Stefan Voßschmidt
Andreas Karsten (Hrsg.)

Resilienz und Kritische Infrastrukturen

Aufrechterhaltung von Versorgungsstrukturen im Krisenfall

Kohlhammer

Kohlhammer

Andreas H. Karsten
Stefan Voßschmidt (Hrsg.)

Resilienz und Kritische Infrastrukturen

Aufrechterhaltung von Versorgungstrukturen im Krisenfall

Verlag W. Kohlhammer

1. Auflage 2019

Umschlagbild: Daniel Friederichs
Gesamtherstellung: W. Kohlhammer GmbH, Stuttgart

Print:
ISBN 978-3-17-035433-3

E-Book-Formate:
pdf: ISBN 978-3-17-035435-7
epub: ISBN 978-3-17-035436-4
mobi: ISBN 978-3-17-035437-1

Inhaltsverzeichnis

A Grundlagen und Begriffe[1]

1 Einleitung

Stefan Voßschmidt & Andreas H. Karsten

Resilienz ist vielleicht das Schlagwort in den derzeitigen Diskussionen über Krisenmanagement. Allen Ortes liest man, dass Organisationen, Behörden, Unternehmen, Staaten, ja selbst die Staatengemeinschaft resilienter werden müssen, wenn sie die heutigen und vor allem die zukünftigen Herausforderungen meistern wollen.

Die beiden Herausgeber Stefan Voßschmidt, Referent im Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, und Andreas H. Karsten, Berater in der Controllit AG, glauben, dass es nur durch einen möglichst allumfassenden Ansatz möglich sein wird Krisen so zu beherrschen, dass die Folgen für die Menschen ein vertretbares Maß nicht überschreiten.

Dies spiegelt sich in diesem Buch wieder. Den Blick für das Ganze nicht verlierend, wenden die Herausgeber die Konzepte, die hinter dem Begriff Resilienz stecken, auf die Betreiber der Kritischen Infrastrukturen (Kritis) an. Die allgemeinen Betrachtungen werden besonders von den Expertinnen und Experten, die als Co-Autorinnen gewonnen werden konnten, an speziellen Beispielen detaillierter dargestellt, um die allgemeinen Prinzipien zu verdeutlichen.

Abschnitt A führt in das Thema ein. Es werden die Methodik des Buches erläutert und die wesentlichen Begriffe diskutiert. Abschließend werden die gesetzlichen Regelungen dargestellt.

Abschnitt B beschreibt die aktuelle Stresssituation der Kritis, also das Umfeld, in dem die Kritis-Betreiber tagtäglich agieren. Neben dem Klimawandel wird auf die politische, gesellschaftliche und wirtschaftliche Situation eingegangen.

1 Wegen der Knappheit des zur Verfügung stehenden Raumes und der aktuellen Thematik des Buchs wird davon Abstand genommen immer korrekt die weibliche und die männliche Form zu benutzen. Auch die Zwischenform »*Innen« erscheint nicht sachgerecht. Daher wählen die Verfasserinnen den Weg, die weibliche und die männliche Form schlicht abwechselt und möglichst gleich zu benutzen. Das bedeutet, reden wir von Verfasserinnen sind Verfasserinnen und Verfasser gemeint, schreiben wir Autoren, meinen wir Autorinnen und Autoren. Beides gleichberechtigt, gleichwertig und vom Bestreben her gleich oft.

Abschnitt C beschäftigt sich mit Möglichkeiten, die Resilienz zu steigern. Detaillierter werden die Notwendigkeit und die Möglichkeiten der Partizipation der Zivilgesellschaft und die Möglichkeiten und Herausforderungen moderner Technologie betrachtet. Abschließend wird die Notwendigkeit von Ausbildung und Training thematisiert.

Abschnitt D beschäftigt sich mittels szenariobasierter Diskussionen näher mit einigen Schockereignissen. Neben wetterbedingten Schocks (hier besonders die Auswirkungen eines Wintersturms auf Kommunen und Polizeien) werden die Themen Pandemie, CBRN, Terrorismus, Cyber und Stromausfall betrachtet.

Im abschließenden **Abschnitt E** werden die Ideen aus den ersten Kapiteln zu einer Road Map zur Steigerung der Resilienz zusammengefasst.

Im Management von Gefahren sind Vulnerabilität und Resilienz zentrale Begriffe. Das Management hat die Aufgabe zu analysieren, ob die Auswirkungen bestimmter Prozesse (z. B. einer Überschwemmung) erhebliche Schäden verursachen und wie die Bewältigungskapazitäten verbessert werden können, um derartige negative Auswirkungen zu vermeiden oder zu reduzieren. Vulnerabilität ist hierbei ein wichtiger Bestandteil der Risikoanalyse, bringt die Schadensanfälligkeit der Gesellschaft zum Ausdruck und verdeutlicht das Verhältnis zwischen äußerer Bedrohung und interner Bewältigungsmechanismen. Vulnerabilität und Resilienz sind im Gefahrenmanagement allerdings nicht als Gegensatzpaar zu verstehen. Sie ergänzen sich durch ihre unterschiedlichen Schwerpunkte vielmehr komplementär. Es sind unterschiedliche Blickwinkel unter denen die Gefahren betrachtet werden. Sie finden sich z. B. auch im Sendai Framework der Vereinten Nationen (Fuchs 2016, 50 f., Zimmermann/Keiler 2015, 195–202). Wir betonen den Blickwinkel der Resilienz.

Im kollektiven Bewusstsein in Deutschland sind vor allem der Stromausfall und Schneechaos im Münsterland November 2005 und das Schneechaos in Schleswig-Holstein und Norddeutschland im Winter 1978/79 geblieben. Mangelnde Vorbereitung, i. B. fehlende Vorräte und fehlende Netzersatzanlagen waren hier die Hauptdefizite. Wie im Kapitel B. *Betrachtungen zur aktuellen Stresssituation der Kritischen Infrastrukturen* dargestellt, ist nicht davon auszugehen, dass die Bevölkerung in unserem Szenario 2019 besser vorbereitet wäre. Denn Risiken werden gesellschaftlich konstruiert. Schon eine tatsächliche Risikowahrnehmung, verstanden als subjektiv konstruierte Wahrnehmung der Bedeutung und potenziellen Auswirkung der Risiken vor dem Hintergrund kultureller Muster und Sozialisation (Dickmann u. a. 2007, 324, Zwick und Renn 2008, 77, Drews 2018, 31ff) findet nicht statt. Sie wird weder durch die Gesellschaft noch durch die Politik oder die Medien gefördert. Damit

findet aber auch keine Diskussion um Verantwortung, z. B. die Selbstverantwortung bei Risiken statt. Auch Folgerisiken und Kaskaden sind keine Themen.

Es ist zu hoffen, dass dieses Buch einen Beitrag zur entsprechenden Bewusstseinserweiterung leistet.

1.1 Hinführung zum Thema

Stefan Voßschmidt

Schon vor mehr als 2000 Jahren formulierte Perikles »Es kommt nicht darauf an, die Zukunft vorauszusagen, sondern darauf, auf die Zukunft vorbereitet zu sein.« Was passiert bei einem langandauernden Stromausfall z. B. mit der Wasserversorgung, dem Lebensmitteleinzelhandel, der staatlichen Infrastruktur insgesamt? Welche Folgen können ein heftiger Sturm, eine langandauernde Hitzeperiode und eine Dürre haben? Westeuropa hat eine Hitzeperiode mit geringen Niederschlägen in den Jahren 2018 und 2019 zum dritten Mal in den zwei Jahrzehnten des dritten Jahrtausends (nach 2003) erlebt. Der Klimawandel zeigt sich anhand vieler Indikatoren und bedeutet in der Tendenz eine Erwärmung der Atmosphäre und eine Steigerung von Naturgefahrenrisiken. Kaskadeneffekte können diese Risiken potenzieren, wie Marc Elsberg in seinem Roman Blackout anhand eines durch einen terroristischen Angriff herbeigeführten Blackouts anschaulich beschreibt. Sind wir auf unsere Zukunft vorbereitet wie Perikles, der große Staatsmann der Athener es fordert? Vielleicht war er glänzend auf den großen Krieg, den Athen (und er) gegen Sparta führte, vorbereitet. Verloren hat ihn seine Heimatstadt dennoch und mit ihm die Großmachtstellung. Die Seuchengefahr, die von den vielen in die Stadt geflohenen Menschen ausging, wurde nicht erkannt und somit auch keine Präventionsmaßnahmen ergriffen. Schon dieses Beispiel lehrt, dass in der Vorbereitung die zentralen Knotenpunkte der Gesellschaft, die Kritischen Infrastrukturen, von elementarer Bedeutung sind (bei Perikles und Athen war es die Gesundheitsvorsorge, vielleicht auch die Hybris der sich überlegen Fühlenden). Es gibt Risiken, die Gesellschaften nicht vorhersehen. Darüber hinaus zeigt es aber auch, dass es nicht nur um Vorbereitung gehen kann, sondern dass mehr notwendig ist, um das adäquate Überleben einer modernen Gesellschaft in der von ihr gewünschten Weise zu gewährleisten: Resilienz.

Diese Resilienz ist umso notwendiger, als die aktuell geschehenden Veränderungsprozesse – Globalisierung, Vernetzung, Digitalisierung – moderne Gesellschaf-

ten verwundbarer machen. Diese Vulnerabilität steigert das Risikoparadoxon: »Je weniger eine Gesellschaft ein Risiko erlebt, desto schlechter ist sie darauf vorbereitet.« Die Gesellschaft Deutschlands im 21. Jahrhundert geht von Stromausfallzeiten von unter 15 Minuten pro Jahr (Wikipedia: Stromausfall) aus und ist gerade deshalb auf das Risiko eines längeren Stromausfalls nicht vorbereitet. Wer weiß, wo Streichhölzer, Kerzen, Taschenlampe sind? Wer findet sie im Dunkeln schnell?

