



> Resilien-Tech

„Resilience-by-Design“: Strategie für die technologischen Zukunftsthemen

acatech (Hrsg.)

acatech POSITION

April 2014

Herausgeber:

acatech – DEUTSCHE AKADEMIE DER TECHNIKWISSENSCHAFTEN, 2014

Geschäftsstelle
Residenz München
Hofgartenstraße 2
80539 München

Hauptstadtbüro
Unter den Linden 14
10117 Berlin

Brüssel-Büro
Rue d'Egmont/Egmontstraat 13
1000 Brüssel
Belgien

T +49 (0) 89 / 5 20 30 90
F +49 (0) 89 / 5 20 30 99

T +49 (0) 30 / 2 06 30 96 0
F +49 (0) 30 / 2 06 30 96 11

T +32 (0) 2 / 2 13 81 80
F +32 (0) 2 / 2 13 81 89

E-Mail: info@acatech.de
Internet: www.acatech.de

Koordination: Dr. Anna Frey, Dr. Martina Kohlhuber

Redaktion: Linda Treugut, Dr. Anna Frey, Dr. Martina Kohlhuber, Sandra Lehmann

Layout-Konzeption: acatech

Konvertierung und Satz: Fraunhofer-Institut für Intelligente Analyse- und Informationssysteme IAIS,
Sankt Augustin

Die Originalfassung der Publikation ist verfügbar auf www.utzverlag.de

> DIE REIHE acatech POSITION

In dieser Reihe erscheinen Positionen der Deutschen Akademie der Technikwissenschaften zu technikwissenschaftlichen und technologiepolitischen Zukunftsfragen. Die Positionen enthalten konkrete Handlungsempfehlungen und richten sich an Entscheidungsträger in Politik, Wissenschaft und Wirtschaft sowie die interessierte Öffentlichkeit. Die Positionen werden von acatech Mitgliedern und weiteren Experten erarbeitet und vom acatech Präsidium autorisiert und herausgegeben.

> INHALT

KURZFASSUNG	6
PROJEKT	10
1 EINLEITUNG	11
2 RESILIENZ IN DER PRAXIS	15
3 HANDLUNGSEMPFEHLUNGEN	18
LITERATUR	25

KURZFASSUNG

Die Flutkatastrophe in Mitteleuropa im Mai 2013 machte auf dramatische Weise die Verletzbarkeit unserer kritischen Infrastrukturen deutlich und zeigte, wie wichtig es ist, dass sich Gesellschaft und Unternehmen an schwerwiegende widrige Ereignisse anzupassen vermögen. Wenn wir auch in Zukunft Menschen und Infrastrukturen wirksam vor finanziellen, sozialen und ökologischen Schäden, verursacht von Naturkatastrophen, Terroranschlägen, Industrieunfällen und anderen Extremereignissen, schützen wollen, müssen wir sowohl Prävention, Vorbereitung und Schutzmaßnahmen als auch adäquate Krisenreaktion und sinnvolles Lernen aus vergangenen Ereignissen in unserer Gesellschaft verankern.

Die digitale Vernetzung unserer Welt, aber auch der demografische Wandel in Deutschland, die drohende Überbevölkerung weltweit sowie häufiger auftretende Extremwetterereignisse führen einerseits zu größeren und andererseits zu bisher nicht beobachtbaren, neuartigen Risiken und machen unsere moderne Industriegesellschaft verwundbarer. Die wachsende Vernetzung innerhalb und zwischen lebenswichtigen Infrastrukturen hat zur Folge, dass Katastrophen in Zukunft immer größeren Schaden anrichten können. Man denke beispielsweise an die Smart Grids der Energieversorgung und die intelligenten Industrie- und Logistiksysteme: Bereits kleine, zunächst harmlos wirkende Störungen können in einer Kettenreaktion zu gravierenden Schäden am ganzen System führen.

Die Sicherheit der kritischen Infrastrukturen, etwa für die Versorgung mit Wasser, Strom oder Lebensmitteln, ist Voraussetzung für unsere Lebensweise und den wirtschaftlichen Wohlstand in Deutschland. Allerdings kann ein Zuviel an Sicherheit die Freiheit und Bürgerrechte der Menschen auch einschränken. Mit der „Nationalen Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)“ unterstützt die Bundesregierung die Zusammenarbeit aller relevanten Akteure aus Staat und Wirtschaft für die Sicherheit der lebenswichtigen Infrastrukturen. Auch im Rahmenprogramm „Forschung für die zivile Sicherheit 2012 – 2017“ räumt die

Bundesregierung dem Schutz der kritischen Infrastrukturen einen hohen Stellenwert ein und fördert die Sicherheitsforschung bei der Suche nach neuen Lösungen für den Schutz von Bevölkerung und Infrastrukturen, die die Balance zwischen Freiheit und Sicherheit bewahren.

Sicherheitsforschung zielt darauf, Verwundbarkeiten aller Art – eben zum Beispiel durch Naturkatastrophen, Terror, Kriminalität oder Unfälle – zu erkennen, zu analysieren und Vorschläge beziehungsweise Technologien zur Minderung oder Vermeidung der Risiken zu entwickeln. Strategien und Verfahren zur zeitnahen Wiederherstellung der normalen Funktion des Systems oder der Infrastruktur nach einer Störung sind ebenso Thema der Sicherheitsforschung. Übergeordnetes und langfristiges Ziel ist der Aufbau einer widerstandsfähigen, fehlertoleranten und robusten Infrastruktur.

Anfangs konzentrierte sich die Sicherheitsforschung auf technologische Möglichkeiten, um Schäden von den Infrastrukturen fernzuhalten. Doch insbesondere in hochvernetzten Infrastrukturen kann keine Technik hundertprozentigen Schutz bieten, ist die vollkommene Kontrolle eine Illusion. Auch mit der besten Vorsorge wird es nicht möglich sein, die Menschen vor allen denkbaren und vorstellbaren Krisenereignissen zu schützen. Inzwischen plant die Sicherheitsforschung auch noch so unwahrscheinliche Katastrophen ein. Statt allein eine technische Perspektive einzunehmen, werden auch die Gesellschaft und ihre Anpassungsfähigkeit in den Blick genommen. Die Vorbereitung der Menschen auf den Ernstfall spielt dabei eine ebenso große Rolle wie die der privatwirtschaftlichen Unternehmen, die etwa 80 Prozent der kritischen Infrastrukturen in Deutschland betreiben. Staatliche Institutionen haben grundsätzlich das Gemeinwohl im Blick und daher ein Interesse, die von ihnen betriebenen Infrastrukturen zu schützen. Privatunternehmen, die ebenfalls kritische Infrastrukturen betreiben, müssen natürlich insbesondere auch die Kostenfaktoren in ihr Kalkül einbeziehen. Gerade wenn auch unerwartete Ereignisse eingeplant werden sollen, macht deren geringe

Eintrittswahrscheinlichkeit Investitionen in die Sicherheit scheinbar unrentabel. Hier gilt es, entsprechende Anreize für den Schutz der Infrastrukturen zu schaffen.

Einen ganzheitlichen Ansatz, der Technik und Gesellschaft gleichermaßen berücksichtigt, bietet in der Sicherheitsforschung das Konzept der Resilienz. Resiliente Gesellschaften sind in der Lage, die menschlichen, ökonomischen und ökologischen Schäden, die durch widrige Ereignisse verursacht werden, so gering wie irgend möglich zu halten. Sie schaffen das, indem sie sich jedweder denk- und durchführbarer Lösungen bedienen, unabhängig davon, ob es sich um Technologien, gesellschaftliche Werkzeuge wie Bildung und den Dialog auf Augenhöhe mit der Bevölkerung oder ökonomische Anreize handelt. Vereinfacht bedeutet Resilienz, die Funktion eines Systems auch bei unerwarteten Störungen zuverlässig aufrechtzuerhalten oder möglichst rasch in einen funktionsfähigen Zustand zurückzuführen.

Resilienz ist die Fähigkeit, tatsächlich oder potenziell widrige Ereignisse abzuwehren, sich darauf vorzubereiten, sie einzukalkulieren, sie zu verkraften, sich davon zu erholen und sich ihnen immer erfolgreicher anzupassen. Widrige Ereignisse sind menschlich, technisch sowie natürlich verursachte Katastrophen oder Veränderungsprozesse, die katastrophale Folgen haben.

Resilienz kann in fünf Phasen unterteilt werden: Zunächst geht es um eine ernsthafte Vorbereitung auf Katastrophen, vor allem im Hinblick auf Frühwarnsysteme (prepare). Durch eine Reduzierung der zugrunde liegenden Risikofaktoren soll zudem – sofern möglich – das Eintreten des katastrophalen Ereignisses an sich verhindert werden (prevent). Tritt es trotzdem ein, kommt es darauf an, dass physische und virtuelle Schutzsysteme fehlerfrei funktionieren und die negativen Auswirkungen gering gehalten werden (protect). Zudem wird schnelle, gut organisierte und effektive Katastrophenhilfe benötigt. Hierbei muss das System soweit wie möglich seine essenzielle Funktionsfähigkeit

aufrechterhalten können (respond). Nach dem Ende des unmittelbaren Schadensereignisses ist es abschließend wichtig, dass das System in der Lage ist, sich zu erholen und die entsprechenden Lehren aus dem Geschehen zu ziehen, um für zukünftige Bedrohungen besser gerüstet zu sein (recover).

Bei der Ablösung eines starren Sicherheitskonzepts durch die konkrete Umsetzung des Resilienzkonzepts in die Praxis sind Länder wie die Vereinigten Staaten, Großbritannien oder die Schweiz Deutschland einige Schritte voraus. Auch hierzulande müssen in Zukunft Resilienzstrategien in Regierungsprogramme aufgenommen werden. Resilienz muss zur fundamentalen Grundvoraussetzung jeglicher technologischer oder gesellschaftlicher Sicherheitslösungen werden, damit Deutschland auch in Zukunft die Sicherheit der Bürgerinnen und Bürger sowie die lebenswichtigen Infrastrukturen wirksam schützen kann.

HANDLUNGSEMPFEHLUNGEN

1. Resilienz als ganzheitliches Konzept zur Minimierung schädlicher Auswirkungen widriger Ereignisse auf unsere Gesellschaft anwenden.

So kann es gelingen, die Funktions-, Anpassungs-, Widerstands- und Lernfähigkeit komplexer Systeme angesichts externer oder interner Störungen nachhaltig zu erhöhen. Dazu müssen geeignete und korrespondierende Maßnahmen technologischer, gesellschaftlicher und ökonomischer Art erforscht, entwickelt, ergriffen und integrativ miteinander kombiniert werden.

