezentrale Steuerung von Erzeugung und Verbrauch, aber die Schnittstellen zwischen den Akteuren und die Entscheidungskompetenzen müssen klar geregelt sein. Darüber hinaus können Anreizstrukturen die wirtschaftlichen Entscheidungen der Akteure am Netz beeinflussen. Es sollte also nicht darum gehen, jede einzelne Erzeugungsanlage im Detail zu steuern, sondern auch lokale Möglichkeiten der Steuerung zu nutzen: „**Wenn das Stadtwerk durch Kopplung verschiedener Möglichkeiten selber einen Minimalbetrieb aufrechterhalten kann, ohne großen Austausch einzugehen, dann ist das ein Fundament von Sicherheit im System. Und was wir zusätzlich regeln müssen, sind die Austauschverhältnisse. Was für Sicherheitsmargen bringen wir da an?"** (Wirtschaft).

Nicht nur für die Unternehmen, auch für die Verbraucherinnen und Verbraucher schafft die Digitalisierung neue Möglichkeiten. Sie können z.B. als Prosumer zu Erzeugern am Markt werden oder variable Tarife nutzen. Auch Car-Sharing und die Elektromobilität verändern die Rolle der Verbraucherinnen und Verbraucher. Sie werden durch die Digitalisierung zu einem relevanten Teil und Akteur des Energiesystems.

Ein Teilnehmer betonte, dass trotz Dynamik und Geschwindigkeit der Digitalisierung Technologien wie bspw. Blockchain zunächst auf ihre Qualität und Nützlichkeit zu prüfen sind, bevor sie eingesetzt werden. In Bezug auf das Energiesystem sollte der Anspruch sein, dass

neue Technologien die Qualität der Versorgungssicherheit erhöhen im Vergleich zum Status Quo. Aufgrund der neuen Rahmenbedingungen im Energiesystem ist dieser Anspruch nicht immer einfach überprüfbar. Zustimmung fand dabei die Aussage, dass die Qualität der Vernetzung des Energiesystems die Grundlage für das tägliche Leben sei.

Ebenfalls wurde die These diskutiert, ob eine verbesserte Resilienz im elektrischen Energieversorgungssystem nur dann erreicht werden kann, wenn die **Funktionen des Backups und der Systemstabilität ebenfalls digitalisiert werden**. Begründet wurde die These damit, dass die Sicherheitsmechanismen so reaktiv sein müssen wie die Schnelligkeit und Präzision der Dynamik, mit der solche Ereignisse eintreten können. Nur durch die Digitalisierung ist es möglich entsprechend schnell und selektiv einzugreifen in der Art, in der auch die Störungen und Bedrohungslagen auftreten. Durch die Kopplung von Netzsteuerung und Kommunikation kann folglich die Resilienz erhöht werden.

Neben all den Chancen, die durch die Vernetzung der Informations- und Kommunikationstechnik mit der Steuerung im Netz verbunden sind, wurden auch problematische Aspekte aufgezeigt. **Die IKT bietet auf der einen Seite die Möglichkeit, Messfehler im System und Fehlverhalten von einzelnen Komponenten zu erkennen. Auf der anderen Seite kann die IKT auch fehlerhafte Informationen einspeisen und damit auch wieder zur Instabilität beitragen**. Betont wurde, dass diese Aspekte bedacht werden müssen, wenn IKT-Systeme miteinander verknüpft werden. Hierbei gilt es zu unterscheiden zwischen systemkritischen Teilen und weniger systemkritischen Teilen.

Mehrfach betonte die Teilnehmerschaft, dass durch die Kombination von dezentraler Erzeugung, Digitalisierung, Speicherung und Sektorkopplung neue Gestaltungsspielräume eröffnet werden. Voraussetzung dafür ist **eine adäquate Marktkommunikation**, damit alle Akteure – auch die, die neu in das System hineinkommen – sich miteinander abstimmen können. Nur so kann die Systemsicherheit und -stabilität auch gewährleistet werden, trotz der gestiegenen Vielfalt an Akteuren.

Gleichwohl kann das Energiesystem in Deutschland und Europa **aufgrund vorhandener Pfadabhängigkeiten nicht komplett neu aufgesetzt werden**. Es gibt aus vielerlei Gründen Grenzen der Gestaltbarkeit, da bereits existierende Infrastrukturen und technologische Systeme sehr viel Kapital binden. Anders ist das in Ländern wie z.B. Indien oder in Afrika, wo es weniger zentrale Infrastrukturen gibt und viele neue Systeme tatsächlich „auf der grünen Wiese“ dezentral geplant und umgesetzt werden können.

2.2.4 Rechtliche Grundlagen des digitalen Energiesystems

Trotz der Unwägbarkeiten und neuen Risiken, die mit der Digitalisierung in das Energiesystem kommen, war sich die Mehrheit der Teilnehmenden darüber einig, dass **die Komplexität der Energiewende nur durch die Digitalisierung bewerkstelligt werden kann**. Als eine

aktuelle politische Maßnahme zur Gestaltung der Energiewende wurde das Gesetz zur Digitalisierung des Energiesystems auf dem Trialog näher besprochen.

Hintergrund des Gesetzes zur Digitalisierung der Energiewende

Im Jahr 2006 formulierte die Richtlinie 2006/32/EG des Europäischen Parlaments und des Rates über Endenergieeffizienz und Energiedienstleistung erstmals Forderungen an die Mitgliedstaaten nach individuellen Zählern, die den „tatsächlichen Energieverbrauch und die tatsächliche Nutzungszeit“ für die Verbraucher wiedergeben (Richtlinie 2006/32/EG, Artikel 13, Absatz 1).[16]

RICHTLINIE 2009/72/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES
vom 13. Juli 2009 über gemeinsame Vorschriften für den Elektrizitätsbinnenmarkt und zur Aufhebung der Richtlinie 2003/54/EG

ANHANG I (2) Die Mitgliedstaaten **gewährleisten, dass intelligente Messsysteme eingeführt werden,** durch die **die aktive Beteiligung der Verbraucher am Stromversorgungsmarkt** unterstützt wird. Die Einführung dieser Messsysteme kann einer wirtschaftlichen Bewertung unterliegen, bei der alle langfristigen Kosten und Vorteile für den Markt und die einzelnen Verbraucher geprüft werden sowie untersucht wird, welche Art des intelligenten Messens wirtschaftlich vertretbar und kostengünstig ist und in welchem zeitlichen Rahmen die Einführung praktisch möglich ist. […]

Die Mitgliedstaaten oder die von ihnen benannten zuständigen Behörden sorgen für die Interoperabilität der Messsysteme, die in ihrem Hoheitsgebiet eingesetzt werden, und tragen der Anwendung der entsprechenden Normen und bewährten Verfahren sowie der großen Bedeutung, die dem Ausbau des Elektrizitätsbinnenmarkts zukommt, gebührend Rechnung.

(vgl. Fußnote 17)

Am 13. Juli 2009 folgte die Richtlinie 2009/72/EG des Europäischen Parlaments und Rates über gemeinsame Vorschriften für den Elektrizitätsbinnenmarkt und zur Aufhebung der Richtlinie 2003/54/EG.[17] Die Mitgliedsstaaten wurden darin aufgefordert, Infrastrukturen für den Aufbau von Smart Metern zu schaffen. Als zeitliche Zielvorgabe wurde ein nationaler Rollout von intelligenten Zählern bis zum Jahr 2020 empfohlen, der auf Basis einer positiven Wirtschaftlichkeitsanalyse mindestens 80 Prozent aller Verbraucher bzw. der in der Analyse empfohlenen Verbrauchergruppe umfassen soll.[18]

[16] Richtlinie 2006/32/EG, abrufbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32006L0032&from=DE
[17] Richtlinie 2009/72/EG, abrufbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32009L0072&from=DE
[18] Bundesnetzagentur (2018): Gesetz zur Digitalisierung der Energiewende, abrufbar unter https://www.bundesnetzagentur.de/DE/Sachgebiete/ElektrizitaetundGas/Unternehmen_Institutionen/Mess-undZaehlwesen/Mess-undZaehlwesen/Smart_Metering/Smart_Metering_node.html

Gesetz zur Digitalisierung der Energiewende

Der europäische Impuls zum Smart-Meter-Rollout ging nach Aussage eines Teilnehmenden zwar in die richtige Richtung, doch in der Ausführung fehlte es aus deutscher Sicht an Sicherheitsanforderungen. Deshalb wurde am 4. November 2015 vom Bundeskabinett der vom Bundesministerium für Wirtschaft und Energie vorgelegte Regierungsentwurf für das Gesetz zur Digitalisierung der Energiewende[19] beschlossen.

„Smart-Meter-Gateways, wie sie aktuell von der deutschen Bundesregierung anvisiert sind, haben viel Potenzial, brauchen aber auch die entsprechenden Sicherheitsstandards. Dieses Potenzial einerseits und die Sicherheit andererseits in ein Produkt zu bringen, stellt eine technologische Herausforderung dar." | POLITIK

Es sieht die stufenweise Einführung des Einbaus und des Betriebs intelligenter Messsysteme bei gleichzeitigen technischen Mindestanforderungen vor, welche Datenschutz und Datensicherheit gewährleisten. Ein wesentlicher Bestandteil des Gesetzes ist das Messstellenbetriebsgesetz (MsbG)[20]. Dieses regelt das Mess- und Zählwesen in Deutschland umfassend neu und ist seit dem 2. September 2016 in Kraft. Neben den allgemeinen Regelungen zur Durchführung des Messstellenbetriebs für Strom- und Gas, enthält es hauptsächlich Vorgaben für den Rollout von intelligenten Messsystemen und modernen Messeinrichtungen.[21]

Das Gesetz zur Digitalisierung der Energiewende ist in Zusammenarbeit mit der Branche entstanden und möchte Vorgaben für intelligente Netze machen und Grundsätze schaffen: **Privacy und IT-Security by Design**. Die Smart-Meter-Technik ist demnach mit Elementen der IT-Security sowie des Datenschutzes ausgestattet und soll ein Grundpfeiler für die Digitalisierung und ein smartes Netz sein.

Auf dem Trialog wurden Visionen besprochen, wie die Zukunft mit Hilfe intelligenter Netze aussehen könnte: so müsste bspw. der Nutzer eines Elektrofahrzeugs nicht mehr manuell nach einer freien Ladestation suchen, sondern das System meldet ihm die nächste freie Station in seiner näheren Umgebung. Dabei spielt Sicherheit eine entscheidende Rolle. Wenn andererseits in einem solchen System die Ladeinfrastruktur gehackt und ein ungewolltes Laden und Entladen aller angeschlossenen Elektromobile programmiert werden

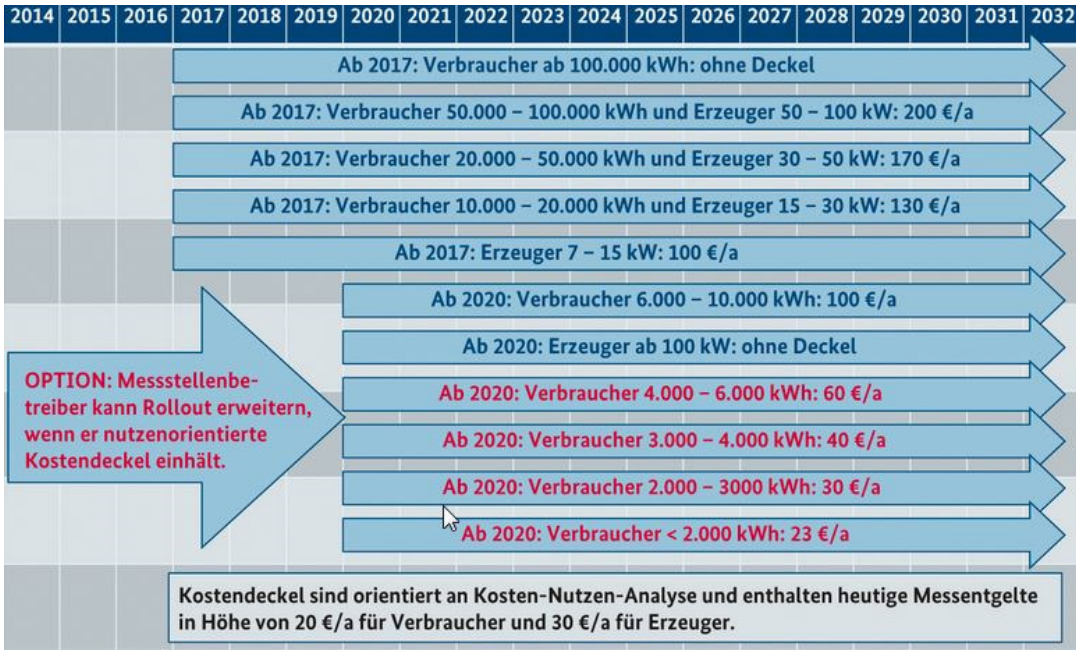
[19] Vgl. Bundesministerium für Wirtschaft und Energie (2016): Gesetz zur Digitalisierung der Energiewende, abrufbar unter https://www.bmwi.de/Redaktion/DE/Downloads/Gesetz/gesetz-zur-digitalisierung-der-energiewende.pdf?__blob=publicationFile&v=4

[20] Vgl. Messstellenbetriebsgesetz (MsbG), abrufbar unter http://www.gesetze-im-internet.de/messbg/MsbG.pdf

[21] Vgl. Bundesnetzagentur (2018): Gesetz zur Digitalisierung der Energiewende, abrufbar unter https://www.bundesnetzagentur.de/DE/Sachgebiete/ElektrizitaetundGas/Unternehmen_Institutionen/Mess-undZaehlwesen/Mess-undZaehlwesen/Smart_Metering/Smart_Metering_node.html#doc488076bodyText1

würde, hätte das enorme systemische Auswirkung. Entsprechend geht es bei der Gestaltung der Smart-Meter-Gateways um langfristig funktionelle und sichere Kommunikationseinheiten.

Wer ist _ab wann_ vom Rollout intelligenter Messsysteme betroffen?



Quelle: Bundesnetzagentur (2018): Gesetz zur Digitalisierung der Energiewende, abrufbar unter https://www.bundesnetzagentur.de/DE/Sachgebiete/ElektrizitaetundGas/Unternehmen_Institutionen/Mess-undZaehlwesen/Mess-undZaehlwesen/Smart_Metering/Smart_Metering_node.html

Solche und ähnliche Sachverhalte in der Summe sind zukünftig zudem relevant für die Stabilität des Energieversorgungssystems und müssen sicher gestaltet sein. Das war der grundlegende Impuls für die Entwicklung der im Gesetz genannten Smart-Meter-Gateways. Sie stellen die Kommunikationsplattformen für ein intelligentes Energienetz dar. Neben dem Ziel der Sicherstellung der Energieversorgung steht zudem ein wirtschaftliches Ziel, welches mit der Hoffnung verbunden ist, dass zahlreiche Dienstleistungen von der Technik profitieren können.

2.2.5 Zukünftige Herausforderungen

Im Zuge der digitalen und energiewirtschaftlichen Transformation wird **die Energieversorgung zu einem cyber-physischen System**[22], in dem zahlreiche Wechselwirkungen stattfinden – zwischen Technik, Markt, Kommunikation und weiteren Bereichen. Die Wechselwirkungskomplexität in diesem System nimmt zu und kann derzeit wissenschaftlich weder modelliert noch simuliert werden.Von den Teilnehmenden wurde betont, dass dadurch viele Folgen nicht absehbar sind und das System an sich noch nicht begreifbar ist. Die besondere Herausforderung besteht demnach darin, den **höheren Vernetzungsgrad in seiner Komplexität sinnvoll zu analysieren.**

Cyber-physische Systeme (CPS)

„[…] bestehen aus vernetzen Maschinen, Geräten und sonstigen Objekten, die kontinuierlich Daten austauschen. Neben der Kommunikation zwischen Menschen mithilfe von Geräten tritt nun auch die Kommunikation zwischen Geräten. Die Technologie der CPS führt zu einer Verschmelzung der physischen und der virtuellen Welt und ist damit insbesondere für das produzierende bzw. verarbeitende Gewerbe relevant“ (vgl. Fußnote 22).

So ist es durchaus denkbar, dass bestimmte Funktionen und Sachverhalte im Energiesystem, die bisher problemlos vonstattengingen, aufgrund komplexer Wechselwirkungen, plötzlich versagen, weil sie mit anderen Sachverhalten, die für sich alleine genommen funktionieren, interagieren. Neben den Risiken durch Cyber-Angriffen liegt demnach auch eine Gefahr in der Vernetzung der unterschiedlichen Einheiten sowie technischer Fehler. **Als Beispiel wurde ein Speicher genannt, der vom Stromzähler abhängt, um sich aufzuladen. Fällt der Stromzähler aus, könnte der Speicher annehmen, es sei kein Strom am Hauptzähler. Also zieht er sich voll. Wenn so eine Situation gleichzeitig mit vielen Speichern auftritt, bricht das Verteilnetz zusammen. „Da brauche ich keinen Hacker**" (Wirtschaft).

„Da habe ich ganz viele sicherheitsrelevante Aspekte, wo ich noch nicht einmal einen Hacker für brauche. Einfach wie Module zusammenarbeiten oder nicht zusammenarbeiten und dann netzwerkmäßige Folgeaspekte entstehen, die nicht antizipiert werden können und die ein ganzes System zum Einsturz bringen können.“ | WIRTSCHAFT

Es wird erkennbar, dass eine weitere Herausforderung darin besteht, bereits jetzt Regeln für ein bisher nicht modellierbares System vorzugeben. Dabei muss damit gerechnet werden, dass Fehler unterlaufen. Entsprechend sollten die **Vorgaben nicht starr sein, sondern sollten ein agiles System und den entsprechenden Rahmen schaffen**.

