Gerold Reichenbach, MdB
Ralf Göbel, MdB
Hartfrid Wolff, MdB
Silke Stokar von Neuforn, MdB

RISIKEN UND HERAUSFORDERUNGEN FÜR DIE ÖFFENTLICHE SICHERHEIT IN DEUTSCHLAND

SZENARIEN UND LEITFRAGEN

Grünbuch des
ZUKUNFTSFORUMS ÖFFENTLICHE SICHERHEIT

INHALT

Im Text befinden sich Hinweise auf Anhänge und weitere Szenarien.
Diese stehen auf www.zukunftsforum-oeffentliche-sicherheit.de zum Download bereit.

VORWORT

Das ZUKUNFTSFORUM ÖFFENTLICHE SICHERHEIT geht auf eine überfraktionelle Initiative des Deutschen Bundestages zurück. Auf Anregung des SPD-Bundestagsabgeordneten Gerold Reichenbach erklärten sich Innenpolitiker aus drei weiteren Fraktionen dazu bereit, eine gemeinsame Plattform für den Bereich der Öffentlichen Sicherheit zu schaffen: die Bundestagsabgeordneten Ralf Göbel (CDU/CSU), Hartfrid Wolff (FDP) und Silke Stokar von Neuforn (Bündnis 90/Die Grünen).

Außerdem tragen Vertreter aus Wirtschaft, Wissenschaft und Nichtregierungsorganisationen diese Initiative mit. Weitere Teilnehmer des ZUKUNFTSFORUMS ÖFFENTLICHE SICHERHEIT sind Repräsentanten von Organisationen der polizeilichen und nicht polizeilichen Gefahrenabwehr sowie Experten aus Bundes-, Landes- und Kommunalbehörden. Zur EU-Ebene hat die Initiative einen losen, aber kontinuierlichen Kontakt aufgebaut.

Das ZUKUNFTSFORUM ÖFFENTLICHE SICHERHEIT hat sich entschieden, ein „Grünbuch" zu verfassen. Eine solche Publikation dient in der Europäischen Union als Mittel zum Anstoß gesellschaftlicher Veränderungsprozesse.

Das Grünbuch des ZUKUNFTSFORUMS ÖFFENTLICHE SICHERHEIT fasst die bisher in den Facharbeitsgruppen und im Forum stattgefundenen Gespräche zusammen und entwickelt daraus zentrale Szenarien und Leitfragen. Auf Basis dieser Arbeit möchte es eine breite Debatte in Politik, Wirtschaft, Verbänden und Öffentlichkeit über die vielfältigen Herausforderungen anstoßen, denen sich heute der Schutz der Bevölkerung gegenübersieht. Gleichzeitig soll mit der Debatte um die Szenarien ein Einstieg in eine politische Bewertung folgen. Das Grünbuch soll hierzu Anhaltspunkte liefern, ohne einer politischen Bewertung oder Lösung vorzugreifen.

MITWIRKENDE

HERAUSGEBER:

Gerold **Reichenbach**, Mitglied im Deutschen Bundestag, Mitglied im Innenausschuss für die SPD-Fraktion, dort Berichterstatter für Bevölkerungsschutz und Themen der Inneren Sicherheit

Ralf **Göbel**, Mitglied im Deutschen Bundestag, Mitglied im Innenausschuss für die CDU/CSU-Fraktion, dort Berichterstatter für Innere Sicherheit; stv. innenpolitischer Sprecher seiner Fraktion

Hartfrid **Wolff**, Mitglied im Deutschen Bundestag, Mitglied im Innenausschuss für die FDP-Fraktion, dort Berichterstatter für Bevölkerungsschutz und Themen der Inneren Sicherheit

Silke **Stokar von Neuforn**, Mitglied im Deutschen Bundestag, Mitglied im Innenausschuss für die Fraktion Bündnis 90/Die Grünen, dort Berichterstatterin für Bevölkerungsschutz und Themen der Inneren Sicherheit; innenpolitische Sprecherin ihrer Fraktion

AUTOREN:

Michael **Bartsch***, Leiter Competence Center Innere und Äußere Sicherheit, T-Systems Enterprise Services GmbH

Marie-Luise **Beck***, Büroleiterin und wissenschaftliche Mitarbeiterin bei MdB Gerold Reichenbach

Detlev L. **Burgartz**, Leiter des Bereichs Kriminalitäts- und Geldwäschebekämpfung, Gesamtverband der Versicherungswirtschaft e.V. (GDV), Leiter der Grünbuch-Arbeitsgruppe „Terrorismus und OK"

PD Dr. Achim **Daschkeit**, Umweltbundesamt, Federal Environment Agency/Germany, Fachgebiet I 2.1 Klimaschutz, Kompetenzzentrum Klimafolgen und Anpassung (KomPass), Dessau, Leiter der Grünbuch-Arbeitsgruppe „Klima"

Prof. Dr. Wolf R. **Dombrowsky***, Leiter der Katastrophenforschungsstelle der Christian-Albrechts-Universität, Kiel

Christian **Endress**, Mitarbeiter Generalsekretariat, Deutsches Rotes Kreuz

Dr. Wolfram **Geier**, Abteilungsleiter Notfallvorsorge und Kritische Infrastrukturen, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Bonn. Leiter der Grünbuch-Arbeitsgruppe „Unternehmenssicherheit und Infrastruktur"

Priv.-Doz. Dr. med. Dr. med. habil. René **Gottschalk**, Facharzt für Innere Medizin, Infektiologie und Öffentliches Gesundheitswesen, Leiter Kompetenzzentrum für hochinfektiöse Erkrankungen; Hessen und Rheinland-Pfalz, Ltd. Medizinaldirektor der Abteilung Infektiologie und stv. Amtsleiter im Stadtgesundheitsamt Frankfurt am Main.

Assessor jur. Benedikt **Liefländer**, Bereichsleiter Malteser Hilfsdienst, Generalsekretariat

LtdMedDir Dr. Harald **Michels**, Leiter des Gesundheitsamtes der Kreisverwaltung Trier-Saarburg

Ortwin **Neuschwander***, Unternehmensberatung Ortwin Neuschwander e. K.

Dr. med. Karsten **Ocker**, Arzt für Arbeitsmedizin, Bundesarzt des Arbeiter-Samariter-Bundes, Vorsitzender der Ständigen Konferenz für Katastrophenvorsorge und Bevölkerungsschutz

Prof. Dipl.-Ing. Reinhard **Ries**, Direktor der Branddirektion in Frankfurt am Main

Hagen **Saberschinsky**, Polizeipräsident in Berlin a. D.

Detlev **Samland***, Partner Pleon GmbH

Prof. Dr.-Ing. Hermann J. **Thomann**, Branchenmanager Government, TÜV Rheinland Group Köln/Berlin, Leiter der Grünbuch-Arbeitsgruppe „Unternehmenssicherheit und Infrastruktur"

Clemens Graf von **Waldburg-Zeil***, Generalsekretär, Deutsches Rotes Kreuz, Leiter der Grünbuch-Arbeitsgruppe „Fähigkeiten, Akteure, Ressourcen, Bevölkerung (FARB)"

Prof. Dr. DVM, Dipl. ECVPH Lothar **Wieler**, Herausgeber „Berliner und Münchner Tierärztliche Wochenschrift", Direktor des Instituts für Mikrobiologie und Tierseuchen, Fachbereich Veterinärmedizin, Freie Universität Berlin. Leiter der Grünbuch-Arbeitsgruppe „Seuchengeschehen"

EXPERTEN:

Prof. Dr. med. Hans Anton **Adams**, Leiter der Stabsstelle für interdisziplinäre Notfall- und Katastrophenmedizin, Medizinische Hochschule Hannover

Oberstleutnant i.G. Dipl.-Ing. Frank **Baumgard**, Referent Zivil-Militärische Zusammenarbeit im Bundesministerium der Verteidigung, Führungsstab der Streitkräfte (Fü S IV 3)

Dr. med. Walter **Biederbick**, Direktor und Professor, Leiter der zentralen Informationsstelle des Bundes für Biologische Sicherheit, Robert Koch-Institut

Albrecht **Broemme**, Präsident der Bundesanstalt Technisches Hilfswerk

Dipl.-Ing. Jochen U. **Budde**, Deutsche Telekom AG, Leiter Verbindungsbüro Nord

Axel **Dechamps**, Vorsitzender des Arbeitskreises V der Ständigen Konferenz der Innenminister/-senatoren der Länder, Bevölkerungsschutz, Feuerwehrangelegenheiten, Rettungsdienst, Zivile Verteidigung, und Mitglied des Arbeitskreises der Ständigen Konferenz der Innenminister/-senatoren der Länder II, Innere Sicherheit, der Ständigen Konferenz der Innenminister und -senatoren, Abteilungsleiter Öffentliche Sicherheit und Ordnung, Berlin

Dr. Uwe **Fischer**, Bundesministerium des Innern, Referat G II 1/Internationale Entwicklungen; Analyse und Bewertung

Jochen **Grimmelt**, Leiter Zivile Notfallvorsorge, Deutsche Bahn Sicherheit GmbH

Sven **Jarmuth**, Vizepräsident, Medizinisches Katastrophenhilfswerk (MHW)

Mit * gekennzeichnete Autoren bilden die Steuerungsgruppe des ZUKUNFTSFORUMS ÖFFENTLICHE SICHERHEIT.

Frank **Jörres**, Teamleiter Erste Hilfe, Rettungsdienst, Katastrophenschutz, Generalsekretariat, Deutsches Rotes Kreuz

Rudolf **Kögel**, Head of Special Business Development Programs, EADS Defence Electronics

Dipl.-Ing. Manfred **Kuntz**, Key Account Manager, Feuerwehr, Meinungsbildner und Interessenvertreter, Dräger Safety AG & Co. KGaA

Dipl.-Ing. Jörg **Marks**, Leiter Bereich Region Ost , Siemens Building Technologies GmbH & Co.oHG, Berlin

Prof. Dr. Sachar **Paulus**, Honorarprofessor für Security Management, Fachlicher Leiter des Kompetenzzentrums für Sicherheit (KomSiB), FH Brandenburg

Dirk **Reinermann**, Referat Kritische Infrastrukturen und IT-Sicherheitsrevision, Bundesamt für Sicherheit in der Informationstechnik

Dipl.-Pol. Frank **Sauer**, Wissenschaftlicher Mitarbeiter am Institut für Politikwissenschaft der Universität der Bundeswehr München; Doktorand an der Goethe-Universität Frankfurt am Main

Prof. Dr. Harald **Schaub**, Abteilungsleiter und Professor für Psychologie, IABG Ottobrunn und Otto-Friedrich-Universität Bamberg

Prof. Dr.-Ing. Jochen **Schiller**, Vizepräsident, Freie Universität Berlin

Dr. Volker **Zurwehn**, Stv. Institutsleiter, Fraunhofer-Institut für Software- und Systemtechnik

Heiner **Wegesin**, Abteilungsleiter Internationaler Terrorismus und Organisierte Kriminalität, Bundesnachrichtendienst

Prof. Dr. Friedemann **Wenzel**, Center for Disaster Management and Risk Reduction Technology (CEDIM), Geophysikalisches Institut, Universität Karlsruhe

Dirk **Würger**, Leiter der Arbeitsgruppe Krisenmanagement, Zivil- und Katastrophenschutz, Senatsverwaltung für Inneres und Sport, Berlin

Ein besonderer Dank für das Mitwirken an und die wertvollen Beiträge in den Konferenzen „Zukunftsforum Öffentliche Sicherheit“ geht an:

Peter **Altmaier**, Parlamentarischer Staatssekretär beim Bundesminister des Innern und Mitglied des Deutschen Bundestages

Roland **Bombardella**, Haut-Commissaire, Haut-Commissariat à la Protection Nationale, Luxembourg

Pia **Bucella**, Direktorin, Europäische Kommission, Generaldirektion Umwelt, Direktion A – Kommunikation, Rechtsangelegenheiten und Bevölkerungsschutz

Christopher **Bunting**, Secretary General, International Risk Governance Council, Geneva, Switzerland

Fred **Chiachiarella**, Leiter Betriebswirtschaft und Informationstechnologie, Gesamtverband der Deutschen Versicherungswirtschaft e.V.

Dr. Markus **Dürig**, Leiter des Referates IT 3 – Sicherheit in der Informationstechnik, Bundesministerium des Innern

Christoph **Flury**, lic. phil., Chef Konzeption und Koordination, Mitglied der Geschäftsleitung, Bundesamt für Bevölkerungsschutz (BABS), Schweiz

Michael von **Foerster**, Head of Association Governmental and Public Affairs, Bosch Sicherheitssysteme, stv. Vorsitzender des Fachverbandes Sicherheitssysteme, ZVEI

Dr. Markus **Hellenthal**, Senior Vice President, Vorsitzender der Geschäftsführung Thales Deutschland

Prof. Dr. Peter **Höppe**, Leiter des Bereichs GeoRisikoForschung/Corporate Climate Centre Münchener Rückversicherungs-Gesellschaft AG

Waldemar **Kindler**, Landespolizeipräsident, Leiter der Abteilung IC „Öffentliche Sicherheit und Ordnung“, Bayerisches Staatsministerium des Innern, Vorsitzender des Arbeitskreises II, Innere Sicherheit, der Ständigen Konferenz der Innenminister und -senatoren

Prof. Dr. Hans-Jürgen **Lange**, Universität Witten/Herdecke, Fakultät für das Studium Fundamentale, Professur für Politikwissenschaft, Sicherheitsforschung und Sicherheitsmanagement

Brandamtmann Dieter **Oberndörfer**, Sachgebietsleiter Frankfurter Institut für Rettungsmedizin und Notfallversorgung der Branddirektion der Stadt Frankfurt am Main

Karl-Andreas **Moll**, Corporate Business Development, 3M Deutschland GmbH

K. John **Pournoor**, MBA, Ph.D., International Government Executive, National Infrastructure, Public Health, Safety, Security and Defense, 3M Company – Government Markets & Public Affairs

Oliver-Patrick **Rodewald**, Fachbereichsleiter für Auslandshilfe und Katastrophenschutz, Johanniter-Unfall-Hilfe e.V.

Bernhard **Schneck**, Geschäftsführer, GeNUA Gesellschaft für Netzwerk- und Unix-Administration mbH

Joachim **Steig**, Country Vice President Geschäftsentwicklung Thales Deutschland, Ministerialdirektor a.D.

Christoph **Unger**, Präsident, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

1. EINLEITUNG

Das Sicherheitsumfeld des einzelnen Menschen und der Gesellschaft hat sich in den vergangenen Jahrzehnten erheblich verändert. Die daraus resultierenden neuen Risiken und Bedrohungen werden höchst unterschiedlich wahrgenommen: Einerseits herrscht eine misstrauische, ängstliche oder gar alarmistische Grundstimmung bei Bevölkerung und Medien, wenn es um die Themen Terrorismus und Gewaltdelikte geht. Andererseits werden Risiken durch Infrastrukturausfälle oder Organisierte Kriminalität kaum thematisiert, sondern eher ignoriert oder unterschätzt.

Permanente technische Innovationen, ein hohes Schutzniveau im Bereich der alltäglichen Gefahrenabwehr, die selbstverständliche jederzeitige Verfügbarkeit von Kommunikationsmitteln und hohe Rechtsstandards suggerieren Sicherheit. Tatsächlich wächst aber die Verwundbarkeit gerade durch weniger offensichtliche, schleichende Risiken und die Verkettung krisenhafter Ereignisse. Dazu gehören die zunehmende und umfassende Abhängigkeit von Infrastrukturleistungen wie der Stromversorgung, die Ausbreitung transnationaler Schattenökonomien oder auch Pandemien, die durch den Klimawandel und die hohe Mobilität von Menschen und Gütern begünstigt werden.

1.1 NEUE HERAUSFORDERUNGEN

Konsens herrscht bislang nur darüber, dass sich Risiken und Bedrohungslagen fundamental geändert haben.

Politik, Wirtschaft und Gesellschaft müssen sich neuen Herausforderungen stellen: Sie müssen die veränderten Risiken betrachten und Strategien zur Krisenbewältigung finden. Dabei geht es nicht darum, die gesetzlichen Regelungen des Bevölkerungsschutzes und die darauf basierenden Maßnahmen der unterschiedlichen Aufgabenträger einfach nur fortzuschreiben. Vielmehr stehen grundsätzliche Entscheidungen für eine Neukonzeption des Risikomanagements und der Krisenbewältigung an. Eine großflächige, vielleicht sogar bundesweite Schadenslage über Tage oder gar Wochen kann sich Deutschland nicht leisten. Vor allem, wenn diese chaotisch gemanagt und nur lückenhaft bewältigt wird. Ein solches Ereignis könnte nicht nur zu humanen Tragödien und hohen wirtschaftlichen Schäden führen, sondern auch einen lang anhaltenden Vertrauensverlust der Bevölkerung in den Staat respektive die Organisationsstärke unseres Gemeinwesens bewirken. Dies hätte unabsehbare Folgen für unser Gesellschaftssystem.

Konsens herrscht bislang nur darüber, dass sich Risiken und Bedrohungslagen fundamental geändert haben. Ungeklärt sind jedoch viele Kernfragen, die wir angesichts der neuen Qualität der Risiken beantworten müssen.

1.2 ZIELE DES GRÜNBUCHS

Mit dem vorliegenden Grünbuch möchte das ZUKUNFTSFORUM ÖFFENTLICHE SICHERHEIT eine öffentliche und parteiübergreifende Diskussion anregen. Das Grünbuch stellt, abseits tagespolitischer Diskussionen, die veränderten Rahmenbedingungen für Öffentliche Sicherheit vor. Daraus leiten sich zentrale Szenarien ab. Diese sind in ihrer Art oder durch ihre Verknüpfung völlig neue Herausforderungen. Erarbeitet wurden sie von führenden Experten aus Politik, Gefahrenabwehr, Verwaltung, Forschung, Industrie, Fachverbänden und Hilfsorganisationen. Das Grünbuch und damit auch das ZUKUNFTSFORUM ÖFFENTLICHE SICHERHEIT zeichnen sich durch eine Verbindung von unterschiedlichen Erfahrungen und Positionen aus, die ansonsten selten interagieren.

Das Grünbuch soll vor allem das öffentliche Problembewusstsein für die Risiken und die zukünftigen Aufgaben schärfen. Erst wenn eine bessere Einschätzung der Risiken für Deutschland möglich ist, können Entscheidungsträger angemessen reagieren und den Schutz der Bevölkerung sicherstellen. Die Darstellung neuer oder bisher kaum beachteter Zusammenhänge soll eine öffentliche Debatte anstoßen, die stärker erkenntnisorientiert und weniger interessengeleitet ist. Das Grünbuch gibt wichtige Impulse für die künftige Ausrichtung politischer Entscheidungen – ohne jedoch politische Lösungen aufzuzeigen.

Das Grünbuch ist eine Einladung an alle, die sich diesen Fragen stellen, an der Debatte mitzuwirken.

1.3 DIE RAHMENBEDINGUNGEN HABEN SICH VERÄNDERT

Das Ende des Ost-West-Konfliktes und die Auflösung der bipolaren Weltordnung vor etwa 20 Jahren führten zu völlig veränderten sicherheitspolitischen Rahmenbedingungen. Die damals aufkeimende Hoffnung auf eine „Friedensdividende" hatte sich schon bald als unrealistisch erwiesen. Auch wenn die Bedrohung durch umfassende territoriale Kriegshandlungen für die Bundesrepublik Deutschland seither unwahrscheinlich geworden ist.

An ihre Stelle sind neue Risiken und Bedrohungen getreten:

- **Internationaler Terrorismus:** Asymmetrische Kriegsführung und neue Verwundbarkeiten moderner Industriegesellschaften haben die ehemals statische Sicherheitsumgebung verändert. Nicht mehr zwischenstaatliche Konflikte, sondern transnationale Bedrohungsfaktoren stehen im Vordergrund. Sie weichen die Trennung von innerer und äußerer Sicherheit auf. Die traditionelle Handlungsfähigkeit der Nationalstaaten ist dadurch zunehmend beeinträchtigt. Dennoch: Die Frage, ob Terrorismus völkerrechtlich als Krieg zu werten ist, bleibt hoch umstritten. Die Erfahrungen im Ausland zeigen, dass eine rein militärische Bekämpfung des Terrorismus keine Chancen hat. Die vielschichtigen Ursachen und Erscheinungsformen des Terrorismus lassen die isolierte klassisch polizeiliche Prävention und Repression unwirksam werden. Der Generaltrend geht in Richtung einer Zunahme äußerer Determinanten. Daher müssen die Bedrohungspotenziale und die (Sicherheits-)Interessen neu bestimmt werden.
- **Transnationale Organisierte Kriminalität** (OK): Drogen-, Menschen- und illegaler Waffenhandel, Schutzgelderpressung, Entführung, organisierter Diebstahl hochwertiger Güter, Eigentums- und Wirtschaftskriminalität, Betrug im Internet usw. sind klassische Betätigungsfelder der OK. Sie agiert weltweit und besitzt einen hohen Professionalisierungsgrad. Die OK steht in symbiotischer Beziehung zum internationalen Terrorismus und ist seine Hauptfinanzierungsquelle. Gleichzeitig bestehen fließende Übergänge zu Wirtschaftsdelikten, wie Geldwäsche, Steuer- und Zolldelikte.
- **Klimaänderungen** und deren Folgen: Für bestimmte Regionen in Deutschland erwarten die Experten eine Zunahme extremer Wetterereignisse, wie Starkregen oder länger andauernde Hitzeperioden. Sie können große Schäden an Sachwerten auslösen und die Gesundheit beeinträchtigen. Schon heute ist ein schleichender Klimawandel zu beobachten. Dieser wird sich aller Voraussicht nach bis Ende des Jahrhunderts intensivieren.
- **Informationsgesellschaft:** Die technische Abhängigkeit von sogenannten „Kritischen Infrastrukturen" ist in alle Lebensbereiche vorgedrungen. Die fortschreitende Ausbreitung von Informations- und Kommunikationstechnologie führt zu neuen Verwundbarkeiten. Besonders betroffen sind elektronische Infrastrukturen – ohne sie funktioniert heute fast nichts mehr. Wegen der hohen Vernetzung können schon kleine Defekte, technisches oder menschliches Versagen oder auch Sabotagehandlungen eines Einzelnen Domino- und Kaskaden-Effekte auslösen. Diese führen schlimmstenfalls zum Zusammenbruch ganzer Systeme.
- **Infektionskrankheiten:** Aufgrund der hohen Mobilität von Gütern und Personen weltweit können sich Infektionskrankheiten innerhalb kürzester Zeit zu einer Epidemie oder Pandemie ausweiten. Krankheitserreger und ihre Überträger können aufgrund des Klimawandels neue Regionen dauerhaft besiedeln. Es ist äußerst fraglich, wie lebenswichtige Infrastrukturleistungen bei hohen Erkrankungsraten aufrechterhalten werden können.
- **Privatisierung der Daseinsvorsorge:** Infrastrukturen und Dienstleistungen sind immer seltener unter direkter staatlicher Hoheit oder in staatlichem Mehrheitsbesitz. Große Bereiche wurden privatisiert oder privatrechtlich

Die technische Abhängigkeit von sogenannten „Kritischen Infrastrukturen" ist in alle Lebensbereiche vorgedrungen.

organisiert. Wirtschaftsunternehmen unterliegen dem Wettbewerb und der Kontrolle durch private Eigentümer. Betriebswirtschaftliche Notwendigkeiten korrespondieren nicht automatisch mit übergreifenden Sicherheitserfordernissen, sodass dies neue Herausforderungen u. a. an rechtliche und kommunikative, angemessene Rahmenbedingungen stellt.

1.4 GLOBALISIERUNG BIRGT NEUE RISIKEN

Die veränderten Rahmenbedingungen sind eng mit der Globalisierung verbunden. Diese Entwicklung hatte schon vor der oben beschriebenen politischen Wende begonnen und sie dauert an: Globalisierung gilt als wichtigster Megatrend bis 2020, denn die Interdependenz von Gesellschaften wird weiter wachsen. Auch sind die Auswirkungen der Globalisierung bislang nicht hinreichend erfasst. Insofern müssen die oben beschriebenen neuen Risiken und Bedrohungen vor dem Hintergrund von Entwicklungen gesehen werden, die heute für die Bundesrepublik Deutschland kaum zu gelten scheinen und daher wenig bewusst wahrgenommen werden.