2. Metriken und Indikatoren zur Bewertung von Verwundbarkeit und Resilienz entwickeln.

Nur wenn die Verwundbarkeit und die Resilienz von Gesellschaften und ihren Subsystemen in ein vernünftiges und operationalisierbares quantitatives Verhältnis

gesetzt werden können, ist es möglich, umfassender als bisher systematisch nach Schwachstellen zu suchen, den Nutzen von Investitionen zu bewerten oder festzustellen, wie bestimmte Maßnahmen Resilienz beeinflussen. Die deutsche Forschung sollte sich deshalb der Herausforderung annehmen, ein nützliches Maß für Resilienz zu entwickeln.

3. Methoden zur Modellierung und Simulation komplexer soziotechnischer Systeme mit hoher gesellschaftlicher Relevanz entwickeln.

Forschungsansätzen, die bestehende Modellierungsansätze erweitern und die Auswirkungen widriger Ereignisse speziell im Hinblick auf Kaskadeneffekte simulieren helfen, sollte in der Sicherheitsforschung größeres Gewicht eingeräumt werden. Entscheidend sind die zuverlässige Identifikation systemkritischer Knotenpunkte und Schnittstellen, deren Schädigung zu Kaskadeneffekten führt, und die Vorhersage des Potenzials zur Selbstorganisation des Systems.

4. Resilience Engineering als eigenständiges Fachgebiet etablieren: Die Erforschung, Entwicklung und Umsetzung resilienten Designs und resilienter Konstruktionsweisen für kritische Infrastrukturen forcieren.

Die Infrastrukturen müssen mithilfe innovativer Technologien für das 21. Jahrhundert fit gemacht werden. Resilience Engineering bedeutet, maßgeschneiderte technologische und interdisziplinäre Methoden und Lösungen zu entwickeln, mit deren Hilfe Systeme von entscheidendem gesellschaftlichen Wert resilient gestaltet werden können.

5. Strategien zur nachhaltigen Stärkung der Eigenverantwortlichkeit der Bürgerinnen und Bürger angesichts widriger Ereignisse entwickeln und umsetzen.

In einem Dialog auf Augenhöhe und mithilfe der Schaffung weitreichender Möglichkeiten zur Partizipation auf verschiedenen, dezentralen Ebenen sollte die Bevölkerung aktiv an der Gestaltung resilienter Gesellschaften beteiligt werden. Vorsorge vor und Akzeptanz von Risiken kann von staatlicher Seite unterstützt werden, etwa durch Lehrinhalte an Schulen, durch Stärken des freiwilligen Engagements in Feuerwehren, bei DRK, THW und vielen weiteren Rettungsorganisationen oder durch weitere konkrete Maßnahmen.

6. Den langfristigen Mehrwert von Resilienz für Gesellschaften aufzeigen.

Es bedarf einer Erweiterung der Perspektive, weg von einer kurzfristigen und kurzsichtigen Nutzenoptimierung, hin zu strategischem und nachhaltigem Denken und Handeln. Dazu müssen künftige Forschungsansätze ökonomische Aspekte von Anfang an mitdenken. So können sie aufzeigen, dass sich Investitionen in Resilienz lohnen. Damit wird aus dem vermeintlichen Kostenträger Resilienz ein Business Case.

7. Anreize für Unternehmen schaffen, ihre Resilienz zu erhöhen.

Es sollte darüber nachgedacht werden, ein standardisiertes Resilienz-Monitoring einzuführen, welches von öffentlicher Seite begleitet und gegebenenfalls koordiniert wird, um gesellschaftlich relevante Unternehmen, die nachweislich ihre Resilienz steigern, in geeigneter Form zu intensivieren und diejenigen gesellschaftlich relevanten Unternehmen, die dem Aufbau von Resilienz nicht nachkommen, durch erhöhte Versicherungsprämien, Zusatzabgaben oder Ähnliches zu beeinflussen.

8. Meldepflichten im Sinne eines Frühwarnsystems einführen.

Trotz der geringen Wahrscheinlichkeit des Eintretens gravierender widriger Ereignisse treten diese faktisch auf. Daher sollte ein nationales Frühwarnsystem eingeführt werden, welches mit einer auf Branchen zugeschnittenen Meldepflicht (zum Beispiel durch branchenspezifische Meldekriterien) verbunden ist, die Unternehmen vorschreibt, sicherheitskritische Ereignisse zu melden.

9. Eine nationale Resilienzstrategie entwickeln.

Es wird eine übergreifende Vision für resiliente Gesellschaften im größeren Kontext der nachhaltigen Entwicklung benötigt. Resilienz als holistisches Konzept kann nicht per Gesetz verordnet werden. Eine nationale Resilienzstrategie kann aber den Grundstein legen, den vielfältigen Herausforderungen der immer komplexer

werdenden, hochtechnisierten Welt mit einem konsistenten und umfassenden Ansatz zu begegnen und davon ausgehend maßgeschneiderte Lösungen für spezifische Probleme zu entwickeln.

10. Resilienz als Schlüsselkomponente nachhaltiger Entwicklung etablieren.

Nachhaltigkeit bedeutet, das menschliche Zusammenleben so zu gestalten, dass es den Bedürfnissen der heutigen Generation entspricht, ohne die Möglichkeiten künftiger Generationen zu gefährden, ihre eigenen Bedürfnisse zu befriedigen. Dazu müssen Gesellschaften überlebensfähig in Anbetracht großer Herausforderungen sein. Überlebensfähigkeit setzt Funktions-, Anpassungs-, Widerstands- und Lernfähigkeit voraus. Genau das ist das charakteristische Wesensmerkmal resilienter Systeme. Das Konzept Resilienz schlägt also eine Brücke zwischen Sicherheits- und Nachhaltigkeitsforschung.

PROJEKT

Diese Position entstand auf Grundlage der acatech STUDIE Resilien-Tech – „Resilience-by-Design“: Strategie für die technologischen Zukunftsthemen (Hrsg. 2014).

> PROJEKTLEITUNG

Prof. Dr. Klaus Thoma, Fraunhofer-Institut für Kurzzeitdynamik – Ernst-Mach-Institut EMI/acatech

> PROJEKTGRUPPE

- Peter Andres, Deutsche Lufthansa AG
- Prof. Dr. Claudia Eckert, Fraunhofer-Einrichtung für Angewandte und Integrierte Sicherheit/acatech
- Alexander Kluge, Deutsche Bahn AG
- KPMG AG Wirtschaftsprüfungsgesellschaft
- Wolfgang Müller-Pietralla, Volkswagen AG
- Prof. Dr. Friedbert Pflüger, European Centre for Energy and Resource Security
- Prof. Dr. Ortwin Renn, Universität Stuttgart/acatech
- Prof. Dr.-Ing. Jochen Schiller, Forschungsforum Öffentliche Sicherheit/Freie Universität Berlin
- Prof. Dr.-Ing. Eckehard Schnieder, Technische Universität Braunschweig/acatech
- Prof. Dr. Klaus Thoma, Fraunhofer-Institut für Kurzzeitdynamik – Ernst-Mach-Institut EMI/acatech

> REVIEWER

- Prof. Dr.-Ing. Bernd Hillemeier, Präsidiumsmitglied acatech (Leitung)
- Prof. Dr.-Ing. habil. Jürgen Beyerer, Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung IOSB/acatech
- Prof. Dr. Leonhard Reindl, Institut für Mikrosystemtechnik (IMTEK), Albert-Ludwigs-Universität Freiburg

> AUFTRÄGE/MITARBEITER

- Dr. Lars Gerhold, Forschungsforum Öffentliche Sicherheit/Freie Universität Berlin
- Gabriel Bartl, Forschungsforum Öffentliche Sicherheit/Freie Universität Berlin
- Lucas Daus, KPMG AG WPG
- Burkhard Kesting, KPMG AG WPG
- Timo Kukuk, KPMG AG WPG

> KONSORTIALPARTNER/MITARBEITER

- Daniel Hiller, Fraunhofer-Institut für Kurzzeitdynamik – Ernst-Mach-Institut EMI
- Dr. Tobias Leismann, Fraunhofer-Institut für Kurzzeitdynamik – Ernst-Mach-Institut EMI
- Benjamin Scharte, Fraunhofer-Institut für Kurzzeitdynamik – Ernst-Mach-Institut EMI

> PROJEKTKOORDINATION

- Dr. Anna Frey, acatech-Geschäftsstelle
- Dr. Martina Kohlhuber, acatech-Geschäftsstelle

> PROJEKTVERLAUF

Projektlaufzeit 07/2012 – 06/2014

> FINANZIERUNG

Das Projekt wurde vom Bundesministerium für Bildung und Forschung (BMBF) gefördert (Förderkennzeichen 13N12276).

GEFÖRDERT VOM



Bundesministerium
für Bildung
und Forschung

Projektträger: Projektträger im VDI Technologiezentrum GmbH

1 EINLEITUNG

Ende Mai 2013 wurde Mitteleuropa von einer gravierenden Flutkatastrophe heimgesucht. Allein in Deutschland starben acht Menschen, hunderttausende verloren Hab und Gut, die finanziellen Schäden werden von der Münchener Rück auf insgesamt mehr als zwölf Milliarden Euro geschätzt. Teilweise erreichte die Flut historische Ausmaße, was unter anderem am Pegelstand der Donau in Passau ersichtlich wurde, der mit über 12,50 Metern so hoch war, wie seit über 500 Jahren nicht mehr.¹ Die außergewöhnliche Hochwasserlage machte auf dramatische Weise die Verletzbarkeit unserer kritischen Infrastrukturen deutlich und zeigte, wie wichtig es ist, dass sich Gesellschaft und Unternehmen an schwerwiegende widrige Ereignisse anzupassen vermögen. Wenn wir auch in Zukunft Menschen und Infrastrukturen wirksam vor finanziellen, sozialen und ökologischen Schäden durch Naturkatastrophen, Terroranschläge, Industrieunfälle und andere Extremereignisse schützen wollen, müssen wir sowohl Prävention, Vorbereitung und Schutzmaßnahmen als auch adäquate Krisenreaktion und sinnvolles Lernen aus vergangenen Ereignissen in unserer Gesellschaft verankern. Diese POSITION greift die Erkenntnisse aus der STUDIE „Resilien-Tech – ‚Resilience-by-design‘: Strategie für die technologischen Zukunftsthemen“² auf und leitet daraus Handlungsempfehlungen ab.

