Dr. André Hahn MdB
Michael Kuffer MdB
Dr. Irene Mihalic MdB
Susanne Mittag MdB
Benjamin Strasser MdB

GRÜNBUCH 2020

zur Öffentlichen Sicherheit

INHALT

MITWIRKENDE

Herausgeberinnen und Herausgeber

Dr. André Hahn MdB

Michael Kuffer MdB

Dr. Irene Mihalic MdB

Susanne Mittag MdB

Benjamin Strasser MdB

Autorinnen und Autoren

Michael Bartsch,
Deutor Cyber Security Solutions GmbH

Marie-Luise Beck,
Deutsches Klima-Konsortium e. V.

Uwe G. Becking

Markus Bensmann,
Malteser Hilfsdienst e. V.

Stephan Boy
Berlin Energie

Albrecht Broemme

Dr. Clemens Gause,
Verband für Sicherheitstechnik e. V.

Dr. Wolfram Geier,
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

Prof. Dr. Lars Gerhold,
Freie Universität Berlin

Dr. Dietmar Gollnick,
e*Message W.I.S. Deutschland GmbH

Christoph Hampe,
Bosch Sicherheitssysteme GmbH

Wolfgang Kast,
Deutsches Rotes Kreuz e. V.

Uwe Kirsche,
Deutscher Wetterdienst

Wolfgang Lohmann,
Inspekteur BPdL im BMI a. D.

Roman Peperhove,
Freie Universität Berlin

Dr. Sigurd Peters

Prof. Dr. Peer Rechenbach

Prof. Dr. Jochen Schiller,
Freie Universität Berlin

Prof. Dr. Birgitta Sticher,
Hochschule für Wirtschaft und Recht Berlin

Jürgen Storbeck,
Direktor Europol a. D.

Prof. Dr. Ingo J. Timm,
Universität Trier

Stefan Truthän,
hhpberlin Ingenieure für Brandschutz GmbH

Expertinnen und Experten

die in Workshops und Arbeitsgruppen, mit redaktionellen Hinweisen und Ausarbeitungen sowie durch fachlichen Rat oder Erfahrungswissen das Entstehen dieser GRÜNBUCH-Ausgabe unterstützt haben:

Laila Abdallah,
Büro Susanne Mittag MdB

Lisa Acker,
ASW Bundesverband

Michael Barth,
genua GmbH

Oberst i. G. Frank Baumgard,
Bundesministerium der Verteidigung

Dr. Andreas Becker,
Deutscher Wetterdienst

Prof. Dr. Thomas Berger,
Universität Hohenheim

Maximilian Bornefeld-Ettmann

Axel Dechamps,
Deutsches Komitee Katastrophenvorsorge

Dr. Christian Endreß,
ASW Bundesverband

Cornelius v. Fürstenberg

Prof. Dr. Frank Gillert,
Technische Hochschule Wildau

Kevin Grigorian,
Johanniter-Unfall-Hilfe e. V.

Sabine ten Hagen-Knauer,
Bundesministerium für
Bildung und Forschung

Christian Diego Hanke

Anne Haufschulz,
Bundesdruckerei GmbH

David Imberman,
Axel Springer SE

Frank Jörres,
Deutsches Rotes Kreuz e. V.

Elisabeth Kaiser MdB

Sebastian Kollberg,
Büro Konstantin Kuhle MdB

Katrin Klüber,
Technisches Hilfswerk

Christian Köhler

Holger Kraft,
Kommando Territoriale
Aufgaben der Bundeswehr

Konstantin Kuhle MdB

Ina Lengert,
Esri Deutschland GmbH

Dr. Andreas Meissner,
Fraunhofer IOSB

Sara Merkes,
Freie Universität Berlin

Ingo Michels,
Esri Deutschland GmbH

Ramon Mörl,
itWatch GmbH

Dr. Hans-Guido Mücke,
Umweltbundesamt

Daniel Müller,
secunet Security Networks AG

Ortwin Neuschwander,
TURMsolutions GmbH

Dr. Harald Olschok,
Bundesverband der
Sicherheitswirtschaft

Dr. Stefan Poloczek,
Berliner Feuerwehr

Dr. Norbert Reez
Bundespolizei

Dr. Johannes Richert,
Deutsches Rotes Kreuz e. V.

Sebastian Riedl,
Büro Michael Kuffer MdB

Thomas P. Schäfer,
secunet Security Networks AG

Marc Schlingheider,
IBM Deutschland GmbH

Prof. Dr. Peter Schmiedtchen,
Dräger Safety AG & Co. KGaA

Prof. Dr. Christoph Schneider,
Humboldt-Universität
zu Berlin

Johannes Schneider,
Büro Dr. Irene Mihalic MdB

Adrian Schwantes,
Bundesverband der
Deutschen Sicherheits- und
Verteidigungsindustrie e. V.

Kim Seele

Christine Skropke,
secunet Security Networks AG

Christoph Stapelfeldt,
Büro Benjamin Strasser MdB

Dr. Berthold Stoppelkamp,
Bundesverband der
Sicherheitswirtschaft

Oliver Stuchel,
T-Systems International GmbH

Dr. Tim Stuchtey

Dr. Claudia Thamm,
Bundesdruckerei GmbH

Devrim Tuncel,
Büro Dr. André Hahn MdB

Thomas Urban,
VdS Schadenverhütung GmbH

Prof. Dr. Martin Voss,
Freie Universität Berlin

Frank Weber,
Malteser Hilfsdienst e. V.

Dr. Uwe H. Wehrstedt,
EMW Exhibition & Media
Wehrstedt GmbH

Hartfrid Wolff
KPMG Law

Prof. Dr. Volker Wulfmeyer,
Universität Hohenheim

Hartmut Ziebs

Wir danken für die freundliche Unterstützung

hhpberlin Ingenieure für
Brandschutz GmbH

Malteser Hilfsdienst e. V.

Bosch Sicherheitssysteme
GmbH

IBM Deutschland GmbH

Freie Universität Berlin

Technisches Hilfswerk

Deutscher Bundestag

1 GRÜNBUCH 2020
Einleitung

1.1 Was ist das ZOES?

Das Zukunftsforum Öffentliche Sicherheit e. V. (ZOES) ist die Denkfabrik zur Gestaltung der zukünftigen Entwicklungen der Öffentlichen Sicherheit in Deutschland. Das ZOES vernetzt Abgeordnete des Deutschen Bundestages mit Expertinnen und Experten aus Ministerien und Bundesbehörden, aus der Wissenschaft, Hilfsorganisationen, Verbänden und der Wirtschaft. Das ZOES fördert den parteiübergreifenden Diskurs über Rollen, über Verantwortung und über Ziele der Gesellschaft, des Staates und der Wirtschaft in der Öffentlichen Sicherheit. Eckwerte sind Rechtsstaatlichkeit und demokratische Verfasstheit.

Das ZOES wird von einem Beirat mit Vertreterinnen und Vertretern der parlamentarischen Fraktionen, des Bundesministeriums des Innern, für Bau und Heimat, des Bundesministeriums für Bildung und Forschung sowie des Forschungsforums Öffentliche Sicherheit begleitet.

Das ZOES organisiert in Räumen des Deutschen Bundestages Fachveranstaltungen mit dem Ziel, Szenarien zu beleuchten, Thesen zu erarbeiten, Leitfragen zu formulieren und Lösungsansätze zu entwickeln. Schwerpunkte sind Resilienz[1] und Kritische Infrastrukturen (KRITIS) in Kommunen, Kreisen, Ländern sowie beim Bund.

1.2 Wie sieht das ZOES die Öffentliche Sicherheit?

Die Öffentliche Sicherheit wird im Allgemeinen definiert als Unversehrtheit der Rechtsordnung, der subjektiven Rechte und Rechtsgüter des Einzelnen sowie staatlicher Institutionen oder sonstiger Träger der Hoheitsgewalt. Das ZOES sieht die Öffentliche Sicherheit allerdings weiter gefasst:

- Öffentliche Sicherheit umfasst die private Umgebung, die Arbeits- und die Freizeitwelt sowie den öffentlichen Raum einschließlich der virtuellen Welt.
- Von besonderer Bedeutung ist das Sicherheitsgefühl der Menschen: Sie erwarten, generell angstfrei leben zu können. Mängel der Öffentlichen Sicherheit sowie Sorgen rund um die berufliche, ökonomische, gesellschaftliche oder politische Zukunft führen zu subjektiver Unsicherheit und damit mittel- bis langfristig zur Erosion von Staat und Gesellschaft.
- Zentrale Voraussetzung für das Grundvertrauen der Menschen in Staat und Politik sind demokratische Legitimation der verantwortlichen Akteurinnen und Akteure, die rechtsstaatlichen Prinzipien verpflichtet sind, sowie vorausschauendes und konsequentes staatliches Handeln. Mangelnde Teilhabechancen, Intransparenz, Rechtsmissbrauch und das Aushöhlen von Staatlichkeit durch Organisationen oder Einzelne untergraben das Vertrauen.
- Freiheit, Rechtsstaat und Öffentliche Sicherheit sind Grundlagen der Demokratie. Öffentliche Sicherheit berücksichtigt neben Belangen von Bürgerinnen und Bürgern auch schützenswerte Positionen von Unternehmen. Die Resilienz staatlicher Institutionen wie auch privater Organisationen sind wichtige Anliegen der Öffentlichen Sicherheit.
- Deutschland ist Bestandteil eines europäischen beziehungsweise internationalen Systems, weshalb unsere Vorkehrungen mit anderen Standards kompatibel sein müssen.

1.3 Welche Ziele verfolgt das ZOES?

Vorrangiges Ziel des ZOES ist es, Zukunftsfragen in Bezug auf die Öffentliche Sicherheit vertrauensvoll und interdisziplinär zu diskutieren, um daraus Antworten für politische Entscheiderinnen und Entscheider zu entwickeln. Hierzu werden Trends und Veränderungsprozesse beobachtet, analysiert und begleitet. Um die Widerstandsfähigkeit von Gesellschaft, Staat und Wirtschaft zu steigern, werden Debatten über Chancen und Risiken von technischen und sozialen Innovationen initiiert.

1 Widerstandsfähigkeit gegen Beeinträchtigungen, die sich aus Prävention, Schadensabwehr und Wiederherstellung ergibt

1.4 Was sind die Ziele der Publikation GRÜNBUCH 2020?

Das GRÜNBUCH 2020 zeigt anhand ausgewählter Szenarien Maßnahmen zur Stärkung der Öffentlichen Sicherheit auf. Die daraus abgeleiteten Handlungsempfehlungen sollen Entscheidungsträgerinnen und Entscheidungsträgern aus Politik, Verwaltung und der Wirtschaft Lösungsansätze unter Beachtung der vernetzten Abhängigkeiten bieten. Ansprüche der Publikation GRÜNBUCH 2020 sind ein offener Diskurs sowie ein angemessenes Verhältnis von Prävention, Aktion und Reaktion. Das GRÜNBUCH 2020 soll die Leserinnen und Leser anregen, sich mit diesen zusammenhängenden Themen zu beschäftigen.

1.5 Welche Szenarien behandelt das GRÜNBUCH 2020?

Aus den Reihen des ZOES wurden 2018 in einem strukturierten Prozess drei Szenarien ausgewählt, die durch ihre Komplexität und Aktualität eine hohe Bedeutung für die Öffentliche Sicherheit haben. Dies sind:

- Klimawandel und Wetterextreme
- Eskalierende Infektionskrankheiten (Epidemien, Pandemien)
- Digitaler Raum und Organisierte Kriminalität (OK)

Klimawandel und Wetterextreme

Am Beispiel eines mehrjährigen Dürre-Szenarios werden die relevanten Folgen für die Öffentliche Sicherheit anschaulich dargestellt. Die massiven Auswirkungen des Klimawandels auf das Privatleben, die Gesellschaft, die Wirtschaft und den Staat bis hin zu gesellschaftlichen und politischen Veränderungen werden skizziert.

Welche Schlüsse müssen für die Öffentliche Sicherheit einschließlich Daseinsvorsorge und Sicherung der Infrastruktur gezogen werden?

Fazit: Infolge des Klimawandels steigen die Temperaturen überall auf der Welt. Folgen sind steigende Meeresspiegel sowie häufigere Hitzewellen, Dürreperioden und andere Wetterextreme. Daher müssen sowohl die Treibhausgas-Emissionen in den kommenden Jahrzehnten beendet (Klimaschutz) als auch die Klimawandel-Risiken bewältigt werden (Klimawandel-Anpassung).

Auch in Deutschland wird es ganzjährig mehr extreme Wetterereignisse geben. Diese führen zur quantitativen und qualitativen Steigerung der Anforderungen an den Bevölkerungsschutz und somit zu mehr Belastungen für die Einsatzkräfte, die Ausstattung und die Infrastruktur. Durch kaskadierende Effekte steigen die Aufwendungen zum Schutz von Gesellschaft, Daseinsvorsorge und Kritischen Infrastrukturen.

Diese Veränderungen müssen in Planungen und Strategien einbezogen, Akteure der Öffentlichen Sicherheit sensibilisiert sowie Präventionsmaßnahmen und adäquate Zusammenarbeit von Bund, Ländern und Kommunen neu bewertet werden.

Interdisziplinäre Forschung, weitergehende Analysen sowie die konsequente Umsetzung des internationalen Abkommens Sendai Framework[2] sind essenziell.

2 Das „Sendai Framework for Disaster Risk Reduction 2015-2030" der Vereinten Nationen beschreibt Ziele und Prioritäten zur Verringerung menschengemachter und naturbedingter Katastrophen. https://www.bbk.bund.de/DE/AufgabenundAusstattung/NationaleKontaktstelleSendai/NationaleKontaktstelleSendai_node.html

Eskalierende Infektionskrankheiten (Epidemien, Pandemien)

Globalisierung und Mobilität erhöhen die Risiken der Mensch-zu-Mensch-Übertragung sowie der Übertragung durch Nahrung oder Krankheitserreger. Somit steigt die Gefahr der schwer kontrollierbaren Verbreitung gefährlicher Infektionskrankheiten. Auch kann Bio-Terror infektiöse, eskalierende Krankheiten auslösen.

Welche Strategien muss die Öffentliche Sicherheit entwickeln? Was ist bei der Krisenkommunikation zu beachten? Wie muss auf Versorgungslücken bei Behandlungskapazitäten und Logistikketten reagiert werden? Welche Vorsorgelücken bestehen hinsichtlich der Hygiene? Wie können diese präventiv, aktiv und reaktiv geschlossen werden?

Fazit: Epidemien und Pandemien haben Auswirkungen auf die Gesundheit großer Personengruppen und somit auch auf die Öffentliche Sicherheit. Globalisierung und „Just-in-time-Logistik“[3] bergen Risiken für Lieferketten und den Betrieb Kritischer Infrastrukturen (KRITIS).

Um negative Auswirkungen zu mildern, sind in allen Sektoren gute Planungen und angemessene Reserven unter Einbeziehung intelligenter Informationsmanagement- und Prognose-Konzepte erforderlich. Dazu sind eine übergreifende Strategie und die Fortschreibung der Pandemieplanungen zwingend erforderlich. Die optimierte Verfügbarkeit von Mangelressourcen ist ein wesentlicher Schlüssel der Vorsorge.

Systemrelevante Akteure müssen einbezogen und gegebenenfalls gestärkt werden. Eine zentrale Rolle kommt dem Öffentlichen Gesundheitsdienst (ÖGD) zu.

Digitaler Raum und Organisierte Kriminalität

Digitalisierung und Innovation ermöglichen globale Kommunikation für und mit jedermann. Neue Technologien und Methoden schaffen einen wachsenden virtuellen Lebens- und Wirtschaftsraum. Dies erfordert ein adäquat vernetztes Sicherheitsdenken sowie zeitgemäße Anstrengungen für Prävention und schnelle Reaktionsfähigkeit.

Was sind Zukunftstrends der Digitalisierung im Hinblick auf die Öffentliche Sicherheit? Welche Veränderungen sind bei der Sicherheitsarchitektur in Deutschland in Bezug auf Cybersicherheit erforderlich? Welche Konsequenzen werden aus dem rasanten Anstieg von Cyberattacken mit Gefahren für KRITIS gezogen? Welche Konsequenzen erfordern die neuen Risiken für Demokratie, staatliches Funktionieren, Wirtschaft und Handel sowie die Bevölkerung?

Welche Konsequenzen erfordern der Anstieg von Straftaten im Internet und inhaltliche Veränderungen wie Cryptojacking[4] und illegaler Handel im Darknet? Wie können kriminelle Manipulationen erkannt und sich selbst verstärkende Effekte in der vernetzten Welt verhindert werden? Wie kann der transnationalen Vernetzung des Verbrechens und den nur mit viel Aufwand angreifbaren kriminellen „Geschäftsmodellen“ begegnet werden?

Fazit: Internet, Digitalisierung und die zunehmende Anwendung Künstlicher Intelligenz bergen einerseits neuartige Risiken und Gefährdungen, bieten andererseits außergewöhnliche Möglichkeiten zur Aufrechterhaltung und Verbesserung der Öffentlichen Sicherheit. Um dieses Verbesserungspotenzial auszuschöpfen, müssen Forschung, technische Ausstattung, Aus- und Fortbildung sowie das Risikobewusstsein optimiert werden.

3 Logistik KNOWHOW, 2019: „Just-in-time“ bezeichnet eine Lieferart, bei der die benötigte Ware zeit- und mengengenau geliefert wird, um die Lagerhaltung am Verarbeitungsort so gering wie möglich zu halten. https://logistikknowhow.com/materialfluss-und-transport/beschaffungslogistik-just-in-time/

4 BKA, Sicherheit in einer offenen und digitalen Gesellschaft, 2018: Unter dem Begriff „Cryptojacking“ versteht man die unautorisierte Nutzung eines fremden Computers zum „Schürfen“ von Kryptowährungen wie Bitcoin.

Rechtliche Veränderungen müssen in Politik und Gesellschaft diskutiert und zeitnah umgesetzt werden.

Um Cyber- und Kriminalitätsangriffe abzuwehren beziehungsweise deren Auswirkungen zu reduzieren, müssen öffentliche und private Maßnahmen besser vernetzt und relevante Systeme gehärtet werden. Dies betrifft Hardware, Software und Prozesse. Eine praxisgerechte, nationale Forschung muss wichtige Impulse setzen.

Eine nationale Cybersicherheitsstrategie mit enger Verknüpfung zu europäischen und zu internationalen Anstrengungen und Cybersicherheitssystemen ist zwingend erforderlich.

Ziel ist eine resiliente Sicherheitsarchitektur mit Standards und reaktionsschnellem Risikobewusstsein.

1.6 GRÜNBUCH 2020 – Fazit

Die dargestellten Szenarien zeigen die Komplexität der Aufgabenstellungen, die unmittelbar bewältigt werden müssen. Dies erfordert vorausschauende und undogmatische Planungen sowie konsequentes Handeln.

- Die fachliche Bearbeitung von komplexen Aufgaben erfordert interdisziplinär zusammengesetzte Teams von Expertinnen und Experten. Risiken, Abhängigkeiten und Nebenwirkungen müssen bedacht werden.
- Grundlage der fachlichen Bearbeitung ist eine gründliche, praxisnahe Forschung in allen Bereichen der Öffentlichen Sicherheit.
- Entscheidungen müssen fachlich vorbereitet, politisch durchgesetzt und praktisch umgesetzt werden.
- Beschlossene Maßnahmen müssen synchron und glaubwürdig kommuniziert werden, insbesondere wenn ihre Umsetzung konfliktträchtig und beschwerlich ist.
- Laufende Prozesse müssen kontinuierlich überprüft und bei veränderten Erkenntnissen nachjustiert werden.
- Viele Wirkungen werden erst mittel- oder langfristig erkennbar sein.

Am GRÜNBUCH 2020 haben dankenswerterweise mehr als 60 Mitglieder des ZOES sowie hinzugezogene Expertinnen und Experten mit großem Engagement mitgewirkt. Somit fasst das GRÜNBUCH 2020 persönliche Erfahrungen, Einschätzungen aus der Fachliteratur und unterschiedliche Überlegungen zusammen; es ist offen für abweichende Meinungen.

Die parlamentarischen Beirätinnen und Beiräte des ZOES als Herausgeberschaft der Publikation GRÜNBUCH 2020 wünschen diesen Beiträgen eine gute Verbreitung und konkrete Umsetzungen.

2 Klimawandel und Wetterextreme: Herausforderung für die Öffentliche Sicherheit

2.1 Schwerpunkt Hitze und Dürre – eine Einführung

Durch den Klimawandel sind langanhaltende Dürreperioden wahrscheinlicher geworden. Die fortschreitende Erderwärmung aufgrund des kontinuierlichen Anstiegs menschengemachter Treibhausgase in der Atmosphäre führt auch zu Änderungen der meteorologischen Extremsituationen.[5] Der „Bericht zur Risikoanalyse im Bevölkerungsschutz 2018“ beschreibt eine sechsjährige Dürre in Deutschland als Szenario. Die Analyse stellt fest, dass die Wirklichkeit das Szenario teilweise schon überholt hat: „Die realen Erfahrungen des Jahres 2018 bestätigen, dass eine Dürre ein durchaus realistisches Szenario für Deutschland ist.“ Im Gegensatz zu Stürmen oder Hochwasserereignissen aber fehlten Erfahrungen mit einer Dürre; die Vorbereitung auf solche Ereignisse sei geboten.[6]

In Deutschland ist die Temperatur seit 1881 im Mittel um 1,5 °C gestiegen[7]. Auch intensive Hitzeperioden haben „sowohl in der Häufigkeit wie auch in der Intensität in ganz Deutschland seit 1951 zugenommen“. Und: „Seit 1951 hat die Anzahl der heißen Tage mit einer Höchsttemperatur von mindestens 30 °C im Flächenmittel von Deutschland von im Mittel etwa drei Tagen pro Jahr auf derzeit im Mittel etwa zehn Tage pro Jahr zugenommen. Mehr als zehn heiße Tage gab es deutschlandweit vor 1994 noch nie.“[8]

Die Klimaforschung kann mittels der Attribution Science[9] zeigen, dass inzwischen jede Hitzewelle in Europa aufgrund des vom Menschen induzierten Klimawandels wahrscheinlicher und intensiver geworden ist. Grund ist der mit der globalen Erwärmung einhergehende Anstieg der potenziellen Verdunstung. Ohne geeignete Gegenmaßnahmen vor Ort steigt damit die Wahrscheinlichkeit sich jährlich wiederholender Dürren.[10]

Aus Sicht des Zukunftsforums Öffentliche Sicherheit sind die Risiken für die Sicherheit, die mit dem Klimawandel und seinen Folgen verbunden sind, in Politik und Öffentlichkeit noch nicht hinreichend bekannt. Die Herausforderung, den Klimawandel zu bewältigen, bedeutet, sich an die Folgen der nicht mehr vermeidbaren Klimaveränderungen systematisch anzupassen (Adaption) und gleichzeitig durch Emissionsreduktionen die globale Erwärmung auf ein weniger gefährliches Maß zu begrenzen (Mitigation). Die Ausführungen konzentrieren sich auf die Möglichkeiten der Adaption an die zu erwartenden Folgen des Klimawandels. Allerdings sind im Interesse des Bevölkerungsschutzes auch die Anstrengungen zur Mitigation von zentraler Bedeutung. Der 1,5-Grad-Bericht des Weltklimarates IPCC zeigt, dass Umfang und Kosten von Adaptionsmaßnahmen in einer 1,5-Grad-Welt deutlich niedriger ausfallen als in einer 2-Grad-Welt. Das gilt noch mehr für 3 Grad oder 4 Grad Celsius globale Erwärmung bis Ende des Jahrhunderts – dem Pfad, auf dem sich die Menschheit derzeit befindet.[11]

5 Dürren hat es schon immer gegeben; deshalb ist der Nachweis eines Zusammenhangs mit dem menschengemachten Klimawandel nicht einfach. Durch einen neuen Zweig der Klimaforschung, die sogenannte Attribution Science (Attributions- beziehungsweise Zuordnungswissenschaft) versucht die Wissenschaft diesen Zusammenhang zu erforschen und darzustellen. Beispiel: Das Hitzeextrem im Juli 2019 in Europa: https://www.worldweatherattribution.org/human-contribution-to-the-record-breaking-july-2019-heat-wave-in-western-europe/. Auch für den Hitzesommer 2018 zeigte sich, dass die Hitze größer war, als sie ohne Klimawandel gewesen wäre und die Dürre trockener; siehe hierzu auch: Interview mit der Attributionsforscherin Friederike Otto: https://www.klimareporter.de/erdsystem/ein-jahrhundert-sommer-alle-paar-jahre

6 Bundestags-Drucksache 19/9521, Seite 2

7 DWD, 2019, https://www.dwd.de/DE/presse/pressemitteilungen/DE/2019/20190326_pressemitteilung_klima_pk_news.html

8 Siehe Seiten 22 und 23, in: Monitoringbericht 2019 zur Deutschen Anpassungsstrategie an den Klimawandel – Bericht der Interministeriellen Arbeitsgruppe Anpassungsstrategie der Bundesregierung, Umweltbundesamt (Hrsg.), https://www.umweltbundesamt.de/sites/default/files/medien/1410/publikationen/das_monitoringbericht_2019_barrierefrei.pdf

9 Attribution Science: Attributions- beziehungsweise Zuordnungswissenschaft versucht zu quantifizieren, wie viel Klimawandel in einzelnen Wetterereignissen steckt. Siehe auch Fußnote 5

10 Eine Arbeit, die die Wahrscheinlichkeit von Dürren sowie deren Intensität und Dauer abschätzt, ist: Samaniego et al. Nature Climate Change 2018, https://www.nature.com/articles/s41558-018-0138-5 Die Autoren schätzen ab, dass sich bei einer globalen Erwärmung von 2 Grad Celsius die Häufigkeit des Auftretens und die Dauer von Dürren verdoppeln. Auch die betroffenen Flächen werden dementsprechend größer.

11 Siehe zum Beispiel Future of the human climate niche, PNAS, 2020, https://www.pnas.org/content/early/2020/04/28/1910114117 Der Fachartikel berechnet, dass in 2070 rund 3,5 Milliarden Menschen in extrem heißen Regionen werden leben müssen, die man heute nur aus der Sahara kennt. Diese Regionen mit einer jährlichen Durchschnittstemperatur von ≥ 29.0 Grad werden dann 19 Prozent der globalen Landoberfläche bedecken; heute sind es nur 0,8 Prozent.

Wissenschaftlich fundierte Zahlen und Statistiken beschreiben den Klimawandel und seine Folgen sehr detailliert; aber es ist nicht immer leicht, sich den konkreten Alltag im Klimawandel vorzustellen. Deshalb beschreiben wir genau das: Wie können wir uns eine Situation mit extremer Hitze und Dürre konkret vorstellen?

2.2 Leseanleitung für das Szenario

Die Auswirkungen einer mehrjährigen Dürre in Deutschland sind komplex und können daher sehr unterschiedlich dargestellt werden. Die Darstellung möglicher „Zukünfte“ in Form von Szenarien ist eine Möglichkeit, die Komplexität zu bewältigen und das Problem zu veranschaulichen. Das folgende Szenario ist nicht als Prognose im engeren Sinne zu verstehen, sondern als mögliche, plausible Beschreibung aus Sicht einer fiktiven Familie. Die im Szenario dargestellten Ereignisse beruhen auf der in der Wissenschaft etablierten Erkenntnis, dass es in Folge des Klimawandels zu einer Zunahme an Hitze- und Dürreperioden kommen wird und hierdurch sowohl Infrastrukturen als auch das gesellschaftliche Leben zunehmend beeinträchtigt werden.

Die folgende Geschichte ist angelehnt an das oben in der Risikoanalyse des Bundes beschriebene Dürreszenario. Erzählt wird aus der Perspektive der Familie Weber. Die Webers sind eine Durchschnittsfamilie. Sie wohnen in einer deutschen Großstadt und haben zwei Kinder. Wir schreiben das Jahr 2030 und befinden uns nach sechs Jahren Dürre[12] auf dem Höhepunkt einer Hitzewelle …

12 Eine gute Zusammenschau, was eine Dürre überhaupt ausmacht sowie aktuelle Informationen findet sich im „Dürremonitor Deutschland“, herausgegeben vom Helmholtz Zentrum für Umweltforschung. https://www.ufz.de/index.php?de=37937

2.3 Szenario

Die Stadt glüht in der Mittagshitze. Das Thermometer klettert auf 45 Grad Celsius – im Schatten. In diesem August 2030 deutet alles auf einen neuen Rekord hin.

Familie Weber hat sich in ihrer Dreieinhalbzimmerwohnung vor den beiden Ventilatoren versammelt, die die stickige Luft umrühren. Elena Weber notiert sich in Gedanken, dass sie sich für das kommende Jahr die Installation einer Klimaanlage nicht mehr vom Denkmalschutz wird untersagen lassen. Selbst die Außenverschattung, die jetzt etwas Erleichterung bringen würde, war abgelehnt worden! Lächerlich, sie, die Ingenieurin der Entwicklungsabteilung für Flugzeugturbinen, sitzt vor der Kühlungstechnik des vorletzten Jahrhunderts, und ihr ist schlecht vor Hitze. Der Denkmalschutz muss seine Grundsätze aus dem vergangenen Jahrhundert genauso überdenken wie … ja, wie eigentlich alles. Alles, was für uns normal ist, unser Alltag, unsere Routinen – das ist nicht ausgelegt für ein Leben mit 45 Grad Celsius, denkt Frau Weber. Aber würde eine Klimaanlage wirklich etwas nützen? Seit dem Stromausfall vorige Woche in Teilen Deutschlands mit vielen Hitzetoten dürfen Klimaanlagen aufgrund des hohen Stromverbrauchs vorerst nicht mehr eingeschaltet werden.

Die Nachrichten melden, dass ausgewählte U-Bahn-Stationen für Obdachlose offengehalten werden sollen. Wie das Trinkwasserproblem[13] gelöst wird, ist allerdings noch nicht klar. Leider wurden der geplante Ausbau der Trinkwassernotversorgung mit Notbrunnen und die Sanierung bestehender Notbrunnen in Deutschland aus finanziellen Gründen nicht realisiert. Zahlreiche vorhandene Notbrunnen sind versandet, kontaminiert und unbrauchbar geworden.