Die veränderten Rahmenbedingungen sind eng mit der Globalisierung verbunden.

Infolge der Globalisierung werden sich u. a. folgende Trends weiterhin verstärken:

- die Erosion des politischen Verpflichtungs- und Ordnungsmodells der (National-)Staatlichkeit und die Reorganisation in neue Strukturen,
- die globalen Kapital- und Güterbewegungen,
- der Austausch von Information und Wissen,
- die Urbanisierung,
- die Migrationsbewegungen (aufgrund von Klimawandel, Ressourcenknappheit und der Globalisierung des Arbeitsmarktes).

1.5 AKTEURE DER ÖFFENTLICHEN SICHERHEIT

Klassischerweise handelt es sich dabei um die Behörden und Organisationen mit Sicherheitsaufgaben (BOS) im Bereich der polizeilichen und der nicht polizeilichen Gefahrenabwehr. Zur polizeilichen Abwehr zählen:

- die Polizeien von Bund und Ländern,
- die Verfassungsschutzämter der Länder und des Bundes,
- der Bundesnachrichtendienst (BND),
- der Militärische Abschirmdienst (MAD).

Im nicht polizeilichen Bereich sind das:

- die Feuerwehren,
- das Technische Hilfswerk (THW),
- die anerkannten privaten Hilfsorganisationen Arbeiter-Samariter-Bund Deutschland e.V. (ASB), Deutsche Lebens-Rettungs-Gesellschaft e.V. (DLRG), Deutsches Rotes Kreuz (DRK), die Johanniter-Unfall-Hilfe e.V. (JUH) und der Malteser Hilfsdienst e.V. (MHD),
- das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK),
- die Ordnungs- und Katastrophenschutzbehörden der öffentlichen Verwaltungen in Kommunen und Ländern,
- die im Rahmen von Artikel 35 Grundgesetz subsidiär einsetzbare Bundeswehr.

Geht man von den oben genannten neuen Risiken und Bedrohungen aus, erweitert sich der Kreis der Akteure. Ohne Anspruch auf Vollständigkeit sei auf die Teilnehmer der vom Bundesamt für Bevölkerungsschutz und Katastrophenhilfe im Jahr 2007 durchgeführten LÜKEX-Übung „Pandemie" hingewiesen. Das waren unter anderem:

- das Robert Koch-Institut,
- das Friedrich-Loeffler-Institut,
- das Bundesamt für Arzneimittel und Medizinprodukte,
- das Paul-Ehrlich-Institut,
- die Bundesanstalt für Landwirtschaft und Ernährung,
- die Ärztekammern,
- Wohlfahrtsverbände,
- Krankenhäuser,
- Alten- und Pflegeheime,
- das Bundesamt für Sicherheit in der Informationstechnik,
- das Eisenbahn-Bundesamt,
- das Bundesverwaltungsamt
- die Deutsche Bahn AG,
- das Bundesarbeitsgericht,
- das Luftfahrt-Bundesamt,
- die Wasser- und Schifffahrtsverwaltung des Bundes,
- der Deutsche Wetterdienst,
- die Bundesbank,
- die Flughafenbetreiber,
- die Medien.

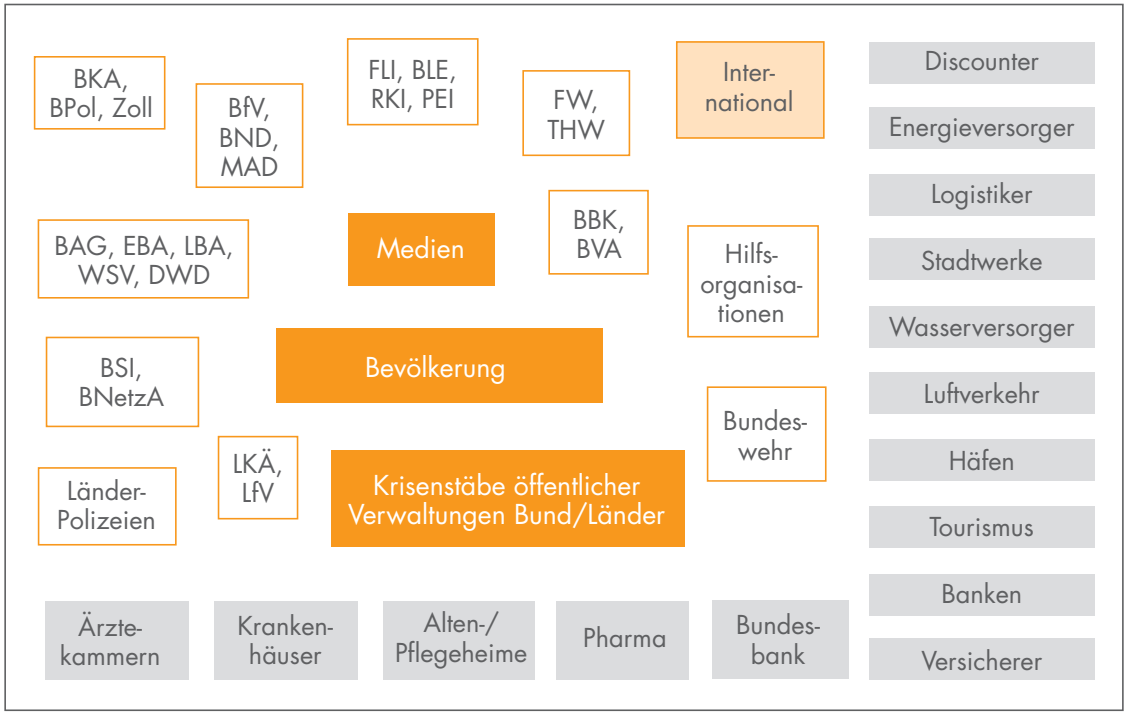
Schließlich ist als zunehmend wichtiger Akteur die private Wirtschaft zu nennen. Sie ist einerseits ein bedeutender Aufgabenträger der Öffentlichen Si-

cherheit. Andererseits ist sie als Betroffene mit den neuen Risiken konfrontiert. Dies gilt insbesondere für Wirtschafts- und Dienstleistungsunternehmen in den Branchen Transport, Logistik und Kommunikation sowie für die Finanz- und Versicherungswirtschaft, Nahrungsmittel- und Energieversorger, die Entsorgungsbranche, aber auch weite Teile der Gesundheitsversorgung und die Sicherheitsdienste.

Zahlreiche ehemals in staatlichem oder öffentlichem Besitz befindliche infrastrukturelle Dienstleistungen sind heute privatisiert oder stehen kurz vor einer Privatisierung. Schätzungsweise drei Viertel der für das gesellschaftliche Leben und die öffentliche Sicherheit und Ordnung wichtigen Infrastrukturbetriebe befinden sich in Privateigentum. Auf diese hat der Staat nur beschränkten Einfluss. Eigentümer und Betreiber von Krankenhäusern sind inzwischen sowohl Kommunen, Städte, Kreise und freie Träger als auch privatwirtschaftliche Unternehmen. Die Folge davon sind unterschiedliche rechtliche Verpflichtungen und Weisungsrechte. Zuletzt muss die Bevölkerung selbst als entscheidender Akteur genannt werden. Sie ist letztlich auch Rechtfertigung, Grund und Financier des Risikomanagements und der Krisenbewältigung des Staates. Und sie kann einen entscheidenden Beitrag zur Krisenprävention und -bewältigung leisten.

Die große Zahl der Akteure hat Vor- und Nachteile. Zum einen entstehen dadurch Ideenvielfalt und Kreativität. Die auf dem Subsidiaritätsprinzip aufbauenden Verantwortlichkeiten sorgen für passgenaue Antworten auf die Bedürfnisse vor Ort. Zentralistische Strukturen könnten das so nicht leisten. Zum anderen müssen bei der Vielzahl der Akteure die Informations-, Kommunikations- und Koordinationsstrukturen gut organisiert sein. Der Ausbau von Risiko- und Krisenkommunikation zwischen allen Beteiligten – dazu gehört nicht zuletzt die Bevölkerung – ist daher für eine erfolgreiche Krisenbewältigung besonders wichtig.

INVOLVIERTE AKTEURE IM FALLE EINER KATASTROPHENLAGE (AUSWAHL)



Quelle: Bericht des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe über die beübten Strukturen der LÜKEX 2007, Influenza-Pandemie (zum Teil erweitert).

2. GRUNDLAGEN DER SZENARIENBILDUNG

Das ZUKUNFTSFORUM ÖFFENTLICHE SICHERHEIT vereint Erfahrungen und Erkenntnisse aus Wissenschaft, Wirtschaft, Politik und Verwaltung. Gemeinsam diskutieren deren Vertreter die veränderten Bedingungen für Öffentliche Sicherheit. Sie definieren die daraus ableitbaren Erfordernisse und können zukünftige Anpassungen antizipieren.

2.1 ANNAHMEN UND METHODE

Die Komplexität der Problemstellung erfordert geeignete Methoden und Verfahren der Erkenntnisgewinnung und Darstellung. Die Mitwirkenden des ZUKUNFTSFORUMS ÖFFENTLICHE SICHERHEIT sind sich einig, dass die physische und politische Existenz der Bundesrepublik Deutschland nur in extremen Ausnahmefällen von einem singulären Ereignis bedroht oder gar zerstört werden kann. Das wäre zum Beispiel ein Meteoriten- oder Kometeneinschlag. Viel wahrscheinlicher ist, dass sich existenzgefährdende, nationale Notlagen erst aus dem Zusammenwirken mehrerer Negativereignisse ergeben. Durch Dominoeffekte werden natürliche, technische, soziale und ökonomische Faktoren interagieren und – je nach Mischungsverhältnis und Dynamik – zu sehr unterschiedlichen Schadensverläufen führen.

Gemeinsam Szenarien entwickeln

Aus der unendlichen Vielfalt möglicher Bedrohungslagen haben die Autoren des Grünbuchs plausible Gefährdungsabläufe ausgewählt und zwei Schlüsselszenarien abgeleitet: (1) Stromausfall und (2) Seuchengeschehen in Deutschland. Dies erfolgte in mehrfachen Rückkoppelungsschleifen und durch Hinzuziehen zusätzlicher Fachkompetenz (Delphi-Methode). Zusätzlich wählten die Autoren eine vertiefende Darstellung zum Thema Sicherheitsbedrohung durch Terrorismus und Organisierte Kriminalität. Drei mögliche Szenarien werden in diesem Zusammenhang kurz skizziert. Sie sind in dem digital bereitgestellten Anhang unter www.zukunftsforum-oeffentliche-sicherheit.de detailliert ausgeführt.

Die ausgewählten Schlüsselszenarien greifen mögliche Bedrohungsabläufe beispielhaft heraus und entwickeln daraus die Aufgabe „Öffentliche Sicherheit der Zukunft". Zusätzliche Begriffsklärungen und vertiefende Hintergrund-Darstellungen sollen den Auswahl- und Klärungsprozess der Forumsmitglieder nachvollziehbar machen. Ausführlichere Texte hierzu sind ebenfalls im digitalen Anhang zu finden.

Grundsätzlich ist zu beachten, dass die Szenarien zunächst einmal plausible, konsistente und mögliche „Geschichten" sind, die aber nicht notwendigerweise eintreten. Diese erdachten Abläufe ermöglichen es, sich Ereignisse in der Zukunft überhaupt vorstellen zu können. Szenarien sind somit eine Methode vorausschauender Konkretisierung und keine Abbildungen des tatsächlich zu Erwartenden.

2.2 DEFINITIONEN UND ZIELE

Öffentliche Sicherheit umfasst im weitesten Sinne den Schutz einer Gesellschaft vor nachteiligen Einwirkungen. Die Definitionen leiten sich aus dem Polizei- und Ordnungsrecht sowie aus dem Bestreben ab, der allgemeinen Wohlfahrt einen Rechtsrahmen und Handlungssicherheit zu geben.

Mit der Gründung von Nationalstaaten haben sich äußere und innere Sicherheit sowie spezifische Bereiche, zum Beispiel soziale Sicherheit, herausgebildet. Obgleich Innere und Öffentliche Sicherheit häufig synonym verwendet werden, unterscheiden sie sich in Bedeutung und Tragweite. Öffentliche Sicherheit kann als ein Oberbegriff von Innerer Sicherheit angesehen werden. Innere Sicherheit verweist vor allem auf eine um ein Gemeinwesen verlaufende Begrenzung, innerhalb derer Schutzaufgaben des Staates exekutiert werden sollen. Öffentliche Sicherheit hingegen stellt das Aufrechterhalten von Strukturen und Funktionen einer Gesellschaft in den Mittelpunkt. Dieses Verständnis drückt sich auch in dem Begriffspaar Öffentliche Sicherheit und Ordnung aus, das im allgemeinen Sprachgebrauch üblich ist.

Die Initiatoren des ZUKUNFTSFORUMS ÖFFENTLICHE SICHERHEIT und die Verfasser des Grünbuchs haben sich deshalb auf ein Verständnis von Öffentlicher Sicherheit geeinigt: allen Menschen,

die in der den Menschenrechten verpflichteten Gesellschaftsordnung der Bundesrepublik Deutschland leben, Sicherheit und Schutz zu gewähren.

Das Ziel aller Sicherheitsbemühungen ist es, Schäden und Beeinträchtigungen von Leib und Leben, der Freiheit und des durch die Rechtsordnung garantierten Vermögens für jeden Einzelnen abzuwenden. Auch sollen die Rechtsordnung selbst und die dafür vorgesehenen Organe und Einrichtungen geschützt werden. Kurzum: Der Fortbestand des Staates muss gewährleistet sein.

Entsprechend lassen sich folgende Schutzziele ableiten:

- Schutz von Menschenleben,
- Schutz der körperlichen und seelischen Unversehrtheit (auch im Sinne von Volksgesundheit),
- Schutz der natürlichen Lebensgrundlagen,
- Schutz demokratischer Strukturen und bürgerlicher Freiheiten,
- Schutz wesentlicher Institutionen der Öffentlichen Sicherheit und Ordnung,
- Schutz von Vermögenswerten, Sach- und Kulturgütern,
- Schutz lebenswichtiger volkswirtschaftlicher Einrichtungen und Strukturen,
- Schutz lebensnotwendiger Versorgungs- und Kommunikationsstrukturen.

Der seit den Terroranschlägen vom 11. September 2001 häufig gebrauchte angelsächsische Begriff „Homeland Security" – und mehr noch der eingedeutschte Begriff „Heimatschutz" – erscheint den Verfassern für ein europäisch angemessenes Verständnis von Zivilgesellschaft und der Verteidigung des Zivilen nicht geeignet.

Was ist eine Katastrophe?

Im allgemeinen und medialen Sprachgebrauch wird der Begriff Katastrophe meist dann gebraucht, wenn die emotionale Betroffenheit über ein bestimmtes Ereignis ausgedrückt oder auch hervorgerufen werden soll. In den Landeskatastrophenschutz-Gesetzen hat der Begriff unterschiedliche Bedeutungen: Die Spannbreite reicht von einer umfassenden Definition, zum Beispiel in Baden-Württemberg und Sachsen-Anhalt, über die Beschränkung auf Großschadenslagen wie in Nordrhein-Westfalen bis hin zum völligen Verzicht des Gebrauchs dieses Begriffes.

Das Grünbuch bezieht sich auf Katastrophe in ihrer eigentlichen Bedeutung als einen weiträumigen und über eine längere Zeit anhaltenden Zusammenbruch zentraler öffentlicher Strukturen, Systeme und Funktionen. Als Folge davon sind die oben genannten Schutzziele ganz oder teilweise gefährdet, weil etwa eine Vielzahl von Menschen betroffen ist oder es erhebliche Sachschäden gab[1]. Katastrophenabwehr bedeutet folglich: Rettung, Bergung, Schutz, Behandlung, Betreuung, Sicherung und Wiederherstellung in einem Umfeld nicht funktionierender beziehungsweise zerstörter Struktur.

Nicht gemeint sind Unglücksfälle oder Großschadenslagen, wie das Zugunglück von Eschede oder der Terroranschlag auf die Londoner U-Bahn. Solch tragischen Ereignissen steht in Deutschland ein sehr gut ausgestattetes Hilfeleistungssystem der Bundesländer und der Kommunen zur Verfügung. Dies gilt auch für die Hochwasser an Oder und Elbe, die in der Regel als Katastrophe bezeichnet werden. Jedoch war dabei die Funktionsfähigkeit des öffentlichen Lebens und der Wirtschaft nicht weiträumig beeinträchtigt. Der Nachschub in das Krisengebiet konnte aus intakter Infrastruktur heraus erfolgen, denn der größte Teil Deutschlands war nicht betroffen. Dort wurden Ressourcen in großem Umfang mobilisiert. Dies konnte sogar gravierende Fehlbevorratung und -verteilung weitgehend kompensieren.

Katastrophenabwehr bedeutet folglich: Rettung, Schutz und Wiederherstellung in einem Umfeld nicht funktionierender beziehungsweise zerstörter Struktur.

[1] Dieses Verständnis entspricht weitgehend der Definition im Katastrophenschutzgesetz des Landes Sachsen-Anhalt (KatSG-LSA) in § 1 (2): „Ein Katastrophenfall im Sinne dieses Gesetzes ist ein Notstand, bei dem Leben, Gesundheit oder die lebenswichtige Versorgung einer Vielzahl von Personen oder erhebliche Sachwerte gefährdet oder wesentlich beeinträchtigt werden und zu dessen Abwehr oder Eindämmung der koordinierte Einsatz der verfügbaren Kräfte und Mittel unter einer gemeinsamen Gesamtleitung erforderlich ist."

3. SZENARIO „STROMAUSFALL IN DEUTSCHLAND“

Eine Grundbedingung für die Funktionsfähigkeit moderner Gesellschaften ist die Verfügbarkeit von Strom. Nahezu alle technischen, administrativen und sozialen Aktivitäten hängen von einer leistungsfähigen, rund um die Uhr vorhandenen Stromversorgung ab. Dies trifft auf Deutschland als eine der führenden Industrienationen besonders zu.

3.1 OHNE STROM GEHT NICHTS

Die Stromversorgung ist eine der zentralen Infrastrukturen für den Betrieb und die Steuerung von industriellen Produktionsprozessen. Sie stellt sicher, dass Trinkwasser, Lebensmittel und Gesundheitsdienstleistungen bereitstehen. Ohne Strom funktionieren Verkehrsträger und Verkehrsleitprozesse nicht, das Notfall- und Rettungswesen steht still. Auch Finanzdienst- und Finanztransferleister, die öffentliche Verwaltung bis hin zum staatlichen Krisenmanagement können ohne Strom nicht arbeiten. Ist die Leistung dieser Kritischen Infrastruktur über einen längeren Zeitraum nicht vorhanden, betrifft das die ganze Gesellschaft. Dass ein solches Szenario realistisch ist, haben die europaweiten „Blackouts“ in den vergangenen Jahren gezeigt, zum Beispiel am 28. September 2003 vor allem in der Schweiz und Italien oder am 4. November 2006 in Deutschland, Belgien, Frankreich, Italien und Spanien. Einer der bislang folgenreichsten Stromausfälle in Deutschland ereignete sich am 25. November 2005 im Münsterland und dauerte mehrere Tage.

Aufgrund der unmittelbaren Abhängigkeit anderer Kritischer Infrastrukturen von der Stromversorgung ist „Stromausfall“ als ein Schlüsselszenario zu verstehen. Beispielsweise ergeben sich für den Bereich Telekommunikation und Informationstechnologie bei einem langfristigen und großflächigen Stromausfall schnell ähnliche Folgen wie bei einer Betroffenheit des Sektors selbst. Entsprechende Konsequenzen müssen daher in diesem Szenario mit betrachtet werden.

HINTERGRUND

Neue Verwundbarkeiten durch die moderne Informations- und Kommunikationstechnik

Informations- und Kommunikationstechnik (IKT) verändert die Gesellschaft und schafft Innovationen. Entscheidend ist dabei das Verschmelzen von Kommunikations- und Informationstechnologie. Durch diese Konvergenz entstehen völlig neue Dienstleistungen. Der breite Einsatz von IKT und die weltweite Vernetzung über das Internet gestalten Prozesse effizienter und erschließen neue Geschäftsfelder. In einigen Branchen wie dem Telekommunikations- oder dem Finanzbereich ist IKT mittlerweile fast alleiniges Betriebsmittel. IKT ist Kritische Infrastruktur.

IKT ist überall

Schon im Privathaushalt bieten sich vielfältige Einsatzmöglichkeiten: Über breitbandige Anschlüsse[2] stehen den Verbrauchern Telefonie, Internet und Fernsehen zur Verfügung. Auch in anderen Bereichen kommen ständig neue Anwendungen hinzu. Ein Beispiel ist die Elektronik im Auto. Ursprünglich unterstützte sie bestehende Funktionen, zum Beispiel die Servolenkung oder das ABS. Heute übernimmt sie Zusatzfunktionalitäten, die

[2] Das Angebot ist umfassend, mehr Information gibt beispielsweise die Internetseite www.breitbandatlas.de. Angebotene Techniken sind neben DSL und Kabel auch Funk, Satellit, Stromkabel, Glasfaser, UMTS, WLAN Hotspots oder zukünftig WiMAX.

HINTERGRUND

weit über das reine Fahren hinausgehen, zum Beispiel die Anzeige von Wartungsbedarf, eine automatische Terminkoordination mit der Werkstatt oder Diebstahlschutz durch Funkchips.

Auch jenseits der „klassischen“ Anwendungen bestehen weitere Einsatzfelder für IKT:

- Im Einzelhandel ermöglichen Logistiksysteme eine bedarfsgerechte Versorgung der Filialen. Moderne Warenwirtschaftssysteme rechnen nicht mehr nur ab, sie aktualisieren gleichzeitig Lagerbestände und initiieren Bestellvorgänge.
- In Krankenhäusern reicht der IKT-Einsatz von Administration über Logistik und Versorgung bis hin zur eigentlichen Medizintechnik und Überwachung von Intensivpatienten. Auch wird die Einführung der Telematik, beispielsweise der Gesundheitskarte, das Gesundheitswesen verändern. Dann sind die Akteure – Ärzte, Krankenhäuser, Apotheker, Heilberufler, Krankenkassen – über die Grenzen einzelner Organisationen und Träger hinaus vernetzt.
- Klassische Kritische Infrastrukturen hängen in hohem Maße von IKT ab. Dazu zählen die Energieversorgung, Wasserver- und -entsorgung. Die komplexen Prozesse im Transportwesen, wie das Management von Flughäfen, die Koordination von Lkw-Flotten oder die Steuerung des Bahnverkehrs, erfordern ebenfalls einen umfassenden IKT-Einsatz. Gleiches gilt für das Steuern von Kraftwerken und Versorgungsnetzen oder für das Lokalisieren und Beheben von Störungen.
- Der Internetzugang erschließt für die Nutzer nicht nur eine Vielfalt von Informationen, Unterhaltungs- und Einkaufsmöglichkeiten, sondern auch E-Government-Angebote von Bund, Ländern und Gemeinden.

Abhängigkeit von IKT und mögliche Folgen

Störungen der IKT wirken sich heute unmittelbar auf die von ihr unterstützten Prozesse und Dienstleistungen aus. Nicht nur die Verwaltung in Behörden und Unternehmen ist betroffen, sondern auch die Produktion. Außerdem können IKT-Störungen in einem Bereich direkt oder indirekt auf andere Bereiche wirken.