Die digitale Vernetzung unserer Welt, aber auch der demografische Wandel in Deutschland, die Bevölkerungsexplosion weltweit sowie häufiger auftretende Extremwetterereignisse führen einerseits zu größeren und andererseits zu bisher nicht beobachtbaren, neuartigen Risiken und machen unsere moderne Industriegesellschaft verwundbarer. Die wachsende Vernetzung innerhalb und zwischen lebenswichtigen Infrastrukturen hat zur Folge, dass Katastrophen in Zukunft immer größeren Schaden anrichten können.³ Man denke beispielsweise an die Smart Grids der Energieversorgung und die intelligenten Industrie- und Logistiksysteme: Bereits

kleine, zunächst harmlos wirkende Störungen können in einer Kettenreaktion zu gravierenden Schäden am ganzen System führen.

Die Sicherheit der kritischen Infrastrukturen, etwa für die Versorgung mit Wasser, Strom oder Lebensmitteln, ist Voraussetzung für unsere Lebensweise und den wirtschaftlichen Wohlstand in Deutschland. Allerdings kann ein Zuviel an Sicherheit die Freiheit und Bürgerrechte der Menschen auch einschränken. Mit der „Nationalen Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)“ unterstützt die Bundesregierung die Zusammenarbeit aller relevanten Akteure aus Staat und Wirtschaft für die Sicherheit der lebenswichtigen Infrastrukturen. Auch im Rahmenprogramm „Forschung für die zivile Sicherheit 2012 – 2017“ räumt die Bundesregierung dem Schutz der kritischen Infrastrukturen einen hohen Stellenwert ein und fördert die Sicherheitsforschung bei der Suche nach neuen Lösungen für den Schutz von Bevölkerung und Infrastrukturen, die die Balance zwischen Freiheit und Sicherheit bewahren.

Sicherheitsforschung zielt darauf, Verwundbarkeiten aller Art – eben zum Beispiel durch Naturkatastrophen, Terror, Kriminalität oder Unfälle – zu erkennen, zu analysieren und Vorschläge beziehungsweise Technologien zur Minderung oder Vermeidung der Risiken zu entwickeln. Strategien und Verfahren zur zeitnahen Wiederherstellung der normalen Funktion des Systems oder der Infrastruktur nach einer Störung sind ebenso Thema der Sicherheitsforschung. Übergeordnetes und langfristiges Ziel ist der Aufbau einer widerstandsfähigen, fehlertoleranten und robusten Infrastruktur.

Anfangs konzentrierte sich die Sicherheitsforschung auf technologische Möglichkeiten, um Schäden von den Infrastrukturen fernzuhalten. Die technologieorientierte Herangehensweise entwickelte einzelne grundlegende Technologien für die Sicherheitsforschung losgelöst voneinander

¹ FAZ.NET 2013.

² Thoma 2014.

³ Coaffee et al. 2009, S. 122-132.

und führte sie erst im Engineering des Endprodukts zusammen. Doch insbesondere in hochvernetzten Infrastrukturen kann keine Technik hundertprozentigen Schutz bieten, ist die vollkommene Kontrolle eine Illusion. Auch mit der besten Vorsorge wird es nicht möglich sein, die Menschen vor allen denkbaren und vorstellbaren Krisenereignissen zu schützen. Die Sicherheitsforschung plant daher auch noch so unwahrscheinliche Katastrophen ein und geht von Bedrohungs- und Gefährdungsszenarien aus. Dieser zweite Ansatz soll zu systematischen, sicherheitsrelevanten Gesamtkonzepten führen und, basierend auf Risikoanalysen, die Angreifbarkeit und Verwundbarkeit der betrachteten Systeme minimieren. Statt allein eine technische Perspektive einzunehmen, wird auch die Gesellschaft und ihre Anpassungsfähigkeit in den Blick genommen. Die Vorbereitung der Menschen auf den Ernstfall spielt dabei eine ebenso große Rolle wie die der privatwirtschaftlichen Unternehmen, die etwa 80 Prozent der kritischen Infrastrukturen in Deutschland betreiben. In der Sicherheitsforschung hat daher das Konzept der Resilienz Einzug gehalten.

Vereinfacht bedeutet Resilienz, die Funktion eines Systems auch bei Störungen zuverlässig aufrechtzuerhalten oder möglichst rasch in einen funktionsfähigen Zustand zurückzuführen. Der Begriff war in den vergangenen 60 Jahren in völlig verschiedenen Wissenschaftsgebieten zu Hause – angefangen von der Entwicklungspsychologie über die Ökologie und die Sozialwissenschaften bis hin zum Ingenieurwesen.

Das Projekt „Resilien-Tech“, dessen Ergebnisse der vorliegenden acatech POSITION zugrunde liegen, erarbeitete das Konzept Resilienz für den Bereich der Sicherheitsforschung, um daraus konkrete Handlungsempfehlungen für Entscheidungsträger in Politik, Wirtschaft und Gesellschaft generieren zu können. Die Projektgruppe hat die Chancen und Perspektiven des Ansatzes für die Entwicklung zukünftiger Szenarien in den für die Sicherheit unserer Gesellschaft

relevanten Handlungsfeldern identifiziert. Dazu wurden drei Experten-Hearings (Workshops) zu den Themen nationale Perspektiven von Resilienz, internationale Perspektiven von Resilienz sowie resiliente Unternehmen durchgeführt.

Die Expertenworkshops erlaubten eine umfassende Analyse und Aufbereitung des Themenkomplexes Resilienz für den Bereich der zivilen Sicherheitsforschung. Unter besonderer Berücksichtigung des Schutzes kritischer Infrastruktursysteme wurden daraus konkrete Lösungswege zur Entwicklung von resilienten technischen wie sozioökonomischen Systemen aufgezeigt. Diese finden sich in den Handlungsempfehlungen für Entscheidungsträger wieder, die als Leitlinien zur Ausgestaltung von zukünftigen Forschungsstrategien und -roadmaps dienen können.

Ein übersichtlicher Resilienzyklus, der in Anlehnung an die Arbeiten des britischen Wissenschaftlers Charlie Edwards⁴ sowie an die Katastrophenmanagement-Kreisläufe entwickelt wurde, veranschaulicht das komplexe Konzept grafisch. Er besteht aus den fünf Resilienzphasen *prepare*, *prevent*, *protect*, *respond* und *recover* (siehe Abbildung 1). Zunächst geht es um eine ernsthafte Vorbereitung auf Katastrophen, vor allem im Hinblick auf Frühwarnsysteme (*prepare*). Durch eine Reduzierung der zugrunde liegenden Risikofaktoren soll zudem – sofern möglich – das Eintreten des Ereignisses an sich verhindert werden (*prevent*). Tritt es trotzdem ein, kommt es darauf an, dass physische und virtuelle Schutzsysteme fehlerfrei funktionieren und die negativen Auswirkungen gering halten (*protect*). Zudem wird schnelle, gut organisierte und effektive Katastrophenhilfe benötigt. Hierbei muss das System soweit möglich seine essenzielle Funktionsfähigkeit aufrechterhalten können (*respond*). Nach dem Ende des unmittelbaren Schadensereignisses ist es abschließend wichtig, dass das System in der Lage ist, sich zu erholen und die entsprechenden Lehren aus dem Geschehen zu ziehen, um für zukünftige Bedrohungen besser gerüstet zu sein (*recover*).

⁴ Edwards 2009, S. 20.

Abbildung 1: Der Resilienzyklus mit den Resilienzphasen prepare, prevent, protect, respond und recover



Quelle: nach Edwards 2009, S. 20, eigene Darstellung EMI.

Basierend auf dem Resilienzyklus wurde im Projekt Resilien-Tech eine Arbeitsdefinition von Resilienz formuliert, die während der Workshops als Grundlage für die Diskussionen diente:

„Resilienz ist die Fähigkeit, tatsächlich oder potenziell widrige Ereignisse abzuwehren, sich darauf vorzubereiten, sie einzukalkulieren, sie zu verkraften, sich davon zu erholen und sich ihnen immer erfolgreicher anzupassen. Widrige Ereignisse sind menschlich, technisch sowie natürlich verursachte Katastrophen oder Veränderungsprozesse, die katastrophale Folgen haben.“

Im Fokus steht hier die Anwendung des umfassenden Konzepts Resilienz gerade auch im Hinblick auf die Resilienz kritischer Infrastrukturen. Um Gesellschaften resilient zu gestalten, sind darüber hinaus soziale Aspekte gleichrangig mit technologischen Aspekten zu beachten.

Resilienz kann nur im konsequenten Zusammenspiel zwischen technischen und gesellschaftlichen Lösungsansätzen gelingen. Denn das Verhalten der Menschen im Katastrophenfall ist ebenso entscheidend wie das Funktionieren der Maschinen und Technologien.

Um der Notwendigkeit von ganzheitlichen Lösungsansätzen für globale, interdependente Probleme und Bedrohungen gerecht zu werden, ist es jedoch essenziell, Resilienz als Brückenkonzept zu etablieren, denn gerade der hohe Grad an wechselseitigen Einflussverhältnissen – zwischen sozialen, technischen, ökonomischen, politischen und ökologischen Faktoren – erfordert holistische Konzepte, welche diese einzelnen Faktoren nicht isoliert, sondern vielmehr als eine Art „Gesamtsystem“ betrachten. Resilienz kann in diesem Sinne als eine „konzeptionelle Innovation für einen neuen Sachverhalt“ verstanden werden.

Die zentrale Frage lautet, was eine resiliente kritische Infrastruktur leisten kann, wenn die Gesellschaft bedroht ist. Zugleich muss diese Frage entgegengesetzt gedacht werden: Kann die Gesellschaft den Ausfall von kritischen Infrastrukturen abfedern? Die beiden Pole können demnach nicht getrennt voneinander betrachtet werden und die Aufspaltung von Resilienz in zwei konzeptuelle Zugänge, die lose nebeneinander stehen, kann nicht zielführend sein. Hieran sollte ein Brückenkonzept anknüpfen. Der Zweiklang von technikwissenschaftlichen und sozialwissenschaftlichen Perspektiven auf Resilienz sollte dann zumindest nicht disharmonisch erfolgen, denn falls nicht beides zusammengedacht wird, besteht die Gefahr, dass technische Innovationen nicht akzeptiert werden und in der Folge auch nicht effizient funktionieren können.