Es haben sich zwei Ansätze etabliert, um Gefahren für eine Gesellschaft zu verringern: Der Ansatz der Reduzierung der Risiken bzw. der Vulnerabilität und der Ansatz der Steigerung der Resilienz der Gesellschaft. Wir folgen letzterem.

Wie können nun die Infrastrukturen gegen Totalausfälle geschützt werden, insbesondere die Lebensadern moderner Gesellschaften, die Kritischen, also lebensnotwendigen Infrastrukturen? Wie können moderne Gesellschaften ihre Verletzlichkeit, ihre Vulnerabilität, verringern? Die Antwort heißt Resilienz. Die Steigerung der Resilienz ist die Methode, mittels derer moderne Gesellschaften diesen Risiken begegnen. Denn in der freiheitlichen Wirtschafts- und Rechtsordnung der westlichen Welt des 21. Jahrhunderts ist es nicht sachgerecht, dass der Staat Lösungen allein mittels rechtlicher Regelungen anstrebt, das Mittel der Wahl sind Recht und Konsens. In Deutschland z. B. hat der Staat aufgrund seiner Verfassung die Verpflichtung zur Daseinsvorsorge, nach Art. 1 Abs. 1 (Menschenwürde), Art. 2. Abs. 2 (Recht auf Leben und körperliche Unversehrtheit), Art. 20 Abs. 1 (Sozialstaatsprinzip) des Grundgesetzes. Diese staatliche Verpflichtung ist rechtlich ausgeprägt durch eine umfassende Gesetzgebung bei gleichzeitiger Tendenz einer möglichst weitgehenden Liberalisierung, deren Höhepunkt in den 90er Jahren des vorigen Jahrhunderts mit der Formel »Privat vor Staat« zusammengefasst wurde. Der Staat zog sich von vielen Aufgaben zurück und schränkte Monopole ein. So bedeutet die Liberalisierung des Strommarktes z. B, dass die vier großen Übertragungsnetzbetreiber ihr Netz (ihre Leitungen) jedem Stromanbieter zur Verfügung stellen müssen, jeder Interessierte diskriminierungsfrei zu versorgen ist und gewünschte Erhöhungen der Netzentgelte von der Bundesnetzagentur genehmigt werden müssen. Moderne Wirtschaftskreisläufe sind derartig auf Effizienz und Effektivität ausgerichtet (Just-in-time Produktion), dass nicht notwendige Regelungen und Auflagen potentiell zu Kostensteigerungen führen, die im Hinblick auf den durch die Globalisierung forcierten Wettbewerb und Kostendruck vermieden werden sollen. Auch Investitionen in die Sicherheit werden unter Wirtschaftlichkeitsgesichtspunkten getätigt – oder eben nicht getätigt. Dies gilt auch für die Kritischen Infrastrukturen und ihre Betreiber.

Kritische Infrastrukturen sind Einrichtungen, Anlagen oder Teile davon, die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind. Durch ihren Ausfall oder ihre Beeinträchtigung würden erhebliche Versorgungsengpässe oder Gefähr-

dungen für die öffentliche Sicherheit eintreten. Kritische Infrastrukturen sind die unverzichtbaren Lebensadern moderner, leistungsfähiger Gesellschaften. Die Gewährleistung des Schutzes dieser Infrastrukturen ist eine Kernaufgabe staatlicher und unternehmerischer Sicherheitsvorsorge und zentrales Thema der Sicherheitspolitik Deutschlands. Diese Aufgabe übernimmt der deutsche Staat in Form eines institutionalisierten Dialogs zwischen Staat und Wirtschaft im UP KRITIS (Umsetzungsplan Kritis/Kritische Infrastrukturen). Es hat sich bewährt, die Betreiber Kritischer Infrastrukturen – nur falls erforderlich – durch gesetzliche Vorgaben dazu zu bringen, Widerstandsfähigkeit und Schutzmaßnahmen zu verbessern. Grundsätzlich wird jedoch auf Kooperation gesetzt. Die erneuerte Kritis-Strategie baut auf dieser Erfahrung auf. Gemeinsam mit allen Beteiligten soll ein Mehr an Schutzmaßnahmen und ein deutliches Plus an Sicherheit für uns alle (auch über Grenzen hinweg) erreicht werden. Rechtliche Regelungen sind nur an zentralen Stellen notwendig und erfolgt. Die wichtigste Regelung ist das IT Sicherheitsgesetz von 2015. Eine weitere Konkretisierung erfolgte in der Cyber-Sicherheitsstrategie für Deutschland 2016 und der Kritis-Verordnung.

INFO

Info:

Resilienz bezeichnet in diesem Zusammenhang die besondere Fähigkeit eines Systems, Ereignissen zu widerstehen beziehungsweise sich daran anzupassen und dabei seine Funktionsfähigkeit zu erhalten oder schnell wiederzuerlangen (BMI 2018).

Es stellt sich nun die Frage, wie die Bevölkerung bei Ausfällen Kritischer Infrastrukturen, insbesondere in Verbindung mit einem Stromausfall, ausreichend versorgt werden kann: Wie resilient ist die jeweilige Versorgungsinfrastruktur und welche Notfallmechanismen können in welcher Form wirken? Kann die Bevölkerung sich ausreichend selbst versorgen?

Bei der Beantwortung dieser Frage sind folgende Rahmendaten zu beachten. Modernes Leben und Wirtschaften beruht maßgeblich auf einer funktionierenden Infrastruktur. Alles ist verfügbar, wird »just in time« geliefert und produziert. Die Lagerhaltung findet auf den Straßen statt. Die Infrastruktur ist in den letzten Jahren und auch in naher Zukunft einem gravierenden Wandel unterworfen, beziehungsweise wird es sein. Von ursprünglich »analoger Hardware« verändert sie sich durch den Einsatz von Informations- und Kommunikationstechnik (IKT) zu digital unterstützten Systemen. Digitalisierung wird somit zu einem zentralen Treiber der Veränderung der Infrastrukturen und ermöglicht gleichzeitig auch eine stärkere Kopplung dieser. Diese Kopplung ist vor allem aus Sicht des Energiesystems vorteilhaft, da

auf diese Weise Nutzenergie- und Energiespeicherpotenziale infrastrukturübergreifend gehoben werden können. Durch die zunehmende Digitalisierung aller Infrastrukturen werden diese jedoch auch deutlich komplexer und damit verwundbarer gegenüber potenziellen Ausfällen. Dies potenziert das Gefährdungspotenzial und unterstreicht die Notwendigkeit, einen lang anhaltenden, großflächigen Blackout zwingend zu verhindern. Die hohe Verwundbarkeit wird unter anderem durch die große Bandbreite und Vielzahl von Hackerangriffen auf Kritische Infrastrukturen, darunter viele Unternehmen und Anlagen im Energiebereich, deutlich. Die Vulnerabilität beschreibt dabei die Anfälligkeit des Systems und seiner Dienstleistung in Bezug auf konkrete interne und externe Störungen beziehungsweise auf strukturell bedingte Schwachstellen im System (Gleich u. a. 2010).

Als Digitalisierung oder digitale Revolution wird die tiefgreifende Veränderung von Wirtschaft und Gesellschaft durch digitale Technologien bezeichnet. Grundlage der Digitalisierung ist das Übertragen analoger Informationen auf digitalen Speichermedien, wodurch sie elektronisch verarbeitet werden können. Die Digitalisierung erfasst dabei alle Gesellschaftsbereiche von Wirtschaft über Politik und Bildung bis zur staatlichen Verwaltung und sozialen Interaktion. Treiber der Entwicklung ist die Vernetzung von Menschen und Geräten untereinander über das Internet. Dadurch entstehen neue Geschäftsmodelle und es verändern sich alte, andere verschwinden auch ganz. Insbesondere große Plattformen sind bisher als Sieger der Digitalisierung hervorgegangen – daher spricht man auch von der Plattform-Ökonomie oder GAFA-Ökonomie. GAFA steht für die vier prestigeträchtigsten Konzerne der Welt Google, Amazon, Facebook und Apple. Microsoft komplettiert diese zu den »big five«.

Relevant sind aber auch andere Rahmenbedingungen. Geglaubt wird heute, was ins Weltbild passt. Obwohl die Gefahr Opfer eines terroristischen Anschlags zu werden seit Jahren sinkt, steigt die Angst davor. Eine zentrale Frage, an der sich die deutsche Gesellschaft scheidet, lautet: Wie bewertet man die Entwicklungen der vergangenen Jahre (Flüchtlingskrise)? Dies erinnert an »Die Grenzen des Wachstums« vom Club of Rome aus den 70er Jahren. Eine der Kernaussagen war, dass es bei Nutzung aller Bodenressourcen ab dem Jahre 2000 nicht mehr möglich sein wird, so viel Nahrung zu erzeugen, dass alle Menschen satt werden können. »Neben dieser Linie hatten die Wissenschaftler die Kurve der absoluten Hoffnungslosigkeit eingezeichnet. Sie zeigte den Verlauf des Problems, falls es gelänge die Produktivität pro Quadratmeter Nutzfläche zu verdoppeln. In diesem als unwahrscheinlich eingestuften Fall käme das wirklich definitive Ende ungefähr im Jahre 2020«, (Wüllenweber, 2018, Zenthöfer 2018).