Die Kräfte der Feuerwehren, des Technischen Hilfswerks (THW) und der Hilfsorganisationen Arbeiter-Samariter-Bund, Deutsches Rotes Kreuz, Johanniter-Unfall-Hilfe und Malteser Hilfsdienst sind erschöpft. Die Trinkwassernotversorgung durch das THW ist über das ganze Land verteilt, aber es reicht nicht[14]. Für Einsatzkräfte wurde immerhin bereits vor Jahren neue Schutzkleidung für spezielle Lagen wie Hitzeperioden und Waldbrände entwickelt, die den Einsatz während solcher Extremlagen erleichtert. Auch die Arbeitsschutzvorschriften wurden inzwischen überarbeitet[15]. Trotzdem sind viele Ehrenamtliche zu Hause geblieben. Sie müssen sich um ihre Familien kümmern oder sind selbst von der Hitze belastet. Die sozialen Medien sind voll von Horrorgeschichten. Überall scheint Hilfe notwendig zu sein, aber kaum noch möglich.

Thomas Weber ist nervös. Seit dem Wochenende läuft hier alles aus dem Ruder. Eigentlich hatte die Familie einen Besuch bei seiner Mutter in einer thüringischen Kleinstadt geplant. Dort ist es kühler, die Kinder freuten sich auf eine frische Brise bei maximal 35 Grad und – und das war der entscheidende Punkt – auf eine Nacht bei etwa 20 Grad. Endlich richtig schlafen. Auch wenn der schöne Thüringer Wald nach fünf Jahren Trockenheit inzwischen eher grau aussieht und stark gelichtet ist[16] – immerhin ist dort die Temperatur erträglicher.

Die Wetteraussichten der vergangenen Tage bestätigten allerdings den Trend der weiteren Temperaturzunahme. Dann kam eine Hiobs-

13 Bei rechtzeitiger Vorsorge wäre auch folgendes Szenario möglich gewesen: Zum Glück wurde bereits zu Beginn der 2020er Jahre das Trinkwassernotversorgungsprogramm des Bundes durch den Haushaltsgesetzgeber bewilligt. Es sah vor, die ursprünglich 5.200 Notbrunnen bundesweit zu sanieren und die teils großen Bestandslücken durch neue Brunnen zu schließen. Darüber hinaus wurde das Notbrunnensystem ergänzt durch mobile Versorgungsmodule des THW, der Hilfsorganisationen und der Feuerwehren sowie neue Verbundleitungen zwischen besonders gefährdeten Versorgungsregionen. Siehe dazu auch unter Handlungsempfehlungen

14 Die Fachgruppen Trinkwasserversorgung des THW sind in der Lage 132.000 Menschen leitungsunabhängig mit 25 Litern pro Person und Tag zu versorgen. Leitungsgebunden sinkt diese Zahl auf rund 22.000 Menschen. In: Bundestags-Drucksache 19/9521, Seite 22

15 Es hätte schlimmer kommen können: Mit der heute üblichen Persönlichen Schutzausrüstung wären viele Einsatzkräfte von Kreislaufzusammenbrüchen und Hitzeerschöpfungen betroffen. Die Ausfälle hätten zusätzlich Lücken ins Personalkonzept gerissen. Siehe auch unter Handlungsempfehlungen

16 Vgl. „Ergebnisse der Waldzustandserhebung 2019“ (Bundesministerium für Ernährung und Landwirtschaft BMEL, 2020), wonach 2019 nur jede fünfte Baumkrone intakt war; bislang seien bereits 180 000 Hektar Wald abgestorben – das entspricht gut zwei Dritteln der Fläche des Saarlands.

botschaft nach der anderen: ein ausufernder Böschungsbrand auf der Autobahn. Vollsperrung. Nichts geht mehr. Außerdem sind viele Straßen aufgrund der Hitze beschädigt[17]. Überall entstanden lange Staus. Eine Notversorgung der gestrandeten Reisenden mit Wasser musste bereitgestellt werden. Die Evakuierung der Autobahn ging nur schleppend voran.

Alle Warn-Apps auf seinem Smartphone zeigten nur eine Farbe: Alarmstufe Rot. Es wird empfohlen, nur Reisen zu unternehmen, die dringend notwendig sind. Oder doch lieber die Bahn nehmen? Aber auch der Zugverkehr ist nur sehr eingeschränkt möglich, weil die Schienen durch die Hitze an vielen Stellen verformt sind.

Die Familie beschloss, nachts zu fahren. Um drei Uhr morgens war die Autobahn immer noch gesperrt, die App weiterhin auf Rot, der Brand noch nicht unter Kontrolle. Morgens um halb sechs dann der Anruf der Mutter: „Wir werden evakuiert!“ Ein zunächst kleiner Brandherd im nahegelegenen Wald hatte sich rasend schnell ausgebreitet. Die Löschteiche und Brunnen waren ausgetrocknet. Jetzt fraß sich die Feuerwalze Richtung Kleinstadt.

„Es wird alles gut! Es wird alles gut!“, rief Herr Weber noch ins Telefon – da war der Anruf auch schon weg. Netzüberlastung. Seither kein Lebenszeichen mehr von der Mutter. Ob es ihr gut geht?

Am nächsten Morgen fährt Herr Weber mit dem Fahrrad zur Arbeit. In manchen Straßen steht unerträglicher Gestank und erinnert daran, dass die Abwassersysteme nicht mehr richtig funktionieren. Als Leiter des Seniorenstifts muss er nach seinem Team und den Bewohnerinnen und Bewohnern schauen. Und überhaupt: Was soll er zu Hause? Bei der Familie liegen die Nerven blank. Kleinste Anlässe führen zu Streit. Zudem macht ihn dieses Nichtstun und Warten fertig.

Nur wenige Beschäftigte sind zur Arbeit erschienen. Die Mitarbeiterinnen und Mitarbeiter haben selbst mit den Hitzefolgen zu kämpfen oder Angehörige, die aufgrund der Hitze jetzt besondere Fürsorge brauchen. Manche sind an den öffentlichen Verkehrsmitteln gescheitert, die jetzt seltener fahren. Dabei werden alle Kräfte so dringend gebraucht. Viele Seniorinnen und Senioren leiden unter lebensbedrohlichen Kreislaufproblemen, vor allem, wenn sie mit Diabetes, Übergewicht oder Herz-Kreislauf-Erkrankungen belastet sind. Viele denken nicht an die notwendige Flüssigkeitszufuhr, weil sie wenig Durst empfinden. Bereits gestern ist eine Bewohnerin auf dem Weg zur Toilette kollabiert und gestorben. Durch die vielen Toten in der Stadt sind auch die Beerdigungsinstitute überlastet. Herr Weber stellt sich die Frage, ob er die Verstorbene zunächst einfach im Keller in einem Leichensack aufbewahren soll. Dann aber lässt sich der Keller nicht mehr als kühler Aufenthaltsraum für die übrigen Bewohnerinnen und Bewohner einrichten. Immerhin haben sie hier einen Hitzeaktionsplan, der die Abläufe sicherer macht. In vielen Krankenhäusern fehlen sie noch immer, von einem nationalen Hitzeaktionsplan ganz zu schweigen.

Das größte Problem ist jedoch die Trinkwasserversorgung. Einige Regionen in Deutschland leben inzwischen mit Ersatzwasserversorgung, die vor allem Krankenhäuser und Pflegeheime vor kaum lösbare Probleme stellt[18]. Was, wenn es hier auch so weit ist? Noch gibt es Mineralwasser für die alten Menschen. Aber wie lange werden die Vorräte noch reichen, wenn der Nachschub aufgrund von Lieferschwierigkeiten nicht mehr funktioniert? Viele Straßen sind wegen hitzebedingter Fahrbahnschäden nicht befahrbar. Was bedeutet das für die benötigten Lebensmittel? Dazu der Streit um zusätzliche Finanzmittel wegen der stark gestiegenen Lebensmittelpreise. Die Liste der ungelösten Probleme wird immer länger. Auch drückt Herrn Weber die Sorge um seine Mutter, von der er immer noch nichts ge-

17 Asphalt quillt auf; Schienen verbiegen sich; es wurde nicht genügend investiert, um die Verkehrswege an die Temperaturen des 21. Jahrhunderts anzupassen, siehe: https://www.unece.org/fileadmin/DAM/trans/doc/2020/wp5/ECE-TRANS-283e.pdf

18 Ersatzwasserversorgung: Wassertransporte (Tankwagen) oder geeignete leitungsunabhängige Brunnen, insbesondere Trinkwassernotbrunnen nach dem Wassersicherstellungsgesetz (WasSiG)

hört hat. Dass die Telefonnetze derzeit immer wieder aussetzen, findet er ansonsten eher entlastend, denn die besorgten Familienangehörigen der Heimbewohnerinnen und -bewohner haben in den zurückliegenden Tagen seine Zeit schon über alle Maßen beansprucht.

Dass die Menschen in der Großstadt auf wichtige Informationen durch die eingerichteten Sendai-Kontaktbüros[19] für Katastrophenvorsorge zurückgreifen können, entspannt die Lage beträchtlich. In den Büros erhält man rund um die Uhr praktische Tipps zum Selbstschutz und zur Selbsthilfe, entweder über den direkten persönlichen Kontakt, über Telefon, Internet oder über die lokale „Sendai-App". Die Büros bieten auch nützliche Informationen zur Anpassung und eine Best-Practice-Datenbank an, die für Kommunen, Unternehmen sowie Bürgerinnen und Bürger abrufbar sind, um sich auf extreme Lagen jeglicher Art lange im Voraus vorzubereiten[20].

Auch für die ambulante Pflege zahlt sich die jahrelange intensive Förderung der Selbstschutz- und Selbsthilfefähigkeiten der Bevölkerung durch den Staat jetzt aus. Denn in dieser Extremsituation sind die Patienten noch hilfsbedürftiger. Durch die Nachbarschaftshilfe (NaHi) können sie einstweilen versorgt werden, bis professionelle Hilfe kommt.

Elena Weber ist eine dieser freiwilligen Helfenden. Sie hat sich beim Freiwilligen-vor-Ort-System (FvOS) in ihrer Gemeinde registrieren lassen und auch an einer Schulung teilgenommen. Sie steht für Hilfe in der Nachbarschaft bereit, die sie auch mit ihrem Kind gut erreichen kann. Wegen der großen Hitze kann der ambulante Pflegedienst nicht mehr all seinen Aufgaben nachkommen; davon ist auch die alleinlebende, pflegebedürftige Frau Meinert im Nachbarhaus betroffen. Der Koordinator der örtlichen Lenkungsgruppe hat Frau Weber daher gebeten, bei ihr nach dem Rechten zu schauen. Bei Frau Meinert findet sie im Kühlschrank die SOS-Dose, der sie die wichtigsten Informationen über die Medikamente entnehmen kann. Ein Aufkleber an der Wohnungstür von Frau Meinert hatte sie auf die SOS-Dose hingewiesen; ein zweiter Aufkleber befand sich an der Kühlschranktür.

Die Nachrichten zeigten gestern Abend, dass es in anderen Regionen nicht so gut aussieht: dort wurde die Bevölkerung kaum zu vorausschauender Eigenvorsorge motiviert. Jetzt blockieren verzweifelte Bürgerinnen und Bürger seit Tagen die Notrufe von Feuerwehren, Rettungsdiensten und der Polizei. Sie brauchen Hilfe und wissen nicht, wie sie sich und ihre Angehörigen adäquat schützen und einfache Maßnahmen der Selbsthilfe anwenden können. Damit werden massiv Einsatzmittel gebunden, die anderweitig dringender gebraucht werden. Eine Journalistin hatte gestern aufgebrachte Menschen interviewt, die sich ihre Situation mit Verschwörungsmythen zu erklären versuchen.

Thomas Weber bleibt bis zum späten Abend im Seniorenstift. Am nächsten Morgen dann der Termin beim Gesundheitsamt: Runder Tisch „Taskforce Hitze". Dort erfährt er: Die Behörden haben nach 17 Hitzetoten in den vergangenen zwei Tagen aus Gesundheitsgründen tagsüber eine Ausgangssperre verhängt[21]. Die Menschen dürfen ihre Wohnungen nur noch im Notfall verlassen. Nach dem Meeting fährt er sofort heim, um nach den Kindern zu sehen. Seine Frau wollte heute in Amsterdam bei einer Konferenz sein. Aber der Flug wurde aufgrund von Kerosinmangel gestrichen. Wann Nachschub kommt, ist unklar. Es droht ein möglicher Totalausfall der Wasserstraßen. Politik und Wirtschaft sind alarmiert.

Elena und die Kinder sind tatsächlich zu Hause. Der Sohn geht schon seit drei Wochen nicht

19 Empfehlungen aus dem UN-Rahmenwerk für Katastrophenvorsorge oder auch Sendai Framework; siehe auch: Handlungsempfehlungen

20 Was wäre gewesen, wenn die Kommunen keine Haushaltsmittel für den Aufbau lokaler Kontaktbüros zur Verfügung gestellt hätten? In diesem Falle hätte Deutschland sein UN-Ziel nicht erreicht, nämlich ein integriertes und nachhaltiges Katastrophenrisikomanagement aufzubauen und seine Resilienz unter anderem gegenüber großen Gefahren wie dem Klimawandel und den daraus resultierenden Extremwetterlagen spürbar zu stärken. Siehe auch unter Handlungsempfehlungen

21 In Indien verhängten die Behörden im Juni 2019 nach mehreren Tagen bei 45 °C Ausgangssperren; vgl. https://www.aerzteblatt.de/nachrichten/103960/Zahlreiche-Tote-durch-Hitzewelle-in-Indien

mehr zur Schule. Die Hitze in den Klassenzimmern war unerträglich. Die Tochter hingegen ging weiterhin in ihre Kindertagesstätte, in der die Temperaturen noch akzeptabel waren – bis zur Ausgangssperre.

Endlich ruft Thomas Webers Mutter an. Die Familie solle sich keine Sorgen machen. Sie sei sicher untergebracht. Aber das Haus! Das Haus ist wahrscheinlich völlig abgebrannt. Herr Weber muss sich setzen, schnappt nach Luft: Unser Haus, mein Haus, mein Kinderzimmer, meine Erinnerungen – alles weg! Wie konnte es nur so weit kommen?

In einer ruhigen Minute recherchiert Herr Weber die Entwicklungen der vergangenen Jahre …

2.4 Historie der Entwicklung

Dass die große Dürre vor sechs Jahren, im Jahr **2025**, begann, hatte zunächst niemand bemerkt. Im Gegensatz zu den meisten Naturkatastrophen beginnt eine Dürre, bevor sich Symptome zeigen.[22] Die Landwirtschaft hatte in den vergangenen Jahren versucht, sich auf trockenere Sommer einzustellen – was jedoch nur teilweise gelungen war[23]. Manche Betriebe hatten die Bewässerungssysteme mit einer Brauchwasser-Aufbereitung gekoppelt, so wie es in Südeuropa gang und gäbe ist. In vielen Gärten standen jetzt aus demselben Grund Zisternen.

Die Niedrigwassersituation an Donau und Rhein im ersten Jahr war zwar ärgerlich und führte zu Preiserhöhungen, aber die Industrie hatte sich darauf eingestellt. Sie hatte wieder Vorrats- und Lagerhaltung auf niedrigem Niveau aufgebaut, um Unterbrechungen von Warenketten aufzufangen. Die extreme Just-in-time-Produktion Anfang des Jahrhunderts war schon allein aufgrund höherer Transportkosten durch die CO_2-Bepreisung zurückgefahren worden. Hinzu kam die gestiegene Vulnerabilität globaler Lieferketten durch häufigere und stärkere Extreme und außergewöhnliche Lagen überall auf der Welt. Ohne moderate Lagerhaltung waren die Ausfallrisiken und die Kosten seit den 2020er Jahren einfach zu groß geworden.

Die inzwischen höhere Waldbrandgefahr hatte die Feuerwehr auch besser im Griff. Die einschlägigen Ausbildungsmodule für Prävention, Früherkennung, Alarmierung und Waldbrandbekämpfung waren erweitert worden. Das hatte sich bereits ausgezahlt. Auch wenn der politische Diskurs um mehr Bundeszuständigkeit noch nicht beigelegt war – beim Thema effizientere Frühwarnsysteme war man immerhin weitergekommen.

22 Vgl. Toby Ault, On the essentials of drought in a changing climate, science, 2020, DOI: 10.1126/science.aaz5492, https://science.sciencemag.org/content/368/6488/256

23 Eine Anpassung durch ausschließlich mehr künstliche Bewässerung wäre problematisch, weil a) bewässerungsbedürftige Anbaukulturen in Deutschland nur bei dauerhaft hohen Preisen auch bewässerungswürdig wären (zum Beispiel Weizen deutlich oberhalb von 200 EUR je Tonne) und weil b) die Ausweitung der künstlich beregneten Flächen in Deutschland eine langfristige Investition und wegen strenger Obergrenzen für die Wasserentnahme auch nur punktuell möglich wären. Zurzeit werden 3 bis 4 Prozent der landwirtschaftlichen Nutzfläche künstlich bewässert.

2026: Im zweiten Jahr begannen in der Wissenschaft, bei zahlreichen NGO sowie einigen Politikerinnen und Politikern Warnungen vor einer langfristigen Dürre laut zu werden. Genau wie im ersten Jahr hatten anhaltende Hochdruckgebiete über Mitteleuropa, Skandinavien und den baltischen Staaten oder Westrussland die Wetterlage fest in der Hand. Berichte in den Medien über die gleichzeitigen Dürren in Deutschland, Frankreich, den Beneluxstaaten, der Schweiz, Österreich, Tschechien, der Slowakei, Polen, Weißrussland, den baltischen Staaten, Schweden, Finnland, Westrussland und Teilen Norwegens häuften sich. Zum ersten Mal flimmerten Bilder über den Bildschirm, auf denen Menschen vor Tankwagen Schlange standen. Man hatte das zuvor nur aus Schwellenländern des globalen Südens gekannt. Die Kompensationszahlungen an die Landwirtschaft verdreifachten sich. In den sozialen Medien brach ein Shitstorm gegen die Landwirtschaftsministerin los. Sogenannte Experten traten auf, die „bewiesen", dass man noch nicht von einer echten Dürre sprechen könne und dass es für den Steuerzahler viel zu teuer wäre, die Landwirtschaft weiter zu subventionieren. Die seriöse Wissenschaft widersprach und wies auf die dekadischen Klimavorhersagen hin, die eine hohe Wahrscheinlichkeit für eine mehrjährige Dürre zeigten. Wissenschaftlerinnen und Wissenschaftler mahnten in einer Stellungnahme Maßnahmen an, um für weitere Dürrejahre besser gewappnet zu sein.

Die Transportengpässe in der Binnenschifffahrt aufgrund der niedrigen Pegelstände konnten trotz der erhöhten Lagerhaltung in der Industrie nicht mehr voll aufgefangen werden. Obwohl der Verbrauch von Erdöl in den Jahren zuvor durch die Energiewende gesunken war, kam es auch hier zu ersten Knappheiten. Der Versuch, den Transport auf die Schiene umzuleiten, war nur wenig erfolgreich, da dort die Kapazitäten durch den vereinbarten Ausbau des Personenverkehrs ausgeschöpft waren. Die Folge: Umsatzausfälle bedrohten die Unternehmen, insbesondere bei der Stahl- und Chemieindustrie. Die Angst vor Insolvenzen stieg[24].

Besorgniserregend war die Einschränkung der Stromproduktion im europäischen Stromverbund. Die Stromproduktion aus Wasserkraft war fast zum Erliegen gekommen. Aber auch die konventionellen Kraftwerke mussten ihre Leistungen herunterfahren, denn durch die niedrigen Pegelstände und die damit verbundene Erwärmung des Wassers durften sie immer weniger Kühlwasser entnehmen.

Die Landwirtschafts-, Umwelt-, Wirtschafts- und Innenministerinnen und -minister des Bundes und der Länder traten zu einem Sondergipfel zusammen. Ein Aktionsplan zur Bekämpfung der Engpässe und Preissteigerungen wurde angekündigt. Aber zunächst kam es zu Konflikten zwischen wasserreichen und wasserarmen Regionen. Man konnte sich auf keinen akzeptierten Wasserentnahmeprozess einigen. NGO forderten, die Energiewende zu beschleunigen und eine unabhängige nationale Wasserkommission zu gründen.

2027: Im dritten Jahr nahm die nationale Wasserkommission ihre Arbeit auf. „Wir stehen vor einer Wasserkrise und müssen Wassermanagement ganz anders denken und die Wasservorräte für unsere Kinder und künftige Generationen bewahren", sagte die Vorsitzende zur Eröffnung. Ähnlich der Kohlekommission von 2018 besteht sie aus Entsandten von Politik, Wissenschaft und Verbänden sowie – und das ist neu – aus zufällig ausgewählten Bürgerinnen und Bürgern. Schon nach der ersten Sitzung empfahl die Kommission ein deutschlandweites Verbot luxuriösen Wasserverbrauchs (Rasensprengen und Swimmingpools) bis zum Ende der Dürre und mahnte die wasserreichen Regionen und Landkreise zur Solidarität mit den wasserarmen. Schließlich wurde eine Überarbeitung des Gesetzes zur Sicherung der Ener-

24 Im dritten Quartal 2018 verzeichnete das Chemie-Unternehmen BASF ein um rund 50 Millionen Euro niedrigeres Betriebsergebnis – bedingt durch höhere Transportkosten und Produktionsverluste. https://www.spiegel.de/wirtschaft/unternehmen/basf-stoppt-tdi-produktion-in-ludwigshafen-wegen-niedrigsp wasser-a-1240547.html

gieversorgung (EnSiG) innerhalb des laufenden Jahres auf die Agenda gesetzt. Die Wasserkommission kritisierte, dass in das Konzept der Versorgungssicherheit Extremwetter nicht mit eingerechnet wurden[25]. Versorgungssicherheit werde ausschließlich marktwirtschaftlich definiert, was nicht mehr zeitgemäß sei.

Gegen Ende des Jahres waren sich Wissenschaft, Wirtschaft und Politik endlich darin einig, dass man von einer Dürre „noch nie dagewesenen Ausmaßes" sprechen konnte. Die Wasserkommission machte darauf aufmerksam, dass es an Erfahrung, aber auch an Vorkehrungen für diese Dimension der Wasserknappheit fehle. Die Trinkwasserpreise begannen zu steigen. Wer sich nicht an die immer weiter ausgedehnten Nutzungsverbote hielt, wurde mit drastischen Geldstrafen belegt – oder von der Wasserversorgung ausgeschlossen. Die meisten Menschen reagierten einsichtig und kooperierend. Aber es gab auch konkrete Fälle des Regelübertritts, die in den Medien prominent aufgegriffen wurden. Es häuften sich Nachbarschaftsstreitereien aufgrund von Wasser. Auch Landrätinnen und Landräte sowie Bürgermeisterinnen und Bürgermeister begannen „ihr" Wasser zu verteidigen. Dazu kamen die Brunnen, die trockengefallen waren. Die Konsequenz: noch mehr Menschen, die an Trinkwasser-Tankwagen der Kommunen Schlange standen. Die Lage verschärfte sich.

2028: Während es in den ersten drei Jahren noch gelungen war, die schlechten Ernten in Mitteleuropa durch Importe auszugleichen, kam es im vierten Jahr nun auch zu ersten Engpässen im Lebensmittelbereich[26]. Einzelne Länder hatten bereits einen Exportstopp verhängt, um ihre eigene Bevölkerung mit Lebensmitteln versorgen zu können. Viele außereuropäische Länder, die Europa einst in großem Maßstab mit frischem Obst und Gemüse sowie Soja als Futtermittel beliefert hatten, waren nur sehr begrenzt in der Lage zu helfen. Sie hatten schon in den 2020er Jahren ihre Agrarexporte verringert, um ihrer eigenen schleichenden Trinkwasserknappheit entgegenzuwirken. Stattdessen hatten sie begonnen, in großem Stil Strom zu produzieren. Große Förderprogramme – teilweise im Rahmen der deutschen Entwicklungszusammenarbeit angeschoben – halfen dabei, Solarfarmen zu gründen und Europa mit grünem Gas zu beliefern.

Neue Importverträge mit anderen Ländern konnten zwar eine echte Krise abwenden – aber die Preise vieler Lebensmittel stiegen deutlich. Gleichwohl wurden die Entschädigungszahlungen an die Landwirtschaft stark gedrosselt. Manche Bundesländer hatten die Bedingungen drastisch verschärft. Viele Landwirtinnen und Landwirte mussten ihren Betrieb aufgeben. Die Verbände protestierten.

Im Laufe des Jahres kam es zu ersten regionalen Abschaltungen von Großabnehmern durch die Stromnetzbetreiber. Diese Maßnahmen wurden erforderlich, weil aufgrund der zu großen Nachfrage die Systemstabilität gefährdet war. Im Vorfeld wurden dazu Regelungen im EnWG[27] getroffen. Demnach sind die Übertragungsnetzbetreiber in Zusammenarbeit mit den nachgelagerten Netzbetreibern verantwortlich für die Gewährleistung einer sicheren und zuverlässigen Versorgung mit elektrischer Energie. Für den Fall, dass es zu Störungen des Systembetriebes kommt, sind die Übertragungsnetzbetreiber befugt, umfangreiche Eingriffe in die Systemlandschaft vorzunehmen. Dazu zählt neben dem An- und Abfahren von Erzeugungseinrichtungen (Windkraftanlagen, Solarkraftwerke und konventionelle Kraftwerke) das Abschalten von Abnehmern.

In diesem Sommer gab es eine weitere starke Nachfrage nach Strom – vor allem für Kühlung – was aufgrund der eingeschränkten Energieproduktion dazu führte, dass das Gesamtsys-

25 Siehe: BMWi-Studie zur Versorgungssicherheit an europäischen Strommärkten, https://www.bmwi.de/Redaktion/DE/Publikationen/Studien/definition-und-monitoring-der-versorgungssicherheit-an-den-europaeischen-strommaerkten.pdf?__blob=publicationFile&v=18

26 „Im Zeitraum des gesamten Ereignisses ist mit Ernteertragsdepressionen zu rechnen. Für das letzte [sechste] Szenariojahr lassen sich unter den angenommenen Szenariobedingungen Ertragsdepressionen von bis zu 60 % einer Durchschnittsernte abschätzen." BT Drs. 19/9521, Seite 12

27 Energiewirtschaftsgesetz, Gesetz über die Elektrizitäts- und Gasversorgung

tem in Schieflage geraten war und nur durch Restriktionen und das Abschalten von Abnehmern stabilisiert werden konnte. Durch Hitze und Dürre gab es Probleme auf allen Feldern:

- Die Energiegewinnung aus Biogasanlagen nahm ab. Aufgrund der Dürre gab es nicht mehr genügend Ernteerträge für diese Anlagen. Zusätzlich kam es zur Konkurrenzsituation zwischen Energiepflanzen und Nahrungsmittelpflanzen für Mensch und Tier.

- Auch wenn die Hitze prinzipiell zu keinen eindeutigen Trends beim Windangebot führt, erlebte Deutschland in diesem Szenario nahezu Flaute über der Ostsee bei mäßigem Wind über der Nordsee. Damit war die Energieerzeugung aus Windkraft ebenfalls reduziert.

- Die letzten verbleibenden Steinkohlekraftwerke wurden durch die Hitze immer ineffizienter. Damit das benötigte Kühlwasser nicht die Flüsse aufheizt und Flora und Fauna vernichtet, kam es entlang des Rheins wegen zu hoher Einleittemperaturen in Verbindung mit Niedrigwasser zu Drosselungen und Abschaltungen ganzer Kraftwerksblöcke. Auch stieg die Konkurrenz zu anderen Industrieprozessen mit Kühlwasserbedarf drastisch.

- Die Braunkohlekraftwerke, die aufgrund ihrer hohen Umweltschädlichkeit durch den hohen Ausstoß an CO_2 in naher Zukunft gänzlich abgeschaltet werden sollen, aber liefen stabiler. Hintergrund ist, dass das Kühlwasser aus dem Grubenwasser der angeschlossenen Tagebaue gewonnen wird. Es unterliegt keinen Beschränkungen in der Entnahme, ist unabhängig vom Wasserstand der Flüsse und hat eine verhältnismäßig geringe Temperatur, da es von unter Tage gefördert wird.

- Auch die Solaranlagen reagierten unter den Hitzerekorden mit einer leichten Abnahme des Wirkungsgrades. Durch die längeren Sommertage, verbunden mit einer längeren Einstrahlung auf die Module, fiel dies nicht allzu sehr ins Gewicht.

Ein anderes Problem bereiteten punktuelle Starkniederschläge am Ende des vierten Jahres. Sie führten zunächst zu lokalen Überschwemmungen, mehreren zerstörten Ortschaften und insgesamt acht Toten. Damit war man noch glimpflich davongekommen. Denn inzwischen waren alle wichtigen Liegenschaften der Einrichtungen des Bevölkerungsschutzes (Rettungswachen, Feuerwachen, Leitstellen und andere) einer Risikoanalyse hinsichtlich von Wetterextremen unterzogen und daraufhin baulich-technisch gehärtet worden, so dass es zu keinen Beeinträchtigungen der Einsatzfähigkeit von Standorten kam.[28] Im weiteren Verlauf führten die Niederschläge zu einer zeitweisen Entspannung der Situation. Die Menschen im ganzen Land schöpften Hoffnung. Expertinnen und Experten waren zuversichtlich, dass nun das Ende der Dürre gekommen sei.

2029: Aber schon Mitte des fünften Jahres waren die Überschüsse an Regenwasser aus 2028 aufgebraucht und das Niederschlagsdefizit wurde wieder größer. Eine Insolvenzwelle erfasste die Landwirtschaft; die Lebensmittelpreise stiegen drastisch. Ein investigativer Journalist veröffentlichte, dass ein Top-Fußballer seinen Swimmingpool heimlich mit Frischwasser hatte füllen lassen, um dort eine Privatparty zu feiern. Der Wasserversorger wurde dafür bestochen. Es kam zu einer medialen Aufregung. Die Staatsanwaltschaft ermittelte. Der Umweltminister trat zurück. In der Folge erschienen beinahe täglich Berichte von illegalen Wasserentnahmen – die sich größtenteils als Falschmeldungen herausstellten. Führende Wissenschaftlerinnen und Wissenschaftler, Persönlichkeiten des öffentlichen Lebens und NGO veranstalteten den ersten Bürger-Wassergipfel „Wem gehört das Wasser – Wirtschaftsgut oder Daseinsvorsorge?“

28 Ohne diese Maßnahmen hätten die Starkregenereignisse zur Überflutung verschiedener Feuer- und Rettungswachen sowie anderer Liegenschaften des Bevölkerungsschutzes geführt und damit die Einsatzfähigkeit in manchen Gebieten spürbar beeinträchtigt. Hinzu wären Ausfälle im Kommunikationsbereich gekommen. Siehe auch unter „Handlungsempfehlungen“.