Hier wird bereits deutlich, dass sowohl die nationale als auch die internationale Perspektive von Resilienz durch eine große Zahl von Themen und Herangehensweisen bestimmt ist. Als kleinster gemeinsamer Nenner jeder Forschung und

jedweder praktischer Umsetzung des Konzepts Resilienz konnten aber Sicherheit, Schutz und Vorsorge der Bevölkerung gegenüber allen Arten von widrigen Ereignissen ausgemacht werden. Resilienz angesichts negativer, wie auch immer gearteter Ereignisse bedeutete für alle Experten eine Minimierung von potenziellen oder bereits eingetretenen Schäden für leibliches und materielles Wohlergehen der Bevölkerung. Es geht um eine für eine nachhaltige Entwicklung notwendige Eigenschaft der Gesellschaft samt ihrer

Teilsysteme – wie zum Beispiel der kritischen Infrastrukturen. Darüber, wie dieses Ziel am besten und nachhaltigsten zu erreichen ist, welche Aspekte besonderer Beachtung bedürfen und wo so etwas wie ein akzeptabler oder guter Zustand bereits erreicht ist, ließ sich hingegen keine umfassende Einigkeit erzielen. Von diesem kleinsten gemeinsamen Nenner ausgehend gab und gibt es also eine Vielzahl an Forschungsthemen, Praxisbeispielen und Ideen, die in den Handlungsempfehlungen berücksichtigt sind.

2 RESILIENZ IN DER PRAXIS

RESILIENZ AUF STAATLICHER EBENE

Wie wird Resilienz in anderen Staaten bereits umgesetzt? Welche Ansätze gibt es, um Resilienz zu quantifizieren? Was sind aus Sicht der Experten die großen ungelösten Fragen im Bereich der Resilienzforschung? In welchen Themenbereichen sollte verstärkt geforscht werden? Was sind vielversprechende beziehungsweise langfristig tragfähige Resilienzansätze angesichts einer fast exponentiell zunehmenden Komplexität unserer hochtechnisierten Lebenswelten?

Die Bedeutung des Konzepts Resilienz in der praktischen Umsetzung ist international weiter fortgeschritten als in Deutschland. In den USA etwa ist die Stärkung der nationalen Resilienz offizielle, präsidentielle Regierungspolitik. Beispielhaft kann die Presidential Policy Directive 21 (PPD 21) zum Thema „Critical Infrastructure Security and Resilience“ genannt werden, die das Weiße Haus im Februar 2013 veröffentlichte. Die PPD 21 hat spezifisch die Resilienz der nationalen kritischen Infrastrukturen im Blick. Ihr Ziel ist die Etablierung einer kooperativen nationalen Anstrengung zur Sicherstellung von Sicherheit, Funktionieren und Resilienz der kritischen Infrastrukturen der USA.⁵ Das Weiße Haus benennt in der PPD 21 zunächst Zuständigkeiten, für die hauptsächlich das Department of Homeland Security (DHS) verantwortlich ist und verteilt dann konkrete Aufgaben und Handlungsanweisungen an das DHS. Außerdem werden die einzelnen Bereiche der kritischen Infrastrukturen und jeweils zuständige Behörden (Sector Specific Agencies, SSAs) aufgelistet und die entscheidenden Begriffe definiert.⁶

Von zentraler Bedeutung ist die Empfehlung der Entwicklung eines „National Critical Infrastructure Security and Resilience R&D Plan“, der Investitionen in Forschung und Entwicklung aufzeigt, die benötigt werden, um die kritischen Infrastrukturen der USA resilient zu gestalten. Kritische Infrastrukturen werden als vital für die Vereinigten Staaten definiert – mit

dem Hinweis, dass jede Beeinträchtigung ihrer Funktionsfähigkeit zu gravierenden Schäden an „security, national economic security, national public health or safety, or any combination of those matters“ führen würde.⁷ Um solche Schäden zu verhindern, müssen die kritischen Infrastrukturen resilient sein. Dafür tragen verschiedene Regierungsbehörden, allen voran das DHS, auf nationaler, bundesstaatlicher, regionaler und lokaler Ebene sowie die Betreiber und Besitzer der Infrastrukturen Verantwortung.

Im Bereich der kritischen Infrastrukturen legt die PPD 21 fest, dass unter anderem Forschung und Entwicklungen zu ganz bestimmten Themen gefördert werden sollen. Dazu zählen erstens die Erforschung resilienten Designs und resilienter Konstruktionsweisen für kritische Infrastrukturen und zweitens eine Erweiterung bestehender Modellierungsansätze durch neue Forschungsansätze, um die Auswirkungen – speziell im Hinblick auf Kaskadeneffekte – widriger Ereignisse auf kritische Infrastrukturen simulieren und untersuchen zu können. Daneben sollen Initiativen unterstützt werden, die Anreize zu Investitionen in Cybersicherheit und resilientes Design kritischer Infrastrukturen fördern. Und auch die strategische Lenkungsrolle des DHS soll mithilfe von Forschung und Entwicklung ausgebaut und unterfüttert werden.⁸

Diese Inhalte der PPD 21 zeigen, dass die Vereinigten Staaten, was die Implementation von Resilienz in konkrete Regierungsdokumente und daraus zu ziehende Konsequenzen, wie etwa eine Intensivierung der Förderung von Forschung und Entwicklung im Bereich Resilienz kritischer Infrastrukturen, angeht, Deutschland einige Schritte voraus sind. Für den deutschen Diskurs kann insofern nur die Notwendigkeit unterstrichen werden, derart konkrete Handlungsempfehlungen in Zukunft ebenfalls in Regierungsprogramme mit aufzunehmen, um im nächsten Schritt die Investitionen in Forschung und Entwicklung zielgerichtet auf die vorhandenen Notwendigkeiten abstimmen zu können.

⁵ The White House 2013, S. 2.

⁶ The White House 2013, S. 1-12.

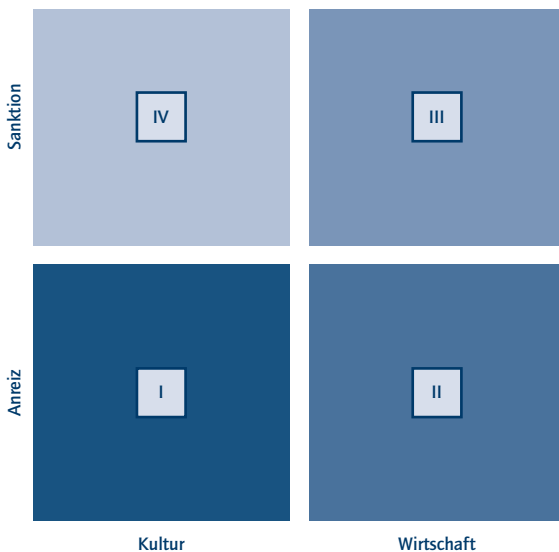
⁷ The White House 2013, S. 11f.

⁸ The White House 2013, S. 8.

RESILIENTE UNTERNEHMEN

Resilienz im unternehmerischen Sinne ist für die Zwecke dieser Position definiert als die Fähigkeit eines Unternehmens, ein mit geringer Wahrscheinlichkeit eintretendes Ereignis unterschiedlicher Art, welches extrem geschäftskritische Auswirkungen haben kann, durch eine gute Vorbereitung (Prävention) und eine unmittelbare Steuerung im Eintrittsfall (Reaktion) zu vermeiden oder abzumildern und somit eine starke Widerstandsfähigkeit gegenüber unvorhersehbaren Situationen in betrieblichen Prozessen zu etablieren, um den Fortbestand des Unternehmens zu sichern. Damit stellt das Konzept eine Erweiterung und einen Ausbau des in vielen Unternehmen bereits verankerten Business Continuity Management (BCM) dar.⁹

Abbildung 2: Quadrantensystem zur Motivation von Unternehmen in puncto Resilienz



Quelle: KPMG AG WPG.

Die Motivation von Unternehmen zur Steigerung von Resilienz ist unterschiedlich. Im Wesentlichen können die verschiedenen Beweggründe in vier Dimensionen beschrieben werden:

1. Anreiz für Resilienz
2. Sanktionierung bei zu geringer Resilienz
3. Kulturelle Motivation
4. Wirtschaftliche Motivation

Unternehmen lassen sich in einem System von vier Quadranten anhand der oben genannten Dimensionen einordnen (vgl. Abb. 2).

Quadrant I: Kulturelle Motivation und Anreize

In diesem Quadranten sollen diejenigen Unternehmen geführt werden, deren Motivation durch ihr kulturelles Umfeld und den daraus abzuleitenden Vorteil geprägt ist.

Quadrant II: Wirtschaftliche Motivation und Anreize

In diesem Quadranten sind diejenigen Unternehmen verortet, deren Motivation auf einem wirtschaftlichen Vorteil basiert.

Quadrant III: Wirtschaftliche Motivation und Sanktion

Dieser Quadrant beschreibt die Situation, dass Unternehmen motiviert sind, Resilienzmaßnahmen umzusetzen, wenn sie wirtschaftliche Nachteile, die wie eine Sanktion wirken, befürchten.

Quadrant IV: Kulturelle Motivation und Sanktion

Dieser Quadrant beschreibt die Situation, dass Unternehmen eine starke Motivation zur Umsetzung von Resilienzmaßnahmen erfahren, wenn sie fürchten müssen, dass sie unmittelbar Nachteile aufgrund von Abweichungen zur kulturellen Norm erfahren müssen, welche sich mittelbar in wirtschaftlichen Nachteilen ausdrücken.

⁹ Vgl. Thoma 2014, Kapitel 3.

Die unterschiedlichen Ziele von Unternehmen und Staat führen unter Umständen zu gegensätzlichen Motivationslagen in puncto Resilienz. Während staatliche Institutionen, sofern sie ihren Auftrag erfüllen, das Gemeinwohl im Blick haben, richten sich Unternehmen stärker an Gewinnmaximierung und Unternehmensstrategien, die diese unterstützen, aus. Konflikte können dann entstehen, wenn Unternehmen hoheitliche Aufgaben übernehmen, wirtschaftlich agieren aber dennoch denselben Resilienzansforderungen unterstehen wie staatliche Organisationen. Hier gilt es, Anreizsysteme zu schaffen, die die Stärkung von Resilienz bei betroffenen Unternehmen begünstigen.

Für solche Unternehmen sind unter Umständen regulatorische Maßnahmen sinnvoll, um genannte Diskrepanzen im Resilienzverhalten zu überwinden. Für alle anderen Unternehmen

ist die intrinsische Motivation ausreichend, um die wirtschaftliche Existenzsicherung selbstständig umzusetzen.

Bestehende Gesetze zur Regulierung von Aspekten der Resilienz sind zu stark auf den Verteidigungsfall ausgerichtet (zum Beispiel Notstandsgesetze), der im Sinne von Ereignissen der Betriebsunterbrechung immer weiter an Bedeutung verliert. Eine Überarbeitung solcher Gesetze erscheint daher sinnvoll. Die Einführung von Meldepflichten für bestimmte Vorfälle ist dann sinnvoll, wenn die Meldungen als Grundlage für ein Frühwarnsystem dienen und so zu stärkerer Prävention beitragen. Die Sinnhaftigkeit solcher Meldepflichten und die Frage, auf welche Ereignisse und Branchen sie sinnvollerweise anwendbar wären, kann Gegenstand zukünftiger Überlegungen sein. Ungeklärt ist auch die Frage, an wen gemeldet werden sollte.