Behörden und Organisationen mit Sicherheitsaufgaben sowie Hilfsdienste setzen ebenfalls IKT ein. Verfügbarkeit und verlässliches Funktionieren der zugrunde liegenden Technologien sind entscheidend für die Handlungsfähigkeit vor allem in Krisensituationen. Beispielsweise ermöglicht die moderne Leitstellentechnik, dass wenige Zentralen die Einsätze für große Regionen steuern. Die Einsatzleitung nutzt IT-gestützte Führungsinformationssysteme. Mangelressourcen werden bundesweit über IKT koordiniert, beispielsweise die geschlossene Internetplattform deNIS II plus, das gemeinsame Melde- und Lagezentrum von Bund und Ländern (GMLZ) im Bundesamt für Bevölkerungsschutz und Katastrophenhilfe oder das regionale System DISMA. Krisenmanagement setzt heute grundsätzlich darauf, dass IKT ständig und verlässlich zur Verfügung steht.

Schwachstellen und Bedrohungen

Bereits das Jahr-2000-Problem hatte verdeutlicht, dass es selbst bei einer bekannten Problemstellung sehr schwierig ist, IKT-Schwachstellen vollständig zu lokalisieren und zu beheben. Die breite Durchdringung fast sämtlicher Bereiche mit IKT wurde hier erstmalig der Bevölkerung vor Augen geführt. Beim Jahr-2000-Problem handelte es sich nur um eine einzelne, sehr frühzeitig bekannte Schwach-

HINTERGRUND

stelle. Heute werden jährlich Tausende zusätzlicher Schwachstellen[3] in Computerprogrammen identifiziert. Einige erlauben es böswilligen Akteuren, über das Internet die betroffenen Systeme vollständig zu kontrollieren. Andere beeinflussen von sich aus das Systemverhalten negativ[4]. Solche Schwachstellen finden sich nicht nur in Standard-Computern, sondern auch in zentralen Komponenten von Rechenzentren, von Prozessleittechnik und des Internets.

Diesen Umstand nutzen Angreifer – insbesondere aus dem kriminellen Milieu – gerne aus. Heute sind nicht mehr jugendliche „Skriptkiddies“ oder „normale“ Hacker für die Mehrzahl der Angriffe verantwortlich. Die Akteure handeln vielmehr professionell. Sie können beispielsweise mittels Schadsoftware eine Vielzahl von schlecht geschützten Rechnern übernehmen, zu sogenannten Bot-Netzen zusammenschalten und auf dem Schwarzmarkt anbieten. Ein spektakuläres Beispiel war die Bot-Netz-Attacke auf Estland im April 2007. Über Wochen war die IKT-Infrastruktur von Banken, Behörden und Börse nicht nur beeinträchtigt, sondern teilweise sogar zusammengebrochen. Bis heute konnte nicht ermittelt werden, wer hinter diesem Angriff steckt. Die Vermutungen reichen von Organisierter Kriminalität über politische Aktivisten bis hin zu geheimdienstlichen Aktivitäten.
Nicht nur die heimischen, oft schlecht gesicherten Computer sind Ziele der organisierten Angriffe. Ein weitaus größerer Schaden entsteht, wenn Firmenrechner und sogenannte Applikationsserver angegriffen werden. Zum Beispiel ist der Milliarden-Skandal der französischen Bank Société Générale im Jahr 2007 auf mangelhafte Berechtigungsverwaltung zurückzuführen: Der dort angestellte Börsenhändler Jérôme Kerviel hatte offenbar Zugriff auf Transaktionsmöglichkeiten, die ihm nicht zustanden.

Auch werden durch sogenanntes „Social Engineering“, dem Erlangen von vertraulichen Daten durch soziale Manipulation, Firmeninfrastrukturen angegriffen. Die meisten Angreifer wollen damit jedoch keinen Totalzusammenbruch der Informationsinfrastruktur erreichen, vielmehr stehen unbemerkte Bereicherung und Industriespionage im Vordergrund.

Ausblick
Im IKT-Bereich lassen sich mit vergleichsweise geringem Aufwand hohe Schäden erzielen, wie der Web-Angriff auf Estland im April 2007 gezeigt hat. Es wird ein Anstieg absichtlicher Störungen erwartet, seien sie terroristisch oder kriminell motiviert. Die Organisierte Kriminalität hat erkannt, dass IT-Angriffe Profit bringen. In den kommenden Jahren ist daher verstärkt mit Aktivitäten und neuen Angriffsmethoden zu rechnen [siehe Terrorismus und OK, S. 28].

Die dominierenden Systeme in Wirtschaft und Verwaltung erfüllen die Anforderungen an Fehlertoleranz und Angriffssicherheit eher schlecht. Heute schon wäre es denkbar, Börsenrechner und damit einen ganzen Finanzplatz lahmzulegen. Oder die Prozesssteuerungstechnik von Energieversorgungsunternehmen außer Betrieb zu setzen.

Die hohe Abhängigkeit von IKT wird in den kommenden Jahren weiter steigen. Damit werden Störungen – insbesondere bei kritischen Prozessen – zunehmend intolerabel. Die eingesetzten IKT-Architekturen werden aber gleichzeitig komplexer. Damit sind sie tendenziell fehleranfälliger und störungsempfindlicher.

Die Herausforderung für die kommenden Jahrzehnte wird daher sein, Software, Hardware und IKT-Architekturen so weiterzuentwickeln, dass sie ein verlässliches Instrument zur Prozessunterstützung darstellen bzw. bleiben. Gleichzeitig muss sichergestellt werden, dass IKT auch bei Störungen handlungsfähig bleibt. Hierzu sollten IT-Infrastrukturen verstärkt redundant ausgelegt sein. Zusätzlich sollten möglicherweise alte proprietäre Technologien bei Bedarf gestuft reaktiviert werden können.

[3] Schwachstellen entstehen in der Regel bei der Programmierung von Software, beim Design oder der Herstellung von Hardware. Mit ihrem Vorhandensein sind sie aber noch nicht bekannt. Manche Schwachstellen werden erst Jahre nach ihrer „Entstehung“ identifiziert.
[4] So geriet zum Beispiel die Ariane 5 am 4. Juni 1996 aufgrund eines Softwarefehlers außer Kontrolle und musste gesprengt werden.

3.2 GRUNDANNAHMEN

Elektrische Energie kann nur in kleinen Mengen gespeichert werden. Im Wesentlichen muss sie im selben Augenblick erzeugt werden, in dem sie verbraucht wird – und umgekehrt. Wenn Kraftwerke unvorhergesehen ausfallen, das Stromnetz an einer Stelle unterbrochen wird oder die Netzsteuerung gestört ist, entstehen in Sekundenschnelle große Schwankungen der elektrischen Spannung. Sobald diese Lastschwankungen nicht sofort wieder ausgeglichen werden, kommt es zu einem Dominoeffekt. Die Folge: Das Stromnetz bricht zusammen. Je größer und weiträumiger der Schaden ist, desto schwieriger gestaltet sich das Wiederanfahren des sensiblen Gleichgewichtes von Stromerzeugung und Stromabnahme.

Ausgangspunkt für das Szenario ist ein mehrtägiger bis mehrwöchiger überregionaler Stromausfall durch eine gravierende Störung in den deutschen Regelzonen. Der Betrieb von Notstromanlagen kann, bedingt durch die Versorgungsknappheit mit Treibstoff, nur zeitweise erfolgen.

Das Szenario „Stromausfall“ würde das ganze Land betreffen. Die mittelbare und unmittelbare Eintrittswahrscheinlichkeit ist hoch. Auch besteht ein hohes Risiko für Menschen, Staat und Wirtschaft. Denn ein Stromausfall würde große Schäden verursachen, unter anderem Sachschäden durch unmittelbare Zerstörung und Folgeschäden wie Versorgungsausfälle und Lieferunterbrechungen. Nach gängigen Bewertungsmaßstäben müssen die Schäden mindestens im zweistelligen Milliarden-Euro-Bereich liegen, um als katastrophal klassifiziert zu werden. Diese Summe wird schnell erreicht, wenn zum Beispiel zahlreiche große Industriebetriebe und der Finanzsektor massiv betroffen sind. Auch der immaterielle Schaden durch einen Stromausfall ist hoch. Er wird unter anderem durch einen Vertrauensverlust der Bevölkerung in Staat und Wirtschaft ausgelöst.

Je länger ein Stromausfall dauert, desto mehr andere stromabhängige Infrastrukturen brechen zusammen. Es wird zunehmend schwierig bis unmöglich, sensible technische Anlagen wieder hochzufahren. Beispielsweise Hochöfen: Bei einem plötzlichen Stromausfall, der nicht dauerhaft durch eine Notstromversorgung abgefangen werden kann, kann der Hochofen überhitzen. Es kann zur Durchschmelze und zu Bränden kommen. Selbst wenn der Stromausfall ohne Schäden bewältigt werden kann, dauert das Wiederanfahren Stunden bis Tage. Der Produktionsausfall reicht in jedem Fall über das Ereignis hinaus.

Bisher kann man aus realen Ereignissen nur Vermutungen darüber ableiten, welche Schäden nach einem mehrtägigen bis mehrwöchigen überregionalen Stromausfall auftreten können.

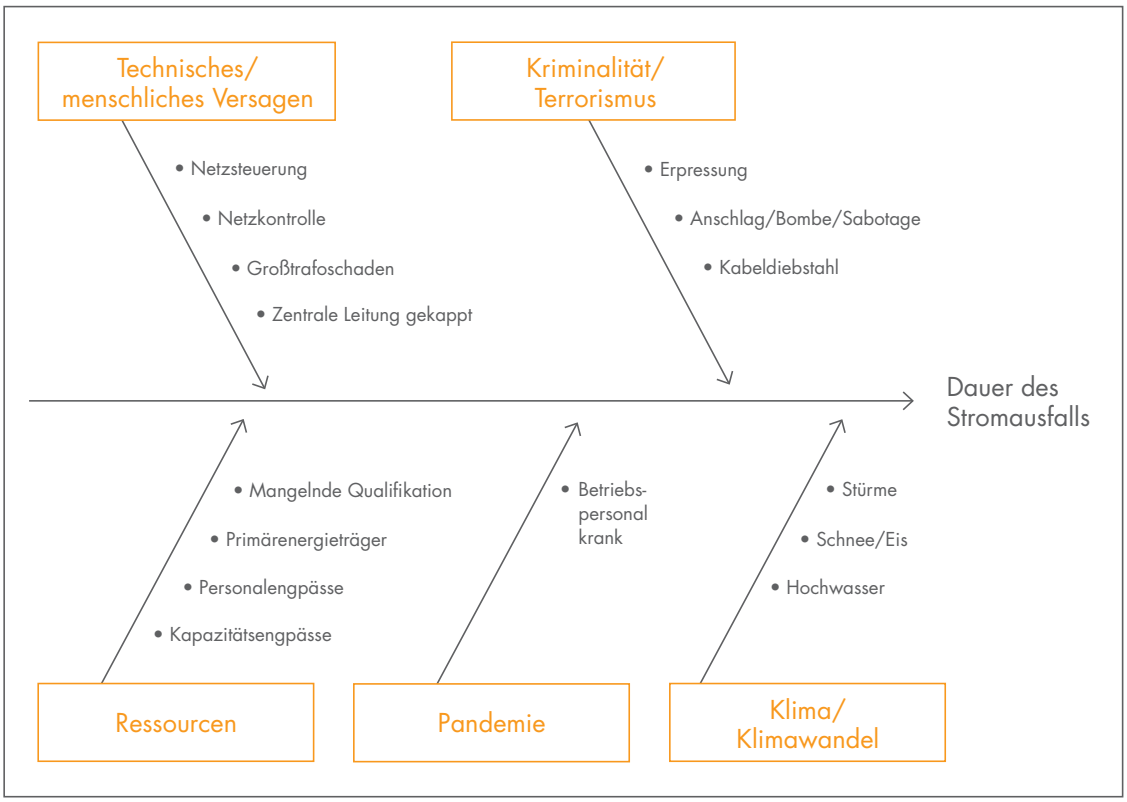
- Der eintägige Stromausfall am 14. August 2003 im gesamten Nordwesten der USA verursachte volkswirtschaftliche Kosten zwischen sieben und zehn Milliarden US-Dollar.[5]
- Der mehrtägige Stromausfall im dünn besiedelten Münsterland im Jahr 2005 löste Schäden von schätzungsweise 130 Millionen Euro aus.
- 1999 starben bei einem Erdbeben in Taiwan etwa 2.000 Menschen. Eine weitere Folge war ein teilweise bis zu drei Wochen andauernder Stromausfall. Unter anderem wurde der Industriepark von Hsinchu, das Herz der taiwanesischen IT-Produktion, völlig von der Stromversorgung abgeschnitten. Obwohl das Erdbeben keine Gebäude zerstörte, erlitt das Werk durch den Stromausfall einen Schaden von 162 Millionen Euro. Der Primärschaden durch die zerstörte Stromverteileranlage lag bei zwei Millionen Euro. Die Sekundärschäden beispielsweise durch Produktionsausfälle, Arbeitslosigkeit und Teilzusammenbrüche von Transportsystemen waren etwa 500 Mal höher als der Primärschaden.
- Eine österreichische Studie aus dem Jahr 2005 errechnete für einen einstündigen landesweiten Stromausfall pro nicht gelieferte Kilowattstunde volkswirtschaftliche Kosten, die um das Sechs- bis Zehnfache über dem Verrechnungspreis einer Kilowattstunde Strom liegen.[6]

Das Szenario „Stromausfall“ würde das ganze Land betreffen. Die mittelbare und unmittelbare Eintrittswahrscheinlichkeit ist hoch.

[5] Bansari Saha, Bill Moddy, The Economic Cost of the Blackout, An Issue Paper on the Northeastern Blackout, August 14, 2003, ICF-Consulting, Fairfax, USA.
[6] Markus Bliem, Ein makroökonomischer Bewertungsansatz zu den Kosten eines Stromausfalls im österreichischen Versorgungsnetz, IHSK DISCUSSION PAPER, 02/2005.

3.3 ALLES KANN AUSLÖSER SEIN

Die Ursachen für einen lang andauernden und überregionalen Stromausfall können vielfältig sein:



Technisches oder menschliches Versagen kann zu grenzüberschreitenden Stromausfällen führen.

Technisches oder menschliches Versagen kann zu gestörten Netzsteuerungs- und Kontrollprozessen und schließlich grenzüberschreitenden Stromausfällen führen. Auch könnten Probleme in der Leittechnik diese Prozesse so stören, dass es zu Ausfällen kommt.

Ein Beispiel: Am 4. November 2006 wurden im Emsland die Stromleitungen absichtlich abgeschaltet, um ein neu gefertigtes Kreuzfahrtschiff aus einer Werft in Papenburg gefahrlos über die Ems in die Nordsee zu überführen. Die Folge: Aufgrund unvorhergesehener Kettenreaktionen hatten etwa zehn Millionen Menschen in verschiedenen Regionen Europas 90 Minuten lang keinen Strom. Kurzzeitig drohte das Ereignis unkontrolliert zu einem europaweiten, lang anhaltenden Blackout zu eskalieren.

Wichtige technische Infrastrukturen im Verteilernetz können durch kriminelle und/oder terroristische Aktionen so gravierend zerstört oder nachhaltig gestört werden, dass die Stromversorgung in den betroffenen Gebieten bis zu mehreren Monaten ausfällt.

Die Organisierte Kriminalität kann die unterschiedlichsten kriminellen Handlungen professionell durchführen, auch ein Angriff auf die Stromversorgung ist denkbar [siehe Hintergrund: Informations- und Kommunikationstechnologie, S. 16 und Terrorismus und OK, S. 28].

Zerstörungen der Technik und Ressourcenmangel können dazu führen, dass Kraftwerksleistungen reduziert werden müssen oder sogar ganz ausfallen. Ein Auslöser kann Hitze sein. Klimaforscher

rechnen in Teilen Deutschlands mit einer signifikanten Zunahme von Hitzeperioden. Sie können zu einer Beeinträchtigung der Kühlwasserversorgung führen, entweder durch erhöhte Temperaturen des Kühlwassers oder Wasserniedrigstände. Beispielsweise standen im Hitzesommer 2003 in Frankreich mehrere Kraftwerke kurz vor der Abschaltung.

Schwere Naturereignisse wie Starkniederschläge, Stürme oder Blitzeis können ebenfalls einen flächendeckenden Stromausfall auslösen. Wie zum Beispiel am 25. November 2005 im Münsterland. Temperaturen um die null Grad Celsius, starke Niederschläge und stürmischer Wind führten dazu, dass sich dicke Eispanzer an den Freileitungsmasten und den Leiterseilen bildeten. Durch Wind und Eis trat das gefürchtete „Leiterseilschwingen" ein. Es kam zu kurzzeitigen automatischen Streckenabschaltungen und länger andauernden Leitungsausfällen. Die Folge: 250.000 Menschen waren mehrere Tage ohne Strom [siehe Hintergrund: Klima, S. 37].

Auch ein extrem hoher Krankenstand aufgrund einer schweren Influenza-Pandemie kann zu einem Stromausfall führen. Bei einer Erkrankungsrate von 30 bis 50 Prozent wird es zu einem massenhaften Ausfall von Arbeitskräften kommen. Diese Situation verstärkt sich, weil einige Menschen aufgrund der Pflegebedürftigkeit von Familienangehörigen zu Hause bleiben werden [siehe Hintergrund: Influenza-Pandemie, S. 33].

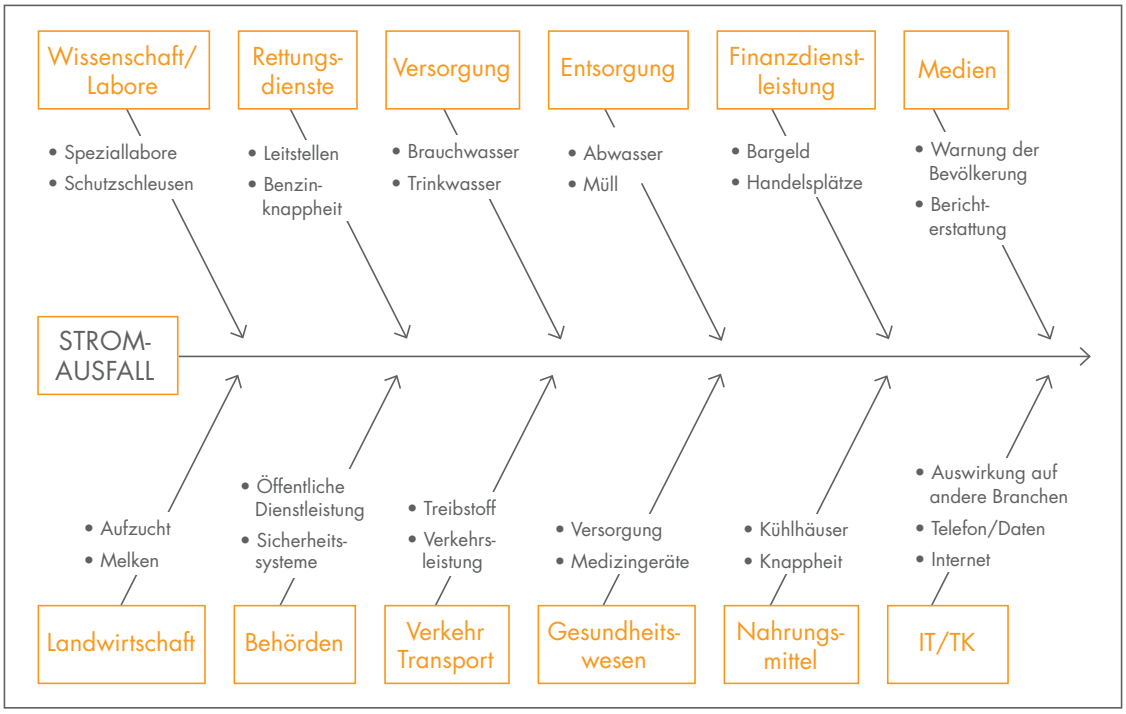
Eine besondere Brisanz bergen Verkettungen von Ursachen. So ist beispielsweise nicht ausgeschlossen, dass es während einer Influenza-Pandemie auch zu einem sehr schweren Wintersturm kommen kann. Denn beide treten häufig in der zweiten Winterhälfte auf. Größte Personalengpässe träfen dann mit einer Extremsituation zusammen, deren Bewältigung einen intensiven flächendeckenden Personaleinsatz erfordern würde. Unter solchen Voraussetzungen könnte es je nach Betroffenheit des Übertragungsnetzes zur Abschaltung zahlreicher Großkraftwerke kommen. Die Folge davon wären Stromausfälle im gesamten europäischen Netz oder schlimmstenfalls ein europaweiter Blackout.

Nicht näher betrachtet werden in diesem Szenario mögliche außenwirtschaftliche Probleme aufgrund einer weiter wachsenden Abhängigkeit Deutschlands von Primärenergieträgern (Öl, Gas, Uran). Auch gewalttätige Konflikte in Regionen, in denen Erdöl oder Erdgas gefördert oder durch die sie transportiert werden, sind außen vor gelassen. Ebenso wenig sollen die Probleme der Netzstabilität näher betrachtet werden. Diese kann unter anderem durch die dynamische Belastung des Netzes gefährdet sein, wie sie beispielsweise durch das Zu- und Abschalten leistungsstarker Off-Shore-Windkraftwerke entstehen kann. Weil diese Anlagen meist in strukturschwachen Gegenden errichtet werden, entsteht ein hoher Bedarf für den nötigen Stromtransfer in andere Regionen. Die heutigen Netzkapazitäten sind diesen neuen Anforderungen nur bedingt gewachsen. Ebenfalls werden die wachsenden Netzbelastungen durch eine weitere Liberalisierung der Strommärkte und den intensiven Stromhandel quer durch Europa nicht beleuchtet. Gleiches gilt für das Thema Kernenergie. Erwähnt werden soll an dieser Stelle nur, dass in Deutschland derzeit noch ausreichend eigene Stromerzeugungskapazitäten (Kraftwerke) vorhanden sind. Das Land könnte sich bei einer störungsbedingten Abkoppelung vom Europäischen Verbundnetz daher noch autark versorgen.

Schwere Naturereignisse können ebenfalls einen flächendeckenden Stromausfall auslösen.

3.4 AUSWIRKUNGEN EINES STROMAUSFALLS

Die Folgen eines flächendeckenden und mehrere Tage dauernden Stromausfalls für eine moderne, auf Technik basierende Gesellschaft sind gravierend und komplex. Jeder Teilbereich der Gesellschaft und alle ihre Akteure sind betroffen.



Auch Bereiche, deren Abhängigkeiten von Strom zunächst nicht offensichtlich sind, werden nur noch eingeschränkt oder gar nicht mehr zur Verfügung stehen …

Massive Auswirkungen auf alle Sektoren der Kritischen Infrastrukturen sind aufgrund ihrer Abhängigkeit von Strom zwangsläufig. Besonders von einem Stromausfall betroffen sind:

- die Informations- und Kommunikationstechnologien (IKT),
- das Transport- und Verkehrswesen mit allen Verkehrsträgern,
- die Industrie- und Produktionsbetriebe,
- das Gesundheitswesen einschließlich des Notfall- und Rettungswesens,
- die Versorgung mit Trink- und Brauchwasser,
- die Nahrungsmittelversorgung einschließlich der Transportlogistik,
- die Entsorgung von Abwasser, Schadstoffen und Müll,
- die Behörden und die Öffentliche Verwaltung,
- das Banken- und Finanzwesen einschließlich der Bargeldversorgung,
- die (Groß-)Forschungseinrichtungen,
- die Medien,
- die Energieerzeugung und -verteilung.

Auch Bereiche, deren Abhängigkeiten von Strom zunächst nicht offensichtlich sind, werden in verhältnismäßig kurzer Zeit nur noch eingeschränkt oder gar nicht mehr zur Verfügung stehen, wie beispielsweise die Wasserversorgung und die Abwasserentsorgung. Elektrische Pumpsysteme sind für deren Funktionsfähigkeit ebenso erforderlich wie elektronische Leit-, Steuerungs- und Überwachungssysteme. Gleiches gilt für das Banken- und Finanzwesen. Die Versorgung mit Bargeld durch Geldautomaten und elektronische Kassensysteme sowie auch der elektronische Zahlungsverkehr und der internationale Wertpapierhandel funktionieren mit Strom. Im Bereich der produzierenden Industrie führt ein Stromausfall zur Reduzierung oder zum Stopp der Produktion. Je nach Branche können auch unmittelbare physische Schäden aufgrund des ungeplanten und unkontrollierten Drosselns oder Herunterfahrens von Prozessen auftreten.