[22] Vgl. Rottmann, Oliver/Kilian, Maike (2015): Digitalisierung in der Energiewirtschaft – Bedeutung, Treiber und Handlungsoptionen für die Energieversorger. Eine deskriptive Studie zum aktuellen Diskussionsstand, abrufbar unter https://www.enviam-gruppe.de/docs/default-source/01_unternehmen_downloads/studie_8mdeg_web.pdf

Von den Teilnehmenden wurde diesbezüglich besonders hervorgehoben, dass das **Risikomanagement unter dem Kriterium der Robustheit tradiert ist:** In einem so stark vernetzten und komplexen System sei davon auszugehen, dass das System jederzeit an irgendeiner Stelle kompromittiert werden kann. Klassische IT-Sicherheitsmechanismen, die darauf aufbauen zu segmentieren, Angreifer draußen zu halten, zu verschlüsseln und Passwörter zu vergeben, reichen dann nicht mehr aus. Bisher wurde bei technischen Systemen in der Risikobemessung so vorgegangen, dass Wahrscheinlichkeiten für Fehler und Folgefehler analysiert wurden, um daraufhin Sicherheitsstrategien zu entwickeln. Die Wahrscheinlichkeiten für Folgefehler wurden zumeist geringer eingeschätzt. „**Bei IT-Systemen und insbesondere bei Cyber-Angriffen ist die Wahrscheinlichkeit für den Folgefehler aber genauso hoch oder sogar höher wie beim ersten. […] Der Angreifer geht mit dem Ziel vor, das System zu hacken und das ist eine andere Risikobemessungsgrundlage, als sie heute bei technischen Systemen in diesem Bereich eingesetzt wird**" (Wissenschaft). Eine weitere Herausforderung besteht folglich auch darin, mit Angreifern, die bereits in die Systeme eingedrungen sind, umzugehen und vorwärtskorrigierend zu arbeiten. Das ist eine völlig neue Art Systeme unter Sicherheitsaspekten zu managen.

> *„D.h. es gibt eine tatsächliche Industrie im Hintergrund, staatliche Organisationen mit vielen tausend Mitarbeitern, die nichts anderes machen, als berufsmäßig Lücken, Angriffsmöglichkeiten zu sammeln, Werkzeuge zu entwickeln, um diese Angriffe dann auch durchzuführen. Und das ist eine völlig andere Situation, auf die wir uns einstellen müssen. Der wir aber mit klassischen Security- und Sicherheitsmechanismen nur noch bedingt nachkommen können."* | WISSENSCHAFT

In der Frage, ob ein Sicherheitsexperte im Energiesystem eine andere Denkweise entwickeln müsste als bspw. in einer Fabrik, waren sich die Teilnehmenden nicht einig. Ein Teilnehmer betonte, dass es für ihn ein wesentlicher Unterschied sei, ob eine Milchfabrik aufgrund von IT-Fehlern stillsteht oder das Stromsystem, bei welchem ein einzelner Ausfall systemkritisch sein kann und zum Gesamtausfall führen kann. Ein anderer Teilnehmer war der Meinung, dass es keinen Unterschied mache. Zwar stünden bei Versagen am Ende unterschiedliche Resultate (im Energiesystem im schlimmsten Fall ein Blackout), dennoch müsse man bei der IT des Energiesystems nichts „genuin Neues lernen" (Zivilgesellschaft), um eine Risikobetrachtung vorzunehmen.

Zu den IKT wurde kritisch angemerkt, dass diese zwar in Verteilnetzen und unteren Spannungsebenen für eine bessere Beobachtbarkeit sorgen, um die volatile Einspeisung beobachten, steuern und regeln zu können. **Jedoch bedeutet mehr IKT auch, dass mehr Komponenten im System sind und somit automatisch eine größere Angriffsfläche existiert und eine größere Auswirkung bei Fehlern möglich ist**, wenn große Mengen an gleichen Komponenten im System installiert werden. Selbst wenn diese jeweils an kleinen Anlagen wie Windrädern angeschlossen sind, dann aber zu mehreren tausenden, skaliert sich der Effekt auf ein großes Kraftwerk und ist demnach systemrelevant. Andererseits sind

die IKT-Komponenten in einem System mit immer mehr dezentralen, wetterabhängigen Erzeugungsanlangen notwendig für die Steuerung. Hinzu kommt allerdings, dass bei immer mehr volatilen Erzeugungsanlagen die meteorologische Prognoseunsicherheit ebenfalls steigt und damit auch die Komplexität.

Ein grundsätzliches Problem wurde in dem Spannungsfeld zwischen „alt und neu" gesehen. Dies gilt vor allem für die Infrastruktur, die zwar ausgebaut werden muss und damit auch neue Komponenten erhält. Jedoch besteht bereits ein großer Teil an Infrastruktur, an die angeknüpft werden muss. Unabhängig davon wie sicher die neuen Komponenten sind, bringen die alten Infrastrukturen auch gewisse Risiken in das digitalisierte System. Ein ähnliches Problem besteht auch bei der Anwendung von Geräten (neue, technologisch sichere Produkte werden auf alte Systeme und Infrastrukturen gesetzt). Selbst wenn es Standards für neue Geräte gibt, werden immer noch alte, unsichere Geräte im System verbleiben, die wiederum potenzielle Angriffspunkte darstellen.

„Immer dann, wenn ich Kommunikationsverbindungen aufbaue, habe ich zwei Möglichkeiten das zu machen: neu, hoch sicher und extrem teuer– oder ich nutze Infrastrukturen, die schon da sind. Dann habe ich aber ein Risiko, dass ich auch nicht nur von der Kostengünstigkeit dieser Kommunikations-Infrastruktur profitiere, sondern, dass ich auch mit den Risiken leben muss und diese beherrschbar gestalten muss."
| POLITIK

Das **Management der Infrastrukturen sowie der verschiedenen Akteure**, die diese Infrastruktur betreiben oder nutzen wollen, wurde als grundlegende Herausforderung gesehen. Besonders die Frage danach, ob eine zentrale oder dezentrale Steuerung der Infrastruktur besser wäre, stand dabei im Mittelpunkt. Als Entscheidungshilfe wurde von den Teilnehmenden dabei die Betrachtung der jeweiligen Rolle der Akteure – Netzbetreiber im Monopol, Erzeuger im Wettbewerb, viele kleine neue Einspeiser (Prosumer) – aufgeführt. Offen blieb die Frage, wie viel Steuerungskompetenz und Verantwortung den Bedienern in einem zunehmend komplexen System zugemutet und wieviel durch automatisierte Prozesse und intelligente Geräte geregelt werden kann.

Die Tatsache, dass **es für die Energiewende weder einen konkreten Fahrplan noch eine Vision davon gab, wie das System am Ende aussehen soll**, hat verschiedene Implikationen. Gerade für Ideen, wie z.B. die Abwicklung diverser Dienste über Smart-Meter-Gateways oder Telematik im Gesundheitswesen, fehlt es an Normen und Standards, die dabei helfen würden, eine durchgängige Interoperabilität zu gewährleisten. Ebenfalls ist die Abstimmung zwischen Standards großer Firmen, Normen, die in Gremien gesetzt werden und dem politischen Rechtsrahmen derzeit noch nicht lückenlos und ebenso wenig widerspruchsfrei.

Der enorme Fortschritt bei der Entwicklung von Technologien (Cloud-Technologien, Virtualisierung, Ambient Technologies, Künstliche Intelligenz) bringt viele spannende Möglichkeiten mit sich, die in kritischen Infrastrukturen jedoch meist ungetestet sind. Diese

Technologien werden zwar in anderen Anwendungsbereichen eingesetzt und wir haben uns daran gewöhnt, dass sie unter Umständen ausfallen können. Jedoch darf das bei kritischen Infrastrukturen nicht passieren. Die Herausforderung besteht demnach darin, solche **Technologien für die Unterstützung des Betriebs kritischer Infrastrukturen zu beobachten und durch Maßnahmen und Mechanismen zu begleiten, die gewährleisten, dass die Versorgungsaufgabe gesichert ist**.

Neben den vielen Herausforderungen, die im Umbau des Energiesystems selbst liegen, wurden von den Teilnehmenden auch Herausforderungen angesprochen, die aus dem Umfeld kommen. So wurde festgehalten, dass sich die Bedrohungslage von Cyber-Attacken verändert hat: es gibt nicht mehr nur isolierte Hacker, die einem Hobby nachgehen, sondern dahinter stehen komplexe Wertschöpfungsnetze.

Eine Teilnehmerin wies zudem auf die Herausforderung der Entwicklung kreislauffähiger Produkte hin: Es muss sichergestellt und entsprechend geplant werden, dass auch in Zukunft ausreichend Rohstoffe wie seltene Erden verfügbar sind, um den Normalbetrieb des Energiesystems aufrecht zu erhalten. Die Notwendigkeit kreislauffähige technische Produkte herzustellen ist insbesondere im digitalen Bereich wichtig, denn „**bei wachsender Produktion derselben und wachsender Menschheit ist es absehbar, dass wir nicht mehr über die Ressourcen verfügen irgendwas digital zu gestalten und zu vernetzen**" (Wissenschaft). Derzeit wird das nicht konsequent umgesetzt. Das Recycling müsste bereits beim Design und bei der Herstellung von Produkten und Geräten stärker mitbedacht werden, sodass weniger Einwegkomponenten produziert werden. Denn ein rückwärtsgewandtes Recycling ist immer schwierig und weniger ergiebig.

Auf die europäische Ebene bezogen bzw. im Vergleich mit den Nachbarländern, wurde der Angriff in der Ukraine 2015 als besorgniserregend eingestuft, da ähnliche Komponenten im „deutschen“ Energiesystem verbaut sind. Es wurden Stimmen laut, ob die Digitalisierung der Infrastrukturen zielführend ist oder zu risikobehaftet und, ob man nicht langsamer und bedachter voranschreiten solle. Als weitere Herausforderung wurde die technologische Standardisierung im europäischen Verbundnetz gesehen. Zum einen müssen nationale differenzierte Strategien trotzdem zu europäisch interoperablen Systemen führen. Zum anderen geht es um IT-Sicherheit. Gerade beim Thema Smart-Meter-Rollout gibt es derzeit recht heterogene Ausprägungen in Europa. Selbst wenn die Messsysteme letztlich interoperabel sind, aber der Zugang zu den Smart Meter unterschiedlich streng geregelt ist, könnten auch Sicherheitsmechanismen kompromittiert werden.

2.3 Dezentralität zwischen Demokratisierungsnarrativ und Sicherheit

Der im Trialog zunächst unter rein technologischen Gesichtspunkten eingebrachte Aspekt der Dezentralität wurde im weiteren Verlauf aus demokratietheoretischer Sicht, unter Aspekten der Sicherheit und Pfadabhängigkeit sowie unter wirtschaftlichen Gesichtspunkten intensiv diskutiert. Es wurde festgestellt, dass er in der gesamten Energiedebatte große Aufmerksamkeit bekommt, da sowohl technologische als auch ökonomische Dynamiken Dezentralität befördern. Grundsätzlich stellt sich bei dem Begriff der Dezentralität immer die Frage, welche Bereiche damit gemeint sind – die Erzeugung, die Eigentumsstruktur, die Kommunikation, die Steuerung oder alle Bereiche?

Mitunter wird der Begriff der Dezentralität **fälschlicherweise mit Demokratisierung gleichgesetzt**. Die Tatsache, im Besitz einer eigenen PV-Anlage oder eines Windrades zu sein, bedeutet nicht automatisch weitreichende Entscheidungen im Energiesystem treffen zu dürfen. Es wurde aber auch festgestellt, dass „eine Monostruktur und eine Kumulation von Macht in einem Demokratieverständnis mit Gewaltenteilung nicht greift“ (Zivilgesellschaft/ Wissenschaft). Tatsächlich ist die Anzahl der Erzeugungsanlagen in Deutschland durch die Energiewende enorm gestiegen und ein kleiner Teil davon gehört den Verbrauchern oder Prosumenten. Entsprechend gibt es eine geringere Marktkonzentration, die durch neue Erzeugungstechnologien, aber auch durch die Digitalisierung (wie bspw. Blockchain) befördert wird.

> *„Energieversorgungsunternehmen gehen nicht in Märkte hinein, weil sie Demokratisierung befördern wollen, sondern, weil sie Geld verdienen wollen unter anderen Parametern als früher. Mit Demokratisierung hat das gar nichts zu tun.“*
> | WIRTSCHAFT

Ein Teilnehmer des Trialogs schwächte den Demokratisierungsgedanken weiter ab mit dem Einwand, dass selbst die Dezentralisierung von Erzeugungsanlagen nicht automatisch zu einem dezentralen Wirtschaftsgefüge oder eine dezentrale Entscheidungsstruktur führt. Demnach kann Eigenstrom nur über die Direktvermarkter auf den Markt gebracht werden, welche meist die gleichen Konditionen anbieten. Somit können Erzeugerinnen und Erzeuger mit ihrem Eigentum nicht frei agieren. Es ist sehr wahrscheinlich, dass diese Zentralisierung von Dienstleistungen auch in Zukunft erhalten bleibt, auch aufgrund von Effizienzgewinnen. Gegebenenfalls kann dem die Blockchain-Technologie ein stückweit entgegenwirken.

In der Diskussion um Dezentralisierung und Demokratisierung sollten zudem die Pfadabhängigkeiten bedacht werden. Wie bereits angemerkt, können ganz neue Energiesysteme, wie bspw. in afrikanischen Ländern, völlig anders geplant und umgesetzt werden. Das hat weniger mit Demokratisierung zu tun als mit der Tatsache, dass keine zentralen Infrastrukturen vorhanden sind. Im Gegensatz dazu kann in Deutschland kein neues System mit durchweg neuen Entscheidungs-, Verantwortungs- und Machtstrukturen auf der grünen Wiese entwickelt werden, da das Energiesystem über Jahrzehnte gewachsen ist von lokalen

Strukturen im 19. Jahrhundert bis zu europäisch-internationalen Strukturen heute. Es gibt bereits technologische und infrastrukturelle Systeme, die Kapital binden, was für die Planung und den Bau komplett neuer Systeme nicht frei verfügbar ist. „**Das ist ein wichtiger Aspekt, der berücksichtigt werden muss, denn das bedeutet im Umkehrschluss, dass wir graduelle, inkrementelle Erweiterungen eines bereits existierenden Systems vornehmen, an das wir viele Anforderungen stellen**“ (Wissenschaft). Dem wurde entgegengehalten, dass es ein Verharren darin gäbe, die vermeintlich einfacheren, steuerbaren zentralen Strukturen aufrechtzuerhalten und somit der Umbruch der energiewirtschaftlichen und -politischen Steuerung gebremst werde.

Weiter wurde im Trialog diskutiert, ob Systemsicherheit besser zentral oder dezentral zu steuern ist. In einem dezentralen System muss darauf geachtet werden, dass trotz der vielschichtigen Struktur die Verantwortlichkeiten für die Versorgungs- sowie Systemsicherheit klar zugewiesen sind. Trotz dezentraler Erzeugung könnte es auch sein, so ein Teilnehmender, dass ein zentraler Durchgriff auf die Energiestrukturen aus Gründen der Versorgungs- und digitalen Sicherheit etabliert wird (Feinsteuerung vom Netzbetreiber bis hin zu einer einzelnen Anlage, wann diese an- und abgeschaltet wird). Hierbei stellt sich die Frage: Wo müssen die Schnittstellen und Entscheidungskompetenzen liegen, da hiermit auch wirtschaftliche Interesse verbunden sind?

Ein Teilnehmender betonte, dass die Resilienz von IT-Systemen durch eine Reduktion der Dezentralität gestärkt werden kann: Je seltener ein Single-Point-Of-Failure , desto besser. Aber **Dezentralität heißt nicht „viele gleiche Systeme an verschiedenen Orten“, sondern viele unterschiedliche Systeme an unterschiedlichen Orten, die einander vollständig kompensieren können und möglichst geringe gegenseitige Abhängigkeiten haben**.

Aus einer wirtschaftlichen Perspektive ergeben sich durch die Dezentralisierung im Rahmen der Sektorkopplung interessante Optionen für Unternehmen: So können sie auf lokaler Ebene ggfs. verschiedene Strategien mit ihrer Wärme- oder Stromproduktion fahren wie etwa überschüssigen Strom für Ladestationen der eigenen Flotte anbieten, Strom speichern oder am Markt die Energie anbieten. D.h. in einer Größenordnung, die oberhalb eines Haushaltes liegt, gibt es durchaus sehr unterschiedliche Strategien, sich am Markt zu bewegen und Sektorkopplung für verschiedene Zwecke einzusetzen. Es kann für Unternehmen interessant sein, autonom über wirtschaftliche Strategien in diesem Bereich zu entscheiden.

Ein weiterer Punkt der Dezentralitätsdebatte im Trialog bezog sich auf die Frage, was mit älteren abbezahlten Erneuerbaren-Energien-Anlagen ab 2020 passieren wird. Im jetzigen Regime der Marktzugänge lohnt es sich nur begrenzt oder gar nicht mehr bei einem Defekt, die Anlage zu betreiben. Es wird bedeutend sein, die Marktintegration der kleinen Akteure politisch zu regeln – entweder durch geeignete Marktzugänge oder die nächste Subvention. Aufgrund von Betriebskosten und Wartungsarbeiten können viele dieser Anlagen mit

aktuellen Strompreisen von rund drei Cent je Kilowattstunden meist nicht wirtschaftlich betrieben werden.

Schließlich wurde auch die Blockchain-Technologie als wichtiger Treiber der Dezentralisierung diskutiert. Diese gesonderte Diskussion soll im nächsten Abschnitt erläutert werden.