Diese Prognosen bewahrheiteten sich nicht. Die Fortschritte in der Nahrungsmittelproduktion konnten auch die »optimistischen« Prognosen bislang immer übertreffen. Die Horrorszenarien realisierten sich nicht. Aber: Apokalypse-Erwartung und Pessimismus wurden zur Grundhaltung gerade des vermeintlich aufgeklärten Teils der Menschheit. Dabei ist z. B. die Armut weltweit zurückgegangen. Weltweit waren 2015 erstmals weniger als 10 % der Menschen absolut arm. 300.000 Jahre lang lebten 90 % unserer Vorfahren am Existenzminimum. Die Sorge um das tägliche Brot regierte. Die Französische Revolution beispielsweise ist auch als Hungerrevolte zu erklären. Wüllenweber (2018) fasst zusammen: »Die tödlichsten Krankheiten besiegt. Das Waldsterben abgewendet. Gewalt, Kriminalität, Analphabetismus, Armut und Hunger entscheidend zurückgedrängt. Die Mauer eingerissen und die Wiedervereinigung ohne Blutvergießen errungen. Hunderttausende Flüchtlinge aufgenommen.« Trotzdem denken ¾ der Deutschen, die Mordrate sei seit dem Jahre 2000 gestiegen, dabei ist sie um 33 % gesunken (Wüllenweber, 2018). Angst ist die Ware der Amateur-Publizisten, die düstere Verlässlichkeit gibt Halt. Deutsche haben eine geringe Unsicherheitstoleranz. Das zeigt sich auch daran, dass keine der weltweit größten Banken in Deutschland beheimatet ist (Bank bedeutet Wagnis), aber dafür die größte Versicherung (Allianz) und die größte Rückversicherung (Munich Re). Möglicherweise ist Angst oder »German angst« ein besonders unterschätzter Risikofaktor. Der Philosoph Erich Fromm ist der Ansicht, der Mensch sei zu fast allem bereit, um sich von Ängsten zu befreien (Fromm 2011, S. 221 f.).

1.2 Überblick über die Rechtsnormen

Stefan Voßschmidt

Neben Seuchen sind die größten zivilen Risiken für die modernen Gesellschaften des 21. Jahrhunderts der Stromausfall und der Ausfall der IT-Technik.

Aber vor allem einige Ereignisse haben die weltpolitische Lage im Besonderen geprägt und zu Umsetzungsprozessen in Rechtsnormen geführt: Der Kalte Krieg mit Berlin-Krise, Korea-Krieg und seinem Höhepunkt der Kuba-Krise. Sie führte in Deutschland ab dem Jahre 1965 zum Erlass der Sicherstellungsgesetze (für die als zentral angesehenen Felder Ernährung, Wasser, Wirtschaft, Verkehr, Arbeit, Post- und Telekommunikation). Zweck war die Sicherstellung der Versorgung der Zivilbevölkerung und der Streitkräfte im Verteidigungsfall.

1986 kam es zum Reaktorunglück von Tschernobyl. Tschernobyl ist zum Symbol für vieles geworden (Hybris zum Beispiel). Es ist aber auch ein Beispiel nicht nur für den GAU

(= größten anzunehmenden Unfall), sondern für den Super-Gau, für etwas, was zuvor undenkbar schien. Der Unfall wurde zum Synonym der von Ulrich Beck definierten Risikogesellschaft. In Deutschland wurde anschließend Regelungsbedarf für Versorgungsprobleme in Friedenszeiten bedingt durch zivile Gefährdungslagen gesehen und die Vorsorgegesetze wurden erarbeitet (vgl. zur Systematik und allgemein Voßschmidt 2018, S. 107ff). Erst im zweiten Jahrzehnt des 21. Jahrhunderts rückte die IT-Technik in den Fokus und mit ihr die Kritis-Betreiber. Die regelnde Vorschrift, »Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme« (IT-Sicherheitsgesetz), ist am 25. Juli 2015 als Artikelgesetz[2] in Kraft getreten. Als Kernbestandteil sehen die neu eingefügten §§ 8 a und 8 b des BSI-Gesetzes vor, dass informationstechnische Systeme, die für die Funktionsfähigkeit von Kritischen Infrastrukturen maßgeblich sind, von den jeweiligen Betreibern durch die Umsetzung von Mindestsicherheitsstandards abzusichern und erhebliche IT-Vorfälle an das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu melden sind. Spiegelbildlich zu den besonderen Pflichten ergeben sich aus den §§ 3 Absatz 3 und 8 b Absatz 2 Nummer 4 des BSI-Gesetzes für Betreiber Kritischer Infrastrukturen besondere Rechte. Diese beinhalten insbesondere die privilegierte Beratung und Information durch das BSI.

Bislang oblag die Bewertung, ob Infrastrukturen für die Versorgung der Allgemeinheit mit wichtigen Dienstleistungen als kritisch anzusehen sind, der Einschätzung des jeweiligen Betreibers. Im Rahmen des UP KRITIS, einer öffentlich-privaten Partnerschaft von Betreibern und dem Bund, wurden in der Vergangenheit Konzepte und Handlungsempfehlungen erarbeitet, um den Schutz der Informationstechnik in Kritischen Infrastrukturen zu verbessern und in den einzelnen Sektoren ein einheitlich hohes IT-Sicherheitsniveau zu erreichen. Dieses System der Selbstregulierung hat zwar zu einer spürbaren Erhöhung des Sicherheitsniveaus geführt. Ausgehend von den in der Praxis erzielten Erfahrungswerten ist jedoch nicht hinreichend sichergestellt, dass sich in den einzelnen Sektoren ein gleichwertiges und hinreichendes Schutzniveau für die eingesetzte Informationstechnik herausbilden kann. Darauf zielen das IT-Sicherheitsgesetz und diese Verordnung durch die Identifizierung Kritischer Infrastrukturen ab. Die Kritis-Betreiber sind zur Umsetzung von Mindestsicherheitsstandards und Meldepflichten verpflichtet. Mit der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV) wird die Vorgabe in § 10 Absatz 1 Satz 1 des BSI-Gesetzes umgesetzt, wonach die Bewertung einer Infrastruktur als kritisch nach einer vorgegebenen Methodik zu erfolgen hat. Die Methodik beruht auf drei aufeinander aufbauenden

2 Gesetz, das mehrere Gesetze ändert

Verfahrensschritten, die jeweils unter umfassender Beteiligung von Experten und Vertretern der betroffenen Ressorts sowie der einzelnen Branchen in den Arbeitskreisen des UP KRITIS und weiteren Kreisen umgesetzt wurden. Die Beteiligung der betroffenen Branchen bereits im Vorfeld des formalen Anhörungsverfahrens folgt dem kooperativen Ansatz des IT-Sicherheitsgesetzes und hat sich aufgrund der Komplexität der zu treffenden Festlegungen als zweckmäßig bewährt.

In einem ersten Schritt wird für die Sektoren Energie, Wasser, Informationstechnik und Telekommunikation sowie Ernährung bestimmt, welche Dienstleistungen aufgrund ihrer Bedeutung als kritisch anzusehen sind. Hierbei orientiert sich die Festlegung der kritischen Dienstleistungen an den in der Gesetzesbegründung benannten Dienstleistungen sowie an den Ergebnissen von Studien, die das BSI beauftragt hatte, um eine umfassende Analyse der Kritis-Sektoren und der darin erbrachten kritischen Dienstleistungen in Deutschland zu erlangen. Weitere Schritte werden folgen. Gleichzeitig wird in vielen Feldern der Ruf nach dem Gesetzgeber laut. Alles und jedes soll geregelt werden, teilweise wird sogar ein Spontanhelfergesetz in Erwägung gezogen. Doch weiß noch jemand welche Normen bei Kritischen Infrastrukturen einschlägig sind? Es gibt zum Beispiel unendlich viele DIN-Normen zum Krisenmanagement, die nicht nur keiner anwendet, die vielleicht nicht praktikabel sind, die aber vor allem niemand überhaupt kennt (Voßschmidt 2020). Deshalb glauben wir dem französischen Philosophen Montesquieu: Wo ein Gesetz nicht notwendig ist, ist kein Gesetz notwendig.

2 Methodik des Buches

Stefan Voßschmidt

Die Methodik dieses Buches ist eigen. Wir wollen praxisrelevant sein, das Thema in der gebotenen Kürze (Praktiker haben wenig Zeit, wir haben uns ein Limit gesetzt) nachvollziehbar und lösungsorientiert behandeln und dies auf möglichst knapper wissenschaftlicher Grundlage. Wir wollen kein Handbuch schreiben mit einem den Stand der Wissenschaft wiedergebenden Literaturverzeichnis, sind daher bewusst und notwendigerweise halbwissenschaftlich. Die Verweise sind teilweise bewusst kurz, auf das Wesentliche begrenzt, teilweise aber auch umfangreich, um bestimmte Gedankengänge nachprüfbar zu machen. Es erfolgt zumeist die Konzentration auf neuere, wichtigere Literatur. So sehr sich die Autoren um Objektivität bemühen, jeder Auswahl, jeder Schwerpunktsetzung haften subjektive Momente an. Um sie nachvollziehbar zu machen, stellen die Autoren sich am Ende des Buches kurz vor.

Die benutzten Begrifflichkeiten werden weit ausgelegt. Wir wählen einen globalen Ansatz bei einer gesamtgesellschaftlichen Betrachtungsweise. Daher kann es keine Beschränkung auf nationale z. B. deutsche Definitionen geben. Bei Großkatastrophen ist nur das abgestimmte und angepasste Handeln effektiv. Hochwasser, Trockenheit oder Radioaktivität machen nicht an Landesgrenzen halt. Begriffe sind Hilfsmittel, nützlich zur Verständigung und zum Klären der Lage, dasselbe gilt für Aufbaustrukturen und bewährte Krisenbewältigungsmechanismen. Deshalb wird in diesem Buch im Bereich von Kritischen Infrastrukturen und Resilienz jeglicher Dogmatismus abgelehnt. Im Krisenmanagement und bei seiner Vorbereitung darf nichts Selbstzweck sein.