Noch ist die ungeheure Fülle von Intra- und Interdependenzen beim Ausfall der Stromversorgung in einzelnen Sektoren und Branchen nicht umfassend untersucht. Daher muss mit weiteren, bislang unentdeckten Folgen gerechnet werden.

Auswirkungen auf die Bevölkerung

Die Bevölkerung wird die Auswirkungen in allen Lebensbereichen zu spüren bekommen. Im privaten Bereich sind die Grundversorgung, das Familienleben und die Freizeit betroffen. Auch am Arbeitsplatz und in Bezug auf Dienstleistungseinrichtungen ist sie unmittelbar und mit aller Härte berührt. Die schwerwiegendsten und direkten Auswirkungen werden im Verlust von Heizung im Winter, Kühlung im Sommer, elektrischem Licht, Telefon, Internet, Rundfunk-/TV-Empfang, der Lebensmittelbevorratung durch Kühlen oder Gefrieren sowie auch im möglichen Verlust der Trinkwasserversorgung liegen. Dann wäre unter anderem auch die Entsorgung von Fäkalien durch die Toilettenspülung nicht mehr gewährleistet. Schon nach kurzer Zeit müssten beispielsweise Hochhäuser aufgrund drohender Seuchengefahr komplett evakuiert werden. Dadurch entsteht ein enormer Bedarf an Notunterkünften. Vor allem in städtischen Gebieten wird dies ein Problem darstellen.

Durch den Ausfall wichtiger Informations- und Kommunikationsmöglichkeiten entsteht Unsicherheit. In der Bevölkerung verbreiten sich Angst und Panik.

Öffentliche Verkehrsmittel werden der Bevölkerung nur sehr eingeschränkt bis gar nicht zur Verfügung stehen. Dies gilt auch für schienengebundene Verkehrssysteme im Nah- und Fernverkehr. Der Individualverkehr würde in Städten zusammenbrechen, weil Ampeln und Straßenbeleuchtung ausfielen. Mittelfristig wäre er durch Treibstoffknappheit gefährdet.

Der allgemeine Einzelhandel wird schließen, weil die Kassensysteme nicht mehr funktionieren, kein Licht vorhanden ist, Heizung, Kühlung, elektrische Türöffnung ausfallen. Aufgrund des Ausfalls computergesteuerter Logistikketten, leerer Warenlager vor Ort wegen der Just-in-time-Logistik wird es sehr schnell zu Engpässen mit Waren des täglichen Bedarfs, vor allem Lebensmitteln, kommen. Sollte die Bevölkerung keine ausreichende Unterstützung von behördlicher Seite erhalten, wird sie sich eigene Wege für ihre Versorgung suchen. Diese werden nicht zwingend rechtsstaatlichen Grundsätzen genügen.

In Ballungsräumen wird die Selbsthilfefähigkeit der Bevölkerung vermutlich geringer sein als auf dem Land. Dagegen sind die öffentlichen Hilfeleistungspotenziale in den Städten oft leistungsfähiger. Trotzdem wäre eine Fluchtbewegung in eher autarke ländliche Gebiete denkbar – vorausgesetzt, es gibt Transportgelegenheiten.

Auswirkungen auf die Behörden, das Notfall- und Rettungswesen sowie die polizeiliche Gefahrenabwehr

Behörden, Rettungswesen und Polizei sind selbst Kritische Infrastrukturen und extrem abhängig von der Stromversorgung. Moderne Leitstellen, die zentral die Alarmierung großer Regionen steuern, computergestützte Führungsinformationssysteme, Krisenmanagementsysteme, Lagebilderstellung – bei allen ist entscheidend, dass Strom für die Informations- und Kommunikationstechnik verfügbar ist [siehe Hintergrund: Informations- und Kommunikationstechnologien, S. 16].

Es hängt stark von der jeweiligen Behörde ab, welche Vorsorge sie für einen Stromausfall getroffen hat. In der Regel werden die Krisenstäbe mit einer Notstromversorgung arbeiten können. Ob und in welchem Umfang die Verwaltungen den Stäben zur Verfügung stehen, hängt vom Einzelfall ab. Erfahrungen aus dem Stromausfall im Münsterland haben gezeigt, dass die Stäbe auf Kreisebene zum Teil personell nicht in der Lage waren, einen 24-Stunden-Betrieb im „Verwaltungs- und Einsatzstab" aufrechtzuerhalten. Kritisch für die Abstimmung und Koordination von Behörden ist die Verfügbarkeit von Kommunikationsmitteln. Bei einem lang anhaltenden, großflächigen Stromausfall ist davon auszugehen, dass auch die öffentlichen Kommunikationssysteme – Mobilfunk, Festnetz und Datennetze – großflächig gestört sein werden. Inwieweit den Behörden hier Ausweichsysteme wie Satellitentelefone zur Verfügung stehen, hängt vom Einzelfall ab. Es gibt derzeit keinen umgesetzten einheitlichen Standard der Ausstattung und Organisation des behördlichen Krisenmanagements. Auch die beschlossene Einführung des neuen digitalen Funksystems für Behörden und Organisationen mit Sicherheitsaufgaben (BOS) wird hinsichtlich der vollen Verfügbarkeit in der Fläche

Behörden, Rettungswesen und Polizei sind selbst Kritische Infrastrukturen und extrem abhängig von der Stromversorgung.

Wesentlich früher als in Krankenhäusern würde es zu Engpässen in den ambulanten Versorgungssystemen kommen.

sowie für alle relevanten Akteure noch einige Zeit dauern. Auch kann dies nur einen begrenzten, ausschließlich technischen Teilaspekt lösen.

Für den neuen BOS-Digitalfunk ist geplant, dass das System bei einem Stromausfall über Batterie drei Stunden lang weiterbetrieben werden kann. Danach muss eine Notstromversorgung organisiert werden.

Das Rettungswesen wäre gleich mehrfach betroffen: Zum einen wären keine Notrufe der Bevölkerung mehr möglich, sobald Telefon und Mobilfunk ausfallen. Zum anderen funktioniert die Koordinierung der Rettungskette nur in dem Maße, in dem die Kommunikation auf Ersatzsysteme ausweichen kann, zum Beispiel durch Notstromversorgung der BOS-Kommunikation oder Satellitentelefone. Engpässe bei der Treibstoffverfügbarkeit wegen ungenügender Notstromversorgung der Tankstellen könnten den Patiententransport nach zwei Tagen zusammenbrechen lassen.

Zwingend ist jedoch, dass die Sicherheits- und Ordnungsbehörden funktionsfähig bleiben. Für Polizei, Feuerwehr und Rettungsdienst müssen zumindest Treibstoffreserven, eine ausreichende Notstromversorgung und ein funktionsfähiges Kommunikationsnetz vorhanden sein.

Auswirkungen auf das Gesundheitswesen

Krankenhäuser verfügen über eine Notversorgung, die den Betrieb kritischer Bereiche wie Operationssäle, Intensivstationen, Röntgen und Labor auch bei einem Stromausfall sicherstellt. Inwieweit ein Krankenhausbetrieb darüber hinaus möglich ist und wie lange der Notbetrieb aufrechterhalten werden kann, hängt vom Einzelfall ab.

Die Notfallkonzepte der Krankenhäuser sehen meist eine frühzeitige Entlassung möglichst vieler Patienten vor. Bei einem flächendeckenden Stromausfall wird das allerdings nicht umsetzbar sein, weil die Wohnungen der Patienten ohne Licht, Trinkwasser, Heizung, Kühlung und Telefon sind. Ein Stromausfall über eine oder gar mehrere Wochen würde folgende Strukturen des Gesundheitsbereichs besonders treffen:

- Alle Bereiche mit kontrollierten Belüftungssystemen wie der OP-Bereich und Isolierstationen würden zusätzliche grundlegende Funktionsbeeinträchtigungen erleiden.
- Probleme entstehen durch den Ausfall der Fahrstühle für Patientenverlegungen, der Notrufsignale, Kühlsysteme und der Hitzesterilisation. Es wird nicht möglich sein, die energieintensiven Systeme zur thermischen Sterilisation von medizinischen Instrumenten aufrechtzuerhalten. Daher können operative Eingriffe nicht durchgeführt werden.
- Der diagnostische Bereich mit Laboren oder bildgebenden Verfahren würde größtenteils ausfallen. Nur noch Basisdiagnostik wäre möglich.
- Spezialisierte Einheiten sind nicht mehr funktionssicher. Beispielsweise Neugeborenen-Intensivstationen oder Einheiten, die eine besondere Raumluftsteuerung aufweisen müssen, wie Knochenmarkstransplantations-Stationen. Ebenso Sonderisolierstationen, die aufgrund hochinfektiöser Erreger mit geregeltem Unterdruck betrieben werden.
- Die Wäscheaufbereitung wird heute in den meisten Fällen von Fremdfirmen erledigt. Sie verfügen nicht über eine Notstromversorgung und werden bei einem Stromausfall ihren Betrieb einstellen.

Die Verantwortlichen würden versuchen, mit Improvisationsmaßnahmen und Verzicht auf gewohnte Standards die Situation so weit wie möglich zu beherrschen. In einigen Bereichen der stationären Versorgung wird dies gelingen, aber die medizinische Versorgung insbesondere auf Intensivstationen ist bei einem flächendeckenden Stromausfall gefährdet. In Deutschland wären etwa 21.000 Intensivbetten betroffen. Bei diesen komplexen und empfindlichen Systemen kann nicht auf Ersatzlösungen ausgewichen oder zeitweilig auf sie verzichtet werden. Bei Ausfall insbesondere der Geräte für künstliche Beatmung werden Patienten sterben oder schwerwiegende Gesundheitsschäden davontragen.

Arztpraxen und ambulante Versorgung

Wesentlich früher als in Krankenhäusern würde es zu Engpässen in den ambulanten Versorgungssystemen kommen. Betroffen wären vor allem die typischen gesundheitlichen Risikogruppen: Säuglinge, Kleinkinder, alte und kranke Menschen.

In Arztpraxen sind keine Notstromeinrichtungen verfügbar. Hier sind neben den Grundfunktionen insbesondere die Diagnostik, die Hitzesterilisation

und therapeutische Anwendungen von einer kontinuierlichen Stromversorgung abhängig. Darüber hinaus werden die niedergelassenen Ärzte vermutlich nur sehr eingeschränkte Dienste anbieten können, weil sie nicht erreichbar sind.

Ein Beispiel für besonders stromabhängige Einrichtungen in der ambulanten Versorgung sind Dialysezentren. Die Opferzahlen könnten hier durchaus in den fünfstelligen Bereich gehen. Auch der Ausfall oder eingeschränkte Betrieb der Blutbanken führt früh zu Engpässen und spätestens nach acht Wochen zu einem völligen Zusammenbruch der Versorgung mit Blutprodukten. Unfallopfer, Tumorpatienten usw. wären betroffen [siehe Anhang 2.1. „Medizinische Versorgung bei Stromausfall“].

Gleiches gilt für Sozialstationen und andere karitative Einrichtungen. Pflegeheime sind insbesondere vom Wegfall der Wasch- und Spülkapazität für die pflegerelevante Ausrüstung betroffen. Auch Hausnotrufsysteme und medizinische Apparate werden nicht einsatzfähig sein, da diese in der Regel über keine vollwertige Notstromversorgung verfügen. Privatwohnungen mit „Dauerpatienten“ zum Beispiel zur Heimdialyse oder beatmungspflichtige Patienten wären von einem Stromausfall besonders hart getroffen.

Auswirkungen auf Gewerbe, Handel und Industrie

Industrie- und Gewerbebetriebe werden größtenteils ihren Betrieb einstellen. Dabei wird es in einzelnen Branchen zu sehr hohen Schäden kommen, zum Beispiel bei Fertigungsprozessen, die nicht ungeregelt heruntergefahren werden dürfen.

Ganz erhebliche Auswirkungen wird ein Stromausfall auf landwirtschaftliche Großbetriebe haben. Bei der Geflügel- und Schweinezucht ist mit Massensterben des Viehs zu rechnen. Ohne Strom können die Tiere nicht mit Wärme, Kühlung und Nahrung versorgt werden. Auch funktionieren weder die elektrischen Melkanlagen noch ist genügend Personal vorhanden, um von Hand zu melken. Die Folgen für die Milchviehhaltung: hohe Ertragsausfälle und zahlreiche tote Tiere.

Die Auswirkungen auf das Finanzwesen und die Börsen werden sehr groß sein. Möglicherweise fallen ganze Handelsplätze in Deutschland aus, weil zahlreiche Handelsbeziehungen nicht realisiert werden können. Öffentliche Einrichtungen werden schließen, wenn keine elektrisch oder elektronisch basierten Systeme funktionieren: Die Aufzüge in Wohn- und Geschäftsgebäuden bleiben stehen. Kaufhäuser und Läden müssen schließen.

Besonders betroffen sind die Entsorgungsbetriebe. Einerseits sind sie selbst nicht mehr funktionstüchtig. Kläranlagen werden ihre Klärprozesse einstellen, Sondermüll wird nicht mehr sachgerecht gelagert und kontrolliert, Hausmüll nicht mehr abtransportiert und verarbeitet. Andererseits kommen auf die Entsorger riesige Mengen neuen Abfalls zu, zum Beispiel massenhaft aufgetaute und verdorbene Tiefkühlwaren.

Versorgung mit Treibstoff und Notstrom

Treibstoff und Notstromaggregate können schon sehr kurzfristig zu einer Engpass-Ressource werden. Bei einer Abfrage von Mineralölkonzernen erhielten wir von einem Unternehmen die Auskunft, dass von 2.200 bundesweiten Tankstellen etwa 15 standardmäßig mit einer Notstromversorgung ausgestattet sind. Im Falle eines Stromausfalls könnten, so die Auskunft des Unternehmens, die anderen Tankstellen über einen internen Logistik-Dienstleister Notstromaggregate ordern. Diese würden innerhalb kurzer Zeit deutschlandweit zur Verfügung gestellt. Offen blieb die Frage, ob die vorhandenen Pumpsysteme mehrheitlich bereits für eine Notstromeinspeisung ausgelegt sind. Möglicherweise müsste man auf manuelle Bedienung ausweichen. Auch hierfür sind technische Vorrichtungen nötig [siehe Anhang 2.2 „Notstromversorgung an Tankstellen“].

Treibstoff und Notstromaggregate können schon sehr kurzfristig zu einer Engpass-Ressource werden.

Notstromaggregate und Ersatzanlagen existieren in den unterschiedlichsten Größenordnungen und Leistungsvolumina. Für die Mehrheit der vorhandenen Aggregate ist der bevorratete Treibstoff auf 12 bis 48 Stunden ausgelegt. Mehr war in der Vergangenheit im Alltag nicht erforderlich. Allgemeinverbindliche bundesweite Vorgaben für die Leistungsumfänge der Notstromversorgung in Unternehmen und anderen Einrichtungen existieren nicht.

Bei dem Stromausfall im Münsterland fehlte eine genaue Kenntnis über verfügbare Ressourcen. Schließlich kamen dort nahezu 300 Notstromaggregate unterschiedlichster Leistungsvolumina und rund 4.000 Helfer zum Einsatz.

HINTERGRUND

Kommunikation beeinflusst Krisenverlauf

Die zentrale Bedeutung guter Risiko- und Krisenkommunikation für die Öffentliche Sicherheit wird noch immer unterschätzt. Kommunikation entfaltet sich auf vier Ebenen: 1. im Vorfeld (präventiv), 2. im Falle einer Krise (reaktiv), 3. nach innen, mit den Akteuren der Gefahrenabwehr, und 4. nach außen, mit der Bevölkerung. Die Medien haben hier eine Schlüsselstellung. Sie können Krisen verstärken, aber auch mildern. Unstrittig ist, dass unzureichende oder keine Verständigung Krisen verschärft. Kommunikation kann selbst zu einer Engpass-Ressource werden, zum Beispiel bei einem Stromausfall oder dem Ausfall von Informations- und Kommunikationstechnologie. Aber auch jegliche andere Verknappung von benötigten Ressourcen führt zu einem Kommunikationsbedarf „on top“, der dann mit den vorhandenen Mitteln bewältigt werden muss.

3.5 NACHHALTIGES RISIKO- UND KRISENMANAGEMENT

Der Stand der Vorbereitungen auf ein Szenario „Stromausfall“ ist in Deutschland sehr heterogen. Nach wie vor gehen viele Akteure davon aus, dass es zu keinem lang andauernden und überregionalen Stromausfall kommen wird. Dabei sind ihnen weder die Komplexität eines solchen Stromausfalls noch die Intra- und Interdependenzen der Infrastrukturen bekannt oder tatsächlich bewusst. Vor allem die Wohnbevölkerung in Deutschland ist auf ein solches Szenario nicht vorbereitet: Weder Selbstschutz- noch Selbsthilfepotenziale sind in nennenswertem Umfang vorhanden. Auch Industrie und Behörden sind höchst unterschiedlich vorbereitet.

Um ein solches Szenario kurzfristig bewältigen zu können, wären zunächst technische und organisatorisch-planerische Fähigkeiten gefordert. Eine genaue Erfassung von Kritischer Infrastruktur zum gezielten Einsatz von Generatoren wäre nötig, um die minimalen Bedürfnisse des öffentlichen Lebens weiterzuführen. Dies sind zu allererst Fernmeldesysteme, Polizei, Feuerwehr, Krankenhäuser, Leitstellen, ausgewählte Einkaufsmärkte, Tankstellen und Banken. Generatoren müssten sofort an vorher genau definierten Stellen zum Einsatz kommen. Die Bevölkerung mit Lebensmitteln und Treibstoff zu versorgen, ist im Falle einer Krise eine der größten Herausforderungen für die Öffentliche Sicherheit.

Mittelfristig müsste die Stromversorgung durch alternative Leitungssysteme, Verbundnetze und Umwegschaltungen so schnell wie möglich wiederhergestellt werden. Dazu ist ein Alarmierungsplan für sofort einsetzbare Reparaturteams und technische Systeme aufzubauen. Die Wiederherstellung der Stromversorgung obliegt den Unternehmen. Die Generatoren-Stromerzeugung verteilt sich hingegen auf verschiedene Akteure: Feuerwehr, Technisches Hilfswerk, Bundeswehr, Bundespolizei und Länderpolizeien, Hilfsorganisationen, Industrie und Gewerbe. Möglicherweise wären durch einen solchen Stromausfall auch die Öffentliche Sicherheit und Ordnung gefährdet. Die Polizeien müssen sich auf Plünderungen einstellen. Eventuell müssen sie sogar Bewegungsbeschränkungen in der Bevölkerung durchsetzen. Weitere Hilfsmittel wären die Schließung öffentlicher Einrichtungen wie Schulen, Bibliotheken und einiger Behörden sowie regionale Zuweisung von Versorgungsstellen.

Grundsätzlich bedarf es eines nachhaltigen Risiko- und Krisenmanagements, das die Prävention in den Vordergrund stellt. Die Schnittstellen sind zu definieren: Das Krisenmanagement muss auf optimierten Kommunikationsstrukturen aufbauen und alle Akteure umfassen. Sowohl die Risikosteuerung als auch das Krisenmanagement müssen von einer sektoralen Betrachtung zu einer prozessualen und ganzheitlichen Betrachtung kommen. Beide sollten nach standardisierten Regeln ablaufen und regelmäßig geübt werden.

3.6 FAZIT

Das Szenario „Stromausfall“ ist ein Schlüsselszenario. Es besitzt Interdependenzen mit anderen lebenswichtigen Infrastrukturen und hat Auswirkungen auf nahezu alle Lebens- und Geschäftsbereiche. Sollte es zu einem solchen überregionalen und lang anhaltenden Stromausfall kommen, wird dies erhebliche Beeinträchtigungen der Bevölkerung und enorme volkswirtschaftliche Schäden nach sich ziehen. Sicherheit und Grundversorgung der Bürger könnten von staatlichen Einrichtungen und privaten Hilfsorganisationen nicht mehr aufrechterhalten werden.

Der Wirtschaftsstandort Deutschland und der Standortvorteil „Sicherheit“ gerieten in eine international geführte, kritische Diskussion. Derzeit ist kein einheitliches Risiko- und Krisenmanagement bei Unternehmen, Staat und anderen Akteuren erkennbar. Der Sensibilisierungsgrad ist gering, die Selbsthilfefähigkeit der Bevölkerung kaum ausgeprägt. Ein Stromausfall dieser Größenordnung wäre eine nationale Katastrophe mit kurz-, mittel- und langfristigen Schäden für die gesamte Gesellschaft.

Derzeit ist kein einheitliches Risiko- und Krisenmanagement bei Unternehmen, Staat und anderen Akteuren erkennbar. Der Sensibilisierungsgrad ist gering, die Selbsthilfefähigkeit der Bevölkerung kaum ausgeprägt.

4. BEDROHUNG DER SICHERHEIT IN DEUTSCHLAND DURCH TERRORISMUS UND ORGANISIERTE KRIMINALITÄT

Der planvoll handelnde und länderübergreifend verbundene internationale Terrorismus gilt als eine der unmittelbarsten Bedrohungen für die Sicherheit Deutschlands. Das wird sich verstärken. Die deutschen Behörden bearbeiten derzeit mehr als 200 Ermittlungsverfahren mit islamistisch-terroristischem Hintergrund. Hinzu kommen Verbotsverfahren gegen islamistische Organisationen in Deutschland, zum Beispiel den Kalifatstaat und die in Deutschland verbotene Vereinigung Hizb-ut-Tahrir. Sie alle stellen aber nur die Spitze des Eisberges zunehmender Radikalisierung eines wachsenden Anteils der muslimischen Bevölkerung Deutschlands dar.

Das Bedrohungspotenzial der OK, insbesondere auch durch ihre Symbiose mit dem Terrorismus, wird eher unterschätzt.

Weniger intensiv nimmt die Öffentlichkeit die Organisierte Kriminalität (OK) wahr. Deren Bedrohungspotenzial, insbesondere auch durch ihre Symbiose mit dem Terrorismus, wird eher unterschätzt. „Organisierte Kriminalität ist die von Gewinn- und Machtstreben bestimmte planmäßige Begehung von Straftaten, die einzeln oder in ihrer Gesamtheit von erheblicher Bedeutung sind […]“, lautet eine gängige Definition. Die Grenzen zu Wirtschaftskriminalität, Geldwäsche und Steuerhinterziehung sind fließend. OK arbeitet hochprofessionell und häufig transnational. Ihre bevorzugten Arbeitsmethoden sind Konspiration, Korruption und Intimidation. Einige Netzwerke können inzwischen als „OK on demand“ bezeichnet werden: Solche Gruppen formieren sich oft nur noch temporär, je nach „Marktlage“. Sie agieren zunehmend global, oft im virtuellen Raum und sehr flexibel. Nach getaner Arbeit trennen sich oft derartige Netzwerke und finden bei Bedarf wieder in neuer Besetzung zusammen [siehe Anhang 3.1 „Bedrohung durch Terrorismus und Organisierte Kriminalität“].

Terrorismus und Organisierte Kriminalität stehen teilweise in engem Zusammenhang mit weltweiten Phänomenen, die die Sicherheit Deutschlands potenziell bedrohen. Dazu zählen insbesondere:

- Demografie, illegale Migration und Integrationsprobleme,
- Proliferation und Aufrüstungstendenzen,
- Staatszerfall in Teilen Afrikas und Asiens sowie andere Regionalkonflikte,
- Ressourcenkonflikte und Energiesicherheit,
- Störungen Kritischer Infrastrukturen,
- Naturkatastrophen und die
- veränderte Rolle der Staaten in einer globalisierten Welt.