2.3.1 Blockchain als Anwendungsbeispiel dezentraler digitaler Systeme

Die Idee hinter Blockchain (BC) ist einen **dezentralisierten Konsensus in einem Peer-to-Peer Netzwerk** zu beglaubigen und damit Vertrauen, Nachvollziehbarkeit und Unveränderbarkeit herzustellen. Alle Vorgänge im Netzwerk werden von den Teilnehmenden des Netzwerkes bestätigt. Damit soll die Technologie eine Vermittlungsinstanz zur Sicherstellung der Vertrauenswürdigkeit einer Transaktion hinfällig machen (z.B. Banken bei Überweisungen). Die **Blockchain ersetzt also die dritte Instanz, indem sie Informationen (z.B. den Kontostand) durch eine kryptographische Funktion festhält und damit nicht mehr kopierbar macht**. Somit wird sichergestellt, dass, um bei dem Beispiel Überweisungen zu bleiben, nur das Geld überwiesen werden kann, welches sich auch auf dem Konto befindet.

Es existieren sowohl private als auch öffentliche Blockchains. Es sind also nicht alle Blockchain grundsätzlich für alle Personen zugänglich. Für jede BC wird bestimmt, wer daran teilhaben darf und welcher Konsensmechanismus ihr zugrunde liegt. Dieser ist zum einen dafür da, um in einem Netzwerk Konsens über eine identische Version der BC zu erzielen. Zum anderen werden durch die Konsensalgorithmen Hürden aufgestellt, um Manipulationen, doppeltes Kassieren von Belohnungen oder Transaktionsgebühren zu verhindern. Ebenfalls besitzt jede Blockchain ein Eskalationsprotokoll, welches besagt, was passiert, wenn jemand versucht zu betrügen. Die drei gängigsten Konsens-Mechanismen sind:[23]

- **Proof of Work (PoW)**: Der Mechanismus beschreibt, dass ein Teilnehmer (Miner) beweisbare Arbeit verrichtet haben muss, um eine Anzahl von Transaktionen bestätigen zu können. Die Belohnung soll seine Arbeit (aufgebrachte elektrische Energie, Einsatz der Hardware, Lösung eines kryptografischen Rätsels) entschädigen. Bisher ist dieser Mechanismus bei Kryptowährungen meistverbreitet, da das Verfahren als robust gilt. Allerdings braucht dieser Mechanismus viel elektrische Energie und mittlerweile spezialisierte Hardware.
- **Proof of Stake (PoS)**: Bei Proof of Stake[24]haben alle Teilhaber den Anspruch darauf, am Konsens mitzubestimmen. Dieser Anspruch auf die Validierung eines Blocks

[23] Für weitere Informationen zu den Konsens-Mechanismen siehe https://www.dev-insider.de/consensus-modelle-in-der-uebersicht-a-631671/
[24] Für weitere Informationen zu PoS siehe https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ

neuer Transaktionen wird jedes Mal erneut deterministisch (durch Pseudozufall) vergeben. Anteilseigner mit mehr Vermögen haben dabei eine etwas höhere Chance darauf, ausgewählt zu werden.[25]
Eskalationsprotokoll: Geld - Wird versucht zu betrügen, so wird das vorab als Pfand hinterlegte Geld einbehalten.

- **Proof of Authority (PoA)**: Dieser Mechansimus ist eine Kombination von PoW und PoS.

Im Trialog wurden die beiden bekanntesten Blockchain-Anwendungen angesprochen: Bitcoin und Ethereum. Während sich Bitcoin auf Finanztransaktionen beschränkt, können bei Ethereum diverse Verträge abgeschlossen werden. Beide Blockchains arbeiten mit PoW.

Wie alle Blockchains[26] ist die Bitcoin-Blockchain eine Datenbank, die dezentral von mehreren Parteien betrieben wird. Alle bisherigen Transaktionen der Datenbank sind in "verketteten" Blöcken dokumentiert, neue Transaktionen werden in neuen Blöcken hinzugefügt. In der Sprache der Buchhalter wäre die Bitcoin-Blockchain das Hauptbuch in einem sehr großen Buchhaltungssystem, welches jedoch nicht zentral abgelegt ist, sondern sich redundant auf den Rechnern aller Teilnehmer befindet. Alle Teilnehmenden haben die Möglichkeit sich die gesamte Bitcoin-Transaktionshistorie von Stunde null an auf ihren Computer herunterzuladen. Somit kann jeder transparent nachvollziehen, woher welche Bitcoins stammen und wohin sie jeweils transferiert wurden. Durch die dezentrale Struktur haben alle die gleiche Version der Transaktionshistorie auf ihrem Computer. Die Wahrscheinlichkeit einer Manipulation ist somit sehr gering, da alle Beteiligten immer alle Vorgänge nachverfolgen können.

In der Diskussion über die Blockchain-Technologie allgemein und in Bezug auf die Digitalisierung des Energiesystems wurden unterschiedliche Standpunkte vertreten. Als Vorteil wurde die grundlegende Idee von BC gesehen: das Umgehen von Zwischeninstanzen, wie z.B. Banken, sodass **zentrale Monopolstrukturen aufgebrochen werden sowie die Transparenz des Systems an sich** (für alle sind die Regeln sichtbar auf der BC abgelegt). Bezogen auf die Transparenz wurde von einer Teilnehmerin betont, dass dadurch wiederum **Vertrauen innerhalb eines Systems** geschaffen werde. Ebenfalls wurde positiv bewertet, das BC auf eine Basis aufbauen, in der das **Vertrauen aus dem System selbst kommt** und nicht als Vertrauen in die Marktteilnehmenden gesetzt werden muss.

[25] Siehe auch Jonas Verhoelen (2017): blockcentric #1: Konsens-Mechanismen der Blockchain, auf codecentric Blog, abrufbar unter. https://blog.codecentric.de/2017/10/konsens-mechanismen-blockchain/
[26] Für weitere Informationen zu Blockchain-Technologien siehe auch Thomas Kaltofen (2017): Blockchain-Technologien im Detail auf computerwoche.de, abrufbar unter https://www.computerwoche.de/a/blockchain-technologien-im-detail,3330877

Anwendungsbeispiele der Blockchain-Technologie im Energiesystem

Tal-Markt

Die Stadtwerke Wuppertal bieten seit Jahresbeginn 2018 den weltweit ersten Blockchain-basierten Handelsplatz für Ökostrom eines kommunalen Energieversorgers an. Über die Homepage können Kunden ihren Strom bei Ökostrom-Anbietern aus der Stadt im Bergischen Land kaufen und ihren Energiemix nach eigenem Gusto zusammenstellen. Jede Transaktion wird per Blockchain fälschungssicher ausgeführt. Dank der Technologie können Daten dezentral ausgetauscht und gespeichert werden.

Für weitere Informationen: https://wsw-talmarkt.de

Pilotprojekt Share & Charge

Motionwerk hat eine Elektroauto-Ladeplattform entwickelt, mit der Haushalte und Unternehmen ihre Ladestationen durch den Verkauf von Dienstleistungen an Fremde monetarisieren können. Die Blockchain ermöglicht es durch einen intelligenten Vertrag, den Preis festzulegen, die Ladestation zu starten und die Zahlung zu tätigen, wenn die Ladung abgeschlossen ist

Für weitere Informationen: https://shareandcharge.com/

Pilotprojekt von Tennet und sonnen

Bei dem Projekt werden Hausspeicher im Verteilnetz genutzt, um zur Stabilisierung des Stromnetzes beizutragen (Redispatch). Die Blockchain von IBM ermöglicht es Tennet, die verfügbare Flexibilität der Batterien zu sehen, die per Knopfdruck aufgerufen werden können. Die Blockchain zeichnet dann den Beitrag jeder Batterie auf, nachdem ein Ereignis aufgerufen wurde.

Für weitere Informationen: https://www.tennet.eu/fileadmin/user_upload/Company/News/German/Hoerchens/2017/20171102_PM-Start-Blockchain-Projekt-TenneT-sonnen.pdf

Grundsätzlich wurde angemerkt, dass differenziert werden muss zwischen den verschiedenen Anwendungsbereichen von BC-Technologien und dem jeweiligen Mehrwert. Da sich momentan alle BC in den Anfangsstadien und der Entwicklung befinden, sollte deren Nutzung weder von vorne herein ausgeschlossen, noch sollte die Technologie überstürzt und unüberlegt eingesetzt werden. Einige Teilnehmenden merkten an, dass BC-basierte Systeme eventuell besser geeignet wären für Nachweispflichten, anstatt für ein Peer-to-Peer Transaktionsmanagement. Gerade **in großen und unübersichtlichen Systemen, wie z.B. bei Abrechnungen oder Zertifkatehandel, könnten Blockchain-Technologien ein möglicher Weg sein um Nachweise zu führen**.

Die Anwendung von BC im Bereich der Energieversorgung wurde von einer Teilnehmerin als sehr positiv bewertet, weil sie ohne einen zentralen Richter ein Konsensus über den Informationsstand ermöglicht, was insbesondere bei Stromverbrauchsdaten sinnvoll sein kann. Die Verwendung von BC im Energiebereich würde zudem die Schwelle für neue Marktteilnehmer, vor allem Privathaushalte senken, die selbst als Marktteilnehmer auftreten wollen. Diese müssen dann nicht mehr wie bisher über einen Energieversorger gehen, sondern könnten das selbstständig im Netzwerk erledigen. Allerdings muss zwischen dem Verkaufsvorgang und der physischen Einspeisung unterschieden werden. Denn auch wenn

durch BC kein Vermittler für den Liefervertrag mehr nötig sein muss, so erfolgt die Einspeisung dennoch in das allgemeine Stromnetz.

Kritik an der Anwendung von BC im Energiesystem kam vor allem aufgrund der Tatsache, dass die **bisherigen BC-Technologien aufgrund des PoW-Mechanismus sehr viel Strom verbrauchen und nicht nachhaltig sind**. So sei es paradox, dass auf der einen Seite versucht wird über BC-Technologien die Digitalisierung der Energiewende voranzutreiben, wenn auf der anderen Seite jedoch die Energiekosten von BC-Transaktionen exponentiell steigen. Das Bitcoin-Netzwerk verbraucht momentan beispielsweise hochgerechnet auf ein Jahr mehr Energie als Bangladesch, Tendenz steigend.[27] Kritisch betrachtet wird hierbei vor allem, dass der hohe Energieverbrauch in keiner Relation zur Gegenleistung (Transaktion) steht.

Von einem Teilnehmenden wurde angemerkt, dass **BC-Technologien Verantwortlichkeiten verwischen** und daher nicht für große, sensible Systeme wie die Netzsteuerung geeignet wären. Er sieht das Potenzial von BC eher in kleineren Netzwerken, z.B. für Abrechnungszwecke oder das Vertragsmanagement.

Schließlich sind vor einem breiteren Einsatz der Technologie im Energiesystem auch **rechtliche Fragen zu klären**: wie wird mit Solidaritätsumlagen und Netzentgelten bei lokalen Peer-to-Peer-Handel umgegangen? Sollten die dezentralen Einspeiser und lokalen Nutzer von geringen Netzentgelten profitieren oder liefe das der Etablierung einer zentralen Versorgungsicherheit zu wider? Welcher rechtliche Rahmen ist für die System- und Datensicherheit notwendig? Diese und weitere Fragen konnten im Trialog nur angeschnitten werden. Es ist aber sehr wahrscheinlich, dass sie bei der weiteren Ausgestaltung der Digitalisierung eine größere Rolle spielen.

2.4 Konzepte und Dimensionen von Sicherheit

Auf dem Trialog wurden unterschiedliche Dimensionen und Konzepte von Sicherheit thematisiert. Grundlegend kann gesagt werden, dass es Vorstellungen gibt, die Sicherheit als etwas Absolutes und Lückenloses sehen – nach dem Prinzip, „wenn ich alle Türen abschließe, dann kommt auch niemand hinein" (Politik). Diese Grundvorstellung der Abschottung (vgl. Flüchtlingsproblematik) ist auf den ersten Blick simpel, stößt aber an ihre Grenzen. Problematisch an dieser "einfachen" Idee von Sicherheit ist, dass sich abgeschlossene Systeme nicht mehr durch den Austausch über ihre Systemgrenzen hinweg weiterentwickeln können. Sie können nur auf bereits Vorhandenes zurückgreifen. Andere Konzepte von Sicherheit sind komplexer, dadurch aber auch flexibler in der Anwendung von Mechanismen, um Sicherheit zu ermöglichen. Auch spielt das Sicherheitsempfinden

[27] Stand 06.03.2018, abrufbar unter https://digiconomist.net/bitcoin-energy-consumption

einzelner Personen oder auch Gruppen eine Rolle (siehe Box). Im Trialog wurde festgehalten, dass der Anspruch nach absoluter Sicherheit hierarchische, monopolisierte und vereinheitlichte Entscheidungen provoziert.

Exkurs Sicherheitsempfinden

Die verschiedenen Konzepte von Sicherheit beinhalten jeweils andere Bewältigungsstrategien. Bezogen auf das Konzept einer absoluten Sicherheit stellt die Aufrechterhaltung des Sicherheitsempfinden eine Herausforderung dar, denn jeder eingetretene Schadensfall, sei es ein Hackerangriff auf ein Wirtschaftsunternehmen oder ein Anschlag auf die Zivilbevölkerung, schadet dem Sicherheitsempfinden. Dadurch wird zum einen von der Politik oder dem betroffenen Unternehmen gefordert, dass sie eine Reaktion zeigen. Zum anderen möchten beide auch eine Reaktion zeigen, um das Sicherheitsempfinden wiederherzustellen. Oftmals werden dabei jedoch Maßnahmen ergriffen, wie auf dem Trialog bemerkt wurde, die in keinem Zusammenhang mit dem Schadensfall stehen, nur damit eine Reaktion gezeigt wurde. Somit wird versucht ein Sicherheitsempfinden zu vermitteln, dass jedoch weiterhin die gleichen Einfallstore besitzt wie zuvor.

Die Option einer alternativen Sicherheitskonstruktion wird oftmals nicht mehr in Erwägung gezogen. Kritisch ist hierbei vor allem, wenn ein Großteil durchschaut, dass die erklärten Maßnahmen, also das Vortäuschen von Sicherheit, gar nicht mit den Problemen zusammenpassen. Dadurch steigt die Wahrscheinlichkeit, dass Teile der Gesellschaft resignieren.

Es muss demnach geklärt werden, welches grundliegende Konzept von Sicherheit angestrebt wird. Eine absolute, partielle oder gefühlte Sicherheit? Ebenfalls drängt sich die Frage auf, ob Sicherheit überhaupt rein technologisch hergestellt und gewährleistet werden kann. Braucht es für eine Antwort nicht weitere Dimensionen und „**wo geht es los mit Regelungsfragen im Politischen, im Sozialen, auch im Psychologischen?**“ (Politik).

Zustimmung gab es auch dafür, dass Energiesicherheit durch Digitalisierung nicht nur technologisch angegangen werden kann, sondern die damit zusammenhängenden Fragen auch im größeren, sozialen und politischen Kontext beurteilt werden müssen. Denn die Energieversorgung zählt zu den kritischen Infrastrukturen. Sie trägt letztlich auch zur Daseinsvorsorge bei und sollte alles andere als unzuverlässig sein. Betont wurde dabei der Stellenwert von Vertrauen: Wenn kein Vertrauen zwischen Behörden, Ämtern, Politikern und Staaten vorhanden ist, dann findet kein veritabler Informationsaustausch statt. Ohne diesen fällt die Gewährleistung von Sicherheit jedoch schwer.

Sicherheitsdimensionen

Auf dem Trialog wurden diverse Sicherheitsdimensionen genannt: Versorgungs- und Rohstoffsicherheit, Investitionssicherheit, Daten- und IT-Sicherheit.

Versorgungssicherheit: Unter den verschiedenen Dimensionen von Sicherheit kommt der **Versorgungssicherheit** eine besondere Rolle zu, da sie ein **zentrales Ziel des Energiesystems ist**. Bei der Versorgungssicherheit geht es u.a. um die Bewahrung des Systems vor Störungen, so dass die Funktionsweise erhalten bleibt und eine Versorgung mit Energie

stattfindet. Es kann zwischen kurz-, mittel- oder langfristiger Versorgungssicherheit unterschieden werden. Gerade die mittel- und langfristige Versorgungssicherheit kann nicht nur aus dem Energiesystem allein gesteuert werden. Die Versorgungssicherheit kann beispielsweise nicht aufrechterhalten werden, wenn ignoriert wird, dass die dafür benötigten Rohstoffe endlich sind. Somit spielt das Konzept der Nachhaltigkeit auch immer in die verschiedenen Dimensionen von Sicherheit mit hinein und sollte auch für kurzfristige Entscheidung nicht ganz außer Acht gelassen werden.

Rohstoffsicherheit: Der Umgang mit Rohstoff- und Ressourcen-Engpässen in Folge der Nutzung von Einwegprodukten ist ein wichtiger Aspekt von Sicherheit, wie eine Teilnehmerin in Erinnerung rief. Bisher gibt es noch viel zu wenig kreislauffähige Produkte und keine starke Lobby, die sich dafür einsetzt. Gerade in Fragen der Digitalisierung, bei der viele Geräte und Komponenten mit seltenen Erden und andere wichtige Metalle zum Einsatz kommen, ist eine sichere und langfristig verfügbare Ressourcenbasis für die konsequente Weiterentwicklung von hoher Bedeutung. Bereits heute sollte das **Recycling im Design der Produkte** bedacht werden. Weiterhin ist die Rohstoffbasis so zu planen, dass der Erhalt des Normalbetriebs gesichert ist, auch wenn ein Ereignis eintritt, dass einen Großteil der Ressourcenvorräte zerstören würde oder einen Zugriff auf diese Vorräte nicht mehr möglich macht.

Investitionssicherheit: Die rasante Entwicklung der Digitalisierung des Energiesystems birgt für Unternehmen Unsicherheiten, da oftmals nicht ersichtlich ist wie schnell sich welche Technologien etablieren und wie diese langfristig regulatorisch gefördert oder gar subventioniert werden. Es gibt eine Verantwortung auf Seiten der Politik einen Rahmen zu setzen, so dass Unternehmen besser einschätzen können, in welche Systeme oder Produkte sie investieren können. Dieser Rahmen sollte ebenfalls dafür sorgen, dass regionale Unterschiede in den Entwicklungen entsprechend abgefangen oder gesteuert werden können (Ballungszentren versus ländlicher Raum).