Unser Begriff der Kritischen Infrastrukturen ist umfassender als der gemeinhin übliche, umfasst auch die lebensnotwendigen Infrastrukturen des ZSKG (Gesetz über den Zivilschutz und die Katastrophenhilfe des Bundes vom 25. März 1997, § 1 Abs. 1 »lebens- oder verteidigungswichtige zivile Dienststellen, Betriebe, Einrichtungen und Anlagen sowie das Kulturgut«) und geht soweit, dass auch die unbekannten Lagen, die so genannten »Schwarzen Schwäne« (Taleb) mit umfasst werden. Mit dem Unbekannten muss gerechnet werden, Vorbereitung tut Not und soweit sie überhaupt möglich ist, bedarf sie weitestgehender Flexibilität. Warum? Dies »Warum« ist am leichtesten mit einer Gegenfrage zu beantworten: Wer hat wirklich vor dem 25. April 1986 mit Tschernobyl gerechnet, wer erwartete den 11. September 2001 und wer »hatte auf dem Schirm«, dass russische Soldaten in ihrer Freizeit und freiwillig die wenigen Separatisten der Krim gegen den Staat Ukraine unterstützen und bei dieser offiziell nicht angeordneten Unterstützung, ihre Waffen, ihre Ausrüstung, ihre Panzer mitnehmen? Dabei ist unerheblich, ob es sich nach der Rumsfeld Unterscheidung (2018) um ein known unknown (etwas, was man nicht wusste, aber hätte wissen können) oder um ein »unknown unknown« (etwas gänzlich unbekanntes, nie Dagewesenes) handelt.

Krisenmanagement bedeutet: Bewältigen einer Lage. Vorbereitungen auf derartige Lagen bzw. Gefahren oder Übungen gehen immer von einem Sachverhalt einer Lage aus. Auch die Kommunikation im Vorfeld (Risikokommunikation) oder während eines Ereignisses (Krisenkommunikation) ist keine reine Theorie, sondern es wird ein konkreter Fall durchgespielt. Dieses bewährte und praxisgerechte Vorgehen legen wir daher auch diesem Buch zugrunde. Ausgangspunkt sind nicht theoretische Überlegungen, sondern ein konkretes zeitgenau beschriebenes, sich entwickelndes Szenario. Ziel ist eine szenariobasierte Diskussion, um anhand eines Beispielszenarios (hier Wintersturm) mögliche Folgen zu erarbeiten. So werden abstrakte Ideen und Ansatzpunkte verdeutlicht. Im Laufe des Buches werden wir immer wieder auf dieses

Szenario zurückgekommen, das sich über Tage entwickelt. Wir haben ein Sturmszenario gewählt, weil derartige Szenarien weltweit häufig vorkommen und durch Klimawandel und Erderwärmung an Häufigkeit und Intensität zunehmen werden.

Jede Autorin verantwortet ihr Kapitel selbst. Die Herausgeber achten auf den roten Faden und ein gewisses Maß an Einheitlichkeit, z. B. einheitliche Benutzung der Begriffe. Bei vielen Begriffen werden die Standarddefinitionen benutzt. Unser Ziel ist Praxisrelevanz, nicht möglichst weitgehende Originalität.

Wenn auch ein Schwerpunkt auf die professionellen und ehrenamtlichen Mitarbeiterinnen der Organisationen im Bevölkerungsschutz gelegt wird, sind von ebenso großer Bedeutung die eher versteckten Helferinnen, die keiner Organisation angehören, die aber bei unterschiedlichsten Lagen ebenso unverzichtbare Hilfe leisten.

3 Begriffsbestimmungen

Stefan Voßschmidt & Andreas H. Karsten

Wie oben bereits beschrieben glauben die beiden Herausgeber, dass es notwendig ist, einen allumfassenden Ansatz zu wählen, wenn man im Krisenfall das Leben der betroffenen Menschen nicht mehr als notwendig einschränken möchte. Deshalb teilen sie nicht die Auffassung, dass bestimmte Bereiche isoliert betrachtet werden können. Den betroffenen Menschen ist es gleichgültig, ob eine ausgefallene Infrastruktur per Definition kritisch und damit besonders schützenswert ist, oder sie als nicht kritisch und deshalb weniger schützenswert erscheint. In den letzten Jahren hat sich für einige dieser Infrastrukturen das Wort »systemrelevant« eingebürgert.

Deshalb werden in diesem Buch die Begriffe »Kritische Infrastruktur«, »Stresssituation« und »Schockereignis«, »Resilienz« und »Kritikalität« weder streng wissenschaftlich noch streng juristisch/verwaltungssprachlich ausgelegt. Vielmehr werden Aspekte aus unterschiedlichen Bereichen und verschiedenen Ländern aufgezeigt. Auch werden die Begriffe unter Umständen etwas unscharf verwendet. Dafür bitten wir bei allen Wissenschaftlerinnen und Linguisten um Verständnis. Unser Ziel ist es nicht, ein wissenschaftliches Werk zu veröffentlichen, sondern allen denen eine Hilfestellung zu geben, die sich Tag für Tag in ihren Organisationen, Unternehmen, Behörden bemühen, resilienter zu werden, um in Krisenfällen das Leben der betroffenen Menschen so gut es geht zu erleichtern.

3.1 Kritische Infrastruktur

Stefan Voßschmidt & Andreas H. Karsten

Im ersten Teil des Kapitels beschreibt Voßschmidt die Situation in Deutschland. Ausgehend von den Definitionen in den Veröffentlichungen des Bundesministeriums des Inneren, des Bundesamtes für Bevölkerungsschutz und des Bundesamtes für Sicherheit in der Informationstechnologie betrachtet er auch den derzeitigen Stand der wissenschaftlichen Diskussion zum Thema Kritische Infrastrukturen.

Im zweiten Teil schaut Karsten über den deutschen Tellerrand hinaus auf ausgewählte Staaten und vergleicht diese mit den deutschen amtlichen Definitionen. Die Einteilung der Infrastrukturen in unterschiedlichen Sektoren verdeutlicht, dass die Festlegung einer Infrastruktur als »kritisch« auch politisch motiviert ist.

3.1.1 Situation in Deutschland

Stefan Voßschmidt

Ziel

Aufgrund der Vernetzung der kritischen Infrastrukturen sowohl über Sektor- wie auch über Ländergrenzen hinweg, bestehen starke, nichtlineare gegenseitige Abhängigkeiten voneinander. Dies kann dazu führen, dass sich eine Stresssituation oder ein Schockereignis bei einem Betreiber der Kritischen Infrastruktur kaskadenartig auf mehrere Betreiber ausbreitet und unter Umständen die Lebens- bzw. Wohlstandsgrundlage der deutschen Bevölkerung gefährdet. Ausgehend von einer erhöhten Stresssituation aufgrund einer winterlichen Wetterlage und dem Schockereignis eines Wintersturmes, werden die Folgen für die 9 Kritis-Sektoren und einige ausgewählte Bereiche des öffentlichen Lebens aufgezeigt, wenn es den Betreibern der Kritischen Infrastrukturen und der staatlichen Gefahrenabwehrbehörden nicht gelingt, die kaskadierenden Ereignisketten zu unterbrechen und möglichst schnell wieder zum Ausgangszustand zurück zu gelangen. Das heißt, wenn die Betreiber, die Menschen in Deutschland und die staatlichen Organe nicht resilient gegenüber der Stresssituation und dem Schockereignis sind. Hier werden noch einige weitere Bedrohungen für die deutschen Betreiber der kritischen Infrastrukturen diskutiert. Zum Anschluss der Szenario-basierten Diskussion werden allgemeine Schritte für die Stärkung der Resilienz und eine agile, resiliente Gefahrenabwehrorganisation vorgestellt.

Darstellung

Kritische Infrastrukturen sind die Lebensadern moderner leistungsfähiger Gesellschaften. Nach der Definition der EU-Richtlinie 2008/114/EG vom 8. Dezember 2008 ist eine Kritische Infrastruktur eine Anlage, ein System oder ein Teil desselben, die von zentraler Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen, der Gesundheit, der Sicherheit und des wirtschaftlichen und sozialen Wohlergehens der Bevölkerung ist und deren Ausfall, Störung oder Zerstörung erhebliche Auswirkungen hätte, da ihre Funktionalität nicht aufrechterhalten werden kann. Die Definition des BMI konkretisiert die Folgen: »Durch [den] Ausfall [Kritischer Infrastrukturen] oder ihre Beeinträchtigung würden erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten.« Die Gewährleistung des Schutzes dieser kritischen Infrastrukturen ist eine Kernaufgabe sowohl der staatlichen, als auch der unternehmerischen Sicherheitsvorsorge und zentrales Thema der Sicherheitspolitik (BMI Schutz kritischer Infrastrukturen 2018). Zur rechtlichen Ableitung des Begriffes und seine Differenzierung in Prävention, Detektierung von Störungen und im worst case darauf zu reagieren und diese zu bewältigen, vgl. Guckelberger 2019, 525ff.,527. Als Rechtsbegriff erscheinen Kritische Infrastrukturen erstmals 2008 in § 2 Absatz 2 Ziffer 3 Satz 4 des Raumordnungsgesetzes, "Dem Schutz kritischer Infrastrukturen ist Rechnung zu tragen." Damit sind sämtliche Kritischen Infrastrukturen gemeint, die IT ist nur ein (allerdings nicht unwichtiger) Teilbereich.

Seit 2015 gilt das erste IT-Sicherheitsgesetz, die Cyber-Strategie für Deutschland wurde 2016 neu formuliert. Ziel der erneuerten Kritis-Strategie ist die Steigerung der gesamtgesellschaftlichen Resilienz. Der im Unterstützungsplan Kritis (UP-KRITIS) institutionalisierte Dialog zwischen Staat und Wirtschaft fördert die Zielerreichung. Die Kritischen Infrastrukturen sind neun Sektoren zugeordnet. Diesen Sektoren kommt zentrale Bedeutung zu. Es sind (deutscher Ansatz):

1. Energie
2. Informationstechnik und Telekommunikation
3. Transport und Verkehr
4. Gesundheit
5. Wasser
6. Ernährung
7. Finanz- und Versicherungswesen
8. Staat und Verwaltung
9. Medien und Kultur.

Andere Länder erweitern diese Sektoren um den Sektor Verteidigungsstreitkräfte, was auch für Deutschland beabsichtigt ist.

Gefahren für Kritische Infrastrukturen

Die neun Sektoren befinden sich zu großen Teilen in privater Hand, so dass Krisenmanagementstrukturen von Unternehmen von zentraler Bedeutung sind. Der Ansatz der Resilienz will diese Strukturen nicht durch staatliche Strukturen ersetzen, sondern härten und ergänzen. Dabei geht es vor allem darum, Gefahren für die Kritischen Infrastrukturen abzuwehren.