4.1 DAS INTERNET ALS NEUE HERAUSFORDERUNG

Moderne Kommunikationstechnik spielt für die weltweit vernetzte, asymmetrische Kriegsführung eine zentrale Rolle: sowohl bei der Kommunikation nach innen als auch nach außen. Die dezentrale und herrschaftslose Struktur des Internets bietet Terroristen und organisierten Kriminellen eine Kommunikations-, Rekrutierungs- und Propagandaplattform. Terroristen geht es um Medienhoheit und Aufmerksamkeit der weltweiten Öffentlichkeit, nicht um militärische Überlegenheit. Sie nutzen daher intensiv Internetforen und Chatrooms, Mobilfunk und Internettelefonie. Teilweise wenden sie dabei moderne Verschlüsselungs- und Verschleierungsmethoden an. Außerdem bietet das Internet selbst die Möglichkeit zum Angriff auf Staat, Wirtschaft und Gesellschaft. Beispielsweise können Bot-Netz-Attacken und Denial-of-Service-Angriffe ganze IT-Systeme lahmlegen. In den kommenden Jahren ist verstärkt mit solchen Aktivitäten und neuen Angriffsmethoden zu rechnen [siehe Hintergrund: Informations- und Kommunikationstechnologie, S. 16].

4.2 SYMBIOSE TROTZ UNTERSCHIEDLICHER ZIELE

Internationaler Terrorismus und OK unterscheiden sich grundlegend in ihren Motiven und Zielsetzungen. Terrorismus des Typs al-Qaida ist politisch oder ideologisch motiviert. Ein wesentliches Element der terroristischen Vorgehensweise ist die Erregung öffentlicher Aufmerksamkeit durch spektakuläre und opferreiche Anschläge. Die Gegner sollen in Angst versetzt und gleichzeitig die eigene potenzielle Anhängerschaft motiviert werden. Die OK hingegen möchte vor allem Gewinne

maximieren. Sie versucht, jegliche Form von Aufmerksamkeit zu minimieren, um ihre illegalen Geschäfte nicht zu gefährden. Daher handelt sie im Verborgenen. Auch versucht sie, den Anschein der Legalität zu erwecken.

Obgleich sie unterschiedliche Ziele verfolgen, weisen OK und Terrorismus bis zu einem gewissen Grad methodische und organisatorische Parallelen und zahlreiche Querverbindungen auf. Auch Terrorismus ist bis zum Endpunkt der Handlungskette – der Durchführung eines Anschlags – auf das Agieren im Untergrund angewiesen. Er bedient sich häufig der Methoden oder etablierten Strukturen und Vertriebsnetze der OK, beispielsweise um falsche Identitäten, Geld und Ressourcen zu beschaffen. Diese werden für Anschlagsvorbereitungen oder das Aufrechterhalten terroristischer Strukturen, wie etwa Trainingslager zur Ausbildung und Indoktrination, verwendet. Neben Spenden und Gewinnen aus legalen Geschäften dienen Rauschgift-, Waffen- oder Diamantengeschäfte eben auch als Finanzquellen des Terrorismus. In umgekehrter Richtung gibt es ebenfalls Verstärkungseffekte: Die Regionalkonflikte auf dem Balkan, im GUS-Raum, im Nahen und Mittleren Osten haben weltweit die Strukturen der OK gestärkt oder neu geschaffen. Auch wenn die Delikte im Hellfeld in Deutschland zuletzt eher zurückgingen, ist die Anzahl der Fälle im Dunkelfeld vermutlich gleichbleibend oder sogar steigend.

Ein Szenario wäre, dass Täter einen Versicherungsbetrug begehen. Das Geld würden sie dazu nutzen, an Waffen, Fahrzeuge, Sprengstoff, Informationen und vor allem strahlendes Material zu gelangen und einen Anschlag mit einer schmutzigen Bombe zu verüben. Im Jahr 2007 wurde der in Deutschland lebende Ibrahim Mohamed K. wegen Mitgliedschaft in einer terroristischen Vereinigung und des Versuchs des bandenmäßigen Betrugs in 28 Fällen zu sieben Jahren Haft verurteilt. K. und seine Mittäter planten einen Versicherungsbetrug, der als Beschaffungskriminalität zur Finanzierung von Terroranschlägen dienen sollte. Sie wollten zunächst Dutzende Lebensversicherungen mit einer Versicherungssumme in Höhe von mehreren Millionen Euro abschließen und die Prämien durch einen vorgetäuschten Autounfall in Ägypten kassieren [siehe Anhang 3.2 „Szenarien Terrorismus und Organisierte Kriminalität", Szenario 1].

4.3 KRISEN AUSLÖSEN UND KRISEN VERSCHÄRFEN

Der internationale Terrorismus nutzt OK-Strukturen im Sinne von Beschaffungskriminalität für seine Aktivitäten. Gleichzeitig schädigt OK auch aus sich heraus in vielfältiger Weise und weitgehend unbemerkt das Gemeinwesen durch Anreize zur Korruption sowie Eigentums- und Wirtschaftskriminalität. OK kann dadurch auf lange Sicht Krisen auslösen. Sie kann aber auch vorhandene Krisen für ihre Zwecke nutzen und verschärfen.

OK kann dadurch auf lange Sicht Krisen auslösen. Sie kann aber auch vorhandene Krisen für ihre Zwecke nutzen und verschärfen.

Der **Drogenhandel** ist das bekannteste Tätigkeitsfeld der OK und eine der einträglichsten Schattenwirtschaften. Der weltweite Gesamtumsatz wird auf 500 bis 800 Milliarden US-Dollar geschätzt. Die sozialen und wirtschaftlichen Folgekosten sind immens, Schätzungen gehen von 147 Milliarden Euro allein in Deutschland aus. Drogenhandel trägt wesentlich zur Finanzierung von Terror- und OK-Gruppen und damit indirekt zur Finanzierung verdeckter und asymmetrischer Kriege bei.

Der lange und schwierige Weg des Heroins oder Kokains von der Ernte über die Produktion, den Transport und den Vertrieb bis hin zum Endabnehmer bedingt eine komplexe organisatorische, logistische, personelle und informationelle Vernetzung. Diese illegalen Strukturen werden deliktübergreifend auch von Terrorgruppen genutzt. Diese haben häufig Anteil an finanziellen Gewinnen und logistischen Möglichkeiten des international organisierten Rauschgifthandels. Das verdeutlicht die gefährliche Symbiose dieser beiden Phänomene [siehe Anhang 3.2 Szenarien „Terrorismus und Organisierte Kriminalität", Szenario 2]. Die illegalen Strukturen des Drogenhandels generieren zudem Korruption, Eigentums- und Wirtschaftskriminalität sowie Beschaffungs- und Ge-

waltkriminalität durch Verteilungskämpfe. Mit Letzteren tragen sie wesentlich zur Erhöhung der allgemeinen Kriminalitätsrate bei.

Die **Eigentums- und Wirtschaftskriminalität** stehen in Deutschland auf Platz zwei der kriminellen Aktivitäten nach der Betäubungsmittelkriminalität. Geldwäsche, Steuer- und Zolldelikte (Schmuggel), Fälschungskriminalität und Bestechung lassen staatliche Strukturen erodieren, nicht nur in fragilen Staaten, sondern auch in Deutschland. Hinzu kommen der Handel unter fremden Namen und der Aufbau von Scheinfirmen, sogenannte Firmenmantelgeschäfte, und verstärkt IT-betriebene Straftaten, wie zum Beispiel das sogenannte Phishing.

Der **Diebstahl besonders hochwertiger oder lebensnotwendiger Güter** ist ein weiteres lukratives Betätigungsfeld der OK. Das Diebstahlsgut wird in einer Wertkonzentration transportiert oder beiläufig in einer Sammelladung oder Lagerstätte platziert. Bekannt ist der massenhafte und generalstabsmäßig durchgeführte Diebstahl sensibler medizinisch-technischer Geräte aus Arztpraxen, von Buntmetallen, von hochwertigern Gütern wie Elektronik und Mikrochips oder von Spezialgeräten aus Baustellen.

Es ist durchaus plausibel, dass solche Diebstähle Engpässe auslösen oder eine bestehende Knappheit verschärfen. Buntmetall-Diebstahl sowie dessen Folgeschäden könnten unmittelbar zu Versorgungsausfällen führen, zum Beispiel bei Fernmeldeeinrichtungen, im Bahnverkehr, in der Ladungs- und Baustellensicherheit. Fehlende medizinische Geräte oder der Diebstahl von Impfstoffen könnten zu Problemen führen oder diese in Krisensituationen verschärfen [siehe Szenarien „Stromausfall" S. 16 und „Seuchengeschehen" S. 30].

Die Bekämpfung des transnationalen Terrorismus wird nur erfolgreich sein, wenn es gelingt, die OK und ihr Umfeld zu beschneiden.

Der **Menschenhandel** hat ein geschätztes Weltmarktvolumen von sieben Milliarden US-Dollar. Die damit verbundene Schleusungskriminalität hat in den vergangenen Jahren deutlich zugenommen. Prostitution gilt als einer der Wachstumsmärkte der Zukunft. Die untere Ebene der Drogenkartelle ist oft bandenmäßig mit OK-Strukturen verwoben, die in den Bereichen Menschenhandel oder Prostitution agieren. Über diese Strukturen kommen jedes Jahr Hunderttausende von illegalen Migrantinnen und Migranten in die westlichen Staaten.

Schutzgelderpressung, Entführungen und Piraterie docken in mannigfaltiger Weise an asymmetrische Konflikte an. OK und Terrorismus schüren wiederum den **Waffenhandel**, der als weitere wichtige Säule der gängigen illegalen Wirtschaft boomt.

Ausgeklügelte Finanzierungsmodelle, deren Komplexität und Symbiosefähigkeiten für die Terrorismusfinanzierung bis heute unterschätzt werden, stehen oft hinter wirtschaftskriminellen Aktivitäten. Beispiele hierfür sind Firmengründungen mit fraglicher Herkunft des Eigenkapitals oder auch die Einfuhr von gestohlenen oder unterschlagenen Fahrzeugen und anderen Gütern aus EU-Ländern. Die OK nutzt dazu unterschiedliche Verschleierungshandlungen, Firmenmantelgeschäfte, Produktpiraterie und Plagiate. Erträge aus dieser, schon fast industriell arbeitenden OK werden grenzüberschreitend unter fremden Namen gewinnbringend angelegt oder direkt an den Verbraucher gebracht.

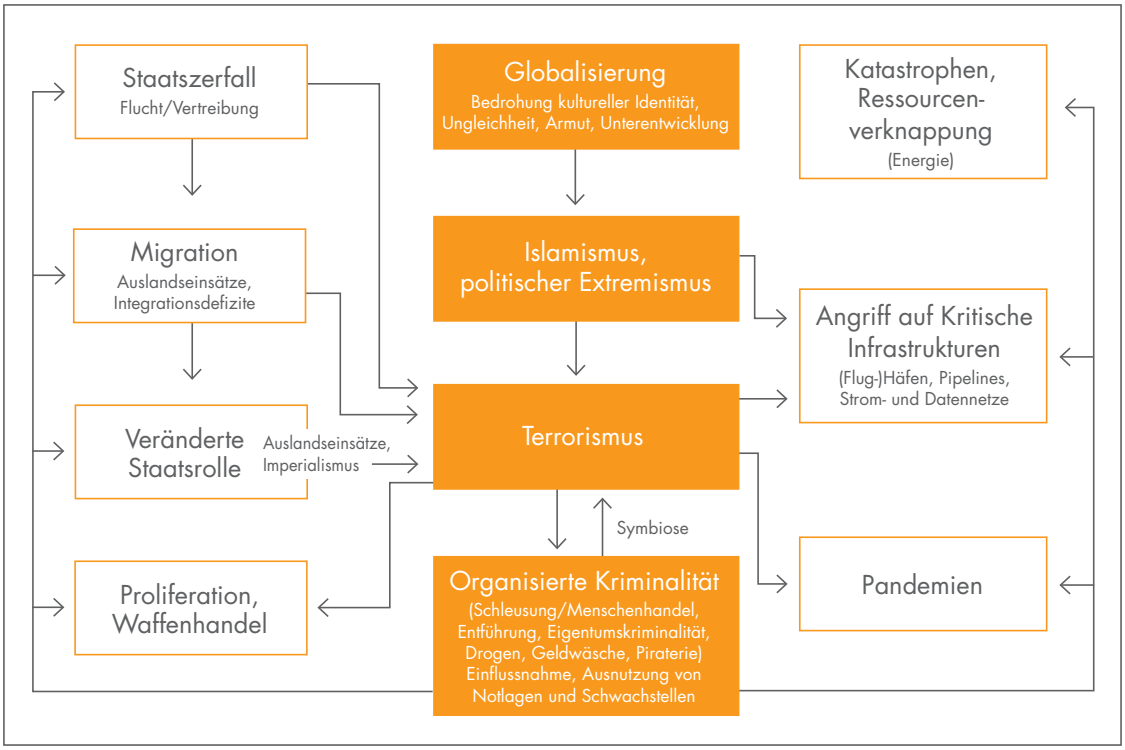
Ziel ist es vielfach, die illegalen Gewinne in die legale Wirtschaft zu investieren. Für ihre Verschleierungszwecke und ihre Karussellgeschäfte benötigt die OK deshalb nach der Straftat „Wechselstuben und Möglichkeiten zur Reinvestition in Luxusgüter". Es ist bekannt, dass Unbeteiligte zum Beispiel gegen Prämien zur Kontennutzung oder zum Kauf von Luxusgütern oder Immobilien animiert werden [siehe Anhang 3.2 „Szenarien Terrorismus und OK", Szenario 3].

Die aufgezählten Delikte gehören statistisch gesehen zu den Massenphänomenen mit hoher Dunkelziffer. Sie besitzen ein enorm sozialschädliches Potenzial und geringe Aufklärungsquoten. Betrugsdelikte haben sich im 20-Jahres-Vergleich verdreifacht und die Anzahl der Tatverdächtigen hat sich verdoppelt. Das Dunkelfeld bei solchen Delikten ist groß. [7] Die Täter werden meist nicht entdeckt und dem Staat fehlen Sanktionsmöglichkeiten. Eine rein deliktbezogene Bearbeitung der Eigentumskriminalität, allein auf Basis der Hellfelder, hat kaum Wirkung. Notwendig wäre eine deliktübergreifende Analyse und Einbindung der verschiedenen Akteure aus der Wirtschaft, der polizeilichen Kriminalstatistik (PKS) und der Strafverfolgungsstatistik (SVS). Andernfalls können grobe Fehleinschätzungen die Folge sein.

Die derzeitig erhältlichen dezentralen, jährlichen Lagebilder aus den Ländern sind von unterschied-

licher Qualität und Quantität. Sie ermöglichen keine ausreichende Betrachtung komplexer wirtschaftlicher sowie deliktübergreifender Zusammenhänge der OK und deren möglicher Terrorismusfinanzierung. Daher sind sie als Evaluationsgrundlage und speziell für schnelle Entscheidungen im Krisenfall ungeeignet.

VERKNÜPFUNG DER BEDROHUNGSFELDER



4.4 FAZIT

Die Bekämpfung des transnationalen Terrorismus wird nur erfolgreich sein, wenn es gelingt, die OK und ihr Umfeld zu Wirtschaftskriminalität, Geldwäsche, Steuer- und Zolldelikten wirksam zu beschneiden. Um der OK die Finanzierungsgrundlagen zu entziehen, muss inkriminiertes Vermögen mit allen rechtsstaatlichen Mitteln konsequent abgeschöpft werden. Dazu müssen grenzüberschreitende bilaterale Regelungen in der Europäischen Union zur Rückgewinnungshilfe von Vermögenswerten aus Eigentumsdelikten geschaffen werden. Datenschutzrechtliche Probleme, die eine Zusammenarbeit der verschiedenen Akteure zur Krisenvermeidung und Bewältigung hemmen könnten, sind zu überprüfen und mit für die Praxis tauglichen Handlungsstrategien zu versehen.

Die Herausforderungen durch Terrorismus und OK können nur in enger nationaler und internationaler Zusammenarbeit bewältigt werden. Die Akteure benötigen Normen und Standards zum Informationsaustausch. Dazu gehören ein Frühwarnsystem zur Krisenvermeidung und eine anlassbezogene Kommunikation zur Alarmierung bei Krisen. Alle Behörden, Institutionen und Organisationen sollten enger als bisher kooperieren. Die Zusammenarbeit sollte rechtlich so gestellt werden, dass die zur Erledigung ihrer Aufgaben notwendigen, eventuell auch vertraulichen Informationen im Rahmen einer vernetzten Sicherheit zum Wohle der Bürger, der Wirtschaft und des Staates eingesetzt werden können.

[7] Zur Bedrohungslage siehe jährliches Bundeslagebild „Organisierte Kriminalität" von BKA, LKAs, BPol u. Zollkriminalamt unter www.bka.de, zur Bedrohungslage in der EU siehe www.europol.europa.eu/publications/OCTA2007.pdf.

5. SZENARIO „SEUCHENGESCHEHEN IN DEUTSCHLAND“

Seuchen haben seit Menschengedenken Staaten und Gesellschaften in existenzielle Krisen gestürzt. Die dabei zu beklagenden Opfer überstiegen häufig die Zahlen selbst schwerwiegender Naturkatastrophen oder Kriege. Durch die Influenza-Pandemie von 1918 bis 1920 sind mehr Menschen ums Leben gekommen als im Ersten Weltkrieg. Die „Pestilenz“ im 14. Jahrhundert hat wahrscheinlich ein Drittel der Bevölkerung Mitteleuropas hinweggerafft und damit tief greifende gesellschaftliche Umwälzungen hervorgerufen.

Das Wissen um die Mikrobiologie und die Fortschritte in der Medizin haben diese Gefahren nur vermeintlich beherrschbar gemacht. Das Auftreten von neuen Krankheitserregern oder epidemische Ausbrüche von bekannten Erregern haben in jüngster Zeit wiederholt deutlich gemacht: Auch zukünftig werden Seuchen und Epidemien eine Gefahrenquelle für die Gesellschaft in Deutschland darstellen und staatliches Handeln erfordern.

Zuvorderst sind hier ein Wiederauftreten von Pockenerkrankungen, zum Beispiel in Form eines Terroranschlages, oder eine pandemische Influenza zu nennen. Für beide Krankheiten hat die Bundesrepublik Vorsorge getroffen oder Vorbereitungen in die Wege geleitet. Dieses Grünbuch weist exemplarisch auf potenzielle Seuchen hin, die unter ungünstigen Umständen vergleichbare Folgen in Deutschland haben könnten.

Viele Krankheiten sind, anders als die bereits erwähnten Pocken und die Influenza, nicht direkt von Mensch zu Mensch übertragbar. Sie brauchen einen „Vektor“, der den Krankheitserreger auf den Menschen überträgt. Häufig sind das Mücken (Malaria, Dengue-, Chikungunya-Fieber) oder Zecken (FSME, Borreliose), aber auch Säugetiere wie Mäuse (Hanta-Virus Erkrankungen) oder Katzen (Lungenpest). Veränderte klimatische Bedingungen in Verbindung mit weltweitem Warenaustausch und Reiseverkehr können die Verbreitung sowohl solcher Vektoren als auch von Erregern begünstigen. Der Klimawandel führt schon heute dazu, dass sich Krankheitserreger und ihre Vektoren in neuen Verbreitungsgebieten dauerhaft ansiedeln.

Erschwerend kommt hinzu, dass das Auftreten einer Krankheit in einem bisher verschonten Gebiet dramatische Folgen haben kann. Es hat sich noch kein Gleichgewicht zwischen Erreger und Immunität in der Bevölkerung gebildet. Die Geschwindigkeit der Ausbreitung des durch Mücken übertragenen West-Nil-Virus in den USA hat gezeigt, wie schnell sich ein „fremder“ Erreger in der Natur ausbreitet und dann zu Erkrankungen beim Menschen führt. Innerhalb von nur drei Jahren ist dieser Erreger von der Ostküste bis zur Westküste vorgedrungen, obwohl intensiv versucht worden war, die Ausbreitung zu verhindern.

HINTERGRUND

Auswirkungen einer Influenza-Pandemie

Etwa 24 Millionen Erkrankte und 103.000 Todesfälle innerhalb von acht Wochen – so könnte, nach Berechnungen der Berufsfeuerwehr Frankfurt am Main, die Bilanz einer Influenza-Pandemie bei mittlerer Erkrankungsrate aussehen. Im Nationalen Pandemieplan (Stand Mai 2007) wird angenommen, dass etwa ein Drittel der Bevölkerung sich mit dem Grippevirus ansteckt. Derzeit muss davon ausgegangen werden, dass alle Altersgruppen gleichermaßen betroffen wären. Rund die Hälfte der Erkrankten würde aufgrund des schweren Krankheitsverlaufes einen Arzt konsultieren und sich behandeln lassen.

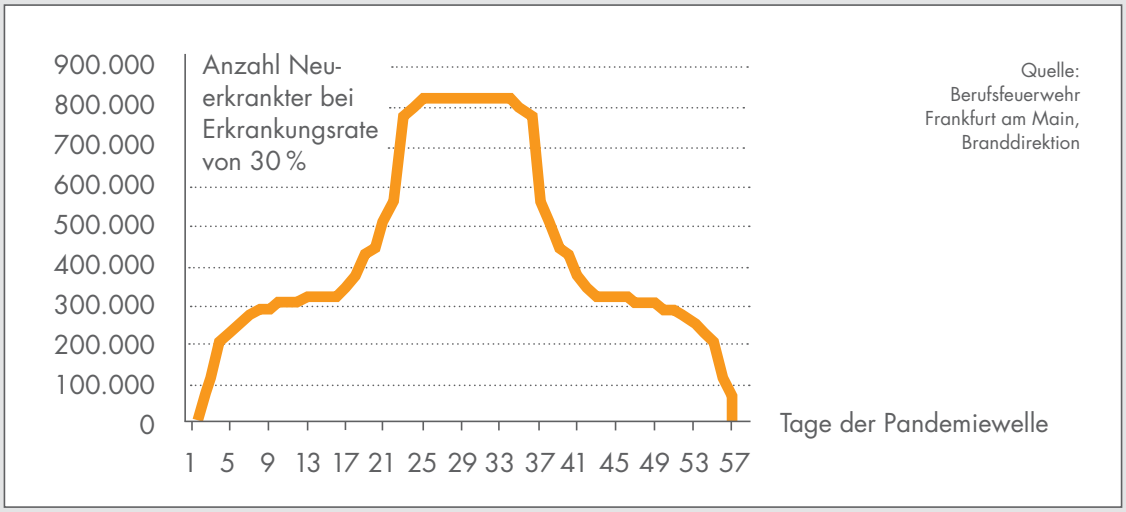
Es wird eine durchschnittliche zusätzliche Belastung der Ärzte von insgesamt 299.000 Arztbesuchen pro Tag erwartet. Vom 21. bis zum 36. Tag der Krankheitswelle könnten jeden Tag etwa 820.000 Menschen neu erkranken. Dies hat nicht nur Auswirkungen auf das Gesundheitssystem, sondern auch deutlich negative Folgen für die Wirtschaft.

Medizinische Versorgung und Wirtschaft besonders betroffen

Bei einer solchen Pandemie käme es zu dramatischen Personalausfällen. Engpässe in lebensnotwendigen Bereichen entstünden besonders dadurch, dass Schlüsselpositionen nicht mehr besetzt werden könnten. Dazu zählen Einsatzkräfte von Polizei und Feuerwehr, aber auch Branchen wie Logistik, Verkehr und Stromversorgung. Staatliche Hilfe wäre nicht mehr in ausreichendem Maße vorhanden, die Bevölkerung wäre weitgehend auf sich gestellt. In einer solchen Lage würde der natürliche Selbsterhaltungstrieb des Menschen geweckt. Viele Gesunde würden ihrem Arbeitsplatz fernbleiben. Entweder weil sie sich nicht anstecken wollen oder weil sie sich um ihre Angehörigen kümmern. Dadurch wird die Lage noch verschärft.

Besonders problematisch ist der Personalausfall im Bereich der niedergelassenen Ärzte, in Krankenhäusern und der polizeilichen und nicht polizeilichen Gefahrenabwehr. Die Arztbesuche, das Transportaufkommen im Rettungsdienst und die stationären Behandlungen werden dann am höchsten sein, wenn auch der krankheitsbedingte Personalausfall seinen Spitzenwert erreicht. Der Ausfall von Arbeitskräften beeinflusst die Wirtschaft auch dann noch, wenn es keine Neuerkrankungen mehr gibt. Das liegt an der durchschnittlichen Dauer vom Erkrankungsbeginn bis zur Genesung. Im Schnitt sind Menschen, die erst am Ende der Pandemiewelle erkranken, erst nach 21 Tagen wieder arbeitsfähig.