2030: Im Januar des sechsten Jahres zogen kräftige Regentiefs durchs Land und brachten wieder leichte Entspannung. Dann drehte der Wind nach Ost, und im Februar wurde das Land von einer extremen Kältewelle heimgesucht. Trockene und kalte Luftmassen polaren Ursprungs, verbunden mit starken Frösten, machten den Menschen und wieder einmal der Landwirtschaft zu schaffen. An manchen Tagen sank das Thermometer auf minus 18 Grad. Der Niederschlag erreichte nur 30 Prozent des vieljährigen Mittelwerts.

Eine hochgradig nervöse Diskussion entspann sich im Netz. Behauptungen, die Kältewelle sei der Beweis, dass es gar keine Klimaerwärmung gebe, machten die Runde. Dementis der Klimawissenschaft und Erläuterungen, wie eine Kältewelle mit dem Klimawandel zusammenhängt, kamen gegen das Wiederaufflammen von Verschwörungsmythen kaum an.

Im **April 2030** wurde es hingegen schon wieder ungewöhnlich warm und im August rollte die größte je gemessene Hitzewelle über Zentraleuropa.

2.5 Handlungsempfehlungen

Die Herausforderung ausreichender Anpassungsmaßnahmen an den nicht mehr vermeidbaren Klimawandel ist groß. Das gilt weltweit, wie auch für Deutschland. Die folgenden Empfehlungen orientieren sich an den Aufgaben des Risiko- und Krisenmanagements und fokussieren bewusst auf die nationale Ebene, beschreiben aber Anschluss- und Schnittstellen. Sie beschränken sich nicht auf die Anforderungen für die im Szenario beschriebene Dürre.

Deutschland verzeichnet ganzjährig Zunahmen extremer Wetterereignisse. Durch Verschränkungen einzelner Ereignisse (Hitze *und* Dürre) und das mögliche Auslösen von kaskadierenden Effekten (Hitze *und* Dürre *und* Wassermangel *und* Stromausfall *und* Lebensmittelengpässe) potenzieren sich die Herausforderungen. Damit verbunden ist eine quantitative und qualitative Steigerung der Einsätze im Bevölkerungsschutz wie Rettungsdienste, Feuerwehren, Zivil- und Katastrophenschutz. Das führt zu deutlich mehr Belastung von Personal und Technik. Gleichzeitig steigen die Anforderungen an den Schutz klima- beziehungsweise wetterbedingt störanfälliger Kritischer Infrastrukturen. Zudem sehen wir kritische Prozesse, die sich mit dem Klimawandel überlagern und die Risiken durch positive Rückkopplungen verschärfen dürften: insbesondere der demografische Wandel (schrumpfende Einsatzkräftepotenziale, vulnerablere Bevölkerung) und sicherheitspolitische Herausforderungen durch internationale Spannungen, die sich auch auf den Bevölkerungsschutz auswirken, nämlich die Zivile Verteidigung einschließlich des Zivilschutzes.

Im Szenario wurden bereits einige Maßnahmen als erfolgreich umgesetzt beschrieben, die heute, 2020, noch nicht einmal in Angriff genommen worden sind[29]. Sie werden hier noch einmal aufgegriffen und benannt.

29 Zum Beispiel: Arbeitsschutzkleidung, Notbrunnen, Kontaktbüros für die Bevölkerung.

Schwerpunkt: Neue Herausforderungen für den Bevölkerungsschutz durch den Klimawandel

Sicherheitsarchitektur überprüfen – Bundeskompetenzen stärken:

Deutschland ist im Bevölkerungsschutz grundsätzlich gut aufgestellt. Die Zuständigkeit der Länder für den Katastrophenschutz und seine föderale Architektur tragen maßgeblich zum Erfolg des Bevölkerungsschutzes bei, insbesondere durch bedarfsorientierte und lokal adäquate (Re-)Aktionen, eine erleichterte Einbindung von Ehrenamtlichen und bürgernahe Entscheidungen. Bei länderübergreifenden, europäischen oder gar internationalen Lagen weisen die Sicherheitsarchitektur und das integrierte Hilfeleistungssystem aber Anknüpfungsprobleme auf. Die COVID-19-Pandemie im Jahr 2020 offenbart diese Schwäche. In gleicher Weise können auch Folgen des Klimawandels wie Dürren, Hitzewellen, Sturmfluten oder Hochwasser eine länderübergreifende kohärente Bewältigung notwendig machen.

Es bedarf der Evaluierung, ob bei länderübergreifenden und national bedeutsamen Gefahrenlagen Kompetenzen, die im Bereich des Katastrophenschutzes liegen, daher auch auf die Bundesebene übertragen werden sollten. Dies kann auch eine Stärkung der Bundesbehörden Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) und Technisches Hilfswerk (THW) sowie Überlegungen für eine Zentralstellenkompetenz des Bundes im Bevölkerungsschutz einschließen. Bisher besitzt der Bund nur im Verteidigungsfall für den Zivilschutz eine klare Zuständigkeit, während die Länder für den Katastrophenschutz grundsätzlich die alleinige Verantwortung tragen. Diese strikte Trennung ist nicht mehr zeitgemäß. Ohne die föderalen Grundprinzipien aufzugeben, ist zu prüfen, wie der Bund im Sinne des Subsidiaritätsprinzips bei besonders gravierenden Krisen- und Schadenslagen mit nationaler Bedeutung besser koordinierend tätig sein kann und grundlegende Entscheidungen zur wirkungsvollen Lagebewältigung und koordinierende Maßnahmen dann schnell, verbindlich und konsistent erfolgen können. Anzustreben sind mehr Verbindlichkeit in der Bund-Länder-Zusammenarbeit sowie eine noch näher auszuformulierende Koordinierungskompetenz, die das föderale Grundprinzip jedoch nicht schädigt.

Nicht nur Pandemiegeschehen (wie sie im Kapitel „Epidemien, Pandemien – Eskalierende Ausbrüche gefährlicher Infektionskrankheiten“ ausführlich beschrieben werden), sondern auch der Klimawandel wird nach heutigen Erkenntnissen zu Krisenlagen wie der beschriebenen lang anhaltenden Dürre mit begleitenden Hitzeperioden, Starkniederschlägen und weiteren extremen Wetterereignissen führen, die eine bundeseinheitliche Vorgehensweise notwendig machen. Beispiele sind:

- Nationaler Hitzeaktionsplan
- Nationale dynamische Lagebilder
- Nationales Ressourcen- und Verfügbarkeitsmanagement
- Nationales Wassermanagement
- Nationale strategische Reserven mit dezentraler Logistik

> *Unsere föderalen Strukturen im Bevölkerungsschutz sind grundsätzlich sinnvoll. Jedoch hat die Bundesregierung den Bedarf an besserer Aufgabenkoordination nicht rechtzeitig erkannt. Trotz Neufassung der Konzeption Zivile Verteidigung im Jahr 2016 ist der Zivilschutz in Deutschland aufgrund föderaler Kompetenzverteilung und immer globalerer Herausforderungen nicht angemessen aufgestellt. Mit einer Zentralstellenkompetenz für das BBK wäre ein wichtiger erster Impuls gesetzt, um in Krisen künftig zu einer besseren Koordination zu kommen.* ***– Benjamin Strasser MdB***

Operative Fähigkeiten des Katastrophenschutzes erweitern:

Ein besonderes Merkmal des überwiegend durch ehrenamtliche Einsatzkräfte getragenen Bevölkerungsschutzes in Deutschland ist die Fähigkeit, Einheiten des Zivilschutzes und des erweiterten Katastrophenschutzes der Länder an Schadensschwerpunkten zusammenzuziehen. Durch den Klimawandel werden sich Bevölkerungsschutzlagen öfter nicht mehr auf örtliche Schwerpunkte konzentrieren, sondern größere Gebiete umfassen. Mehrere oder gar alle Bundesländer werden gleichzeitig betroffen sein. Die Ressourcen des Bundes, die im Einsatzfall den Bundesländern zur Verfügung stehen, müssen daher erweitert werden:

- Die Kapazitäten zur Trinkwasseraufbereitung einschließlich Anlagen zur Ausgabe des Trinkwassers an die Bevölkerung müssen ausgebaut werden.

- Ebenso müssen hinreichende Kapazitäten zum Trinkwassertransport und zur -verteilung zur Verfügung stehen, um die betroffene Bevölkerung aus Gebieten mit funktionierender Trinkwasserversorgung beliefern zu können.

- Neben einer erhöhten Gefahr für Einschränkungen der Trinkwasserversorgung wird der Klimawandel auch die Gefahr von Ausfällen bei der Stromversorgung erhöhen. Um auch wichtige Einzelabnehmer (zum Beispiel Krankenhäuser, Wasser- und Klärwerke, Einkaufszentren) gegebenenfalls mit Notstrom versorgen zu können, sollte das von der Bundesregierung beim THW bereits etablierte bundesweit flächendeckende Versorgungsnetz[30] mit Notstromaggregaten weiter gestärkt werden.

- Zudem müssen – auch vor dem Hintergrund der Erfahrungen aus der COVID-19-Pandemie – die strategischen Notreserven des Bundes erweitert werden. Hier geht es insbesondere um Reserven bei Schutz-, Betreuungs- sowie Einsatzausstattung.

- Um eine Verteilung der Bundesreserven sicherzustellen, müssen die logistischen Kapazitäten erweitert und um eine Koordinierungsstelle ergänzt werden.

> *Das Tempo, mit dem die Klimakrise zuschlägt, ist atemberaubend und die Auswirkungen sind allgegenwärtig. Die extreme Trockenheit sowie die Hitzewellen in den vergangenen Jahren haben uns auch in Deutschland vor Augen geführt, dass wir neben einem wirklich effektiven Klimaschutz zunehmend Klimaanpassungsmaßnahmen ergreifen müssen. Ein wichtiger Baustein ist für mich, dass wir unsere ‚Blaulichtorganisationen' besser für die neuen Herausforderungen rüsten. Hierzu zählt auch ein konsequenter Ausbau der luftgestützten Waldbrandbekämpfung durch Hubschrauber oder Löschflugzeuge. Eine Einbindung dieser Ressourcen in ‚rescEU' wäre gleichzeitig ein Beitrag zum europäischen Katastrophenschutz und Ausdruck gelebter Solidarität.*
>
> ***– Dr. Irene Mihalic MdB***

30 https://www.thw-bv.de/was-wir-machen/neuigkeiten/detail/gute-neuigkeiten-aus-dem-haushaltsausschuss-fuer-das-thw

Klimawandel und zukünftige Klimaprojektionen konzeptionell in alle Facetten der Katastrophenvorsorge einbeziehen:

In diesem Kontext kommen insbesondere folgende Aufgaben auf den Bevölkerungsschutz zu:

- Ertüchtigung und Ausbau der Trinkwassernotversorgung
- Ausbau und Bereitstellung von Notfallreserven, zum Beispiel Ausbau und Systematisierung der Ernährungssicherheit
- Überarbeitung und Anpassung von Notfall-, Ausbildungs- und Einsatzplänen
- Einführung regionaler beziehungsweise bundesweit abgestimmter Aktionspläne (etwa Hitzereaktionspläne)
- Sicherstellung erforderlicher haupt- und ehrenamtlicher Personalressourcen bei Rettungsdiensten, Feuerwehren und im Zivil- und Katastrophenschutz durch eine gezielte nachhaltige Ehrenamtsförderung sowie durch die Gewährleistung guter Arbeitsbedingungen[31] für hauptamtliches Personal
- Ergänzung der technischen Ressourcen für extremwetterbedingte Lagen, insbesondere für Wald- und Vegetationsbrände, für Hitzeperioden, Dürren, Starkniederschläge und Stürme
- Entwicklung und Einführung lageadäquater persönlicher Schutzausrüstungen für die Einsatzkräfte bei extremen Wetterlagen (zum Beispiel Hitzewellen)
- Härtung der eigenen Liegenschaften und Infrastrukturen gegenüber Wetterextremen und Stromausfall
- Ausbau des Warn- und Informationsmanagements für die Bevölkerung

> *Die Projektion gibt uns die Möglichkeit, die Bedarfe für den zivilen Bevölkerungsschutz für die Zukunft noch zielgenauer und wirkungsvoller zu planen. Denn die Ausstattung unserer Rettungskräfte und Sicherheitsbehörden muss sich ebenso wie in anderen Bereichen auch technisch und in der Infrastruktur an die Herausforderungen des Klimawandels anpassen, um unsere Bevölkerung weiterhin bestmöglich zu schützen."* ***– Michael Kuffer MdB***

31 Dazu zählen insbesondere: Schichtdienste, die nicht gesundheitsschädlich sind, moderne Persönliche Schutzausrüstung, familienfreundlicher Dienstbetrieb, gute Bezahlung und soziale Anerkennung.

Resilienz in Wirtschaft und Gesellschaft stärken:

Die Ökonomisierung in vielen Bereichen hat zu einseitiger Beachtung von (betriebswirtschaftlicher) Effizienz zulasten von Resilienz geführt. Zudem haben die Kommunen in den vergangenen Jahren besonders unter Finanznot gelitten. Es wurde Personal abgebaut, und Aufgaben wurden privatisiert. Um gegen klimawandelbedingte Risiken und Schäden gewappnet zu sein, muss Effizienz gegen Resilienz sorgsam abgewogen und mit gesellschaftlich zu bestimmenden Schutzzielen in Einklang gebracht werden. Zu einem systematischen Auf- und Ausbau der Resilienz in Wirtschaft und Gesellschaft gehören insbesondere:

- Härtung von Kritischen Infrastrukturen und systemrelevanten Strukturen sowie Dienstleistungen gegenüber Extremwetterereignissen:
  - Im Versorgungsbereich: unter anderem Wasser- und Abwasser, Energie, Treibstoff, Transportwege, Müllabfuhr
  - Im Gesundheitsbereich: unter anderem Krankenhäuser, Arztpraxen, Notfallrettung, Apotheken
  - Informations- und Kommunikationsdienstleistungen
- Flächendeckende Förderung der Selbstschutz- und Selbsthilfefähigkeit der Bevölkerung und Steigerung dieser Fähigkeiten in allen Bevölkerungsgruppen
- Risiko- und Krisenkommunikation, angepasst an die unterschiedlichen Zielgruppen von Politik, Wirtschaft und Gesellschaft

> *Unsere Wirtschaftsordnung, die auf nahezu unbegrenztes Wachstum und größtmöglichen Profit setzt, hat die Erderwärmung befeuert und unser Ökosystem an den Rand des Zusammenbruchs gebracht. Die Auswirkungen auf Mensch und Umwelt, vor allem im globalen Süden, sind verheerend. Neben einer klimaangepassten Katastrophenvorsorge erfordert die Klimakrise daher einen grundsätzlichen Wandel in der Art und Weise, wie wir produzieren und wie wir konsumieren. Wichtig ist, dass dieser notwendige ökologische Wandel sozial gerecht gestaltet wird, damit nicht die sozial Benachteiligten den Großteil der Kosten zur Bewältigung der Klimakatastrophe tragen müssen."* ***– Dr. André Hahn MdB***

Risikoanalysen für bessere Prävention und Vorbereitung auf klimawandelbedingte Krisen:

Risikoanalysen sind die Grundlage für politische und administrative Entscheidungen und liefern Hinweise für die Prävention. Notwendig sind auf den Klimawandel fokussierte Vulnerabilitäts- und Risikoanalysen auf allen Ebenen, um den Klimawandel als Katastrophenrisiko besser zu verstehen. Dazu gehören auch das Erfassen von Verlusten durch Unterlassung von Klimaanpassung und Klimaschutz (Mitigation). Verluste betreffen sowohl materielle Güter (Gebäude, Straßen, Unternehmen) als auch natürliche Ressourcen (Wald, Biodiversität, Wasser) als auch ideelle Verfasstheiten (gesellschaftlicher Zusammenhalt, Vertrauen in Demokratie oder Regierungshandeln)

Das UN-Rahmenwerk für Katastrophenvorsorge länderübergreifend und sektorübergreifend umsetzen:

Das UN-Rahmenwerk für Katastrophenvorsorge (Sendai Framework) ist eine internationale Strategie mit dem übergeordneten Ziel, die Resilienz in den Unterzeichnerstaaten zu stärken. In Deutschland wird das Sendai-Rahmenwerk strategisch von einer interministeriellen Arbeitsgruppe der Bundesregierung und operativ von einer Nationalen Kontaktstelle am BBK umgesetzt.

Bei Verwirklichung eines derzeit verfolgten kohärenten, interaktiven und akteursbezogenen Ansatzes bis 2030 wird dies positive Auswirkungen auf Klimaschutz und Klimaanpassung in Deutschland und damit auf ein verbessertes Katastrophenrisikomanagement haben. Die Philosophie ist dabei der Risiko- und Krisenmanagementkreislauf mit den Sektoren Prävention, Vorsorge, Bewältigung und nachhaltigem Wiederaufbau. Die Ziele sollen unter anderem durch die Stärkung der Interdisziplinarität, der Vernetzung sowie querschnittlicher Betrachtungsweisen des Katastrophenrisikomanagements und damit des Bevölkerungsschutzes erreicht werden. Ebenso sind die Einrichtung von regionalen und lokalen Büros für Behörden, Unternehmen, Verbände und die Bürgerinnen und Bürger als Informationsdienstleister, Netzwerker und Kommunikator vor Ort sowie der Austausch über Best-Practice-Börsen angedacht. Parallel dazu sollen Übersichten zu bestehenden Fördermöglichkeiten für das Katastrophenrisikomanagement und die Klimaanpassungsmaßnahmen kontinuierlich dargeboten und neue Förderlinien initiiert werden. Über die Nationale Kontaktstelle, die EU-Kommission und die UN-Organisationen werden gute Lösungsansätze aus Deutschland in die Nachbarstaaten, die EU und die Weltgemeinschaft transferiert, aber auch umgekehrt Best Practice aus dem Ausland nach Deutschland gebracht.

Schwerpunkt: Klimavorsorge und Katastrophenvorsorge verzahnen

Die Folgen des Klimawandels sind schon heute überall spürbar und betreffen alle Sektoren. Die Anpassung an den nicht mehr vermeidbaren Klimawandel muss daher über Grenzen und Zuständigkeiten hinweg erfolgen. Klimapolitik und Sicherheitspolitik werden in der Außenpolitik längst zusammengedacht: Deutschland arbeitet im UN-Sicherheitsrat daran, den Schwerpunkt „Klimawandel und Sicherheitspolitik" auf der Agenda des Sicherheitsrats zu verankern. Auch auf nationaler Ebene müssen Umweltpolitik (Klimaanpassung/Klimavorsorge) und Innenpolitik (Katastrophenvorsorge) besser miteinander verzahnt werden.

Die „Deutsche Anpassungsstrategie an den Klimawandel" (DAS) von 2008 sowie die „Aktionspläne Anpassung" (APA) von 2011, 2015 und Herbst 2020 tragen diesem Gedanken Rechnung. Sie sind der Rahmen für Anpassungsaktivitäten in Deutschland. Gerade die Extremereignisse erfordern übergreifendes Handeln staatlicher und privater Akteure. Generelle Ziele sind dabei, die Verwundbarkeit gegenüber dem Klimawandel zu verringern und gleichzeitig die Widerstandskraft sowie Anpassungs- und Lernfähigkeit zu erhöhen. Im Vordergrund stehen dabei drei Leitprinzipien, die in den Sektoren und Regionen unterschiedlich umgesetzt werden sollten:

Vorsorge gegenüber Folgen des Klimawandels stärken und systematisch in Planungs- und Investitionsentscheidungen berücksichtigen:

Analog zur Katastrophenvorsorge ist Klimavorsorge wichtig, um Schäden durch Klimaereignisse oder andere Naturereignisse erst gar nicht entstehen zu lassen. Vorsorge heißt auch im Sinne eines Climate Mainstreaming[32] Pläne und Programme auf den Prüfstand zu stellen. Zum Beispiel gilt es, Regionalpläne oder Investitionsprogramme daraufhin zu prüfen, ob sie unter künftig veränderten klimatischen Bedingungen realisierbar sind.

- **Beispiel Bauvorsorge:** Wohngebäude und gewerbliche Gebäude und Industrieanlagen müssen zukünftig für Extremereignisse wie Starkregen oder Hitze ausgelegt sein.

- **Beispiel Landwirtschaft:** Landwirtinnen und Landwirte müssen sich jetzt schon an künftige Klimabedingungen anpassen, um weitere Schäden und Ernteausfälle zu vermeiden. Eine moderne Landwirtschaft schont natürliche Grundlagen und pflegt Kulturlandschaften in verantwortungsvoller Weise, denn diese sind das wesentliche Kapital zur Sicherung unserer Nahrungsmittelversorgung. Voraussetzung für diesen grundlegenden Paradigmenwechsel ist eine intensive Unterstützung und Begleitung durch die Politik. Ebenfalls muss das Wasserressourcenmanagement angepasst werden, um künftige Wassernutzungskonflikte zu entschärfen. Langfristig besteht auch in Deutschland das Risiko von Grundwasserknappheit, was heute schon durch entsprechende Anpassungen in Trink- und Brauchwasserversorgung adressiert werden muss.

32 Climate Mainstreaming: Klimaanpassung als Leitbild, das heißt. bei allen gesellschaftlichen und politischen Vorhaben die Auswirkungen auf die Resilienz von Klimarisiken grundsätzlich und systematisch zu berücksichtigen. Siehe auch 23. Zukunftsforum zum Themenschwerpunkt „Klimawandel – eine Herausforderung für die Öffentliche Sicherheit" vom 16.10.2014, Vortrag von Dr. Helge Wendenburg, ehem. Leiter der Abteilung Wasserwirtschaft, BMU.

Klimavorsorge, Katastrophenvorsorge und die Nachhaltigkeitsziele verbinden:

Die Nachhaltigkeitsziele (Sustainable Development Goals, SDG) wurden 2015 auf UN-Ebene verankert. Die Umsetzung ist seither eine bundesweite Aufgabe. Prinzipiell gilt: Je besser diese Ziele erreicht werden, desto besser ist der Schutz vor Schäden durch Klimaextreme. Kriterien der Nachhaltigkeit, wie sie in den SDG beziehungsweise in der deutschen Nachhaltigkeitsstrategie festgeschrieben sind, sind daher für Klimavorsorge und Katastrophenvorsorge gleichermaßen relevant.

- **Beispiel Mobilität:** Sowohl im Güter- als auch im privaten Verkehr kann es durch Extremereignisse zu erheblichen Einschränkungen der Mobilität und der Versorgung mit Gütern kommen – etwa Unterbrechung von Lieferketten, eingeschränkte Versorgung mit Treibstoff. Eine nachhaltige Mobilität ist dadurch gekennzeichnet, dass sie soweit wie möglich unabhängig von den Folgen solcher Störungen ist, indem sie beispielsweise auf E-Mobilität setzt oder – insbesondere in Städten – nichtmotorisierten Verkehr in den Vordergrund stellt.

- **Beispiel Trinkwasser:** Hitzewellen und Dürreperioden können dazu führen, dass es regional zu Engpässen in der Wasserversorgung kommen kann. Dabei ist die Versorgung mit Trinkwasser vor allem für besonders betroffene Menschen (ältere Menschen, Kranke, Kinder) von besonderer Bedeutung. Trinkwasserversorgung ist daher ein wesentlicher Aspekt eines insgesamt schonenden Umgangs mit Wasserressourcen – dieser soll unter veränderten Klimabedingungen gewährleisten, dass Wasser auch weiterhin für weitere Zwecke genutzt werden kann, zum Beispiel für notwendige Bewässerung in der Landwirtschaft oder für industrielle Prozesse. Nachhaltige Wassernutzung bedeutet ebenso, verschwenderischen Umgang mit Wasser zu vermeiden.

Resilienz stärken und Lehren aus der Vergangenheit ziehen:

Vorsorge ist wichtig – aber nicht alles. Immer wieder kommt es zu Ereignissen, die nicht vorhersehbar waren. Deshalb ist es für moderne, arbeitsteilig organisierte und stark vernetzte Gesellschaften wie in Deutschland wichtig, ständig Lehren aus vergangenen Ereignissen zu ziehen und sich so gut wie möglich auch auf das Unvorhersehbare vorzubereiten. Der „reasonable worst case"-Ansatz[33] der Risikoanalyse im Bevölkerungsschutz ist kein Katastrophenszenario, sondern ein sehr gutes Mittel, permanent zukünftige mögliche Entwicklungen zu antizipieren. Eine Lehre ist, die Vorsorge zu stärken (siehe oben), aber auch die Robustheit, zum Beispiel von Infrastrukturen, zu erhöhen. Hierfür sind unter anderem bestehende Regeln und technische Normen und Regelwerke für Energieversorgung, Bau und Gebäudetechnik zu überprüfen und klimafest auszugestalten. Auch Fachgesetze müssen kontinuierlich daraufhin überprüft werden, ob sie den Klimawandel angemessen berücksichtigen.

33 Reasonable Worst Case Szenario: Szenario ist hoch unwahrscheinlich aber plausibel

Schwerpunkt: Nachhaltige Investitionen in eine klimaresiliente Gesellschaft

Finanz- und Personalausstattung nachhaltig finanzieren:

Im politischen Verteilungskampf hat es der Bevölkerungsschutz besonders schwer, weil Eintrittswahrscheinlichkeit und Schadenshöhe stets unsicher sind. Vor allem aber ist der größte Feind des Bevölkerungsschutzes sein Erfolg: Passiert in einer Krise nichts, erregt das kaum Aufmerksamkeit und kann die Rechtfertigung für eine nächste Finanzierung eher schwieriger machen. „There is no glory in prevention." Gleichwohl: der Engpass bei Filtermasken und Schutzkleidung in der Coronakrise hat die Notwendigkeit der Finanzierung von Vorsorge in den gesellschaftlichen Mainstream gerückt. Auch Anpassungsmaßnahmen im Bevölkerungsschutz an den Klimawandel, Klimavorsorge und Katastrophenvorsorge, die Umsetzung internationaler Programme wie des Sendai Frameworks – sie alle benötigen nachhaltige Investitionen. Eine nachhaltige Finanz- und Personalausstattung benötigter Strukturen auf allen Ebenen kann aber nach allen Erkenntnissen die Kosten für auftretende Schäden und die Schadensbewältigung reduzieren und ist daher auch volkswirtschaftlich lohnend.

- **Beispiel Trinkwassernotversorgung:** Aufgrund fehlender Haushaltsmittel ist die Trinkwassernotversorgung beziehungsweise die Ertüchtigung von Notbrunnen nach wie vor in der Konzeptphase.

> *Bei der Umsetzung des Klimaschutzgesetzes ist es an den thematisch beteiligten Ministerien, im Rahmen von Ordnungsrecht und zur Verfügungstellung von Fördermitteln, die jetzt absehbaren Umsetzungsschritte aufzunehmen und für die nächsten Jahre weiterzuentwickeln. Dies muss in einer Beschlusslage des Bundestages manifestiert werden. Da die Sicherheitslage, wie das GRÜNBUCH zeigt, nicht nur aufgrund des Klimawandels volatil ist, ist es auch hier erforderlich, erste Umsetzungsmaßnahmen noch in dieser Wahlperiode festzuschreiben und finanziell sowie organisatorisch zu unterlegen."* ***– Susanne Mittag MdB***

Schwerpunkt: Forschung

Forschungsfragen zur Krisenbewältigung: Die Auswirkungen des Klimawandels auf die Öffentliche Sicherheit sind angesichts des zu erwartenden Umfangs und bisher kaum erforschter Tiefe nur bedingt abzusehen. Einige zentrale Fragestellungen, die durch zukünftige Forschung untersucht werden sollten, werden im Folgenden aufgelistet. Im Kern geht es hierbei um eine differenzierte Analyse, aus der Maßnahmen abgeleitet werden können, die die Auswirkung der Krise verringern und die Bewältigungsmöglichkeiten verbessern.

Welche sicherheitsrelevanten Bereiche (Kritische Infrastrukturen, vor allem Wasserversorgung, Stromversorgung, Transport, Lebensmittelversorgung) sind durch Hitze oder Dürre betroffen?

- Welche kaskadierenden Effekte (auch unter Einbeziehung einer europäischen und globalen Perspektive) sind frühzeitig zu erkennen, um präventive Maßnahmen einzuleiten?
- Wie sind diese Bereiche auf den Eintritt der Katastrophe vorbereitet? Welche Notfallpläne bestehen lokal, regional, auf Bundesebene und für Europa (oder darüber hinaus)?
- Wie kann die Aufgaben- und Lastenverteilung bei großflächigen klimabedingten Lagen (unter anderem Hitze und Dürren) zwischen Ländern und Bund geregelt werden?
- Welche rechtlichen und ökonomischen Vorkehrungen sind zu treffen, die in der Situation schnell und zielgerichtet eingesetzt werden können?
- Welche Möglichkeiten der europäischen Kooperation zur Bewältigung einer Hitze- oder Dürrelage (oder vergleichbarer Lagen) bestehen oder sind zu entwickeln?

Welche gesellschaftlichen Gruppen sind von dem Hitze-Dürre-Szenario besonders betroffen? Was kann zur Steigerung deren Resilienz von diesen selbst und von anderen getan werden?

- Wie kann die Bevölkerung durch Information und Warnung auf das Szenario vorbereitet werden?
- Inwieweit muss eine systematische Vorbereitung auf derartige Krisenereignisse in der Gesellschaft verortet werden (beispielsweise in Bildungseinrichtungen)?

Welche sozialen Konflikte sind durch Ressourcenknappheit und Verteilungsprobleme zu erwarten? Welche Maßnahmen zur Konfliktentschärfung und -bewältigung sind zu ergreifen?

- Wie kann der gesellschaftliche Diskurs über Verteilungsgerechtigkeit bei knappen Ressourcen präventiv gestaltet werden?
- Welche sozialen Konflikte sind aufgrund einer klimabedingten Migration zu erwarten, und wie kann damit umgegangen werden?

Wie ist die materielle und personelle Leistungsfähigkeit der Behörden und Organisationen mit Sicherheitsaufgaben (BOS) im Falle eines Hitze-Dürre-Szenarios?

- Entspricht deren materielle Ausstattung den Notwendigkeiten zur Lagebewältigung?
- Wie gut sind sie personell aufgestellt und durch Ausbildung und Übungen darauf vorbereitet?
- Wie ist die Motivation beziehungsweise Einsatzbereitschaft der Angehörigen der BOS in einer derartigen Situation aufrechtzuerhalten?