Allgemein ist das Gefahrenpotential nach seinem Schwerpunkt in natürliche Gefahrenursachen und anthropogene (im Wesentlichen von Menschen hervorgerufene) Gefahrenursachen zu unterscheiden. Als besondere Gefahrenpotentiale sind zu nennen:

Tabelle 1:

Natürliche Gefahren	Anthropogene Gefahren
Extremwetterlagen und deren Folgen	Unfälle und Havarien
Erdbeben/Erdbewegungen	Technisches/menschliches Versagen
Feuer (Wald- und Heidebrände)	Systemfehler
Epidemien/Pandemien	Sabotage
Extraterrestrische Gefahren	Terrorismus/organisierte Kriminalität/ Kriege
Unbekanntes / »Schwarze Schwäne«	

Wichtig ist es, sich vor Augen zu führen, wo die Abhängigkeit von Staat und Bevölkerung besonders groß ist und was die größten Risiken sind:

- Längerfristiger, flächendeckender Ausfall der Stromversorgung (Blackout)
- IT- Ausfall
- Pandemie
- Kaskadeneffekte
- Unbekannte Lagen/schwarze Schwäne
- Verhalten der Bevölkerung.

Ein besonderes Risiko stellt ein langfristiger Blackout dar. Sollte die Stromversorgung zusammenbrechen würden viele Funktionalitäten entfallen. Die Zuständigen (Stromnetzbetreiber und Bundesnetzagentur) würden sich um eine Wiederinbetriebnahme bemühen, könnten aber darüber hinaus nichts veranlassen, solange kein Strom zur Verteilung vorhanden ist. Wie lange eine Wieder-Inbetriebnahme des Netzes und der Stromversorgung dauert, hängt davon ab, ob sich Kraftwerke im Eigenbedarf ge-

fangen haben, ein Inselbetrieb möglich ist und wie viele schwarzstartfähige Kraftwerke zur Verfügung stehen. Nur schwarzstartfähige Kraftwerke können ihren Betrieb selbsttätig, ohne zusätzlichen Stromimpuls, aufnehmen. Auch die meisten erneuerbaren Energien (Windkraftanlagen, Fotovoltaik, Bio-Gasanlagen) verfügen über diese Funktionalität nicht. Überlegungen, derartige Anlagen zu inselbetriebsfähigen Microgrids (wikipedia Inselnetz 2018) zusammenzuschließen, sind in Deutschland bislang nicht über das Versuchs- bzw. Planungsstadium hinausgekommen. Zudem gilt das Verletzlichkeitsparadoxon: Je seltener ein Ereignis eintritt, umso schlechter ist das betroffene Land darauf vorbereitet. Die erfahrene Netzstabilität verstärkt das Gefühl der Unverletzbarkeit. Wer in Deutschland hat Erfahrungen, um mit einem Stromausfall zurecht zu kommen. Wie kommen die Beschäftigten bei einem Blackout an ihren Arbeitsplatz? Sollten viele Menschen in einer derartigen Situation den Notruf wählen, überlasten sie die Funkzellen und erreichen in der kurzen Phase, in der die Mobiltelefone nach einem Stromausfall noch funktionieren, niemanden.

Kommunikation und Mobilität wären bei einem Blackout eingeschränkt. Die Einsatzfähigkeit weiterer Bereiche ist davon abhängig, dass eine Notstromversorgung funktioniert. Diese basiert im Wesentlichen auf Dieselaggregaten, die regelmäßig aufgefüllt werden müssen. Unser Blick sei beispielhaft auf die Nahrungsmittelversorgung gerichtet. Bei einem Blackout ist davon auszugehen, dass die Notstromversorgung von Lebensmitteleinzelhandel und Lebensmitteldiscountern nur dazu ausreicht, um Kassen und Türen geordnet herunterzufahren bzw. zu schließen. Ein ordnungsgemäßer Verkauf ist nicht mehr möglich. Alte Konzepte der Ernährungssicherstellung sahen vor, dass in derartigen Fällen jeglicher Handel für 48 Stunden ausgesetzt wird. Erst danach erfolgt ein strukturierter Verkauf (Voraussetzung Lebensmittelmarke und Bargeld) durch den Handel mit Unterstützung staatlicher Stellen (neu etablierte Ernährungsämter). Es gibt mehrere Gründe, warum dieses Konzept nicht mehr als praktikabel angesehen wird, denen auch das neue ESVG von 2017 Rechnung trägt.

Im Rahmen der Haushaltsführung werden von vielen, aber nicht von allen, Vorräte für mehrere Tage angelegt

- Ca. 1/4 der Befragten hält Vorräte für 1 Woche vor
- Ca. 1/5 der Befragten hält aber keine Vorräte vor
- Je ländlicher die Region, desto mehr Vorräte werden vorgehalten.

In Kernbereichen von Mittelzentren, Großzentren und Ballungsräumen halten 23 % der Befragten keine Vorräte vor. Die Tendenz ist eher steigend und schließt auch vulnerable Bevölkerungsgruppen ein (Eltern mit kleinen Kindern, Alte, Kranke, immobile Menschen). Auch Krankenhäuser und Seniorenstifte/Altenheime haben ihre Versorgung im Regelfall an Caterer outgesourct und verfügen über so gut wie

keine Nahrungsmittelvorräte. Auch die Vorräte an Trinkwasser sind gering. Bei einem Stromausfall werden viele Wasserversorger mangels ausreichenden Wasserdrucks die Wasserversorgung nicht aufrechterhalten können. Damit fehlt das Leitungswasser als Trinkwasser. Selbst wenn es noch Stunden zur Verfügung stehen sollte, fehlen zumeist geeignete Geräte (Kanister), das Wasser abzufüllen. Ein Ausfall auch des Brauchwassers und damit der Toilettenanlagen in Hochhäusern und Krankenhäusern führt innerhalb von Stunden zu hygienischen Problemen.

Es zeigt sich, dass ein derartiges Szenario unmittelbar Auswirkungen auf die konkrete Versorgung der Bevölkerung mit Nahrungsmitteln und Wasser hat. Diese sind im gesamten Sektor Ernährung (Versorgung mit Lebensmitteln) zu verzeichnen.

Der Sektor Ernährung umfasst:

- Landwirtschaft (Primärproduktion),
- Be- und Verarbeitung (Sekundärproduktion), Lagerung und
- Vertrieb von Lebens- und Futtermitteln.

Handelnde Akteure sind: Landwirtschaftliche u. gewerbliche Unternehmen der privaten Wirtschaft mit ihren betrieblichen Einrichtungen.

Auch Extremwetterereignisse können große Auswirkungen auf die Landwirtschaft und damit auf die Ernährung haben. Das sind z. B

- Gemüse, Obst
  - Erschwerte Anbaubedingungen und abnehmende Erträge bei Hafer, Roggen, Kartoffeln, Zuckerrüben, Kernobst
  - Erforderlichkeit einer Umorientierung auf angepasste Kulturen z. B. Soja, Ölfrüchte, Hirse und entsprechende Anbaumethoden
  - Erhöhter Aufwand an Pflanzenschutzmitteln durch steigenden Befalls- und Infektionsdruck
- Wasser
  - Abnehmende Niederschlagsmengen und veränderte Verteilung erfordern Wasserspeichermanagement
  - Ausbau des Bewässerungsanbaus gegen Hitzestress und
  - Wassermangel in Hauptentwicklungsphasen
- Nutztierhaltung
  - Leistungseinbrüche und Verluste bei Tierbeständen durch Hitzestress
  - Gefährdung der Tierbestände durch Auftreten neuer Krankheiten

- Verlust an Flächen durch Überschwemmungen.
  - Zu erwarten sind Ertragsrückgänge.

Flächenverluste können nicht durch Ausweitung von Agrarflächen kompensiert werden, da Ackerland in Deutschland eine knappe Ressource ist. Nach einer Studie des Umweltbundesamtes wird Deutschland ab 2030 seinen Bedarf an agrarischen Erzeugnissen nicht mehr aus der Produktion auf eigenen Flächen sicherstellen können.

Ein Stromausfall wäre auch in der Nahrungsmittelerzeugung nur durch Notstrom kompensierbar. Dabei zeigt sich besonders deutlich, dass Dieseltreibstoff und entsprechende Aggregate in ausreichendem Maße vorhanden sein müssen, um die schwersten Folgen eines Blackouts abzuwenden:

- Dieselversorgung
  - Eigenverbrauchstankstellen sind Puffer für Dieselversorgung
  - Potentiell bestehen Versorgungsreichweiten bis zu mehreren Monaten
  - Keine belastbaren Daten über Anzahl und Kapazitäten.
- Stromversorgung
  - Nach Tierschutz-Nutztierhaltungsverordnung (VO) sind Ersatzsysteme zur Versorgung der Tiere mit Licht, Luft, Wasser und Futter vorzuhalten.
  - Diese VO gilt nach herrschender Meinung nicht für den Betrieb von Melkanlagen. Diese Regelungslücke wird seit dem Stromausfall im Münsterland 2005 in Fachkreisen erörtert.

Seit einigen Jahren muss ein IT-Ausfall als ähnlich gravierend wie ein Stromausfall bewertet werden. Daher bestimmt die Kritis-VO (Rechtsverordnung nach § 10 des BSI-Gesetzes), dass Betreiber Kritischer Infrastrukturen ihre Vorkehrungen entsprechend § 8 a Absatz 1 BSIG zur Vermeidung von Störungen nach dem Stand der Technik dem BSI nachweisen müssen (vgl. Kapitel A.4.1).