NEUERKRANKTE WÄHREND EINER ACHTWÖCHIGEN INFLUENZA-PANDEMIE



5.1 DAS CHIKUNGUNYA-VIRUS

Das Chikungunya-Virus[8] wird hauptsächlich von der Gelbfiebermücke (Aedes aegypti), aber auch von anderen Aedes-Arten, wie der asiatischen Tigermücke (Aedes albopictus), auf den Menschen übertragen. Selbst Mücken, die nicht der Gattung Aedes angehören, können in einzelnen Regionen als Vektoren dienen. Virusreservoir sind Affen, Nagetiere und Vögel. Während einer Epidemie stellt der Mensch das Hauptreservoir dar. Die Übertragung Mensch–Mücke–Mensch dominiert das Ausbruchsgeschehen. Beim Menschen verläuft die Krankheit nur sehr selten tödlich. Nach einer Inkubationszeit von drei bis zwölf Tagen bekommen die Kranken hohes Fieber, starke Kopfschmerzen, Entzündung der Augenbindehäute sowie Muskel- und Gelenkschmerzen. Die Gelenke sind geschwollen und häufig so berührungsempfindlich und schmerzhaft, dass selbst einfache Verrichtungen des täglichen Lebens nicht mehr möglich sind. Die Behandlung besteht in der Linderung der Symptome. Eine spezifische Therapie oder einen Impfschutz gibt es nicht. In der Regel klingen die Symptome nach ein bis drei Wochen ab. Bei etwa zehn Prozent der Menschen dauern die Gelenkschmerzen mehrere Monate, manchmal Jahre. Das Chikungunya-Fieber wurde ursprünglich in Ostafrika entdeckt und kommt derzeit vor allem rund um den Indischen Ozean in Asien (unter anderem Malaysia, Thailand, Kambodscha, Myanmar, Sri Lanka, Indien, Indonesien) und Afrika (unter anderem Tansania, Madagaskar, Mauritius, Seychellen) vor. Inzwischen sind auch andere tropische Regionen in Asien und Afrika wie die Philippinen, Gambia, Senegal und Guinea betroffen.

Ein Hinweis darauf, mit welcher Geschwindigkeit sich das Virus verbreiten und unvorhergesehen zu einer unkontrollierbaren Epidemie führen kann, gab der Ausbruch dieser Krankheit Ende 2005/Anfang 2006 auf La Réunion. Die Insel mit knapp 800.000 Einwohnern ist östlich von Madagaskar gelegen und gehört zu den Übersee-Departements Frankreichs. Innerhalb von nur acht Wochen erkrankte ein Drittel der Bevölkerung. Verantwortlich dafür war die Verkettung zweier Ereignisse: eine Extremwetterlage und die Mutation des Chikungunya-Virus. Der Hauptüberträger des Virus, die Gelbfiebermücke, kommt auf La Réunion praktisch nicht vor. Eine winzige Veränderung im Erbgut des Virus hatte jedoch zu einer Anpassung an die dort weit verbreitete Tigermücke geführt. Wochenlange Starkniederschläge lösten eine Massenvermehrung dieser Mücke aus und schafften die Grundlage für eine explosionsartige Verbreitung des Virus.

[8] Chikungunya [sprich: Tschickungúnja] soll der Bantu-Sprache entstammen und „sich zusammenkrümmen“ bedeuten.

Auf dem Höhepunkt des Ausbruchs waren knapp 20 Prozent der Inselbewohner – und damit auch des medizinischen Personals – gleichzeitig erkrankt. Nur durch das Einfliegen von medizinischem Fachpersonal aus dem Mutterland Frankreich konnte ein totaler Zusammenbruch des öffentlichen Lebens und der Versorgung verhindert werden.

Das Chikungunya-Virus hat inzwischen Mittelmeeranrainer der Europäischen Union erreicht. Im Jahr 2007 ist das Virus in Norditalien aufgetreten. Dort wurden Menschen durch heimische Mücken infiziert, nachdem die Krankheit wahrscheinlich durch einen Reisenden aus Indien eingeschleppt worden war. In Deutschland wurden im Frühjahr 2008 am Oberrhein Eier der Tigermücke in einem Einzelfall nachgewiesen. Allerdings ist bis heute nicht von einer nennenswerten Population auszugehen.

Der zunehmende Temperaturanstieg in Mitteleuropa führt schon heute zu sehr milden, in den Niederungen weitgehend frostfreien Wintern und zu Sommern mit tropischen Temperaturen. Eine Folge davon ist, dass sich Krankheitsüberträger wie die erwähnten Aedes-Arten aus den Tropen und Subtropen bis nach Deutschland ausbreiten können und hier heimisch werden. Die Mücken sind auch nicht mehr nur auf die natürliche Ausbreitung angewiesen. Vielmehr „nutzen" sie die hohe Mobilität von Gütern und Menschen, zum Beispiel den Transport von Altreifen aus den Tropen nach Europa, wo der inzwischen wieder wertvolle Rohstoff recycelt wird. Die Mücken legen im tropischen Herkunftsland ihre Eier in dem Regenwasser, das sich in den Altreifen gesammelt hat, ab. So begeben sie sich mitsamt dem Altmaterial auf Weltreise. Auch in Importbetrieben von Zimmerbambuspflanzen in den Niederlanden konnte inzwischen die asiatische Tigermücke nachgewiesen werden.

Grundannahmen

Die aktuellen Ergebnisse regionaler Klimamodelle rechnen für Deutschland tendenziell mit einer deutlichen Zunahme heißer Tage und Nächte sowie einer gestiegenen Anzahl und Dauer von Hitzeperioden. Die Modelle gehen davon aus, dass sich Niederschläge in Deutschland künftig anders verteilen: Im Sommer wird es zu kürzeren, aber heftigeren Niederschlägen kommen. Diese generellen Trends müssen nicht in jedem Jahr zu beobachten sein. Es wird Jahre geben, die relativ „durchschnittlich" sein werden, und andere, in denen sich der Klimawandel schon deutlich zeigt. Diese Variabilität des Klimas steht dabei nicht im Gegensatz zur generellen, langfristigen Entwicklung.

Basierend auf den klimatischen Berechnungen und den Erfahrungen mit dem Ausbruch des Chikungunya-Fiebers auf La Réunion wird das Szenario für Deutschland, insbesondere für den Süden und Westen, angenommen. Zwar sind heute die Voraussetzungen in Deutschland noch nicht gegeben, aber in 10 bis 20 Jahren könnte dieses Szenario eintreten. Es geht davon aus, dass die Gegenden entlang dem Rhein, der Naturraum Alp und das Bayerische Hügelland über Wochen Tageshöchsttemperaturen über 30 Grad Celsius und „tropische Nächte" in einem bisher ungekannten Ausmaß verzeichnen. Eine solche Situation ist in gewissem Ausmaß mit den Bedingungen des Hitzesommers 2003 vergleichbar. Hinzu kommen immer wieder auftretende intensive Niederschläge von kurzer Dauer. Experten registrieren schon heute, dass sich das Niederschlagsmuster in diese Richtung verändert hat und künftig verändern wird. Beispielsweise kann der Durchzug mehrerer Gewitter derartige schauerartige Niederschläge verursachen. Eine solche Wetterlage kann mehrere Tage oder länger als eine Woche andauern und in der Summe zu flächenhaften Niederschlägen und zu teilweise großflächigen Überschwemmungen führen. Klimamodelle projizieren, dass sich diese Tendenz in der Veränderung der Niederschlagsmuster weiter verstärken wird.

Außerdem könnten folgende mögliche, zukünftige Entwicklungen die Ausbreitung des Chikungunya-Fiebers begünstigen:

- Die klimatischen Verhältnisse haben sich so verändert, dass sich im Süden und Westen Deutschlands eine stabile Population von tropischen Aedes-Mücken gebildet hat. Auch haben sich kälteresistente Tigermücken aus Norditalien in Deutschland ausgebreitet.
- In Norditalien und Südfrankreich hat sich das Chikungunya-Fieber dauerhaft auf einem niedrigen, aber stabilen Niveau etabliert. Von dort werden immer wieder einzelne Fälle nach Deutschland eingeschleppt.
- Auch der Übertragungsweg durch den Ferntourismus aus den Ländern um den Indischen Ozean wird immer wieder bedient. Schon für das Jahr 2006 sind 57 Fälle einer solchen Übertragung gezählt worden.

Zwar sind heute die Voraussetzungen in Deutschland noch nicht gegeben, aber in 10 bis 20 Jahren könnte dieses Szenario eintreten.

Das Szenario

Ein Sommer-Hochwasser und eine Hitzewelle führen zu einer explosionsartigen Vermehrung der Tigermücken. Damit haben sie die Grundlage für eine massenhafte Verbreitung des Virus geschaffen. Die bisher üblichen Maßnahmen der Mückenbekämpfung entfalten nicht die gewünschte Wirkung, weil den Aedes-Mücken schwerer beizukommen ist als ihrer ortsansässigen Verwandtschaft.

Wie sich in Südostasien gezeigt hat, sind diese Stechinsekten an das Leben in Städten sehr gut angepasst. Sie können sich bereits in kleinsten Wasserlachen und Pfützen wie Blumenuntersetzern, Getränkedosen oder Ähnlichem vermehren. Auch verfügt Deutschland, etwa im Vergleich zu Frankreich, über wenig medizin-entomologische Expertise und Einrichtungen zur Mückenbekämpfung.

Zudem sind die Aedes-Mücken überwiegend tagaktiv. Die Tagaktivität hat einen entscheidenden Einfluss auf die Stechraten der Mücken: Es ist für den Menschen schwerer, sich wirksam gegen tagaktive Insekten zu wehren als gegen nachtaktive. Gegen Letztere helfen schon einfache Moskitonetze. Tagaktive Mücken können nur durch Repellenzien oder stichsichere Kleidung effektiv abgewehrt werden. Die Folge sind weit höhere „Opferzahlen“, wie der explosionsartige Ausbruch des Chikungunya-Fiebers auf La Réunion gezeigt hat.

… mehrere Millionen Menschen benötigen gleichzeitig medizinische Betreuung und bleiben dem Arbeitsplatz fern.

Auf dem Höhepunkt des Ausbruchs in dem Szenario beträgt die Rate der Neuerkrankungen acht Prozent der Bevölkerung pro Woche. Diese Zahlen traten in La Réunion tatsächlich auf. Die Erkrankung hält in der Regel ein bis drei Wochen an. Deshalb wird ein signifikanter Anteil der Bevölkerung, der zur Aufrechterhaltung der Grundversorgung und des öffentlichen Lebens notwendig ist, betroffen sein. Legt man die Zahlen von La Réunion zugrunde, ist anzunehmen, dass auf dem Höhepunkt des Ausbruchs 15 bis 25 Prozent der Menschen in der betroffenen Region gleichzeitig erkrankt sein werden. Das heißt, mehrere Millionen Menschen benötigen gleichzeitig medizinische Betreuung und bleiben dem Arbeitsplatz fern. Das medizinische Personal wird wahrscheinlich genauso wie der Rest der Bevölkerung betroffen sein.

Verschärft wird die Situation zusätzlich dadurch, dass

- aufgrund der Hitzewelle die medizinischen Kapazitäten für die Versorgung der besonders betroffenen alten und chronisch kranken Menschen ohnehin bis über die Grenzen hinaus belastet sind,
- aufgrund des Hochwassers die Kräfte der Katastrophenabwehr und die subsidiären Kräfte der Bundeswehr extrem ausgelastet sind,
- Beschäftigte und Helfer, die nicht krank sind, wegen der Pflege von Familienangehörigen dem Arbeitsplatz und dem Einsatzort fernbleiben,
- Helfer der Hochwasserbekämpfung aus Angst um die eigene Gesundheit ihre Hilfeleistung einstellen, da nur die Symptome der Erkrankung behandelt werden können und keine Schutzimpfung möglich ist.

Das Szenario spitzt sich nochmals zu, sobald auch heimische Mückenarten den Krankheitserreger auf den Menschen übertragen. Zudem ist absehbar, dass viele Menschen versuchen werden, die betroffenen Regionen zu verlassen und in krankheitsfreie Gebiete zu flüchten. Solche Fluchtbewegungen verschärfen eine krisenhafte Situation zusätzlich.

In den betroffenen Regionen kommt das öffentliche Leben zum Stillstand. In der Bevölkerung kann Angst oder gar Panik entstehen, die vielleicht durch eine entsprechende Medienberichterstattung verstärkt würde.

Schmerzmittel, andere lindernde Medikamente und Repellenzien werden schnell zu einer Engpass-Ressource. Es ist denkbar, dass die gut etablierten Strukturen der Organisierten Kriminalität einen Schwarzmarkt mit Medikamenten, auch mit nicht zugelassenen, gefälschten oder wirkungslosen Präparaten, aufbauen und damit die Krisenlage weiter verschärfen [siehe Terrorismus und Organisierte Kriminalität, S. 28].

HINTERGRUND

Folgen des Klimawandels in Deutschland

Der globale Klimawandel macht sich auch in Deutschland bemerkbar. Die Jahresmitteltemperatur stieg in den vergangenen 100 Jahren um etwa 0,8 Grad Celsius. Dieser Erwärmungstrend beschleunigte sich im Laufe der vergangenen Jahrzehnte deutlich und ist nun mit 0,15 Grad Celsius je Dekade auf fast das Doppelte gestiegen. Betrachtet man einzelne Regionen und Jahreszeiten, zeigt sich: Vor allem im Westen Deutschlands haben die Niederschläge zum Teil erheblich zugenommen, am stärksten im Winter. Im Osten hingegen nahmen vor allem die sommerlichen Regenfälle ab. Extreme Wetterereignisse, wie Hitzeperioden und Starkniederschläge, treten dafür länger, häufiger und intensiver auf. Dieser Trend wird sich fortsetzen. Wegen ihres hohen Schadenspotenzials sind diese auch volkswirtschaftlich besonders bedeutsam [siehe Anhang 4.1 „Klimawandel"].

Institutionen wie das Umweltbundesamt, der Deutsche Wetterdienst (DWD) und Klimaforschungsinstitute haben in den vergangenen Jahren ihre Ergebnisse regionaler Klimamodelle veröffentlicht. Sie basieren allesamt auf globalen Klimamodellen und ermitteln denkbare Klimaänderungen in Deutschland bis zum Jahr 2100. Beim Vergleich des möglichen Klimas der Jahre 2071 bis 2100 mit dem Zeitraum 1961 bis 1990 zeigen die Klimamodelle, dass

- die Temperaturen in Deutschland um 1,5 bis 3,7 Grad Celsius steigen könnten – allerdings regional und jahreszeitlich unterschiedlich,
- es weniger Frosttage, dafür mehr heiße Tage und mehr Tropennächte geben wird,
- Zahl und Dauer von Hitzewellen zunehmen werden,
- sich die sommerlichen Niederschläge durchschnittlich um 30 Prozent verringern und gleichzeitig die Häufigkeit von Starkniederschlägen zunimmt,
- Gletscher und Schneebedeckung in den Alpen weiter zurückgehen werden und
- der Meeresspiegel um 60 bis 80 Zentimeter steigen könnte.

Der DWD hat vier regionale Klimamodelle miteinander abgeglichen und kommt zu folgenden Ergebnissen: Die Experten gehen von einer Erhöhung der Jahresmitteltemperatur um 1 bis 2,25 Grad Celsius bis zum Jahr 2050 aus. Betrachtet man das ganze Jahrhundert, könnte die Temperatur möglicherweise sogar um zwei bis vier Grad Celsius steigen. Die jährliche Niederschlagsmenge wird aller Voraussicht nach zum Ende des 21. Jahrhunderts kaum Unterschiede zu heute aufweisen. Aber es wird wohl zu einer deutlichen Verschiebung des Niederschlagszyklus kommen. Die Sommerniederschläge werden, je nach Projektion, um 15 bis 40 Prozent abnehmen. Gleichzeitig wird es im Winter mehr regnen. Nur in den östlichen und südlichen Landesteilen ist bis zum Jahr 2050 generell mit einer gewissen Austrocknung zu rechnen: Die Experten erwarten dort 5 bis 15 Prozent weniger Niederschlag.

Regionale Wirkung des Klimawandels

Eine Betrachtung der Naturräume Deutschlands verdeutlicht die regionalen Unterschiede des Klimawandels und seiner Folgen. Für die Küstenregionen von Nord- und Ostsee wird bis zum Ende des 21. Jahrhunderts ein vergleichsweise geringer Temperaturanstieg erwartet. Ursachen dafür sind die Nähe zum Meer und das relativ ausgeglichene, gemäßigte Küstenklima. Allerdings verändert sich die Häufigkeit sogenannter Temperaturkenntage zum Teil deutlich. Das sind Eistage, Frosttage, Sommertage oder Tropennächte. Für die Nordseeküste und das nordwestdeutsche Tiefland berechnen die Modelle eine überdurchschnittliche Zunahme an Niederschlägen im Winter. An der Ostseeküste und im nordostdeutschen Tiefland wird mit einer besonders starken Abnahme der sommerlichen Niederschläge gerechnet. Dies könnte in den heute schon von Trockenheit betroffenen nordöstlichen Regionen Deutschlands zu Problemen führen. Deshalb sind Anpassungsmaßnahmen – zum Beispiel in der Land- oder Wasserwirtschaft – notwendig.

Die zentralen Mittelgebirge und der Harz werden, so die regionalen Projektionen, das im Vergleich zu anderen Teilen Deutschlands kühlere Klima beibehalten. Die Zahl der Frosttage ändert sich in dieser Region weniger stark als in tiefer gelegenen Gebieten. Allerdings wird sich die Zahl der Sommertage gebietsweise mehr als verdoppeln. Das Nieder-

HINTERGRUND

schlagsniveau in diesen Regionen ist schon heute hoch. Die Experten des DWD rechnen mit einer überdurchschnittlichen Abnahme der sommerlichen Niederschläge im Harz und im Harzvorland. Die Winterniederschläge hingegen werden überdurchschnittlich steigen.

Die Region der links- und rechtsrheinischen Mittelgebirge fällt besonders wegen des projizierten Niederschlagverhaltens auf. Hier berechnen die Modelle für die winterlichen Niederschläge die höchste Steigerung in ganz Deutschland. Die Niederschläge im Sommer nehmen hingegen vergleichsweise wenig ab. In den linksrheinischen Mittelgebirgen wird es insgesamt mehr Niederschläge geben. Das könnte Folgen für die Land- und Forstwirtschaft sowie für den Hochwasserschutz haben. Im Oberrheingraben macht sich der Klimawandel besonders mit einer deutlichen Zunahme heißer Tage und Nächte sowie der steigenden Zahl und Dauer der Hitzeperioden bemerkbar. Diese Zunahme ist besonders für das Gesundheitswesen eine Herausforderung.

Im Süden Deutschlands, speziell im Alpenvorland, im Naturraum Alp und im Nordbayerischen Hügelland wird die Temperatur ebenfalls stark steigen. Besonders deutlich könnten sich vor allem im Sommer auch die Niederschläge in Süd- und Südwestdeutschland verringern. Durch die hohen sommerlichen Temperaturen würden sich die Verdunstung der verbliebenen Niederschläge erhöhen und entstehende Wasserprobleme weiter verschärfen.

Der Klimawandel zeigt sich auch an der Zunahme extremer Wetterereignisse, wie Hitzeperioden und Starkniederschläge. Sie treten länger, häufiger und intensiver auf. Es ist nicht möglich, die Schäden solcher Ereignisse im Vorhinein zu berechnen. Ein Blick in die jüngere Vergangenheit zeigt jedoch die mögliche Dimension für Deutschland: Beispielsweise verursachte das Elbe-Hochwasser im Jahr 2002 in Deutschland gesamtwirtschaftliche Schäden von 9,4 Milliarden Euro. Die Orkane „Lothar“ und „Martin“ aus dem Jahr 1999 lösten Schäden in Höhe von mehr als 14 Milliarden Euro aus. Als Folge des heißen Sommers 2003 zählten Statistiker in Deutschland etwa 7.000 Todesfälle mehr als in normalen Sommern.

Doppelstrategie: Anpassung und Vermeidung

Auch wenn noch nicht alle Details künftiger Klimaänderungen und -folgen bekannt sind, versuchen Experten, den Auswirkungen des Klimawandels mit einer Doppelstrategie zu begegnen:

- zum einen die langfristig angelegte Vermeidung (Mitigation) der Emission von Gasen in die Atmosphäre, die das Klima der Erde beeinflussen. Eine Wirkung wird nach mehreren Jahrzehnten oder gar Jahrhunderten eintreten. Bei dieser Strategie geht es um den Schutz des „Kollektivgutes“ Klima.
- zum anderen eine vorausschauende Anpassung (Adaption) der natürlichen und sozialen Systeme an den momentanen und erwarteten Klimawandel. Selbst wenn von heute an keine treibhausrelevanten Emissionen in die Atmosphäre gelangen würden, wird sich das Klima aufgrund der Trägheit des Systems in den kommenden Jahrzehnten verändern.

Auf internationaler Ebene werden, vor allem seit der Klimakonferenz auf Bali im Dezember 2007, Adaptation und Mitigation gleich behandelt. Im Sommer 2007 wurde auf europäischer Ebene ein Grünbuch dazu veröffentlicht. Aller Voraussicht nach wird Ende 2008 ein Weißbuch folgen. Auf nationaler Ebene erarbeitet die Bundesregierung eine Anpassungsstrategie an den Klimawandel. Auch auf regionaler und kommunaler Ebene entfalten sich Aktivitäten zu Klimaschutz und Anpassung. Die Anpassung an den Klimawandel – verstanden im Sinne der Vorsorge – hat vor allem einen regionalen und lokalen Fokus. Es hat sich gezeigt, dass entsprechende Anpassungsmaßnahmen dabei den größten Nutzen bringen.

Damit die Instrumente zur Anpassung an den Klimawandel erfolgreich sind, müssten möglichst genaue Informationen zu Klimaänderungen und Verletzlichkeit (Vulnerabilität) vorliegen. Weiterhin ist entscheidend, etablierte und neue Instrumente der Planung und Raumordnung verstärkt im Sinne der Anpassung an Hochwasser, an Stürme, an Wasserknappheit, an Hitzewellen usw. einzusetzen. Das Ziel ist, die Art und Weise der aktuellen und künftigen Landnutzung klimagerecht zu gestalten. Beispielsweise sollten in Gebieten, in denen immer wieder Hochwasser

auftritt, nach Möglichkeit keine Gebäude errichtet werden. Es ist zu erwarten, dass Konflikte um die künftige Landnutzung stärker werden können. Auch werden in Zukunft auf nationaler, regionaler und kommunaler Ebene unterschiedliche Interessen bei der Nutzung bestimmter Räume bestehen.

Eine langfristige, nachhaltige Entwicklung ist notwendig. Nur so können Klimaschutz, Klimaanpassung und weitere Nutzungsansprüche an den Raum miteinander verknüpft werden. Neben den bereits etablierten Instrumenten haben die Verantwortlichen in den vergangenen Jahren im Sinne einer „Klima-Governance" über neue Formen der Steuerung nachgedacht.

5.2 DAS SARS-VIRUS

Mit dem Chikungunya-Virus stecken sich Menschen über den Vektor Aedes-Mücke an. Ein Krankheitserreger wie das SARS-Virus ist von Mensch zu Mensch übertragbar. Daraus entstehen zusätzliche Herausforderungen.