Inwieweit können private Anbieter (etwa private Rettungsdienste, Pflegedienste) in die staatlichen Strukturen zur Bewältigung von Krisenlagen eingebunden werden?

Wie können die Analysen und Konzepte bezogen auf das Szenario Hitze/Dürre, die in unterschiedlichen Disziplinen und Ländern entwickelt wurden und werden, strukturiert und systematisch zusammengeführt werden?

Forschung zu Prävention und Vorhersage – Schwerpunkt Landwirtschaft:

Die Auswirkungen des Klimawandels auf die Landwirtschaft und damit auf Wasserverfügbarkeit und Erzeugerpreise sind angesichts des zu erwarteten Umfangs und bisher kaum erforschter Tiefe nur bedingt abzusehen.[34]

Entscheidend werden die weitere Entwicklung und der Betrieb saisonaler Wettervorhersagesysteme sein. Diese dienen sowohl als Grundlage für akute Warnungen über mehrere Monate im Voraus, als auch für die langfristige Anpassung. Die Entwicklung von Dürren oder extremen Niederschlagsperioden können abgeschätzt und es können im Vorfeld Schutzmaßnahmen ergriffen werden, um die Vulnerabilität zu reduzieren und Adaptionsmaßnahmen zu optimieren. Dazu müssen die Ensemblevorhersagesysteme auf kleine Skalen im Kilometerbereich heruntergebrochen werden, um bestmögliche Aussagen für einzelne Regionen treffen zu können.

Insbesondere fehlen Robustheitsanalysen, wie die mittelfristige Anpassungsfähigkeit der deutschen Landwirtschaft in Zukunft gestärkt werden könnte, indem etwa Sortenwahl und Betriebszweige neu ausgerichtet, die Maschinenausstattung angepasst und womöglich Bewässerungsstrategien erwogen werden. Derartige Robustheitsanalysen mit einzelbetrieblicher, agrarökonomischer Bewertung ließen sich mit den jetzt verfügbaren Höchstleistungsrechnern berechnen. Sie erfordern jedoch ein validiertes bioökonomisches Modellsystem mit feiner räumlicher Auflösung sowie agrar- und naturwissenschaftliche Expertise.

Um die Anpassungsstrategien effektiv umsetzen zu können, ist ein intensiver Dialog mit Vertreterinnen und Vertretern der landwirtschaftlichen Praxis erforderlich, einschließlich der Berufsverbände (Bauernverbände, Deutsche Landwirtschafts-Gesellschaft) sowie der im Bereich Beratung und Ausbildung relevanten Akteurinnen und Akteure (Ministerien, Landwirtschaftsämter und Kammern). Hierzu wird Forschung zur Etablierung von sogenannten Innovationsplattformen benötigt, um die Forschungsergebnisse gemeinsam mit der landwirtschaftlichen Praxis, den Berufsverbänden, Landwirtschaftskammern, Ministerien sowie der interessierten Öffentlichkeit teilen und umsetzen zu können.

34 Siehe auch: BT Drs. 19/9521, Seite 12, wonach es gegenwärtig „einen Mangel an Forschungsarbeiten und empirischen Daten, anhand derer die Auswirkungen auf Ernteerträge und -qualitäten sowie auf die Tierhaltung bei Dürre/Hitze belastbar abgeleitet werden können“ gibt.

3 Epidemien, Pandemien – Eskalierende Ausbrüche gefährlicher Infektionskrankheiten – Status quo, Szenarien, Leitfragen, Handlungsempfehlungen

3.1 Einführung

Die Megatrends der Globalisierung und die damit verbundene enge Vernetzung begünstigen den Ausbruch von Pandemien. Durch die stark gestiegene globale Mobilität hat die Verbreitungsgeschwindigkeit von Erregern zugenommen. Beispielhaft sind die – teils unbemerkte – Ausbreitung von SARS-CoV-2, aber auch des SARS-Erregers im Jahre 2002/2003 innerhalb weniger Wochen auf allen Kontinenten. In der hypervernetzten Welt herrschen optimale Bedingungen für die rasche Entwicklung von Infektionskrankheiten. Gleichzeitig kann die Zerstörung von Ökosystemen die Ausbreitung von Infektionskrankheiten und Pandemien begünstigen. Die Übertragung von Erregern aus dem tierischen Bereich auf den Menschen (sogenannte Zoonosen) ist wissenschaftlich dokumentiert. Das Risiko ist damit allgegenwärtig und zu berücksichtigen. Dies alles stellt eine beträchtliche Gefahr für die Volkswirtschaft, den materiellen Wohlstand und die allen Menschen zugänglichen öffentlichen Güter wie Gesundheitsversorgung und Öffentliche Sicherheit dar. Eine Begrenzung der Ausbreitung kann nur durch schnelles regionales Handeln erreicht werden.

Die deutsche Volkswirtschaft ist in hohem Maße von der Funktionsfähigkeit des globalisierten Marktes abhängig. Fallen systemrelevante Produktions- und Lieferwege weg, fallen Arbeitskräfte in hoher Zahl krankheits- oder quarantänebedingt aus, kommen Unternehmen zum Stillstand, wird der Alltag quasi zum Erliegen gebracht. Dann ist von bisher unvorstellbaren ökonomischen und gesellschaftlichen Folgen auszugehen. Pandemien haben das Potenzial, das Vertrauen in die demokratischen Institutionen nachhaltig zu erschüttern, insbesondere bei unzureichender Krisenkommunikation und unzureichendem Krisenmanagement. Dieses Worst-Case-Szenario gilt es, mit allen geeigneten Mitteln zu verhindern.

3.2 Ausgangslage und Herausforderungen

Neuartige Erreger können auch nach Deutschland gelangen und flächendeckend die Bevölkerung gefährden. Dies belegt die Pandemie durch den Erreger SARS-CoV-2 im Erscheinungsjahr dieser GRÜNBUCH-Ausgabe eindrücklich. Ein eskalierender Ausbruch stellt das deutsche Gesundheitssystem, Politik und Wirtschaft vor immense Herausforderungen, die mit erheblichen wirtschaftlichen Folgekosten einhergehen.[35]

Falls eine Eindämmung nicht gelingt, kann dies zu einem, mit kaum vorstellbaren gesellschaftlichen und politischen Konsequenzen verbundenen, wirtschaftlichen Zusammenbruch führen. Gleichzeitig müssen die gesellschaftlichen und sozialen Folgen durch die zu ergreifenden Maßnahmen sorgsam mit dem Ziel der Infektionseindämmung abgewogen werden.

Es müssen frühzeitig Maßnahmen ergriffen werden, um die Ausbreitung zu stoppen. Je früher und zielgenauer das geschieht, desto geringer ist die Wahrscheinlichkeit schwerer gesellschaftlicher und wirtschaftlicher Verwerfungen. Dabei sind frühzeitige Identifikation von Verdachtsfällen sowie adäquater Umgang mit Kontaktpersonen essenziell. Es muss davon ausgegangen werden, dass der Erreger Deutschland zu einem Zeitpunkt erreicht, an dem international weder Medikamente zur Behandlung, noch ein Impfstoff zur Verfügung stehen.

Oberstes Ziel ist es, eine Überforderung des Gesundheitssystems und den Tod zahlreicher Menschen zu verhindern, wie es zum Beispiel bereits in der Risikoanalyse zum Bevölkerungsschutz 2012 dargestellt wird.[36] Dies erfordert ein effektives Zusammenwirken aller im Gesundheitswesen und in der Gefahrenabwehr beteiligten Akteurinnen und Akteure. Die dafür erforderlichen gesetzlichen Regelungen und Maßnahmenplanungen müssen ergänzt

35 Vgl. dazu: Weissbuch 2016 zur Sicherheitspolitik und zur Zukunft der Bundeswehr; Bundesministerium der Verteidigung (Hrsg.)

36 Bundestagsdrucksache 17/12051 (Unterrichtung durch die Bundesregierung: Bericht zur Risikoanalyse im Bevölkerungsschutz 2012) in einer Fallkonstellation mit „Pandemie durch Virus Modi-SARS“

werden. Weiterhin fehlen die Kapazitäten und Ressourcen, insbesondere Beatmungsplätze für intensivpflichtige Patientinnen und Patienten und Schutzausrüstung für medizinisches und pflegerisches Personal in Arztpraxen und Kliniken, anderen stationären und ambulanten Einrichtungen, für Pflegedienste und Behörden, so dass die erforderliche Daseinsvorsorge zur Abwehr eskalierender Infektionskrankheiten nicht ausreichend gegeben ist. Die Akteurinnen und Akteure im Gesundheitswesen (zum Beispiel niedergelassene Ärztinnen und Ärzte, Krankenhäuser, Gesundheitsämter und Apotheken) müssen gemeinschaftlich Maßnahmenplanungen durchführen, trainieren und kontinuierlich fortschreiben sowie mit den kommunalen Gefahrenabwehrbehörden harmonisieren. Nur auf dieser Grundlage können die agierenden Entscheidungsträgerinnen und -träger wirkungsvoll handeln. Um in der Begrenzung der Ausbreitung effektive Maßnahmen umsetzen zu können, müssen Wirkmechanismen einzelner Maßnahmen bekannt sein, etwa verschiedene Strategien zur Eindämmung von Infektionen. Hier besteht noch Forschungsbedarf, um optimale Handlungsoptionen aufzuzeigen.

3.3 Bestehende und neue Risiken

Durch die Pest wurde etwa ein Drittel der damaligen Weltbevölkerung ausgelöscht, ganze Regionen wurden entvölkert. Als folgenschwerste Pandemie der Moderne ist die so genannte Spanische Grippe in die Geschichte eingegangen. Entgegen einer Letalität bei herkömmlicher Influenza von etwa 0,1 Prozent lag die Mortalitätsrate der Spanischen Grippe bei 2,5 Prozent. Die Spanische Grippe trat in drei, sich teilweise überlagernden Wellen auf. Nach einer genetischen Mutation brach fast zeitgleich in Frankreich, Spanien, dem afrikanischen Kontinent, Indien und den Vereinigten Staaten von Amerika eine zweite, schwerere Welle in Kombination mit Bronchopneumonien[37] auf. Die dritte und letzte Welle war von sehr unterschiedlichen Krankheitsbildern und Verläufen geprägt. Bis Mitte der 1920er Jahre kam es immer wieder zu Neuinfektionen. Das öffentliche Leben kam während der Pandemie in vielen Städten zum Erliegen. Der öffentliche Nahverkehr, Fernverkehrsverbindungen und der Postbetrieb wurden teilweise eingestellt. Viele Schulen blieben in Deutschland geschlossen. Der Personalausfall in Bergwerken, Fabriken und der Landwirtschaft führte zu einer empfindlichen Störung bei der Herstellung wichtiger Produkte und Nahrungsmittel. Exakte Angaben zu den Opferzahlen liegen nicht vor. Aktuelle Berechnungen gehen von fast 50 Millionen Toten aus[38]. Die tatsächlichen Zahlen könnten noch höher liegen.

Im Grünbuch des Zukunftsforums Öffentliche Sicherheit (ZOES) vom September 2008 wurden potenzielle Risiken und Effekte einer Influenza-Pandemie thematisiert. Weiterhin wurde darauf hingewiesen, dass infolge der klimatischen Änderungen die Ausbreitung von Vektoren (zum Beispiel Gelbfiebermücke, Aedes aegypti) auch in Deutschland zu erwarten ist und sich somit tropische Krankheiten auch in unseren Regionen verbreiten können. Es ist zu beobachten, dass schon jetzt potenzielle Vektoren in unseren Regionen Lebensbedingungen finden, die eine massive Ausbreitung möglich erscheinen lassen.

Das ZOES greift diese Thematik erneut auf, da die Behandlung einer Vielzahl von gleichzeitig hospitalisierten Patientinnen und Patienten weiterhin nicht hinreichend gewährleistet werden kann. Die Betrachtungen beziehen sich auf Mensch-zu-Mensch-Übertragung, die Ausbreitung über Lebensmittel oder bioterroristische Angriffe und erfolgen dabei unabhängig von spezifischen Erregern.

Mit der Mensch-zu-Mensch-Übertragung einer Infektionskrankheit ist eine rasante Eskalation möglich. Neben den Erfordernissen der medizinischen Versorgung müssen Maßnahmen zur Begrenzung der weiteren Verbreitung getrof-

37 Bakterielle Lungenentzündungen, die mit Antibiotika zu behandeln sind

38 Laura Spinney: 1918 – Die Welt im Fieber: Wie die Spanische Grippe die Gesellschaft veränderte, Seiten 198 ff.

fen werden. Dies trifft bei der Ausbreitung über Lebensmittel gleichermaßen zu. Die Identifizierung von erregerbehafteten Lebensmitteln kann mehrere Tage in Anspruch nehmen und ist nicht immer eindeutig.

Mit bioterroristischen Angriffen können sowohl eine direkte Mensch-zu-Mensch-Übertragung als auch eine Verseuchung von Lebensmitteln erfolgen. Die möglichen Ursachen für einen eskalierenden Ausbruch einer gefährlichen Infektionskrankheit stehen in diesem Beitrag nicht im Fokus der Betrachtungen. Es wird insbesondere dargestellt, welche Maßnahmen umgesetzt werden müssen, um eine Vielzahl erkrankter Menschen zeitgerecht zu versorgen und die weitere Ausbreitung zu begrenzen.

Seit Ende der 1990er Jahre rücken Gesundheitsthemen verstärkt in den Zusammenhang von Sicherheit und Stabilität und halten Einzug in grundlegende Strategiedokumente, wie dem Weißbuch der Bundesregierung zur Sicherheitspolitik und zur Zukunft der Bundeswehr[39] von 2016.

Die Bewältigung einer großen Gesundheitslage „Pandemien und Infektionskrankheiten“ zählt zu den Herausforderungen auch für die deutsche Sicherheitspolitik[40]. Die Münchner Sicherheitskonferenz beschäftigte sich mehrfach mit gesundheitspolitischen Themen.

Um eskalierende Infektionsausbrüche bewältigen zu können, bedarf es detaillierter Maßnahmenplanungen. Entscheidungen müssen in Kenntnis effektiver Wirkmechanismen zur Begrenzung der Ausbreitung und der Versorgung erkrankter Patientinnen und Patienten getroffen werden. Die im Gesundheitswesen beteiligten Akteurinnen und Akteure, wie zum Beispiel

- ambulant kassen- und privatärztlich tätige Ärztinnen und Ärzte
- Krankenhäuser
- Gesundheitsämter
- Diagnose- und Therapieeinrichtungen
- ambulante und stationäre Pflegeeinrichtungen
- Rettungsdienst (Notfallrettung und qualifizierter Krankentransport)
- Feuerwehr
- Apotheken und Einrichtungen der Arzneimittel- sowie Medizinprodukteversorgung
- Einheiten des Zivil- und Katastrophenschutzes
- Polizei

mit ihren jeweils vorhandenen Kapazitäten müssen harmonisiert und diese Ressourcen müssen koordiniert zur Wirkung gebracht werden. Ein signifikantes Beispiel in der COVID-19-Pandemie ist die Versorgung mit Medizinprodukten und insbesondere Verbrauchsmaterial zum Infektionsschutz. Für ein gutes Zusammenwirken der Beteiligten ist zwingend erforderlich, dass die Maßnahmenplanung auf der Basis klarer Regelungen erfolgt, koordiniert umgesetzt, kontinuierlich fortgeschrieben und regelmäßig in gemeinsamen Übungen trainiert wird.

39 Bundesregierung (Hrsg.), WEISSBUCH Zur Sicherheitspolitik und zur Zukunft der Bundeswehr, 2016, Seiten 34 - 44

40 Stahlhut, B.: Bedrohungseinschätzung des Weißbuches 2016 – Wie passt Gesundheit und Sicherheit zusammen in: Lüder S, Stahlhut B. (Hrsg.), Konturen einer Gesundheits-Sicherheitspolitik, Berliner Wissenschafts-Verlag (2018), Seite 128

Szenario Mensch-zu-Mensch-Übertragung

Die grundlegenden, systembedingten Herausforderungen im Bereich eskalierender Infektionskrankheiten werden nachfolgend am Beispiel der Mensch-zu-Mensch-Übertragung dargestellt.

Unzureichende Versorgungsstrukturen:

Die Gesamtverteidigungsrichtlinie 1989[41] kommt zum Ergebnis, dass das weitgehend auf die Normalversorgung im Frieden ausgerichtete Gesundheitswesen den Anforderungen eines Massenanfalls von Patientinnen und Patienten nicht rechtzeitig Rechnung tragen könne. Diese Feststellung bestätigt sich in einem dem Deutschen Bundestag 2013 durch die Bundesregierung zugeleiteten Szenario einer hypothetischen Pandemie durch ein fiktives Virus Modi-SARS, die mit mindestens 7,5 Millionen Toten in Deutschland einhergeht[42].

Auch die Erkenntnisse aus den jährlichen saisonalen Grippewellen sowie die Erfahrungen aus der EHEC-Epidemie[43] in Norddeutschland (2011) und nicht zuletzt die noch bestehende Pandemie von COVID-19 belegen, dass die im Gesundheitswesen zur Bekämpfung einer größeren Gesundheitslage vorhandene strukturelle Basis und die Kapazitäten unzureichend sind. Dies wirft die Frage auf, welches Ministerium auf Ebene des Bundes für alle Fragestellungen der Gesundheitssicherheit zuständig ist. Trotz seines Namens kann es nicht allein das Bundesministerium für Gesundheit (BMG) sein, zumal die Bekämpfung einer Pandemie neben rein gesundheitlichen auch verfassungsrechtliche, wirtschaftliche und soziale Fragen aufwirft.

Das derzeitige Gesundheitswesen berücksichtigt den gesundheitlichen Bevölkerungsschutz nur unzureichend. Die Regelungen im Sozialgesetzbuch V (SGB V) beziehen sich auf das Verhältnis der gesetzlichen Krankenversicherung zu Leistungsempfängern und Leistungserbringern und berücksichtigen besondere Situationen bei einem Massenanfall von Verletzten oder Erkrankten nur ungenügend.

Der Sachverständigenrat zur Begutachtung der Entwicklung im Gesundheitswesen (SVR) soll laut § 142 SGB V „unter Berücksichtigung der finanziellen Rahmenbedingungen und vorhandener Wirtschaftlichkeitsreserven Prioritäten für den Abbau von Versorgungsdefiziten und bestehenden Überversorgungen und […] Möglichkeiten und Wege zur Weiterentwicklung des Gesundheitswesens“ aufzeigen. Insbesondere in den Gutachten „Bedarfsgerechte Versorgung – Perspektiven für ländliche Regionen und ausgewählte Leistungsbereiche“[44] (vorgelegt 2014) und „Bedarfsgerechte Steuerung der Gesundheitsversorgung“[45] (vorgelegt 2018) formuliert der SVR Empfehlungen. Zu beobachten ist, dass viele dieser Empfehlungen zu gesetzgeberischem Handeln führten.

Der Vorsitzende des Sachverständigenrates Gesundheit hält die derzeitige Diskussion um die Notfallversorgung für zu eingeschränkt. Es wurde betont, dass das wichtige Thema Großschadensereignisse (wie zum Beispiel Terrorlagen) im Rahmen der Analysen und Empfehlungen zur Reform der Notfallversorgung bislang kaum beachtet wurde. Dies weist erneut auf ein gravierendes Schnittstellenproblem hin, da hier fachlich und regulatorisch unterschiedliche Welten, insbesondere gewerblich tätige Krankenhäuser, Katastrophenschutz, Rettungsdienst, Feuerwehr und Polizei, aufeinanderstoßen, die bisher vielfach eher auf ihre Eigenständigkeit bedacht sind. Von einer integrativen Kultur des nahtlosen Miteinanders von Gefahrenabwehr

41 Vgl. dazu Bundesminister des Innern (Hrsg.), Rahmenrichtlinie für die Gesamtverteidigung – Gesamtverteidigungsrichtlinie – vom 10. Februar 1989, Seite 26.

42 Drucksache 17/12051

43 EHEC, enterohämorrhagische Escherichia coli. Viele Patienten litten zusätzlich unter dem hämolytisch-urämischen Syndrom (HUS) und benötigten Dialyse

44 Bedarfsgerechte Versorgung – Perspektiven für ländliche Regionen und ausgewählte Leistungsbereiche; Sachverständigenrat zur Begutachtung der Entwicklung im Gesundheitswesen; 2014

45 Bedarfsgerechte Steuerung der Gesundheitsversorgung; Sachverständigenrat zur Begutachtung der Entwicklung im Gesundheitswesen; 2018

und Gesundheitswesen sind wir in Deutschland leider noch weit entfernt[46].

Der Beschluss des Gemeinsamen Bundesausschusses (G-BA) vom 19.04.2018 zu den stationären Notfallstufen (siehe Abbildung 1) basiert auf den Empfehlungen des SVR.

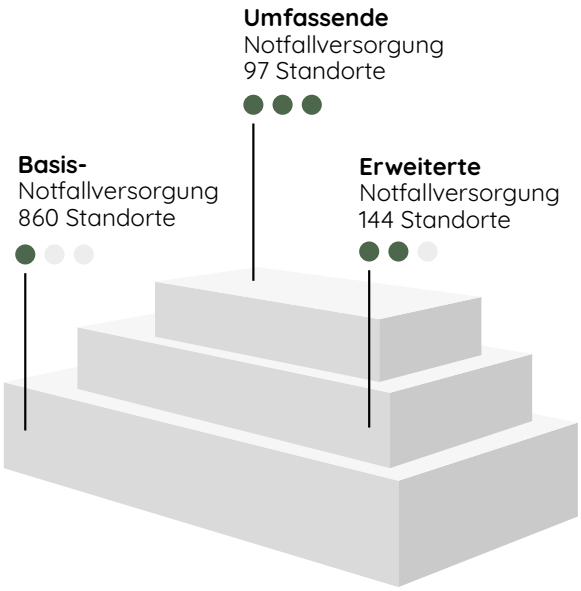


Abbildung 1: Prinzipielle Darstellung der geplanten stationären Notfallstufen

Gesundheitssicherheit erfordert Vorsorge. Die in Abbildung 1 dargestellte künftige Struktur der stationären Notfallstufen berücksichtigt nur unzureichend die erforderlichen kapazitiven Vorhaltungen zur Bewältigung eines eskalierenden Ausbruchs einer Infektionskrankheit, deren adäquate Bereitschaftsplanung und Evaluierung, kontinuierliches Training und Übung. Kurz: Investitionen in Vorhaltung, Planung und Übung. Gesundheitssicherheit erfordert insbesondere klare und schnell anzuwendende Rechtsgrundlagen, schnelle Entscheidungen sowie die Bereitstellung ausreichender Finanzmittel.

Defizite in Vorsorge, Kooperation und Aktivierung:

Problematisch ist hier, dass es keine permanente sektorübergreifende Abstimmung auf Bundesebene zwischen dem Bundesministerium des Innern, für Bau und Heimat (BMI), dem Bundesministerium für Gesundheit (BMG) sowie den nachgeordneten Behörden und der Selbstverwaltung des Gesundheitswesens, insbesondere Spitzenverband der gesetzlichen Krankenkassen, Kassenärztliche Bundesvereinigung, Deutsche Krankenhausgesellschaft und dem Gemeinsamen Bundesausschuss, gibt. Es fehlt somit eine Gewährleistung dafür, dass die Vorsorgemaßnahmen von Bund, Ländern und allen weiteren Akteuren im Gesundheitswesen verzahnt und ohne Lücken sind. Erforderliche Konzepte müssen gemeinschaftlich erarbeitet, kontinuierlich harmonisiert, fortgeschrieben und hinreichend finanziert werden. Derzeit gibt es keine ständig und stetig gepflegte Kooperation mit den Eigentümerinnen und Eigentümern und Betreiberinnen und Betreibern von Behandlungseinrichtungen.

Eine umfassende Notfallversorgung im Falle eines eskalierenden Ausbruchs einer Infektionskrankheit ist nicht auf freiwilliger Basis sicherzustellen, sondern ist im Rahmen der Daseinsvorsorge zwingend geboten. Sie bedarf gemeinsamer Planung zwischen Bundes-, Landes- und kommunalen Gesundheitsbehörden und allen weiteren Beteiligten des Gesundheitswesens, deren kontinuierliche Anpassung an Veränderungen sowie einer gesicherten Finanzierung.

Etablierte Maßnahmenplanungen, Führungsorganisation und Handlungsabläufe im Bereich der Gefahrenabwehr sind auf die Bewältigung klassischer Großschadensereignisse ausgerichtet. Sie treffen auf ein Gesundheitswesen, dessen Ressourcen ausschließlich auf die Bewältigung des Alltags ausgerichtet sind und auch hier schon mancherorts an seine Grenzen stößt. Hinzu kommt auch, dass die örtlichen und

46 iX-Highlights 50. KW 2019 Seite 6, Hrsg. iX - Institut für Gesundheitssystem-Entwicklung,

fachlichen Grenzen regional unterschiedlich organisiert sind. Um das Ziel zu erreichen, den eskalierenden Ausbruch einer Infektionskrankheit frühzeitig zu stoppen und Todesfälle auf ein Minimum zu begrenzen, müssen hier gemeinschaftliche Maßnahmenplanungen umgesetzt, kontinuierlich fortgeschrieben und in Übungen auf regionaler Ebene trainiert werden. Die wenigen bisher durchgeführten Übungen zeigen, dass auftretende Ressourcenprobleme unterschätzt werden[47]. Dies lässt vermuten, dass Planungen, die weitgehend ohne direkte Beteiligung des Gesundheitswesens erstellt werden, teilweise unrealistisch sind. Das gilt beispielsweise für die vorzeitige Entlassung von Patientinnen und Patienten, um in nennenswertem Umfang zusätzlich Behandlungskapazitäten zu schaffen.

Kapazitäten können derzeit nur dadurch erreicht werden, indem medizinisch notwendige, geplante Behandlungen auf einen unbestimmten Zeitpunkt verschoben werden müssen. Die Erfahrungen der Good Practice während der laufenden Corona-Pandemie müssen wissenschaftlich ausgewertet, optimiert und für zukünftige Ereignisse weiterentwickelt werden. Es kommt darauf an, dass sich die Einrichtungen des Gesundheitswesens frühzeitig auf den neuartigen Erreger einstellen, ihre Behandlungskapazitäten darauf ausrichten und Maßnahmen ergreifen, um infizierte Personen nicht in Kontakt mit „normalen“ Erkrankten zu bringen.

Da die wirtschaftliche Grundlage der Einrichtungen des Gesundheitswesens auf der Abrechnung einzelner Leistungen mit den Krankenkassen basiert und die gesetzlichen Grundlagen keine über den alltäglichen Bedarf hinausgehende Finanzierung, insbesondere von materiellen Vorhaltungen, Aus- und Fortbildung sowie entsprechendem Training vorsehen, muss die Finanzierung neu geregelt werden.

Die letzte und auch einzige länderübergreifende Krisenkommunikationsübung (LÜKEX 2007), die sich mit einer Influenza-Pandemie befasste, liegt nunmehr bereits 13 Jahren zurück. Neue Regelungen, wie der nationale Pandemieplan[48] sowie die Allgemeine Verwaltungsvorschrift über die Koordinierung des Infektionsschutzes in epidemisch bedeutsamen Fällen[49] waren bisher nicht Bestandteil von entsprechenden regionalen oder überregionalen Übungen. In diesem Zusammenhang muss darauf hingewiesen werden, dass Erfahrungsberichte von Übungen nicht nachhaltig ausgewertet werden können, wenn sie aufgrund einer Einstufung nur wenigen ausgewählten Akteurinnen und Akteuren zugänglich sind.

Ein eskalierender Ausbruch einer Infektionskrankheit erfordert eine umfassende Risikobetrachtung, die alle Bereiche des Gesundheitswesens und der Gefahrenabwehr einbezieht. Eine intensive Zusammenarbeit mit den Akteurinnen und Akteuren im Gesundheitswesen und der Gefahrenabwehr auf kommunaler Ebene findet derzeit kaum statt. Es fehlen auch entsprechende gesetzliche Regelungen, welche die Akteurinnen und Akteuren des Gesundheitswesens verpflichten, Maßnahmenplanungen durchzuführen, fortzuschreiben, in Übungen zu trainieren und deren Finanzierung sicherzustellen. Lediglich in einzelnen Ländern wie beispielsweise Berlin werden regelmäßig Übungen mit den Krankenhäusern durchgeführt. Diese haben zu einer Optimierung vieler Detailprozesse in den Krankenhäusern und zur Harmonisierung mit den Gefahrenabwehrbehörden, insbesondere dem Rettungsdienst, geführt.

