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