Die verschiedenen Dimensionen zeigen auf, dass eine nachhaltige Sicherheit nur gewährleistet werden kann, wenn ein **sektorübergreifendes Verständnis von Sicherheit entwickelt wird**. Folglich bedeutet Sicherheit im Energiesystem nicht nur eine stabile Energieversorgung zu gewährleisten, sondern u.a. auch Daten- und Rechtssicherheit, Umweltschutz, Kosten für die Verbraucher und Rohstoffsicherheit. Diese einzelnen Punkte sind nicht additiv zu betrachten, sondern müssen zusammen gedacht und behandelt werden, denn sie beeinflussen einander. Dabei besteht eine besondere Herausforderung sich dennoch auf Schwerpunkte zu fokussieren, um diese tiefergehend zu ergründen.

„Hier können Standards helfen, einen Großteil der Probleme abzudecken. Aber wir hatten auch einen Fall, wo diskutiert wurde, dass entgegen eines Standards gehandelt wurde und dadurch ein größerer Blackout oder eine Katastrophe in einem Kraftwerk verhindert wurde. Was dazu führt, dass es also sinnvoll sein kann, im rechten Moment den Standard links liegen zu lassen. Das impliziert, dass die Person, die das entscheidet, die Kompetenz dazu hat." | WIRTSCHAFT

Die Teilnehmenden waren sich einig, dass **eine absolute Sicherheit nicht erreicht werden kann**. Im Bereich der Digitalisierung der Energiewende wurde die Chance einer 80-prozentigen Sicherheit gegenüber heute i.d.R. geforderten 100-prozentigen Sicherheit durch die Anwendung von Standards eingebracht. Ein weiterer Punkt für die Sicherheit im Energiesystem ist, wie Risiken bewertet werden und wie mit ihnen umgegangen werden kann und soll. Denn Risiken können auch eine Chance sein: So kann der Bediener an der Leitwarte auf der einen Seite ein Sicherheitsproblem sein, da er nur ein gewisses Maß an Komplexität überschauen kann. Auf der anderen Seite kann er jedoch für Sicherheit sorgen, indem er situativ und außerhalb des Protokolls handelt. Analog kann für die Blockchain-Technologie gesagt werden: Sie können durch ihre dezentrale Struktur Vertrauen in einem System schaffen oder es auch verspielen, wenn schlussendlich wieder zentrale Strukturen daraus erwachsen.

Die Dimensionen Datensicherheit und IT-Sicherheit wurden während des Trialogs ausführlich diskutiert und haben sich neben der Versorgungssicherheit als zentral in der Diskussion über die Digitalisierung des Energiesystems gezeigt. Im Folgenden werden die genannten Aspekte der zwei Dimensionen genauer ausgeführt.

2.4.1 Datensicherheit und das Energiesystem

Bei immer wiederkehrenden Schlagzeilen über Datenmissbrauch in digitalisierten Märkten und Anwendungen erstaunt es nicht, dass auch auf dem Trialog das Thema Datensicherheit diskutiert wurde. Zum einen ging es um die Datensicherheit der Verbraucherinnen und Verbraucher sowie der Prosumer gegenüber der Wirtschaft und zum anderen um die Datensicherheit von Unternehmen, Behörden und weiteren Institutionen gegenüber Cyberangriffsgruppen. Letzteres fällt eher in den Bereich IT-Sicherheit, welche im Folgekapitel behandelt wird.

Die zunehmende Digitalisierung bringt die Sorge vieler Verbraucherinnen und Verbraucher mit sich, dass sie den Überblick über die Verwendung ihrer Daten verlieren und sie das nicht mehr eigenständig steuern können. Es wurde festgehalten, dass es wichtig sei, wie Anbieter kommunizieren, welche Daten des Verbrauchers verwendet und eingesehen werden. Von den Teilnehmenden wurde gefordert, dass dies **offen, klar und verständlich geschieht und nicht nur im Kleingedruckten**. Grundsätzlich wurde hierbei die Frage aufgeworfen, ob es überhaupt eine Selbstbestimmung des Verbrauchers gibt oder, ob er

verführt bzw. durch Intransparenz dazu verleitet wird einzuwilligen? Mehrmals wurde ein grundsätzliches Bedenken geäußert, dass durch die Digitalisierung der Energiewende und den damit zusammenhängenden Möglichkeiten (Elektromobilität, Selbsteinspeiser, usw.) **die Kunden gläserner werden und es nicht mehr ersichtlich ist, wer genau Zugriff auf welche Daten hat**. Einstimmigkeit herrschte darüber, dass Daten nur an den Anbieter weitergeleitet werden dürfen, bei dem der Kunde auch bewusst eingewilligt hat. Es darf keine Weitergabe an Dritte stattfinden. Aus der Wirtschaft wurde das Interesse an Kundendaten bestätigt, um beispielsweise einfacher Optimierungsvorschläge für Produkte bereitzustellen oder personenbezogene Werbung zu ermöglichen. Dabei wurde auch das Spannungsverhältnis angesprochen zwischen dem Profitziel der Unternehmen durch passgenaue Angebote und dem Wunsch auf Verbraucherseite gut beraten, jedoch nicht unkontrolliert beworben zu werden. Die Freigabe personenbezogener Daten ist auch für Verbraucherinnen und Verbraucher oftmals eine Frage der **Abwägung zwischen dem Kundenmehrwert**, bspw. in einem Payback-System oder der **Wertbeimessung der eigenen Daten**. Selbstverständlich gibt es in diesem Bereich eine gesetzliche Regelung, wie mit den Daten umgegangen werden muss. Dennoch bleibt ein „zunehmendes Unbehagen“ (Wirtschaft) darüber, was mit der ansteigenden Datentransparenz des einzelnen Nutzers passiert.

Ein weiteres Argument war, dass aus einer traditionellen, zentralistischen Perspektive es von Vorteil sein könnte, möglichst viele Daten an einem einzigen Ort zu speichern, damit man die Kontrolle darüber hat. Ein Teilnehmer äußerte dazu die Einschätzung, dass Nutzerinnen und Nutzer in Zukunft verstärkt wissen wollen, wohin ihre Daten gehen und nicht möchten, dass diese im gesamten System verstreut sind. Ein Ansatz wäre, dass die Daten in einer kontrollierbaren Weise in den Einheiten vorhanden sind, wo sie wirklich gebraucht werden. Dieser Ansatz würde von der Datenstruktur her auf ein zelluläres System verweisen.

Eine weitere Feststellung war, dass sich die Verbraucherinnen und Verbraucher grundsätzlich darüber bewusst sein müssen, dass **bestimmte Technologien wie die Elektromobilität ohne eine Datenkommunikation nicht funktionieren**. Wenn Verbraucherinnen und Verbraucher nicht bereit sind in diesem Kontext ihre Daten zur Verfügung zu stellen, können sie die Technologie nicht nutzen. In diesem Kontext wurde auch erwähnt, dass **ein gewisses Maß an Datentransparenz notwendig ist, wenn die Daten bspw. für die Resilienz des Gesamtsystems relevant sind**. So sind Verbraucher mit 10 000 kWh im Jahr oder mehr in der Masse systemrelevant. Demnach muss zumindest der Netzbetreiber genug Informationen haben, um das System stabil halten zu können. Der gesellschaftliche Vorteil ist in einer solchen Konstellation höher als der Schutzbedarf der einzelnen Daten des Verbrauchers, wie in einem der Trialog-Workshops festgehalten wurde.

Die jedoch wichtigste und aktuellste Technologie in Bezug auf Datensicherheit in der Energiewende betrifft das Smart-Meter-Gateway, dessen datenschutzkonformer Einsatz rechtlich durch das **Gesetz zur Digitalisierung der Energiewende** gesichert werden soll. Das Gesetz macht Vorgaben zur Nutzung von Daten sowie zu technischen Standards. Darüber hinaus wurde das Bundesamt für Sicherheit in der Informationstechnik (BSI) damit beauftragt, Anforderungen an vertrauenswürdige Produktkomponenten, Kommunikationsinfrastrukturen sowie den IT-Betrieb zu entwickeln. Ein Teilnehmer lobte die Verfahren zur Entwicklung des Smart-Meter-Gateway sowie die anvisierten Lösungen. Demnach ist der Datenschutz gut angelegt, da es eine Zwischeninstanz gibt, die den Zugriff auf die Datenhaltung organisiert. Die zertifizierten Administratoren (z.B. Trianel[28]) erteilen Zugriffsrechte auf die Daten. Ebenfalls betreiben sie das Rechenzentrum, an dem die Geräte hängen. Dadurch wird es unwahrscheinlich, dass personenbezogene Daten in falsche Hände kommen. Derjenige, der die Daten bekommt, bekommt sie für einen bestimmten Zweck (z.B. die Abrechnung einer Energielieferung) und er darf sie nur dafür verwenden. Alles andere würde aufgrund der Rechtsgrundlage als Ordnungswidrigkeit, im Zweifelsfall als Straftat, geahndet werden. Welche Daten im Rahmen der Digitalisierung der Energieversorgung erhoben werden dürfen, steht in Teil 3 „Regelungen zur Datenkommunikation in intelligenten Energienetzes" des Gesetzes zur Digitalisierung der Energiewende. Der Gesetzestext gibt auch vor, dass jeder Vertrag, der eine Datenkommunikation zur Folge hat, ein Formblatt enthalten muss, auf dem die Datenkommunikation geregelt ist (§54 Transparenzvorgaben für Verträge).

Während in den ersten Jahren nur große Verbraucher von mehr als 10.000 kWh/a den Einbau von intelligenten Messstellen vornehmen müssen, sollen später auch Haushalte mit über 6000 kWh/a hinzukommen. Hier stellte sich die Frage, wie mit der Datentransparenz und den Kosten im Mehrfamilienhaus umgegangen wird. Was passiert, wenn bspw. der Vermieter eines größeren Komplexes entscheidet, dass er Smart-Metering einsetzen will, auch wenn es nicht vorgeschrieben ist oder, wenn es einen Mieter gibt, dessen Verbrauch über 6000 kWh/a liegt – müssen sich dann alle Mieter unterordnen? Die generelle Voraussetzung laut Gesetz ist, dass auch bei Nutzung dieser Infrastruktur die Rechnung des Mieters nicht größer sein darf als vorher (durch den regulären Messstellenbetrieb). Umgekehrt können Mieter den Vermieter alle 2 Jahre anfragen, ob die Technik genutzt werden kann, damit alles automatisch abgelesen wird und nicht für Gas, Wasser etc. jeweils jährlich ein einzelner Ablesevorgang nötig ist.

[28] Vgl. pv magazine (2018): Trianel als Smart Meter Gateway Administrator zertifiziert, abrufbar unter https://www.pv-magazine.de/2018/01/30/trianel-als-gateway-administrator-zertifiziert/

2.4.2 IT-Sicherheit und die Lücke im System

Die IT-Sicherheit im Energiesystem hat eine besondere Bedeutung. Da es sich um eine kritische Infrastruktur handelt, ist ihre Versorgungsaufgabe stets aufrecht zu erhalten. Ausfälle sind nur minimal verkraftbar. Hinzu kommen die Größe, das Alter und entsprechende Pfadabhängigkeiten des Systems sowie der Regelungsbedarf über nationale Grenzen hinweg. Während es eine Reihe von Herausforderungen gibt das System sicher zu halten, gibt es für den Angreifer eines IT-Systems nur ein Ziel: Eine Sicherheitslücke zu finden und in das System einzudringen, um etwas zu zerstören, zu erpressen oder Daten abzugreifen. Somit ist der Angreifer im Vorteil, da sein Ziel viel weniger komplex ist und dafür meistens keine hochkomplexe Software benötigt wird.

„Die Angreifer da draußen machen viel simplere Angriffe. Die machen nicht hoch komplexes. Aus dem einfachen Grund, dass sie ihr Wissen nicht „verfeuern" wollen. Ich bin doch als viel zitierter russischer Hacker nicht unterwegs, um die Welt zu beeindrucken wie toll ich hacken kann. Ich bin da, um Schaden anzurichten und wenn ich das mit geringem Aufwand kann, dann mache ich das auch mit geringem Aufwand. Sie betreiben in Ihrem Unternehmen auch nicht mehr Aufwand als Sie müssen, um ein gestecktes Ziel zu erreichen. Solange das Ziel erreicht wird, sind Sie glücklich."
| ZIVILGESELLSCHAFT

Grundsätzlich herrscht in der IT-Sicherheit, insbesondere für große Systeme, ein Dilemma zwischen zeitgemäß sinnvollen Maßnahmen und Regelungen, die den jeweiligen IT-Verantwortlichen absichern. Ein IT-Verantwortlicher eines Unternehmens oder einer Institution wird Regeln, Zertifikate, Best Practices und Standards einhalten, um sich selbst abzusichern, dass er alles nach Vorgabe versucht hat zu lösen - unabhängig davon, ob es tatsächlich sinnvoll war. Standards werden nie für alle, jedoch für die meisten Fälle entwickelt. Im Gegensatz dazu ist es für die Angreifer irrelevant, wer verantwortlich ist oder, wem im Nachhinein vorgeworfen wird, fahrlässig gehandelt zu haben. Sie möchten ins System rein. Bei immer schneller werdenden Fortschritten in der IT ist es nicht leicht große, vernetzte Systeme nicht nur technisch, sondern auch standard- und regelbasiert auf aktuellem Niveau zu halten.

Einfallstore für Cyber-Angriffe bieten vor allem **Nischensoftware**. Diese wird in der Regel speziell auf einen bestimmten Rahmen zugeschnitten (z.B. Anzeigetafeln der Deutschen Bahn, kleinere Produktionsanlagen) und deshalb nur von wenigen Personen benutzt. Zusätzlich wird an sie die Anforderung gestellt, dass sie einen dauerhaften Betrieb gewährleisten muss. Dadurch wird Nischensoftware meist nicht mit dem Internet verbunden, selten ein Update aufgespielt und fungiert dadurch in einem geschlossenen System.

Die Teilnehmenden gaben an, dass Sicherheitslücken oft viel zu spät erkannt und geschlossen werden. Als Beispiel wurde der Hackerangriff auf den Bundestag im Jahr 2015 angeführt, bei dem die Sicherheitslücke über Monate unerkannt blieb. Ebenso wird zu wenig über erkannte Schwachstellen und dem Umgang mit diesen gesprochen. Ein Austausch fände kaum statt. Es wurde kritisiert, dass zu viel Geld in Firewalls fließe und zu wenig bis

gar kein Geld in Detektionsmechanismen und Backups investiert wird. Ein Fachmann verwies auf den Security Lifecycle, der aus drei Phasen besteht. Nur eine davon zielt auf die Prävention (1) ab und Phase (2) und (3) auf Detektion und Reaktion. Es muss ein Umdenken stattfinden: statt ausschließlich auf die Abwehr von Cyberangriffen zu fokussieren, sollte zunehmend auch in Maßnahmen zur Aufdeckung von Angriffen sowie zur Wiederherstellung von Systemen investiert werden.

„Es gibt viele tausend Angriffe pro Tag. Es gibt nichts Dümmeres als diesen Satz, denn, wenn ich den Angriff bemerkt habe, dann ist er per se fehlgeschlagen. D.h. es ist ein Angriffsversuch. Mich interessiert nicht, ob ich 5.000 oder 100.000 Angriffsversuche habe. Mich interessiert der eine Angriff, den ich nicht bemerkt habe."
| ZIVILGESELLSCHAFT

Des Weiteren kam im Trialog die Frage auf, ob IT-Expertinnen und Experten in der Energieversorgung im Vergleich zur IT in Unternehmen umdenken müssen. Ein fachkundiger Teilnehmer beantwortete die Frage mit einem Nein, da die **CIA-Schutzziele für jedes Gerät immer dieselben sind: Vertraulichkeit (Confidentiality), Integrität (Integrity) und Verfügbarkeit (Availability)**. In Bezug auf das Beispiel Smart Meter bedeutet das, dass man ein Netz aus Geräten baut, die alle diese Schutzziele erfüllen. In der Sicherheitsbetrachtung wird abgewogen, wie viel Macht und Einflussmöglichkeiten einem oder mehreren Geräten über das Gesamtsystem gegeben wird. Das Netzwerk wird dann unter der Maßgabe „assume compromise" betrachtet: Was ist der größtmögliche Verlust, der passieren kann unter der Annahme, dass ein Angriff gelingt. Diese Vorgehensweise wird schon seit vielen Jahren so angewandt und trifft auch für das Energiesystem zu – nur, dass ein Blackout der schlimmste Ausfall sein könnte. Im Vergleich zu dem Ausfall der Schokoladenproduktion in einem Milka-Werk, wie es in 2017 der Fall war, wäre dies unmissverständlich ein schwerwiegenderer Vorfall.

Grundsätzlich wurde die Frage diskutiert, **warum eigentlich noch kein gesamteuropäischer Stromausfall stattgefunden hat, obwohl es rein technisch möglich wäre?** Ein Teilnehmender vertrat die Meinung, dass bisher noch niemand ein wirkliches Interesse daran hatte. Definitiv kann es ihm zufolge nicht daran liegen, dass die vorhandenen kritischen Infrastrukturen 100 % sicher sind.

2.5 „Faktor Mensch"

Das Thema „Faktor Mensch" zog sich wie ein roter Faden durch den Trialog. Einerseits schwang die Sorge eines Bedeutungsverlusts des Menschen durch die Technologisierung und Digitalisierung in der Debatte mit. Andererseits wurde konstatiert, dass durch die Digitalisierung und die damit einhergehende Dezentralisierung ein anderes Menschenbild seine technologische Übersetzung ins Energiesystem findet.