Die medizinische Versorgung von Patientinnen und Patienten bei einem eskalierenden Ausbruch einer Infektionskrankheit betrifft in den Krankenhäusern insbesondere den kritischen Bereich der Intensivversorgung. Detailliertere Daten zu bettenführenden Bereichen

47 Auswertungsbericht der dritten länderübergreifenden Krisenmanagementübung, LÜKEX 2007, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

48 Nationaler Pandemieplan Teil I; Strukturen und Maßnahmen; Robert Koch-Institut; 2017 und Teil II, Wissenschaftliche Grundlagen; Robert Koch-Institut; 2016

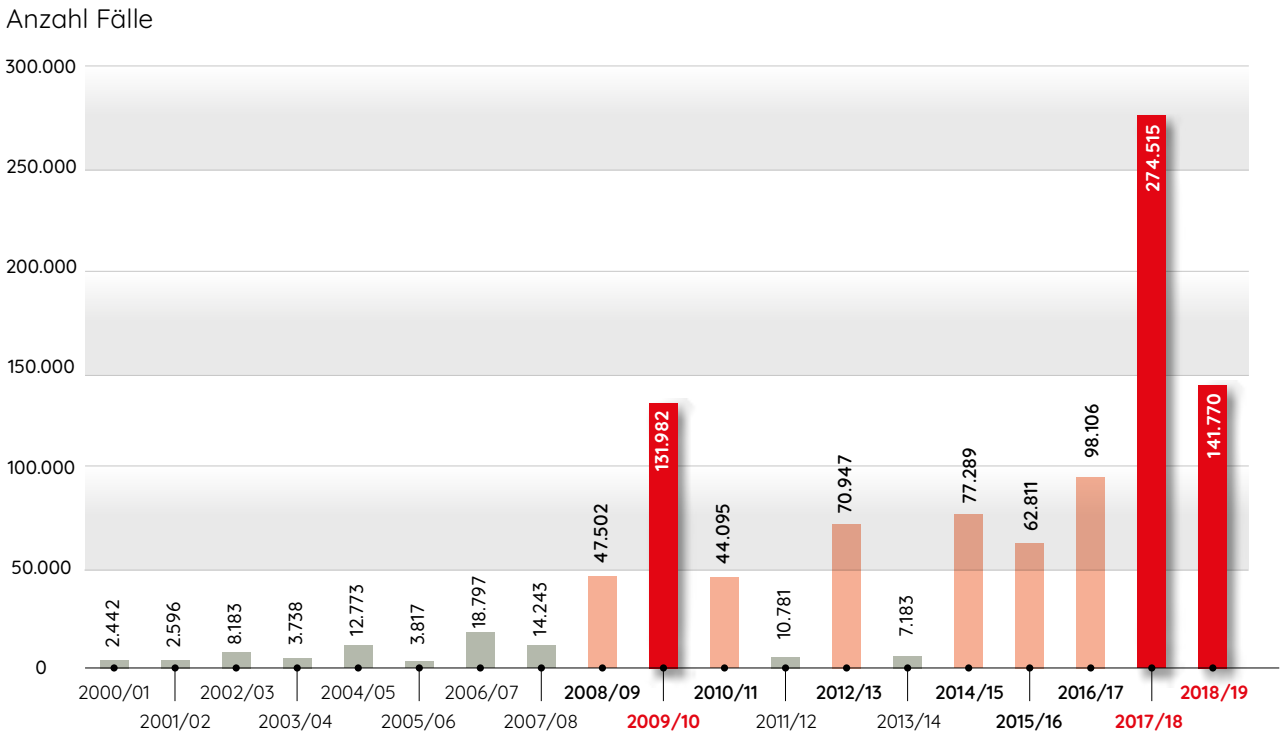
49 Allgemeine Verwaltungsvorschrift über die Koordinierung des Infektionsschutzes in epidemisch bedeutsamen Fällen (Verwaltungsvorschrift-IfSG-Koordinierung – IfSGKoordinierungs-VwV): 2013

beziehungsweise spezifischen Versorgungsbereichen, in denen Patientinnen und Patienten versorgt werden können, die aufgrund der Schwere ihrer Erkrankung einer ständigen Überwachung und/oder therapeutischen Intervention bedürfen, gibt es üblicherweise nicht. Das betrifft zum Beispiel Intensivstationen mit Beatmungsmöglichkeiten, Intermediate Care, Stroke Units sowie spezielle intensivmedizinische Überwachungs- und Behandlungseinheiten wie neonatologische Intensivversorgung oder kardiologische Überwachungseinheiten.

Dass hohe Zahlen von erkrankten Infektionspatienten auch innerhalb Deutschlands allein auftreten können, zeigt Abbildung 2. Im Winter 2017/2018 traten doppelt so viele saisonale Influenza-Patienten auf, wie während der internationalen Influenza-Pandemie in 2009.

Abbildung 2: Influenza-Patienten pro Jahr in Deutschland [50]

Deutschland verfügt über umfassend ausgebaute Systeme der Notfallversorgung in ambulanten und stationären Einrichtungen sowie über ein ebenfalls gut etabliertes Rettungswesen. Bei einem eskalierenden Ausbruch einer Infektionskrankheit sind alle drei Versorgungsbereiche betroffen. Die medizinische Versorgung von Infektionspatientinnen und -patienten betrifft insbesondere Praxen von Allgemeinärztinnen und Allgemeinärzten, Internistinnen und Internisten, HNO-Ärztinnen und HNO-Ärzten, Pädiaterinnen und Pädiatern sowie in Krankenhäusern insbesondere den Bereich der internistischen Intensivversorgung. Trotz des insgesamt moderaten Verlaufs der Influenzapandemie (Erregertyp H1N1) im Jahr 2009 waren die Behandlungsplätze für extrakorporale Membranoxygenierung (ECMO) durch schwer erkrankte Patientinnen und Patienten zeitweise vollständig ausgelastet. Das Gesundheitssystem ist nur aufgrund des moderaten Krankheitsverlaufs nicht zusammengebrochen. Aggressivere Influenza-Viren oder andere Infektionskrankheiten, die eine höhere Frequenz von stationär zu behandelnden oder von intensivpflichtigen



50 Quelle: Robert Koch-Institut: SurvStat@RKI 2.0, https://survstat.rki.de, Abfragedatum: 26.09.2019

Patienten verursachen – wie im Falle des COVID-19-Erregers SARS-CoV-2 offensichtlich –, könnten zum Zusammenbruch des Gesundheitssystems führen[51].

Bedarf spezifischer Planungen:

Dieses Ergebnis wird in der bereits genannten Bundestagsdrucksache 17/12051 (Unterrichtung durch die Bundesregierung: Bericht zur Risikoanalyse im Bevölkerungsschutz 2012) in einer Fallkonstellation mit „Pandemie durch Virus Modi-SARS“ beschrieben. In der Simulation wird festgestellt, dass in der ersten Welle (Tag 1 bis 411) insgesamt 29 Millionen Menschen in Deutschland erkranken könnten, im Verlauf der zweiten Welle (Tag 412 bis 692) insgesamt 23 Millionen Menschen und während der dritten Welle (Tag 693 bis 1052) insgesamt 26 Millionen Menschen. Für den gesamten zugrunde gelegten Zeitraum geht das Szenario von mindestens 7,5 Millionen Toten aus.

Durch einen eskalierenden Ausbruch einer Infektionskrankheit wird die Funktionalität aller einzelnen Versorgungsglieder nachhaltig gestört. Infolge der Vielzahl der gleichzeitig erkrankten Menschen können notwendige Instandsetzungen, Liefertermine, Produktions- und Versorgungsleistungen nicht in dem erforderlichen Umfang realisiert werden. Diese Einschränkungen der Funktionalität auf allen Ebenen verursacht zwangsläufig Wirkungen bezüglich der jeweiligen Kapazitäten[52]. Sie müssten somit infolge der Vielzahl von erkrankten Menschen nachhaltig gesteigert werden, etwa in der Logistik, in der Produktion wichtiger Güter, die in der Lage benötigt werden, oder in der Instandhaltung. Auf der Grundlage der internationalen sowie der nationalen Regelungen sind detaillierte Maßnahmenpläne in allen Instanzen der Versorgungskette auszuarbeiten und kontinuierlich fortzuschreiben. Dafür stehen internationale und nationale Normen, wie beispielsweise „Sicherheit und Schutz des Gemeinwesens; Aufrechterhaltung der Betriebsfähigkeit“ zur Verfügung.

Die etablierten Versorgungskapazitäten basieren bisher weitgehend auf den Anforderungen des täglichen Bedarfs. Um bei einem Massenanfall von Verletzten (MANV) infolge von Unglücksfällen reagieren zu können, sind Konzepte und Maßnahmenpläne etabliert, die eine kurzfristige Steigerung der Kapazität ermöglichen. Die dort fixierten Vorhaltungen im Rettungsdienst, im Katastrophenschutz und in der Krankenhaus-Alarm- und -Einsatzplanung sind in erster Linie an traumatologischen Notfällen orientiert. Beispielhaft seien der Terroranschlag vom 19. Dezember 2016 auf dem Breitscheidplatz in Berlin oder das Zugunglück von Bad Aibling am 9. Februar desselben Jahres genannt. Die Vorhaltungen für einen MANV sind für einen eskalierenden Ausbruch einer Infektionskrankheit nicht ausreichend und weder qualitativ noch quantitativ geeignet. Es muss geprüft werden, welche materiellen Ressourcen erforderlich sind, um eine wirksame Kapazitätssteigerung für die Versorgung intensivpflichtiger Patientinnen und Patienten auch in diesem Bereich zu etablieren.

Weiterhin ist bei der Mensch-zu-Mensch-Übertragung die Frage zu stellen, mit welchen Maßnahmen in das gesellschaftliche Leben eingegriffen werden muss, um die weitere Verbreitung zu begrenzen. Dies hat sich in der COVID-19-Pandemie als eine der zentralen Fragen ergeben und war im öffentlichen Diskurs nicht nur Gegenstand medizinischer, sondern auch wirtschaftlicher, sozialwissenschaftlicher oder verfassungsrechtlicher Betrachtungen. Das Infektionsschutzgesetz (IfSG) lässt eine Reihe von grundsätzlichen Möglichkeiten zu. Im nationalen Pandemieplan[53] wird festgestellt, dass die Studienlage begrenzt ist. Dies bedeutet, dass die Entscheidungsträgerinnen und Entscheidungsträger derzeit über keine ausreichend

51 Vgl. Bundestagsdrucksache 17/12051

52 Wurmb, Scholtes, Kolibay, Rechenbach, Kowalzik; Alarm- und Einsatzplanung im Krankenhaus: Die Vorbereitung auf Großschadenslagen; Anästhesiol Intensivmed Notfallmed Schmerzther; 2017; 52: 594-605; DOI 10.1055/s-0042-120230

53 Nationaler Pandemieplan Teil II, Wissenschaftliche Grundlagen; Seiten 107 ff

qualifizierten Informationen verfügen, welche Wirkung die einzelnen, potenziell begrenzenden, Maßnahmen zeigen und welche, auch verfassungsrechtlichen, sozialen und ökonomischen, Konsequenzen damit verbunden sein werden. Folglich können Entscheidungen bezüglich Maßnahmen nur situativ und auf Sicht getroffen werden, ohne deren voraussichtliche Wirkung valide vorhersagen zu können. Es ist darüber hinaus möglich und hat sich auch in der COVID-19-Pandemie in gewissem Maße bestätigt, dass regional unterschiedliche Maßnahmen angeordnet werden und kein bundesweit einheitliches Abwehrkonzept greift, wodurch individuell auf regional unterschiedliche Entwicklungen eingegangen werden kann.

In den Untersuchungen der Influenza-Pandemie 1918[54] in den Vereinigten Staaten wird gezeigt, dass eine konsequente Schließung der Schulen, Theater und sonstiger öffentlicher Veranstaltungen die Zahl der täglichen Neuerkrankungen deutlich reduzieren konnte. Der zeitliche Verlauf der Pandemie verlängert sich jedoch. Diese Studien erscheinen aufgrund der derzeitigen gesellschaftlichen Lebensformen in Deutschland nicht übertragbar oder repräsentativ. Gleichwohl ist es geboten, durch Forschung die potenziellen Maßnahmen bezüglich ihrer Wirksamkeit zur Begrenzung des Ausbruchs und den damit verbundenen gesellschaftlichen, sozialen und ökonomischen Effekten zu untersuchen. Es liegt auf der Hand, dass dies anhand des Verlaufs der COVID-19-Pandemie in Deutschland zeitnah und umfassend erfolgen sollte.

Bedeutung von Kommunikation und Selbsthilfe:

Ein eskalierender Ausbruch trifft auf eine Bevölkerung, die zwar das organisierte, professionelle Hilfeleistungssystem des Alltags kennt. Sie hat aber mit der Praxis von größeren Notfällen, Katastrophen und der damit einhergehenden Bewältigung im Rahmen der Selbst- und Fremdhilfe kaum Erfahrungen. Die Bevölkerung benötigt für solche Situationen besondere Handlungskompetenzen. Deshalb muss die Selbsthilfefähigkeit der Bevölkerung, zielgruppengerecht und an elementaren Handlungskompetenzen wie Hygienemaßnahmen, häuslicher Pflege und medizinischer Ersthilfe orientiert, in weitaus größerem Umfang als bisher gestärkt werden. Hierfür ist die in § 24 Zivilschutz- und Katastrophenhilfegesetz (ZSKG) angelegte Ausbildung der Bevölkerung in Erster Hilfe mit Selbstschutzinhalten und zu Pflegehilfskräften ein wichtiges Instrument.

Ferner muss die Bevölkerung umfassend über Gefahren und Folgen einer Pandemie unterrichtet werden. Wer Gefahren abwenden will, muss sie kennen. Die Bevölkerung muss nachvollziehen können, dass die Eindämmung einer Pandemie ein aktives Krisenhandeln des Staates erfordert und dieses Handeln für eine bestimmte Zeit die öffentlichen, beruflichen und privaten Kontakte jedes Einzelnen zum Wohle der Allgemeinheit einschränken kann. Die Bevölkerung muss auch auf Veränderungen in der medizinischen Versorgung vorbereitet werden.

54 The 1918 Influenza and its Modern-Day Implications, Federal Reserve Bank of St. Louis Re-view, March/April 2008, 90(2), pp. 75-93;

Weitere mögliche Szenarien

Über die Mensch-zu-Mensch-Übertragung hinaus gibt es zusätzliche Wege für die Verbreitung von Infektionskrankheiten, die einen dynamischen Verlauf nehmen können und erhebliche Risiken für die Bevölkerung bergen. Diese Ursachen sowie spezifische Prävention müssen jeweils stärker in Vorsorge und Gefahrenabwehr einfließen. Deshalb werden sie nachfolgend dargestellt.

Infektionskrankheiten durch Lebensmittel:

Auch wenn mit der Ausbreitung des Erregers SARS-CoV-2 weltweit eine für unsere Zeit einmalige Pandemie aufgetreten ist, sind doch trotzdem weitere Szenarien in der Planung zu berücksichtigen. So nimmt die Inzidenz einiger durch Lebensmittel übertragener Erkrankungen zu. Trotz insgesamt hoher Standards der Lebensmittelsicherheit und Hygiene in Deutschland ist die Relevanz lebensmittelübertragbarer Krankheiten weltweit ungemindert hoch. Bakterielle, parasitäre und virale Erreger können durch Lebensmittel übertragen werden. Lebensmittelbedingte Krankheiten wie Norovirus-Gastroenteritis, Campylobacter-Gastroenteritis, Salmonellosen, enterohämorrhagische Escherichia Coli (EHEC), Listeriosen, Hepatitis A, Hepatitis E, Giardiasis oder Brucellose zählen zu den häufigsten meldepflichtigen Krankheiten. Zu den durch Lebensmittel übertragbaren Erkrankungen gehören extrem häufige, aber verhältnismäßig milde Erkrankungen wie Norovirus-Gastroenteritis, aber auch seltene, allerdings schwer verlaufende Erkrankungen wie das hämolytisch-urämischen Syndrom (HUS) oder Botulismus.

Seit 2014 erkrankten in Deutschland mindestens 37 Menschen zwischen 31 und 91 Jahren aus 12 Bundesländern an einem „Sigma1“ genannten Listeriose-Ausbruch, der durch Listeria monocytogenes des Sequenz-Clusters-Typ 2521 verursacht wurde. Die Fälle mit Erkrankungsbeginn zwischen 2014 und 2017 konnten dank neuer Methoden rückwirkend zugeordnet werden. Viele der Erkrankten dürften sich über Krankenhäuser oder Altenheime infiziert haben.

Mindestens drei Erkrankte sind bisher direkt oder indirekt an den Folgen der Listeriose verstorben. Die wahrscheinlichste Ursache sind kontaminierte Wurstprodukte[55].

Die Dunkelziffer der durch Lebensmittel verursachten Infektionskrankheiten ist jedoch beträchtlich. Nicht immer wird eine erregerspezifische Diagnostik von Ärztinnen und Ärzten eingeleitet und wenn, dann ist diese nicht in allen Fällen erfolgreich. Dabei erlauben neuartige Methoden wie die Molekulare Surveillance eine sensitivere Detektion und das Erkennen von Ausbrüchen von Infektionsketten, wo vorher für den Öffentlichen Gesundheitsdienst nur Einzelfälle ohne erkennbaren Zusammenhang standen. Dieser zunehmende technische Fortschritt ermöglicht den zusammenarbeitenden Gesundheits- und Lebensmittelbehörden die Beseitigung von Infektionsquellen und damit das Verhindern neuer Fälle. Hier muss jedoch festgestellt werden, dass viele Gesundheitsämter, Veterinärämter und Dienststellen der Lebensmittelüberwachung nicht mit entsprechenden technischen oder personellen Ressourcen ausgestattet sind. Neue wissenschaftliche Methoden sind nicht flächendeckend implementiert. Es ist geboten, dass alle beteiligten Akteurinnen und Akteure nach einheitlichen Standards arbeiten, um frühzeitig Gefahrenpotenziale für einen eskalierenden Ausbruch einer Infektionskrankheit zu identifizieren. Diese Standards müssen mit gesetzlichen Regelungen verbindlich eingeführt und umgesetzt werden.

Neue Übertragungswege infolge des Klimawandels:

Schon im Grünbuch des Zukunftsforums von 2008 wurde auf die potenziellen Risiken und Effekte einer Influenza-Pandemie hingewiesen

55 Epidemiologisches Bulletin 2019;41:431 – 432 | DOI 10.25646/6308.2; Listeriose-Ausbruch mit Listeria monocy-togenes Sequenz-Cluster-Typ 2521 (Sigma1) in Deutschland.

und das durch das Coronavirus SARS-CoV-2 verursachte Lungenleiden COVID-19 als Szenario vorweggenommen. Ebenso enthält die damalige Publikation auch Hinweise auf die Ausbreitung von Vektoren (Gelbfiebermücke, Aedes aegypti) aufgrund klimatischer Veränderungen. Diese Vektoren können tropische Krankheiten in unseren Regionen verbreiten. Dabei wurde zunächst angenommen, dass dies noch zehn bis 20 Jahre dauern könnte. Seit der Veröffentlichung des Grünbuchs sind nunmehr bereits mehr als zehn dieser 20 Jahre vergangen.

Ein gemeinsam vom Robert Koch-Institut und dem Umweltbundesamt erarbeiteter Rahmen zu Handlungsempfehlungen behandelt im Zuge der Thematik Klimawandel und Gesundheit[56] auch Infektionskrankheiten. Hier heißt es:

„Durch Klimawandel, fortschreitende Globalisierung, individuelle Mobilität, internationalen Handel und Bevölkerungsfluktuationen gewinnen Infektionskrankheiten, die bisher in Mitteleuropa oder Deutschland nicht mehr oder noch nicht aufgetreten sind, zunehmend an Bedeutung. Zu diesen Infektionskrankheiten gehören solche, bei denen blutsaugende Tiere, vorwiegend Insekten (verschiedene Mückenarten) oder Zecken ein Glied im Infektionszyklus dieser Krankheiten sind. Eine Ausbreitung von Mückenarten, die in Deutschland bisher nicht oder nur begrenzt vorkommen, erscheint wahrscheinlich. Solche Mückenarten haben unter bestimmten ökologischen und epidemiologischen Bedingungen das Potential tropische Viren zu übertragen (zum Beispiel Chikungunya-Virus, Dengue-Virus). Im Zusammenhang mit dem Klimawandel als einem Kofaktor könnte sich bei in Deutschland bereits endemischen Infektionskrankheiten (zum Beispiel der durch Nagetiere übertragene Hantavirus-Erkrankungen oder der durch Zecken übertragene Lyme-Borreliose) die geografische Verbreitung und die Durchseuchung der Vektoren beziehungsweise Reservoirtiere und damit auch die Krankheitsinzidenz beim Menschen verändern."

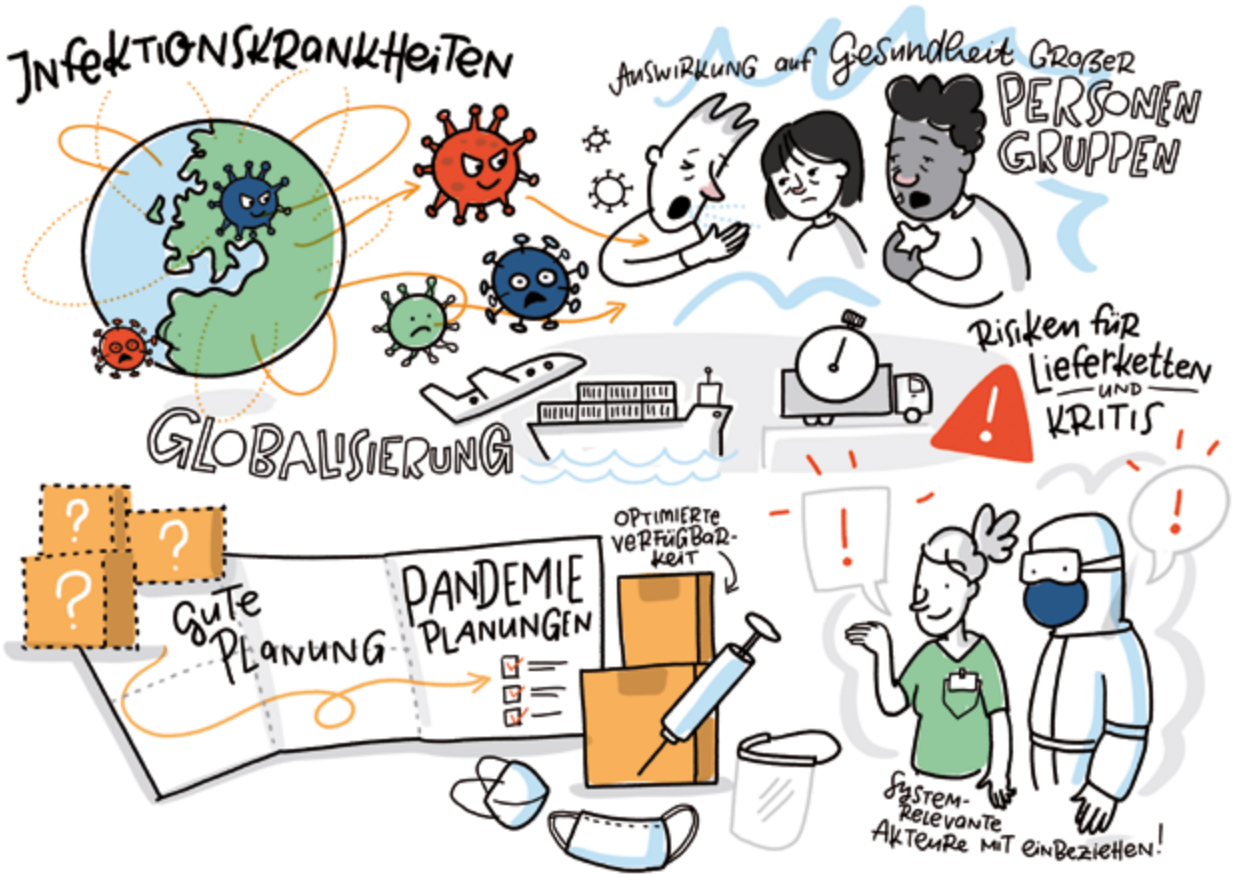
Schon jetzt zeigt sich, dass einzelne Erreger (zum Beispiel West-Nil-Virus) nördlich der Alpen vorkommen. Die Eintrittswahrscheinlichkeit eines durch Vektoren verursachten eskalierenden Ausbruchs einer Infektionskrankheit steigt weiter, so dass auch diese Ursache künftig intensiv bearbeitet werden muss. Wenn es gelingt, die genannten gesetzlichen Regelungen umzusetzen, die Maßnahmenplanung in allen Ebenen mit allen Akteuren durchzuführen und ausreichende Kapazitäten für die Versorgung intensivpflichtiger Patienten zu etablieren, können auch die potenziellen Herausforderungen eines vektorbedingten Ausbruchs einer Infektionskrankheit bewältigt werden.

Gefahr bioterroristischer Anschläge:

Immer wieder haben terroristische Gruppierungen Anstrengungen unternommen, um mit biologischen Agenzien Anschläge zu verüben und Menschen nachhaltig zu schädigen. Diese Aktivitäten blieben weitgehend örtlich begrenzt. Ein Beispiel ist der im Jahr 2018 in Köln vereitelte Anschlag mit Rizin. Laut einem Gutachter des Robert Koch-Instituts hätte dieser Anschlag zu 13.500 Todesopfern und ebenso vielen Verletzten führen können[57]. Es ist weiterhin grundsätzlich denkbar, dass international agierende Terrorgruppierungen die Möglichkeiten für eine großflächigere oder internationale Ausbreitung von Infektionskrankheiten mit entsprechenden biologischen Auslösern nutzen. Zur Herstellung entsprechender Agenzien ist spezielles Fachwissen erforderlich. Die entsprechenden Geräte und Einrichtungen sind jedoch überall problemlos zu beschaffen.

56 Klimawandel und Gesundheit Allgemeiner Rahmen zu Handlungsempfehlungen für Behörden und weitere Akteure in Deutschland; RKI, BMG und BMU; 2013

57 Frankfurter Allgemeine Zeitung vom 31.08.2019: „Rizin reichte für 13.500 Tote", Bericht über den Prozess vor dem Oberlandesgericht Düsseldorf


INFEKTIONSKRANKHEITEN
AUSWIRKUNG auf Gesundheit GROßER PERSONEN GRUPPEN
GLOBALISIERUNG
RISIKEN für Lieferketten UND KRITIS
GUTE PLANUNG
PANDEMIE PLANUNGEN
OPTIMIERTE VERFÜGBARKEIT
SYSTEM-RELEVANTE AKTEURE MIT EINBEZIEHEN!

3.4 Leitfragen

Aus den skizzierten Teilszenarien und den bestehenden Rahmenbedingungen in Gesundheitswesen und Gefahrenabwehr ergeben sich Leitfragen, die der Klärung bedürfen. Sie wurden teils innerhalb des 2006 durch die Bundesregierung beschlossenen Sicherheitsforschungsrahmenprogramms mit verschiedenen Bekanntmachungen zu biologischen Gefahren bereits angesprochen. Die Identifikation weiteren Forschungsbedarfs ist aber auf der Grundlage des hier ausgeführten und gerade auch vor dem Hintergrund des gegenwärtigen COVID-19-Ausbruchs und des Umgangs damit erforderlich.

- Wie kann man das Bewusstsein der Gesellschaft mit ihren vielfältigen Gruppierungen gegenüber Infektionserkrankungen der Mensch-zu-Mensch-Übertragung sensibilisieren und kontinuierlich aufrechterhalten?

- Durch welche Maßnahmen kann bei einem überdurchschnittlichen, spontanen regionalen Anstieg von Infektionserkrankungen (Mensch-zu-Mensch-Übertragung) die sich entwickelnde Epidemie begrenzt werden (etwa Schließung von Schulen, Kindergärten, Geschäften, Verlagerung von Tätigkeiten ins Homeoffice, Social Distancing und dergleichen mehr)?

- Durch welche Maßnahmen kann die weitere Ausbreitung einer Epidemie (Mensch-zu-Mensch-Übertragung), die Deutschland von außen erreicht hat, begrenzt werden?

- Welche ökonomischen, sozialen, soziologischen und sozialpsychologischen Effekte müssen berücksichtigt werden, wenn Versammlungsstätten sowie Einrichtungen der öffentlichen Infrastruktur (Theater, Kinos, Restaurants, Kongresse, Kindertagesstätten, Schulen, Universitäten) geschlossen und andere Einrichtungen sowie Wirtschaftszweige zur Begrenzung der Ausbreitung vorübergehend stillgelegt werden?

3.5 Handlungsempfehlungen

Um den Gefahren eskalierender Infektionskrankheiten wirkungsvoll zu begegnen, bedarf es neuer strategischer Überlegungen, für die auch weitere wissenschaftliche Erkenntnisse gewonnen werden müssen. Außerdem sind Rechtsetzung, Planung und deren Verankerung in der Praxis zu verbessern. Eine zentrale Rolle spielen bessere Sensibilisierung und Kommunikation, damit die Bekämpfung einer Epidemie oder Pandemie von Anfang an als das verstanden wird, was sie ist: eine gesamtgesellschaftliche Aufgabe mit einem großen Kreis direkt involvierter Akteurinnen und Akteure. Insbesondere positive Erkenntnisse aus der COVID-19-Pandemie, müssen erfasst und weiterentwickelt werden.

Im Einzelnen empfehlen wir die unverzügliche Umsetzung der nachfolgenden Maßnahmen:

Entwicklung einer nationalen „Public Health"-Strategie zur Eindämmung und Kontrolle von Pandemien, um die gesellschaftlichen, sozialen und ökonomischen Konsequenzen so gering wie möglich zu halten:

Eine optimierte gesundheitliche Versorgung für alle Menschen muss als ressortübergreifendes Ziel verankert werden. Die Gesundheit der Bevölkerung ist Aufgabe der öffentlichen Daseinsvorsorge, sodass Versorgungskapazitäten auch mögliche Krisensituationen berücksichtigen sollten. Der Mangel an medizinischem und pflegerischem Fachpersonal muss konsequent angegangen werden. Hier bedarf es einer angemessenen Vergütung, besserer Arbeitsbedingungen und guter Ausbildungsstrukturen.

> *Die resultierende Umsetzungsstrategie muss umgehend angegangen werden, zumal die hier notwendigen gesundheitlichen Vorkehrungen grundsätzlich für alle Varianten von großflächigen Katastrophenfällen erforderlich sind. In jedem Fall gibt es massive gesundheitliche Auswirkungen, die gesellschaftlich und wirtschaftlich unmittelbare Folgen haben. Daher muss jetzt eine Auswirkungsanalyse im Bereich Innen, der im Katastrophenfall zuständig ist, stattfinden, unter maßgeblicher Beteiligung von Gesundheit, aber auch Arbeit und Soziales, Forschung, etc. unter Einbeziehung laufender Evaluationen der Länder."*
>
> ***– Susanne Mittag MdB***

Kontinuierliche Weiterentwicklung und Anpassung des nationalen Pandemieplans, einschließlich einer Strategie zur frühzeitigen Entwicklung und Implementierung von Testverfahren, um Überlastung der Kapazitäten der Gesundheitsversorgung zu verhindern:

Dies schließt die wirtschaftliche Sicherung des Betriebs der Einrichtungen des Gesundheitswesens in Pandemielagen ein. Auf europäischer Ebene sind geeignete Pandemiepläne zu entwickeln und Maßnahmen zur besseren Koordinierung einzelstaatlicher Pläne zu ergreifen.

Verankerung nationaler Gesundheitslagen in allen zur Aufrechterhaltung der medizinischen Versorgung erforderlichen (systemrelevanten) Bereichen:

Mit der Implementierung der ergänzenden gesetzlichen Regelungen müssen diese verpflichtend geübt und trainiert werden. Dies gilt auch für Entscheidungsträgerinnen und Entscheidungsträger der Gefahrenabwehr (zum Beispiel Landrätinnen und Landräte mit den Katastrophenabwehrleitungen) und private Akteurinnen und Akteure zur Vertiefung der bestehenden Regelungen und der Abwägung ihrer Anwendung.