Über diese Szenarien hinaus stellt sich die Frage, ob Teile der Kritischen Infrastrukturen bereits selbst eine Kritische Infrastruktur sein können oder ob unter diesem Begriff nur der gesamte Sektor zu subsumieren ist. Müssen künftige Entwicklungen mit bedacht werden? D. h. ist nur die Versorgung Deutschlands mit Gas kritisrelevant oder auch die einzelne Pipeline, z. B. Nord-Stream 2. Hier zeigen sich Verbindungen zu global-strategischen Gedanken. Noch ist Russland davon abhängig, dass sein Gas störungsfrei durch die Ukraine nach Westeuropa fließt. Nord-Stream 2 würde Russland von dieser Bindung befreien. Maßnahmen zur Destabilisierung der Ukraine sind nicht ausgeschlossen. Eine Destabilisierung der Ukraine

könnte zu einer Gefahr für die Sicherheit der EU werden. Gleichzeitig bedeutet die Transportmöglichkeit durch Nord-Stream 2 eine Erweiterung der Optionen, sie könnte das Risiko einer (z. B. leitungskapazitätsbedingten) Gasmangellage reduzieren, also die Resilienz steigern. Eine weitere Frage lautet: Werden die traditionellen Automobilkonzerne weiter die Wirtschaftslokomotive Deutschlands sein oder gehört Elon Musk und Tesla die Zukunft. Müssen Kritische Infrastrukturen gegenwarts- oder zukunftsbezogen gedacht werden? Warum ist die Kritische Infrastruktur Flughafen nicht besser gegen Drohnen geschützt? Der Londoner Flughafen Gatwick mussten wegen Drohnenflugs am 20. Dezember 2018 geschlossen werden. 110.000 Flugreisende waren betroffen. Auch deutsche Flughäfen sind nicht besser gesichert, Drohnenabwehrsysteme fehlen (Deutsche Flughäfen ungeschützt vor Drohnenangriffen 2018, S. 17). Neben erkennbaren »to dos« z. B. Sicherheitsmängeln und Ihrer Beseitigung, ist Phantasie gefragt, um die Kritischen Infrastrukturen für die Zukunft resilienter werden zu lassen.

Erkennen von Kritis-Gefahren

Bund, Länder und Kommunen arbeiten im Bevölkerungsschutz eng zusammen. Wichtige Akteure bei der Krisenbewältigung sind darüber hinaus die Hilfsorganisationen und Betreiber Kritischer Infrastrukturen. Gefahren für Kritische Infrastrukturen zu erkennen, zu bewerten und Maßnahmen zur Reduzierung dieser Gefahren umzusetzen, ist Inhalt des Risikomanagements. Die organisatorische Vorbereitung auf die Bewältigung von Krisen ist Gegenstand des Krisenmanagements. Die Integration gemeinsamer Themen in Form eines integrierten Risiko- und Krisenmanagements von einerseits Betreibern Kritischer Infrastrukturen und andererseits Behörden der allgemeinen Gefahrenabwehr steigert die Wirksamkeit der Maßnahmen und verbessert die Krisenbewältigung. Denn ein abgestimmtes Risiko- und Krisenmanagement im Umfeld einer Katastrophe oder der Zivilen Verteidigung sind notwendig, um eine stetige Weiterentwicklung und Verbesserung der Resilienz der Bevölkerung vor den drohenden Gefahren zu ermöglichen. Im Rahmen des integrierten Risiko-Krisenmanagements müssen in einem sich wandelnden Sicherheitsumfeld, die Plausibilität des Eintritts extremer Gefahren und deren Schadenswirkungen abgeschätzt und, darauf aufbauend, zielgerichtet Präventiv- und Notfallmaßnahmen umgesetzt werden. Instrumente aus dem Risiko- und Krisenmanagement werden von den unterschiedlichen Akteuren aus den jeweiligen Aufgabengebieten heraus angewendet. So nutzt die Gefahrenabwehr die Instrumente, um Schäden von der Bevölkerung abzuwenden und zum Schutz der Bevölkerung möglichst schnell auf den Eintritt von Schäden reagieren zu können. Betreiber Kritischer Infrastrukturen zielen mit den Maßnahmen aus ihrem Risiko- und Krisenmanagement auf den Schutz des Personals

und die Aufrechterhaltung ihrer kritischen Dienstleistung ab. Die Bevölkerung sollte Eigenvorsorge betreiben, indem sie Vorräte an Wasser und Lebensmitteln vorhält und sich über Verhaltensempfehlungen informiert, um auf Gefahren adäquat reagieren und Ausfälle von Kritischen Infrastrukturen in Teilen kompensieren zu können. Durch die Integration des Risiko- und Krisenmanagements von Gefahrenabwehr und Betreibern Kritischer Infrastrukturen werden deren Präventiv- und Notfallmaßnahmen methodisch und in der Umsetzung miteinander verknüpft. Fragestellungen der Gefahrenabwehr oder des Zivilschutzes fließen in die Strukturen des betrieblichen Risikomanagements von Kritischen Infrastrukturen ein. Alle Akteure können ihr Risikomanagement nur mit aktuellen Informationen aus dem jeweils anderen Bereich optimal einsetzen. Hierzu werden die Maßnahmen der Gefahrenabwehr mit denen der verschiedenen Betreiber Kritischer Infrastrukturen eng verzahnt. Dies erfolgt durch den strukturierten Austausch von Informationen, die diese u. a. in ihrem jeweiligen Risikomanagement gewonnen haben. Ein integriertes Krisenmanagement bietet die Grundlage und den Handlungsrahmen für ein abgestimmtes und zielgerichtetes Vorgehen aller Akteure der Krisenbewältigung. Hierzu zählen Maßnahmen zur Etablierung von einrichtungsübergreifenden Krisenmanagementstrukturen, Übungen in diesen Strukturen und ein kontinuierlicher Verbesserungsprozess dieses Systems. Die Einbindung von Betreibern Kritischer Infrastrukturen erfolgt über deren Teilnahme an den länderübergreifenden Krisenmanagementübungen (LÜKEX-Übungen), den UP KRITIS und das Seminarangebot der AKNZ (System des Krisenmanagements in Deutschland, BMI 2015). Dabei muss sich das Augenmerk auch auf kritische Dienstleistungen richten.

Kritische Dienstleistungen sind für die Bevölkerung wichtige, teils lebenswichtige Güter und Dienstleistungen. Bei einer Beeinträchtigung dieser kritischen Dienstleistungen würden erhebliche Versorgungsengpässe, Störungen der öffentlichen Sicherheit oder vergleichbare dramatische Folgen eintreten (Bundesamt für Bevölkerungsschutz, Glossar).

3.1.2 Internationaler Vergleich

Andreas H. Karsten

Wann eine Infrastruktur als »kritisch« zu betrachten ist, wird weltweit durchaus unterschiedlich bewertet. Schon die Definitionen zeigen verschiedene Schwerpunktsetzungen auf (vgl. CIPedia: Critical Infrastructure).

Während die deutsche Definition konkret nur den Schutz der Versorgung und der öffentlichen Sicherheit anspricht, bezieht zum Beispiel die kanadische Definition das wirtschaftliche Wohlergehen der Kanadier mit ein. Kanada geht auch besonders darauf ein, dass nationale Infrastrukturen mit solchen außerhalb von Kanada vernetzt sein könnten. Der Unterschied wird am Beispiel der Automobilindustrie deutlich: Nach deutscher Vorstellung gehören deren Betriebe nicht zu den Kritischen Infrastrukturen, nach der kanadischen schon. Schaut man sich die Entwicklung des Großraums von Detroit an, so kann man durchaus die kanadische Auffassung teilen, dass das wirtschaftliche Wohlergehen von Bewohnern einer Region ebenfalls eine Grundlage der nationalen Stabilität und staatlichen Funktionalität darstellt. Vergleicht man nun die Region Detroits mit der von Südostniedersachsen, so kann man sich schon fragen, ob der deutsche Ansatz eventuell zu kurz greift.

Basierend auf den unterschiedlichen Definitionen werden in den verschiedenen Staaten verschiedene Infrastrukturen als Kritisch angesehen (vgl. CIPedia: Critical Infrastructure Sector). Einige Infrastrukturen werden allerdings einheitlich zu den kritischen gezählt:

- Wasser, Ernährung, Gesundheit
- Energie, Information, Kommunikation
- Transport
- Staat, Finanzwirtschaft

Diese sollten bei der Stärkung der Resilienz Deutschlands besondere Priorität besitzen. Allerdings können die anderen Kritischen Infrastrukturen aufgrund von Kaskadeneffekten Krisen in diesen Schlüsselsektoren auslösen, falls die Kaskaden nicht zu unterbrechen sind.

3.2 Stresssituation und Schockereignisse

Andreas H. Karsten

Die Stabilität eines Systems (Gesellschaft, Staat, Unternehmung, Gruppe) wird durch zwei grundsätzlich verschiedene Arten von Ereignissen belastet bzw. bedroht:

- **Schockereignisse:**
  Seltene, plötzlich eintretende, verheerende Ereignisse mit einem sehr starken aber kurzem Anstieg der Belastung (Katastrophen, Epidemien, Terroranschlag) (vgl. Kapitel D.2.1).

- **Stresssituationen:**
  Chronische Belastungen, die lange anhalten und häufig langsam ansteigen (Klimawandel, mangelhafte Transportinfrastruktur, Lebensmittelversorgung, Arbeitslosigkeit, Angst vor Schockereignissen).

Dabei spielt es keine Rolle, ob die Ereignisse real oder eingebildet sind, wie das Thomas Theorem besagt: Definiert jemand eine Situation als real, dann ist sie in ihren Konsequenzen real.

Wir Menschen neigen dazu, Schockereignisse als gefährlicher anzusehen als Stresssituationen (vgl. Fukushima und Kernenergie mit Klimawandel und Kohleverstromung). Ob dies berechtigt ist, lässt sich erst in der historischen Rückschau beurteilen. Beide Arten addieren sich zu der Gesamtbelastung des Systems, die zu starken Einschränkungen der Leistungen bis zum Totalzusammenbruch führen kann.