Gerechte Möglichkeiten schaffen

Besonders die **Chance, durch dezentrale Strukturen mehr Bottom-Up- anstatt Top-Down Ansätze** zu gehen, wurde mehrmals erwähnt mit dem Verweis auf mehr Selbst- und Mitbestimmung. Diese Selbst- und Mitbestimmung darf jedoch nicht auf einen kleinen wohlhabenden Teil der Gesellschaft reduziert sein, sondern sollte für alle gleichermaßen möglich sein. Ansätze wie das Mieterstrommodell geben beispielsweise nun auch Mietern die Möglichkeit eigenen, also auf dem Gebäude erzeugten Strom, zu nutzen. Bisher kam dies im Rahmen der EEG-Förderung nur den Eigenheimbesitzer zugute. Neben unausgewogenen Subventionen und Fördermechanismen kommt es im Transformationsprozess auch immer wieder zu nicht gerecht verteilten Abgaben und Entgelten, wie bspw. Ausnahmen für Industrieunternehmen. In diesem Zusammenhang wurde auch die Frage des Gegenwerts von Sicherheit gestellt. Hier wird es in Zukunft nicht nur um die physikalische Sicherheit der Infrastruktur oder die Versorgungssicherheit im Sinne der Rohstoffbereitstellung gehen, sondern auch um Cybersicherheit. Wieviel ist diese uns Wert und wie kann der Gegenwert im System gerecht beglichen werden?

Neue Optionen nutzen

Als Eigenenergieerzeuger und -verbraucher nehmen Verbraucherinnen und Verbraucher eine neue Rolle als Prosumenten wahr. Haushalte und Personen können aber auch anderweitig ein aktiverer Teil des Energiesystems werden: indem sie variable Stromtarife nutzen, Energieanbieter wechseln, Energie einsparen und über Car-Sharing oder einen eigenen PKW zur Elektromobilität beitragen. Entscheidend im Kontext der Energiewende war vor allem der Punkt, dass **der Mensch bewusst und selbstbestimmt zum Energiesystem und zur Transformation beitragen kann und somit zu einem relevanten Akteur im Vergleich zum konventionellen Energiesystem wird.**

Nach Meinung der Teilnehmenden sollte diese neue Rolle des Menschen im Energiesystem anerkannt und befördert werden. Den Vorreitern und Pionieren der Energiewende, die als aktive Bürgerinnen und Bürger die Transformation mit Ideen und Lösungen mitgestalten, gilt eine besondere Wertschätzung. Auch wenn sie nur einen sehr kleinen Teil der Bevölkerung ausmachen, haben sie viele Veränderungen mit angestoßen.

Verantwortlichkeiten zwischen Mensch und Maschine

Im zukünftigen Energiesystem wird die Anzahl von Erzeugungsanlagen in Deutschland in einem mehrstelligen Millionenbereich liegen. Die Steuerung dieser Anlagen im Sinne der Versorgungssicherheit und des Lastmanagements wird aufgrund der hohen Anzahl und der wetterbedingten Fluktuation **ohne unterstützende intelligente Systeme durch Personen nicht mehr machbar sein**. Unter der Voraussetzung, dass es eine stärkere Verbindung zwischen den IKT- und Energienetzen gibt, wurde nach der zukünftigen Rolle der Bediener in

den Leitwarten gefragt: Was wird zukünftig noch manuell gesteuert und in welchem Umfang sind die Netzleitingenieure überhaupt noch in der Lage angemessen auf Fehler oder Angriffe auf das IKT-System zu reagieren?

Der Mensch wurde in einem digitalen Energiesystem zum einen als Schwachstelle gesehen, da für ihn die Komplexität eines vernetzten Systems zu hoch ist. Zum anderen wurde er aber auch als Sicherheitsgarant gesehen, in dem er flexibel agiert und von Standards, die nicht auf 100 % der Fälle zutreffen, abweichen kann – vorausgesetzt er hat die nötigen Kompetenzen.

„Wir brauchen immer einen Supervisor, der Mensch ist immer die letzte Instanz, die entscheidet."
|WIRTSCHAFT

Daran anschließend wurde diskutiert, ob **der Mensch durch Automatisierung, Algorithmen und künstliche Intelligenz ersetzt wird.** Ein Teilnehmer vertrat die Meinung, dass der Mensch weiterhin eine tragende Rolle in digitalisierten Systemen spielen wird. Ein wahrscheinliches Szenario ist, dass der Mensch Aufgaben an Algorithmen delegieren wird, sodass diese unterstützend wirken nach dem Prinzip **„menschliche Verantwortung und Algorithmen im Dienste des Menschen"** (Wissenschaft). Begründet wurde diese Annahme mit dem Beispiel des Flugverkehrs: Theoretisch steuern die Piloten die Maschine, praktisch sind aber die meisten Prozesse automatisiert und werden auf Kommando des Piloten durchgeführt.

Das **Spannungsfeld zwischen Bediener und Algorithmus** warf zudem die Frage nach der Verantwortung auf. Je nachdem wie ein System gefahren wird, muss gefragt werden, ob bspw. der Netzbetreiber (Bediener) oder der Software-Entwickler (Algorithmus) die Verantwortung bei einem möglichen Schadensfall trägt.

Ein wichtiges Fazit der Teilnehmenden war, dass **die Gesamt-Resilienz eines Systems sowohl von der Technik als auch von den Personen abhängt, die im System wirken**. Daher wurde der Schulung der Mitwirkenden eine entscheidende Bedeutung zugeschrieben. Mehrheitlich wurde betont, dass Ausbildungsberufe, Schulungen, Weiterbildungen sowie auch Standards bei den Weiterbildungen im Energiesystem vorangetrieben werden sollten. Somit könnten u.a. Einstellungsfehler und Fehler in den Geräten schneller erkannt und behoben werden.

2.6. Zusammenarbeit für mehr Sicherheit

Das Thema Zusammenarbeit ist im Rahmen der Digitalisierung der Energiewende auf vielen Ebenen bedeutsam: lokal, national, europäisch sowie international müssen sich Akteure auf der politischen, wirtschaftlichen sowie gesellschaftlichen Ebene abstimmen.

Besonderer Fokus galt im Trialog der **Zusammenarbeit innerhalb des europäischen Verbundsystems. Aufgrund seiner Ausdehnung, Komplexität und Steuerung über nationale Grenzen hinweg bedarf es einer Zusammenarbeit, die auch kulturelle, soziale, wirtschaftliche und politische Unterschiede der einzelnen Mitgliedstaaten im Blick hat**. Kennzeichnend für das europäische Energiesystem sind dessen verteilte Verantwortlichkeiten. Bemängelt wurde, dass diese noch nicht ausreichend aufeinander abgestimmt sind. Es gibt zwar Energieversorgungsunternehmen, die länderübergreifend agieren und eine Reihe von Aspekten werden ebenfalls zunehmend länderübergreifend oder regional gesteuert. **Wenn es jedoch um Cybersicherheitsthemen geht, werden Entscheidungen immer noch national getroffen, ohne die Komplexität der Wechselbeziehungen zwischen den Energie- und IT-Sektoren der Mitgliedstaaten einzubeziehen.**[29] Von den Teilnehmenden wurde betont, dass diese Herangehensweise nicht adäquat ist und noch kein ausreichendes Zusammenspiel der beiden Ebenen existiert.

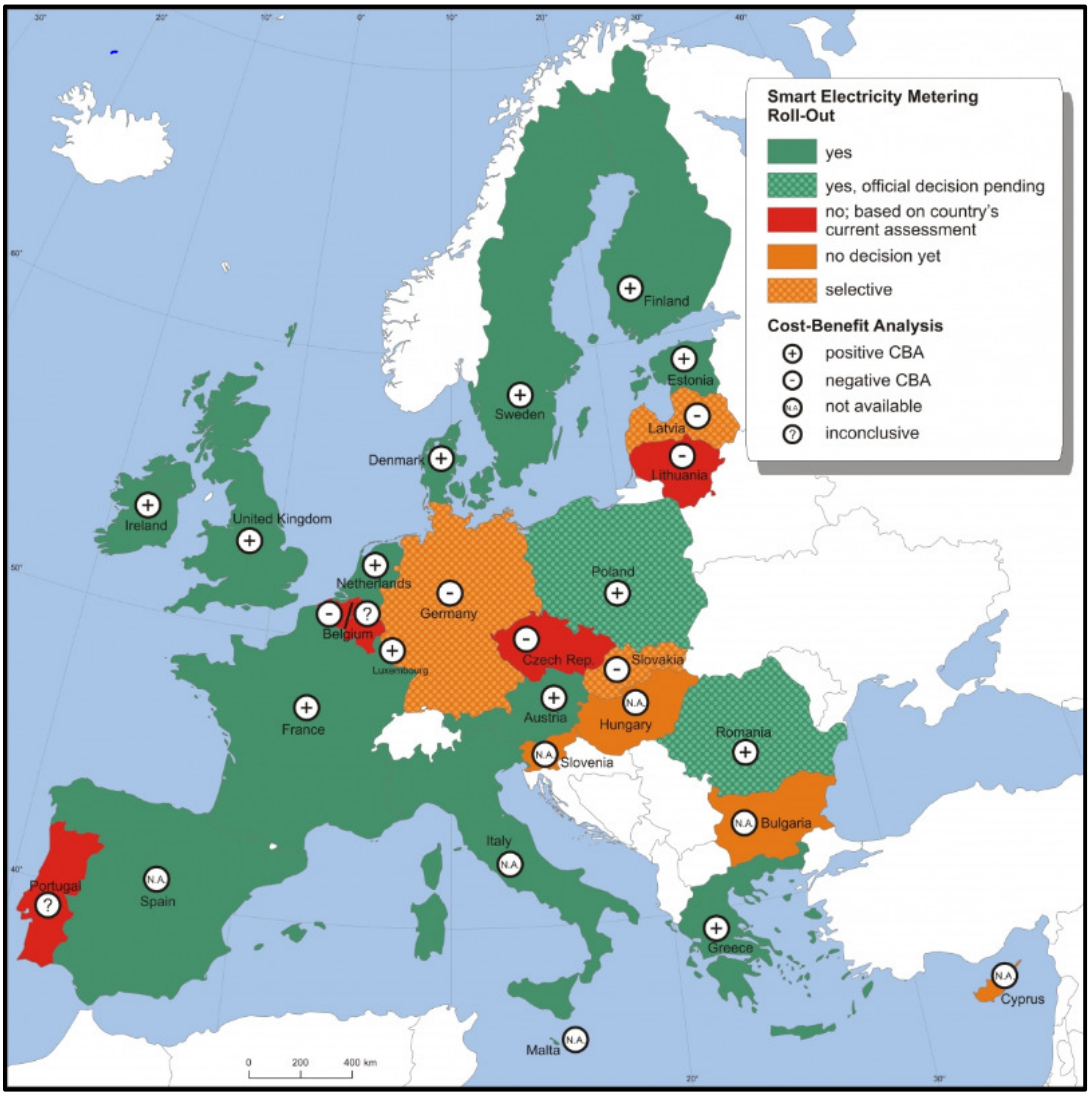
„Die Energiesituation in den einzelnen Mitgliedsländern ist so unterschiedlich, dass man bis jetzt noch nicht eine einzige Energiepolitik und eine Energieregulierung für alle verlangt hat.“ | POLITIK

Als konkretes Beispiel auf EU-Ebene wurden die Smart-Meter Technologien genannt, die in den Mitgliedstaaten unterschiedlich entwickelt werden. Während in einigen EU-Staaten bereits Smart-Meter installiert wurden, stehen in anderen EU-Staaten noch vorgeschaltete Entscheidungen bspw. zu den Kosten-Nutzen-Analysen aus.

Ebenfalls nicht einheitlich sind die Funktionen und Anforderungen der Smart-Meter. In der Vorstellung der Europäischen Kommission soll der Zweck der Smart-Meter sein, die Stromverbrauchswerte festzuhalten und zu kommunizieren, um so Abrechnungsvorgänge zu vereinfachen. Während die Mitgliedstaaten diesem Zweck in der Entwicklung der Smart-Meter selbstverständlich folgen müssen, strebt bspw. Deutschland einen Smart-Meter an, der zusätzlich Potenziale für weitere Funktionen mitbringt wie medizinische Dienstleistungen oder Ambient Assisted Living. „Alles, was per se höchste Vertraulichkeit verlangt und wo der normale Router zu Hause nicht sicher genug wäre […]“ (Politik). In Bezug auf die Sicherheit der Smart-Meter wurde signalisiert, dass der Impuls für den Rollout sehr früh kam, aber erst im Winterpaket das Thema „Datenschutz und Datensicherheit nach höchstmöglichen Standards“ aufgegriffen wurde. In der Zwischenzeit haben eine Mitgliedsländer bereits Technologien installiert und diesen Punkt gegebenenfalls weniger stark beachtet als Deutschland. Andere Länder haben Interesse am deutschen Ansatz signalisiert.

[29] Siehe auch: Enisa – European Union Agency For Network and Information Security (2016): Report on Cyber Security Information Sharing in the Energy Sector, Final Version 1.1

Abbildung 1: Entwicklung des Smart-Meter-Rollouts in Europa



Quelle: European Commission, Joint Research Centre, abrufbar unter http://ses.jrc.ec.europa.eu/smart-metering-deployment-european-union

Neben der technisch heterogenen Ausprägung der Smart-Metering-Messsysteme und der Herausforderung der Interoperabilität kann auch die Realisierung des Zugangs zu diesen Systemen problematisch sein: Wenn ein Land den Zugang stark reglementiert, ein anderes Land aber nicht, ist letztlich auch der Sicherheitsmechanismus kompromittiert. Das zeigt, dass eine europäische Zusammenarbeit so früh wie möglich, aber auch fortlaufend geschehen sollte, um Schwachstellen, Risiken und Chancen gemeinsam auszuloten.

Ein weiteres Themenfeld war die **Zusammenarbeit zwischen Wirtschaft und Politik, insbesondere bei der Herausforderung „Sicherheit in die Produkte zu bekommen“** (Politik

und Verwaltung)**.** Sicherheit wurde bereits in der Vergangenheit in diversen elektronischen, digitalen Produkten beachtet und mit Standards versehen, die mitunter freiwillig von der Wirtschaft entwickelt wurden. Bei der Digitalisierung des Energiesystems möchte der Staat stärker eingreifen „und einen verbindlichen Stempel“ (Politik und Verwaltung) daruntersetzen. Das erzeugt Reibungsfläche zwischen den Akteuren.

Für Deutschland wurde angemerkt, dass eine Zögerlichkeit von Seiten der Unternehmen besteht, Wissen über Schwachstellen in ihren IT-Systemen zu teilen. Im Fokus stand dabei das **Spannungsverhältnis einer vernünftigen Abwägung zwischen dem offenen Umgang mit Schadensfällen, sodass andere daraus lernen können, und der Vermeidung einer Bloßstellung, welche dem Unternehmen schaden könnte**. Auch der Austausch mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) wird mitunter kritisch beurteilt. Demnach wird das BSI von Seiten der Wirtschaft eher als schleppende Behörde gesehen, die Unternehmen bei zügigen Reaktionen stört.

Ein weiterer Teilnehmender betonte, dass statt hoch angesiedelter Gesprächsforen oftmals der informelle Austausch auf Arbeitsebene zwischen IT-Administratoren sehr fruchtbar sein kann. Deutlich wird hieran zum einen, dass es Differenzen zwischen wirtschaftlichen Interessen und politisch-kulturellen Sicherheitsvorstellungen bestehen. Zum anderen, dass der Faktor Mensch auch hier eine Rolle spielt. Ein Stichwort in diesem Zusammenhang ist Vertrauen, welches für eine erfolgreiche Kooperation in einem sensiblen Thema wie Cybersicherheit von großer Bedeutung ist.

2.7 Schlussbetrachtung

Im Trialog zur **Digitalisierung der Energiewende** debattierten die Teilnehmenden aus Politik und Verwaltung, Wirtschaft, der organisierten Zivilgesellschaft und der Wissenschaft gemeinsam mit Mitgliedern des Projekts ESYS darüber, wie robuste digitale Energieinfrastrukturen geschaffen werden können. Ziel des Trialogs war es die Perspektiven der unterschiedlichen Stakeholdergruppen zu sammeln, um somit gemeinsam den Antworten auf die Fragen, wie die Digitalisierung kritischer Energieinfrastrukturen gestaltet werden kann, welche Chancen sich daraus ergeben und welche Risiken und Herausforderungen entstehen, näher zu kommen.

Es konnte festgehalten werden, dass die Mehrheit der Teilnehmenden die Digitalisierung eines zunehmend erneuerbaren, dezentralen Energiesystems für nützlich ansieht, um die Versorgungssicherheit aufrecht zu erhalten und die Erneuerbaren weiter auszubauen. Neben der Versorgungssicherheit spielen aber auch andere Dimensionen von Sicherheit eine Rolle, wie z.B. IT-Sicherheit, Datensicherheit und Investitionssicherheit. Diese müssen im Blick gehalten werden, auch bei der Erforschung einer bestimmten Sicherheitsdimension.

Betont wurde, dass Sicherheitskonzepte, die eine sehr kurzfristige oder sektorielle Perspektive einnehmen und weder die Breitenwirkungen noch die Interdependenzen sehen, zu kurz greifen. **Für eine notwendige, durchdachte, nachhaltige Sicherheit muss ein Sektorüberschreitendes Verständnis, also ein integrierter Ansatz entwickelt werden**. Ebenfalls dürfen bei der Betrachtung des Gesamtsystems und der Möglichkeiten der Weiterentwicklung **nicht die vorhandenen Pfadabhängigkeiten vernachlässigt werden, ebenso wie der internationale Kontext**.