> *Die COVID-19 Pandemie hat deutlich gemacht, wie wichtig eine länderübergreifende Zusammenarbeit und Koordination im Krisenfall ist. Ich bin davon überzeugt, dass der Bund mehr Verantwortung beim Katastrophenschutz übernehmen muss. Dafür muss das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) gestärkt und zu einer Zentralstelle für Bund-Länder-übergreifende und besondere Lagen ausgebaut werden, wie wir sie im polizeilichen Bereich vom Bundeskriminalamt kennen. Darüber hinaus sollten wir die Erfahrungen aus der Pandemie auch zum Anlass nehmen, um den medizinischen Katastrophenschutz zu stärken. Es zeigt sich, dass wir in unserem Gesundheitssystem Vorsorge für die verschiedensten Krisenszenarien treffen müssen."* ***– Dr. Irene Mihalic MdB***

Schaffung beziehungsweise Anpassung von Rechtsgrundlagen, die im Falle einer pandemischen Gesundheitslage hinreichend bestimmt sind und unter Beachtung der Bedeutung der Grundrechte in einem demokratischen Rechtsstaat Bund, Ländern und Kommunen die zur Bewältigung der Lage erforderlichen Zuständigkeiten und Befugnisse zuweisen.

> *Die Bekämpfung einer Pandemie ist nicht nur eine gesundheitliche Herausforderung, sie ist zugleich eine Bewährungsprobe für Rechtsstaat und Demokratie. Das Coronavirus hat vor Augen geführt, dass eine epidemische Notlage einhergehen kann mit drastischen Einschränkungen von Bürgerrechten und der Schwächung der Parlamente, weil Entscheidungen maßgeblich durch Regierungen oder Krisenstäbe getroffen werden. Damit sich aus einer gesundheitlichen Lage aber keine Verfassungskrise entwickelt, darf es für Parlamente und Bürgerrechte keine noch so kurze Auszeit geben. Das Grundgesetz gilt in jeder Situation."* ***– Dr. André Hahn MdB***

Schaffung von Rechtsgrundlagen zur Sicherstellung der Gesundheitsversorgung und zum Aufbau und dauerhaften Vorhalten von „Notreserven" im Bereich von Schutzausrüstung, Laborkapazitäten, Isolationsmöglichkeiten und so weiter[58]:

Es ist zu berücksichtigen, dass nicht nur intensiv-medizinische Betreuung von Schwerstkranken mit Beatmungsgeräten, sondern auch Kapazitäten für mittelschwer Erkrankte, die eine Sauerstoffversorgung benötigen, geschaffen werden müssen. Selbst bei einem erfolgreichen Eindämmen der Epidemie kann die vorhandene Kapazität für die nötige Krankenhauspflege leicht überfordert werden. Dabei sollten sich die Anstrengungen nicht auf das abstrakte Konzept der Betten konzentrieren, sondern auf die spezifisch nötige Infrastruktur, insbesondere auf die Sauerstoffversorgung und die Anzahl der Beatmungsgeräte oder Dialyseplätze sowie die entsprechende Personalausstattung. Diese Reserven müssen personell und technisch langfristig tragfähig sein und dem jeweiligen Stand von Wissenschaft und Technik angepasst werden, zum Beispiel durch Investitionen, Schulung, Prüfung und Wartung. Die Vorhaltung von Pockenimpfstoff ist als isolierte Maßnahme nicht ausreichend. Hier erscheint zum Beispiel eine Strategie zur länderübergreifenden Logistik geboten. Zugleich ist die Abhängigkeit bei der Produktion von Medikamenten und Medizinprodukten von einigen wenigen Ländern zugunsten von Produktionsstandorten in Europa zu überwinden.

> *Die jüngsten Erfahrungen aus der COVID 19-Pandemie in Deutschland haben gezeigt, dass das System des gesundheitlichen Bevölkerungsschutzes in Deutschland wirksam und krisenfest aufgestellt ist. Ungeachtet dessen müssen wir Ausrichtung, Kapazitäten und Zuständigkeiten fortwährend hinterfragen und dort, wo es notwendig ist, neuen Gegebenheiten und Herausforderungen anpassen. Das Szenario hilft uns zusammen mit den Erkenntnissen der vergangenen Monate dabei, dort nachzusteuern wo es notwendig ist, um unsere Bevölkerung auch in Zukunft mit allen zur Verfügung stehenden Mitteln zu schützen."* ***– Michael Kuffer MdB***

58 Siehe auch Eckpunktepapier „Corona-Folgen bekämpfen, Wohlstand sichern, Zukunftsfähigkeit stärken", Ergebnis Koalitionsausschuss 3. Juni 2020

Stärkung des Öffentlichen Gesundheitsdienstes (ÖGD) mit ausreichenden Ressourcen und gut qualifiziertem Personal:

Für Prozesse und Entscheidungswege in Pandemiesituationen muss es eingespielte Standardverfahren geben. Es muss verhindert werden, dass Gesundheitsämter in identischen Situationen unterschiedlich verfahren und damit Unsicherheit bei der Bevölkerung erzeugen. Die digitale Erreichbarkeit (Apps zur Kommunikation, Koordination) der lokalen Gesundheitsbehörden ist sicherzustellen[59]. Es müssen flächendeckend einheitliche Standards in quantitativer und qualitativer sowie in personeller und technischer Hinsicht im ÖGD verpflichtend etabliert werden, beispielsweise auch integrierte modulare Surveillance. Ein personeller Aufwuchs in Lagen muss vorgeplant und umfassend realisiert werden können.

Alle Akteurinnen und Akteure im Gesundheitssystem, insbesondere die niedergelassenen Ärtzinnen und Ärtze, Apotheken, Gesundheitszentren (Therapie und Diagnostik), müssen vollständig in die Maßnahmenplanung integriert werden:

Daraus folgt, dass alle Einrichtungen mindestens eine kontinuierliche, gegebenenfalls automatisierte, Meldepflicht von Verdachtsfällen gegenüber dem öffentlichen Gesundheitsdienst (ÖGD) haben müssen. Es sind technische Einrichtungen zu nutzen, die dem ÖGD die Möglichkeit eröffnen, sofort zu handeln. In diese Betrachtung müssen Pflegeheime einbezogen werden, wenn die Verlagerung der Patientinnen und Patienten in Krankenhäuser begrenzt bleiben soll oder auch eine besondere Gefährdung für Patientinnen und Patienten dieser Einrichtungen wie bei COVID-19 besteht. Damit das vom ÖGD kommunal umgesetzt werden kann, bedarf es einer bundesrechtlichen Regelung bei Beachtung der Länderzuständigkeiten. Das Bewusstsein, bedeutsame Akteurinnen und Akteure der gesundheitlichen Versorgung zu sein, muss insbesondere bei niedergelassenen Ärztinnen und Ärzten und Apotheken sowie den kassenärztlichen Vereinigungen gestärkt werden.

Notwendig ist eine Aufklärungs- und Informationskampagne über Gefahren und Folgen von Infektionskrankheiten sowie die Selbsthilfe-Ausbildung der Bevölkerung:

Die Bevölkerung muss alle Kommunikationswege kennen und nutzen können. Sie muss wissen, dass die Mitwirkung Aller erforderlich ist, um die Verbreitung gefährlicher Erreger schnellstmöglich einzudämmen und ein demokratisches Zusammenleben (sowohl politisch und sozial, als auch wirtschaftlich) zu garantieren. Der Verbreitung von Desinformation in den Sozialen Medien muss entgegengewirkt werden. Wichtigste Botschaft: Hochansteckende Erreger sind ein Risiko für alle. Staatliches Handeln orientiert sich an der wissenschaftlichen und praktischen Evidenz. In derartigen Lagen gilt es, entschieden, aber nicht panisch zu handeln.

> *In der aktuellen Situation zeigt sich die herausragende Bedeutung guter Krisenkommunikation. Die Entwicklung von Risiko- und Krisenkommunikationskonzepten stärker in den Fokus zu nehmen, kann im Ernstfall Leben retten. Derartige Konzepte können oder müssen aber auch die Grenzen der Kapazitäten des Katastrophenschutzes und damit die Notwendigkeit zur Eigenvorsorge betonen. Ihre wichtigste Aufgabe bleibt aber die einheitliche Informationsvermittlung und die klare Benennung von Ansprechpartnern."*
>
> ***– Benjamin Strasser MdB***

59 Siehe auch Bundesgesundheitsministerium: Zweites Gesetz zum Schutz der Bevölkerung bei einer epidemischen Lage von nationaler Tragweite

Der Ausbau und die Intensivierung der Forschung ist insbesondere aufgrund der gewonnen Erkenntnisse aus der COVID-19-Pandemie geboten:

Innerhalb des Sicherheitsforschungsprogramms des Bundes wurde im Rahmen verschiedener Bekanntmachungen zu biologischen Gefahren und Pandemien bereits die Bewältigung national bedeutender Gesundheitslagen angesprochen. Die Forschungsaktivitäten in diesem Bereich müssen intensiviert werden. Der ungewollte Feldversuch zur Bewältigung der COVID-19-Pandemie liefert vielfältige Erkenntnisse, die sowohl bezüglich der Bewältigung von biologischen Gefahrenlagen (zum Beispiel Schulschließungen, Wirksamkeit selbstgefertigter Schutzmasken und weitere) als auch bezüglich ereignisunabhängiger Themen (zum Beispiel Home-Office, personelle und materielle Notfallreserven, Verkehrsbeschränkungen, spezifische Wirtschaftszweige und dergleichen mehr) einer umfassenden wissenschaftlichen Analyse unter Berücksichtigung vielfältiger Cluster (etwa Wirtschaft, Gesundheitsversorgung, Grundrechtseingriffe, alternative Arbeitsformen und ähnliche) bedürfen.

Bei Eintritt einer Pandemie müssen alle staatlichen Behörden der Bevölkerung frühzeitig umfassende und abgestimmte Information sowie konkrete Handlungsanweisungen zur Verfügung stellen.

Learning by Doing

Als sich unsere Gruppe im Februar 2019 aus dem Zukunftsforum Öffentliche Sicherheit zusammengefunden hat, um das Thema „Pandemien“ des Grünbuchs zu aktualisieren, gab es noch keine Corona-Problematik und auch keine darauffolgende Pandemie. Erst nach dem redaktionellen Abschluss unseres Berichtes begann SARS-CoV-2 auf Europa überzugreifen. Wir sind nun deshalb übereingekommen, unsere Ausarbeitung der aktuellen Situation in der COVID-19-Pandemie anzupassen, in unseren Augen wesentliche und unabhängig von dieser Pandemie zu treffende Aussagen aber so stehen zu lassen. Eine grundlegende Überarbeitung wäre erst nach einigen Monaten, bei Vorliegen weiterer Erkenntnisse und notwendigen Folgerungen, sinnvoll gewesen.

Unser Bericht ist keinesfalls überholt. Er stellt, auch kritisch beleuchtet, die Situation vor der COVID-19 Pandemie dar. Viele unserer Anmerkungen sind durch die Realität bestätigt worden. An vielen Stellen sind kurzfristig Verbesserungen erreicht worden, die für zukünftige Ereignisse nützlich sein werden. Zugunsten der Versorgungsketten beim Massenanfall von Verletzten ist ein eskalierendes Infektionsgeschehen völlig aus dem Blick geraten. Sowohl im Grünbuch als auch im Bundestagsbericht von 2012 (Risikoanalyse Bevölkerungsschutz Bund: Pandemie durch Virus Modi-SARS vom 10.12.2012) sind wesentliche Probleme prognostiziert worden. So haben auch wir den Finger in die Wunde legen müssen. Notwendige Ergänzungen sollten einer zukünftigen Publikation vorbehalten bleiben, an der wir uns gern beteiligen werden. Eine Überschrift „Lessons Learned“ wäre jetzt verfrüht.

4 Der digitale Raum und die Organisierte Kriminalität – Stand heute mit Ausblick für die kommenden fünf Jahre – Die Zukunft hat schon begonnen

4.1 Einführung

IT-Sicherheitspolitik ist aufgrund der stark gestiegenen Bedeutung digitaler Technik und der Digitalisierung praktisch aller Lebensbereiche zu einer politischen Schlüsselfrage geworden. Die Informationstechnik (IT) ist leistungsfähiger, mobil nutzbar, intuitiver und allgegenwärtig geworden, dauernder Weiterentwicklung unterworfen, zunehmend kaum wahrnehmbar und ein selbstverständlicher Bestandteil des privaten und öffentlichen Lebens. Hieraus entstehen für die Wirtschaft und die Gesellschaft enorme und vielfältige Chancen, aber auch Risiken, die zum Teil noch nicht abzuschätzen sind.

Die heutigen Veränderungen aufgrund der dynamischen Fortentwicklung von IT und deren Nutzung lassen umfassende globale Umwälzungen der politischen, technologischen, wirtschaftlichen und sozialen Machtgefüge erkennen, die nicht allein, aber entscheidend auf der digitalen Transformation sowie dem virtuellen Aktions- und Lebensraum des Netzes beruhen. Für unsere Gesellschaft, unsere Industrie, unsere staatliche Ordnung und unsere demokratischen Werte ergeben sich daraus zahlreiche Konsequenzen. Deshalb sind die kommenden Jahre von entscheidender Bedeutung. Staat und Gesellschaft sind gefordert, entsprechend zu agieren, um den digitalen Wandel unserer Gesellschaft proaktiv und im Sinne demokratischer Rechtsstaatlichkeit zu begleiten und aktiv politisch zu gestalten. Nicht angemessenes Handeln könnte zum Verlust der technischen Kontrolle und zu gesellschaftlicher Verunsicherung führen.

4.2 Ausgangslage und Herausforderungen

Die stark durch den Mittelstand geprägte deutsche Industrie ist in ihrer technologischen Entwicklung immer stärker auf Know-how aus Ländern wie China, USA und Indien angewiesen. Die Wertschöpfung verlagert sich zunehmend von materiellen Gütern und Ressourcen in die virtuelle Welt. Dabei entstehen durch die großen internationalen Konzerne wie Alphabet, Amazon, Apple, Facebook und Microsoft mit ihren Plattformen internationale Monopole, die durch Marktmacht und Nutzerakzeptanz zunehmend Quasi-Standards etablieren. Insbesondere der Mittelstand verliert dadurch die potenziell schützenden und innovationsfördernden Funktionen von Normen wie DIN/ISO. Vergleichbares gilt für die Finanzwelt und den Handel. Deutschland und die Europäische Union müssen deshalb dafür sorgen, dass dort die technische Sicherheit und die Sicherheitsforschung prioritär in die weitere Entwicklung aufgenommen werden.

Social Media und Plattform-Ökonomie werden unser soziales, politisches und wirtschaftliches Leben zunehmend gestalten und dominieren. Suchmaschinen treffen Vorauswahlen aufgrund von Algorithmen, anstatt auf Informationen im freien, offenen Netz zu verweisen, und erhöhen die Gefahr von Einseitigkeit und Beeinflussung.

Die Vernetzung wird nicht nur im globalen und regionalen, sondern auch im lokalen und privaten Rahmen weiter fortschreiten. Die Digitalisierung führt schon in 2020 weltweit zu einer Vernetzung von 7,8 Milliarden Menschen und zu 50 Milliarden verbundenen Geräten im Internet of Things (IoT). Vernetzte Lieferketten, vernetzte Autos, Smart Home, „intelligente“ Strom- und Versorgungsnetze, vernetztes Gesundheitswesen bis hin zu vernetzten Implantaten werden immer mehr Teil unseres Lebens. In diesem Rahmen kommt der Künstlichen Intelligenz (KI) eine Schlüsselrolle zu. Sie wird eine immer komplexere Gestaltung und Nutzung der vernetzten Systeme ermöglichen und ganz neue Anwendungen und Geschäftsmodelle eröffnen.

Industrieroboter steigern in mittelständischer und Großindustrie die Wertschöpfung. Der Einsatz von automatisierten Transportsystemen wie Drohnen oder autonomen Fahrzeugen wird in der Logistik eine zunehmend wichtige Rolle einnehmen und neue Herausforderungen für

die sichere Steuerung von Verkehrsströmen ergeben. Roboter im Versorgungsbereich von Krankenhäusern und Roboter für Demenzkranke sind in den USA, im Vereinigten Königreich, in China und Japan auf dem Vormarsch. Auch im privaten Bereich halten Roboter oder intelligente Assistenten Einzug, zum Beispiel Staubsauger- und Rasenmähroboter, Sprachassistenten und Social Robots.

Die rapide und dynamische Weiterentwicklung von Künstlicher Intelligenz wird insbesondere für Berufsgruppen, deren Arbeit auf Informationsverarbeitung beruht, erhebliche Veränderungen bringen und bis hin zum Verschwinden von Beschäftigungsmodellen oder zu neuen Geschäftsmodellen führen. Dies zeigt sich bereits in der Medizin bei Labor- und Diagnostikberufen und an den Finanzmärkten bei Analysten und Maklern.

Enorme Entwicklungssprünge sind durch den Einsatz von Quantencomputern in immer kürzerer Zeit zu erwarten. Blockchain setzt sich weiter durch und wird als kryptographisch vernetzte Datenbank weiterentwickelt. Künstliche Intelligenz revolutioniert bereits heute durch aktuelle Technologien wie der Mustererkennung mit Deep Learning/Machine Learning beispielsweise die Medizin, die Prothetik, die medizinische Analyse und Versorgung.

Neben großen Chancen bestehen neue Risiken. Die Kriminalität kann durch KI neue Missbrauchspotenziale erschließen. Analog zu dem Nutzen der KI in gesellschaftlichen und wirtschaftlichen Zusammenhängen eröffnet sie auch der Organisierten Kriminalität (OK) vollkommen neue Möglichkeiten. Auch die Sicherheitsbehörden werden voraussichtlich immer öfter auf KI bei der Gefahrenabwehr und der Kriminalitätsbekämpfung zurückgreifen. Dabei – wie etwa bei den Diskussionen um einen flächendeckenden Einsatz der automatischen Gesichtserkennung durch die Bundespolizei – müssen Fragen um die Verhältnismäßigkeit solcher Methoden und die mögliche Verletzung von Grundrechten durch ihren Einsatz eine wichtige Rolle spielen.

Gesellschaft, Politik und Wirtschaft haben schon jetzt und künftig noch dringender grundsätzliche ethische Probleme zu lösen und Zukunftsfragen zu beantworten: Wie gehen wir damit um, dass durch den exponentiellen Aufwuchs von Informationen und Daten Menschen und Institutionen transparenter und damit angreifbarer und potenziell manipulierbarer wird?

Inwiefern lassen wir es zu, dass Roboter und KI für uns Entscheidungen in Grundsatzfragen und im täglichen Leben übernehmen? Wollen wir Entscheidungen zur Sicherheit in wachsendem Ausmaß an technische Systeme verlagern? Und wie schaffen wir es zum Beispiel bei der Weiterentwicklung von Informationssystemen und deren Nutzung oder beim Einsatz von KI durch Sicherheitsbehörden, einen hohen Standard an Grundrechtsschutz, insbesondere im Bereich der informationellen Selbstbestimmung, zu gewährleisten?

Überlassen wir es den weltweit führenden IT-Konzernen oder anderen Staaten ob, in welchem Umfang und nach welchen ethischen Kriterien Standards für Informationsverarbeitung und KI entwickelt und eingesetzt werden?:

4.3 Bestehende und neue Risiken

Inhärente Risiken im digitalen Raum

In der globalisierten Welt führt der scheinbar exponentielle Einsatz von Informations- und Kommunikationssystemen zu einem Technologiedruck, der auf beinahe alle Akteurinnen und Akteure in allen Lebens- und Wirtschaftsbereichen wirkt. Es wird zunehmend schwerer, sich der Nutzung aktueller Technologien zu entziehen, da eine Partizipation am Wirtschafts- und Sozialleben anders kaum möglich ist. So potenzieren sich mögliche Risiken der Technologie durch frühen oder sogar zu frühen massenhaften Einsatz. Die Weiterentwicklung und steigenden Abhängigkeiten von Hightech-Systemen in der Daseinsvorsorge, Produktion und Logistik, Kommunikation, im Gesundheitswesen

und öffentlichen Verkehr drohen wegen der damit verbundenen Komplexität neue Schwachpunkte zu entwickeln: Die Vernetzung von IT-Systemen kann in Bruchteilen von Sekunden bei einem scheinbar unbedeutenden Crash, begünstigt durch Kaskadeneffekte, weite Teile von Kommunikation, Logistik, Versorgung und sozialem Leben zum Stillstand bringen. Dies wird besonders dadurch befördert, dass Netzwerke ohne erkennbaren ökonomischen oder technologischen Mehrwert miteinander verbunden werden, deren Planungs- und Sicherheitsarchitekturen dieses nicht berücksichtigen. Es entstehen sogenannte systemische Risiken, die insbesondere durch eine hohe Dynamik bei gleichzeitiger Intransparenz und Komplexität sowie räumlicher Entgrenzung von Ursache und Folge gekennzeichnet sind.[60]

Der nach wie vor bestehende Mangel an qualifiziertem Personal, insbesondere im IT-Sicherheitsbereich, stellt ein besonderes Risiko in Deutschland und der EU dar. Die Nachfrage nach IT-Fachkräften insgesamt ist in Deutschland hoch. Circa 80.000 Stellen sind in diesem Bereich schon jetzt unbesetzt. Trotz erheblicher Steuerungsmaßnahmen wie der Etablierung neuer Studiengänge oder der Anwerbung von Fachkräften steigt die Zahl weiter. Es muss davon ausgegangen werden, dass der Arbeitskräftemangel auch die nächsten Jahre andauern wird. Eine mögliche Alternative in Form von Nutzung sicherheitsrelevanter IT-Fähigkeiten im Ausland birgt auch Risiken.

Risiken durch Angriffe im digitalen Raum

Außer den dem digitalen Raum innewohnenden Risiken ergeben sich auch neue Herausforderungen durch den bewussten Missbrauch von IT-Systemen, beispielsweise durch die Ausnutzung von Vernetzung und von Sicherheitslücken bei der Ausführung von Angriffen, durch die Verlagerung oder die Schaffung krimineller Märkte durch OK, durch Datenmissbrauch oder Industrie- und Wirtschaftsspionage. Ausführende und verantwortliche Akteurinnen und Akteure können einzelne IT-Expertinnen und Experten, die OK, Terrororganisationen, Staaten oder konkurrierende Wirtschaftsunternehmen sein[61]. Neue kriminelle Methoden und Märkte sowie flexible Strukturen krimineller Organisationen schaffen insbesondere durch die hohen Ausbreitungsgeschwindigkeiten und die leichte Übertragbarkeit auf andere Sektoren ein großes Gefahrenpotenzial, auf das sich unsere präventiven und repressiven Abwehrmechanismen permanent und effektiv einstellen müssen, die aber auch das subjektive Sicherheitsbewusstsein von Bürgerinnen und Bürgern und Gesellschaft zutiefst beeinflussen.

Ein wiederkehrendes Problem ist die Verwendung von Schadprogrammen zur Erpressung von Lösegeld (Ransomware). Zunehmend werden, wie bei der WannaCry-Attacke, nicht nur staatliche Institutionen, Banken, Industrie und Handelsketten, sondern auch Bürgerinnen und Bürger direkt bedroht. Dieses wird insbesondere durch den vermehrten Einsatz von körpernahen Sensoren und weiteren innovativen Technologien wie dem IoT und der Miniaturisierung bis hin zur sogenannten Nanotechnologie begünstigt. So werden immer mehr und immer sensiblere Daten digital erhoben und können somit durch kriminelle Akteure missbraucht werden. Die Regulierung hält damit noch nicht Schritt. Kaum mitgedacht, erforscht und prognostiziert sind die Risiken durch die kriminelle Nutzung von KI.

Inhaltlich und methodisch zu unterscheiden sind einerseits strafbare Handlungen, die sich gegen Kommunikationsnetze, informationstechnische Systeme oder deren Daten selbst richten. Andererseits, und darum geht es hier, gibt es das strafrechtlich relevante Handeln von Einzelpersonen, Banden oder OK, bei dem die moderne Informations- und Kommunika-

60 Mertens, P., Barbian, D. Beherrschung systemischer Risiken in weltweiten Netzen. Informatik Spektrum 38, 283–289 (2015). https://doi.org/10.1007/s00287-015-0900-2

61 Im Rahmen dieser Analyse werden wir im Weiteren auf die Organisierte Kriminalität fokussieren. Viele der Angriffs- und Bedrohungsarten gehen aber in gleicher oder ähnlicher Form auch von den übrigen hier genannten Akteursgruppen aus.

tionstechnik zur Planung, Vorbereitung oder Ausführung herkömmlicher Kriminalität genutzt wird. So stellt der virtuelle Raum einen weiteren bedeutsamen Gestaltungsbereich für Kriminalität dar. Kriminalität und die damit einhergehenden Täterprofile und -strukturen verändern sich somit in den kommenden Jahren durch die Digitalisierung mutmaßlich in Qualität und Quantität. Verbrechen können durch den technischen Vorteil von Skalierung in IT-Systemen schneller und massenwirksamer begangen werden. In Verbindung mit gegebenenfalls nur schwach gesicherten Computern und IoT-Geräten können große Bot-Netze im Internet gebildet werden, die für kriminelle Aktivitäten eingesetzt werden. Unter Nutzung moderner Logistik und virtueller Währungen müssen sich Lieferant und Kunde von illegalen Produkten nicht mehr persönlich begegnen. Diese neuen Technologien ermöglichen es Täterinnen und Tätern bei professioneller Anwendung, leichter anonym zu bleiben und weniger Spuren für die Strafverfolgung zu hinterlassen.

Das Angriffsziel der OK reicht dabei in Deutschland von einzelnen Bürgerinnen und Bürgern bis hin zum Sozial- und Gesundheitssystem. Einerseits sind Menschen gefährdet, die sich mit eingeschränkten Kenntnissen vergleichsweise unerfahren und langsam im schnell ändernden digitalen Raum bewegen. Andererseits macht der leichtfertige Umgang mit persönlichen Daten in sozialen Netzwerken sehr anfällig für Erpressung oder Missbrauch.

Schon bestehende und künftige Big-Data-Technologien und Analysemethoden helfen der OK, potenzielle Opfer herauszufiltern und Gewinnchancen zu berechnen. Unternehmen wie Cambridge Analytica können schnell gegründet und nicht nur für politische Ziele, sondern könnten auch für kriminelle Zwecke missbräuchlich eingesetzt werden.

Das kriminelle Aktionsfeld im digitalen Raum führt zu einem Wandel krimineller Strukturen und Arbeitsweisen. Dazu gehört der Aufbau von flexiblen und schnell agierenden virtuellen Strukturen, die sich auch legale Wirtschaftsbereiche zunutze machen. OK erzielt mit Hilfe des Netzes eine größere Breitenwirkung und entwickelt neue, effiziente und effektive illegale Aktivitäten. Kriminelle Spezialisten, die ihre Dienste im Darknet anbieten, werden in spezifischen illegalen Projekten von Einzeltätern, losen Gruppierungen oder OK eingesetzt. Diese Diversifizierung gilt in besonderer Weise für Cyberangriffe, Spionage, Produktpiraterie, Betrügereien und illegalen Handel im Netz sowie Geldwäsche. Auf spezifische Bestellungen oder für kurzfristige Projekte setzen sich für die gewünschten illegalen Endprodukte und Dienstleistungen kriminelle Gruppen immer wieder neu zusammen und planen und koordinieren sich auf Online-Plattformen. Wie in der analogen Kriminalität ermöglichen die Digitalisierung, Vernetzung und Methoden der KI arbeitsteilige Prozesse, indem sich zum Beispiel eine Gruppierung um die Produktion kümmert, einzelne oder mehrere IT-Spezialistinnen und Spezialisten für die Auftraggebenden einen Webshop für illegale Produkte und Dienstleistungen erstellen und wiederum eine andere Gruppe Transport und Lieferung betreut oder den regionalen Kleinhandel übernimmt. Dieser internationale Trend schließt Akteurinnen und Akteure innerhalb und außerhalb der EU ein und wird sich künftig immer mehr verstärken.

Die virtuelle Tatbegehung schafft eine neue quantitative und qualitative Dimension der kriminellen Gefährdung (Darstellung von sexuellem Missbrauch, illegaler Handel, illegales Glücksspiel, Geldwäsche). Diebstahl von Fähigkeiten in Computerspielen, Identitätsdiebstahl oder Einsatz von Schadsoftware bei Konkurrenten bereichern das kriminelle Spektrum. Ein Beispiel ist Cryptojacking, bei dem die Bandbreite der Internetverbindung und Prozessorleistung des Computers eines Nutzers zur Erzeugung und Verfügung von virtuellen Zahlungsmitteln wie Bitcoin gestohlen werden, während der Nutzer eine ansonsten unauffällige Website besucht. In diesem Rahmen ergeben sich auch neue Formen der Erpressung von Wirtschaft und Gesellschaft, zum Beispiel die Zugangsverweigerung zu ihren Guthaben in Cryptocurrency. Dieses weist große Parallelen zu Ransomware-Attacken auf.

Kriminelle nutzen nicht nur das Darknet, sondern mit dem Anstieg des Online-Handels auch immer häufiger das offene Internet[62]. Bei illegalem Handel und illegalen Dienstleistungen nutzen sie auch verschlüsselte Kommunikation in den Geschäftsabläufen oder den Einsatz modernster Logistik. Da OK in erster Linie gewinnorientiert ist, stehen Produktion und Handel von illegalen Gütern und Dienstleistungen im Mittelpunkt. Gewinne werden dann durch raffinierte Geldwäsche-Mechanismen gesichert und reinvestiert. Kriminalität droht legale Wirtschaftsbereiche künftig immer mehr zu infiltrieren, zumal sich das kriminelle Geschäftsmodell in vergleichbarer Weise wie legale Produktion und Handel globalisiert. Die Instrumente und Methoden der Weltwirtschaft von Produktion, Kommunikation, Handel, Logistik, Finanzierung und der virtuellen Märkte werden von legaler und illegaler Wirtschaft gleichermaßen genutzt. Die Produktion beziehungsweise Fälschung von Produkten und Handel findet jedoch in weitgehend von staatlichen Institutionen unkontrollierten Regionen statt. Im Internet sind das beispielsweise Social Media und virtuelle Marktplätze oder entsprechende Systeme im Darknet, die über TOR erreichbar sind. OK nutzt zusätzlich moderne Transportketten und das Netz von fast unkontrollierbaren Freihäfen und Logistikzentren mit sich ständig verändernden Vertriebswegen und -methoden, um dann die kriminogenen Güter an den Endabnehmer zu liefern.

Moderne Kriminalität reagiert äußerst flexibel auf die illegalen und legalen Bedürfnisse potenzieller Kundinnen und Kunden. Sie schafft oder baut latent vorhandene illegale Bedürfnisse sogar aus, wie der in der Vergangenheit mengenmäßig noch unbedeutende, inzwischen aber ausgeweitete Handel mit Missbrauchsdarstellungen, der Handel mit Dopingmitteln, der Aufwuchs von illegalem Online-Glücksspiel und der Handel mit menschlichen Organen, etwa zur Finanzierung von Flucht oder aufgrund Erpressung von Lösegeldern, beispielhaft zeigen[63] [64].