So führt eine hohe Arbeitslosigkeit (Stresssituation) zu sozialen Spannungen (Stresssituation), die wiederum zu inneren Unruhen (Schockereignis) führen können.[3] Daneben sinken die Steuereinnahmen. Dadurch wird der Staat gezwungen, weniger auszugeben (Stresssituation). Dies führt über kurz oder lang zu einer Verringerung der Ausgaben für die öffentliche Sicherheit und Ordnung (Feuerwehr, Katastrophenschutz, Rettungsdienst, Polizei, Geheimdienste, Streitkräfte). Dadurch kann der Staat inneren Unruhen schlechter begegnen und wird anfälliger gegenüber Terroranschlägen und Erpressungen durch andere Staaten (Schockereignisse). Was ihn wiederum für Auslandsinvestitionen unattraktiver macht und somit die Gefahr einer steigenden Arbeitslosigkeit heraufbeschwört (Stresssituation). Und nun beginnt dieser Teufelskreis von vorne. In der Vergangenheit wurden beide Bereiche weitestgehend getrennt betrachtet und unterschiedliche Behörden und Organisationen versuchten, vorbeugende, vorbereitende und abwehrende Maßnahmen zu finden. Zum Beispiel kümmerten sich auf kommunaler Ebene die Brand- und Katastrophenschutzämter sowie die Polizeien um die Schockereignisse. Planungs-Sozial- Umwelt-, Arbeitsämter und einige mehr konzentrierten sich auf die Stresssituationen.

Obwohl in den einzelnen Behörden ein umfangreiches Fachwissen zur Verfügung steht, fehlt solch einem Ansatz die zusammenhängende, allumfassende Herangehensweise, die bei der heutigen stark vernetzten Welt dringend erforderlich ist, um die Gefahr eines Systemversagens entgegenzutreten. Einige Städte haben dies

3 Siehe z. B. Deutschland Anfang der 30er Jahre, den Arabischen Frühling oder die Situation in den südlichen EU-Staaten nach dem Jahrtausendwechsel.

erkannt und versuchen z. B. durch die Ernennung von Resilienz-Verantwortlichen darauf zu reagieren (siehe Rockefeller Foundation: 100 Resilient Cities Initiative).

3.3 Resilienz

Andreas H. Karsten

Derzeit befinden wir uns in einer revolutionären Phase. Die Welt verändert sich grundlegend. Und diese Veränderung gefährdet unser Leben so wie wir es heute leben. Am gravierendsten sind vielleicht

- der Klimawandel,
- die Globalisierung weiter Lebensbereiche bei gleichzeitig wachsendem Nationalismus und Protektionismus in anderen Bereichen,
- die Verschiebung der weltweiten staatlichen Macht von West nach Ost,
- die Abnahme staatlicher Macht gegenüber nichtstaatlichen Akteuren,
- das Ende der Zeit der Aufklärung und das Erstarken von religiösen und pseudo-religiösen Bewegungen (von: »Ich denke also bin ich« zu »Ich glaube also bin ich«),
- der technologische Wandel, wie Künstliche Intelligenz, Nanotechnologie und Bio-/Gentechnologie,
- die Atomisierung der Arbeitsabläufe, deren einzelne Arbeitsabschnitte weltweit bearbeitet und dann zusammengefügt werden,
- die eng verknüpfte Zusammenarbeit von Menschen und Maschinen auch bei geistigen Tätigkeiten,
- das Anwachsen von Unsicherheit und Zukunftsängste bei vielen Menschen. Die heutige Welt ist ungewiss und mehrdeutig bei gleichzeitigem weit verbreiteten »Risiko-Analphabetismus«.

Unsere Unfähigkeit, auf diese Veränderungen adäquat zu reagieren, liegt zum großen Teil daran, dass wir nicht in der Lage sind, komplexe, gegenseitig voneinander abhängige, nichtlineare und miteinander vernetzte Systeme wirklich zu verstehen und resilient zu gestalten.

INFO

Info:

Laut Duden (2019) stammt das Wort Resilienz vom lateinischen Wort resilire ab, was »zurückspringen« bedeutet.

Tabelle 2: ***Verknüpfungen von Mensch, Resilienz und Kritischen Infrastrukturen***

Gebiet	Definition Resilienz
Psychologie	Fähigkeit von Menschen, Krisen jeglicher Art zu bewältigen und sie durch Rückgriff auf persönliche und sozial vermittelte Ressourcen als Ausgangspunkt für positive Entwicklungen zu nutzen.
Ökosystem	Fähigkeit eines Ökosystems bei einer ökologischen Störung die grundlegende Organisationsweise zu erhalten und nicht in einen qualitativ anderen Zustand überzugehen.
Ingenieur-wissenschaften	Fähigkeit eines technischen Systems, bei externen und internen Störungen und Teilausfällen wesentliche Systemleistungen aufrechtzuerhalten.
Soziologie	Fähigkeit einer Gesellschaft, externe Störungen zu verkraften (widerstehen und/oder zu regenerieren), ohne dass sich wesentliche Strukturen, Funktionen und Kontrollprozesse ändern.
Urbanistik	Fähigkeit städtischer Strukturen, primäre Lebensgrundlagen bei inneren und/oder äußeren Störungen durch die Aufrechterhaltung zentraler Funktionen zu sichern.
Management	Fähigkeit eines organisatorischen oder betriebswirtschaftlichen Systems gegenüber Störungen (Schockeffekte) und Veränderungen (Stresssituationen) zu widerstehen. Dies kann in einer proaktiven und/oder in einer reaktiven Form erfolgen.

Der Begriff wird in verschiedenen Wissenschaften etwas unterschiedlich verwendet:

Wenn wir im Folgenden von der Resilienz der Kritischen Infrastrukturen sprechen, so soll dieser Begriff möglichst breit gefasst werden.

Ziel der Bemühungen ist es, Deutschland auch in Krisensituationen »am Laufen zu halten«. Dabei werden jeweils die Menschen im Mittelpunkt stehen, die sich in Deutschland aufhalten. Deren Wohlergehen ist sowohl das eigentliche Ziel wie auch letztendlich die wesentliche Voraussetzung resilienter Kritischer Infrastrukturen (siehe Bild 1).

Resilienz ist sowohl Ziel als auch Weg. Es ist ein iterativer und agiler Prozess, in dem immer wieder neue Informationen, neues Wissen für die immer wiederkehrenden Überprüfungen und Neuplanungen der eigenen Aktivitäten genutzt werden. Die Definitionen von Resilienz im Bereich Bevölkerungsschutz/Krisenmanagement sind international ähnlich. So schreibt die EU-Kommission: »Resilienz ist die Fähigkeit eines Individuums, einer Gemeinschaft oder eines Landes, Stress und Schocks, die

durch Katastrophen, Gewalt oder Konflikte verursacht werden, zu bewältigen, sich anzupassen und sich schnell zu erholen. Nach Geier ist »ein Kernelement einer resilienten Gesellschaft neben den Kritischen Infrastrukturen die Bevölkerung, deren Widerstandsfähigkeit so hoch sein sollte, dass sie im Katastrophenfall nicht als schwächstes Kettenglied zum eigentlichen Risiko wird.« (Geier, 2018). Die Bevölkerung kann nur resilient sein, wenn die Kritischen Infrastrukturen resilient sind und die Kritischen Infrastrukturen können nur resilient sein, wenn die Bevölkerung resilient ist. In diese wechselseitige Abhängigkeit müssen alle Bereiche eingebunden werden: der Mensch, die Familie, die Gemeinschaft in Mehrfamilienhäusern, die Zivilgesellschaft, Gemeinden und Regionen, die Landesregierungen, die Bundesregierung, überstaatliche Organisationen, die Wirtschaft; letztendlich die gesamte Welt (siehe auch Kapitel A.3.4). Aufgrund der heutigen Vernetzung und Bedrohungen ist es nahezu unmöglich, gewisse Bereiche des Lebens aus den Betrachtungen auszuschließen. Bei allen Betrachtungen sollte aber nie das oben genannte, eigentliche Ziel aus den Augen verloren werden: der Mensch. Dabei ist dieser sowohl als schützenwertes Ziel (siehe Grundgesetz) wie auch als mögliche Störgröße auf die jeweiligen Systeme zu betrachten. Psychologische und soziologische Faktoren dürfen deshalb nicht außer Acht gelassen werden.

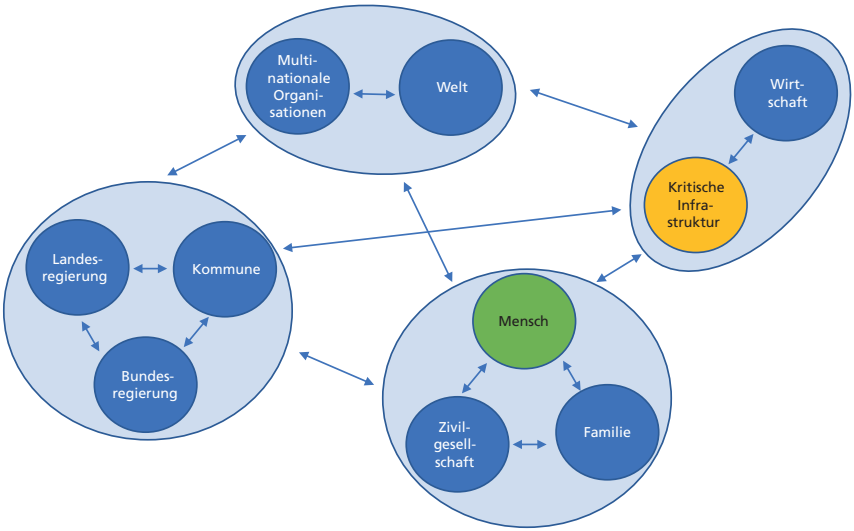

Bild 1: ***Verknüpfungen von Mensch und Kritischen Infrastrukturen***

Resilienz auf der persönlichen Ebene ist wichtig für das psychosoziale Wohlergehen der Menschen. Neben materiellen Faktoren, wie Lebensmitteln und Trinkwasser, sind eine positive Eltern-Kinder-Beziehung und gegenseitige soziale Netzwerke entscheidend für die Resilienz auf persönlicher Ebene. Allerdings kann ein starkes Vertrauen auf starke, lokale Netzwerke auch die Resilienz von Gemeinschaften verringern, wenn die Menschen z. B. eher den Gerüchten in diesen Netzwerken vertrauen als den amtlichen Verlautbarungen. Solch eine Situation kann schnell zu Panik und sozialen Unruhen führen.