Ein weiteres prominentes Thema der Trialog-Diskussion war die Dezentralisierung des Energiesystems. Während der Demokratisierungsansatz weitestgehend verworfen wurde, konnte jedoch ein „Aktivierungspotenzial" der Dezentralisierung und Digitalisierung festgehalten werden: **das Thema Energie wird weit in die Gesellschaft hineingetragen und es existieren viele neue Teilhabeoptionen für die Verbraucher, Prosumer und Unternehmen**. Bezogen auf die Steuerung des Energiesystems wurde ein Mittelweg zwischen Dezentralität und Zentralität gefordert. Ein Vorschlag war, dass anstatt der Vorstellung nachzuhängen, dass es eine zentrale Steuerung bis zum kleinsten Element gibt, andere Möglichkeiten sinnvoller wären. Eine Option sei z.B. über Anreizstrukturen die wirtschaftlichen Entscheidungen von Einheiten in der Größenordnung oberhalb von privaten Haushalten mit zu beeinflussen. Somit könnte ein Fundament von Sicherheit geschaffen werden, indem z.B. einzelne Komponenten des Systems, wie Stadtwerke, durch Sektorkopplung selbstständig einen Minimalbetrieb aufrechterhalten können, ohne einen großen Austausch eingehen zu müssen.

Ein wichtiges Thema war der Faktor Mensch und die Frage nach seiner zukünftigen Rolle im Energiesystem im Vergleich zu automatisierten Prozessen. **Die Teilnehmenden kamen darüber ein, dass es in Zukunft beides geben wird: Menschliche Verantwortung und Algorithmen im Dienste des Menschen**. Dabei wurde bemängelt, dass es bisher zu wenig gute Programmierer und zu wenige speziell auf die Digitalisierung ausgerichtete Berufe in der Energiewirtschaft gibt. Eine Empfehlung war daher, dass sich Ausbildungen für Berufe, wie z.B. Elektroniker, ändern und mit einer viel stärkeren digitalen Komponente ergänzt werden sollten. Zusätzlich sollte es weitaus mehr Schulungen und Fortbildungen für Personal geben, damit den neuen Herausforderungen entsprechend begegnet werden kann. Das vom Bundeswirtschaftsministerium geförderte Kompetenzzentrum Digitales Handwerk (KDH) unterstützt bspw. den handwerklichen Mittelstand bei der Erschließung technischer und wirtschaftlicher Potenziale, die sich aus der digitalen Transformation für das Handwerk ergeben[30].

[30] siehe auch: https://handwerkdigital.de/

Im Trialog wurde zudem über Standards in unterschiedlichen Bereichen des Energiesystems diskutiert. Standards im Bereich der Sicherheit helfen einen Großteil, jedoch nicht alle Probleme abzudecken. Zudem wurde die Wirtschaftlichkeit von Standards betont. Durch Standards sind zum einen alle auf demselben Stand, was z.B. die Vernetzung untereinander erleichtern kann (z.B. durch gleiche Komponenten, Plug-and-Play). Zum anderen können durch Standards Veränderungen flächendeckender an die Masse kommuniziert werden (z.B. durch Updates).

Das grundlegende Dilemma von Standards – vorab definierten Strukturen versus flexiblen Anforderungen – konnte nicht aufgelöst werden. So treffen Standards und Zertifikate nur für bestimme, vorab definierte Fälle zu. Gerade durch die Digitalisierung des Energiesystems treten jedoch fortlaufend neue Anforderungen auf, auf die teilweise die gesetzten Standards nicht mehr zutreffen. Somit steht die Feststellung, dass Improvisationsfähigkeit Resilienz erhöht mit der anknüpfenden Frage, wie man diese in Standards „hinein bekommt“, weiter zur Diskussion.

Im Bereich der IT-Sicherheit konnten folgende Punkte als richtungsweisende Antworten auf die Frage „wie schaffen wir robuste digitale Energieinfrastrukturen?“ identifiziert werden:

- Es sollte **mehr Austausch über Probleme, bemerkte Angriffe oder Schadsoftware geben**. Besonders der Austausch in kleiner Runde auf der Arbeitsebene bzw. im inoffiziellen Rahmen scheint dafür geeignet.
- Ebenfalls sollten andere digitalisierte Systeme (z.B. Luftfahrtbereich), die nicht mehr alleine von Menschenhand geführt werden können, betrachtet werden. Daraus könnten weitere Schlüsse für die Energieversorgung gezogen werden.
- Im IT-Bereich können Risiken dadurch eingedämmt und Resilienz geschaffen werden, indem die **Komplexität von Programmiersystemen verringert und mehr Qualitätssicherung betrieben wird**. Bei der Entwicklung von sicherheitssensibler Software wie bspw. dem Smart-Meter sollte man Wettbewerb schaffen, indem mehrere Unternehmen mit der Entwicklung systemtauglicher, interoperabler Lösungen beauftragt werden. Diese Unternehmen konkurrieren jedoch nicht um Marktanteile, sondern um Qualität. Fällt später in der Nutzung eine dieser Softwarelösungen aus, gäbe es immer noch weitere Alternative, auf die sich das System stützen kann.
- **Daran anschließend sollte Dezentralität unterstützt werden: viele unterschiedliche Systemkomponenten, die einander vollständig kompensieren können und möglichst geringe gegenseitige Abhängigkeiten haben** (Je weniger ausfallen kann, desto besser). Es sollte ein Mittelmaß zwischen sehr vielen, nicht mehr steuerbaren Einheiten im Vergleich zu einem zentralen Element geben.

- Gestützt auf den IT-Security Lifecycle wurde ein Umdenken im Bereich des Risikomanagements gefordert. Systeme sollten unter der Annahme entwickelt werden, dass „etwas passieren“ könne.
- Trotz Komplexität von IT-Themen ist der Dialog mit der Gesellschaft wichtig, gerade im Energiebereich. Es muss eine gemeinsame Sprache gefunden werden, um nicht nur zur technologischen Entscheidungen zu gelangen, sondern auch zu gesellschaftlich und politisch tragfähigen.

Offene Fragen

Es konnten nicht alle Fragen abschließend geklärt werden, sondern müssen mitunter auch in die weitere Forschungsarbeit einfließen:

- Wie kann sichergestellt werden, dass für die Fälle, in denen ein **Standard** nicht greift, trotzdem die richtige Entscheidung getroffen wird? Wie verlässlich ist ein zertifizierter und getesteter Standard (System, Software etc.)? Welches Minimalset an Standards wird benötigt?
- Zukünftig wird es weltweit unterschiedlich (von zentral bis dezentral) konzipierte Energiesysteme geben. Wo sind die **Schnittstellen** zwischen den Akteuren, wo liegen die Entscheidungskompetenzen und wie sollen die Austauschverhältnisse geregelt werden? Welcher Minimal-Grid-Code wird für die Zusammenarbeit zwischen den Ländern benötigt?
- Ist eine dezentrale Organisation des Risikos (= Managen der Infrastruktur) besser geeignet als die Art und Weise, wie es zurzeit gehandhabt wird? Wie viele unterschiedliche Subsysteme können unabhängig voneinander stabil sein?
- Welche **Vision** haben wir für den Abschluss der Energiewende? Wie können wir den Weg dorthin gestalten?
- Wie kann sichergestellt werden, dass Sicherheitslücken schnell entdeckt und ausgebessert werden? Wie kann gewährleistet werden, dass die "Instandhaltung der Sicherheit" ein fortlaufender Prozess ist?
- Wie wird mit dem Aushandeln von Datentransparenz im Mehrfamilienhaus umgegangen, wenn der Vermieter Smart-Metering nutzten will, einzelne Haushalte aber unterschiedlich viele Daten weitergeben möchten?
- Wer bezahlt für Sicherheit und wie bringen wir Gerechtigkeit ins System? Was ist der Gegenwert von Sicherheit?
- Was bedeutet es, wenn die Netzstromsolidarität einbricht? Wie sollten Regelungen aussehen, sodass sich Produzenten und Konsumenten nicht durch bilateralen Handel (bspw. über Blockchain) aus dem Gesamtsystem verabschieden können?
- In welchen Bereichen kann die Wirtschaft selbst durch Normung sichere Standards

zur Digitalisierung kritischer Infrastrukturen etablieren? Wo braucht es staatliche Regulierung? Wie können Unternehmen mit diesen Entwicklungen strategisch umgehen?

- Vor dem Hintergrund der Dezentralisierungsdiskussion stellt sich die Frage, welche Rolle die Kommunen bei der Etablierung von digitaler Sicherheit im Energiesystem spielen könnten? Wenn aufgrund von Sicherheitsaspekten, aber auch von Beteiligungsbegehren ein zentraler Masterplan nicht greift, ist es möglich Richtwerte oder Wenn-Dann-Bedingungen in Sicherheitskonzepte einzubauen?

3 Ausblick auf Folgeaktivitäten

Dieser Bericht wird den Wissenschaftlerinnen und Wissenschaftlern des Projekts ESYS für ihre weitere Arbeit zur Verfügung gestellt. Die Ergebnisse dieses Berichts dienen zudem als Grundlage für das Fachgespräch, welches am Mittwoch, den 30. Mai 2018 stattfindet.

Der Trialog zum Thema Cyber Resilienz war der vierte Trialog in der zweiten Projektphase des Akademienprojekts Energiesysteme der Zukunft. Bis zum Ende der Projektlaufzeit im Februar 2019 erhalten die Arbeitsgruppen des Akademienprojekts die Möglichkeit mit den Trialogen in den Dialog mit der Gesellschaft zu treten und aktuelle Forschungsfragen durch dieses Format auf Augenhöhe mit Akteuren aus Politik, Wirtschaft und organisierter Zivilgesellschaft zu diskutieren.

Der nächste Trialog fand unter dem Titel „Bioenergiepotenziale richtig bewerten und nutzen, Nebenwirkungen eindämmen. Wie soll eine langfristige Bioenergiestrategie gestaltet sein?“ am 23. Februar 2018 statt. Ziel des Trialogs war eine breite gesellschaftliche Diskussion zum Beitrag und Potenzialen von Bioenergie in der zukünftigen Energieversorgung Deutschlands und zur Rolle von Bioenergie mit Kohlendioxidabscheidung und Speicherung (CCS) für den Klimaschutz.

Der nächste Trialog findet am Montag, den 28. Mai 2018 in Kooperation mit der ESYS-Arbeitsgruppe „Energieversorgung zentral/dezentral“ statt. Unter dem Titel „Dezentralisiert! Die Balance für ein nachhaltiges, zuverlässiges und bezahlbares Energiesystem finden“ werden Fragen, wie unser Energiesystem 2050 aussehen soll und wie die Entwicklungen des Energiesystems in eine dezentralere oder zentralere Richtung – mit Blick auf Gesamtkosten, Akzeptanz oder Arbeitsplätze – zu bewerten sind, gemeinsam zwischen ESYS-Fachleuten und Stakeholdern aus Politik und Verwaltung, Wirtschaft und organisierter Zivilgesellschaft diskutiert.

4 Annex

Annex I: Konzept der Trialoge®

Das Trialog-Verfahren

Die Trialoge der HUMBOLDT-VIADRINA Governance Platform sind ein erprobtes Verfahren, um **gesellschaftspolitische Diskussionen fair und vertrauensbildend** zu gestalten und politische Entscheidungsprozesse fundiert vorzubereiten. Hauptpunkte des Verfahrens sind eine ganztägige Trialog-Veranstaltung mit relevanten Stakeholdern im Rahmen des zu diskutierenden Themas sowie die anschließende Analyse der Diskussion.

Als Stakeholder fungieren in den Trialogen Vertreterinnen und Vertreter von Politik, Wirtschaft und organisierter Zivilgesellschaft, begleitet von Wissenschaft und Medien. Sie treten in einen argumentativen Austausch miteinander, einer sog. **Deliberation**. Ziel unserer Trialog-Veranstaltungen ist es, **Verständigungsprozesse durch Perspektivenvielfalt und die Begründung von Argumenten zu initiieren und Grundkonsense zu erarbeiten.**

Die Teilnehmerinnen und Teilnehmer decken aufgrund ihrer unterschiedlichen Funktionen, Erfahrungen und Machtpotentiale und dank der Deliberation untereinander ein breites Spektrum wesentlicher gesellschaftlicher Perspektiven ab. Durch ihre argumentative, durchaus konflikthafte Auseinandersetzung schaffen sie Transparenz, eröffnen Win-Win-Situationen und bereiten so einen überparteilichen Korridor vor, innerhalb dessen **gemeinwohlorientierte Lösungen** gefunden und nachhaltige Entscheidungen getroffen werden können.

Dazu ist es unabdinglich, dass die Offenheit des vertraulichen Austausches gewahrt wird und Positionen nicht von vornherein ausgeschlossen werden. Ebenso sollen die Positionen nicht einfach nebeneinander oder einander gegenübergestellt werden, sondern argumentativ aneinander anknüpfen. Nur so kann ein Verständigungsprozess angeregt werden, der breit akzeptierte Lösungen vorbereitet.

Wichtig ist zu diesem Zweck, die Teilnehmenden so auszuwählen, dass sie in ihrem Bereich kompetent und ebenso argumentationsfähig wie verständigungswillig sind. Über die **Chatham House Rule**[31] wird Vertraulichkeit hergestellt, die durch eine kompetente und faire Moderation weiter unterstützt wird.

[31] „Bei Veranstaltungen (oder Teilen von Veranstaltungen), die unter die Chatham-House-Regel fallen, ist den Teilnehmern die freie Verwendung der erhaltenen Informationen unter der Bedingung gestattet, dass weder die Identität noch die Zugehörigkeit von Rednern oder anderen Teilnehmern preisgegeben werden dürfen.“ Royal Institute of International Affairs, London.

Trialoge im Rahmen des Projektes „Energiesysteme der Zukunft“

Das Projekt „Trialoge als transdisziplinäre Dialogplattform für die interdisziplinären Arbeitsgruppen im Projekt: Energiesysteme der Zukunft II“ wird im Zeitraum 2016 – 2019 insgesamt acht Trialoge für die ESYS-Arbeitsgruppen durchführen. Im April 2013 haben acatech – Deutsche Akademie der Technikwissenschaften, die Nationale Akademie der Wissenschaften Leopoldina und die Union der deutschen Akademien der Wissenschaften das interdisziplinäre Projekt „**Energiesysteme der Zukunft**“ (ESYS) gestartet. Rund 100 Expertinnen und Experten aus Wissenschaft sowie unternehmensseitiger Forschung erarbeiten seitdem wissenschaftlich fundierte Handlungsoptionen für die Gestaltung einer sicheren, bezahlbaren und nachhaltigen Energieversorgung. Um die Positionen unterschiedlicher Stakeholder einbeziehen zu können, tauschen sich die ESYS-Arbeitsgruppen in verschiedenen Dialogformaten mit Vertreterinnen und Vertretern der Politik, Wirtschaft und organisierten Zivilgesellschaft aus. Das Projekt ESYS wird vom Bundesministerium für Bildung und Forschung gefördert. Acatech hat die Federführung übernommen.

Die **Trialoge** ergänzen die wissenschaftlichen Arbeitsgruppen des Projekts durch eine Erweiterung hin zur **Transdisziplinarität**. Im Zentrum der Diskussion stehen die interdisziplinäre Forschungsarbeit der Arbeitsgruppen und deren Implikationen für die Gesellschaft ebenso wie gesellschaftliche Anliegen in Bezug auf das Thema der Arbeitsgruppen. Damit soll wissenschaftlich-analytische Forschung stärker mit gesellschaftlichem Erfahrungswissen und gesellschaftlich-politischen Entscheidungs- und Problemlösungsprozessen zusammengebracht werden. Diese bieten den wissenschaftlichen Arbeitsgruppen die Möglichkeit, in einem vergleichsweise kleinen und vertraulichen Rahmen ihre (Zwischen-)Ergebnisse methodisch reflektiert mit Vertreterinnen und Vertretern der Gesellschaft - also aus Wirtschaft, Politik und organisierter Zivilgesellschaft - ganztägig zu diskutieren. Sie erhalten so eine Rückkoppelung zu ihrer Forschungsarbeit durch die Gesellschaft, deren Interessenvertreterinnen und -vertreter zugleich Wissensträger sind. Durch die transdisziplinären Trialoge können neue Herangehensweisen an wissenschaftliche Themen eröffnet werden, weitere Forschungsbedarfe aufgedeckt und neues Wissen durch Verständigung generiert werden. Gleichzeitig wird die verfügbare Wissensbasis auch für Vertreter der Gesellschaft vertieft und damit das gesellschaftliche Handlungsvermögen gesteigert. Langfristig trägt ein gesellschaftlich robustes Wissen, insbesondere in der Energiewende dazu bei, dass wichtige anstehende Entscheidungen gesellschaftlich informiert unterstützt werden und Politik nachhaltig gestaltet werden kann. Entsprechend möchten die Trialoge wissenschaftlicher Arbeit nicht konfrontativ abprüfen, sondern sie stellen eine Möglichkeit zum partnerschaftlichen Austausch dar mit dem besten Nutzen für alle Beteiligten.

Annex II: Durchgeführte Agenda

Risiken smart managen.
Wie schaffen wir robuste digitale Energieinfrastrukturen?

Am 14. Dezember 2017, im Allianz Forum (Pariser Platz 6, 10117 Berlin)

09:00 Anmeldung und Kaffee

09:30 Begrüßung und Einführung
Prof. Dr. Dr. h.c. G. Schwan, HUMOBLDT-VIADRINA Governance Platform

09:50 Inhaltliche Einführung
Prof. Dr. Sebastian Lehnhoff, OFFIS Institut für Informatik

10:10 kurze Fragerunde

10:20 Input-Vorträge aus Wirtschaft und organisierter Zivilgesellschaft

Dr. Friederike Ernst, Gnosis und Blockchain Bundesverbands e.V.