3 HANDLUNGSEMPFEHLUNGEN

acatech gibt insgesamt zehn Handlungsempfehlungen zur Verbesserung des Schutzes kritischer Infrastrukturen. Die Handlungsempfehlungen wurden aus den Ergebnissen der STUDIE „Resilien-Tech – ‚Resilience-by-design‘: Strategie für die technologischen Zukunftsthemen“¹⁰ abgeleitet. Diese Handlungsempfehlungen für politische Entscheidungsträger bilden in ihrer Bandbreite sehr bewusst völlig verschiedene Aspekte des komplexen Konzepts Resilienz ab. Sie adressieren unterschiedliche Zielgruppen und bewegen sich auf mehreren Abstraktionsebenen. Damit wird sichergestellt, dass Resilienz in der Tat als holistisches Konzept im Kontext der anwendungsorientierten Sicherheitsforschung verwendet wird und den Mehrwert entfalten kann, der überhaupt erst die intensive Beschäftigung mit diesem Konzept lohnend macht. Die Handlungsempfehlungen können in ihrer Gesamtheit als Agenda auf dem Weg zur resilienten Gesellschaft von morgen verstanden werden. Sie weisen die ersten Schritte des Weges und werfen selbst wiederum eine Vielzahl neuer Fragen auf, die beantwortet werden müssen, um das Ziel einer resilienteren Gesellschaft zu erreichen.

HANDLUNGSEMPFEHLUNG 1

Resilienz als ganzheitliches Konzept zur Minimierung schädlicher Auswirkungen widriger Ereignisse auf unsere Gesellschaft anwenden. So kann es gelingen, die Funktions-, Anpassungs-, Widerstands- und Lernfähigkeit komplexer Systeme angesichts externer oder interner Schocks nachhaltig zu erhöhen. Dazu müssen geeignete und korrespondierende Maßnahmen technologischer, gesellschaftlicher und ökonomischer Art erforscht, entwickelt, ergriffen und integrativ miteinander kombiniert werden.

Was heißt das?

Der holistische Ansatz des a priori unklaren Konzepts Resilienz ist der zentrale Mehrwert, den die Verwendung des Begriffs der deutschen Gesellschaft langfristig bieten kann. Warum ist das so? Das Wort Resilienz läuft aufgrund seiner

Begriffsgenese und der bisherigen Verwendung Gefahr, zu einem inhaltsleeren und beliebigen Schlagwort zu degenerieren, welches verschiedene Akteure je nach ihren spezifischen Interessen bewusst völlig unterschiedlich verstehen. Dieser Gefahr kann durch ein konsistentes und klares Verständnis davon, was den Kern von Resilienz ausmacht, entgegengewirkt werden. Der Kern besteht demnach darin, dass resiliente Gesellschaften in der Lage sind, die menschlichen, ökonomischen und ökologischen Schäden, die durch widrige Ereignisse verursacht werden, so gering wie irgend möglich zu halten. Sie schaffen das, indem sie sich jedweder denk- und durchführbarer Lösungen bedienen, unabhängig davon, ob es sich um Technologien, gesellschaftliche Werkzeuge wie Bildung und den Dialog auf Augenhöhe mit der Bevölkerung oder ökonomische Anreize handelt. Insbesondere das Zusammendenken der verschiedenen Lösungsmöglichkeiten und ihre zielgerichtete kombinierte Verwendung vor, während und nach einem Krisenfall machen resiliente Gesellschaften aus. Ihr besonderes Kennzeichen ist es, dass sie auf ständig wechselnde Umwelteinflüsse dynamisch reagieren und sich an unerwartete gravierende Ereignisse anpassen können. Resilienz ist insofern kein statischer Zustand, sondern eine Eigenschaft lernfähiger und beweglicher, adaptiver Systeme. Dieses Verständnis von Resilienz wird so bereits in Ländern wie den USA, Großbritannien und der Schweiz sowohl als Ausgangspunkt für Forschungsprogramme genutzt als auch in konkretem Regierungshandeln umgesetzt. Auch in Deutschland sollte dies künftig ernsthaft in Betracht gezogen werden.

HANDLUNGSEMPFEHLUNG 2

Metriken und Indikatoren zur Bewertung von Verwundbarkeit und Resilienz entwickeln. Nur wenn die Verwundbarkeit und die Resilienz von Gesellschaften und ihren Subsystemen in ein vernünftiges und operationalisierbares quantitatives Verhältnis gesetzt werden können, ist es möglich, umfassender als bisher systematisch nach Schwachstellen zu suchen,

¹⁰ Thoma 2014.

den Nutzen von Investitionen zu bewerten oder festzustellen, wie bestimmte Maßnahmen Resilienz beeinflussen. Die deutsche Forschung sollte sich deshalb der Herausforderung annehmen, ein nützliches Maß für Resilienz zu entwickeln.

Was heißt das?

Vulnerabilitäten lassen sich identifizieren, kategorisieren, messen, abbilden und miteinander vergleichen. Die Verwundbarkeit bestimmter geografischer, technologischer oder sonstiger Einheiten gegenüber spezifischen Bedrohungen wird bereits sowohl in Deutschland als auch in anderen Ländern wie zum Beispiel den USA erhoben. Hier besteht die Herausforderung in einer Verstärkung dieser Anstrengungen sowie der systematischen, interdisziplinären Ausweitung auf potenziell betroffene Systeme und alle Arten von Bedrohungen. Der Forschungsbedarf ist aufgrund der Komplexität der Phänomene evident. Noch deutlich schwieriger und bisher ohne gänzlich zufriedenstellende Lösung geblieben ist die Herausforderung, eine geeignete Methode zur Messung von Resilienz zu entwickeln. Die Forscher stehen einer Vielzahl an konzeptionellen Schwierigkeiten und methodischen Fallstricken gegenüber: Welche Variablen sind wie wichtig? Mithilfe welcher Indikatoren lassen sie sich operationalisieren? Kann die Resilienz verschiedener Systeme miteinander verglichen werden? Welche Dimensionen müssen integriert werden und wie können sie gewichtet werden? Sind qualitative oder quantitative, absolute oder relative Maße sinnvoll? Und wie kann Resilienz als dynamische Eigenschaft mithilfe einer Bewertung oder Messung zu einem bestimmten Zeitpunkt sinnvoll erhoben werden? Trotz der Vielzahl an offenen Fragen lohnt sich die Anstrengung. Zudem muss die Resilienzmessung kein perfektes Ergebnis produzieren. Vielmehr wird eine hinreichend differenzierende Aussage über den Grad der Resilienz zwischen verschiedenen untersuchten Einheiten angestrebt, um so besonders resiliente Systeme als Vorbilder und besonders wenig resiliente Systeme als der Hilfe bedürftig identifizieren zu können. Deshalb sollte sich die deutsche Forschungslandschaft mithilfe der entschlossenen Unterstützung der

politisch Verantwortlichen und im Schulterschluss mit allen relevanten Akteuren – wie zum Beispiel den Betreibern kritischer Infrastrukturen – dieser Herausforderung annehmen.

HANDLUNGSEMPFEHLUNG 3

Methoden zur Modellierung und Simulation komplexer soziotechnischer Systeme mit hoher gesellschaftlicher Relevanz entwickeln. Forschungsansätzen, die bestehende Modellierungsansätze erweitern und die Auswirkungen widriger Ereignisse speziell im Hinblick auf Kaskadeneffekte simulieren helfen, sollte in der Sicherheitsforschung größeres Gewicht eingeräumt werden. Entscheidend sind die zuverlässige Identifikation systemkritischer Knotenpunkte und Schnittstellen, deren Schädigung zu Kaskadeneffekten führt, und die Vorhersage des Potenzials zur Selbstorganisation des Systems.

Was heißt das?

Um die Resilienz komplexer Systeme zielgerichtet erhöhen zu können, benötigen die verantwortlichen Akteure ein detailliertes, genaues Verständnis des Verhaltens der Systeme und ihrer exakten Funktionsweise auch und gerade im Extremfall. Dafür können sie natürlich nicht auf das Eintreten externer oder interner Schocks warten. Sie müssen vielmehr bereits im Vorhinein bei der Planung des Systems sowie während des Normalzustands, wenn das System wie vorgesehen funktioniert, in der Lage sein, Extremfälle möglichst wirklichkeitsnah nachzustellen. Auf diese Weise können sie Schwachstellen erkennen, Gegenmaßnahmen planen, Fehler korrigieren und alles tun, um das System möglichst umfassend auf das Eintreten widriger Ereignisse vorzubereiten. Die Simulation und Modellierung komplexer Systeme versetzt sie genau dazu in die Lage. Es existiert schon heute eine Vielzahl an Möglichkeiten zur Modellierung. Gerade vor dem Hintergrund der fortschreitenden Komplexitätszunahme und der größer werdenden Interdependenzen vormals unabhängiger Subsysteme werden

aber weitergehende, fortschrittlichste Methoden benötigt, um das Systemverhalten auch für das Eintreten unerwarteter Ereignisse zuverlässig abbilden zu können. Daher sollte verstärkt an der Erforschung von Methoden gearbeitet werden, die nicht nur das „Durchrechnen“ vorher festgelegter Szenarien erlauben. Zukünftige Modellierungsansätze müssen das Gesamtsystem darstellen können, ohne vorher definierte Szenarien einzubeziehen. Das Ziel sind multimodale Simulationen, die in einem integrierten Ansatz technische und soziale Systeme und ihr komplexes Zusammenspiel abbilden können. Hierfür werden Investitionen in Forschung und Entwicklung benötigt, die auch im Hinblick auf eine Standardisierung und Vereinbarkeit verschiedener Modellierungsansätze getätigt werden sollten.

HANDLUNGSEMPFEHLUNG 4

Resilience Engineering als eigenständiges Fachgebiet etablieren: Die Erforschung, Entwicklung und Umsetzung resilienten Designs und resilienter Konstruktionsweisen für kritische Infrastrukturen forcieren. *Die Infrastrukturen müssen mithilfe innovativer Technologien für das 21. Jahrhundert fit gemacht werden. Resilience Engineering bedeutet, maßgeschneiderte technologische und interdisziplinäre Methoden und Lösungen zu entwickeln, mit deren Hilfe Systeme von entscheidendem gesellschaftlichen Wert resilient gestaltet werden können.*

Was heißt das?

Die nachhaltige und zuverlässige Funktionsfähigkeit der kritischen Infrastrukturen moderner Gesellschaften ist buchstäblich überlebensnotwendig für diese. Ohne Energie, Wasser, Nahrung, Mobilität, Kommunikation usw. ist menschliches Zusammenleben nicht denkbar. Um die Funktions-, Anpassungs-, Widerstands- und Lernfähigkeit der kritischen Infrastrukturen angesichts widriger Ereignisse jedweder Art sicherzustellen und zu erhöhen, ist Resilience

Engineering das Mittel der Wahl. Resilience Engineering ist die ingenieurwissenschaftlich-interdisziplinäre Erforschung und Entwicklung von Vorgehensweisen und Methoden zur Erhöhung von Widerstandsfähigkeit, Anpassbarkeit und Selbstorganisation von Systemen hohen gesellschaftlichen Werts. Dahinter verbirgt sich eine konsequente und frühzeitige Einbeziehung technologischer Lösungsansätze für Sicherheitsprobleme aller Art in jegliche Planungs- und Umsetzungsaktivitäten bedeutender gesellschaftlicher Projekte von der individuellen bis zur Gesamtsystemebene. Ziel ist es, kritische Teilfunktionen dieser Systeme im Schadensfall auch außerhalb der Standardanforderungen kontrolliert aufrecht zu erhalten und einen katastrophalen Totalausfall zu vermeiden. Es werden maßgeschneiderte technologische Lösungen zur Erhöhung der Resilienz einzelner Infrastrukturen benötigt, die gleichzeitig hinsichtlich ihrer Wirkung und ihrer Effekte auf das Gesamtsystem optimiert und durch intelligente Lösungen aus anderen Bereichen wie der Ökonomie, der Ökologie oder der Sozialwissenschaften ergänzt werden. Beispielhaft kann man an dieser Stelle auf Technologien wie selbstheilende, adaptive Werkstoffe oder durch energieautarke, automatisierte Sensornetzwerke intelligent und lernfähig gestaltete Bauwerke verweisen. Resilience Engineering ermöglicht es zudem, die Entstehung nicht kompatibler Insellösungen zu vermeiden. Der ganzheitliche Aspekt von Resilienz kommt hier insofern zum Tragen, als Technologien künftig sowohl untereinander als auch nach außen anschlussfähig für weitere Lösungsmöglichkeiten sein müssen. Dieses neuartige Verständnis der Rolle der Ingenieurwissenschaften, wenn es um die Sicherstellung und Erhöhung der Resilienz der Gesellschaft und insbesondere deren kritischer Infrastrukturen geht, sollte in den nächsten Jahren auch in Deutschland verstärkt Einzug in das nationale Sicherheitsforschungsprogramm halten und sich insbesondere in den sicherheitsrelevanten Strategien der deutschen Bundesregierung wie zum Beispiel dem nationalen Plan zum Schutz Kritischer Infrastrukturen (KRITIS) wiederfinden.

HANDLUNGSEMPFEHLUNG 5

Strategien zur nachhaltigen Stärkung der Eigenverantwortlichkeit der Bürgerinnen und Bürger angesichts widriger Ereignisse entwickeln und umsetzen. *In einem Dialog auf Augenhöhe und mithilfe der Schaffung weitreichender Möglichkeiten zur Partizipation auf verschiedenen, dezentralen Ebenen sollte die Bevölkerung aktiv an der Gestaltung resilienterer Gesellschaften beteiligt werden. Vorsorge vor und Akzeptanz von Risiken kann von staatlicher Seite unterstützt werden, etwa durch Lehrinhalte an Schulen, durch Stärken des freiwilligen Engagements in Feuerwehren, bei DRK, THW und vielen weiteren Rettungsorganisationen oder durch weitere konkrete Maßnahmen.*

Was heißt das?

Der erste Schritt dazu ist die Schaffung eines verantwortungsvollen Bewusstseins dafür, was alles passieren könnte. Nur wer mit dem Eintreten widriger Ereignisse rechnet, kann sich mental und durch Handeln darauf vorbereiten und wird so in die Lage versetzt, den Schock möglichst unbeschadet zu überstehen. Ein derartiges Bewusstsein zu schaffen und effizient Katastrophenschutz und -vorsorge zu betreiben, erfordert beispielsweise regelmäßige Notfall- und Katastrophenübungen. So werden Routinen eingeübt und Selbstverständlichkeiten aufgebaut, die im Krisenfall Leben retten können. Regelmäßige Übungen für den Ernstfall schaffen zudem die Überzeugung – und damit ein Stück weit die Fähigkeit selbst – gegenüber Katastrophen aller Art gerüstet und gut vorbereitet zu sein. In Deutschland engagieren sich bereits heute sehr viele Menschen freiwillig bei Feuerwehren und Rettungsorganisationen. Dieses Potenzial gilt es zu erhalten und weiter auszubauen sowie bei der Schaffung eines Bewusstseins für Katastrophen in der gesamten Bevölkerung zu nutzen. Ein weiterer Weg, der künftig verstärkt beschritten werden sollte, ist die Einbindung entsprechender Lerninhalte in Schulunterricht und Weiterbildungsangebote. Die Fokussierung auf Bildung und Ausbildung von Menschen zur Erhöhung ihrer Resilienz ist ein sehr wichtiger Aspekt auf dem Weg hin

zu resilienteren Gesellschaften. Dabei muss eine Überfrachtung, die zur Gleichgültigkeit gegenüber Gefahren führt, genauso vermieden werden wie eine dauerhafte Verunsicherung aufgrund der unüberschaubaren Risiken. Mithilfe der Integration verschiedener Methoden zur Stärkung der Eigenverantwortlichkeit der Bürger soll es langfristig gelingen, neben der Befähigung Einzelner auch Sozialkapital und sozialen Zusammenhalt auf nachbarschaftlicher, lokaler Ebene zu stärken. Denn diese Faktoren können bei Eintreten eines widrigen Ereignisses einen großen Einfluss darauf haben, wie gut die jeweilige geografische Einheit den entsprechenden Schock übersteht. Insofern sollten zukünftig Forschungsanstrengungen wie auch Umsetzungsbemühungen, welche die Eigenverantwortlichkeit der Bürgerinnen und Bürger stärken, auf verschiedenen Ebenen forciert werden.

HANDLUNGSEMPFEHLUNG 6

Den langfristigen Mehrwert von Resilienz für Gesellschaften aufzeigen. *Es bedarf einer Erweiterung der Perspektive, weg von einer kurzfristigen und kurzsichtigen Nutzenoptimierung, hin zu strategischem und nachhaltigem Denken und Handeln. Dazu müssen künftige Forschungsansätze ökonomische Aspekte von Anfang an mitdenken. So können sie aufzeigen, dass sich Investitionen in Resilienz lohnen. Damit wird aus dem vermeintlichen Kostenträger Resilienz ein Business Case.*

Was heißt das?

Gesellschaften, deren Wirtschaftssystem marktwirtschaftlich organisiert ist, nutzen für Entscheidungen über Investitionen grundsätzlich eine mehr oder weniger ausgeklügelte Kosten-Nutzen-Rechnung. Staatliche Investitionsentscheidungen sind von dieser Logik teilweise ausgenommen, da ihnen häufig kein direkter Nutzenzuwachs in Form von monetärem Benefit entgegensteht. Nichtsdestotrotz versucht auch der Staat mit dem Einsatz seiner knappen Mittel ein bestmögliches Ergebnis im Rahmen der zuvor definierten

Anforderungen zu erreichen. Die Mittel sollen möglichst effizient und effektiv genutzt werden. Entscheidend ist die Bewertungsgrundlage, anhand derer darüber befunden werden soll, ob der Mitteleinsatz effizient und effektiv ist. Maßnahmen zur Erhöhung der Resilienz einer Gesellschaft kosten Geld, von benötigten Investitionen in Forschung und Entwicklung, über den zusätzlichen Aufwand für resiliente Konstruktionsweisen kritischer Infrastrukturen bis hin zu Kosten für die Implementation des Konzepts in Lerninhalte an Schulen. Trotzdem ist Resilienz kein „kostspieliges Add-on“, kein verzichtbarer Luxus, sondern vielmehr Grundvoraussetzung für die Nachhaltigkeit von Investitionen. Denn in Anbetracht der immer größer werdenden Herausforderungen, denen sich unsere Gesellschaften gegenübersehen, sind Systeme, die bei der ersten kleinen Störung zusammenbrechen, weil sie unter der Maßgabe der bedingungslosen Kostenreduktion gestaltet wurden, kein langfristig tragbares Modell. Die durch Resilienz im ersten Moment entstehenden Mehrkosten lohnen sich in einer auf Nachhaltigkeit ausgerichteten Betrachtungsweise gleich in mehrfacher Hinsicht: zum einen durch die Vermeidung menschlichen Leids im Falle des Eintretens widriger Ereignisse, zum anderen aber auch finanziell. Einer Untersuchung des Multi-Hazard Mitigation Council zufolge verhindert jeder Dollar, der in Maßnahmen zur Mitigation im Vorfeld von Erdbeben, Fluten und Stürmen investiert wird, im Nachhinein Schäden von ungefähr vier Dollar.¹¹ Dafür ist es selbstverständlich erforderlich, genau zu wissen, wo sich welche Investitionen wie sehr lohnen. Zukünftige Forschungsanstrengungen zur Erhöhung der gesellschaftlichen Resilienz sollten deshalb ökonomische Aspekte von Anfang an mitberücksichtigen.

HANDLUNGSEMPFEHLUNG 7

Anreize für Unternehmen schaffen, ihre Resilienz zu erhöhen. *Es sollte darüber nachgedacht werden, ein standardisiertes Resilienz-Monitoring einzuführen, welches von öffentlicher Seite begleitet und gegebenenfalls koordiniert wird,*

um gesellschaftlich relevante Unternehmen, die nachweislich ihre Resilienz steigern, in geeigneter Form zu intensivieren und diejenigen gesellschaftlich relevanten Unternehmen, die dem Aufbau von Resilienz nicht nachkommen, durch erhöhte Versicherungsprämien, Zusatzabgaben oder Ähnliches zu beeinflussen.

Was heißt das?

Unternehmen versuchen grundsätzlich, durch ihre Geschäftstätigkeit ihren Gewinn zu maximieren. Dazu benötigen sie einen möglichst störungsfreien und reibungslosen Ablauf ihrer Geschäfte. Deshalb betreiben die meisten Unternehmen zumindest implizit Risikovorsorge, das heißt sie wappnen sich durch geeignete Gegenmaßnahmen für den Fall des Eintretens bestimmter widriger Ereignisse. Entscheidend sind dabei die vermutete Schadenshöhe sowie die Eintrittswahrscheinlichkeit. Resilienz bezieht sich im unternehmerischen Kontext auch auf die Ereignisse, deren Eintreten unerwartet, demzufolge sehr unwahrscheinlich ist. Obwohl die Schadenshöhe zum Beispiel bei Naturkatastrophen enorm sein kann, sind nur die wenigsten Unternehmen auf derartige Risiken vorbereitet. Die geringe Eintrittswahrscheinlichkeit macht Investitionen scheinbar unrentabel. Daher sollte künftig nach Wegen gesucht werden, die Unternehmen dabei helfen, resilienter angesichts unwahrscheinlicher, aber gravierender widriger Ereignisse zu werden. Eine erfolgversprechende Maßnahme kann die Einführung von Versicherungspflichten gegenüber widrigen Ereignissen sein, wobei jene auch veranlasst werden müssen, derartige Versicherungen anzubieten. Daneben bietet sich eine Überwachung der von Unternehmen getätigten Schritte hin zu mehr Resilienz von staatlicher Seite an. Dazu bedarf es Regularien darüber, was Unternehmen tun müssen, um resilienter zu werden, zum Beispiel die Durchführung von Notfall- und Krisenübungen oder die Einrichtung gewisser Redundanzen und Puffer im Geschäftsablauf. Die Einhaltung oder Nichtbeachtung dieser Regularien kann dann von staatlicher Seite entsprechend belohnt oder sanktioniert werden. Wie das auf effektive Weise gelingen kann,

¹¹ The National Academies 2012, S. 13.

ohne die Wettbewerbsfähigkeit von Unternehmen zu gefährden, ist eine Frage, zu deren Beantwortung noch einige Anstrengungen unternommen werden müssen.

HANDLUNGSEMPFEHLUNG 8

Meldepflichten im Sinne eines Frühwarnsystems einführen. *Trotz der geringen Wahrscheinlichkeit des Eintretens gravierender widriger Ereignisse, treten diese faktisch auf. Daher sollte ein nationales Frühwarnsystem eingeführt werden, welches mit einer auf Branchen zugeschnittenen Meldepflicht (zum Beispiel durch branchenspezifische Meldekriterien) verbunden ist, die Unternehmen vorschreibt, sicherheitskritische Ereignisse zu melden.*

Was heißt das?

Die meisten Unternehmen rechnen im normalen Tagesgeschäft nicht mit dem plötzlichen Eintreten schwerer Schocks. Daher mangelt es vielen von ihnen an einem entsprechenden Gefahrenbewusstsein. Meldepflichten für bestimmte Vorfälle können diese Art Bewusstsein stimulieren. In diesem Sinne können sie als Frühwarnsystem dienen und so zu einer deutlich stärkeren Prävention beitragen. Die zu erwartenden Befürchtungen von Unternehmen, durch derartige Meldepflichten unter Umständen an einem öffentlichen Pranger zu stehen und in ihrer Geschäftstätigkeit geschädigt zu werden, müssen dabei ernst genommen und durch eine entsprechende Ausgestaltung der Meldepflichten entkräftet werden. Außerdem muss vor der Einführung derartiger Regelungen intensiv untersucht werden, für welche Ereignisse und Branchen diese implementiert werden sollen und welche Informationen an wen gemeldet werden müssen. Die Pflichten sollten sich nur an solche Unternehmen richten, für die ein teilweiser oder gänzlicher Zusammenbruch ihrer Geschäftstätigkeit gravierende negative Auswirkungen auf die lokale, regionale oder nationale Wirtschaft haben könnte. Derartige Meldepflichten scheinen zudem gerade für die zunehmende Bedrohung

durch Cyber-Kriminalität besonders sinnvoll, da sie dort die Aufmerksamkeit für bevorstehende oder wahrscheinliche Attacken erhöhen sowie eine zielgerichtete Bekämpfung erlauben. Selbstverständlich gilt es auch hier, mithilfe eines durchdachten Systems mögliche Reputationschäden und sonstige Benachteiligungen für die betroffenen Unternehmen von vorneherein auszuschließen.

HANDLUNGSEMPFEHLUNG 9

Eine nationale Resilienzstrategie entwickeln. *Es wird eine übergreifende Vision für resiliente Gesellschaften im größeren Kontext der nachhaltigen Entwicklung benötigt. Resilienz als holistisches Konzept kann nicht per Gesetz verordnet werden. Eine nationale Resilienzstrategie kann aber den Grundstein legen, den vielfältigen Herausforderungen der immer komplexer werdenden, hochtechnisierten Welt mit einem konsistenten und umfassenden Ansatz zu begegnen und davon ausgehend maßgeschneiderte Lösungen für spezifische Probleme zu entwickeln.*

Was heißt das?

Das ganzheitliche Konzept Resilienz kann seinen vollen Nutzen für die Gesellschaft nur dann entfalten, wenn es auch auf der politischen Ebene angenommen und als notwendig erkannte Maßnahme entschlossen unterstützt wird. Dazu bedarf es in einem ersten Schritt der einer nationalen Resilienzstrategie. Durch eine solche Strategie wird deutlich, dass Regierung und verantwortliche Behörden die Erhöhung der Resilienz der Gesellschaft und ihrer relevanten Subsysteme als unabdingbar für deren Zukunftsfähigkeit erkannt haben. Sie kann zugleich Ausgangspunkt für konkrete Pläne zur Umsetzung resilienzerhöhender Maßnahmen sein, zum Beispiel im Bereich der kritischen Infrastrukturen. Dazu gehört auch eine ständige Überprüfung der einzelnen Bereiche der Regierung, wie zum Beispiel nachgeordneter Katastrophenschutzbehörden, im Hinblick darauf, ob sie Resilienz in angemessener Weise als Organisationsprinzip

in ihre Arbeit aufnehmen und zur Umsetzung hinreichend stark mit anderen verantwortlichen Stellen kooperieren können. Vor allen Dingen in der anwendungs- und lösungsorientierten Sicherheitsforschung kann Resilienz als zugrunde liegende Handlungsmaxime die Basis aller künftigen Forschungsanstrengungen bilden. Damit lassen sich innovative Ideen und Ansätze schneller und besser identifizieren, Forschungslücken aufdecken und ein möglicher Mehrwert, den einzelne Lösungen zur ganzheitlichen Resilienz der Gesellschaft beitragen, zuverlässig bewerten. Die Handlungsempfehlungen 2 bis 8 sind insofern vor diesem Hintergrund als die Themen und Bereiche zu verstehen, in denen durch eine Intensivierung der Bemühungen in Forschung und Entwicklung Deutschland und Europa insgesamt resilienter gestaltet werden können.

HANDLUNGSEMPFEHLUNG 10

Resilienz als Schlüsselkomponente nachhaltiger Entwicklung etablieren. *Nachhaltigkeit bedeutet, das menschliche Zusammenleben so zu gestalten, dass es den Bedürfnissen der heutigen Generation entspricht, ohne die Möglichkeiten künftiger Generationen zu gefährden, ihre eigenen Bedürfnisse zu befriedigen. Dazu müssen Gesellschaften überlebensfähig angesichts großer Herausforderungen sein. Überlebensfähigkeit setzt Funktions-, Anpassungs-, Widerstands- und Lernfähigkeit voraus. Genau das ist das charakteristische Wesensmerkmal resilienter Systeme. Das Konzept Resilienz schlägt also eine Brücke zwischen Sicherheits- und Nachhaltigkeitsforschung.*

Was heißt das?

Nachhaltigkeit ist im Laufe der letzten beiden Jahrzehnte zu einem der wichtigsten politischen Leitmotive weltweit geworden. Das gilt in sogar noch größerem Maße für Deutschland, wo beispielsweise durch die Idee der Energiewende ein Kernbestandteil nachhaltiger Entwicklung bereits in der Praxis umgesetzt werden soll. Nachhaltigkeit bedeutet aber

weit mehr als nur die Umstellung der Energieversorgung einer Gesellschaft von fossilen Energieträgern auf regenerative Gewinnung. Die Vereinten Nationen etwa definieren sieben Schlüsselkomponenten nachhaltiger Entwicklung und sind so in der Lage, die drei entscheidenden Dimensionen des Konzepts mit Inhalt zu füllen. Nachhaltig ist eine Entwicklung dann, wenn sie sowohl ökologisch und ökonomisch als auch sozial sinnvoll für die lebende und für zukünftige Generationen ist. Dieser Ansatz wird als Dreisäulen-Modell der Nachhaltigkeit bezeichnet. Die sieben Schlüsselkomponenten nachhaltiger Entwicklung sind dann folgerichtig faire Beschäftigung, nachhaltige Energieversorgung, Nahrungssicherheit und nachhaltige Landwirtschaft, eine nachhaltige Stadtentwicklung, sichere Wasserversorgung, ein nachhaltiger Umgang mit den Ozeanen und die resiliente Gesellschaft. Jede dieser Schlüsselkomponenten bedarf für sich noch einer weiteren Spezifizierung, um daraus konkrete Handlungsempfehlungen zur Erhöhung der Nachhaltigkeit von Gesellschaften abzuleiten. Klar ist aber, dass nur durch eine intensive und insgesamt gleichrangige Beachtung der sieben Schlüsselkomponenten die Entwicklung der Welt nachhaltig gestaltet werden kann. Resilienz bedeutet in diesem Kontext das Vermögen, die Funktions-, Anpassungs-, Widerstands- und Lernfähigkeit angesichts elementarer Veränderungsprozesse bei gleichzeitig auftretenden gravierenden Schadensereignissen zu wahren. Das wiederum ist für Nachhaltigkeit im Sinne der Zukunftsfähigkeit menschlicher Gesellschaften überlebensnotwendig. Ergo kann Nachhaltigkeit nur gelingen, wenn sie Resilienz mitdenkt. Sowohl Sicherheits- als auch Nachhaltigkeitsforschung sollten daher Resilienz als Teil ihrer Programmatik begreifen und entsprechende Forschungsaktivitäten hervorbringen.

Diese zehn Handlungsempfehlungen sind in ihrer Gesamtheit als eine Art Blaupause für den Aufbau resilienterer Gesellschaften zu verstehen. Gleichzeitig können sich Entscheidungsträger aus ihnen wie aus einem Werkzeugkasten bedienen. Wie bereits erwähnt decken sie eine sehr große

Bandbreite völlig unterschiedlicher Aspekte des komplexen Konzepts Resilienz ab. Ohne den Blickwinkel unnötig zu verengen und damit die Nützlichkeit des Konzepts zu untergraben, konzentrieren sie sich auf Wege zur Erhöhung der Resilienz kritischer Infrastrukturen. Dabei werden komplexe und interdependente kritische Infrastrukturen als soziotechnische Systeme verstanden. Für sie wie für Gesellschaften

insgesamt gilt es, einen Resilience-by-design-Ansatz in künftige Forschungsstrategien zu integrieren und so Resilienz zur fundamentalen Grundvoraussetzung jeglicher technologischer oder gesellschaftlicher Sicherheitslösungen zu machen, damit Deutschland auch in Zukunft die Unversehrtheit der Bürgerinnen und Bürger sowie die lebenswichtigen Infrastrukturen wirksam schützen kann.