Resilienz auf kommunaler Ebene umfasst Faktoren wie

- die Qualität der Umwelt
- der Umgang mit den natürlichen Ressourcen
- der Zugang zu den kommunalen Ressourcen bzw. Infrastrukturen wie Trinkwasser oder Abwasser
- Sicherheit und Ordnung
- die Einkommenssituation
- die Vielfalt der Lebensmittelversorgung
- die Verfügbarkeit eines sozialen Netzes und die Teilnahmemöglichkeiten an der Gemeinschaft
- die demographische Entwicklung.

Je größer die betrachteten Systeme werden, umso wichtiger werden Institutionen, Strategien und Prozesse.

In städtischen Kommunen spielt die Verwaltung eine wichtigere Rolle für die Resilienz als in ländlichen. Die Abhängigkeiten der meisten urbanen Infrastrukturen (Trinkwasser, Abwasser, Lebensmittelversorgung, soziale Netzwerke) von den Kritischen Infrastrukturen der vier Sektoren elektrische Energieversorgung, Informations- und Kommunikationstechnologie, Verkehr und Verwaltung sind essentiell. Genauso wichtig ist es, dass die Menschen in den städtischen Gebieten über einen Arbeitsplatz und ein gesichertes Einkommen verfügen. In Großstädten kommt noch die innere Sicherheit als entscheidender Faktor hinzu. Resilienz ist ein ebenenübergreifendes und fachdisziplinübergreifendes Phänomen. Resilienz ist ein nie endender Prozess. Sobald sich die Mitglieder eines Systems nicht mehr bemühen, die Resilienz zu steigern, wird diese zwangsläufig abnehmen.

Im Folgenden soll unter Resilienz sowohl die Widerstands- als auch die Regenerationsfähigkeit eines Systems (vom Menschen bis zur Welt) verstanden werden. Vereinfacht gesprochen geht es um die Krisenfestigkeit eines Systems. Maßnahmen zur Steigerung der Resilienz eines Systems können somit vorausschauend und

anpassend sein (Widerstandsfähigkeit) wie auch dazu führen, dass dieses nach einer Störung wieder schnell auf die Beine kommt (Regenerationsfähigkeit).

Dabei sind sowohl Stress- als auch Schockereignisse in die Überlegungen einzubinden (siehe Kapitel A.3.2). Ein Schockereignis, wie ein Wintersturm, das während einer Stresssituation eintritt, z. B. eine Überalterung der Eisenbahnverkehrsinfrastruktur kann zu einem bundesweiten und tagelangen Erliegen des Bahnverkehres durch Sturmschäden, Vereisungen usw. führen. Dies hätte wiederum erhebliche Auswirkungen auf die Lebensmittelversorgung der Bevölkerung und auch der Einsatzkräfte, was wiederum die Behebung der Schäden negativ beeinflusst und eventuell eine Negativspirale in Gang setzt, die in einer existenziellen Krise des Landes enden kann. Aber auch Stresssituationen wie erhebliche Zukunftsängste aufgrund der modernen Technologien oder die (scheinbar) unaufhaltsame Globalisierung – mit der einhergehenden steigenden Angst vor dem Verlust des individuellen und nationalen sozialen Standards und der individuellen und nationalen Identität – können die Widerstands- und Reaktionsfähigkeit (häufig unbemerkt) soweit schwächen, dass ein unter normalen Umständen leicht beherrschbares Schockereignis, wie das Eintreffen einer großen Anzahl von Flüchtlingen, zu einer Krisensituation führen kann.

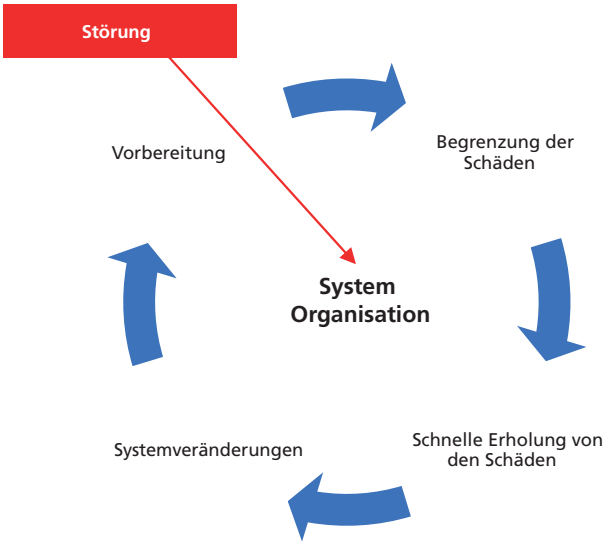

Bild 2: ***Resilienz-Kreislauf***

Ziel von Resilienz ist es, dass die betrachteten Systeme oder Organisationen (Mensch, Familie, Gemeinde/Stadtteil, Stadt, Wirtschaftsunternehmen, Ökosystem, Staat usw.) bei dem Einfluss von Stress- oder Schockereignissen nicht nur weiter funktionieren, sondern im besten Fall sogar weiter florieren. Wichtige, nicht endende Aufgaben sind (siehe auch Bild 2):

- Vorbereiten auf den Eintritt von Störungen
  - Antizipieren – Planen – Vorbereiten
  - Risiken vermindern oder managen
  - Gefährdungen vermeiden
- Begrenzen der Schäden nach Eintritt einer Störung
  - Anpassen – Absorbieren – Zurechtkommen
- Schnelle Erholung von den Folgen der Störungen
  - Wieder auf die Beine kommen – Erholen
  - Minimierung der Verluste oder Kosten
  - Überleben – Fortbestehen – Aufrechterhalten
- Systemveränderung zu einem »besseren« Zustand
  - Adaptieren – Entwickeln
  - Transformieren
  - Lernen
  - Reorganisieren

Kontrovers diskutiert wird das Ziel der Recovery-Phase. Reicht es, sich darauf vorzubereiten, dass nach dem Eintritt einer Krise das System möglichst schnell wieder in den ursprünglichen Zustand, den alten »Normalzustand« zurückgebracht werden kann, oder muss man sich darauf vorbereiten, dass ein neuer, besserer Zustand erreicht wird, damit das System zukünftiger resilienter ist? Aber wie sieht dieser bessere Zustand aus? In Bezug auf die Flüchtlingssituation ist die Frage zu beantworten, ob der anzustrebende zukünftige Zustand die »Festung Europa« oder aber Deutschland, »das Land des Lebens, der Freiheit, der Hoffnung und das Bestreben nach Glückseligkeit für alle Menschen auf der Welt« oder aber etwas dazwischen sein soll.

Betrachtet man den Menschen als einen Teil des Systems, so kann der ursprüngliche »Normalzustand« nach einer Störung nie mehr erreicht werden, denn das Bewusstsein der Menschen hat sich durch die Störung unumkehrbar verändert.

3.4 Kritikalität

Andreas H. Karsten

Laut Duden bedeutet Kritikalität eine große Wichtigkeit von etwas, dessen Verlust eine existenzielle Gefährdung darstellt. Die Kritischen Infrastrukturen besitzen eine hohe Kritikalität für unser Gemeinwesen. Wichtig ist nicht die Infrastruktur an sich, sondern das Produkt oder die Dienstleistung, die sie den Menschen letztendlich zur Verfügung stellt (ein Medikament, eine ärztliche Behandlung etc.).

Am 28. Januar 1986 explodierte die Challenger Raumfähre. Dabei starben alle sieben Astronauten und eine Raumfähre im Wert von 196 Milliarden US $ wurde total zerstört. Ursache dieses Unglücks war ein poröser Gummi-Dichtungsring (englisch O-Ring) an einer der seitlichen Feststoffraketen. Das Versagen eines kleinen, billigen Bauteils hat zu einem der schwersten Unglücke der NASA geführt. Die wesentliche Lehre aus diesem Unglück ist: Werden in einem komplexen System die Verlässlichkeit einzelner Teile immer mehr verbessert, wird die Verlässlichkeit der übrigen Teile immer bedeutender.

Hohe Kritikalität besaß im Challenger-Beispiel unerkannter Weise der Gummi-Dichtungsring.

Dass das O-Ring-Prinzip auch bei Planungen auftritt, zeigen zwei Beispiele:

Am 23.09.1999 verglühte die NASA Marssonde »Mars Climate Orbiter« in einer Höhe von 57 km über der Marsoberfläche. Der marsnächste Punkt der Umlaufbahn sollte allerdings 150 km betragen. Ursache dieses Navigationsfehlers war die Nichtbeachtung der unterschiedlichen Nutzung von Maßeinheiten (metrisches und US-System) bei der Herstellung der 125 Millionen US $ teuren Sonde.
Hier war Kritikalität des verwendeten Einheitensystems verantwortlich für den Verlust.

Der Bau der Rheinbrücke zwischen dem deutschen und dem schweizerischen Laufenburg erfolgte von beiden Uferseiten aus. Beim Fortschritt der Bauarbeiten wurde festgestellt, dass zwischen den beiden Brückenteilen eine Höhendifferenz von 54 Zentimeter lag. Zwar hatte man bei der Planung berücksichtigt, dass die Schweiz als Referenzpegel für die Höhengaben in Metern über Normal Null das Mittelmeer und Deutschland die Nordsee verwendet und beide eine Differenz von 27 Zentimeter aufweisen, aber man hat die Differenz mit dem verkehrten Vorzeichen eingerechnet.

Die Kritikalität der richtigen Anwendung der Grundrechenarten war ein diesem Fall entscheidend.