Linus Neumann, Chaos Computer Club (CCC)

10:55 Kaffeepause

11:15 Diskussion zwischen allen Teilnehmenden

13:00 Mittagspause

14:00 Input-Vortrag Politik & Verwaltung

Alexander Kleemann, Bundesministerium für Wirtschaft und Energie (BMWi)

14:45 Parallele Workshops

WS 1: Ist die Resilienz kritischer Infrastrukturen durch die Digitalisierung gefährdet? Wie können Standards die Energiewende gelingen lassen?
Maximilian Dauer, Siemens AG und Martin Uhlherr, Deutsches Institut für Normung (DIN)

WS 2: Verändert die digitale Energiewende die Rolle privater Haushalte?
Dr. Thomas Engelke, Verbraucherzentrale Bundesverband

16:00 Kaffeepause

16:15 Vorstellung der Workshop-Ergebnisse

16:30 Diskussion zwischen allen Teilnehmenden und Zusammenfassung

17:00 Ausklang der Veranstaltung

Annex III: Stakeholderauswertung

Einladungsmanagement

Basis für die Einladungen war die detaillierte Kontaktdatenbank der HUMBOLDT-VIADRINA Governance Platform, die relevante Akteure aus verschiedenen Stakeholdergruppen des Themenbereichs Energie umfasst. Sofern entscheidende Akteure für das konkrete Thema aus den Stakeholdergruppen noch nicht vorlagen, wurden diese gezielt recherchiert. Auf Grundlage dieser Datenbank von rund 2000 Kontakten wurden entsprechend ihrer Schwerpunktsetzung 757 Personen eingeladen. Es wurden gemäß dem Trialog-Konzept eine Anzahl von etwa 50 Teilnehmenden und eine etwa gleichmäßige Verteilung in Bezug auf die drei Stakeholdergruppen Politik und Verwaltung, Unternehmenssektor und organisierte Zivilgesellschaft angestrebt. Neben den Wissenschaftlerinnen und Wissenschaftlern der Arbeitsgruppe Energieunion wurden Vertreterinnen und Vertreter aus weiteren wissenschaftlichen Institutionen eingeladen. Auch die Medien erhielten die Möglichkeit zur Teilnahme.

Zur Veranstaltung hatten sich 67 Personen angemeldet. Tatsächlich teilgenommen haben schließlich **49 Personen** (18 weiblich, 31 männlich), die **38 Organisationen und Unternehmen** vertraten. Die Ausfälle waren zumeist aufgrund kurzfristiger Termine sowie Krankheit zustande gekommen. Unter den Teilnehmenden waren drei Vertreterinnen der HUMBOLDT-VIADRINA sowie vier Mitarbeiterinnen und Mitarbeiter von acatech.

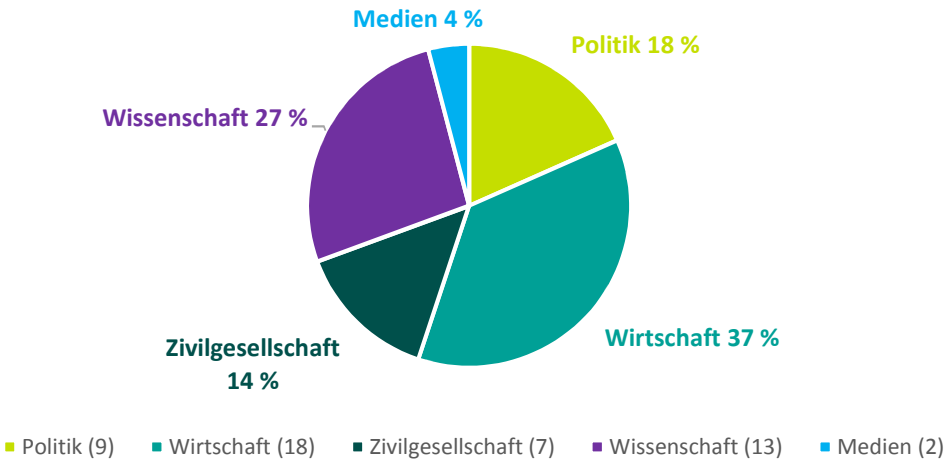
Zusammensetzung der Teilnehmenden gemäß Stakeholdergruppen

Die Teilnehmenden der Veranstaltung verteilten sich entsprechend der Kernidee des Trialog-Konzepts auf die Bereiche Politik und Verwaltung, Wirtschaft, organisierte Zivilgesellschaft und Wissenschaft.

Von Seiten der **Wissenschaft** nahmen insgesamt 13 Vertreterinnen und Vertreter teil, u.a. aus dem Institut für ökologische Wirtschaftsforschung (IÖW), dem Wissenschaftszentrum Berlin für Sozialforschung (WZB), dem OFFIS- Institut für Informatik und der Stiftung Wissenschaft und Politik (SWP).

Einen etwas größeren Anteil (18 Personen) stellte bei diesem Trialog die Stakeholdergruppe **Wirtschaft**. Vertreten waren große Unternehmen aus den Bereichen Energieversorgung und -erzeugung (EnBW; Vattenfall, innogy se) sowie Beratung (Ecofys, Strategieberatung Neue Mobilitätssysteme). Ebenfalls nahmen diverse Organisationen und Verbände aus dem IT- und Digitalisierungsbereich, wie die STROMADAO UG, VHP Ready - Virtual Heat and Power, Webolution GmbH, Gnosis und der Digitalverband Bitkom sowie ein Vertreter der Siemens AG teil.

Zusammensetzung der Teilnehmenden gemäß Stakeholderzugehörigkeit (n=49)
Werte in absoluten Zahlen siehe unten.



Die **organisierte Zivilgesellschaft** wurde u.a. durch die Verbraucherzentrale Bundesverband, den Chaos Computer Club (CCC) und den Deutschen Gewerkschaftsbund (DGB) mit insgesamt 7 Personen vertreten.

Aus dem **politischen Bereich** kamen 9 Vertreterinnen und Vertreter des Bundesministeriums für Wirtschaft und Energie, der Energie.Agentur.NRW, dem Deutschen Institut für Normung (DIN) und dem Umweltbundesamt (UBA). Die **Medien** waren durch eine Redakteurin des Tagesspiegels und das Fachmedium BIZZenergy vertreten.

Aufgrund von Krankheit und terminlichen Engpässen fielen insbesondere im Bereich der organisierten Zivilgesellschaft kurzfristig einige angemeldete Personen aus, so dass die Balance der Stakeholderzusammensetzung nur mäßig eingehalten werde konnte.

Übersicht der vertretenen Institutionen

Die folgende Übersicht listet die vertretenden Institutionen auf, aus denen die Teilnehmenden entsandt wurden. Sie verdeutlicht die breite Zusammensetzung der Teilnehmerschaft:

4Sing GmbH, Governance and Strategic Foresight
acatech - Deutsche Akademie der Technikwissenschaften, Geschäftsstelle Energiesysteme der Zukunft
activeMind AG
Bitkom
BIZZenergy
Blockchain Bundesverband e.V.
Buildings Performance Institute Europe (BPIE)
Bundesministerium für Wirtschaft und Energie (BMWi)
Center for Innovation & Sustainability in Tourism
Chaos Computer Club (CCC)
Der Tagesspiegel
Deutscher Gewerkschaftsbund (DGB)
Deutsches Institut für Normung (DIN)
Die Denkbank
Ecofys
EnBW Energie Baden-Württemberg AG
Energie City Leipzig
EnergieAgentur.NRW
European Center for Sustainability Research (ECS)
HUMBOLDT-VIADRINA Governance Platform gGmbH
innogy Innovation Hub
innogy SE
Institut für betriebliche Bildungsforschung (IBBF)
Institut für Klimaschutz, Energie und Mobilität – Recht, Ökonomie und Politik e.V. (IKEM)

Institut für ökologische Wirtschaftsforschung (IÖW)
Johanssen & Kretschmer
OFFIS - Institut für Informatik Oldenburg
Siemens AG
STROMDAO UG
Sustainable Strategies
SWP-Stiftung Wissenschaft und Politik
Umweltbundesamt (UBA)
Vattenfall GmbH
Verbraucherzentrale Bundesverband e.V.
VHP Ready - Virtual Heat and Power
Webolution GmbH
WFS Wachstums-Förderungs-Strategie - Systemberatung für zukunftsweisende Lösungen"
Wissenschaftszentrum Berlin für Sozialforschung (WZB)

Annex IV: Impulspapier für den Trialog

Impulspapier zum Trialog am 14. Dezember 2017

HUMBOLDT-VIADRINA Governance Platform

Risiken smart managen.
Wie schaffen wir robuste digitale Energieinfrastrukturen?

Dr. des. Achim Eberspächer (Geschäftsstelle Energiesysteme der Zukunft), Prof. Dr. Sebastian Lehnhoff (Univ. Oldenburg), Dr. Christoph Mayer (OFFIS)

Die Hacker hatten den Angriff vom 23. Dezember 2015 viele Monate vorbereitet: Zunächst schleusten sie Schadsoftware in die Computersysteme dreier ukrainischer Stromversorger ein. Über einen langen Zeitraum sammelten sie in deren Netzen Informationen zu den verwendeten Computersystemen – unter anderem Zugänge, Userdaten und Passwörter – bis sie die Kontrolle über die leittechnischen Systeme übernehmen konnten. Damit gelang es ihnen, mehrere Umspannwerke vom Netz zu trennen. Gleichzeitig löschten sie Systemdateien und legten das Call-Center eines der Versorger lahm, damit dieser sich nicht durch Anrufe betroffener Kunden ein Bild vom Ausmaß der Ausfälle machen konnte. Bis es den Verteilnetzbetreibern gelang, die Versorgung wiederherzustellen, waren über 200.000 ukrainische Haushalte ohne Strom.[32] Wer Marc Elsbergs Roman „Blackout“ gelesen hat, für den könnten solche Ereignisse als Vorgeschmack auf großflächige und langdauernde Stromausfälle wirken, die durch die Digitalisierung des Stromsystems überhaupt erst möglich werden. Digitalisierung erschiene somit als Entwicklung, die das Energiesystem effizienter, aber auch anfälliger macht: für (Hacker-)Angriffe genauso wie für andere neue Störungsquellen wie Datenfehler.

Auf der anderen Seite tragen Informations- und Kommunikationstechnologien (IKT) seit langem dazu bei, das Energiesystem sicher zu betreiben. IKT ist etwa notwendig, um das Netz zu überwachen und zu steuern, kritische Situationen frühzeitig zu erkennen und abgestimmt Gegenmaßnahmen zu ergreifen. IKT-Maßnahmen betreffen insbesondere den Informationsaustausch sowohl zwischen Akteuren als auch zwischen Geräten und Teilsystemen. Fehler wie die großen europäischen Stromausfälle im Jahr 2006, ausgelöst durch das planmäßige Abschalten einer Leitung für die Durchfahrt eines Kreuzfahrtschiffs über die Ems, wären durch einen besseren Informationsaustausch vermieden worden.

Die IKT zeigt sich also als janusköpfig – aber was heißt das nun für die Anforderungen an die zukünftigen digitalen Energieinfrastrukturen? Welche Risiken, aber auch welche Chancen bieten diese Entwicklungen? Welche neuen Herausforderungen und Rollen könnten hier auf unterschiedlichste Beteiligte zukommen? Wie schnell und wie radikal können und müssen Energieinfrastrukturen digitalisiert werden?

„Robustheit“ und „Resilienz“ als Leitbilder

Das Energiesystem ist eine kritische Infrastruktur: Kritische Infrastrukturen (KRITIS) sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere drastische Folgen eintreten würden. Bedeutende Eigenschaften einer kritischen Infrastruktur sind daher Robustheit und Resilienz.

[32] Vgl. E-ISAC/Sans: Analysis of the Cyber Attack on the Ukrainian Power Grid. Defense Use Grid, 2016, URL: http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.

Man bezeichnet ein technisches System als ***robust***, wenn es die meisten erwartbaren Störereignisse bewältigt, ohne dass seine Funktionsfähigkeit wesentlich beeinträchtigt wird. Das Stromsystem leistet dies u.a. durch das sogenannte N-1-Prinzip: Jedes wesentliche Element im System gibt es einmal mehr als für die Höchstlast im Normalbetrieb nötig. Wenn ein Stromerzeuger, eine Leitung oder ein Transformator ausfällt, übernimmt ein anderer seine Funktion, ohne dass es zu Stromausfällen kommt.

Gegenüber Belastungen mit potenziell großem Schaden, die sich schlecht quantifizieren und prognostizieren lassen und überraschend eintreffen, ist *Resilienz* die beste Versicherung.[33]

> Resilienz ist die Fähigkeit eines Systems, seine Funktionsfähigkeit unter Belastungen aufrechtzuerhalten beziehungsweise kurzfristig wiederherzustellen.

Resilienz geht über Robustheit noch hinaus. Man bezeichnet ein System als ***resilient***, wenn seine Funktionsfähigkeit bei Störungen nur wenig beeinträchtigt wird, es zu keinen größeren Schäden kommt und nach der Störung so schnell wie möglich wieder die volle Leistung zur Verfügung steht.

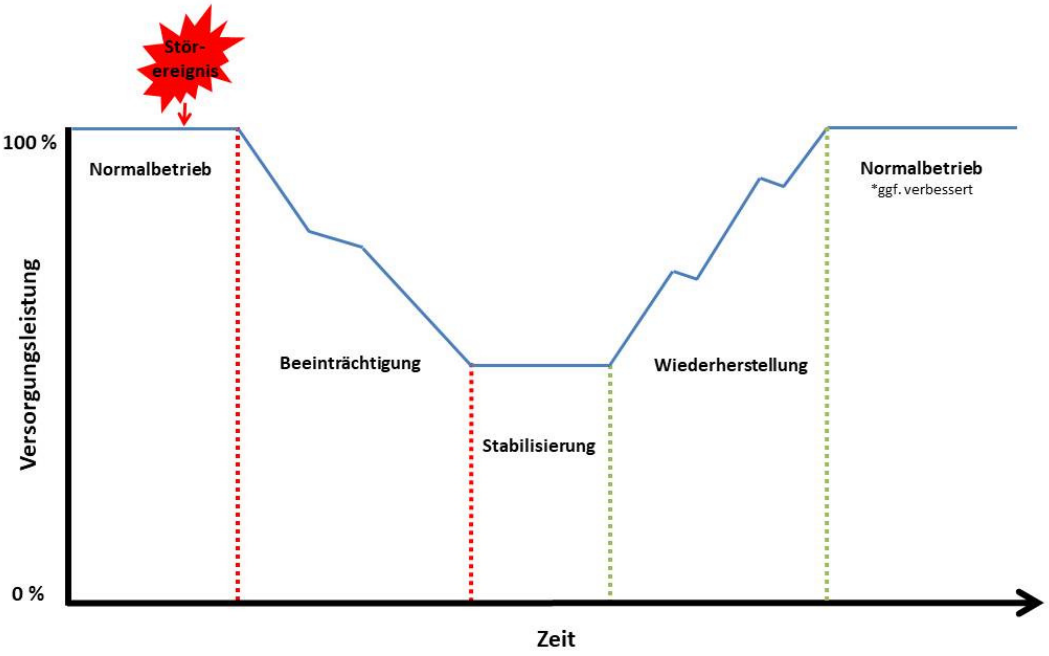


Abbildung 2: Wiederherstellung der Funktionsfähigkeit eines resilienten Systems

Insbesondere das deutsche Stromsystem hat in der Vergangenheit Robustheit und Resilienz immer wieder eindrucksvoll bewiesen. Gemessen am SAIDI-Index[34], dem wichtigsten Indikator für die Zuverlässigkeit des

[33] acatech – Deutsche Akademie der Technikwissenschaften/Nationale Akademie der Wissenschaften Leopoldina/Union der deutschen Akademien der Wissenschaften (Hrsg.): Das Energiesystem resilient gestalten. Maßnahmen für eine robuste Versorgung (Schriften reihe zur wissenschaftsbasierten Politikberatung), 2017, URL: https://energiesysteme-zukunft.de/fileadmin/user_upload/Publikationen/pdf/ESYS_Stellungnahme_Das_Energiesystem_resilient_gestalten.pdf.

[34] Der **System Average Interruption Duration Index (SAIDI)** gibt die durchschnittliche Ausfalldauer je versorgtem Verbraucher an, wobei jedoch weder lange andauernde Stromausfälle, noch solche von weniger als drei Minuten berücksichtigt werden. SAIDI misst die Zuverlässigkeit eines Stromsystems.

Stromsystems, ist die deutsche Stromversorgung eine der zuverlässigsten der Welt. Sie steht nun allerdings vor neuen Herausforderungen.