OK profitiert auch von der sozialen Toleranz gegenüber geschmuggelten oder gefälschten Luxusgütern wie E-Zigaretten und Tabakerhitzungssystemen, Textilien, Uhren und davon, dass Betrug gegenüber staatlichen Einrichtungen (Steuerhinterziehungen, Sozialbetrug, Subventionsbetrug) oder großen Unternehmen wie Versicherungen eine gewisse gesellschaftliche Akzeptanz erlebt. Die Fälschungen von Luxusgütern ist auf Pharmazeutika, Ersatzteile von Fahrzeugen und Maschinen ausgeweitet und wird immer stärker Alltagsgüter und Nahrungsmittel einbeziehen, die dann auch in legale Vertriebsnetze eingespeist werden. Cyberspionage und 3D-Drucker ermöglichen es zunehmend, in kürzester Zeit Hightech-Produkte und auf dem Markt erfolgreiche Artikel so zu fälschen, dass sie selbst von Experten kaum von Originalen zu unterscheiden sind. Grenzen zwischen legalen und illegalen Produktions- und Vertriebsprozessen verwischen. Gefälschte Industrieprodukte werden immer häufiger über legale Vertriebswege in den autorisierten Handel eingeschleust. Für Kundinnen und Kunden wird es schwieriger, gefälschte Produkte als solche zu identifizieren und zu melden. Da die eigentlichen Produkteigenschaften von den gefälschten Produkten nicht erfüllt werden, erodiert das Vertrauen in die Originalhersteller. Auch die Sicherheit, insbesondere beim Einbau in weitere Produkte und Systeme, wird massiv beeinträchtigt.

Der starke Anstieg von Paketverkehr und Expressdiensten steigert zum Beispiel bei Einfuhr und Verteilung von gefälschten Pharma- und Elektronikprodukten den Zugang zu den Verbrauchern, prognostizieren Europol und das European Intellectual Property Office (IPO).[65] Eine EU-Regulation (Regulation (EU) No 608/2013) ermöglicht ein vereinfachtes Prüfverfahren bei

62 OECD/EUIPO: Trade in Counterfeit Pharmaceutical Products“, Report. 2020. Seiten 45 ff. http://www.oecd.org/gov/trade-in-counterfeit-pharmaceutical-products-a7c7e054-en.htm

63 Bundeszentrale für Politische Bildung: Leere Körper, Zeitschrift Fluter Nr. 50, https://www.fluter.de/sites/default/files/leere_koerper.pdf

64 Europarat: Organ transplant tourism, Resolution 2327. 2020. http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=28600&lang=en#

65 Europol and the European Union Intellectual Property Office (EUIPO): 2017 Situation Report on Counterfeiting and Piracy in the European Union, Report. 2017. https://www.europol.europa.eu/publications-documents/2017-situation-report-counterfeiting-and-piracy-in-european-union

kleinen Versandstücken und gibt so den Kontroll- und Strafverfolgungsbehörden nur sehr begrenzten Zugriff auf Daten über Herkunft, Transportmittel und -wege. Auffallend ist dementsprechend der Trend, gefälschte hochpreisige oder technisch anspruchsvolle Produkte wie Smartphones, E-Zigaretten und Tabakerhitzungssysteme, aber auch Ersatzteile für technische Geräte und Kraftfahrzeuge im „Ameisenverkehr" in Einzelstücken oder kleinen Mengen postalisch direkt an Käuferinnen und Käufer zu senden und so aktuelle Kontrollmethoden von Zoll und Polizei zu unterlaufen. Die wirtschaftlichen Akteure, von Patentberechtigten über Handelsunternehmen bis zu den Paketdiensten, die für solche kriminellen Aktivitäten genutzt werden, haben dabei kaum eine Möglichkeit, illegalen Warenverkehr zu entdecken. So können kriminelle Massenprodukte aus aller Welt fast gefahrlos in die EU und nach Deutschland geliefert werden. Das bisherige verfügbare Fachpersonal bei Polizei und Zoll kann aus Kapazitätsgründen nur genau definierte gefährliche Produkte im offenen Netz und im Darknet beobachten. Es ist davon auszugehen, dass sich dieses Problem zukünftig noch verschärfen wird, falls nicht die Reaktionszeit von Strafverfolgungsbehörden beschleunigt wird. Strafprozessuale Probleme ergeben sich etwa hinsichtlich der Zuständigkeit der jeweiligen Strafverfolgungsbehörden bei der Bestimmung des Tatorts in Fällen von Massenkriminalität, im globalen Rechtshilfeverkehr zur Vernehmung, Beweiserhebung oder vorläufigen Festnahme zwecks Auslieferung oder bei der Vermögensabschöpfung der illegalen Gewinne.

Auch die gelegentliche Schließung von Marktplätzen im Internet wird kurz- und mittelfristig einem weiteren Anstieg dieser Kriminalität keinen Einhalt gebieten, zumal zu erwarten ist, dass die Schließung bedeutsamer krimineller Marktplätze wie des „Wall Street Market" wohl zu einem Anstieg von etwas kleineren Marktplätzen im Darknet und im offenen Netz führen wird, die sich auf spezifische Sprachen, Nationalitäten und ethnische Gruppen spezialisieren.[66]

Desinformation kann durch den Einsatz digitaler Medien und KI (zum Beispiel Deepfakes) immer glaubwürdiger gestaltet, durch Bots in die breite Masse getragen und so zu gefährlichen Instrumenten in Politik und wirtschaftlichem Wettbewerb entwickelt werden. Auch im wirtschaftlichen und politischen Kontext besteht die Gefahr, dass Konkurrentinnen und Konkurrenten mit Hilfe krimineller Spezialistinnen und Spezialisten oder der OK zur Verfolgung ihrer Geschäftsinteressen und politischer Interessen solche Instrumente einsetzen.[67] Die Europäische Kommission hat bereits 2018 mit einem Aktionsplan gegen Desinformation das Bedrohungspotenzial durch Desinformationskampagnen als sehr hoch beschrieben und Gegenmaßnahmen formuliert.[68]

KI wird bei Deepfakes in Bild- und Tonmanipulationen neue Varianten bringen, die für die Öffentlichkeit, aber auch für Expertinnen und Experten kaum erkennbar sind und somit in Politik und Wirtschaft (CEO-Fraud, politische und wirtschaftliche Beeinflussung) enormes Schadenspotenzial aufweisen. Allgemein besteht die Gefahr, dass sich OK schon in den nächsten Jahren der Möglichkeiten von KI in einer großen Vielfalt von kriminellen Aktivitäten bedienen könnte, insbesondere im Bereich des illegalen Handels.

66 Europol: Internet Organised Crime Threat Assessment (IOCTA). Report, 2018. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018

67 ASW Bundesverband, Complexium, Deloitte: Desinformation – Lage, Prognose und Abwehr, 2017. https://asw-bundesverband.de/fileadmin/user_upload/dokumente/Studien_etc/studie_desinformation.pdf

68 Europäische Kommission: Aktionsplan gegen Desinformation. 2018, Report. https://eeas.europa.eu/sites/eeas/files/aktionsplan_gegen_desinformation.pdf

Fazit: Durch die geschilderten Möglichkeiten wird „Crime as a service“ im digitalen Raum zu einem höchst bedeutsamen Geschäftsmodell, auf das sich OK und neue flexible Tätergruppen spezialisieren.[69]

Neue Begehungsformen und Gewinnchancen in der virtuellen Welt des Internets lassen befürchten, dass in den kommenden Jahren kriminelle Gewinne und Investitionen ebenso wie politische, wirtschaftliche und soziale Macht von OK zunehmen könnten. Gewinne würden dann mit stark steigender Tendenz durch raffinierte Geldwäschemechanismen im Netz (Cryptocurrency) gesichert und reinvestiert.

4.4 Aktuelle staatliche Gegenstrategien und Konzepte

Das bislang nur unzureichend auf Resilienz setzende Cybersicherheitskonzept Deutschlands sollte ausgebaut werden. Der Nachholbedarf in Bezug auf IT-Sicherheit ist gewaltig. Relevante Veränderungen werden in der deutschen Sicherheitspolitik nur punktuell und in Ansätzen berücksichtigt. Deutsche Strategien und Konzepte beruhen in erster Linie auf kürzlich stattgefundenen Störungen der IT-Landschaft und Attacken auf Systeme sowie auf Lageberichten, die sich auf erstattete Anzeigen, abgeschlossene Ermittlungsverfahren oder Verurteilungen stützen. Beispielhaft dafür ist die politisch und öffentlich aufmerksam wahrgenommene Polizeiliche Kriminalstatistik (PKS), die in aller Regel polizeilich bekannte Sachverhalte von vor zwei Jahren beschreibt. Die PKS 2019 lässt wenig Schlussfolgerungen und Prognosen zu Cybersecurity und Cybercrime für die nächsten drei bis fünf Jahre zu, zumal gerade im Bereich Cybercrime ein extrem hohes Dunkelfeld besteht. Das BKA schätzt, dass allenfalls zehn Prozent ins Hellfeld kommen[70]. Während es schon klare Aussagen zur künftigen technologischen, soziologischen und ökonomischen Entwicklung im digitalen Raum und seinen Auswirkungen gibt, liegen diese in der Sicherheitsforschung, der Kriminologie und der Kriminalistik kaum und in der politischen Umsetzung nur begrenzt vor. Mehr Aufschluss über Art, Dynamik und Tendenz der kriminellen Entwicklung wird der periodische Sicherheitsbericht bieten, der Anfang 2021 erscheinen soll.

Zur Cybersecurity erklärt das BSI, dass die Abwehr von Cyberangriffen auch in einer weiterhin angespannten IT-Sicherheitslage in Deutschland erfolgreich sei, obwohl die Qualität vieler Cyberangriffe zugenommen hat. Aus Sicht des BSI könnten „die Schutzmaßnahmen des Bundesamts für Sicherheit in der Informationstechnik (BSI) die Informationssicherheit in den Regierungsnetzen und bei Kritischen Infrastrukturen gewährleisten”[71]. Dabei stellt sich vor allem die Frage, ob eine ausreichende Resilienz der IT-Sicherheitsstruktur derzeit wirklich gegeben ist. Auch im Bereich IT-Sicherheitsforschung besteht weiterhin ein großer Forschungsbedarf, gerade auch unter dem Gesichtspunkt digitaler Souveränität. Mit den drei etablierten und international renommierten Kompetenzzentren für IT-Sicherheitsforschung ATHENE (zuvor CRISP), CISPA, und KASTEL[72] hat Deutschland hier in den vergangenen Jahren eine solide Basis etabliert.

Das Niveau der Cybersicherheit in Deutschland lässt sich aber nicht gleichermaßen für deutsche Industrie- und Wirtschaftsunternehmen, die Gesellschaft und die Bürgerinnen und Bürger bewerten. Die vielfältigen und komplexen Angriffsmöglichkeiten erfordern Kompetenzen und Personal in unterschiedlichsten Bereichen der Cybersicherheit, die von einzelnen Unternehmen, kommunalen Verwaltungen oder Privatpersonen kaum geleistet werden können.

69 Europol: Internet Organised Crime Threat Assessment (IOCTA). Report, 2018.
https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018

70 Münch/BKA: Potsdamer Konferenz für Nationale Cybersicherheit, 23.5.2019.

71 BSI Lagebericht zu IT Sicherheit in Deutschland 2019

72 ATHENE: Nationales Forschungszentrum für angewandte Cybersicherheit, Fraunhofer-Gesellschaft. https://www.athene-center.de/. Zuvor CRISP: Center for Research in Security and Privacy.
CISPA: Helmholtz Center for Information Security. https://cispa.saarland/de/research/
KASTEL: Kompetenzzentrum für angewandte Sicherheitstechnologie, Karlsruher Institut für Technologie. https://www.kastel.kit.edu/index.php

Noch verwundbarer als Industrie und Wirtschaft sind Gesellschaft und Familien. Die privaten Haushalte öffnen vielfach bildlich gesprochen Tür und Tor im digitalen Raum, um Innovationen und Komfortfunktionen in unterschiedlichsten Geräten – von Haushaltsgeräten über Telekommunikation bis hin zu Herzschrittmachern und anderen medizinischen Hilfsmitteln – zu nutzen. Damit gehen technische Sicherheitsrisiken, Einfallstore und Datenweitergabe einher, die von der Kriminalität für Angriffe ausgenutzt werden können. Dass staatliche und rechtliche Fürsorge und Vorsorge sowie Standardisierung Bürgerinnen und Bürger und die Gesellschaft im digitalen Raum angemessen schützen, ist eine besonders anspruchsvolle staatliche Aufgabe, zumal eine Cyberattacke gegen einen Staat oder ein Versorgungsunternehmen bei einem Kollateralschaden auch Privatpersonen und Wirtschaftsunternehmen trifft. Daher ist in diesem Bereich eine Bündelung von Kompetenzen und Ressourcen erforderlich, um ein hohes Maß an Sicherheit auch im Bereich der nicht kritischen Infrastruktur zu erreichen und zu verhindern, dass Nutzerinnen und Nutzer auf Sicherheitskonzepte und Bekämpfungsmaßnahmen der Global Player der IT angewiesen sind.

Eine zu prüfende Möglichkeit zur Qualitätsverbesserung in der Verbrechensbekämpfung könnte in der Übernahme vereinbarter europäischer Standards zur strategischen und konzeptionellen Planung der Bekämpfung von Kriminalität liegen. Deutschland kann von Best Practices auf der Ebene der EU und einiger Mitgliedsstaaten lernen. Die EU hat mit dem sogenannten EMPACT Cycle[73] beispielsweise ein dynamisches, sich ständig an Veränderungen anpassendes System entwickelt und umgesetzt.

So erstellt Europol im Rahmen des EMPACT Cycle permanent Analysen zu schwerer Kriminalität, Organisierter Kriminalität, Cybercrime und Terrorismus, die es der EU ermöglichen, eine zukunftsorientierte Sicherheitsagenda – aktuell für 2019 bis 2021 – festzulegen und im Verlauf permanent anzupassen. Diese Bedrohungs- und Risikoanalyse ergibt sich aus Beiträgen der Mitglieds- und Partnerstaaten, anderer EU-Agenturen wie die Grenz- und Küstenwache Frontex, das Europäische Amt für Betrugsbekämpfung (OLAF) und die Agentur der Europäischen Union für justizielle Zusammenarbeit in Strafsachen Eurojust sowie internationaler Organisationen wie die Vereinten Nationen, die Internationale kriminalpolizeiliche Organisation Interpol, die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) und der Arbeitskreis Financial Action Task Force on Money Laundering (FATF), die mit Forschungen und Prognosen namhafter Wissenschaftlerinnen und Wissenschaftler und eigenen Berechnungen und Erkenntnissen ergänzt werden. Auf dieser Basis werden durch den ständigen Ausschuss der EU für operative Zusammenarbeit im Bereich der inneren Sicherheit (COSI) mehrjährige Strategiepläne für die prioritären Kriminalitätsbereiche festgelegt, die dann mittels operativer Aktionspläne und Berichterstattung verfolgt werden. Im letzten Schritt wird eine Prüfung und Bewertung durch die EU-Kommission und den COSI durchgeführt. Damit wird die klassische, reaktiv geprägte Bekämpfung von Kriminalität mit wesentlichen proaktiven Elementen versehen, um so Strafverhütung, Strafverfolgung und Aufrechterhaltung der Öffentlichen Sicherheit und Ordnung mit Hilfe moderner rechtlicher, ordnungs- und finanzpolitischer Regelungen und Maßnahmen eng miteinander zu verknüpfen. Zusätzlich wird ein Innovationslabor bei Europol geschaffen, das den Innovations- und Technologietransfer beschleunigen soll[74].

Wie Fälle in der Vergangenheit wiederholt verdeutlicht haben, mangelt es den Ermittlungs- und Strafverfolgungsbehörden in Deutschland aktuell oft an einem stringenten Konzept sowie ausreichenden Kapazitäten für effektive und erfolgreiche Ermittlungsarbeit im digitalen

73 Die EU hat im Frühjahr 2017 mit einer Laufzeit bis 2021 ihren aktuellen Vierjahresplan für die Bekämpfung der schweren und organisierten Kriminalität angenommen. Europäischer Rat. https://www.consilium.europa.eu/de/policies/eu-fight-against-organised-crime-2018-2021/

74 Beschluss der Innen- und Justizminister der EU vom 8.10.2019.

Raum. Insbesondere neue Begehungsformen und hoch agile Tätergruppen stellen etablierte behördliche Strukturen und Prozesse vor erhebliche Herausforderungen. Großen international organisierten und verübten Straftaten (beispielsweise Manipulation des Libor, Cum-Ex-Straftaten oder der internationalen Wirtschaftskriminalität), welche auch unter Beteiligung deutscher Staatsangehöriger und Organisationen stattfanden, konnten die deutschen Behörden daher teils nur unter Zuhilfenahme von Informationen und Ermittlungsfähigkeiten ausländischer Partner nachgehen. Dies zeigt deutlich, dass in der technischen und personellen Ausstattung, der Organisation sowie der Schulung von Mitarbeiterinnen und Mitarbeitern von unter anderem Staatsanwaltschaften, Kriminalpolizeien, der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) oder der Steuerfahndungen fortdauernder Handlungs- und Anpassungsbedarf besteht, um mit den Entwicklungen der OK im digitalen Raum bestmöglich Schritt halten zu können.

Eine immer größere und wichtigere Rolle im digitalen Raum kommt zudem Whistleblowerinnen und Whistleblowern, Journalistinnen und Journalisten sowie Bloggerinnen und Bloggern zu, ohne deren Enthüllungen und investigative Recherchen viele Ermittlungen gar nicht begonnen und erfolgreich beendet worden wären, zum Beispiel im Fall der sogenannten Panama Papers.

In Deutschland sind in den vergangenen Jahren viele rechtliche Normen modifiziert, neues Personal eingestellt, moderne Technik beschafft und Aus- sowie Fortbildung verändert worden. Das BKA und die deutschen Polizeibehörden sind dabei, die Cyberkompetenz auszubauen. Im BKA zum Beispiel existiert seit Neuestem die Abteilung Cybercrime mit mehr als 100 Mitarbeitenden, die in wenigen Jahren auf 280 Mitarbeiterinnen und Mitarbeiter anwachsen soll. Allerdings wirken die bürokratischen Hürden, Rekrutierungsprobleme, mangelnde Optionen für Aus- und Fortbildung und langsame Entscheidungsprozesse kontraproduktiv. Das übergreifende Informationsmanagement zwischen Behörden und Ministerien muss fortwährend auf Effizienz und Effektivität geprüft werden. Hierfür bietet das Konzept „Polizei 2020“ eines interoperablen Datenhauses eine gut geeignete Basis und könnte einen deutlichen Fortschritt leisten. Das Projekt müsste äußerst zügig und unter Wahrung hoher Datenschutzstandards umgesetzt werden. Grundlage ist die sogenannte Saarbrücker Agenda, auf die sich die Innenministerinnen und -minister des Bundes und der Länder bereits am 30. November 2016 verständigt hatten.

Die wirksame Bekämpfung von Geldwäsche ist bereits heute eine große Herausforderung. Sie wird für deutsche Behörden durch das komplexe Zusammenspiel internationaler Institutionen und unterschiedlicher Rechtsräume erschwert. Präventionsmaßnahmen gegen Geldwäsche, die in Deutschland und Europa auf dem Prinzip der Legitimationsprüfung „Know your Customer“ aufbauen, werden mit den bestehenden Instrumenten womöglich keine Erfolge erzielen können. Auf Ermittlungen zu illegalen Finanzströmen unter Nutzung von Cryptocurrency, die schon in den kommenden Jahren das bevorzugte Zahlungsmittel für illegalen Handel und Dienstleistungen werden könnte, scheinen deutsche Strafverfolgungsbehörden noch nicht ausreichend vorbereitet zu sein. Künftige High Privacy Cryptocurrency könnte das Problem für Ermittlungsbehörden verschärfen.

Ausgewogene demokratische Souveränität, das Machtmonopol des Staates und die sich daraus ergebenden politischen, wirtschaftlichen und sozialen Strategien sind durch monopolartige Stellungen von Technologieunternehmen, die unseren Alltag bestimmen, bedroht. Schon jetzt sind kleinere EU-Staaten wie Irland volkswirtschaftlich sehr von IT-Konzernen abhängig. Zusätzlich werden technische Innovationen aus der privaten Wirtschaft zunehmend zu Auslösern und Treibern der Technisierung der Sicherheit. Um zu verhindern, dass staatliche Sicherheitskonzepte künftig ausschließlich von der Adaption privater Systeme abhängig sind, kommt der eigenen Entwicklung technischer Sicherungssysteme eine zentrale Rolle zu. Der Erfolg von Prävention gegen und Strafverfolgung von Missbrauchsdarstellungen, Hasskriminali-

tät und illegalen Produkten und Dienstleistungen im Netz, insbesondere in Social Media, hängen ohne ausreichendes staatliches Handeln andernfalls nur noch von der Bereitschaft und dem tatsächlichen Tätigwerden von Facebook, Google, Amazon und anderen ab.

Unser System staatlicher Gewährleistung von Öffentlicher Sicherheit und Ordnung sowie von Kriminalitätsbekämpfung wird im digitalen Raum vor neue Herausforderungen gestellt, für die auch neue Antworten gefunden werden müssen. Gleiches gilt für die Fähigkeiten von Industrie, Handel und Bevölkerung, um sich selbst wirkungsvoll zu schützen. Die uns aus der analogen Welt vertrauten Mechanismen der Strafverfolgung greifen nur unzureichend, wenn die Ursache einer Sicherheitsbedrohung oder der eigentliche kriminelle Tatort außerhalb des deutschen Hoheitsbereichs liegen. Die für Cybersecurity und Cybercrime so bedeutsamen Notwendigkeiten von Prävention, Detektion und Repression, deren Bewältigung sich auf nationaler Ebene bereits schwierig gestaltet, weiten sich sehr schnell zu einem Problem der Koordination aus, wenn Sachverhalte außerhalb der EU liegen.

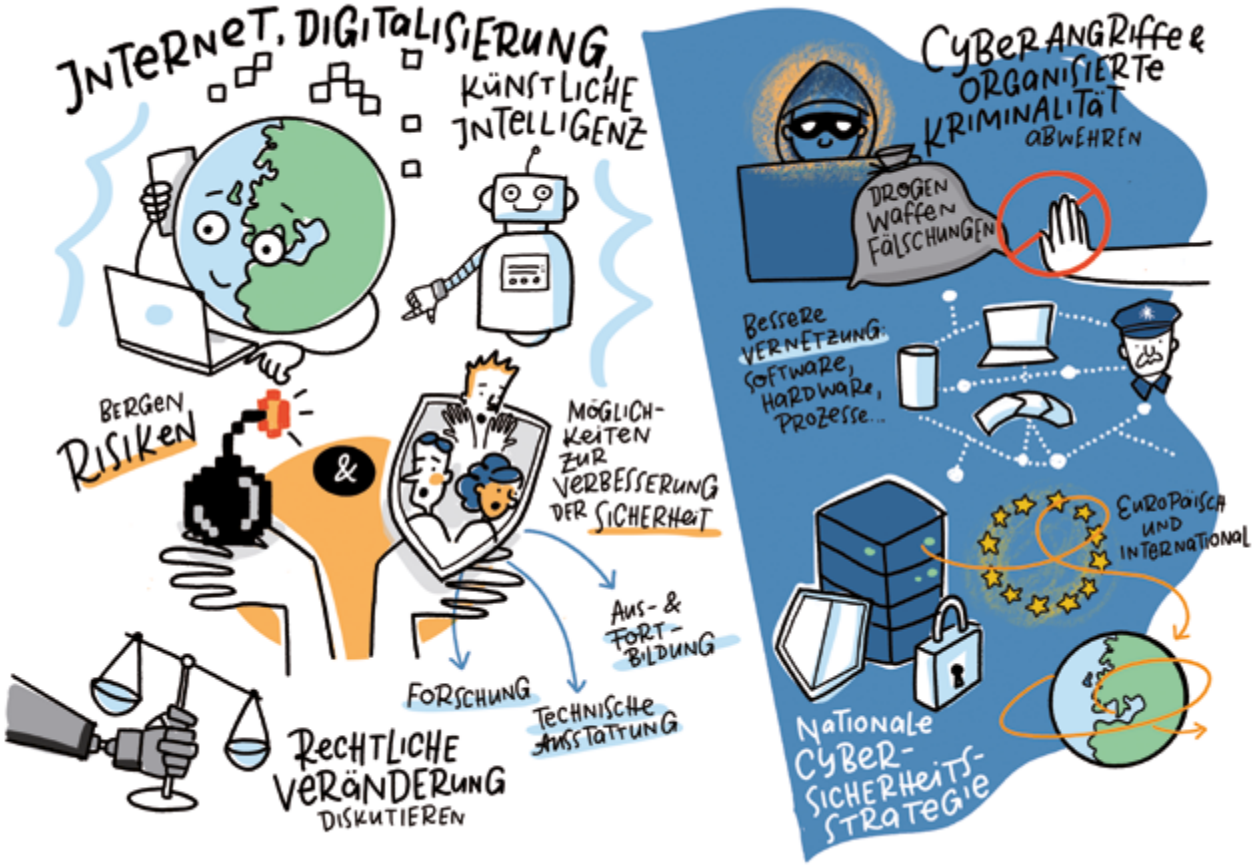
Kooperation der Strafverfolgungsbehörden wird insofern immer wichtiger. Mit dem Vertrag von Lissabon sind bestimmte hoheitliche Zuständigkeiten von den Mitgliedsstaaten auf Rat, Kommission und Agenturen der Europäischen Union wie zum Beispiel Europol, OLAF und Eurojust übergegangen sind oder werden, beispielsweise auf die Europäische Staatsanwaltschaft. Hierbei bedarf es weiterer Harmonisierung des Strafrechts und des Strafprozessrechts, einer wirksamen Rechts- und Fachaufsicht europäischer Agenturen und ausreichender parlamentarischen Kontrolle der politischen Institutionen. Zudem muss die ausreichende Finanzierung der EU-Agenturen gewährleistet sein. Zwar sind in den vergangenen Jahren im Rahmen der Vereinten Nationen, des Europarats und der Europäischen Union eine Vielzahl von Strafrechtskonventionen und Kooperationsvereinbarungen getroffen worden. Trotzdem bleiben strafprozessuale Hindernisse, wie im Abschnitt Risiken durch Angriffe im digitalen Raum erläutert, eine Schwachstelle in der Bekämpfung von globalisiertem Verbrechen durch deutsche und europäische Behörden und im globalen Rahmen, denn die notwendige Ausarbeitung und politische Verhandlung solcher Rechtswerke ist kleinteilig und zeitaufwendig. In diesem Zeitrahmen können sich aus der Weiterentwicklung des Netzes und den sich daraus ergebenden neuen Formen von Produktion, Transport, Bankenhandel und Kommunikation die Möglichkeiten und die Gefahren für unsere Gesellschaft und Wirtschaft oft schon grundlegend verändert haben.

Hoffnungsvoll stimmen aber die bisherigen und künftigen Planungen und deren Umsetzung, die unter der deutschen Ratspräsidentschaft weitergetrieben werden sollen. Richtige Schritte waren die rasche Errichtung und der permanente Ausbau des Cyberzentrums bei Europol, die Entwicklung und Inbetriebnahme des Informationssystems SIENA oder auch die EU-Richtlinie zur Bekämpfung von Organisierter Kriminalität beziehungsweise die 5. EU-Geldwäscherichtlinie von 2018. Auch die internationalen Joint Investigation Teams, deren Einrichtung die EU ermöglicht, haben sich bewährt und werden von den meisten EU-Staaten zunehmend angenommen. Deutsche Behörden beteiligen sich oft an solchen Teams, rufen sie aber nur selten national oder international ins Leben.

Ein weiterer wichtiger Pfeiler der Sicherheitsarchitektur in Deutschland ist die Sicherheitsforschung, welche scheinbar einen hohen Stellenwert für Politik und Gesellschaft besitzt. Auf der Bundesebene werden bereits drei Kompetenzzentren für IT-Sicherheit gefördert, die in den letzten zehn Jahren gegründet wurden: ATHENE (zuvor CRISP), CISPA, und KASTEL. Diese Institute fokussieren auf technische Sicherheitsprobleme aus der IT-Perspektive und leisten auf diesem Gebiet bereits hervorragende Arbeit. Ob damit der ganzheitliche und nachhaltige Bedarf der Sicherheitsbehörden – auch im Benchmark mit anderen Staaten – befriedigt wird, muss hinterfragt und geprüft werden. Zusätzlich wird seit 2012 das eigene Förderprogramm „Forschung für die zivile

Sicherheit“ vom Bundesministerium für Bildung und Forschung gemeinsam mit dem Bundesministerium für Inneres, Bau und Heimat angeboten. Hier können Kommunen und Sicherheitsbehörden gemeinsam mit Forscherinnen und Forschern sowie Entwicklerinnen und Entwicklern aus Wissenschaft und Wirtschaft eine Förderung für konkrete Projektvorhaben zur Pilotierung oder Demonstration von innovativen Ansätzen beantragen. Auch auf der EU-Ebene können im EU-Forschungsprogramm „Horizont 2020“ Projekte unterstützt werden.

Während diese Art der Forschungsförderung im Prinzip gut geeignet ist, um Innovationen aus der Wissenschaft in die praktische Anwendung zu überführen, kann in der praktischen Umsetzung nach bisherigen Erfahrungen nur eingeschränkt grundlegende Forschung angeregt werden, die direkt aus dem alltäglichen Bedarf der Sicherheitsbehörden entsteht. Dadurch scheint eine Kleinteiligkeit beim Technologietransfer zu entstehen, die zur strategischen Ausrichtung nicht förderlich ist. Zusätzlich sind die in der Wissenschaft notwendigen Zeiträume für die Durchführung von Forschungsvorhaben aus Sicht der Bedarfsstellen zu lang, und häufig fehlen konkrete Ergebnisse, die direkt in die Praxis übernommen werden können. Auch fehlt ein Forschungs- und Innovationstransferansatz, der Sicherheitsbehörden und Wissenschaft zusammenbringt, um besser zukünftige Gefährdungen der Öffentlichen Sicherheit durch neue Technologien und kriminelle Geschäftsmodelle noch frühzeitiger zu erkennen. Solche Anwenderlabore könnten Innovationen beschleunigen. Problematisch ist nicht zuletzt die Zeitdauer zwischen Ausschreibung des Förderprogramms und Vergabe sowie Beendigung der Forschung und Implementierung – hier böte sich eine stärkere Beteiligung der späteren Nutzer an der Forschung an.