Die Mobilität von Menschen und Gütern hat in den vergangenen Jahren stark zugenommen. Eine Untersuchung der Bewegung von Geldnoten in den USA (Bill-Tracking) zeigte zum Erstaunen der Wissenschaft: Heute muss mit sehr viel höheren Ausbreitungsgeschwindigkeiten von Erregern gerechnet werden, als dies in bislang verwendeten Modellrechnungen angenommen wird. Kommende Pandemien werden sich nach anderen Gesetzen und sehr viel schneller ausbreiten. Im Fokus der neuen Modellrechnungen stehen vor allem Luftverkehrsknoten wie London, New York und Frankfurt/Main. Diese sind für eine rapide weltweite Ausbreitung einer Epidemie verantwortlich – und zwar weitgehend unabhängig vom Ort des ersten Auftretens eines Krankheitserregers.

Die Erfahrungen mit der Verbreitung von SARS belegen dies eindrücklich. Mitte November 2002 traten in der chinesischen Provinz Guangdong erste Fälle einer atypischen Form einer Lungenentzündung auf, die von der Weltgesundheitsorganisation (WHO) als Severe Acute Respiratory Syndrome (SARS) bezeichnet wurde. Seinen Weg um die Welt begann der Erreger Ende Februar 2003. SARS verbreitete sich extrem schnell und ausnahmslos durch infizierte Patienten auf dem Flugweg. Städte mit internationaler Flughafenanbindung wiesen die höchsten Fallzahlen auf. Die klassischen seuchenhygienischen Maßnahmen zur Eindämmung von Epi- und Pandemien, wie Quarantäne von Kontaktpersonen und Isolierung von Patienten, waren hierbei die einzigen Mittel, die Pandemie zu beenden. Denn es gab und gibt keine Therapie gegen dieses Virus. Auch waren die Krankenhäuser zunächst nicht auf eine so ansteckende Lungenentzündung vorbereitet. Die Konsequenz war, dass zunächst tragischerweise vor allem medizinisches Personal infiziert wurde.

Heute muss mit sehr viel höheren Ausbreitungsgeschwindigkeiten von Erregern gerechnet werden.

Die Todesrate bei SARS ist mit etwa zehn Prozent extrem hoch. Zum Vergleich: Die saisonale Grippe fordert etwa 0,1 Prozent Todesopfer, die Zahl der Sterbefälle während einer Influenza-Pandemie würde bei ein bis maximal zwei Prozent liegen.

Andererseits hat dieses neue Virus im Vergleich zu anderen Erregern auch Eigenschaften, die eine Pandemie mit katastrophalen Ausmaßen bisher verhinderten:

- Das Virus kann erst nach dem Auftreten der Symptome von Erkrankten auf andere Menschen übertragen werden. Anders als zum Beispiel HIV, Masern- oder Influenza-Viren, die bereits vor dem Auftreten der Symptome übertragbar sind. Das SARS-Virus befindet sich beim Erkrankten vor allem im unteren Atemtrakt. Erst bei voller Symptomatik der Erkrankung ist die Anzahl der Viren auch im oberen Atemtrakt so hoch, dass durch Husten oder Niesen andere Menschen angesteckt werden können.
- Die Umweltresistenz des SARS-Virus ist nicht sonderlich hoch. Bereits gründliches Händewa-

schen kann den Erreger inaktivieren.
- Eine Übertragung des Erregers kann durch das Tragen eines Mund-Nasen-Schutzes, ähnlich wie bei der Influenza, verhindert werden, weil die Tröpfcheninfektion den typischen Übertragungsweg darstellt.
- Bei Kindern und jungen Erwachsenen verläuft die Erkrankung sehr mild und es gab in dieser Gruppe so gut wie keine Todesfälle. Ab dem 65. Lebensjahr betrug die Todesrate allerdings mehr als 50 Prozent.

Das SARS-Virus hatte weltweit nur etwa 8.000 Menschen angesteckt. Dennoch waren die globalen ökonomischen Auswirkungen dieser Pandemie bemerkenswert. Obwohl Kanada „nur“ 251 Erkrankte mit 43 Todesfällen hatte, wurde der wirtschaftliche Schaden auf knapp eine Milliarde US-Dollar beziffert.

Grundannahmen und Szenario

Dem SARS-Virus könnte eine Mutation ein beachtliches Bedrohungspotenzial verleihen. SARS wäre dann gefährlicher als die Influenza.

Viren haben grundsätzlich eine hohe Mutationsrate. Nur wenige Veränderungen im Erbmaterial des Erregers können dazu führen, dass das Virus neue Eigenschaften annimmt. Die Epidemie des Chikungunya-Fiebers auf La Réunion war durch eine solche Mutation entscheidend begünstigt worden. Dem SARS-Virus könnte eine Mutation ein beachtliches Bedrohungspotenzial verleihen. SARS wäre dann gefährlicher als die Influenza. Denkbar wäre, dass das SARS-Virus durch Mutationen
- schon vor dem Auftreten von Symptomen ansteckend wirkt,
- seine Umweltresistenz erhöht,
- auch bei dem jüngeren Teil der Bevölkerung einen aggressiveren Krankheitsverlauf auslöst
- oder eine Kombination aus den obigen drei Faktoren zur Folge hat.

Für das Szenario wird eine Mutation angenommen, die dem Virus die Fähigkeit verleiht, schon vor dem Auftreten von Symptomen den oberen Atemtrakt zu besiedeln. Das SARS-Virus ist in etwa so infektiös wie das Grippevirus und wäre mit der projizierten Mutation genauso leicht übertragbar. Die Folge wäre eine massive Ausbreitung der Krankheit mit Patientenzahlen, wie man sie für eine Influenza-Pandemie annimmt – aber mit einer zehn bis hundert Mal höheren Letalität. Verschärfend kommt hinzu, dass keine Medikamente zur Behandlung von SARS und kein Impfstoff existieren. Die Auswirkungen wären kaum abzuschätzen, gleichwohl katastrophal.

Rechnet man die Zahlen der SARS-Erkrankung aus dem Jahr 2003 auf eine Pandemie mit einem mutierten SARS-Virus und mehreren Millionen Betroffenen hoch, ergeben sich zudem ökonomische Schäden in Größenordnungen, die selbst für westliche Volkswirtschaften nicht mehr zu kompensieren wären.

5.3 AUSWIRKUNGEN DER SZENARIEN

Das Chikungunya-Virus, aber vor allem eine hochinfektiöse Variante des SARS-Virus bedrohen den Menschen an Leib und Leben. Viel unmittelbarer als bei einem Stromausfall, der für die meisten Menschen erst nach einigen Tagen lebensbedrohlich werden kann, können sich Angst und Panik in der Bevölkerung ausbreiten.

Auswirkungen auf die Bevölkerung

Die Selbsthilfefähigkeit der Bevölkerung ist nicht sehr ausgeprägt. Die Ausbildung in Erster Hilfe wird in Deutschland kaum vorangetrieben. Das ist im Krisenfall ein klares Defizit. Häusliche und familiäre Krankenbetreuung oder Nachbarschaftshilfe sind dann von der ganzen Bevölkerung gefordert. Dadurch bleiben auch Personen dem Arbeitsplatz fern, die eigentlich gesund und arbeitsfähig sind. Schließen öffentliche Einrichtungen wie Schulen oder Kindergärten aufgrund von Quarantänemaßnahmen, betreuen Eltern ihre Kinder zu Hause und fehlen ebenfalls an ihrem Arbeitsplatz.

Auswirkungen auf Behörden, das Notfall- und Rettungswesen, die polizeiliche Gefahrenabwehr und das Gesundheitswesen

Beim Auftreten solcher Seuchen müssten die Akteure möglichst zielgerichtet handeln, um wenigstens eine Basisversorgung sicherzustellen. Sie müssten sich auf Betreuung, Behandlung und Transport der Kranken sowie die Eindämmung des Virus bzw. seiner Übertragung konzentrieren.

Was Betreuung, Behandlung und Transport der Erkrankten anbelangt, wären die Maßnahmen bei-

[9] MANV: „Massenanfall von Verletzten“ oder auch Erkrankten ist ein feststehender Begriff im Katastrophenschutz.

der Szenarien zunächst identisch: In sehr kurzer Zeit ist ein Massenanfall von Erkrankten (MANV)[9] zu bewältigen. In beiden Fällen stehen weder Impfung noch heilende Medikamente zur Verfügung. Der geschwächte Allgemeinzustand der Erkrankten wird mit supportiven Maßnahmen, wie Infusionen oder künstlicher Beatmung, behandelt. Die Behandlung der SARS-Erkrankten ist wegen der Ansteckungsgefahr wesentlich aufwändiger, schwieriger und gefährlicher. In beiden Fällen besteht keine Möglichkeit, durch frühe Impfungen für geschütztes Kernpersonal zu sorgen.

Das Gesundheitswesen wäre völlig überfordert. Die vorhandenen Ressourcen sind auf ein normales Krankheitsaufkommen und lokale Schadensereignisse zugeschnitten. Eine solche Krise könnte nicht einmal ansatzweise bewältigt werden. Das liegt auch an dem steigenden ökonomischen Druck, durch den Überhänge in den Versorgungsstrukturen abgebaut wurden, und der zunehmenden Privatisierung des Gesundheitswesens.

Für die Basisversorgung der Erkrankten müsste sichergestellt sein, dass

- Behelfskrankenstationen, -häuser und Behelfseinrichtungen zur Betreuung errichtet und durch Hilfsorganisationen und den öffentlichen Gesundheitsdienst betrieben werden,
- Hausnotruf und häusliche Betreuung trotz der zusätzlichen Belastung durch das öffentliche Gesundheitswesen und die Hilfsorganisationen/Wohlfahrtsverbände gewährleistet sind,
- eine ausreichende Versorgung mit Medikamenten, Infusionen, Hygieneartikeln und Desinfektionsmitteln durch die Industrie vorhanden ist.

Die heute fehlende Vorratshaltung von medizinischem Material stellt ein weiteres Problem dar. Durch die Just-in-time-Logistik halten Krankenhäuser beispielsweise regulär Infusionen für zwei Tage vor. Zudem existieren kaum belastbare Informationen über den Bedarf an zusätzlichen, lebenswichtigen medizinischen Ressourcen im Falle einer solchen Krise. Über die Anzahl und Art des zusätzlichen Materials, das während des Hitzesommers im Jahr 2003 – mit europaweit etwa 70.000 Todesopfern – benötigt wurde, gibt es bis heute keine zuverlässige, überregionale Studie.

Die Maßnahmen zur Eindämmung der Seuchengeschehen sind unterschiedlich:

- Das Chikungunya-Virus würde vor allem durch die Dezimierung der Überträger-Mücken bekämpft werden. Eventuell wäre eine Abriegelung der von der Tigermücke befallenen Regionen nötig.
- Die hochinfektiöse Variante des SARS-Virus würde einschneidendere Maßnahmen verlangen: zum Beispiel die Seuchengebiete abriegeln, die Ansteckungsrate durch Mund-Nasen-Schutz mindern, Desinfektionsschleusen errichten, Einschränkungen der Bewegungsfreiheit in der Bevölkerung durchsetzen.

Schon nach kurzer Zeit würde in beiden Szenarien die „Engpass-Ressource Mensch" entstehen. Der gesunde – und trotz Ansteckungsgefahr weiterhin arbeitswillige – Mensch wird zum Engpass auf allen Ebenen. Gleichzeitig steigt im gesamten Gesundheits- und Gefahrenabwehrbereich der Bedarf an Arbeitskräften. Letztlich gilt für alle Bereiche, vom Rettungsdienst über die Krankenhäuser bis hin zu den unmittelbar wichtigen Energie- und Lebensmittelversorgern: Das fehlende Personal löst die gefürchteten Kaskaden- und Dominoeffekte aus.

Das Gesundheitswesen wäre völlig überfordert.

Es kommt zwangsläufig zu Mehrfachverplanung von medizinischem Personal und ehrenamtlichen Kräften. Das führt zu weiteren Engpässen in den Hilfsorganisationen. Generell ist mit Ausfällen von Personal mit wichtigen Spezialfähigkeiten zu rechnen, das praktisch nicht ersetzbar ist.

Bei einem mit La Réunion vergleichbaren Ausbruch des Chikungunya-Fiebers in Deutschland würde versucht werden, Unterstützung aus anderen Regionen Deutschlands in das Krisengebiet zu bringen. Doch könnten durch eine Ausweitung der Wetterlage auch die anderen Regionen belastet und die Verfügbarkeit von Kapazitäten stark eingeschränkt sein.

Weiterhin ist fraglich, ob ein Bundesland einem anderen Bundesland Engpass-Ressourcen zur Verfügung stellen würde. Die Länder sind dazu gesetzlich nicht verpflichtet und würden das Risiko eingehen, im Falle einer Ausweitung der Katastrophe selbst keine ausreichenden Kapazitäten zu haben. Die Erfahrung mit dem Elbe-Hochwasser hat gezeigt, dass Länder oder Landkreise hier zum vorsorgenden Horten von Ressourcen („Bunkermentalität") neigen.

In dem SARS-Szenario würde das Seuchengeschehen in kurzer Zeit so weit außer Kontrolle geraten, dass nur eine Quarantäne von Kontaktpersonen, Isolierung von Patienten und andere Maßnahmen des Seuchenschutzes, wie Schließung von Schulen oder Verbot von Massenveranstaltungen, sinnvoll wären. Als Ultima ratio bliebe eine Unterbindung des Personen- und Warenverkehrs mit der Folge der Abriegelung ganzer Städte oder Regionen. Diese Maßnahmen würden aus sich heraus die Krisen extrem verschärfen und die Auswirkung der Katastrophe potenzieren.

Eine einheitliche überregionale Notfallplanung, die eine grundsätzliche Strategie der Abwehr einer Pandemie umfasst, ist nicht vorhanden. Das erschwert ein Krisenmanagement auf allen Ebenen.

Die Erfahrungen mit der SARS-Erkrankung in Kanada zeigten, dass weniger die Infektion selbst, als vielmehr die notwendigen Maßnahmen zu ihrer Bekämpfung die Krisen- und Katastrophenlage hervorriefen.

Auswirkungen auf Gewerbe, Handel und Industrie

Der hohe Krankenstand und das zusätzliche Fernbleiben von Mitarbeitern zum Beispiel wegen der Versorgung Angehöriger oder aus Angst vor Ansteckung führen zu empfindlichen Einschränkungen in allen Wirtschaftsbereichen. Selbst Gegenmaßnahmen wie Rückrufaktionen von in Urlaub befindlichen Mitarbeitern können diesen Notstand nur lindern. Sind kritische Infrastrukturen über das Gesundheitswesen hinaus in ihrer Funktion eingeschränkt, kommt es zu Kaskadeneffekten. Das verschlimmert die Situation zusätzlich.

5.4 PARALLELITÄT DER AUSWIRKUNGEN

Die Engpässe durch Personalausfall in der Energieversorgung, im ITK-Bereich, im Verkehrs- und Logistikbereich und allen anderen kritischen Infrastrukturen können zu ähnlichen Effekten führen, wie sie bereits im Szenario Stromausfall beschrieben wurden.

5.5 FAZIT

Seuchen sind bedeutende Risiken und Gefahren für die Menschen und die Gesellschaft in Deutschland. Sie bedrohen trotz aller Fortschritte in der Medizin auch heute noch die beiden wichtigsten Schutzgüter eines Gemeinwesens: die Gesundheit und die Nahrungsmittelgrundlage des Menschen [siehe dazu auch die Tiererkrankung Maul- und Klauenseuche in Anhang 5.1 „Szenarien Seuchengeschehen“]. Daher wird eine entsprechende Vorbereitung auf solche Ereignisse auch künftig Kernbereich der staatlichen Daseinsfürsorge sein müssen.

Mit dem „Bund-Länder-Rahmenkonzept zu notwendigen fachlichen Vorbereitungen und Maßnahmen zur Seuchenbekämpfung nach bioterroristischen Anschlägen ‚Teil Pocken‘“ und dem nationalen „Pandemieplan Influenza“ bestehen in Deutschland grundlegende Dokumente für die Vorbereitung auf ein großflächiges Seuchengeschehen. Diese können als Beispiel für ein Risiko- und Krisenmanagement herangezogen werden. Allerdings beziehen sich die Dokumente ausschließlich auf die jeweiligen Seuchenausbrüche. Sie lassen ähnlich gelagerte Krisensituationen außen vor.

Eine einheitliche überregionale Notfallplanung, die eine grundsätzliche Strategie der Abwehr einer Pandemie umfasst, ist nicht vorhanden. Das erschwert ein Krisenmanagement auf allen Ebenen. Es bleibt offen, ob bei einer deutschlandweiten Seuche die derzeitigen föderalen Strukturen des Gesundheitswesens und des Katastrophenschutzes die geeignete Organisationsform sind. Vor allem, wenn in einer Krisensituation Mangelressourcen über die Grenzen von Bundesländern hinweg verteilt werden müssten.

6. FÜR EINEN MODERNISIERTEN SICHERHEITSBEGRIFF

Die Szenarien zeigen: Das eigentlich Neue der Informationsgesellschaft ist die zunehmend komplexe, inzwischen weltumspannende Koppelung von Systemen durch Metadatenströme. Dadurch entsteht eine neue Qualität von Verletzlichkeit und Risiko. Sicherheit hängt heute zunehmend von der Datenverfügbarkeit und dem reibungslosen Funktionieren von Kommunikation ab. Verläuft diese falsch, können umfassende Krisen entstehen. Sie können ein Ausmaß erreichen, das bislang nur für den Spannungs- oder Verteidigungsfall denkbar war.

Unter diesen Bedingungen bedeutet „Öffentliche Sicherheit" in erster Linie, dass komplexe Prozesse und Systeme – lokale, nationale bis hin zu transnationalen – möglichst problemlos funktionieren. Das Grünbuch zeigt auf, an welchen Stellen dieses Funktionieren gefährdet ist, und fragt, wie solchen Systemausfällen oder gar Krisen begegnet werden kann. Je mehr Ressourcen mobilisiert werden, desto widerstandsfähiger und krisenfester („resilienter") sind Gesellschaft und Staat.

Die zentrale Frage lautet: Womit können die Verantwortlichen ein solches reibungsloses Funktionieren durchsetzen, aufrechterhalten und – im Falle einer Krise – möglichst rasch zurückgewinnen? In welchem Umfang und wie lange können die einzelnen Funktionalitäten ausfallen, bis Gesellschaft und Staat existenziell gefährdet wären? Welche Mittel („funktionale Äquivalente") sind notwendig, um diese Ausfälle überbrücken, umgehen oder kompensieren zu können?

„Öffentliche Sicherheit" bedarf somit einer materiellen und einer konzeptionellen Bestimmung:

- Die **materielle Bestimmung** bezieht sich auf Art und Umfang der erforderlichen funktionalen Äquivalente: Was wird benötigt, um Systemausfälle überbrücken und das Gesamtsystem funktionstüchtig halten zu können?
- Die **konzeptionelle Bestimmung** bezieht sich auf den Maßstab von „Sicherheit". Wie viel oder wie wenig Funktionsverlust erscheint für welchen Funktionsträger akzeptabel? Wie viel oder wie wenig kann dieser sich im Vergleich zu anderen Funktionsanbietern leisten? Sicherheit kostet und muss wie andere Güter erwirtschaftet werden. Damit wird Sicherheit auch zu einem bedeutenden Standortfaktor.

Sicherheit kann in modernen Gesellschaften nicht länger national oder rein sektoral definiert und gleichfalls nicht mehr unabhängig hervorgebracht werden. Das belegen Krisen wie SARS oder ein flächendeckender Stromausfall. Sicherheit braucht globale Rahmenbedingungen und Überwachungsinstrumente.

Aus der Klimafolgenforschung ist bekannt, dass langfristige, schleichende und weltweite Veränderungen grundlegend neue Erkenntnisverfahren erfordern, zum Beispiel Modellierung und Simulation. Auch müssen neue Reaktionsweisen eingeführt werden, wie langfristige Steuerung, Vermeidung, Anpassung, Akzeptanz und Legitimation.

Bevölkerungsschutz ist nicht allein staatliche Aufgabe, auch die Wirtschaft trägt Verantwortung; vor allem, wenn sie Kritische Infrastrukturen betreibt. Außerdem trägt

jeder Bürger Verantwortung – sei es als Wille und Fähigkeit zu Selbstschutz oder als Hilfe für andere. Dies erfordert einen veränderten Umgang mit Gefahr und Risiko. Notwendig ist ein „Human Resources Management", das die Bürger als Potenzial und Partner sieht. Nur wenn ein gemeinsames Verständnis kollektiver Sicherheit entsteht, werden die Bürger bereit sein, Beiträge zu leisten und im Ernstfall Einschränkungen hinzunehmen. Sicherheit ohne materielle wie immaterielle Kosten ist unmöglich. Freiheit und Sicherheit sind jedoch kein Widerspruch.

6.1 LEITFRAGEN: SICHERHEITSPHILOSOPHIE UND SCHUTZZIELE

- Sind die bisherigen **Sicherheitsphilosophien** und die dazu entwickelten **Sicherheitsarchitekturen** weiterhin gültig? Auf welche Gefahren müssen sich Gesellschaft und Staat einrichten? Mit welchen Instrumenten können Bedrohungen frühzeitig erkannt werden?
- Muss es besondere **Rechte** auf einen noch zu definierenden „Grundschutz" geben – neben den allgemeinen Menschen-, Völker- und Grundrechten?
- Wie lässt sich der Informationsbedarf moderner Gesellschaften decken? Und wie können gleichzeitig die bürgerlichen **Grundrechte** und die Belange informationeller Selbstbestimmung gewahrt bleiben?
- Welcher Vermittlungsinstrumente bedarf es, damit zukünftige Bedrohungen wahrgenommen und angemessen beantwortet werden? Reichen die bestehenden Formen der **Risiko- und Krisenkommunikation** aus?
- Wie viele **Krisen** und wie viele **Schadwirkungen** halten Gesellschaft und Staat aus? Welche Ressourcen und Fähigkeiten sind nötig, um diese Schäden zu überstehen und langfristig widerstandsfähig zu sein? Was leisten Staat, Wirtschaft und Bürger? Welche staatlichen Schutzleistungen erwarten alle Beteiligten?
- Welche Widerstandskraft (Resilienz) wird kurz-, mittel- und langfristig von Gesellschaft, Staat und Wirtschaft erwartet? Was sollen die **Kritischen Infrastrukturen**, vor allem Stromversorgung und Informations- und Kommunikationstechnologien, leisten?
- Welche Formen der **internationalen Zusammenarbeit** werden für ein krisenfestes Management transnationaler Infrastrukturen benötigt? Und welche Formen der internationalen Zusammenarbeit müssen zur Bewältigung oder Abwehr grenzüberschreitender Gefahren entwickelt werden?
- Sind **technische, organisatorische und rechtliche Standardisierungen notwendig**, um transnationale Rahmenbedingungen für globale Sicherheit entwickeln zu können?
- Wie müssen **Kommunikation und Kooperation** zwischen den Akteuren der polizeilichen und der nicht polizeilichen Gefahrenabwehr, der privaten und öffentlichen Institutionen, der nationalen und internationalen Ebenen gestaltet werden?
- Angesichts veränderter Bedrohungslagen, vor allem bei „schleichenden" Ereignissen, sind neben reaktiven Maßnahmen auch **präventive Verfahren und Instrumente** notwendig. Wie lassen sich diese innerhalb Deutschlands implementieren? Und wie lassen sie sich international harmonisieren, zum Beispiel bei Pandemien und Umweltveränderungen?

- Sind die erwarteten Auswirkungen vital bedrohlicher Lagen auf die **Volkswirtschaft** (Klimawandel und Ressourcenmangel) überstehbar? Wären die dadurch bewirkten Verluste akzeptabel?
- Sind die Auswirkungen spezifischer Gefahren, beispielsweise Organisierte Kriminalität, **auf Volkswirtschaft und Gesellschaft** ausreichend beschrieben und gibt es ein öffentliches Bewusstsein dafür? Gibt es geeignete Antworten darauf, wie die Abschöpfung illegaler Gewinne oder Social Surveillance?