LITERATUR

Coaffee, J./Wood, D./Rogers, P.: „The Everyday Resilience of the City. How Cities Respond to Terrorism and Disaster“. In: Hrsg.: Croft, S., *New Security Challenges*, Basingstoke: Palgrave Macmillan 2009.

Edwards, C.: *Resilient Nation*, London: Demos 2009.

Frankfurter Allgemeine Zeitung: *Schadensbilanz des Hochwassers. Rekordverdächtige Flut*, 2013. URL: <http://www.faz.net/aktuell/wirtschaft/wirtschaftspolitik/schadensbilanz-des-hochwassers-rekordverdaechtige-flut-12276172.html> [Stand: 01.08.2013].

Holling, C. S.: *From complex regions to complex worlds*, 2004. URL: <http://www.ecologyandsociety.org/vol9/iss1/art11> [Stand: 6.10.2013]

Kaufmann, S.: *Resilienz – ja, bitte! Nur wie?*, 2013. URL: <http://www.sicherheitspolitik-blog.de/2013/04/29/resilienz-kaufmann/> [Stand: 6.10.2013]

Pimm, S. L.: *The balance of nature? Ecological issues in the conservation of species and communities*, Chicago: University of Chicago Press 1991.

The National Academies: *Disaster Resilience. A National Imperative*, Washington, D.C. 2012.

The White House: *Presidential Policy Directive/PPD-21*, Subject: Critical Infrastructure Security and Resilience, 2013, URL: <https://www.fas.org/irp/offdocs/ppd/ppd-21.pdf> [Stand: 31.07.2013].

Thoma, K. (Hrsg.): *Resilien-Tech – Resilience-by-design: Strategie für die technologischen Zukunftsthemen* (acatech STUDIE), München: Utz Verlag 2014.

> BISHER SIND IN DER REIHE acatech POSITION UND IHRER VORGÄNGERIN acatech BEZIEHT POSITION FOLGENDE BÄNDE ERSCHIENEN:

acatech (Hrsg.): *Future Business Clouds. Cloud Computing am Standort Deutschland zwischen Anforderungen, nationalen Aktivitäten und internationalem Wettbewerb* (acatech POSITION), München: Herbert Utz Verlag 2014.

acatech (Hrsg.): *Privatheit im Internet. Chancen wahrnehmen, Risiken einschätzen, Vertrauen gestalten* (acatech POSITION), Heidelberg u. a.: Springer Verlag 2013.

acatech (Hrsg.): *Geoessource Boden – Wirtschaftsfaktor und Ökosystemdienstleister. Empfehlungen für eine Bündelung der wissenschaftlichen Kompetenz im Boden- und Landmanagement* (acatech POSITION), Heidelberg u. a.: Springer Verlag 2012.

acatech (Hrsg.): *Perspektiven der Biotechnologie-Kommunikation. Kontroversen – Randbedingungen – Formate* (acatech POSITION), Heidelberg u. a.: Springer Verlag 2012. Auch in Englisch erhältlich (als pdf) über: www.acatech.de

acatech (Hrsg.): *Faszination Konstruktion – Berufsbild und Tätigkeitsfeld im Wandel. Empfehlungen zur Ausbildung qualifizierter Fachkräfte in Deutschland* (acatech POSITION), Heidelberg u. a.: Springer Verlag 2012.

acatech (Hrsg.): *Anpassungsstrategien in der Klimapolitik* (acatech POSITION), Heidelberg u. a.: Springer Verlag 2012.

acatech (Hrsg.): *Die Energiewende finanzierbar gestalten. Effiziente Ordnungspolitik für das Energiesystem der Zukunft* (acatech POSITION), Heidelberg u. a.: Springer Verlag 2012. Auch in Englisch erhältlich (als pdf) über: www.acatech.de

acatech (Hrsg.): *Menschen und Güter bewegen. Integrative Entwicklung von Mobilität und Logistik für mehr Lebensqualität und Wohlstand* (acatech POSITION), Heidelberg u. a.: Springer Verlag 2012.

acatech (Hrsg.): *Biotechnologische Energieumwandlung in Deutschland. Stand, Kontext, Perspektiven* (acatech POSITION), Heidelberg u. a.: Springer Verlag 2012.

acatech (Hrsg.): *Mehr Innovationen für Deutschland. Wie Inkubatoren akademische Hightech-Ausgründungen besser fördern können* (acatech POSITION), Heidelberg u. a.: Springer Verlag 2012. Auch in Englisch erhältlich (als pdf) über: www.acatech.de

acatech (Hrsg.): *Geoessource Wasser – Herausforderung Globaler Wandel. Ansätze und Voraussetzungen für eine integrierte Wasserressourcenbewirtschaftung in Deutschland* (acatech POSITION), Heidelberg u. a.: Springer Verlag 2012. Auch in Englisch erhältlich (als pdf) über: www.acatech.de

acatech (Hrsg.): *Future Energy Grid. Informations- und Kommunikationstechnologien für den Weg in ein nachhaltiges und wirtschaftliches Energiesystem* (acatech POSITION), Heidelberg u. a.: Springer Verlag 2012. Auch in Englisch erhältlich (als pdf) über: www.acatech.de

acatech (Hrsg.): *Cyber-Physical Systems. Innovationsmotor für Mobilität, Gesundheit, Energie und Produktion* (acatech POSITION), Heidelberg u. a.: Springer Verlag 2011. Auch in Englisch erhältlich (als pdf) über: www.acatech.de

acatech (Hrsg.): *Den Ausstieg aus der Kernkraft sicher gestalten. Warum Deutschland kerntechnische Kompetenz für Rückbau, Reaktorsicherheit, Endlagerung und Strahlenschutz braucht* (acatech POSITION), Heidelberg u. a.: Springer Verlag 2011. Auch in Englisch erhältlich (als pdf) über: www.acatech.de

acatech (Hrsg.): *Smart Cities. Deutsche Hochtechnologie für die Stadt der Zukunft* (acatech BEZIEHT POSITION, Nr. 10), Heidelberg u. a.: Springer Verlag 2011. Auch in Englisch erhältlich (als pdf) über: www.acatech.de

acatech (Hrsg.): *Akzeptanz von Technik und Infrastrukturen* (acatech BEZIEHT POSITION, Nr. 9), Heidelberg u. a.: Springer Verlag 2011.

acatech (Hrsg.): *Nanoelektronik als künftige Schlüsseltechnologie der IKT in Deutschland* (acatech BEZIEHT POSITION, Nr. 8), Heidelberg u. a.: Springer Verlag 2011.

acatech (Hrsg.): *Leitlinien für eine deutsche Raumfahrtspolitik* (acatech BEZIEHT POSITION, Nr. 7), Heidelberg u. a.: Springer Verlag 2011.

acatech (Hrsg.): *Wie Deutschland zum Leitanbieter für Elektromobilität werden kann* (acatech BEZIEHT POSITION, Nr. 6), Heidelberg u. a.: Springer Verlag 2010.

acatech (Hrsg.): *Intelligente Objekte – klein, vernetzt, sensitiv* (acatech BEZIEHT POSITION, Nr. 5), Heidelberg u. a.: Springer Verlag 2009.

acatech (Hrsg.): *Strategie zur Förderung des Nachwuchses in Technik und Naturwissenschaft. Handlungsempfehlungen für die Gegenwart, Forschungsbedarf für die Zukunft* (acatech BEZIEHT POSITION, Nr. 4), Heidelberg u. a.: Springer Verlag 2009. Auch in Englisch erhältlich (als pdf) über: www.acatech.de

acatech (Hrsg.): *Materialwissenschaft und Werkstofftechnik in Deutschland. Empfehlungen zu Profilbildung, Forschung und Lehre* (acatech BEZIEHT POSITION, Nr. 3), Stuttgart: Fraunhofer IRB Verlag 2008. Auch in Englisch erhältlich (als pdf) über: www.acatech.de

acatech (Hrsg.): *Innovationskraft der Gesundheitstechnologien. Empfehlungen zur nachhaltigen Förderung von Innovationen in der Medizintechnik* (acatech BEZIEHT POSITION, Nr. 2), Stuttgart: Fraunhofer IRB Verlag 2007.

acatech (Hrsg.): *RFID wird erwachsen. Deutschland sollte die Potenziale der elektronischen Identifikation nutzen* (acatech BEZIEHT POSITION, Nr. 1), Stuttgart: Fraunhofer IRB Verlag 2006.

> acatech – DEUTSCHE AKADEMIE DER TECHNIKWISSENSCHAFTEN

acatech vertritt die deutschen Technikwissenschaften im In- und Ausland in selbstbestimmter, unabhängiger und gemeinwohlorientierter Weise. Als Arbeitsakademie berät acatech Politik und Gesellschaft in technikwissenschaftlichen und technologiepolitischen Zukunftsfragen. Darüber hinaus hat es sich acatech zum Ziel gesetzt, den Wissenstransfer zwischen Wissenschaft und Wirtschaft zu unterstützen und den technikwissenschaftlichen Nachwuchs zu fördern. Zu den Mitgliedern der Akademie zählen herausragende Wissenschaftler aus Hochschulen, Forschungseinrichtungen und Unternehmen. acatech finanziert sich durch eine institutionelle Förderung von Bund und Ländern sowie durch Spenden und projektbezogene Drittmittel. Um den Diskurs über technischen Fortschritt in Deutschland zu fördern und das Potenzial zukunftsweisender Technologien für Wirtschaft und Gesellschaft darzustellen, veranstaltet acatech Symposien, Foren, Podiumsdiskussionen und Workshops. Mit Studien, Empfehlungen und Stellungnahmen wendet sich acatech an die Öffentlichkeit. acatech besteht aus drei Organen: Die Mitglieder der Akademie sind in der Mitgliederversammlung organisiert; das Präsidium, das von den Mitgliedern und Senatoren der Akademie bestimmt wird, lenkt die Arbeit; ein Senat mit namhaften Persönlichkeiten vor allem aus der Industrie, aus der Wissenschaft und aus der Politik berät acatech in Fragen der strategischen Ausrichtung und sorgt für den Austausch mit der Wirtschaft und anderen Wissenschaftsorganisationen in Deutschland. Die Geschäftsstelle von acatech befindet sich in München; zudem ist acatech mit einem Hauptstadtbüro in Berlin und einem Büro in Brüssel vertreten.

Weitere Informationen unter www.acatech.de