4.5 Empfehlungen zur Gewährleistung von Cybersecurity und der effektiven Bekämpfung von Cybercrime und OK in Deutschland

Die vielfältigen Risiken, Herausforderungen und Schwächen in der bestehenden Sicherheitsinfrastruktur erfordern ein entschlossenes, integratives und konsistentes Handeln. Dazu empfehlen wir:

Entwickeln einer adaptiven nationalen Cybersicherheitsstrategie

Die nationale Cybersicherheitsstrategie bedarf der Aktualisierung und Erweiterung. Sie sollte auf einer Grundlage von umfassenden Informationen und Analysen stehen, mit der Strategie der EU kompatibel sein und globale Strategien fortlaufend berücksichtigen. Sie sollte über eine Zielsetzung mit Zwischenzielen, jährlicher Evaluierung, genauem Zeitplan und Flexibilität zur Berücksichtigung noch jetzt unbekannter technischer, rechtlicher, politischer und sozialer Veränderungen verfügen. Cybersecurity sollte auch politisch Chefsache sein. In diese Cybersicherheitsstrategie ist als wichtiger Pfeiler eine Cybercrimestrategie einzufügen. Technische Cybersecurity und Bekämpfung von Cybercrime haben sich zu ergänzen.

Cybersicherheitsstrategie neu denken:

Um die Strategie aktuell und effektiv zu halten, sind Mechanismen und Instrumente zur Beobachtung und Prognose der technologischen Veränderungen, der politischen, wirtschaftlichen und sozialen Nutzung des digitalen Raumes und der Risiken und Bedrohungen von Cybersecurity durch Cybercrime (und Cyberwarfare) herauszubilden. Sie sind so zu gestalten, dass sie in der Gesamtstrategie und in unmittelbaren Schutzmaßnahmen umgesetzt werden können. Andere Staaten oder die EU-Agentur Europol[75] bedienen sich dazu einer permanenten Risiko- und Gefährdungsanalyse. In diesem Rahmen ist eine Beteiligung von Stakeholdern in Gesellschaft, Technologie und Wirtschaft zwingend erforderlich.

Um den globalen Herausforderungen Rechnung zu tragen, sollten die traditionellen Betrachtungsweisen und aktuellen Methoden und Strukturen deutscher und europäischer Sicherheitspolitik mit neuen Perspektiven ergänzt werden und dabei natürlich auch neue Erkenntnisse und Empfehlungen aus politischen, sozialen und ökonomischen Strategien aufgenommen werden. Die EU und Deutschland müssen neue Ansätze in der Verbrechensbekämpfung, der Strafverfolgung und der kriminalistischen Ausbildung finden.

Digitalpolitik muss als Teil der Sicherheitspolitik verstanden werden. Künstliche Intelligenz und

> *Wir halten eine fachübergreifende Cyberstrategie für unbedingt und zeitnah erforderlich – nicht nur eine Risiko- und Gefährdungsstrategie, sondern auch eine Umsetzungsstrategie. Cybersicherheit darf künftig politisch nicht nur als Nebenprodukt gesehen werden. Vielmehr müssen bei gesetzlichen Regelungen im IT-Bereich nicht nur die haushalterischen Auswirkungen dargestellt werden, sondern auch die für den Cybersicherheitsbereich. Die Umsetzungsstrategie sollte umgehend, also noch in dieser Wahlperiode, erstellt werden, zwecks Implementierung zum Zeitpunkt der Regierungsbildung im Herbst 2021."*
> ***– Susanne Mittag MdB***

75 Europol: Internet Organised Crime Threat Assessment (IOCTA), Report, 2019. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019

anderen Schlüsseltechnologien müssen verstärkt hinsichtlich ihrer sicherheitstechnischen Implikationen berücksichtigt und in eine digitale Sicherheitsstrategie überführt werden. Eine solche Cybersicherheitsstrategie erfordert bereits in der Digital-, Industrie- und Forschungspolitik die Berücksichtigung sicherheitskritischer oder -gefährdender Risiken. Dabei müssen die Wertegrundlagen der EU und Deutschlands Priorität haben.

virtueller Zahlungsmittel –, Innovationsbereitschaft von Politik, Gesellschaft und Wirtschaft und zeitgerechte Umsetzung von Erkenntnissen sowie Best Practices anderer Staaten.

Da Zukunftsprognosen natürlich einen teilweise erheblichen Unsicherheitsfaktor in sich tragen, sind Strategien und Konzepte flexibel zu gestalten, um künftigen Herausforderungen proaktiv, effektiv und effizient begegnen zu können. Außerdem empfiehlt es sich, ein sorgfältiges lang-, mittel- und kurzfristiges Zeitmanagement vorzusehen, um Kontinuität mit schneller Reaktion auf politische, rechtliche, soziale und vor allem technologische Veränderungen zu verbinden.

> *Unsere Sicherheitsbehörden sind tagtäglich gefordert, Kriminalität wirksam zu bekämpfen – dies gilt mehr denn je online wie offline! Wie das Szenario verdeutlicht, nehmen der Umfang und die Herausforderungen durch Organisierte Kriminalität im digitalen Raum in rasendem Tempo zu. Es ist deshalb zwingend nötig, dass wir unseren Beamtinnen und Beamten die passenden Werkzeuge an die Hand geben, die sie brauchen, um Kriminellen schnell und wirksam das Handwerk zu legen. Wenn es um Verbrechensbekämpfung geht, kann und darf es nicht zweierlei Maßstab geben!“* ***– Michael Kuffer MdB***

Analyse- und Planungsfähigkeit stärken:

Die strategische, konzeptionelle Planung zur Bekämpfung von Kriminalität sollte so weiterentwickelt werden, dass ein dynamisches, sich ständig an Veränderungen anpassendes Planungssystem entwickelt und umgesetzt werden kann. Hier bietet es sich an, die in Europa vereinbarten und in einigen Mitgliedsstaaten praktizierten Standards zu analysieren und in Bezug auf die Anwendbarkeit in Deutschland zu bewerten. Für ein solches Planungsinstrument sollte geprüft werden, ob eine Kompatibilität zu dem EMPACT Cycle der EU sinnvoll und realisierbar ist. Dieser dynamische Planungsprozess sollte neben aktuellen nationalen und internationalen Daten von Polizei und Sicherheitsbehörden und deren regelmäßigen Risiko- und Bedrohungsanalysen ebenfalls neue Ergebnisse der wissenschaftlichen Forschung berücksichtigen. Ebenso sollte Folgendes einbezogen werden: eine realistische Einschätzung der Kompetenz und Einsatzfähigkeit von Justiz, Polizei und sonstigen Sicherheitsbehörden, gesellschaftliche und wirtschaftliche Veränderungen – zum Beispiel auf Grund sozialer Medien oder

Kontinuierliche Adaptivität der Strategie sicherstellen:

Der Zeitfaktor spielt eine wichtige Rolle für Erfolg und Misserfolg von Strategien, Konzepten und Maßnahmen im digitalen Raum. Die dynamischen technischen und sozialen Veränderungen, die Globalisierung des Verbrechens sowie die virtuellen Dimensionen von Rechtsgut und Tatort schaffen Handlungsdruck für innovative politische, aber auch neue polizeiliche Strategien und Konzepte und Selbstschutzmaßnahmen der Wirtschaft. Die Aktions- und Reaktionszeit der Strafverfolgungsbehörden auf Bedrohungen, Risiken und Veränderungen im digitalen Raum müssen verkürzt werden. Wegen interdependenter Netzwerke muss die Politik permanent auf präventives und reaktives Krisenmanagement vorbereitet sein.

Internationale Kooperationen aufbauen und vertiefen:

Das internationale Informationsmanagement zu Cybersecurity, das weitgehend in informellen Netzwerken betrieben wird, muss über die EU hinaus global weiter ausgebaut werden. Gleiches gilt für das Informationsmanagement zu Cybercrime und OK, das teilweise bereits über Interpol, immer mehr im Rahmen von Europol, aber meist noch bilateral stattfindet. So können Cyberrisiken und Netzzusammenbrüche durch Sofortreaktionen wirkungsvoll verhindert oder deren Konsequenzen abgemildert werden. Phänomenbedingte internationale Allianzen, wie zum Beispiel auf der Ebene der Vereinten Nationen, sind ein geeignetes Mittel. Ermittlungen zu Cybercrime sind mit internationalen Teams oder parallelen, gut koordinierten nationalen Ermittlungen zu führen. Dies bedarf der Verbesserung der politischen, rechtlichen und methodischen Grundlagen.

Taskforces einsetzen:

Gerade aufgrund des sich immer schneller wandelnden digitalen Raumes, der Gefahren von Crashs für Kritische Infrastrukturen (KRITIS) und der sehr anpassungsfähigen Kriminalität kommt es darauf an, auf neue Bedrohungen und akute Beeinträchtigungen von KRITIS unmittelbar zu reagieren, das Ausmaß von kriminellen Aktivitäten und Schäden gering zu halten und Ermittlungen in kurzer Zeit justiziell entscheidungsreif zu machen. Hierfür bietet sich in vielen Fällen das Modell von Taskforces an. Rudimentär existiert so etwas für Informationsmanagement und Analyse im Gemeinsamen Terrorismusabwehrzentrum (GTAZ), für Drogen oder Zigarettenschmuggel in der Gemeinsamen Ermittlungsgruppe Rauschgift (GER) oder Zigaretten (GEZig) oder international für verschiedenste Kriminalitätsbereiche durch Joint Investigation Teams (JIT).

> *Die Forderung nach intensiverer internationaler Kooperation ist auch in Cybercrime und Organisierter Kriminalität absolut berechtigt, wäre für Deutschland jedoch der zweite Schritt vor dem ersten. Verstärkt über das Internet begangene Taten und somit strukturell oft ungeklärte Tatorte offenbaren, dass in Deutschland längst überfällige Reformen hinsichtlich Strukturen und föderaler Kooperation dringend angegangen werden müssen. Bund und Länder müssen sich dazu im Rahmen einer Föderalismuskommission an einen Tisch setzen.* ***– Benjamin Strasser MdB***

Implementieren einer resilienten Sicherheitsarchitektur

Die Umsetzung der Cybersicherheitsstrategie erfordert ein Bündel von Maßnahmen, die zu widerstandsfähigen IT-Strukturen in der Sicherheitsarchitektur führen. Wichtig ist hierbei überregional, intersektoral und integrierend zu denken und zu gestalten. Es werden präventive und situative Strukturen für die Cybersicherheit zu schaffen sein, die jeweils an aktuelle Anforderungen agil angepasst werden können. Solche Mechanismen sollten vorbereitet werden, um etwa bei plötzlichen Netzausfällen umfassende Handlungsfähigkeit sicherzustellen.

Wegen der Komplexität von Risiken im digitalen Raum und akuten Bedrohungen durch Cybercrime und OK ist ein mehrstufiger Aufbau empfehlenswert. Für die strategische Planungs- und Entscheidungsebene ist an eine ständige Arbeitsgruppe auf Ministerial- und Behördenleiterebene zu denken, die sich monatlich und zusätzlich anlassbezogen trifft, um politische Entscheidungen vorzubereiten und strategische Maßnahmen zu entscheiden.

Die strategische Ebene sollte je nach Bedarf Wissenschaft und Forschung sowie Wirtschaft und Gesellschaft einbeziehen. Auf taktischer Ebene dominieren Behörden von Bund und

Ländern eine Taskforce, die die strategischen Entscheidungen vorbereitet und dann auch umsetzt. Hier mag es eine Aufspaltung in eine taktische Arbeitsgruppe für die Sicherheit von Informationstechnologien sowie das Gefahren- und Risikopotenzial für und aus dem Netz einerseits und einer taktischen Arbeitsgruppe für polizeiliche und verwaltungsrechtliche Gefahrenabwehr und Ermittlungsaufgaben andererseits geben. Auf dieser Ebene ist auch das nationale Krisenmanagement anzusiedeln, wie es beim ersten Auftauchen von Emotet erforderlich gewesen wäre, denn Emotet gilt laut BSI als eine der größten Bedrohungen durch Schadsoftware weltweit und verursacht auch in Deutschland hohe Schäden[76]. Auch auf dieser Ebene empfiehlt es sich, zugunsten einer effektiven Analyse fachliche Kompetenz, innovative Methoden und Technologie aus Wirtschaft und Wissenschaft einzubeziehen.

Ergänzt werden sollte das mit operativen Taskforces, mit schnellen Einsatzkräften zur Identifizierung und Bewertung von Schadensfällen, ersten Schutzmaßnahmen und Ermittlungen.

Effektive Strukturen und Organisationen schaffen:

Unabhängig von der Einrichtung solcher Taskforces sind Strukturen und Organisationen zu überdenken: Bisher sind Zuständigkeiten für Cybersicherheit in Politik und Verwaltung breit gestreut. Institutionen sind oft nach jeweils augenblicklichem Bedarf eingerichtet worden, was zu einem Flickenteppich von nicht aufeinander abgestimmten Institutionen mit Überschneidungen und parallelem Agieren führt. Eine sinnvolle Koordination und Kooperation ist noch nicht gewährleistet. Ob die Gesamtverantwortung zentral bei einem Ministerium und einer Behörde festgelegt wird oder eine Netzwerkzuständigkeit gewählt wird, kann dahinstehen. Wichtig ist aber eine permanente Funktions- und Qualitätskontrolle – über jährliche Lage- und Rechenschaftsberichte hinaus mit anlassbezogenen Zwischen- und Spezialberichten, die sowohl im Parlament als auch in Behörden, Wirtschaft, Gesellschaft und Medien analysiert und diskutiert werden. Damit kann auch das Bewusstsein für Gefahren im digitalen Raum gestärkt werden.

Sicherheit durch Standards stärken:

Die Cybersicherheit von Produkten, die über IoT verbunden sind, hat entscheidende Bedeutung. Das BSI sollte nicht nur vornehmlich die Aufgabe haben, staatliche Institutionen und KRITIS zu schützen, sondern künftig noch stärker auch Verbraucherinnen und Verbraucher. Dafür ist das BSI in seiner Rolle weiter zu stärken. Regierung und BSI müssen in Kooperation mit der Industrie dafür sorgen, dass bereits in der Entwicklung von Produkten in allen Bereichen wirkungsvolle Cybersecurity eingebaut wird. Hierzu sollte geprüft werden, inwieweit die geltenden Regeln zur Produkthaftung im digitalen Raum ausreichend sind.

Aber auch der Nutzer von IoT sollte mitwirken. Inzwischen ist im angelsächsischen Raum ein sogenannter Code of Practice for Consumer IoT geschaffen worden. Dieser bietet Unterstützung für die Produktion von Waren, die IoT nutzen. International müssen dafür Grundlagen und Standards geschaffen werden, wie einen bindenden Industriestandard, der auf dem Code des Europäischen Instituts für Telekommunikationsstandards basiert.

Eine neue Kultur des Informationsmanagements und der Kooperation schaffen:

Informationsaustausch, Gefährdungsanalysen, Kooperationen und Maßnahmen sollten sich der Dynamik im nicht an Grenzen gebundenen digi-

76 Emotet liest die Kontaktbeziehungen und E-Mail-Inhalte aus den Postfächern infizierter Systeme aus. Es lädt weitere Schadsoftware nach, wie zum Beispiel den Banking-Trojaner Trickbot. Diese Schadprogramme führen zu Datenabfluss oder ermöglichen den Kriminellen die vollständige Kontrolle über das System. https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/emotet.html

talen Raum anpassen. Auch für den Bereich der systemischen Risiken ist es notwendig, Informationen aus unterschiedlichsten Quellen so zu integrieren, dass Analysen und Schlussfolgerungen in konkreten Situationen ermöglicht werden.

sicherzustellen, damit diese ihre Aufgaben bei der Bekämpfung von OK und Cybercrime erfüllen können. Wichtig ist hierbei, dass die Sicherheitsgewährleistung und die Ermittlungshoheit unter staatlicher Verantwortung verbleiben.

> *Neue Entwicklungen in der Informationstechnologie spielen auch bei den Sicherheitsbehörden eine immer größere Rolle. Mit neuen Anwendungen auf Grundlage der sogenannten Künstlichen Intelligenz verknüpfen Polizei, aber auch Geheimdienste zum Teil hoch sensible Datenbestände und werten große Datenmengen automatisiert aus. Programme zur Gesichtserkennung und Kriminalitätsprognose greifen dabei tief in Grundrechte auch völlig unbescholtener Bürgerinnen und Bürger ein und sind zugleich höchst fehleranfällig. Der Aspekt des Datenschutzes muss in der Polizeiarbeit eher gestärkt und nicht geschwächt werden. Dazu bedarf es einer stärkeren Regulierung und eines Bewusstseins, dass dem Einsatz bestimmter Technologien in einem Rechtsstaat klare Grenzen gesetzt sind."* ***– Dr. André Hahn MdB***

Angesichts des exponentiell zunehmenden Informationsumfangs ist zu prüfen, unter welchen Bedingungen insbesondere unter Beachtung grundrechtlicher Positionen der Einsatz von KI möglich und erforderlich ist, um die notwendigen Regulierungen, Kontrollen, Eingriffe und Ahndungen zeitlich und inhaltlich effektiv und effizient zu unterstützen.

Aufgrund der dynamischen Entwicklung im digitalen Raum und der neuartigen Risiken und Bedrohungen durch Cybercrime ist zu prüfen, in welchen Bereichen eine Bündelung von Kompetenzen und Ressourcen sinnvoll sein kann. Dies muss unter strikter Beachtung rechtsstaatlicher Prinzipien, des Gewaltmonopols des Staates sowie verfassungsrechtlicher Positionen von Bürgerinnen und Bürgern erfolgen.

Im Bereich der Prävention sollte dort, wo es sinnvoll erscheint, die Kooperation mit der Wirtschaft gesucht werden, um Informationen, Expertise und Technologien, wenn erforderlich, nutzbar zu machen. Dabei ist zu bedenken, dass der Übergang von privater Vorsorge und staatlicher Prävention fließend ist. Die sachliche und personelle Ausstattung der Strafverfolgungsbehörden ist im angemessenen Umfang

Präsenz im Netz erhöhen:

Insbesondere für Sicherheitsbehörden, Polizei und Zoll heißt es, im Netz präsent zu sein. Schon jetzt findet ein Großteil des Wirtschaftslebens im digitalen Raum statt. Kommunikation und soziales Leben spielen sich zunehmend in Social Media ab, und auch politische Arbeit und Verwaltungsabläufe vollziehen sich zu einem immer höheren Anteil im Netz. Auch Kriminalität wird entsprechend dieser Entwicklung folgen. Staat, Polizei, Justiz und Sicherheitsbehörden müssen imstande sein, ihre präventiven und repressiven Aufgaben zur Gewährleistung der Öffentlichen Sicherheit und Ordnung im virtuellen Raum besser wahrzunehmen. Hier sollte der Schwerpunkt auf Prävention durch Transparenz und Aufklärung liegen. Bürgerinnen und Bürger sowie Wirtschaftsunternehmen sind ständig über neue Gefahren und neue kriminelle Modi Operandi zu informieren.

Voraussetzungen schaffen

Sowohl die Strategieentwicklung als auch deren Umsetzung setzen umfangreiche Neuorientierungen in der Sicherheitsforschung, der Kompetenzbildung, im Risiko- und Bedrohungsbewusstsein aller Akteure sowie die Einbindung der Industrie und Wirtschaft voraus.

Sicherheitsforschung als unabdingbar verstehen:

Die Sicherheitsforschung ist in Deutschland auf der Ebene der Förderinstrumente grundsätzlich gut aufgestellt. Sie muss aber schneller und flexibler den immer neuen Anforderungen angepasst und künftig noch mehr als bisher als zwingender Bestandteil einer Sicherheitsstrategie verstanden werden. Dabei ist es wichtig, neben Rechtswissenschaft, Volkswirtschaft, Politologie, Kriminologie und Soziologie auch technische Entwicklungen und Kompetenzen zu berücksichtigen. Innovative Technologien oder Geschäftsmodelle bergen mitunter das Risiko neuer Herausforderungen für die Öffentliche Sicherheit. Die Neuerungen sollten frühzeitig auf relevante Auswirkungen, kriminelle Nutzungspotenziale, aber auch auf systemische Risiken untersucht werden. Die klassische Sicherheitstechnik erweitert sich vor dem Hintergrund der zunehmenden Vernetzung massiv und dehnt sich in bisher ungesicherte physische Systeme aus. Daher sollten Ingenieurwissenschaften und Informatik für die Beurteilung der Risiken und Chancen für die Öffentliche Sicherheit durch den digitalen Raum, Methoden der Künstlichen Intelligenz und insbesondere des Maschinellen Lernens auf vernetzte physische sowie sozio-digitale Systeme (KRITIS, Smart Home, Drohnen, Automotive, UAV und so weiter) einbezogen werden.

Die Verankerung von Forschungsprojekten und -ergebnissen in den Sicherheitsbehörden – also auf der Seite der Projektpartnerinnen und Projektpartner – ist noch ausbaufähig. Rechtswissenschaft, Volkswirtschaft, Politologie, Kriminologie und Soziologie müssen um entsprechende, für den digitalen Raum relevante Zukunftsforschung ergänzt werden. Ziel eines „Security Foresight“ muss es sein, die Sicherheit unter Aufrechterhaltung unserer demokratischen Werte, der Menschenrechte und unseres gesellschaftlichen Selbstverständnisses weiter zu verbessern, beispielsweise durch Förderprogramme, wie das „Forum Privatheit – Privatheit und selbstbestimmtes Leben in der digitalen Welt“. Die Untersuchung und Abschätzung von nicht intendierten Nebenfolgen technischer Systeme sollte Gegenstand jedes Entwicklungsprozesses sein, auch in Hinblick auf die Entwicklung, Einführung und Nutzung von Sicherheitstechnologien.

Allgemein sind Forschungsvorhaben im Sicherheitsbereich intensiver auf künftige Herausforderungen in der Öffentlichen Sicherheit wie bei Cybersecurity und im Cybercrime auszurichten. Die effektive und zeitnahe Umsetzung der Ergebnisse sollte die Regel und Teil der Planung werden. Gegenwärtig findet die Implementierung häufig erst mit erheblichem Verzug statt. Neben der disziplinären und sektoralen Zusammenarbeit sind in der Sicherheitsforschung auch die Kooperationsformen ausbaufähig. So zeigt sich beispielsweise in der KI, dass Innovationen sehr schnell in Bereichen angewendet werden, in denen bereits große Datenmengen verfügbar sind oder Start-ups sich mit neuen Ideen an den Markt trauen. In der Sicherheitsforschung bestehen aber nur eingeschränkt öffentlich zugängliche Daten, Prozesse und Modelle, da diese nicht nur positive Entwicklungen fördern, sondern auch in sich als Täterwissen fungieren können. Zusätzlich ist die Distanz zwischen Personen in der Grundlagenforschung und den Sicherheitsbehörden als Anwender relativ groß, da in den meisten Universitäten entsprechende Fachdisziplinen und Studienangebote für Kriminologie oder Forensik fehlen und somit kein direkter Kontakt zwischen Forschern und Anwendern besteht.

Ein wichtiges Ziel für die Sicherheitsforschung sollte es sein, die Geschwindigkeit des Innovations- und Technologietransfers zu erhöhen und den Informationsaustausch in Hinblick auf den Bedarf der Sicherheitsbehörden zu verbessern.

Für solche Kooperationsformen sollte es neben Kompetenzzentren in der Forschung mit ihren zwingenden disziplinären Schwerpunkten auch Anwendungslabore geben, in denen Sicherheitsbehörden besonders wichtige Herausforderungen der Praxis ins Zentrum stellen und geeignete Institutionen der Wissenschaft und Wirtschaft einbinden können. Auch zivilgesellschaftliche Expertise aus beispielsweise Hackathons oder ähnlichen Formaten leistet einen wichtigen Beitrag in der Weiterentwicklung von Sicherheitsanwendungen.

Kompetenzen für Sicherheitstechnik und Cybersicherheit bilden:

Eine hochwertige Aus- und permanente Fortbildung in Cybersicherheit sind die Grundlagen für Erfolg und Widerstandsfähigkeit von Staat und Gesellschaft. Sie müssen in den kommenden Jahren höchste Priorität haben. In Deutschland wächst das akademische Angebot zunehmend. Im Studienführer „Sicherheit studieren. Studienangebote in Deutschland 2.0“ werden immer mehr Studiengänge im Bereich IT-Sicherheit verzeichnet. Der Bedarf von gut ausgebildeten Fachkräften und Führungspersonal für IT, Vernetzung, Cybersecurity, aber auch für OK-Bekämpfung, wird aber wohl wesentlich schneller ansteigen. Die MINT-Fächer in den Schulen sind deutlich zu stärken. Ein flexibleres und innovativeres Dienstrecht und Personalmanagement sind fortwährend weiterzuentwickeln, um temporäre Personalwechsel zwischen Industrie, Wissenschaft und Öffentlichem Sektor zu ermöglichen. Zudem ist eine verbesserte Aufklärung über die bereits bestehenden Möglichkeiten im gegenseitigen flexiblen Personalmanagement notwendig.

Risiko- und Bedrohungsbewusstsein schaffen:

Politik, Regierungen und Verwaltungen, Industrie und Wirtschaft und insbesondere die Gesellschaft sind mit den Risiken der modernen Kommunikationslandschaft, der Existenz des IoT und deren Einfluss auf unser tägliches Leben noch besser vertraut zu machen. Nur mit einem umfassenden Cybersicherheitsbewusstsein sowie digitalen und sicherheitstechnischen Grundfähigkeiten und entsprechendem Verhalten der Bürgerinnen und Bürger können Angriffe weitgehend abgewehrt, Schäden minimiert und Gegenmaßnahmen wirkungsvoll getroffen werden. Hierzu gehört auch der Einsatz von moderner Verschlüsselungstechnik in der Kommunikation zum Schutze der Privatsphäre und persönlicher Daten.

In vielen Staaten gibt es dafür Awareness-Programme, die teilweise als Best Practice übernommen werden können. Das ist kein einmaliger Prozess, sondern sollte ein auf Dauer angelegtes Programm sein. Gleichzeitig muss eine Kommunikationsstrategie entwickelt werden, um die Öffentlichkeit auch bei fehlendem Bewusstsein für Risiken und Bedrohungen adäquat adressieren zu können. Bei Cyberrisiken handelt es sich für die Allgemeinheit nur auf der Auswirkungsseite um erfahrbare Risiken. Die eigentlichen technischen Vorgänge sind aber kaum wahrnehmbar. Daher muss die kommunikative Einbettung bei Alltagserfahrungen der Bürgerinnen und Bürger ansetzen und sollte nicht als Bedrohungskommunikation oder belehrend erfolgen. Cybersicherheit muss künftig Teil jeder politischen und fachlichen Beratung, Planung und Entscheidung für praktisch alle Lebensbereiche sein.

> *Die Bekämpfung der Organisierten Kriminalität ist und bleibt von hoher Bedeutung. Während der öffentliche Fokus oft auf besonders auffälligen Kriminalitätsphänomenen liegt, agieren einflussreiche Organisationen, wie zum Beispiel die Gruppen der Mafia und insbesondere der 'Ndrangheta, häufig eher unauffällig im Hintergrund. Dabei müssten gerade die oft fließenden Grenzen zwischen der Schattenwirtschaft und legalen Wirtschaftsbereichen stärker betrachtet werden, um eine Infiltrierung letzterer zu unterbinden. Im Spannungsfeld der IT-Sicherheit wird es in den kommenden Jahren vor allem darauf ankommen, die Resilienz unserer IT-Infrastrukturen deutlich zu erhöhen. Dazu zählen die Festsetzung von Sicherheitsstandards und der Verzicht auf sogenannte ‚Backdoors', die letztlich auch Kriminellen Angriffsmöglichkeiten bieten."*
>
> ***– Dr. Irene Mihalic MdB***

Wirtschaft, Industrie und Märkte einbinden:

Wirtschaft, Industrie und Märkte müssen mit sicherheitsrelevanten Herausforderungen durch OK im digitalen Raum Schritt halten.

Dafür gilt: Zur Verhütung und Bekämpfung von OK und zum Schutz von Wirtschaft, Bevölkerung und Gemeinwesen vor Gefahren aus dem digitalen Raum muss der Planungsprozess in seinen Abläufen, Zeiträumen sowie in seiner Intensität, Tiefe und Umsetzung grundlegend verändert und verbessert werden. Rechtliche, technologische, soziologische, kriminologische und kriminalistische Forschung zu oben genannten Phänomenen sollten erweitert und intensiviert werden. Gesetzgeberisch muss fortwährend überprüft werden, ob aufgrund der neuen Herausforderungen durch den digitalen Raum und die dortigen Sicherheits- und Kriminalitätsrisiken Überarbeitungen von Strafrecht, Strafprozessrecht, Rechtshilferecht, Verwaltungsrecht, Wirtschaftsrecht und Gesundheitsrecht notwendig sind.

Behörden, Banken und Unternehmen sind fortlaufend gegen Angriffe auf ihre IT-Strukturen und Spionage zu härten. Gleichzeitig sind kriminelle Bedrohungen inhaltlich anderer Art zum Beispiel durch Frühwarnsysteme, Filter und so weiter zu erkennen und zu bewerten, um Gegen- und Schutzmaßnahmen zu ergreifen; entsprechend muss das BSI gestärkt werden. Ein modernes und stets aktuelles Informations- und Kommunikationsmanagement, das die Zusammenarbeit zwischen Strafverfolgungsbehörden, sonstigen Verwaltungsbehörden, Privatwirtschaft und Forschungseinrichtungen ermöglicht, sollte eingeführt werden.

Impressum

GRÜNBUCH 2020
des Zukunftsforums
Öffentliche Sicherheit e. V.

1. Auflage 12/2020

ISBN 978-3-00-067510-2

Zukunftsforum Öffentliche Sicherheit e. V.

Friedrichstraße 95
10117 Berlin
Tel. +49 30 20 64 17 17
Fax +49 30 20 64 17 16

info@zukunftsforum-oeffentliche-sicherheit.de
www.zukunftsforum-oeffentliche-sicherheit.de

Druck

DCM Druck Center Meckenheim GmbH
www.druckcenter.de

Zukunftsforum
Öffentliche Sicherheit

ISBN 978-3-00-067510-2