6.2 LEITFRAGEN: RESSOURCEN UND MOBILISIERUNG

- Im Prinzip ist alles Ressource: Natur, Menschen, Wissen. Welche Ressource wird wie und unter welchen Bedingungen zu einem **vitalen Mangel**? Wie kann dieser kompensiert, ersetzt oder überbrückt werden?
- Welche **natürlichen Ressourcen** müssen geschützt werden? Welche müssen vorgehalten werden – in Form von Mindestreserven oder Sicherstellungsgesetzen? Und welche Ressourcen müssen entwickelt oder gebildet werden?
- Was ist in einer Krise oder Katastrophe unverzichtbar? Wie lange können Gesellschaft und Staat existenzbedrohliche Mangellagen überstehen (materielle, physische und psychische **Durchhaltefähigkeit**)?
- Ab welcher Größenordnung wird ein Mangel lebensbedrohlich? Wie lassen sich Ressourcen **mobilisieren und verteilen** (zum Beispiel bei einer Influenza-Pandemie, bei der etwa 24 Millionen Menschen betroffen sein könnten) ?
- Welche **Reaktionsstrategien** stehen in Krisenfällen zur Verfügung und wie können sie kommuniziert und eingeübt werden?
- Inwieweit sind Gesellschaft und Staat bereit, für derartige Krisenfälle Kapazitäten zur Verfügung zu stellen – zum Beispiel für Beobachtung, Analyse, Bewertung und **Beschaffung**? Wie sind diese Aufgaben verteilt?
- Müssen **Zuständigkeiten** neu strukturiert und anders verteilt werden?
- Welche mittel- und langfristige **Finanzierung** ist für derartige Bedrohungslagen sicherzustellen?
- Welche personellen und psychischen Ressourcen müssen gebildet werden, um eine **effiziente Prävention** zu erreichen?
- Welche **Führungssysteme**, welche **Ausrüstung**, welche **Ausbildung**, welche **Übung**sszenarien und -verfahren sind notwendig?
- Welche Bedeutung haben **Kooperationsbereitschaft und -fähigkeit** der Akteure für eine effiziente Krisenbewältigung?
- Wie und mit welchen Ressourcen kann die **Bundeswehr** im Zuge der Amtshilfe eingeplant werden (ZMZ/CIMIC)? Wie kooperieren die Ressourcenträger – von der regionalen bis hin zur EU-Ebene?
- Kritische Infrastrukturen sind inzwischen überwiegend privatwirtschaftlich organisiert – sind die vielfältigen **Ressourcenträger** aller Sektoren miteinander vernetzt und ausreichend kooperationsfähig?
- Sind spezifische Ressourcenträger wie der öffentliche **Gesundheitsdienst** bestmöglich eingebunden? Ist die Ausstattung der Krankenhäuser bei einer großflächigen Krise wie einem Stromausfall oder einer Epidemie ausreichend? Ist sie einem massenhaften Anfall von Verletzten (MANV) gewachsen? Mit welchen Ressourcen lassen sich Kapazitätsengpässe beheben? Welche Lösungen können einen Überbedarf an stationären Kapazitäten ausgleichen?

6.3 LEITFRAGEN: KRITISCHE INFRASTRUKTUREN

- Ist das Konzept **„Kritische Infrastruktur"** angesichts neuer Bedrohungen ausreichend definiert? Sind alle Komponenten systematisch erfasst?
- Sind die **Wechselwirkungen** zwischen den Infrastrukturen genügend modelliert und anwendbar getestet?
- Reichen die vorhandene Sensorik sowie die heute verfügbare Kommunikationstechnik aus, um eventuelle **Angriffe auf Kritische Infrastrukturen** rechtzeitig erkennen und abwehren zu können?
- Sollen industrielle Betreiber von Kritischen Infrastrukturen **Mindeststandards** im Hinblick auf physikalische Bedrohungen einhalten und deren Umsetzung behördlicher Prüfung unterzogen werden?

6.4 LEITFRAGEN: BEVÖLKERUNG UND BEVÖLKERUNGSSCHUTZ

- Welche **vorbeugenden Schutzmaßnahmen und Fähigkeiten** sind bei großflächigen und lang anhaltenden Ereignissen zur Schadensbegrenzung erforderlich?
- Wie kann die **Selbsthilfefähigkeit der Bevölkerung** gestärkt werden? Kann ein Bewusstsein für die Wichtigkeit der Selbsthilfe geschaffen werden?
- Wie viel **Vorsorge** ist geboten und welche Risiken müssen der Bevölkerung als akzeptabel vermittelt werden?
- Existieren adäquate **Schutzmaßnahmen** und -ausrüstungen für die Bevölkerung im Falle einer großflächigen Gefahrenlage, insbesondere einer Epidemie, Pandemie oder radiologischen Bedrohung?
- Was muss getan werden, damit sich die Bevölkerung in einem Krisenfall **solidarisch und resilient** verhalten kann?
- Liegen empirische Erkenntnisse über **Risikoakzeptanz** und Resilienzpotenzial der Bevölkerung vor? Erlauben sie Aussagen über das erwartbare Verhalten bei großflächigen Gefahrenlagen wie einer Epidemie?
- Was muss getan werden, um das Verhalten der Bürger in entsprechenden Krisen **realistisch abschätzen** zu können?

6.5 LEITFRAGEN: RISIKO- UND KRISENKOMMUNIKATION

- Wie muss ein **Kommunikationskonzept** für den Krisenfall aussehen? Wie muss der Informations- und Datenaustausch organisiert werden?
- Welche Kommunikationsmöglichkeiten stehen zur Verfügung? Welche **Informations- und Kommunikationssysteme** sind aufzubauen?
- Wie kann die **Alarmierung** sichergestellt und mit Informationen über die Art der Gefahr verknüpft werden? Wie werden Information und Aufklärung der Bevölkerung sichergestellt?
- Wie können **Helfer koordiniert** und Ressourcen gebündelt werden – auch wenn die Kommunikationssysteme zusammengebrochen sind?
- Wie können **Medien** die Notwendigkeit von Prävention vermitteln?

6.6 LEITFRAGEN: INSTITUTIONELLE ERFORDERNISSE UND UMSETZUNG

- Gibt es national einen **Bedarf der Rechtsangleichung** bei Kooperation, Koordination, Lageerstellung und Lageverteilung? Ist dies auf europäischer und internationaler Ebene erforderlich?
- Sind die **föderalen Strukturen** in Deutschland für ein Risiko- und Krisenmanagement geeignet?
- Wie können in einem föderalen System wirksame und notwendige **Führungs- und Entscheidungsstrukturen** für überregionale Krisensituationen geschaffen werden?
- Wie können **Bund, Länder und Kommunen** die neuen Risiken für die Öffentliche Sicherheit in ihrem Zuständigkeitsbereich frühzeitig identifizieren, abschätzen und eventuell verhindern? Welche Strukturen müssten institutionalisiert werden?
- Wie kann ein **ganzheitliches, die Interdependenzen berücksichtigendes Risiko- und Krisenmanagement** für die beschriebenen Ereignisse etabliert werden? Welche Standards müssen erarbeitet und gesetzt werden? Welche Akteure im öffentlichen und nicht öffentlichen Bereich müssen zusammenarbeiten? Welche gesetzlichen Grundlagen und institutionellen Voraussetzungen sind zu schaffen? Welche Verantwortlichkeiten und Zuständigkeiten sind festzulegen? Bleibt das Subsidiaritätsprinzip der leitende Gedanke?
- Gibt es geeignete **übergreifende Einsatzplanungs- und Führungssysteme?** Ist eine ausreichende und übergreifende Führungsfähigkeit vorhanden?
- Wie müsste ein geeignetes **Frühwarnsystem** konzipiert sein?

07 GLOSSAR

Asymmetrische Kriege: Auseinandersetzungen mit schwerwiegenden, kriegsähnlichen Folgen zwischen qualitativ ungleichartigen Konfliktparteien/Akteuren (z. B. Terroristen vs. Staaten) mit zum Teil ungleichartigen Mitteln und/oder Methoden.

Bipolare Weltordnung: Die während des Kalten Krieges herrschende Bezeichnung für die beiden sich mit hoher militärischer Präsenz gegenüberstehenden Bündnissysteme NATO und Warschauer Pakt.

Bill-Tracking: (von engl. bill: „Geldnote" und tracking, „Auffinden, Verfolgen") Erstellung von Bewegungsprofilen definierter Geldnoten zu wissenschaftlichen Zwecken. Vor einigen Jahren wurde eine Anzahl von markierten Dollar-Noten in Umlauf gebracht. Wer eine markierte Geldnote bekommt, kann sich seither online registrieren, seinen momentanen Aufenthaltsort angeben und den Schein wieder in Umlauf bringen. Die Internetseite ist mittlerweile so populär, dass schon ca. 50 Millionen individuelle Geldscheine registriert sind.

Borreliose (auch: Lyme-Borreliose): Häufigste von Zecken übertragene Erkrankung in Deutschland, die durch das Bakterium Borrelia burgdorferi ausgelöst wird. Circa 240.000 Neu-Infektionen und ca. 60.000 Neu-Erkrankungen pro Jahr. Eine Impfung gibt es in Europa noch nicht. Die sog. Borrelien wandern nach der Infektion aus dem Blutkreislauf in das Gewebe und befallen dort auch Nervensystem und Gelenke. Das kann u. a. zu chronischen und neurologischen Erkrankungen wie Arthrose, Meningitis und Herzerkrankungen führen. Siehe auch: FSME.

BOS: Abkürzung für Behörden und Organisationen mit Sicherheitsaufgaben. Hierzu zählen vor allem die Bundespolizei, die Polizeien der Länder, der Zoll, die Bundesanstalt THW, die Feuerwehren, die Katastrophenschutzbehörden, die Zivil- und Katastrophenschutzorganisationen sowie Trägerorganisationen des Rettungsdienstes.

Bot-Netze/Bot-Netz-Attacke: (Kurzform für „Robot") Ein Programm, das ferngesteuert auf einem zuvor z. B. per Trojaner übernommenen PC arbeitet. Von Bot-Netzen spricht man, wenn derartige PCs zu Netzen zusammengeschlossen werden und per Fernsteuerung zeitgleich Aktionen wie das Verschicken von Spam oder das Ausführen von DDoS-Angriffen durchführen. Es wurden bereits Bot-Netze mit mehreren Hunderttausend Bots beobachtet.

CIMIC: siehe ZMZ.

Dengue-Fieber: (auch als Sieben-Tage-Fieber, Polka-Fieber oder Knochenbrecherfieber bekannt) Infektionskrankheit, die durch Stechmücken übertragen wird. Die Symptome sind oft unspezifisch oder einer schweren Grippe ähnlich, können aber auch innere Blutungen umfassen.

Denial-of-Service-Angriff/DoS-Angriff: Bei einem Denial-of-Service-Angriff wird ein IT-System von anderen Rechnern aus mit Netzwerkpaketen bombardiert. Ziel ist es, dieses zu blockieren und somit zu verhindern, dass reguläre Benutzer darauf zugreifen können. Das angegriffene IT-System kann die gewaltigen Paketmengen oft nicht verarbeiten und bricht überlastet zusammen. Starten mehrere Quellen gleichzeitig einen Angriff, spricht man von einem DDoS-Angriff (Distributed-Denial-of-Service-Angriff).

deNIS: Abkürzung für deutsches Notfallvorsorge- und Informationssystem. Das elektronische Informationssystem ist beim Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) in Bonn angesiedelt. Es fasst Informationen zum Bevölkerungsschutz zusammen, bereitet diese auf und stellt sie bestimmten Bedarfsträgern (z. B. Bundesbehörden, Länderbehörden, Hilfsorganisationen) zur Verfügung. Für interessierte Bürger und die Fachöffentlichkeit ist ein offenes Internetportal, deNIS I (siehe: www.denis.bund.de), vorhanden. Den Lagezentren der Bundesressorts und der Länderinnenministerien sowie den Zentralen der Hilfsorganisationen steht die geschlossene Plattform, deNIS II^{plus},

zur Verfügung. Hierbei handelt es sich vor allem um ein geografisches Informationssystem (GIS) zur Unterstützung des Krisenmanagements bei besonderen Gefahrenlagen.

Digitalfunk: Auf moderner digitaler Technik beruhender Rundfunk, Fernsehen und das im Aufbau begriffene digitale Sprech- und Datenfunknetz der BOS. Der Digitalfunk löst die veraltete analoge Technik ab und ist leistungsfähiger als diese.

DISMA: Ein Software-Tool, mit dem mögliche Gefahren frühzeitig erkannt und die Auswirkungen von Störfällen begrenzt werden können. DISMA ist modular aufgebaut und besteht im Wesentlichen aus den Komponenten Sachdaten (Erfassung, Übersichten, Recherchen), Gefahrenabschätzung, Karte (Lageführung und Verknüpfungen mit den Sachdaten) sowie Planung.

Dominoeffekt: Abfolge von Ereignissen, von denen jedes Einzelereignis zugleich Ursache für das nachfolgende Ereignis ist. Die Gesamtheit der Ereignisse ist auf ein und dasselbe Anfangsereignis zurückzuführen.

Dunkelfeld: Summe der Straftaten, die den Strafverfolgungsbehörden nicht bekannt geworden sind und deshalb auch nicht in der Polizeilichen Kriminalstatistik (PKS) erfasst werden konnten. Ein großes Dunkelfeld besteht u. a. bei allen Formen der Organisierten Kriminalität (z. B. Rauschgift, Wirtschaftskriminalität).

Epidemie: Ausbreitung einer bekannten oder neuen Infektionskrankheit in einer begrenzten Region (Stadt, Land, mehrere Länder) während einer begrenzten Zeitdauer, wenn die Fallzahlen für diese Erhebung über ein durch vorherige saisonale Zahlen „erwartetes" Maß an Fällen für diese Erkrankung hinausgehen. Bei neuen Infektionskrankheiten ist dieses erwartete Maß gleich „null", sodass auch sehr kleine Fallzahlen als Epidemie gewertet werden.

FSME: Abkürzung für Frühsommer-Meningoenzephalitis. Bekannteste und am besten erforschte durch Zecken übertragene Erkrankung, die durch das FSME-Virus ausgelöst wird. Die Erkrankung verläuft mit grippeähnlichen Symptomen und kann bei einem Teil der Patienten zu einer Entzündung von Gehirn und Hirnhäuten (Meningoenzephalitis) führen. Das Verbreitungsgebiet ist auf Süddeutschland begrenzt, „wandert" aber infolge der milden Winter immer weiter nach Norden. Eine Schutzimpfung ist für FSME-Endemiegebiete ratsam. Siehe auch: Borreliose.

GMLZ: Abkürzung für Gemeinsames Melde- und Lagezentrum von Bund und Ländern. Das GMLZ ist eine ständig erreichbare Einrichtung im Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) in Bonn. Seine Aufgaben umfassen (1) die ständige Lagebeobachtung, (2) die Beschaffung, Analyse, Verarbeitung, Koordinierung, Weitergabe und den Austausch von Meldungen und Informationen und (3) die Prognoseerstellung von Schadensentwicklungen im Ereignisfall (s. www.bbk.bund.de). Im Falle der Katastrophenhilfe soll es die für den Katastrophenschutz zuständigen Akteure der Länder mit länderübergreifenden Experten- und Ressourcenrecherchen unterstützen. Im Rahmen des EU-Gemeinschaftsverfahrens nimmt das Lagezentrum als Kontakt- und Vermittlungseinrichtung auch internationale Aufgaben wahr. Dem GMLZ sind Mitarbeiter des Bundes, der Länder und der Hilfsorganisationen zugeordnet.

Hanta-Viren: Durch Säugetiere übertragene Viren, die Lungenerkrankungen, akutes Nierenversagen oder schwere hämorrhagische Fiebererkrankungen verursachen. Hanta-Viren sind weltweit verbreitet. In Mitteleuropa sind beispielsweise einige Regionen in Niedersachsen, Hessen, Bayern und Baden-Württemberg sowie in Österreich Teile der Steiermark als Endemiegebiete bekannt.

Hellfeld: Umfasst die den Strafverfolgungsbehörden bekannt gewordenen und in der Polizeilichen Kriminalstatistik (PKS) dargestellten strafbaren Handlungen einschließlich der strafbaren Versuche.

Interdependenzen: Wechselwirkungen oder gegenseitige Beeinflussungen verschiedener Systeme, Systemteile oder Infrastrukturen aufgrund von gegenseitigen Abhängigkeiten untereinander.

Intimidation: Einschüchterung, Bedrohung.

Jahr-2000-Problem: Schwachstelle älterer Computersysteme, die zum Jahreswechsel 1999/2000 zu undefinierten Fehlerzuständen und Systemabstürzen mit unvorhersehbaren Folgewirkungen hätte führen können und in wenigen Fällen auch geführt hat. Grund war die Jahreszahl, die in jenen Systemen nur zweistellig dargestellt wurde. Dadurch war das Jahr „2000" gleichbedeutend mit dem Jahr „1900".

Kaskadeneffekt: Umschreibung für Abläufe von Stufenprozessen; sofern sich die Stufen verstärken bzw. aufschaukeln, wird von einem Lawineneffekt gesprochen. Bezogen auf schadenswirksame Prozesse, können diese sehr klein beginnen und sehr groß enden (siehe klassische Schneelawinen). Infrastruktursysteme können auf bestimmte Ereignisse in einer selbstverstärkenden Abfolge reagieren.

Kritische Infrastrukturen: Bezeichnung für Organisationen und Einrichtungen mit wichtiger Bedeutung für das Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden (Definition des Arbeitskreises KRITIS im Bundesministerium des Innern vom 17.11.2003).

LÜKEX: Abkürzung für Länderübergreifende Krisenmanagement-Exercise. LÜKEX ist eine im zweijährigen Rhythmus durchgeführte Stabsrahmenübungsserie von Bund und Ländern im Auftrag des Bundesministeriums des Innern zum Überprüfen und Beüben der Krisenmanagementfunktionen in Bundes- und Länderbehörden unter Einbeziehung kommunaler Ebenen und der Wirtschaft.

Metadatenströme: Datenströme, die sich auf primäre Datenflüsse zur eindeutigen Bestimmung, Kontrolle und Steuerung beziehen. Digitalisierte Daten benötigen Daten zur Dekodierung, aber auch Referenzdaten wie Zeiten, Ortsangaben, Sender und Empfänger. Jeder Eintrag in eine Datenbank braucht „identifizierende" (Schlagworte) und „auffindende" Metadaten. Je mehr Daten anfallen, desto wichtiger werden die Daten über die Daten und desto größer wird die Gefahr, die primären Daten nicht mehr „lesen" zu können, sobald ihre Metadaten beschädigt werden.

Pandemie: Ausbreitung einer bekannten oder neuen Infektionskrankheit während einer begrenzten Zeitdauer über ein durch vorherige saisonale Zahlen „erwartetes" Maß an Fällen für diese Erkrankung. Bei neuen Infektionskrankheiten ist dieses erwartete Maß gleich „null", sodass auch sehr kleine Fallzahlen als Pandemie gewertet werden. Der Unterschied zur Epidemie besteht im Umfang der Ausbreitung: Es sind Kontinente, ggf. die gesamte Erde betroffen.

Phishing: (Kunstwort aus engl. Password und Fishing) Betrügerische Aneignung und Missbrauch von Zugangsdaten für Online-Banking und andere Bezahlsysteme im Internet.

Redundanz: Das mehrfache Vorhandensein identischer Strukturen und Ressourcen zum Zweck der Erhöhung der Ausfallsicherheit eines Systems.

Repellenzien: Schutzmittel, die Stechmücken und andere Insekten am Landen auf der Haut hindern oder zum sofortigen Weiterfliegen zwingen. Wirksamkeit und Wirkdauer sind hohen Schwankungen unterworfen, je nach Umständen wie Schwitzen, Außentemperatur oder Präparat.

Resilienz: Bezeichnung für die Widerstandskraft von Organismen und Systemen (Mensch, technische Anlagen, Gesellschaft etc.). Resiliente Systeme verfügen über die Fähigkeit, sich geeignet, d.h. durch die Kombination von Wissen, Fertigkeiten und mobilisierbaren Ressourcen, vor extremen Belastungen, Widrigkeiten oder Schadwirkungen schützen und dadurch ihre Vitalfunktionen länger aufrechterhalten zu können.

Schattenwirtschaft: Sämtliche wirtschaftliche Aktivitäten innerhalb einer Volkswirtschaft, deren Wertschöpfung nicht in das Bruttoinlandsprodukt eingeht. Zumeist sind dies durch illegale Machenschaften erzielte wirtschaftliche Gewinne, die ohne Zahlung von Steuern und sonstige Abgaben in den legalen Wirtschaftskreislauf eingebracht werden und dadurch den Wettbewerb verzerren

und sich den Gemeinschaftsaufgaben einer Gesellschaft bzw. den Verpflichtungen gegenüber dem Staat entziehen. Beispiele hierfür sind Geldwäsche, Kapitalflucht, Schmuggel, transnationale Korruption, Organisierte Kriminalität, Proliferation von nuklearem Material, Drogenhandel und illegaler Diamanten- und Waffenhandel, ebenso unregulierte Umschlagplätze für Waren und Güter (Internet) sowie illegale Migrationsbewegungen (Menschenhandel).

Schmutzige Bombe: Eine mit konventionellem Sprengstoff bestückte Waffe, die bei der Explosion nukleares Material freisetzt und damit die Umgebung kontaminiert. Explosion und Kontamination sind wesentlich schwächer als bei einer Nuklearwaffe. Die Herstellung ist im Vergleich sehr viel einfacher.

Subsidiaritätsprinzip: (Nachrangigkeitsprinzip) Aus der katholischen Soziallehre stammendes Prinzip, das die Rangfolge der Zuständigkeiten für die Hilfeleistung in einem Gesellschaftssystem beschreibt. Danach soll die unterste Ebene (im Idealfall der einzelne Mensch) die notwendigen Maßnahmen leisten; erst wenn sie (er) dazu nicht in der Lage ist, übernimmt die jeweils nächsthöhere Ebene die Verantwortung. Diese Konzeption betrachtet die Verantwortlichkeit des Staates als nachrangig (subsidiär). Gleichzeitig gewährleistet sie, dass Entscheidung und Ausführung möglichst bürger- bzw. bedarfsnah getroffen werden. Der Katastrophen- und Bevölkerungsschutz in Deutschland orientiert sich an diesem Prinzip. Der subsidiäre Aufbau der Verantwortlichkeit im deutschen Hilfeleistungssystem reicht von der kommunalen Ebene bis hin zur Landesebene. Der Bund ist nur im Verteidigungsfall eingebunden. Das Gemeinschaftsverfahren der EU stützt sich wiederum generell auf dieses Prinzip.

Vektor: (lat. für „Träger") Bezeichnung für Überträger von Infektionserregern. Im Falle des beschriebenen Chikungunya-Fiebers sind dies Mücken aus der Gattung Aedes.

Vital/Vitalfunktion: Für belebte oder unbelebte Organismen und Systeme unabdingbar für ihre Funktionstüchtigkeit. Im Bevölkerungsschutz markiert die Frage nach vitalen Funktionen oder Zuständen den Punkt, ab dem Handlungsbedarf bzw. Schutzbedarf besteht. Zum Beispiel ist ein vitaler Wassermangel bezogen auf den Menschen „lebensbedrohlich", für die wasserkühlungsabhängige Anlage eines AKW ist er „funktionsbedrohlich".

ZMZ: Abkürzung für Zivil-militärische Zusammenarbeit (engl. Civil-Military Cooperation, CIMIC). Bezeichnet das Zusammenwirken von Streitkräften und zivilen Stellen. Nach dem Grundgesetz ist in der Bundesrepublik Deutschland die Bundeswehr subsidiär in die Gefahrenabwehr bei Naturkatastrophen und besonders schweren Unglücksfällen eingebunden.

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

IMPRESSUM:

Herausgeber:
Gerold Reichenbach,
Ralf Göbel,
Hartfrid Wolff,
Silke Stokar von Neuforn

Verlag:
ProPress Verlagsgesellschaft mbH,
Behörden Spiegel-Gruppe Berlin/Bonn

Redaktionelle Bearbeitung und Layout:
Pleon GmbH, Berlin

Druck:
Oktoberdruck GmbH, Berlin

Stand/Auflage:
September 2008, 1. Auflage/5.000

ISBN 978-3-934401-18-1

www.zukunftsforum-oeffentliche-sicherheit.de