Zentrale Entwicklungen

Für die Herausforderungen, die die Digitalisierung der kritischen Infrastruktur Energie mit sich bringt, sind drei Entwicklungen maßgeblich:

1. Der **Umbau des Energiesystems** in Richtung Erneuerbarer Energien schreitet voran. Kleinere Anlagen, deren Erzeugung wetterabhängig schwankt, ergänzen und ersetzen Großkraftwerke. Durch immer mehr dezentrale Einspeisung etwa aus Photovoltaik-Dachanlagen kehren Lastflüsse sich um und beanspruchen das Verteilnetz immer stärker. Das Geschehen im Verteilnetz wird maßgeblich für die Energieversorgung – auch bei der Systemsicherheit. Diese technologische Herausforderung für die Systemstabilität führt zu Anpassungen unter anderem bei Systembetrieb, Netzausbau, Markt, Akteuren, Betreiberstrukturen oder der Regulierung. Demand Side Management, Eigenverbrauchsoptimierung oder Elektromobilität werden diese Komplexität noch weiter erhöhen. Ohne Informationstechnologie wäre es nicht möglich gewesen, die Millionen neuer Erzeuger – insbesondere Photovoltaik-Dachanlagen[35] – relativ reibungslos ins System zu integrieren. Der weitere Umbau des Energiesystems und die damit steigende Komplexität werden einen massiv höheren Einsatz von IKT erfordern. Eine Schwierigkeit ist es hierbei, dass die die IKT-Komponenten, die nötig sind, um die Stromversorgung nach einem Ausfall wieder hochzufahren, selbst von der Stromversorgung abhängig sind.
2. Die großen **Digitalisierungstrends** werden unsere Welt vielfältig verändern. Ambient Intelligence, Internet of Things and Services, Cloud-Lösungen und Outsourcing sind nur einige davon, die in allen Teilen der Gesellschaft große Auswirkungen haben werden. Auch in der Energieversorgung finden sich viele entsprechende Anwendungen in Erprobung oder schon im Betrieb. In diesem Umfeld müssen neue Regularien geschaffen werden, etwa zu Datenschutz, Monopolrecht und Sicherheit. Disruptionen auf Geschäftsmodellebene werden auch in der Energieversorgung Einzug halten. Die Blockchain-Technologie könnte die Bereitstellung von Kilowattstunden in kleinen Mengen als Mikrotransaktionen detailliert nachvollziehbar machen und die zugehörigen Abrechnungen radikal vereinfachen.
3. Gleichzeitig verändert sich die **Bedrohungslage für Cyberattacken**. Komplexe und hochprofessionalisierte Wertschöpfungsnetzwerke sind entstanden, die Schwachstellen in digitalen Infrastrukturen ausnutzen, um Profit zu erzielen. Eine weitere Bedrohung entsteht durch Staaten, die Cyberattacken durchführen oder beauftragen. Die Bedrohungslage wird nach Ansicht vieler Expertinnen und Experten noch dadurch verschlimmert, dass staatliche Organisationen – wie die NSA oder vorgesehene Stellen im Bundesinnenministerium für Cyberangriffe – Wissen über Sicherheitslücken geheim aufkaufen und Angriffswerkzeuge entwickeln. Dadurch bleiben Schwachstellen in IKT-Systemen lange Zeit bestehen, während die Angriffswerkzeuge in die Hände krimineller Angreifer gelangen können[36]. Das Bundesinnenministerium plant sogar, „Hintertüren“ in vernetzten Geräten und Computern gesetzlich festzuschreiben, also eine technische Möglichkeit für den Staat, jederzeit auf jedes Gerät zugreifen zu können. Für die Kriminalitätsbekämpfung wäre das ein großer Gewinn, zugleich aber auch ein unüberschaubares Sicherheitsrisiko.

[35] Die Anzahl der Windkraftanlagen in Deutschland betrug 2016 etwas über 27.000 (https://www.wind-energie.de/infocenter/statistiken/deutschland/windenergieanlagen-deutschland).
[36] Das Schadprogramm WannaCry, das im Mai 2017 über 250.000 Rechnerin 150 Ländern infizierte, beruht vermutlich auf einem Werkzeug, das für die NSA entwickelt wurde.

Die skizzierten Entwicklungen machen die digitalisierte kritische Infrastruktur Energie komplexer. Je komplexer und dynamischer ein System, desto schlechter lassen sich die Wirkungen einzelner Störfaktoren und ihr Wechselspiel prognostizieren. Daher können selbst bei bester Vorabanalyse unter anderem bei Sicherheitsvorschriften, Grid Codes und Regulierung Fehler begangen werden, die das Energiesystem gefährden können.

Thesen und Handlungsbedarf

Beinahe alle weiteren kritischen Infrastrukturen wie etwa Transport, Wasserversorgung oder auch die medizinische Versorgung hängen unmittelbar von Energie im Allgemeinen und Strom im Besonderen ab. Allein der finanzielle Schaden durch einen großräumigen Stromausfall wäre gewaltig: Eine Studie schätzte die Kosten eines nur einstündigen deutschlandweiten Stromausfalls an einem Werktag im Winter auf 0,6 – 1,3 Milliarden Euro.[37] Schafft man es nicht, das neue Energiesystem resilient zu gestalten, kann das drastische Folgen haben. Gleichzeitig ermöglicht hohe Robustheit und Resilienz viel mehr Freiheiten für alle Akteure, die Energiewende durch ihre Ideen und Initiativen ohne viele Einschränkungen voranzubringen. Die Digitalisierung ist und bleibt tragende Säule der Energiewende.

Dies führt zu zwei zentralen Anforderungen: erstens (mindestens) die Absicherung des heutigen Standes bei Robustheit und Resilienz und zweitens das Beibehalten des Tempos oder besser noch die Beschleunigung der Energiewende. Aus ihnen müssen und können Priorisierungen der notwendigen Maßnahmen zur Erreichung von (Cyber-)Resilienz abgeleitet werden.

These 1: Die Resilienz des zukünftigen Energiesystems steht und fällt mit der Digitalisierung der Funktionen zur Systemstabilisierung.

Schon heute beruht die Resilienz des Energiesystems auch auf Digitalisierung, da sie über eine genaue Kenntnis und Prognose des Netzzustandes die Maßnahmen zwischen den Akteuren hilft abzustimmen und durchzuführen. Zentral sind hier die Übertragungsnetzbetreiber, die durch digitale Messtechnik und Software genauestens über ihr Netz Bescheid wissen, durch Vernetzung ihrer IKT-Systeme untereinander auch über den Netzzustand über das eigene Verantwortungsgebiet hinaus. Sie haben auch die Möglichkeit, auf digitalem Weg Maßnahmen zur Systemsicherheit auszulösen, wie beispielsweise das Wiederhochfahren von Teilsystemen nach einem Blackout. Die zur Systemstabilität notwendigen Abregelungen Erneuerbarer Erzeuger im Verteilnetz (Einspeisemanagement) erfolgen ebenfalls durch digitale Prozesse, auch wenn der Automatisierungsgrad heute noch eher niedrig ist.

Eine neue Herausforderung ist, dass die Durchführung der Maßnahmen, etwa dem Wiederhochfahren des Systems nach einem Blackout, auf vielen Einzelmaßnahmen beruht, da die beteiligten Anlagen (etwa kleinere Erzeuger) dezentral installiert sind. Die Koordination dieser Einzelmaßnahmen ist ohne Digitalisierung nicht möglich. Wie zentral oder dezentral ein Systemwiederaufbau zukünftig koordiniert sein wird und wie die Richtlinien dazu aussehen werden, ist heute noch unklar.

Ob Nutzen oder Gefahren überwiegen, entscheidet sich insbesondere an den folgenden Punkten:

[37] Vgl. Thomas Petermann, Harald Bradke, Arne Lüllmann, Maik Poetzsch, Ulrich Riehm: Was bei einem Blackout geschieht. Folgen eines langandauernden und großflächigen Stromausfalls. Studien des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag, Bd. 33, Berlin: Nomos, 2011, URL: http://www.tab-beim-bundestag.de/de/pdf/publikationen/buecher/petermann-etal-2011-141.pdf, S. 67.

- **Komplexität beherrschen:** Digitalisierung hilft dabei, Komplexität zu beherrschen. Anlagen können beispielsweise durch gemeinsame Steuerung zusammengefasst werden („virtuelle Kraftwerke“), um Systemdienstleistungen zu erbringen, Netzbetreiber können Informationen zu Marktgeschehen und (physischen) Netzzuständen zusammenführen und analysieren, um bei Netzproblemen schnell die richtigen Maßnahmen zu treffen. Auch diese technischen Maßnahmen beruhen in hohem Maße auf der Nutzung von IKT und der Kommunikationsanbindung der energietechnischen Anlagen. Auf der anderen Seite schafft die Digitalisierung zusätzliche Komplexität. Schließlich wird eine unüberschaubar große Zahl miteinander vernetzter IKT-Komponenten, von den Smart Homes über smarte Elektroautos bis zu an das Internet angeschlossenen Kühlschränken, zu systemkritischen Bestandteilen des Energiesystems. Diese Bestandteile müssen in ihrem Zusammenspiel und der Wirkung auf das Energiesystem ausreichend abgeschätzt und gesteuert werden können. Damit bilden sie aufgrund der erhöhten Komplexität, die in das System eingeführt wird, eine neue potenzielle Fehlerquelle.

- **Risikomanagement:** Auf den ersten Blick erscheint manchen die geringstmögliche Digitalisierung des Energiesystems als bester Garant der Versorgungssicherheit: Was nicht digitalisiert ist, kann auch nicht „gehackt“ werden. Tatsächlich hielte ein geringer Digitalisierungsgrad das Risiko von erfolgreichen Angriffen auf Teile der IKT gering. Jedoch würde dadurch – neben dem dadurch bedingten großen Effizienzverlust –voraussichtlich ein weniger sicheres System entstehen, da die Möglichkeiten der Digitalisierung zur Resilienzverbesserung zu wenig genutzt würden. Außerdem besteht das Risiko nationaler technologischer Sackgassen: Andere Länder könnten stärker auf Digitalisierung setzen und ihre ausgereiften Lösungen mittelfristig am Markt durchsetzen.
  Auf der anderen Seite wird von einigen vertreten, dass Digitalisierung uneingeschränkt eine bessere Kontrollierbarkeit des Energiesystems ermöglicht: Systemverantwortliche Netzbetreiber könnten in Störfällen jederzeit die Kontrolle über alle Einheiten übernehmen. Was aber dem Netzbetreiber als Optionen zur Systemsicherung zur Verfügung steht, etwa das Abschalten von Erzeugungsanlagen oder Verbrauchern, könnte auch bösartig genutzt werden, wenn jemand Zugang zu den entsprechenden IKT-Systemen bekommt. Dasselbe gilt für eine unbewusste Risikoaffinität: Bei der Digitalisierung werden wichtige Aspekte, etwa die systemischen Auswirkungen bei Fehlern, unzureichend beachtet (s.u.). und die Verantwortung für IT-Sicherheit wird dementsprechend weitgehend als Thema des jeweiligen individuellen Akteurs betrachtet, beispielsweise eines Netzbetreibers.

- **Organisation der verteilten Verantwortlichkeiten:** Für die sichere Digitalisierung des Energiesystems sind unterschiedliche Akteure verantwortlich: nationale und supranationale Gesetzgeber und Regulierer, Netzbetreiber, Normierungsgremien und vergleichbare Verbände oder auch neue, noch zu schaffende Institutionen. Dies birgt das Risiko, dass die Verantwortlichkeiten des IKT-Einsatzes und der Absicherung ineffektiv auf Akteure verteilt werden oder ungewollte Akteurskonflikte entstehen: So wäre denkbar, dass sich widersprechende Regelungsmechanismen festgelegt werden, also sich Maßnahmen gegenseitig blockieren oder wichtige Verantwortlichkeiten keinem Akteur verbindlich zugeordnet werden. Für die verantwortlichen Akteure bestünde dann auch die Verpflichtung, die nötigen Kompetenzen dazu aufzubauen.

- **Absicherung durch vorhandenes Know-How:** Alle Maßnahmen müssen auf solidem Fundament entwickelt werden, das durch die Kenntnisse und die Erfahrung der Expertinnen und Experten vorgegeben wird. Das wird aber nicht reichen: Dafür sind heutige Energiesysteme – und künftige höchstwahrscheinlich erst recht – einfach zu vernetzt und dynamisch. Die heutigen Mechanismen zu Resilienz sind

daher zumindest um Maßnahmen zu ergänzen, die stärker auf Automatisierung und dezentralen Anlagen basieren, und in Teilen gegebenenfalls neu auszurichten. Die Rolle des Menschen wird sich in einem zunehmend automatisierten System ändern, wie die Erfahrungen anderer Branchen wie etwa der Luftfahrt zeigen.

- **Rigidität versus Flexibilität:** Um mögliche Fehler bei der Regulierung, den Grid Codes oder dem Marktdesign abzufangen, werden Flexibilitäten benötigt, die frühzeitig bedacht werden müssen. Auf der anderen Seite können zu hohe Freiheitsgrade und zu viel Flexibilität aber auch zur Störung des Systems beitragen, sei es aus böser Absicht oder unabsichtlich, etwa durch marktliche motivierte Vorgänge oder „fehlerhafte“ technische Anwendungsrichtlinien.

Aus dem bisher Gesagten ergibt sich, dass die Digitalisierung im Energiesektor besonderen Anforderungen gerecht werden muss. Resilienz bedeutet auch, nach Störfällen eine „Lernschleife“ einzubauen: Der Vorfall wird analysiert und verbindliche Maßnahmen werden erarbeitet, um beim nächsten Mal weniger oder keinen Schaden zu erleiden (s.u. „Aufgabenverteilung“). Dies setzt einen einheitlichen Stand von Sicherheitsmaßnahmen voraus, der sich an den Systemgrenzen orientiert und nicht an Staatsgrenzen haltmacht. Dies führt zur nächsten These.

These 2: In einem hoch vernetzten Energiesystem – technisch wesentlich digital gesteuert und koordiniert – können Risiken für Resilienz und Robustheit durch die Digitalisierung nur auf Systemebene ausreichend verstanden werden, da sich lokale Fehler auf das ganze System auswirken können. Dieser Aspekt ist jedoch unterbelichtet.[38]

Was müsste passieren?
Im Folgenden werden einige Punkte zur weiteren Diskussion vorgeschlagen.

- **Maßnahmen zu IT-Sicherheit:** Es finden sich in der Praxis kaum Maßnahmen, die systemisch gedacht werden.[39] Viele neue Entwicklungen (Backdoors in Hardware und Software, Cloud, „Internet of Things“) sind noch nicht auf dem Radar. Der Einsatz von Cloud-Lösungen im Bereich kritischer Infrastrukturen kann im schlechtesten Fall die nationale Souveränität in Frage stellen, ohne dass dies bekannt ist.
- **Aufgabenverteilung:** (s.o.) Welche Maßnahmen können / müssen welche privaten Akteure übernehmen? Was ist von welchen Netzbetreibern zu organisieren? Welche Regelungen sind staatlich vorzugeben? Das Wissen über erfolgreiche oder abgewehrte Attacken muss auf geeignete Weise zwischen allen Akteuren geteilt werden. Zwar besteht hier bereits die Initiative UP KRITIS, in der (deutsche) Betreiber Kritischer Infrastrukturen, ihre Verbände und zuständige Behörden zusammenarbeiten. Informationen werden dort derzeit aber nur in sehr eingeschränktem Maße ausgetauscht. Eine Pflicht zur sehr weitgehenden Teilung von Informationen über erfolgreiche Hackerangriffe kann andererseits, etwa aus Furcht vor Imageschäden, dazu führen, dass diese Pflicht ein Papiertiger bleibt.

[38] Vgl. beispielsweise Cyber Security in the Energy Sector, EC, 2017, abrufbar unter https://ec.europa.eu/energy/en/news/new-report-cyber-security-energy-sector-published
[39] Vgl. Matthias Uslar et al.: Schutz- und Sicherheitsanalyse im Rahmen der Entwicklung von Smart Grids in der Schweiz“, 2016, URL: http://www.bfe.admin.ch/smartgrids/index.html?lang=de&dossier_id=06727

- **Internationalisierung:** Das Energiesystem kann nur unzureichend national abgesichert werden. Wie man am Störereignis 2006 (Abschaltung der Leitung über die Ems) gesehen hat, können lokale Aktionen zu dramatischen Störungen an weit entfernten Orten führen (hier u.a. in Spanien und Italien). Eine supranationale Abstimmung ist daher zwingend nötig. Angriffe auf die IKT des Stromsystems können sogar als kriegerischer Akt durch andere Staaten durchgeführt werden. Dann ist eine komplexe Gemengelage von Organisationen (nationale Regierungen, EU, ENTSO-E, NATO) damit befasst, auf das Problem zu reagieren. Die Mitglieder dieser Organisationen sind bei weitem nicht deckungsgleich, es existieren nicht einmal Gremien zur gemeinsamen Absprache. Einem Angriff, der grenzübergreifend erfolgt und dessen Schäden erst in Summe systemrelevant sind, könnte heute nicht angemessen begegnet werden.
- **Systemische Sicht:** Es muss untersucht werden, wie Vorgänge in der digitalen Welt Robustheit und Resilienz des (physischen) Energiesystems beeinflussen. So ist es denkbar, dass im Strombereich Marktmanipulationen oder Fehlinformationen über Markttransaktionen zu Fehlern bei der Planung von Reservekapazitäten führen, was in der Folge zu Ausfällen bei der Stromlieferung führt. Der Strommarkt basiert in Zukunft voraussichtlich auf immer kürzeren Planungszyklen, so dass Angriffe dieser Art wirksam sein könnten. Im Prinzip muss in Systemen das schwächste Glied der Kette gesichert werden. Was aber ist ein Kettenglied in einem digitalisierten System?

Fazit

Massive Digitalisierung ist notwendig, um das Energiesystem auch in Zukunft resilient zu halten – doch fehlt es zur Umsetzung noch an sehr vielen Stellen an Wissen, Koordination oder schlicht Verständnis für das Thema. Viele Maßnahmen, um die Resilienz des Energiesystems zu erhöhen, werden also Maßnahmen im Umfeld der IKT sein, die insbesondere den Informationsaustausch sowohl zwischen Akteuren als auch zwischen Geräten und Teilsystemen betreffen. Unter Fachleuten herrscht Einigkeit: Ohne IKT ist weder ein sicherer noch ein effizienter Systembetrieb denkbar. Schon heute ist die Digitalisierung tragende Säule im Energiesystem und ihre Bedeutung wird weiter wachsen. Das Konfliktpotenzial, sowohl einen Beitrag zur Systemsicherheit zu leisten als auch neue Risiken für die Systemsicherheit zu schaffen, ist bislang jedoch kaum betrachtet. Beide Aspekte bedürfen daher dringend intensiver Analyse, Abstimmung unter den Akteuren und wirksamer Maßnahmen, um die Energiewende erfolgreich durchführen zu können. Die erfolgreiche effiziente und resiliente Digitalisierung des Energiesystems ist wesentliches Erfolgskriterium für die Energiewende.

HUMBOLDT-VIADRINA
Governance Platform

Kontakt

HUMBOLDT-VIADRINA Governance Platform gGmbH
Pariser Platz 6 (Allianz Forum)
10117 Berlin

Telefon: +49 30 20620 140
Email: energie.trialoge@governance-platform.org
Website: www.governance-platform.org

Bericht vom 20.04.2018

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung