Bundesamt
für Bevölkerungsschutz
und Katastrophenhilfe

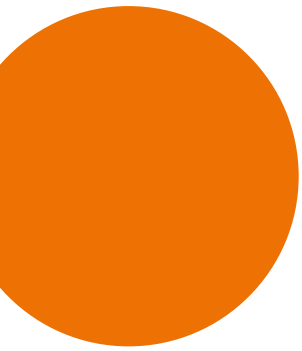
10 Jahre „KRITIS-Strategie“

Einblicke in die Umsetzung der
Nationalen Strategie zum Schutz Kritischer Infrastrukturen

Fachinformation

Praxis im Bevölkerungsschutz

Band 21



10 Jahre „KRITIS-Strategie“

Einblicke in die Umsetzung der Nationalen Strategie zum Schutz Kritischer Infrastrukturen

Herausgeber:
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)

unter Mitarbeit von:
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)
Bundesanstalt für Landwirtschaft und Ernährung (BLE)
Bundesanstalt Technisches Hilfswerk (THW)
Bundesinstitut für Bau-, Stadt- und Raumforschung (BBSR) im Bundesamt für Bauwesen und Raumordnung (BBR)
Bundesministerium der Finanzen (BMF)
Bundesministerium des Innern, für Bau und Heimat (BMI)
Bundesministerium für Bildung und Forschung (BMBF)
Bundesministerium für Umwelt, Naturschutz und nukleare Sicherheit (BMU)
Bundesministerium für Verkehr und Digitale Infrastruktur (BMVI)
Bundesministerium für Wirtschaft und Energie (BMWi)
Bundesnetzagentur (BNetzA)
Konferenz Nationaler Kultureinrichtungen (KNK), SicherheitsLeitfaden Kulturgut (SiLK)
Nationale Kontaktstelle für das Sendai Rahmenwerk der Vereinten Nationen beim BBK

Stand:
Februar 2020

Inhalt

Vorwort

Christoph Unger
Präsident des Bundesamtes für
Bevölkerungsschutz und Katastrophenhilfe

Sehr geehrte Leserinnen und Leser,

„In Deutschland ist die Versorgung der Bevölkerung und der Unternehmen mit Energie-, IT- und Transportdienstleistungen, Trinkwasser und vielen weiteren lebenswichtigen Einrichtungen sehr gut. Der Sicherheitsstandard und die Ausfallsicherheit Kritischer Infrastrukturen sind auf einem hohen Niveau. Angesichts teilweise neuer und wachsender Gefahren dürfen wir uns mit dem Erreichten jedoch nicht zufrieden geben. Der internationale Terrorismus, Naturereignisse, aber auch zunehmend komplexe Technologien stellen uns vor dauerhafte Herausforderungen."

Diese Worte fand der damalige Bundesinnenminister, Dr. Wolfgang Schäuble, anlässlich der Verabschiedung der Nationalen Strategie zum Schutz Kritischer Infrastrukturen durch das Bundeskabinett am 17. Juni 2009.

Im Grunde hat diese Aussage auch heute noch Bestand: Auch wenn die Versorgungssicherheit in Deutschland im internationalen Vergleich nicht zuletzt wegen hoher Sicherheitsstandards weiterhin einen Spitzenplatz einnimmt, stehen wir angesichts terroristischer und hybrider Bedrohungen, klimatischer Veränderungen oder systemischer Komplexitätssteigerungen nicht zuletzt im Zuge der Digitalisierung weiterhin vor großen Herausforderungen und dürfen es uns nicht bequem machen.

Insofern hat sich in den vergangenen 10 Jahren auf diesem Gebiet auch sehr viel verändert. Der Schutz Kritischer Infrastrukturen wurde als eines der zentralen Themen der Inneren Sicherheit aufgegriffen und hat sich als Eckpfeiler zum Schutz der Bevölkerung und ihrer Lebensgrundlagen etabliert. Dies zeigt sich nicht zuletzt darin, dass Maßnahmen zu ihrem Schutz Gegenstand der Gesetzgebung wurden und der Schutz Kritischer Infrastrukturen explizit als solcher benannt wird.

Als Meilenstein kann die Institutionalisierung gemeinsamer Arbeitsstrukturen zwischen den Ressorts auf Bundesebene sowie zwischen Bund und Ländern gewertet werden. Die Erkenntnis, dass der Schutz Kritischer Infrastrukturen als Querschnittsthema der koordinierten, ressort- und ebenenübergreifenden Kooperation bedarf, setzte sich im Verlauf der vergangenen Jahre durch und manifestierte sich in ressortübergreifenden Arbeitsgruppen auf Bundesebene sowie in einer etablierten Bund-Länder-Zusammenarbeit. Begleitet durch die öffentlich-private Partnerschaft von Staat und Betreibern im UP KRITIS verfügt der Schutz Kritischer Infrastrukturen in Deutschland über ein System von Kooperationsbeziehungen der wesentlichen Akteure, auf das alle Beteiligten durchaus stolz sein können.

Auch in methodischer Hinsicht hat sich der Blick auf Kritische Infrastrukturen weiterentwickelt: Von der Trennung des physischen Schutzes stationärer Anlagen und der IT-Sicherheit in Netzen zu einem integrierten Schutzsystem, von einer anlagenbezogenen Sichtweise zu einer mehr systemischen Betrachtung, von Kritischen Infrastrukturen als Ausgangspunkt zu kritischen Dienstleistungen war es ein längerer, manchmal verschlungener, manchmal auch anstrengender Weg. Letztlich hat es sich aber immer gelohnt!

Viele, wenn auch nicht alle Ergebnisse der Arbeit zum Schutz Kritischer Infrastrukturen sind im nun vorliegenden Bericht zur Umsetzung der Nationalen Strategie dokumentiert. Mit den ersten – noch „Strategie-losen" – Schritten zum Schutz Kritischer Infrastrukturen setzt er bereits vor Verabschiedung der Nationalen Strategie an und zeigt anhand von Beispielen die Entwicklung im Verständnis und im Vorgehen beim Schutz Kritischer Infrastrukturen in Deutschland.

Die Prognose des Bundesinnenministers 2009, die Strategie werde „das grundsätzliche Denken, Handeln und Verhalten in allen sicherheitspolitischen Fragestellungen zum Schutz Kritischer Infrastrukturen positiv beeinflussen", hat sich angesichts der hier dokumentierten Auswahl an Umsetzungsschritten durchaus bestätigt.

An der Erstellung des Berichtes haben viele Behörden aus verschiedenen Ressorts mitgearbeitet und dafür Beiträge zugeliefert. Ohne ihr Engagement und ihre Aktivitäten beim Schutz Kritischer Infrastrukturen und ohne ihre Bereitschaft, hierüber auch zu berichten, hätte diese Dokumentation nicht erstellt werden können. Für diese behörden- und ressortübergreifende Mitarbeit, die als solche bereits den querschnittlichen Charakter beim Schutz Kritischer Infrastrukturen unterstreicht, danke ich allen Beteiligten ausdrücklich.

Dieser erste Bericht versteht sich als Bericht des Bundes. Mein Wunsch wäre, die strukturellen Entwicklungen beim Schutz Kritischer Infrastrukturen aufzunehmen, indem Bund und Länder künftig gemeinsam über Fortschritte beim Schutz Kritischer Infrastrukturen berichten.

Aber zunächst wünsche ich Ihnen eine anregende Lektüre.

Bonn im Februar 2020

Christoph Unger

Kurzfassung

Quelle: Christoph Hetzmannseder / Moment / Getty Images

Die Anfänge des Schutzes Kritischer Infrastrukturen in Deutschland (→ Kapitel 1.1)

Erste Aktivitäten zum Schutz Kritischer Infrastrukturen wurden in Deutschland Ende der 1990er-Jahre unternommen. Mit der Einrichtung der ressortübergreifenden Arbeitsgruppe „AG KRITIS“ wurde 1997 auf Initiative des Bundesministeriums des Innern (BMI) nicht nur eine erste organisatorische Struktur für den Schutz Kritischer Infrastrukturen, sondern auch das bis heute geläufige Akronym „KRITIS“ geschaffen. Ein Jahr später entstand im Bundesamt für Sicherheit in der Informationstechnik (BSI) das erste Referat, das sich dem Schutz Kritischer Infrastrukturen widmete. In den nächsten Jahren erhielt das noch neue Politikfeld eine inhaltlich und konzeptionell breitere Ausrichtung: Nicht nur IT-Sicherheitsaspekte, sondern ein breiter Gefahrenansatz sollte zukünftig den Schutz Kritischer Infrastrukturen prägen. Im 2004 gegründeten Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) wurde daher eine weitere Organisationseinheit zum Schutz Kritischer Infrastrukturen in einer Bundesbehörde geschaffen. Eine Reihe methodischer Instrumente entstand in den Folgejahren, etwa das „Basisschutzkonzept“ (BMI 2005a; → Infobox 1) und ein Leitfaden zum Risiko und Krisenmanagement für Unternehmen und Behörden (aktuelle Version: BMI 2011a; → Kapitel 2.1.1). Programmatische Akzente setzte insbesondere der „Nationale Plan zum Schutz der Informationsinfrastrukturen“ (BMI 2005b) mit dem „Umsetzungsplan Bund“ für Bundesbehörden und dem „Umsetzungsplan KRITIS“ für Betreiber Kritischer Infrastrukturen (BMI 2007a).

Ein Strategischer Rahmen: Die „Nationale Strategie zum Schutz Kritischer Infrastrukturen (→ Kapitel 1.2)

Im Jahr 2007 begannen die Arbeiten an einer übergreifenden strategischen Grundlage für den Schutz Kritischer Infrastrukturen, die 2009 zur Verabschiedung der „Nationalen Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)“ (BMI 2009) durch das Bundeskabinett führten. Die Strategie sollte zum einen den bewährten, bereits praktizierten Ansätzen einen Rahmen geben, zum anderen Weiterentwicklungs- und Ergänzungsbedarf aufzeigen. Insbesondere in der steigenden gesellschaftlichen Abhängigkeit von (untereinander immer stärker vernetzten) Infrastruktursystemen und in einer neuen Qualität terroristischer Bedrohungen und Naturgefahren erkennt die Strategie zukünftige Herausforderungen und leitet daraus die Notwendigkeit ab, sich einem breiten Spektrum Kritischer Infrastrukturen und einem breiten Gefahrenspektrum zuzuwenden. Der All-Gefahren-Ansatz, der IT-Sicherheitsaspekte und den sogenannten „physischen Schutz“ verknüpft, bildet folglich ein Kernelement der KRITIS-Strategie. Ebenso prominent wird die bereits im „Umsetzungsplan KRITIS“ (BMI 2007a) angelegte Ausrichtung auf alle Phasen des Risiko- und Krisenmanagements platziert. Durchzogen wird die Strategie vom „kooperativen Ansatz“ als Form der Zusammenarbeit von Staat und Wirtschaft sowie dem grundsätzlichen Vorrang freiwilliger Selbstverpflichtung der Wirtschaft vor gesetzlicher Regelung. Im Umfeld der Entstehung der KRITIS-Strategie diskutierten Bund und Länder über die Einteilung von Sektoren Kritischer Infrastrukturen. Die daraus hervorgegangene, zwischen Bund und Ländern abgestimmte Sektorenliste wurde zwar letztlich nicht in der Strategie selbst veröffentlicht, sie ist aber eng mit ihr verbunden (→ Infobox 2). Die KRITIS-Strategie ist eher „Wegweiser“ denn „ausgebaute Straße“ für den Schutz Kritischer Infrastrukturen in Deutschland. Einzelne Schritte werden nicht detailliert beschrieben, sondern waren im Zuge der Umsetzung zu konkretisieren. Einblicke in diesen Prozess geben die nachfolgenden Kapitel des vorliegenden Umsetzungsberichts (→ Kapitel 2).

Entwicklung und Umsetzung methodischer Grundlagen (→ Kapitel 2.1)

Methodische Grundlagen beschreiben Vorgehensweisen für einen bestimmten Adressatenkreis und Anwendungsbereich und erfüllen damit unterschiedliche Funktionen im Kontext des Schutzes Kritischer Infrastrukturen: Sie konkretisieren einen Gegenstandsbereich, formulieren Erwartungen an einzelne Akteursgruppen, strukturieren die Zusammenarbeit zwischen ihnen und schaffen Schnittstellen zu bereits etablierten

Verfahren. Einige sind in bindende Vorgaben oder formale Instrumente eingeflossen, andere dienen unverbindlich als Orientierung. Dabei beginnen methodische Grundlagen bereits in der Entwicklungsphase, Wirkung zu entfalten: Sie zwingen zu einer intensiven Auseinandersetzung mit dem betreffenden Sachverhalt und waren oft Ausgangspunkt für akteursübergreifende Kooperationen.

Es ist Aufgabe der Betreiber Kritischer Infrastrukturen - seien es Unternehmen oder Behörden - für einen sicheren und zuverlässigen Betrieb ihrer Anlagen und Einrichtungen zu sorgen. Der Leitfaden für ein einrichtungsbezogenes Risiko- und Krisenmanagement für Betreiber Kritischer Infrastrukturen aus allen Branchen (BMI 2011a) gehört daher zu den zentralen methodischen Grundlagen des Schutzes Kritischer Infrastrukturen (→ Kapitel 2.1.1). Die im Leitfaden vorgestellte Methodik orientiert sich an anerkannten Standards, die in enger Zusammenarbeit mit Betreibern auf den Schutz Kritischer Infrastrukturen zugeschnitten wurden. Darauf aufbauend sind eine Reihe branchenspezifischer Leitfäden sowie ein Verfahren für die strukturierte Zusammenarbeit zwischen Betreibern und staatlichen Stellen beim Risiko- und Krisenmanagement entstanden (→ Kapitel 2.5.2 und Kapitel 2.5.4).

Damit sich Betreiber Kritischer Infrastrukturen ihrer besonderen Verantwortung bewusst werden und staatliche Stellen ihre Ansprechpartner auf Betreiberseite ausfindig machen können, wurde eine Methodik zu Identifizierung Kritischer Infrastrukturen entwickelt und als Leitfaden veröffentlicht (BBK 2019a, → Kapitel 2.1.2). Da es u. a. von der Betrachtungsebene abhängt, ob eine konkrete Anlage oder Einrichtung als kritisch bewertet wird, kann die hier beschriebene Methodik auf den jeweiligen Anwendungskontext angepasst werden. Ein Anwendungsfall auf Bundesebene ist die in der *BSI-Kritisverordnung* geregelte Identifizierung von Kritischen Infrastrukturen im Sinne des *IT-Sicherheitsgesetzes* (→ Infobox 16). Auf Basis der Haager Konvention werden Kulturgüter mit besonderer identitätsstiftender Bedeutung identifiziert (→ Infobox 3).

Die Risikoanalyse im Bevölkerungsschutz des Bundes untersucht, welche Auswirkungen unterschiedliche, in Form von Szenarien beschriebene Gefahrenereignisse auf die Bevölkerung und ihre Lebensgrundlagen hätten (→ Kapitel 2.1.3). Die Folgen z. B. von Stürmen oder Pandemien hängen maßgeblich davon ab, wie sehr kritische Dienstleistungen beeinträchtig werden (vgl. BT-Drs. 17/12051; BT-Drs. 18/208). Im Rahmen der Risikoanalyse wird daher nach Festlegung des Szenarios zunächst die Betroffenheit Kritischer Infrastrukturen untersucht, um darauf aufbauend eine Gesamtbetrachtung der Auswirkungen vorzunehmen. Ausfälle Kritischer Infrastrukturen haben somit als „indirekte“ Auswirkungen eines Ereignisses ihren festen Platz in der Methode für die Risikoanalyse im Bevölkerungsschutz.

In einem „Modellvorhaben der Raumordnung“ wurden die Potenziale der Regionalplanung zur Risikovorsorge unter besonderer Berücksichtigung der Belange Kritischer Infrastrukturen untersucht (vgl. BMVI/BBSR 2015). Mit ihrer von der räumlichen Situation ausgehenden Herangehensweise an das Risikomanagement eröffnet die Raumplanung dem Schutz Kritischer Infrastrukturen eine sektorenübergreifende Perspektive. Sie kann sichtbar machen, wo, z. B. aufgrund der räumlichen Nähe unterschiedlicher Infrastrukturen, eine Fokussierung auf einzelne, branchenspezifische Sicherheitsvorschriften zu kurz greift oder einer ganzheitlichen Lösung im Weg stehen würde. Um die Möglichkeiten des vorsorgenden Risikomanagements, etwa in der Regionalplanung, nutzen zu können, bedarf es der Entwicklung entsprechender methodischer Grundlagen (→ Kapitel 2.1.4). Überlegungen zum Umgang mit Kritischen Infrastrukturen sind in das „Handbuch zur Ausgestaltung der Hochwasservorsorge in der Raumordnung“ eingeflossen (vgl. BMVI 2017; → Infobox 4).

Der Handlungsrahmen für den Schutz Kritischer Infrastrukturen (→ Kapitel 2.2)

Der Staat, so heißt es im Leitbild zur KRITIS-Strategie, „steuert primär moderierend, nötigenfalls normierend, die Maßnahmen zur Sicherung und zur Sicherstellung des Gesamtsystems sowie der Systemabläufe“ (BMI 2009, S. 2). Diesem Leitgedanken entsprechend lag und liegt der Schwerpunkt beim Schutz Kritischer Infrastrukturen

auf nichtregulativen Instrumenten. Ein übergreifendes „Gesetz zum Schutz Kritischer Infrastrukturen“ gibt es in Deutschland nicht. Allerdings wurden im Lauf der Zeit einzelne Aspekte des Schutzes Kritischer Infrastrukturen in Fachgesetzen festgeschrieben (→ Kapitel 2.2.1), sei es um Vorgaben von europäischer Ebene in deutsches Recht zu überführen oder um auf nationaler Ebene erkannten Regelungsbedarf zu decken. Die rechtlichen Regelungen mit explizitem Bezug zum Schutz Kritischer Infrastrukturen haben unterschiedliche Formen und Funktionen: Sie formulieren teilweise abstrakte Zielsetzungen, schreiben Befugnisse von Behörden fest oder machen konkrete Vorgaben für Betreiber. Insbesondere das 2015 in Kraft getretene *IT-Sicherheitsgesetz* hat als Artikelgesetz Spuren in vielen Fachgesetzen hinterlassen. Es hat den Bedarf ausgelöst, Aspekte seiner Umsetzung per Verordnung untergesetzlich zu regeln, und zudem die Entwicklung von Standards zur rechtssicheren Umsetzung in Gang gesetzt. Anhand des *Energiewirtschaftsgesetzes* lässt sich nachvollziehen, wie der allgemeine Rechtsrahmen zum Schutz Kritischer Infrastrukturen mit bereichsspezifischen Regelungen verknüpft wird (→ Infobox 5).

Normen und Standards werden zur Konkretisierung gesetzlicher Vorgaben genutzt, insbesondere hinsichtlich des abstrakten „Stands der Technik“, auf den Gesetze häufig Bezug nehmen. Diese Funktion erfüllen sie auch im Kontext des Schutzes Kritischer Infrastrukturen (→ Kapitel 2.2.2): Sie kommen in der einen oder anderen Form in allen Sektoren Kritischer Infrastrukturen zur Anwendung, enthalten technische Spezifikationen, beschreiben Verfahrensweisen oder organisatorische Abläufe. Viele Normen und Standards haben ganz generell zuverlässige und sichere Abläufe zum Ziel, manche beziehen sich aber auch ganz ausdrücklich auf den Schutz Kritischer Infrastrukturen. Doch nicht nur die fertigen Normen und Standards entfalten Wirkung: Bei ihrer Erarbeitung werden mitunter neue Themen in einem strukturierten Prozess von Expertenseite beleuchtet und gemeinsame Positionen gefunden.

Lange bevor sich der Politikbereich „Schutz Kritischer Infrastrukturen“ etablierte, wurde die Aufrechterhaltung zentraler Versorgungsleistungen in definierten Krisensituationen Gegenstand gesetzlicher Regelungen (→ Kapitel 2.2.3): Die Vorsorgegesetze enthalten Regelungen zur Bewältigung von Versorgungsengpässen in Friedenszeiten, während die Sicherstellungsgesetze auf Versorgungskrisen im Spannungs- oder Verteidigungsfall ausgelegt sind (Art. 80a oder 115a GG). Die in diesen Gesetzen adressierten Versorgungsbereiche korrespondieren zu einem gewissen Grad mit den Sektoren Kritischer Infrastrukturen. Ein Beispiel für eine Rechtsnorm, die Versorgungskrisen sowohl in Friedenszeiten als auch im Spannungs- und Verteidigungsfall adressiert, ist das 2017 novellierte Ernährungsvorsorge- und -sicherstellungsgesetz (→ Infobox 6).

Schutz Kritischer Infrastrukturen als inhaltliches Querschnittsthema (→ Kapitel 2.3)

Der Schutz Kritischer Infrastrukturen hat vielfältige Berührungspunkte mit anderen Politikbereichen, insbesondere aufgrund seines breiten Gegenstandsbereichs über alle neun Sektoren und aufgrund des All-Gefahren-Ansatzes. Aus diesem Grund finden sich Teilaspekte des Schutzes Kritischer Infrastrukturen auch in weiteren politischen Strategiedokumenten wieder und werden dort kontextspezifisch aufgegriffen (→ Kapitel 2.3.1). Einige der betreffenden Strategien konzentrieren sich auf Ausschnitte aus dem Gefahrenspektrum. Beispielsweise ist die „Cyber-Sicherheitsstrategie für Deutschland“ (BMI 2016a) auf Gefahren ausgerichtet, die im Cyber-Raum entstehen (→ Infobox 7), während die „Deutsche Anpassungsstrategie an den Klimawandel“ (BReg 2008) die Auswirkungen des Klimawandels in den Blick nimmt (→ Infobox 8). Andere konkretisieren die Herangehensweise beim Schutz Kritischer Infrastrukturen innerhalb einer Branche, z. B. die „Sicherheitsstrategie für die Güterverkehrs- und Logistikwirtschaft“ (BMVI 2014, → Infobox 9). Einen besonders großen Rahmen spannt das „Sendai Rahmenwerk für Katastrophenvorsorge“ der Vereinten Nationen auf (NKS 2019): Es umschließt das gesamte All-Gefahrenspektrum und adressiert den Schutz Kritischer Infrastrukturen als Teil der gesamtgesellschaftlichen Katastrophenvorsorge (→ Infobox 10).

Die „Konzeption Zivile Verteidigung“ (BMI 2016b) bildet den zivilen Teil der Gesamtverteidigung ab, fokussiert also auf Gefahren, die im Zusammenhang mit bewaffneten Konflikten und hybriden Bedrohungslagen auftreten können (→ Kapitel 2.3.2). Aspekte des Schutzes Kritischer Infrastrukturen sind integraler Bestandteil der Konzeption und treten dementsprechend auch an mehreren Stellen zutage. So können etwa Vorgaben zur Aufrechterhaltung von Staats- und Regierungsfunktionen als gefahrenspezifische Maßnahmen für den Schutz Kritischer Infrastrukturen im Sektor *Staat und Verwaltung* aufgefasst werden (→ Infobox 11).

Um gezielt den wissenschaftlichen Erkenntnisgewinn zum Nutzen des Schutzes Kritischer Infrastrukturen fördern zu können, ist eine Säule des Rahmenprogramms „Forschung für die zivile Sicherheit“ diesem Themenfeld gewidmet (BMBF 2018, → Kapitel 2.3.3). In allen Forschungsprojekten werden Anwender, wie Behörden und Organisationen mit Sicherheitsaufgaben oder Infrastrukturbetreiber, eng einbezogen, um die Praxistauglichkeit der hier entwickelten Lösungen sicherzustellen. Zudem werden gesellschaftliche, rechtliche oder ethische Fragen von vornherein berücksichtigt (→ Infoboxen 12, 13 und 14). Im Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit werden Forschungsvorhaben mit Bezug zum Schutz Kritischer Infrastrukturen gefördert, die spezifisch auf IT-Sicherheit ausgerichtet sind (ITS|KRITIS, → Infobox 15).

Schutz Kritischer Infrastrukturen als akteursübergreifende Aufgabe (→ Kapitel 2.4)

„Zur Stärkung des Schutzes Kritischer Infrastrukturen bedarf es“, so heißt es in der KRITIS-Strategie (BMI 2009, S. 12), „einer intensiven Zusammenarbeit, Abstimmung und Information zwischen und unter den Partnern und Akteuren“. Grund dafür ist die ausgesprochen vielfältige Akteurslandschaft, die den Schutz Kritischer Infrastrukturen ausmacht: Verantwortlichkeiten sind zwischen Betreibern und staatlichen Stellen aufgeteilt, fachliche Zuständigkeiten liegen bei mehreren Ressorts, Aufsichtsfunktionen werden von Behörden auf unterschiedlichen administrativen Ebenen wahrgenommen, Betreiber Kritischer Infrastrukturen sind in diversen Verbänden organisiert, zahlreiche Forschungseinrichtungen widmen sich unterschiedlichen Teilfragen des Schutzes Kritischer Infrastrukturen – und damit sind immer noch nicht alle in der KRITIS-Strategie unter der Überschrift „kooperativer Ansatz“ aufgeführten Akteursgruppen genannt (→ Kapitel 1.2). Dem Auftrag zur Zusammenarbeit sind die Beteiligten im Laufe der Zeit in vielfältiger Weise nachgekommen.

Der Schutz Kritischer Infrastrukturen wird als gesamtstaatliche Aufgabe wahrgenommen. Die Zusammenarbeit zwischen Behörden von Bund und Ländern nimmt dabei eine zentrale Stellung ein, die Schaffung entsprechender Strukturen ist ein wichtiger Schritt zur Umsetzung der KRITIS-Strategie (→ Kapitel 2.4.1). Zeitgleich zur Verabschiedung der KRITIS-Strategie wurde der Schutz Kritischer Infrastrukturen in der Fortschreibung (2008/2009) des „Programms Innere Sicherheit“ der Innenministerkonferenz verankert (IMK 2009). Auch das Programm bewertet die Intensivierung der Zusammenarbeit aller staatlichen Ebenen als erforderlich. Bereits seit 2012 finden regelmäßig informelle Arbeitstreffen unter Beteiligung der Innenressorts von Bund und Ländern statt. Diese haben sich als Plattform des Austauschs zu ebenenübergreifenden Fragen des Schutzes Kritischer Infrastrukturen bewährt und werden nun stärker an die formale Gremienstruktur der Innenressorts angebunden.

Die partnerschaftliche Zusammenarbeit von staatlichen Stellen und vorwiegend privatwirtschaftlichen Betreibern genießt beim Schutz Kritischer Infrastrukturen einen hohen Stellenwert. Institutioneller Ausdruck dessen ist insbesondere der UP KRITIS, eine öffentlich-private Kooperation zwischen Betreibern Kritischer Infrastrukturen, deren Verbänden und den zuständigen staatlichen Stellen (→ Kapitel 2.4.2; UP KRITIS 2014a). Die Zusammenarbeit im UP KRITIS hat zum einen die Form eines strukturierten Informationsaustauschs über Cyber-Sicherheitsvorfälle, Auffälligkeiten und die aktuelle IT-Bedrohungslage (operativ-taktische Zusammenarbeit). Zum anderen werden branchenspezifische und branchenübergreifende Fragestellungen in Branchen- und Themenar-

beitskreisen bearbeitet (strategisch-konzeptionelle Zusammenarbeit).

Bei der Implementierung des *IT-Sicherheitsgesetzes* fungiert der UP KRITIS als Schnittstelle zwischen staatlichen Stellen und den Betreibern Kritischer Infrastrukturen (BSI 2017a, → Infobox 16). Diese Funktion erfüllte er u. a. bei der Erarbeitung der Rechtsverordnung zur Identifizierung von Kritischen Infrastrukturen im Sinne des Gesetzes. Die Branchenarbeitskreise des UP KRITIS waren die erste Anlaufstelle, als die Fachexpertise von Behörden- und Betreiberseite in sogenannten „Kernteams" gebündelt werden musste, um die Parameter der Verordnung branchenspezifisch anwendbar zuzuschneiden. Darüber hinaus haben sich die Branchenarbeitskreise des UP KRITIS als ideales Umfeld für die Erarbeitung „branchenspezifischer Sicherheitsstandards" erwiesen. Mit deren Hilfe werden die Vorgaben des *IT-Sicherheitsgesetzes* nach dem „Stand der Technik" anwenderspezifisch konkretisiert (→ Kapitel 2.2.2).

Die Zusammenarbeit zwischen Akteuren des Bevölkerungsschutzes und den Betreibern Kritischer Infrastrukturen ist für die Risikominderung bzw. Krisenbewältigung entscheidend. Deshalb ergänzt das Verfahren des sogenannten „Integrierten Risikomanagements" (BBK 2018a) die jeweilige Einzelperspektive der Akteure um eine Gesamtbetrachtung. Es legt den Schwerpunkt auf die Schnittstellen und den gegenseitigen Austausch von Informationen, Erkenntnissen und Ergebnissen (→ Kapitel 2.4.3). Das inzwischen mehrfach auf seine Praxistauglichkeit getestete Verfahren ist jüngst in Form einer DIN-Spezifikation formalisiert worden (DIN SPEC 91390:2019-12). Ein Beitrag zur Entwicklung des Integrierten Risikomanagements wurde im Forschungsprojekt „KIRMin" geleistet (→ Infobox 17).

Das Zusammenspiel von betreiberseitigem und behördlichem Krisenmanagement einzuüben, ist Gegenstand der Länder- und Ressortübergreifenden Krisenmanagementübung (Exercise) „LÜKEX" (→ Kapitel 2.4.4). Unter der Annahme außergewöhnlicher Krisenszenarien werden Vertreterinnen und Vertreter von Behörden und von Betreibern Kritischer Infrastrukturen in ganz besonders fordernde Interaktionssituationen gebracht. Es geht darum, die Fähigkeiten von Mitarbeiterinnen und Mitarbeitern weiterzuentwickeln, Kommunikationswege mit anderen Übungsbeteiligten „einzuschleifen" und ganz allgemein die Umsetzung von Verfahren des Krisenmanagements gemeinsam zu erproben und zu verbessern. Die Übungen werden systematisch ausgewertet und dokumentiert (vgl. BBK 2019b).

Ein Szenario, dem in den letzten Jahren besonders viel Aufmerksamkeit von besonders vielen Akteuren entgegengebracht wurde, ist der „großflächige, langanhaltende Stromausfall" (→ Kapitel 2.4.5). In Deutschland ist nicht nur eine Stelle für die Notfallplanung für Stromausfallszenarien zuständig. Vielmehr setzen eine Vielzahl staatlicher Akteure in Bund, Ländern und Kommunen sowie Betreiber Kritischer Infrastrukturen jeweils in eigener Zuständigkeit Maßnahmen um. Dieses Maßnahmengefüge aus der Vogelperspektive zu betrachten, Wissensstände laufend zu erfassen, Arbeitshilfen zu erarbeiten und ggf. auch Planungs- und Informationslücken in der Notfallplanung für Stromausfall zu erkennen, ist Sinn und Zweck des „Rahmenkonzepts Notstrom". Zu seinen Bausteinen gehören u. a. Empfehlungen für die Einrichtung einer Notstromversorgung (BBK 2015, → Infobox 18) und die Treibstoffversorgung bei Stromausfall (BBK 2017, → Infobox 19), die Weiterentwicklung von Notstromkapazitäten (THW 2014, → Infobox 20) und die Information der Bevölkerung (BBK 2019c, → Infobox 21).

Schutz Kritischer Infrastrukturen als sektorale Aufgabe (→ Kapitel 2.5)

Beim Schutz Kritischer Infrastrukturen wird der Berücksichtigung sektorenübergreifender Verknüpfungen und Abhängigkeitsbeziehungen viel Bedeutung beigemessen. Dass viele Ansätze und Aktivitäten in diesem Kontext dennoch eine sektorale Ausrichtung aufweisen (→ Infobox 2), steht dazu allerdings nicht im Widerspruch. Vielmehr gibt es einen Bedarf, übergeordnete Herangehensweisen für unterschiedliche sektorale Kontexte zu konkretisieren und grundsätzliche Fragestellungen in sektorenspezifischer Weise zu bearbeiten. Beispielsweise wurden vielfach Methoden zur Anwendung innerhalb eines Sektors, einer Branche oder sogar eines bestimmten Ein-

richtungstyps zugeschnitten und auch außerhalb des UP KRITIS haben sich sektorale Netzwerke mit Bezug zum Schutz Kritischer Infrastrukturen gebildet.

Unter dem Eindruck folgenschwerer Ereignisse, u. a. dem Brand der Herzogin Anna Amalia Bibliothek (2004) und des Elbehochwassers (2002), begannen im Jahr 2006 initiiert durch die Konferenz Nationaler Kultureinrichtungen (KNK) die Arbeiten am „SicherheitsLeitfaden Kulturgut“ (SiLK). Das internetgestützte Beratungs- und Evaluierungsinstrument deckt Themen rund um den Schutz von Kulturgütern ab und richtet sich an Museen, Bibliotheken und Archive als Betreiber wichtiger Einrichtungen im KRITIS-Sektor *Kultur und Medien* (→ Kapitel 2.5.1).

Zur Sensibilisierung und Unterstützung von Betreibern und Behörden mit Aufgaben im Sektor *Wasser* hat das BBK zwei Empfehlungen zur Sicherheit der Trinkwasserversorgung herausgegeben (→ Kapitel 2.5.2). Der erste Teil unterstützt die Aufgabenträger der Wasserversorgung in den Kommunen bei der Untersuchung und Bewertung von Risiken, insbesondere im Zusammenhang mit außergewöhnlichen Gefahrenlagen (BBK 2019d). Der zweite Teil beschreibt die Schritte zur Erarbeitung einer Notfallvorsorgeplanung (BBK 2019e).

Bei der Ausgestaltung des Risikomanagements im Sektor *Finanz- und Versicherungswesen* nehmen die Rundschreiben der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) eine zentrale Rolle ein (→ Kapitel 2.5.3). Sie definieren Mindestanforderungen an das Risikomanagement (BaFin 2017) im Kredit- und Finanzdienstleistungswesen oder konkretisieren in den bank-, versicherungs- und kapitalverwaltungsaufsichtlichen Anforderungen auch IT-Sicherheitsaspekte für Betreiber Kritischer Infrastrukturen (BaFin 2018a; BaFin 2019a; BaFin 2019b; → Kapitel 2.5.3).

Für Krankenhäuser als Kritische Infrastrukturen im Sektor *Gesundheit* wurden methodische Grundlagen zum Risiko- und Krisenmanagement in mehreren Veröffentlichungen adressatenspezifisch zugeschnitten. Unter Beteiligung von Expertenkreisen und Praxispartnern entstand zunächst ein Leitfaden für das Risikomanagement im Krankenhaus (BBK 2008). Im Leitfaden „Risikoanalyse Krankenhaus-IT“ (BSI 2013a) werden IT-Sicherheitsfragen im Klinikbetrieb aufbereitet. Das für 2020 angekündigte Handbuch zur Krankenhausalarm- und -einsatzplanung wird zu planerischen Maßnahmen anleiten, um die Kapazität und Funktionalität von Krankenhäusern in Schadenslagen aufrechtzuerhalten (→ Kapitel 2.5.4).

Im BMVI-Expertennetzwerk werden die Kompetenzen und das Know-how von sieben Ressortforschungseinrichtungen und Fachbehörden im Geschäftsbereich des Bundesministeriums für Verkehr und digitale Infrastruktur (BMVI) gebündelt und auch Fragen des Schutzes Kritischer Infrastrukturen im Sektor *Transport und Verkehr* behandelt. In unterschiedlichen Themenfeldern werden z. B. die aktuellen und in Zukunft zu erwartenden Auswirkungen von klimatisch bedingten Extremereignissen auf unterschiedliche Verkehrsträger untersucht und Anpassungsoptionen entwickelt (→ Kapitel 2.5.5).

Grenzüberschreitende Zusammenarbeit beim Schutz Kritischer Infrastrukturen (→ Kapitel 2.6)

Die Notwendigkeit einer grenzüberschreitenden Kooperation im europäischen Raum spiegelt sich schon in drei der vier vertraglich vereinbarten Grundfreiheiten des europäischen Binnenmarktes wider: in der Dienstleistungsfreiheit, im freien Warenverkehr und im freien Kapital- und Zahlungsverkehr als konstitutionelle Grundlage der Europäischen Union. Um z. B. die Funktionsfähigkeit der Transeuropäischen Verkehrs-, Energie- und Telekommunikationsnetze als Teil des Binnenmarktes sicherzustellen, ist ein gemeinsames Grundverständnis aller Mitgliedstaaten über Infrastruktursicherheit unverzichtbar. Als Antwort auf die Terroranschläge vom 11. September 2001 auf der einen Seite und die Herausforderungen durch die Digitalisierung auf der anderen Seite entwickelte die Europäische Kommission sektorübergreifende Initiativen zum Schutz europäischer bzw. nationaler kritischer Infrastrukturen und beeinflusste insbesondere mit der „EPSKI-Richtlinie“ (RL 2008/114/EG) und der „NIS-Richtlinie“ (RL 2016/11487/EU) auch die nationale Gesetzgebung (→ Kapitel 2.6.1).

Besonderen Stellenwert hat auch die bilaterale Zusammenarbeit, die sich häufig im Rahmen gegenseitiger Verträge, Abkommen oder Absichtserklärungen vollzieht und in Arbeitsprogrammen konkretisiert wird. Umfang und Intensität der Zusammenarbeit variieren und reichen, je nach Vereinbarung, von einem Informations- und Erfahrungsaustausch über einzelne konkrete Projekte bis zu mehrjährigen Schulungs- und Ausbildungsprogrammen. In der 2008 begründeten Kooperation im „D-A-CH-Format“ tauschen sich Vertreterinnen und Vertreter aus Deutschland, Österreich und der Schweiz zu programmatischen Überlegungen, methodischen Vorgehensweisen und konkreten Umsetzungsmaßnahmen aus und diskutieren über Unterschiede und Gemeinsamkeiten beim Schutz Kritischer Infrastrukturen (→ Kapitel 2.6.2).

Nicht zuletzt ist die Zusammenarbeit in internationalen Organisationen ein wichtiger Baustein, um den Schutz Kritischer Infrastrukturen auch auf nationaler Ebene zu stärken (→ Kapitel 2.6.3). Deutschland ist Mitglied internationaler Organisationen wie der North Atlantic Treaty Organization (NATO) sowie der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) und beteiligt sich auch in diesem Rahmen an der Weiterentwicklung des Schutzes Kritischer Infrastrukturen.

1

Kapitel

Quelle: domin_domin / E+ / Getty Images

Von den Anfängen des Schutzes Kritischer Infrastrukturen zur Nationalen Strategie

Die vorliegende Veröffentlichung gibt schwerpunktmäßig Einblicke in die Aktivitäten, die zur Umsetzung der „Nationalen Strategie zum Schutz Kritischer Infrastrukturen" – kurz: KRITIS-Strategie (BMI 2009) – unternommen wurden. Als die Strategie verabschiedet wurde, lagen die ersten Schritte zum Schutz Kritischer Infrastrukturen in Deutschland allerdings schon mehr als zehn Jahre zurück. Bereits im Vorfeld wurde über die strategische Ausrichtung und zentrale Konzepte des Schutzes Kritischer Infrastrukturen diskutiert und auch das institutionelle Gefüge des Politikfelds hat seine Wurzeln in dieser Zeit (→ Kapitel 1.1). Die KRITIS-Strategie basiert auf diesen Vorarbeiten und steht in vielerlei Hinsicht damit in Beziehung – z. B. indem sie bereits bestehende Kooperationsformen fortschreibt, zuvor getrennten Verfahren einen gemeinsamen Rahmen gibt, aber auch frühere strategische Grundlagen ablöst (→ Kapitel 1.2). Auf diese Weise lenken die nachfolgenden Ausführungen den Blick auf die „Gewordenheit" des Schutzes Kritischer Infrastrukturen und bilden den Hintergrund für die Beiträge in → Kapitel 2.

1.1 Die Anfänge des Schutzes Kritischer Infrastrukturen in Deutschland

Vielfach wird der Beginn des Schutzes Kritischer Infrastrukturen als eigenständiges Themenfeld mit der so genannten Jahrtausendproblematik („Y2K"), den informationstechnischen Herausforderungen des Übergangs vom 20. in das 21. Jahrhundert, oder mit der veränderten sicherheitspolitischen Lage nach den Terroranschlägen vom 11. September 2001 in Verbindung gebracht. Natürlich waren dies auch Marksteine beim Schutz Kritischer Infrastrukturen in Deutschland, jedoch finden sich erste Spuren einer systematischen Befassung bereits in den späten 1990er-Jahren. International gingen zu diesem Zeitpunkt Impulse von der Veröffentlichung des Abschlussberichts einer Expertenkommission in den USA aus. Der Bericht mit dem Titel „Critical Foundations" gab nicht nur vielfach Anstoß zur Befassung mit dem fortan als „Schutz Kritischer Infrastrukturen" bezeichneten Themenfeld, auch der Begriff selbst geht auf die Arbeiten der Expertenkommission, der President's Commission on Critical Infrastructure Protection, zurück (PCCIP 1997).

Im Jahr 1997 wurde im Bundesministerium des Innern (BMI) eine ressortübergreifende Arbeitsgruppe zum Thema Schutz Kritischer Infrastrukturen eingerichtet. Damit wurde nicht nur die erste organisatorische Struktur zum Thema geschaffen, sondern mit deren abkürzender Bezeichnung „AG KRITIS" auch das nachfolgend in Deutschland verwendete Akronym „KRITIS" für „Kritische Infrastruktur(en)" eingeführt. Die AG KRITIS hatte die Aufgabe, Bedrohungsszenarien aufzuzeigen, über die Informationstechnik angreifbare Schwachstellen in den Infrastrukturen zu identifizieren und Möglichkeiten zur Vermeidung oder Verminderung potentieller Schäden zu erarbeiten. „Kritische Infrastrukturen" wurden damals als Organisationen und Einrichtungen mit (lebens-)wichtiger Bedeutung für das staatliche Gemeinwesen definiert, bei deren Ausfall oder Störungen für größere Bevölkerungsgruppen nachhaltig wirkende Versorgungsengpässe oder andere dramatische Folgen eintreten. Die AG KRITIS legte sich auf sieben Sektoren fest (→ Infobox 2). Mit Vorlage des Abschlussberichtes Mitte des Jahres 2000 endete die Arbeit der AG. Ihren organisatorischen Niederschlag fand sie aber bereits 1998, als im Bundesamt für Sicherheit in der Informationstechnik (BSI) das erste Referat zum „Schutz KRITIS" auf der Bundesebene geschaffen wurde.

Als Reaktion auf die Anschläge vom 11. September 2001 und nach Sicherheitsgesprächen zwischen dem Bundesinnenminister und Betreibern Kritischer Infrastrukturen wurde 2002 im BMI eine ressortübergreifende Projektgruppe KRITIS (PG KRITIS) eingerichtet. Neben gemeinsamen Gefährdungseinschätzungen und der Verständigung über Schutzmaßnahmen einigte sich die PG KRITIS in Anlehnung an die Vorarbeiten aus der AG KRITIS auf eine Definition des Begriffs „Kritische Infrastrukturen" und die Einteilung von nunmehr acht Sektoren (→ Infobox 2). Zwar wurde der Schutz Kritischer Infrastrukturen damals in die Anti-Terror-Gesamtstrategie der Bundesregierung eingebunden, allerdings bezogen sich die Aktivitäten auch zu diesem Zeitpunkt auf ein breites Gefahrenspektrum. Inhaltlich bewegte sich der Schutz Kritischer Infrastrukturen zwischen Fragen des sogenannten „phy-

sischen Schutzes“ und der IT-Sicherheit, also dem Schutz vor Gefahren, die sich speziell aus der zunehmenden informationstechnischen Vernetzung der Infrastrukturen ergeben. So wurden 2001/2002 im Auftrag des BSI Analysen erstellt, um einen Überblick über die (dann noch sieben) KRITIS-Sektoren zu erhalten, kritische Prozesse zu identifizieren und deren IT-Abhängigkeiten und Verwundbarkeiten aufzuzeigen. Im Ergebnis wurde zu dieser Zeit ein lediglich geringer Handlungsbedarf bezüglich IT-Gefahren gesehen. Vielmehr wurde ein hohes Gefährdungspotenzial mit Blick auf physische Bedrohungen diagnostiziert.

Ebenfalls im Jahr 2002 greift die von der Innenministerkonferenz (IMK) verabschiedete „Neue Strategie zum Schutz der Bevölkerung in Deutschland“ (BBK 2010) das Thema Schutz Kritischer Infrastrukturen auf und stellt das Themenfeld in den Kontext des sich zu diesem Zeitpunkt neuaufstellenden Bevölkerungsschutzes. Parallel wird in der Akademie für Krisenmanagement, Notfallplanung und Zivilschutz (AKNZ) eine Projektgruppe KRITIS eingerichtet. Die Arbeiten an der Studie „Risiken für Deutschland“ (BBK 2005), die sich ausführlich mit der Bedeutung des Schutzes Kritischer Infrastrukturen für den Bevölkerungsschutz auseinandersetzt, beginnen. Nach Gründung des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe (BBK) im Jahr 2004 wird die Projektgruppe in das „Zentrum Schutz Kritischer Infrastrukturen“ im BBK überführt und damit neben dem BSI eine zweite Organisationseinheit mit dem Themenschwerpunkt Schutz Kritischer Infrastrukturen in einer Bundesbehörde geschaffen. Das BBK wird, so heißt es 2003 in der Begründung zum *Gesetz über die Errichtung des BBK*, mit der „planerischen Vorsorge zum Schutz der Bevölkerung und kritischer Infrastrukturen“ beauftragt, „soweit nicht Fragen der informationstechnischen Abhängigkeit von kritischen Infrastrukturen“ betroffen sind, die in die Zuständigkeit des BSI fallen (vgl. BT-Drs. 15/2286). Die beiden inhaltlichen Schwerpunkte, physischer Schutz und IT-Sicherheit, kommen von nun an auch institutionell in der Arbeit zweier Behörden mit unterschiedlichem Aufgabenprofil zum Ausdruck; gleichzeitig prägt die intensive Zusammenarbeit zwischen BBK und BSI die Entwicklung des Politikfelds Schutz Kritischer Infrastrukturen.

Empfehlungen zum sektorübergreifenden, physischen Schutz Kritischer Infrastrukturen wurden erstmalig 2005 im sogenannten „Basisschutzkonzept“ veröffentlicht (BMI 2005a; → Infobox 1). Neben einer Herangehensweise an die Analyse potenzieller Gefährdungen enthält das Basisschutzkonzept Vorschläge für bauliche, organisatorische, personelle und technische Schutzmaßnahmen. Zwei Jahre später folgte die erste Ausgabe des Leitfadens „Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement“ (BMI 2007b; aktuelle Version: BMI 2011a; → Kapitel 2.1.1). In diesem Leitfaden für Unternehmen und Behörden werden methodische Grundlagen für den Aufbau und die Weiterentwicklung von Risiko- und Krisenmanagementstrukturen vorgestellt und von Beispielen und Checklisten begleitet. Der 2005 vom BMI herausgegebene „Nationale Plan zum Schutz der Informationsinfrastrukturen“ (NPSI, BMI 2005b) fokussierte auf die Informationsinfrastrukturen. Der NPSI wurde für die Adressatengruppen Betreiber Kritischer Infrastrukturen und Bundesbehörden mit einem „Umsetzungsplan KRITIS“ (BMI 2007a) und dem „Umsetzungsplan Bund“ (aktuelle Version: BMI 2017) operationalisiert. Der Umsetzungsplan KRITIS war der offizielle Startschuss für die Institutionalisierung des heutigen „UP KRITIS“ (UP KRITIS 2014a; → Kapitel 2.4.2), einer Kooperation zwischen staatliche Stellen, Betreibern und Fachverbänden mit dem Ziel, den Schutz der Kritischen Infrastrukturen branchen- und sektorenübergreifend zu verbessern.

Auf Grundlage eines Beschlusses des Arbeitskreises V der IMK wurde 2007 eine länderoffene Arbeitsgruppe unter dem Vorsitz des Bundes eingerichtet, um Empfehlungen zur Zusammenarbeit zwischen Bund und Ländern zum Schutz Kritischer Infrastrukturen zu erstellen. Die Vorlage des Berichtes im Herbst 2010 wurde von der Einschätzung der Arbeitsgruppe begleitet, dass es sich beim Schutz Kritischer Infrastrukturen um eine fortlaufende Aufgabe handele, für die über den Auftrag der Arbeitsgruppe hinausgehender, vor allem koordinierender Handlungsbedarf bestehe. Damit wurde die Basis für eine Verstetigung des Schutzes Kritischer Infrastrukturen auch über die Verwaltungsebenen hinweg gelegt (→ Kapitel 2.4.1).

In der Europäischen Union (→ Kapitel 2.6.1) nahm das Thema Schutz Kritischer Infrastrukturen spätestens 2004 deutlich Fahrt auf. Die Veröffentlichung von Mitteilungen der Kommission zum Schutz kritischer Infrastrukturen im Rahmen der Terrorismusbekämpfung (KOM 2004) und das „Europäische Programm für den Schutz kritischer Infrastrukturen" (EPSKI, KOM 2006) haben nicht nur politisch-strategisch, sondern auch rechtlich die Rahmenbedingungen beim Schutz Kritischer Infrastrukturen in Deutschland und den anderen Mitgliedstaaten nachhaltig beeinflusst.

Infobox 1: Das Basisschutzkonzept

Mitte 2004 wurde durch das BMI angeregt, ein branchenübergreifendes Konzept insbesondere für den „physischen Schutz" von Einrichtungen und Anlagen zu erarbeiten. Ergebnis ist der Leitfaden „Schutz Kritischer Infrastrukturen - Basisschutzkonzept. Empfehlungen für Unternehmen" (BMI 2005a), kurz: das Basisschutzkonzept. Es umfasst im Grunde klassische Maßnahmen. Diese waren zwar in Teilen schon in gesetzlichen Quellen wie der *Störfall-Verordnung* oder dem *Aktiengesetz* beschrieben, wurden aber hiermit einem breiteren Adressatenkreis zugänglich gemacht. Auch wenn dem Basisschutzkonzept ein All-Gefahren-Ansatz zugrunde liegt, lässt sich ein Schwerpunkt im Bereich terroristischer Bedrohungen bzw. Kriminalität ausmachen – was angesichts der zeitlichen Nähe seiner Veröffentlichung zu den Terroranschlägen von Madrid im März 2004 nicht verwundert.

Im Leitfaden wird „Basisschutz" als „Mindestschutz" (BMI 2005a, S. 18) verstanden und grundsätzlich ein generalisierender, auf möglichst breite Anwendbarkeit ausgelegter Ansatz verfolgt. Zwar werden Schritte für einen strukturierten Analyse- und Planungsprozess beispielhaft aufgelistet, Risikofaktoren erläutert und Gefahrenarten beschrieben, doch auch ein Fragenkatalog sowie eine Musterchecklist bleiben letztlich eher abstrakt. Eine Ergänzung um sektoren- bzw. branchenspezifische Spezialschutzkonzepte bzw. eine Anpassung auf die individuell-unternehmensspezifischen Bedarfe gilt als unerlässlich. Dabei ist im Basisschutzkonzept selbst ein stufenweises Vorgehen angelegt: Während die Rolle des Staates von der ersten bis zur dritten Stufe zugunsten des unternehmerischen Parts abnimmt, entwickelt sich parallel der Anteil der benötigten Informationen von öffentlich zugänglichen Hinweisen hin zu unternehmensinternen Daten.

Abbildung 1: Das Basisschutzkonzept (BMI 2005a) bezieht sich u. a. auf die *Störfall-Verordnung* (Quelle: Johner Images/Getty Images).

Auch wenn es sich beim Basisschutzkonzept um ein „Pflichtprogramm" handelt, das im Grunde in jedem Unternehmen umgesetzt sein sollte, ist es national und international auf großes Interesse gestoßen. Diese Akzeptanz lässt sich sicherlich auch darauf zurückführen, dass das Konzept in einer Arbeitsgruppe mit Betreibern erstellt wurde, d. h., die beteiligten Fachleute waren gleichzeitig auch Anwender des Basisschutzkonzepts. Gerade bei der Entwicklung methodischer Grundlagen zum Schutz Kritischer Infrastrukturen hat sich diese Akteurskonstellation auch später vielfach bewährt (→ Kapitel 2.1).

1.2 Ein strategischer Rahmen: Die Nationale Strategie zum Schutz Kritischer Infrastrukturen

Mit Beginn der Arbeiten zum Schutz Kritischer Infrastrukturen in Deutschland in den späten 1990er-Jahren setzten vielfältige Aktivitäten ein: Es wurden generelle Empfehlungen sowie spezielle Handreichungen erarbeitet, Studien durchgeführt und organisatorische Strukturen aufgebaut (→ Kapitel 1.1). Es gab in dem Sinne jedoch keine in sich geschlossene Vorgehensweise mit einer strategischen Zielsetzung. Der NPSI (BMI 2005b) und insbesondere sein „Umsetzungsplan KRITIS" (BMI 2007a) wiesen bereits in diese Richtung: Es wurden strategische Ziele in der Prävention, der Reaktion und der Nachhaltigkeit von Maßnahmen zur Aufrechterhaltung kritischer Geschäftsprozesse formuliert. Zudem wurde in einer Roadmap die Einrichtung von Arbeitsgruppen zu den Themen Notfall- und Krisenübungen, Krisenreaktion und Krisenbewältigung, Aufrechterhaltung kritischer Infrastrukturdienstleistungen sowie nationale und internationale Zusammenarbeit angekündigt. Entsprechend dem NPSI fokussierte sich der Umsetzungsplan KRITIS auf den Schutz der *Informations*infrastrukturen und richtete sich im Wesentlichen an privatwirtschaftliche Betreiber Kritischer Infrastrukturen.

Erste konkretere Überlegungen zu einer Gesamtstrategie zum Schutz Kritischer Infrastrukturen entwickelten sich ab 2007. In einem Eckpunktepapier wurden zentrale programmatische Festlegungen getroffen, die sich so auch in der 2009 verabschiedeten Strategie wiederfinden. Die Diskussionen zu den Eckpunkten, zu einem Leitbild und zu ersten Vorentwürfen einer Strategie wurden zunächst zwischen den zuständigen Referaten im damaligen BMI und den beiden Geschäftsbereichsbehörden BBK und BSI geführt. Mitte 2008 konnte der Entwurf der Strategie in eine erste Ressortabstimmung gegeben und Anfang 2009 in einer zweiten Ressortabstimmung verabschiedet werden. Auch die Länder und die Wirtschaft nahmen zum Entwurf Stellung, bevor im Juni 2009 der Kabinettbeschluss zur KRITIS-Strategie (BMI 2009) herbeigeführt wurde.

Zu diesem Zeitpunkt wurden bereits seit über zehn Jahren Maßnahmen zum Schutz Kritischer Infrastrukturen umgesetzt (→ Kapitel 1.1). Die Strategie fasst daher, wie es im Leitbild heißt, „die Zielvorstellungen und den politischen Rahmen, wie er bereits praktiziert wird [...], zusammen und ist Ausgangspunkt, das bislang Erreichte auf konsolidierter Grundlage fortzusetzen und mit Blick auf neue Herausforderungen weiterzuentwickeln" (BMI 2009, S. 2). Zum Erreichten werden in einem Kapitel zur „bisherigen Bilanz" (BMI 2009, S. 3f.) Vorsorgemaßnahmen zur IT-Sicherheit gezählt, wie z.B. der IT-Grundschutz und der NPSI, mit dessen Umsetzungsplan KRITIS die Kooperationen zwischen Behörden und Infrastrukturbetreibern etabliert wurde. Diese Zusammenarbeit hatte im „Basisschutzkonzept" (BMI 2005a) und im Leitfaden zum Risiko-und Krisenmanagement für Unternehmen und Behörden (BMI 2007b, → Kapitel 2.1.1) sowie in der Einbindung von Betreibern in die Übungsreihe „LÜKEX" (→ Kapitel 2.4.4) bereits ihren Ausdruck gefunden. Darüber hinaus wird der Start des Programms „Forschung für die zivile Sicherheit" (BMBF 2007, → Kapitel 2.3.3) zum Erreichten gezählt. Zukünftige Herausforderungen für den Schutz Kritischer Infrastrukturen als Aspekt der Inneren Sicherheit erkennt die KRITIS-Strategie in einer steigenden gesellschaftlichen Abhängigkeit von untereinander immer stärker vernetzten Infrastruktursystemen und in einer neuen Qualität von terroristischen Bedrohungen und Naturgefahren. Sie leitet daraus die Notwendigkeit ab, sich einem breiten Spektrum Kritischer Infrastrukturen sowie einem breiten Gefahrenspektrum zuzuwenden (vgl. BMI 2009, S. 3f.).

Zu den Kernelementen der KRITIS-Strategie gehört folgerichtig die Orientierung am sogenannten „All-Gefahren-Ansatz" (vgl. Tabelle 1). „Kritische Infrastrukturen", so heißt es in der Strategie, „können durch verschiedene Gefahren bedroht sein, die bei Risiko- und Gefährdungsanalysen sowie der Auswahl von Handlungsoptionen gleichermaßen zu berücksichtigen sind" (BMI 2009, S. 7). Gefahrenspezifische Aktivitäten sind demnach einzelne Bausteine. Damit bildet die KRITIS-Strategie einen gemeinsamen Rahmen für Aktivitäten, die auf die IT-Sicherheit Kritischer Infrastrukturen und auf den sogenannten „physischen Schutz" ausgelegt sind.

Naturereignisse	Technisches/menschliches Versagen	Terrorismus, ~~Kriminalität,~~ Krieg
Extremereignisse, u. a. Stürme, Starkniederschläge, Temperaturstürze, Hochwasser, Hitzewellen, Dürren	Systemversagen, u. a. Unter- und Überkomplexität in der Planung, Hardware-, Softwarefehler	Terrorismus
Wald- und Heidebrände	Fahrlässigkeit	Sabotage
Seismische Ereignisse	Unfälle und Havarien	Sonstige Kriminalität
Epidemien und Pandemien bei Mensch, Tier und Pflanzen	Organisatorisches Versagen, u. a. Defizite im Risiko- und Krisenmanagement, unzureichende Koordination und Kooperation	Bürgerkriege und Kriege
Kosmische Ereignisse, u. a. kosmische Energiestürme, Meteoriten und Kometen		

Tabelle 1: Übersicht zum „All-Gefahren-Ansatz" der KRITIS-Strategie (Quelle: nach BMI 2009, S. 7).

Ein weiteres zentrales Element der Strategie ist die Weiterführung einer bereits im Umsetzungsplan KRITIS angelegten Herangehensweise: die Ausrichtung des Schutzes Kritischer Infrastrukturen auf alle Phasen des Risiko- und Krisenmanagements (vgl. Abbildung 2). Im Rahmen der „Prävention" sollen Risiken im Vorfeld erkannt und gravierende Störungen und Ausfälle möglichst vermieden oder auf ein Mindestmaß reduziert werden; im Rahmen der „Reaktion" sollen die Folgen von Störungen und Ausfällen durch Notfallmanagement, Redundanzen und Selbsthilfekapazität so gering wie möglich gehalten werden (vgl. BMI 2009, S 10). Erkenntnisse über Gefährdungen sind in fortlaufenden Analysen zu aktualisieren. Der Umsetzungstand ist in Evaluationsprozessen zu überprüfen und fortzuschreiben. Die getroffenen Maßnahmen sollen zudem regelmäßig Gegenstand von Übungen sein. Auch das Lernen aus zurückliegenden Ausfallereignissen und der Erfahrungsaustausch zwischen Akteuren im In- und Ausland werden als Teilaspekte der „Nachhaltigkeit" des Schutzes Kritischer Infrastrukturen betrachtet (vgl. BMI 2009, S. 10-11).

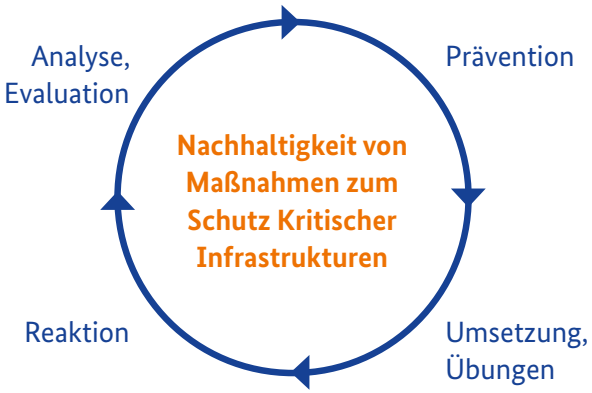


Abbildung 2: Schematische Darstellung zum „Risikomanagement-Kreislauf für Kritische Infrastrukturen" (Quelle: nach BMI 2009, S. 11).

Zwar richtet sich die Strategie in erster Linie an den Bund, jedoch werden auch viele weitere Akteure angesprochen: staatliche Stellen auf allen Ebenen ebenso wie Betreiber Kritischer Infrastrukturen und ihre Verbände, Wissenschaft und Forschung und letztlich auch die Bevölkerung. Dabei nehmen die verschiedenen Akteure unterschiedliche Rollen ein und unterscheiden sich bezüglich Intention, Inhalt und Intensität ihres Engagements beim Schutz Kritischer Infrastrukturen voneinander: von „Gewährleistern" (Staat) und „Bereitstellern" (Betreiber) über „Entwickler" (Forschung, Wissenschaft) bis hin zu „Bedarfsträgern".

Besondere Bedeutung kommt dabei der Zusammenarbeit zwischen Staat und Wirtschaft zu, da diese beiden Akteure in der Verantwortung für die Verfügbarkeit wichtiger Infrastrukturleistungen stehen. Dabei steht der „kooperative Ansatz" im Mittelpunkt, d. h. eine Zusammenarbeit, die sich durch gemeinsame Interessen und gemeinsame Ziele auszeichnet und das – im hoheitlichen Staat klassische – Über-/Unterordnungsverhältnis zugunsten eines partnerschaftlichen Miteinanders ergänzt. Der Staat, so heißt es im Leitbild der Strategie (BMI 2009, S. 2), steuert „primär moderierend, nötigenfalls normierend" beim Schutz Kritischer Infrastrukturen, räumt also freiwilligen Selbstverpflichtungen grundsätzlich Vorrang vor gesetzlichen Regelungen ein. Aus unternehmerischer Sicht ist darüber hinaus die Orientierung an der Verhältnismäßigkeit, d. h. der Erforderlichkeit, Geeignetheit und Angemessenheit der Mittel als Leitprinzip des Schutzes Kritischer Infrastrukturen zentral (BMI 2009, S. 10).

Wie die Zusammenarbeit von staatlichen Behörden auf der einen Seite und privaten Akteuren auf der anderen Seite strukturiert und planerisch umgesetzt werden kann, wird in der Strategie lediglich skizziert. Als Meilensteine werden generalisierend u. a. die Festlegung von Schutzzielen, die Analyse und Bewertung von Gefahren oder auch die Vereinbarung von Schutzmaßnahmen einschließlich ihrer Umsetzung sowie ein kontinuierlicher Risikokommunikationsprozess genannt (vgl. BMI 2009, S. 14). Diese Verfahrensweisen der staatlich-privaten Kooperation lassen sich auf alle administrativen Ebenen (Bund, Land und Kommune) übertragen – auch wenn sich die Strategie als Bundesstrategie vornehmlich an Akteure auf Bundesebene richtet, zeigt sich auch an dieser Stelle ihre ebenenübergreifende Perspektive.

Insgesamt versteht sich die KRITIS-Strategie mehr als „Wegweiser" denn als „ausgebaute Straße" für eine strukturierte Herangehensweise an den Schutz Kritischer Infrastrukturen in Deutschland. Daher wurden die einzelnen, in der Strategie beschriebenen Arbeitspakete auch nicht detailliert ausgeführt, sondern waren im Zuge der Strategieumsetzung zu konkretisieren. Einen Einblick in die Aktivitäten, die in den letzten zehn Jahren auf dieser Basis unternommen wurden, gibt das nachfolgende → Kapitel 2.

Infobox 2: Sektoren und Branchen Kritischer Infrastrukturen im Laufe der Zeit

Um den Gegenstandsbereich des Schutzes Kritischer Infrastrukturen zu konkretisieren, wurden im Laufe der Zeit mehrere Sektoreneinteilungen vorgenommen. Diese Einteilungen sind das Ergebnis von Diskussionen über die Ausrichtung des Schutzes Kritischer Infrastrukturen und spiegeln damit auch ein Stück weit die Entwicklung des Politikfeldes wider. Die erste Version wurde von der 1997 eingerichteten, ressortübergreifenden AG KRITIS vorgenommen, die 2000 ihren Abschlussbericht vorlegte (→ Kapitel 1.1). Diese Einteilung enthielt insgesamt sieben Sektoren (vgl. Tabelle 2). Auch wenn die Bezeichnung des Sektors *Gesundheitswesen* nicht unmittelbar darauf schließen lässt, hatten auch die Versorgung mit Trinkwasser und Lebensmitteln darin ihren Platz. Diese erste Sektoreneinteilung der AG KRITIS wird z. B. im Jahresbericht 2003 des BSI verwendet (vgl. BSI 2004).

Die 2002 eingesetzte PG KRITIS legte sich auf insgesamt acht Sektoren fest (vgl. Tabelle 2). Ein mit *Versorgung* überschriebener Sektor fasste nun die Versorgung mit Wasser, Lebensmitteln und Leistungen aus dem Gesundheitsbereich zusammen, ergänzt um die Notfallversorgung. Neu eingeführt wurden durch die PG KRITIS die Stichworte *Medien* und *Kulturgüter*, die in ähnlicher Form auch in der aktuellen Sektoreneinteilung zu finden sind. Nicht weitergeführt wurde hingegen der durch die PG KRITIS verfolgte Ansatz, auch Großforschungseinrichtungen und den Sektor *Gefahrstoffe* in die Einteilung aufzunehmen. Letzterer unterscheidet sich von den anderen Sektoren dadurch, dass er keinen „Dienstleistungsbereich" beschreibt, der seiner gesellschaftlichen Bedeutung wegen schützenswert ist. Die von den Gefahrstoffen ausgehende Gefahr entsteht durch deren Freisetzung, nicht durch den Ausfall einer Dienstleistung. Insofern zeugt die Aufnahme dieses Sektors auch von einem anderen, breiteren Verständnis dessen, was *Kritische* Infrastrukturen ausmacht und worauf der Schutz Kritischer Infrastrukturen ausgelegt sein sollte. Die Sektoreneinteilung der PG KRITIS wurde im NPSI (BMI 2005b) und später in der ersten Auflage des Leitfadens zum Risiko- und Krisenmanagement für Unternehmen und Behörden (BMI 2007b) veröffentlicht.

Als 2009 die KRITIS-Strategie (BMI 2009) verabschiedet wurde (→ Kapitel 1.2), war die Abstimmung über eine neue Sektoreneinteilung noch nicht abgeschlossen. Die KRITIS-Strategie enthält daher eine ähnlich anmutende, aber nicht als Sektoreneinteilung überschriebene Übersicht „technischer Basisinfrastrukturen“ und „sozioökonomischer Dienstleistungsinfrastrukturen“ (vgl. BMI 2009, S. 5). Erst 2011 wurde eine zwischen den Bundesressorts und den Ländern abgestimmte Einteilung von nun neun KRITIS-Sektoren vorgelegt (vgl. Tabelle 2) und z. B. in der überarbeiteten zweiten Auflage des Leitfadens zum Risiko- und Krisenmanagement (BMI 2011a) veröffentlicht.

Die neben dem Wegfall des Sektors *Gefahrstoffe* wohl auffälligste Änderung ist die Auflösung des bisherigen Sektors *Versorgung* in die drei separaten Sektoren *Ernährung*, *Gesundheit* und *Wasser* (BBK/BSI 2011). Diese bis heute gültige Sektoreneinteilung wird durch eine auf Bundesebene abgestimmte Einteilung von insgesamt 29 einzelnen Branchen weiter differenziert (vgl. Tabelle 3). Zieht man diese hinzu, wird ersichtlich, dass einige in den früheren Versionen zur Bezeichnung von Sektoren verwendete Begriffe nun auf Ebene der Branchen verwendet werden, z. B. die *Justiz* oder auch das *Notfall- und Rettungswesen*.

<table>
<tr><th>Sektoreneinteilung der AG KRITIS (BSI 2004, S. 67)</th><th>Sektoreneinteilung der PG KRITIS (BMI 2005b, S. 21)</th><th>aktuelle Sektoreneinteilung von Bund und Ländern (BMI 2011a, S. 8; BBK/BSI 2011)</th></tr>
<tr><td>Energie</td><td>Energie (Strom, Mineralöl, Gas)</td><td>Energie</td></tr>
<tr><td>Telekommunikation und Informationstechnik</td><td>Informations- und Kommunikationstechnologie</td><td>Informationstechnik und Telekommunikation</td></tr>
<tr><td>Transport und Verkehrswesen</td><td>Transport und Verkehr</td><td>Transport und Verkehr</td></tr>
<tr><td rowspan="2">Gesundheitswesen
(inkl. Lebensmittel- und Trinkwasserversorgung)</td><td rowspan="3">Versorgung
(Wasser, Lebensmittel, Gesundheit, Notfallversorgung)</td><td>Gesundheit</td></tr>
<tr><td>Wasser</td></tr>
<tr><td>Ernährung</td></tr>
<tr><td>Notfall- und Rettungswesen</td><td>*</td></tr>
<tr><td>Finanz- und Versicherungswesen</td><td>Banken und Finanzen</td><td>Finanz- und Versicherungswesen</td></tr>
<tr><td>Behörden und Verwaltung</td><td>Behörden, Verwaltung, Justiz</td><td>Staat und Verwaltung</td></tr>
<tr><td></td><td>Medien, Großforschungseinrichtungen und Kulturgüter</td><td>Medien und Kultur</td></tr>
<tr><td></td><td>Gefahrstoffe
(Chemieindustrie und Biostoffe)</td><td></td></tr>
</table>

*Hinweis: Notfall- und Rettungswesen ist eine Branche innerhalb des Sektors *Staat und Verwaltung*

Tabelle 2: Entwicklungsschritte der Einteilung von Sektoren Kritischer Infrastrukturen und aktuelle Fassung (Zusammenstellung: BBK).

Sektoreneinteilung (Bund und Länder) (BBK/BSI 2011)	Brancheneinteilung (Bund) (BBK/BSI 2011)	Kritische Dienstleistungen (Diskussionsstand) (BBK 2019a, S. 38)
Energie	Elektrizität, Mineralöl, Gas	Stromversorgung, Gasversorgung, Kraftstoff- und Heizölversorgung, Fernwärmeversorgung
Ernährung	Ernährungswirtschaft, Lebensmittelhandel	Lebensmittelversorgung
Finanz- und Versicherungswesen	Banken, Börsen, Versicherungen, Finanzdienstleister	Zahlungsverkehr, Bargeldversorgung, Kreditvergabe, Wertpapier- und Derivatehandel, Versicherungsdienstleistungen
Gesundheit	medizinische Versorgung, Arzneimittel und Impfstoffe, Labore	Medizinische Versorgung, Versorgung mit Arzneimitteln (einschließlich Impfstoffen und Schutzwirkstoffen nach Strahlenschutzrecht), Versorgung mit Medizinprodukten, Laboratoriumsdiagnostik
Informationstechnik und Telekommunikation	Telekommunikation, Informationstechnik	Leitungsgebundene und ungebundene (auch weltraumbasierte) Sprach- und Datenübertragung, Datenspeicherung und -verarbeitung
Medien und Kultur	Rundfunk (Fernsehen und Radio), gedruckte und elektronische Presse, Kulturgut, symbolträchtige Bauwerke	Warnung und Alarmierung, Versorgung mit Informationen, Herstellen von Öffentlichkeit, Aufbewahrung identitätsstiftender Kulturgegenstände und Dokumente, Vermittlung kultureller Identität, Langzeitsicherung und -lagerung von mikroverfilmten Dokumenten der deutschen Geschichte gemäß Haager Konvention zum Schutz von Kulturgut
Staat und Verwaltung	Regierung und Verwaltung, Parlament, Justizeinrichtungen, Notfall- und Rettungswesen einschließlich Katastrophenschutz	Umsetzung von Recht im Rahmen der Eingriffs- und Leistungsverwaltung, (polizeiliche und nicht-polizeiliche) Gefahrenabwehr, Verteidigung, Gesetzgebung, Kontrolle der Regierung, Rechtsprechung und deren Vollzug
Transport und Verkehr	Luftfahrt, Seeschifffahrt, Binnenschifffahrt, Straßenverkehr, Logistik, Schienenverkehr	Leistungen zum Transport von Personen, Leistungen zum Transport von Gütern, Satellitennavigationssysteme und satellitengestützte Positions-, Navigations- und Zeit- sowie meteorologische Dienste
Wasser	öffentliche Wasserversorgung und öffentliche Abwasserbeseitigung	Trinkwasserversorgung, Abwasserbeseitigung

Tabelle 3: Aktuell gültige, zwischen Bund und Ländern abgestimmte Einteilung der Sektoren Kritischer Infrastrukturen, Brancheneinteilung des Bundes sowie Diskussionsstand zu kritischen Dienstleistungen (Zusammenstellung: BBK).

Etwas später gewann das Konzept der „kritischen Dienstleistung“ im Kontext des Schutzes Kritischer Infrastrukturen an Bedeutung. Der Begriff bezeichnet eine „Dienstleistung, die von Betreibern Kritischer Infrastrukturen zur Versorgung der Allgemeinheit erbracht wird und deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen, zu Gefährdungen der öffentlichen Sicherheit oder zu vergleichbaren Folgen führen würde“ (BBK 2019f, S. 34). Kritische Infrastrukturen sind für die Bereitstellung kritischer Dienstleistungen innerhalb der Sektoren und Branchen von besonderer Bedeutung. Der Begriff der kritischen Dienstleistung bringt also nichts vollkommen Neues zum Ausdruck, komplettiert aber die Begriffssystematik um einen zentralen Aspekt und dokumentiert auch eine gewisse Akzentverschiebung – vom Schutz der Infrastruktur zur Aufrechterhaltung der Dienstleistung. Insbesondere das *IT-Sicherheitsgesetz* und die zu seiner Umsetzung erlassene *BSI-Kritisverordnung* haben dem Konzept der kritischen Dienstleistung in den letzten Jahren Gewicht verliehen (→ Kapitel 2.2.1 und Infobox 16). Die Auflistung kritischer Dienstleistungen in Tabelle 3 gibt den derzeitigen Diskussionsstand wieder (BBK 2019a; → Kapitel 2.1.2).

Abbildung 3: Die Sektoren werden häufig in Form der „Sektoren-Torte“ dargestellt (hier alphabetische Anordnung, Quelle: nach BBK/BSI 2011).

Quelle: Natalia Klenova / EyeEm / Getty Images

2

Kapitel

Was den Schutz Kritischer Infrastrukturen in den letzten zehn Jahren bewegt hat

Der „runde Geburtstag“ der KRITIS-Strategie (BMI 2009) gibt Anlass, auf die vielen Schritte zurückzuschauen, die in den letzten zehn Jahren zum Schutz Kritischer Infrastrukturen gegangen wurden. Dies geschieht im Folgenden nicht in Form einer auf Vollständigkeit ausgelegten Bestandsaufnahme, sondern – wie im Titel angekündigt – in Form von Einblicken in unterschiedliche Aspekte dessen, was das Politikfeld in diesem Zeitraum geprägt und wie es sich entwickelt hat.

Zu diesen Aspekten gehört es auch, die in der Strategie prominent platzierten Forderungen nach einer querschnittlichen Herangehensweise und einer akteursübergreifenden Ausrichtung des Schutzes Kritischer Infrastrukturen mit Leben zu füllen. Beide werden in einzelnen Kapiteln ausführlich betrachtet, kommen aber bereits in der Form dieser Veröffentlichung zum Ausdruck: An den nachfolgenden Einblicken haben sich unterschiedliche Institutionen, vor allem Bundesbehörden mehrerer Ressorts, beteiligt. Sie haben dabei immer auch ihre spezifische Sicht auf den Schutz Kritischer Infrastrukturen einfließen lassen. Für die Bereitschaft, sich an dieser Veröffentlichung zu beteiligen und Beiträge aus ihrer fachlichen Arbeit zuzuliefern, geht unser Dank insbesondere an

- das Bundesministerium des Innern, für Bau und Heimat (BMI) mit seinen Geschäftsbereichsbehörden: das Bundesamt für Sicherheit in der Informationstechnik (BSI), die Bundesanstalt Technisches Hilfswerk (THW) und das Bundesinstitut für Bau-, Stadt- und Raumforschung (BBSR) im Bundesamt für Bauwesen und Raumordnung (BBR),
- das Bundesministerium der Finanzen (BMF) und die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin),
- das Bundesministerium für Bildung und Forschung (BMBF),
- das Bundesministerium für Umwelt, Naturschutz und nukleare Sicherheit (BMU),
- das Bundesministerium für Verkehr und Digitale Infrastruktur (BMVI),
- das Bundesministerium für Wirtschaft und Energie (BMWi) und die Bundesnetzagentur (BNetzA),
- die Bundesanstalt für Landwirtschaft und Ernährung (BLE),
- die Nationale Kontaktstelle für das Sendai Rahmenwerk der Vereinten Nationen (NKS) beim BBK
- das Team des SicherheitsLeitfadens Kulturgut (SiLK) der Konferenz Nationaler Kultureinrichtungen (KNK).

Die im nachfolgenden Kapitel zusammengestellten Beiträge sind einzelnen Themenbereichen zugeordnet:

- Entwicklung und Umsetzung methodischer Grundlagen (→ Kapitel 2.1)
- Gestaltung des Handlungsrahmens (→ Kapitel 2.2)
- Vorstellung des Schutzes Kritischer Infrastrukturen als inhaltliches Querschnittsthema (→ Kapitel 2.3)
- sowie als akteursübergreifende (→ Kapitel 2.4),
- als sektorale (→ Kapitel 2.5) und
- als grenzüberschreitende Aufgabe (→ Kapitel 2.6).

Viele Beiträge haben allerdings enge Bezüge zu anderen Themenbereichen: So kann etwa die Zusammenarbeit auf europäischer Ebene der Ausgestaltung des Rechtrahmens dienen oder in sektoralen Kooperationsformen die Entwicklung methodischer Grundlagen voranbringen. Aus diesem Grund enthalten die nachfolgenden Ausführungen viele Querverweise. Leserinnen und Leser können der Gliederung folgen oder sich entlang der Verweise ein Bild davon machen, was den Schutz Kritischer Infrastrukturen in den letzten zehn Jahren bewegt hat.

2.1

Kapitel

Quelle: Sean Gladwell / Moment / Getty Images

Entwicklung und Umsetzung methodischer Grundlagen

Methodische Grundlagen beschreiben Vorgehensweisen für einen bestimmten Adressatenkreis und Anwendungsbereich und erfüllen damit unterschiedliche Funktionen im Kontext des Schutzes Kritischer Infrastrukturen: Sie konkretisieren einen Gegenstandsbereich, formulieren Erwartungen an einzelne Akteursgruppen, strukturieren die Zusammenarbeit zwischen ihnen und schaffen Schnittstellen zu bereits etablierten Verfahren. Einige sind in bindende Vorgaben oder formale Instrumente eingeflossen, andere dienen unverbindlich als Orientierung. Dabei beginnen methodische Grundlagen bereits in der Entwicklungsphase, Wirkung zu entfalten: Sie zwingen zu einer intensiven Auseinandersetzung mit dem betreffenden Sachverhalt und waren oft Ausgangspunkt für akteursübergreifende Kooperationen.

Es ist Aufgabe der Betreiber Kritischer Infrastrukturen - seien es Unternehmen oder Behörden - für einen sicheren und zuverlässigen Betrieb ihrer Anlagen und Einrichtungen zu sorgen. Der Leitfaden zum einrichtungsbezogenen Risiko- und Krisenmanagement für Betreiber Kritischer Infrastrukturen aus allen Branchen gehört daher zu den zentralen methodischen Grundlagen des Schutzes Kritischer Infrastrukturen (→ Kapitel 2.1.1). Die im Leitfaden vorgestellte Methodik orientiert sich an anerkannten Standards, die in enger Zusammenarbeit mit Betreibern auf den Schutz Kritischer Infrastrukturen zugeschnitten wurden. Darauf aufbauend sind eine Reihe branchenspezifischer Leitfäden sowie ein Verfahren für die strukturierte Zusammenarbeit zwischen Betreibern und staatlichen Stellen beim Risiko- und Krisenmanagement entstanden (→ Kapitel 2.5.2 und Kapitel 2.5.4).

Damit staatliche Stellen ihre Ansprechpartner auf Betreiberseite ausfindig machen und sich Betreiber Kritischer Infrastrukturen ihrer besonderen Verantwortung bewusst werden können, wurde eine Methodik zu Identifizierung Kritischer Infrastrukturen entwickelt und als Leitfaden veröffentlicht (→ Kapitel 2.1.2). Da es u. a. von der Betrachtungsebene abhängt, ob eine konkrete Anlage oder Einrichtung als kritisch bewertet wird, kann die hier beschriebene Methodik auf den jeweiligen Anwendungskontext angepasst werden. Ein Anwendungsfall auf Bundesebene ist die in der *BSI-Kritisverordnung* geregelte Identifizierung von Kritischen Infrastrukturen im Sinne des *IT-Sicherheitsgesetzes* (→ Infobox 16). Auf Basis der *Haager Konvention* werden Kulturgüter mit besonderer identitätsstiftender Bedeutung identifiziert (→ Infobox 3).

Die Risikoanalyse im Bevölkerungsschutz des Bundes untersucht, welche Auswirkungen unterschiedliche, in Form von Szenarien beschriebene Gefahrenereignisse auf die Bevölkerung und ihre Lebensgrundlagen hätten (→ Kapitel 2.1.3). Die Folgen von z. B. Stürmen oder Pandemien hängen maßgeblich davon ab, wie sehr kritische Dienstleistungen beeinträchtig werden. Im Rahmen der Risikoanalyse wird daher nach der Festlegung des Szenarios zunächst die Betroffenheit Kritischer Infrastrukturen untersucht, um darauf aufbauend eine Gesamtbetrachtung der Auswirkungen vorzunehmen. Ausfälle Kritischer Infrastrukturen haben somit als „indirekte“ Auswirkungen eines Ereignisses ihren festen Platz in der Methode für die Risikoanalyse im Bevölkerungsschutz.

Mit ihrer von der räumlichen Situation ausgehenden Herangehensweise an das Risikomanagement eröffnet die Raumplanung dem Schutz Kritischer Infrastrukturen eine sektorübergreifende Perspektive. Sie kann sichtbar machen, wo – z. B. aufgrund der räumlichen Nähe unterschiedlicher Infrastrukturen – eine Fokussierung auf einzelne, branchenspezifische Sicherheitsvorschriften zu kurz greift oder einer ganzheitlichen Lösung im Weg stehen würde. Um die Möglichkeiten des vorsorgenden Risikomanagements in der räumlichen Planung nutzen zu können, bedarf es der Entwicklung entsprechender methodischer Grundlagen (→ Kapitel 2.1.4).

2.1.1 Risiko- und Krisenmanagement für Betreiber Kritischer Infrastrukturen

Für die Funktionsfähigkeit Kritischer Infrastrukturen zu sorgen, liegt in der Verantwortung ihrer Betreiber – seien es private Unternehmen oder öffentliche Einrichtungen. Ihnen obliegt es, die Risiken für ihre Anlagen und Einrichtungen strukturiert zu ermitteln und darauf aufbauend vorsorgende Maßnahmen umzusetzen (Risikomanagement), um Störungen oder Ausfälle Kritischer Infrastrukturen möglichst zu vermeiden oder zumindest ihre Auswirkungen zu mindern. Gleichzeitig sind sie gefordert, Vorgehensweisen für den effektiven und effizienten Umgang mit Krisen zu etablieren (Krisenmanagement): Im Ereignisfall müssen Verfahren greifen, um die negativen Folgen von Ausfällen zu mindern und eine schnelle Rückkehr in den Regelbetrieb zu unterstützen. Ein umfassendes Risiko- und Krisenmanagement der Betreiber Kritischer Infrastrukturen ist daher für die Aufrechterhaltung der Versorgung mit kritischen Dienstleistungen grundlegend.

Um staatliche und private Betreiber Kritischer Infrastrukturen bei der Etablierung eines Risiko- und Krisenmanagements zu unterstützen, hat das BMI in Zusammenarbeit mit dem BBK und dem BSI sowie mit Experten der unternehmerischen Praxis im Jahr 2007 den Leitfaden „Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement für Unternehmen und Behörden“ veröffentlicht und 2011 überarbeitet (BMI 2011a). Der Leitfaden beschreibt – untergliedert in fünf Phasen – die methodischen Grundlagen, um ein Risiko- und Krisenmanagement in Einrichtungen aufzubauen oder bereits bestehende Vorkehrungen sinnvoll zu ergänzen (vgl. Abbildung 4). Dabei orientiert er sich an international anerkannten Vorgehensweisen, beispielsweise an der DIN ISO 31000 „Risikomanagement - Leitlinien“ und formuliert konkrete Anforderungen an das Risiko- und Krisenmanagement von Kritischen Infrastrukturen (→ Kapitel 2.2.2).

Die Ausführungen zur Methodik in diesem Leitfaden können von Betreibern Kritischer Infrastrukturen in allen Sektoren und Branchen (→ Infobox 2) gleichermaßen genutzt werden. Um spezifisch auf einzelne Branchen zugeschnittene Handlungsempfehlungen geben zu können, wurde auf dieser Methodik aufbauend eine ganze Reihe weiterer Leitfäden verfasst. Sie beschäftigen sich z. B. mit der Durchführung von Risikoanalysen in der Trinkwasserversorgung (→ Kapitel 2.5.2) oder mit dem Risikomanagement im Krankenhaus (→ Kapitel 2.5.4). Diese Veröffentlichungen greifen branchenspezifische Aspekte auf, die im sektorübergreifenden Leitfaden nicht betrachtet werden können.

Der Risiko- und Krisenmanagement-Leitfaden für Unternehmen und Behörden richtet sich an die Betreiber Kritischer Infrastrukturen. Sowohl in der Vorbereitung als auch in der tatsächlichen Bewältigung einer Ausfallsituation ist allerdings gerade die Zusammenarbeit zwischen den Betreibern und den staatlichen Stellen von zentraler Bedeutung. Im besten Fall findet daher schon frühzeitig eine enge Verzahnung zwischen betrieblichem und behördlichem Risiko- und Krisenmanagement statt (→ Kapitel 2.4.3). Die zu diesem Zweck entwickelte Verfahrensweise für ein Integriertes Risikomanagement basiert ebenfalls auf der in Abbildung 4 schematisch dargestellten Methode.

Um den Zugang zum Risiko- und Krisenmanagement zu erleichtern, können Mitarbeiterinnen und Mitarbeiter von Unternehmen und Behörden Seminare und Übungen an der Akademie für Krisenmanagement, Notfallplanung und Zivilschutz (AKNZ) des BBK besuchen. Die Inhalte der Lehrveranstaltungen bauen auf dem Risiko- und Krisenmanagement-Leitfaden für Unternehmen und Behörden auf.

2.1.2 Kritisch oder nicht? Methodik zur Identifizierung

Der Bund und die Länder haben sich auf die Einteilung von Sektoren Kritischer Infrastrukturen verständigt. Auf Bundesebene wurde zusätzlich eine Unterteilung der Sektoren nach Branchen abgestimmt (→ Infobox 2). Allein auf dieser Basis können noch keine konkreten Einrichtungen oder Anlagen benannt und deren Betreiber direkt adressiert werden. Das ist allerdings notwendig, damit sich die Betreiber ihrer besonderen

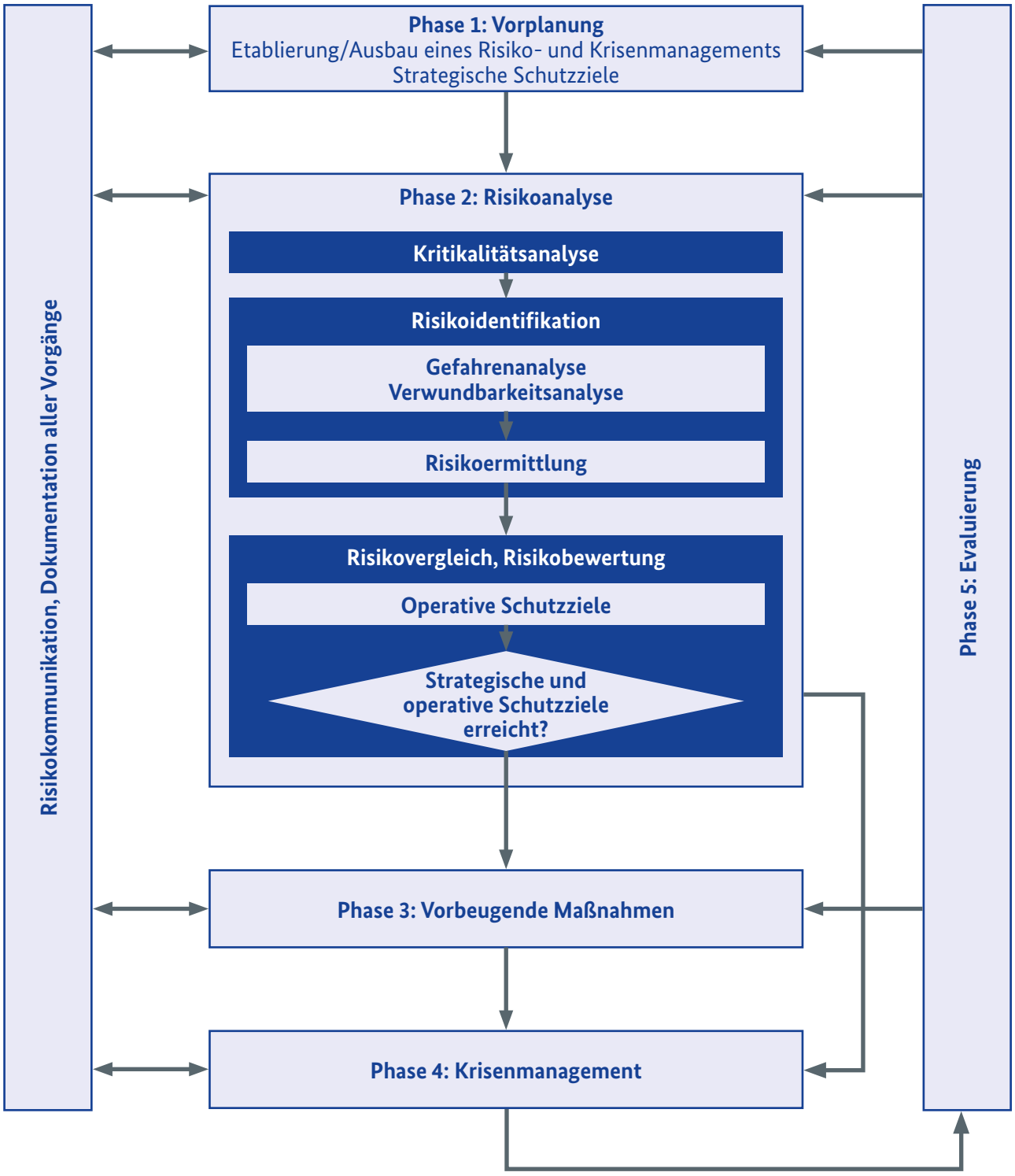


Abbildung 4: Schematische Darstellung des Risiko- und Krisenmanagements (nach BMI 2011a, S. 12).

Verantwortung für den Schutz der von ihnen betriebenen Infrastrukturen bewusst sein können und Behörden (auf allen Ebenen) wissen, an welche Betreiber sie z. B. im Sinne des Integrierten Risikomanagements (→ Kapitel 2.4.3) herantreten sollten. Je nach Fragestellung ist daher die Identifizierung von kritischen Dienstleistungen, Prozessen, Anlagen/Einrichtungen oder deren Betreibern Bestandteil des Risikomanagements, sowohl aus Sicht des Bevölkerungsschutzes als auch aus Sicht der KRITIS-Betreiber. Das Thema Identifizierung ist also für den Schutz Kritischer Infrastrukturen zentral.

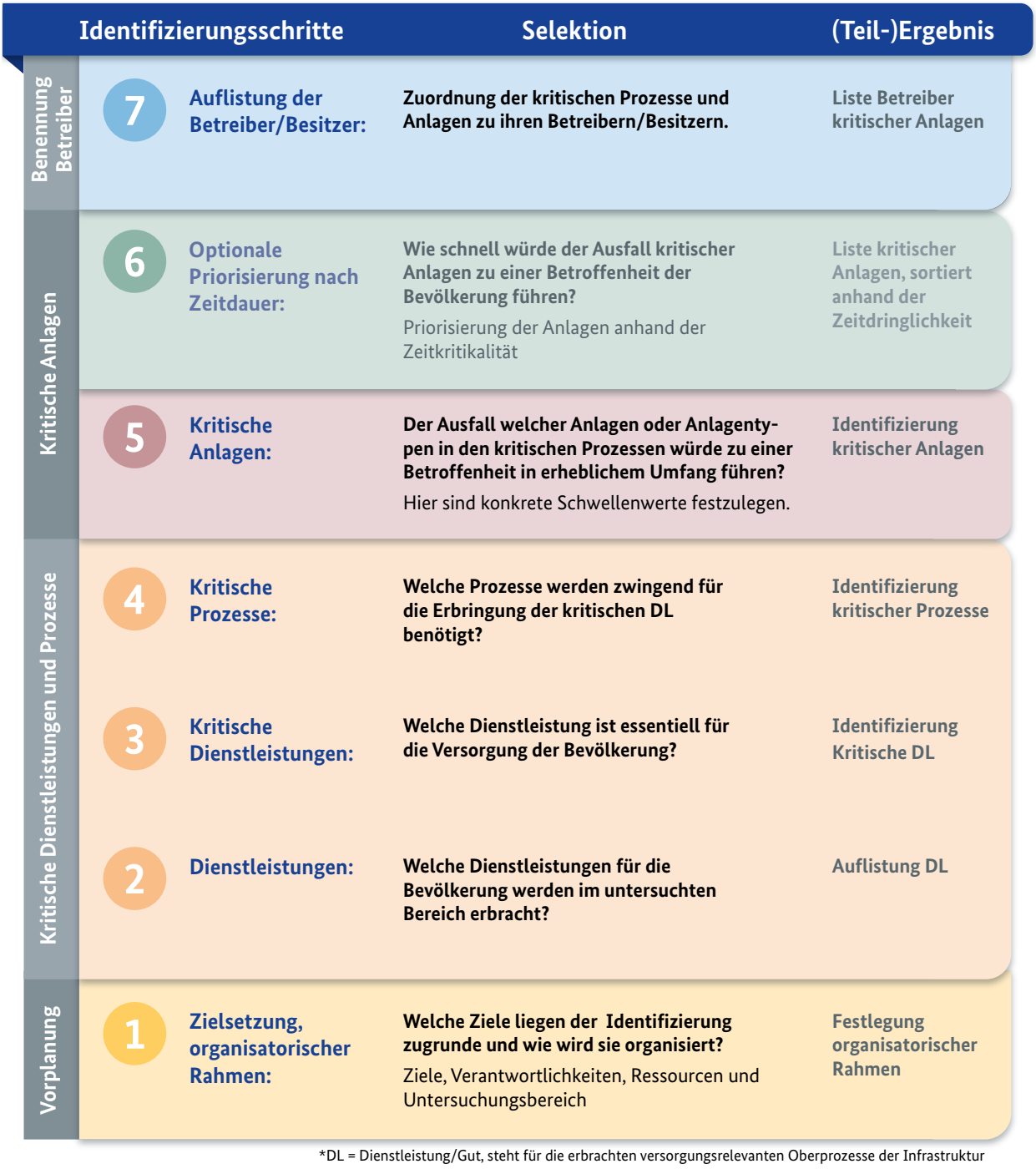


Abbildung 5: Ablauf des Verfahrens zur „Identifizierung in sieben Schritten“ (Quelle: BBK 2019a, S. 23).

Um den Zugang zur Identifizierung zu erleichtern, wird im Leitfaden „Schutz Kritischer Infrastrukturen – Identifizierung in sieben Schritten“ (BBK 2019a) die methodische Herangehensweise schrittweise erläutert. In verschiedenen Anwendungskontexten und auf unterschiedlichen Ebenen können auf diesem Weg kritische Dienstleistungen, Prozesse, Anlagen/Einrichtungen und Betreiber ausfindig gemacht und in das Risikomanagement eingebunden werden. Das BBK begleitet derzeit einige Anwender bei der Umsetzung dieser Methode. Die Bundesressorts haben sich darauf verständigt, in Deutschland kein zentrales Register aller Kritischen Infrastrukturen oder ihrer Betreiber zu führen. Gegen ein solches Register sprechen u. a. Sicherheitsgründe, da es ausgesprochen sensible Informationen enthalten würde. Welche Anlage als kritisch gilt und welcher Betreiber als KRITIS-Betreiber angesprochen wird, hängt zudem von der Betrachtungsebene ab: Eine aus Bundessicht nicht kritische Einrichtung könnte für die Gefahrenabwehr einer Kommune durchaus

eine kritische Bedeutung haben. Die Frage lautet also weniger „kritisch – ja oder nein?“, sondern „im betrachteten Kontext kritisch – ja oder nein?“.

Die Notwendigkeit, einzelne Anlagen oder Einrichtungen als kritisch zu identifizieren und deren Betreiber konkret zu benennen, hat im Zusammenhang mit Gesetzen eine besondere Bedeutung: Dem Bestimmtheitsgrundsatz folgend müssen die Adressaten einer gesetzlichen Regelung eindeutig benannt werden können. So wurde zur Umsetzung einer EU-Richtlinie (vgl. RL 2008/114/EG) ein Identifizierungsverfahren zur Bestimmung „*europäisch* kritischer Infrastrukturen“ im Verkehrs- und Energiesektor eingesetzt (→ Kapitel 2.2.1 und Infobox 5). Auf nationaler Ebene führte die Verabschiedung des *IT-Sicherheitsgesetzes* im Jahr 2015 die Notwendigkeit zur Festlegung und Durchführung eines Identifizierungsverfahrens herbei. Welche Anlagen als „kritisch im Sinne des IT-Sicherheitsgesetzes“ gelten, ist in der *BSI-Kritisverordnung* geregelt (→ Infobox 16). Der Verordnung liegt dieselbe Identifizierungsmethode zugrunde, die auch im o. g. Leitfaden beschrieben wird – sie ist also ein spezifischer Anwendungsfall der in verschiedenen Kontexten einsetzbaren Methode.

Infobox 3: Ein besonderer Fall: Identifizierung von Kulturgut im Sinne der *Haager Konvention*

Viele Kulturgüter haben eine große identitätsstiftende Bedeutung. Man spricht von einer hohen „symbolischen Kritikalität“ (BMI 2009, S 5). Der Verlust dieser Kulturgüter kann eine Gesellschaft emotional erschüttern und psychologisch aus dem Gleichgewicht bringen. Auch im Rahmen kriegerischer Auseinandersetzungen können Schäden an Kulturgütern entstehen. Gerade wegen ihrer symbolischen Kritikalität laufen sie in diesen Situationen Gefahr, beschädigt, zerstört oder entwendet zu werden.

Unter dem Dach der Organisation der Vereinten Nationen für Bildung, Wissenschaft und Kultur (UNESCO) wurde daher die Haager Konvention zum Schutz von Kulturgut bei bewaffneten Konflikten, kurz: *Haager Konvention*, ausgehandelt. Sie wurde im Jahr 1954 verabschiedet, ist Teil des humanitären Völkerrechts und wurde inzwischen weltweit von 133 Staaten ratifiziert – auch von Deutschland (vgl. *Gesetz zu der Konvention vom 14. Mai 1954 zum Schutz von Kulturgut bei bewaffneten Konflikten* vom 11. April 1967). Zwar ist in Deutschland die Kulturhoheit der Länder grundgesetzlich verankert (Art. 30 GG), mit der Umsetzung der *Haager Konvention* als Spezialfall bezogen auf bewaffnete Konflikte ist allerdings der Bund beauftragt. Die Aufgabe ist dem BMI zugewiesen und wird vom BBK sowie im Auftrag des Bundes von den Ländern wahrgenommen. Die Umsetzung der *Haager Konvention* ist Teil der „Konzeption Zivile Verteidigung“ (BMI 2016b, → Kapitel 2.3.2).

Da nicht alle Kulturgüter gleichermaßen geschützt werden können, müssen die im Sinne der *Haager Konvention* besonders gefährdeten Objekte identifiziert werden. Als „besonders gefährdet“ gelten in diesem Kontext Kulturobjekte, die weithin bekannt sind, mit denen sich viele Menschen emotional verbunden fühlen und deren Bedeutung auch von Nichtfachleuten nachempfunden werden kann. Es geht also nicht nur um die aus fachöffentlicher Sicht „besonders hochwertigen“ Denkmale oder Kunstwerke, sondern um deren Symbolwert und deren emotionale Bedeutung für die Menschen. Zwar wurden bis in die 1980er-Jahre bereits rund 10.000 Objekte erfasst, allerdings bestehen Zweifel an Aktualität und Handhabbarkeit der bereits erstellten Auflistungen. Das Kriterium der symbolischen Kritikalität eröffnet eine neue Perspektive für die Identifikation gefährdeter Objekte und gibt Anlass zu deren Neubewertung.

Abbildung 6: Das „Blue Shield“ ist das internationale Kennzeichen für Kulturgut nach der *Haager Konvention* (Quelle: UNESCO).

2.1.3 Kritische Infrastrukturen in der Risikoanalyse des Bundes

Um über den Umgang mit Risiken angemessen entscheiden und Planungen zum Schutz der Bevölkerung zielgerichtet vorantreiben zu können, muss geklärt werden, mit welchen Gefahren in Deutschland zu rechnen ist, mit welchen Folgen ihr Eintritt verbunden sein könnte und wie der Bevölkerungsschutz darauf vorbereitet wäre. Diese Fragen sind Gegenstand der Risikoanalyse im Bevölkerungsschutz des Bundes. Sie ist seit 2009 in § 18 des *Zivilschutz- und Katastrophenhilfegesetzes* (→ Kapitel 2.2.1) verankert und wird vom Bund im Zusammenwirken mit den Ländern durchgeführt. Das BMI ist beauftragt, dem Deutschen Bundestag jährlich über die Umsetzung zu berichten. Die Ergebnisse der Analysen werden als Bundestagsdrucksachen veröffentlicht.

Bisher wurden folgende Risikoanalysen durchgeführt:

- Extremes Schmelzhochwasser aus den Mittelgebirgen (2012; BT-Drs. 17/12051)
- Pandemie durch Virus Modi-SARS (2012; BT-Drs. 17/12051)
- Wintersturm (2013, BT-Drs. 18/208)
- Sturmflut (2014, BT-Drs. 18/3682)
- Freisetzung radioaktiver Stoffe aus einem Kernkraftwerk (2015, BT-Drs. 18/7209)
- Freisetzung chemischer Stoffe (2016, BT-Drs. 18/10850)
- Zusammenfassende Betrachtung bisheriger Risikoanalysen (2017, BT-Drs. 19/9520)
- Dürre (2018, BT-Drs. 19/9521)
- 2019 laufend: Erdbeben

Die Risikoanalyse basiert auf Szenarien, also fiktiven, aber plausiblen Ereignisverläufen. Die dazu ausgewählten „denkbaren Extremereignisse“, wie z. B. ein Wintersturm, werden hinsichtlich ihrer Intensität, räumlichen Ausdehnung, ihrer Dauer sowie ihres Ablaufs usw. beschrieben. Dadurch wird es möglich, ihre Auswirkungen auf die

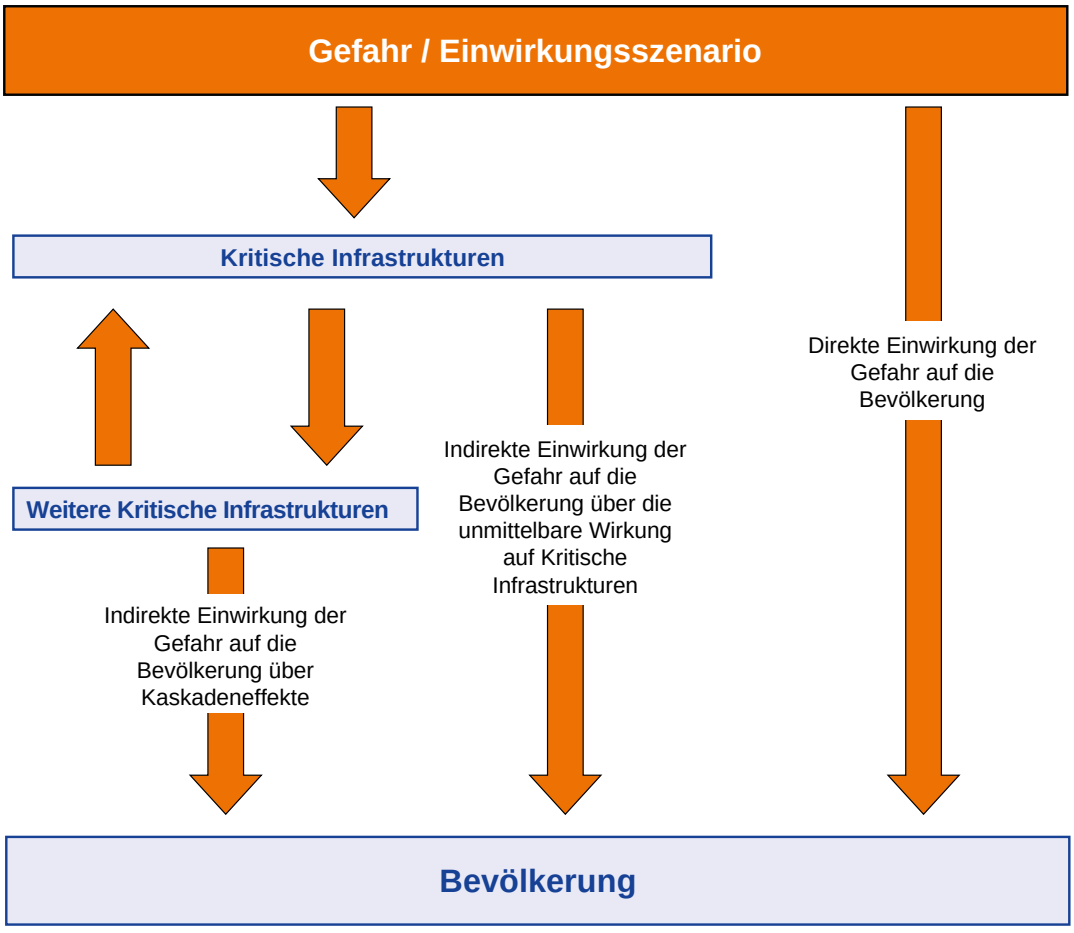


Abbildung 7: Gefahren können direkte und indirekte Auswirkungen haben, die in einer Gesamtbetrachtung berücksichtigt werden müssen (Quelle: nach BBK 2012, S. 30).

Schutzgüter „Mensch“, „Umwelt“, „Wirtschaft“ und „Immateriell“ abzuschätzen. Um ein konkreteres Bild von den Auswirkungen entstehen zu lassen, werden für jedes Schutzgut mehrere Schadensparameter unterschieden. Für das Schutzgut „Mensch“ wird z. B. die Anzahl der erwarteten Todesfälle, der Verletzten bzw. Erkrankten, der Hilfebedürftigen und der vermissten Personen betrachtet.

Die unter Annahme eines Szenarios zu erwartenden Folgen hängen oft ganz maßgeblich davon ab, von welcher Betroffenheit Kritischer Infrastrukturen ausgegangen wird. Deshalb wird für jedes analysierte Szenario zunächst untersucht, mit welchen Auswirkungen auf die KRITIS-Sektoren (→ Infobox 2) zu rechnen ist, und erst auf dieser Basis wird die Betroffenheit der o. g. Schutzgüter abgeleitet. Beispielsweise wurde angenommen, dass der im Jahr 2013 analysierte Wintersturm auch mit regionalen Stromausfällen einhergeht. Dadurch war nicht nur von einer bestimmten Anzahl an Personen auszugehen, die aufgrund des Sturms Hilfe in Anspruch nehmen müssen, etwa weil sie Verletzungen erlitten haben oder ihr Zuhause beschädigt wurde. Es musste zusätzlich mit einer gewissen Anzahl Menschen gerechnet werden, die aufgrund der Stromausfälle vorübergehend hilfebedürftig werden und z. B. mit einer Beeinträchtigung der Trinkwasserversorgung konfrontiert wären. Ausfälle Kritischer Infrastrukturen müssen demnach als „indirekte“ Auswirkungen eines Ereignisses bei der Gesamtbetrachtung mitgedacht werden (vgl. Abbildung 7) und haben daher in der Methode für die Risikoanalyse im Bevölkerungsschutz ihren festen Platz.

Für die Umsetzung der Risikoanalyse im Bevölkerungsschutz auf Bundesebene wurden im Jahr 2011 ein Lenkungsausschuss der Bundesressorts (koordiniert durch das BMI) sowie ein Arbeitskreis der Geschäftsbereichsbehörden (koordiniert durch das BBK) eingerichtet. Der Lenkungsausschuss nimmt u. a. die Auswahl der als bundesrelevant erachteten Gefahren vor. Für diese werden in gefahrenspezifisch zusammengesetzten Arbeitsgruppen des Arbeitskreises Szenarien beschrieben und analysiert. Hierbei werden bereits vorhandene Erkenntnisse und Informationen zusammengeführt und in die Struktur der Methode eingepasst. Bei Bedarf werden auch Expertisen anderer Bereiche, z. B. aus der Wissenschaft, von Institutionen auf Länderebene oder auch von Betreibern Kritischer Infrastrukturen, in die Analyse eingebunden. Auf diesem Weg ist ein breites „Risikoanalyse-Netzwerk“ entstanden, das mit jeder weiteren Analyse weiter ausgebaut wird.

2.1.4 Schutz Kritischer Infrastrukturen als Aufgabe der Raumplanung

Das *Raumordnungsgesetz* (ROG, → Kapitel 2.2.1) betont in § 2 Abs. 2 Satz 3 mit dem Grundsatz, dem Schutz Kritischer Infrastrukturen Rechnung zu tragen, die raumordnerische Aufgabe eines vorsorgenden Risikomanagements. Damit werden Fragen aufgeworfen: Welcher Stellenwert soll dem Schutz Kritischer Infrastrukturen in Raumordnungsplänen zukommen? Wie können die Potenziale der Raumordnung in der Vorsorge für den Schutz Kritischer Infrastrukturen ausgeschöpft werden? Wir kann der Schutz Kritischer Infrastrukturen im Sinne eines integrierten Risikomanagements mit bereits wahrgenommenen Aufgaben in Einklang gebracht werden (z. B. mit dem vorbeugenden Hochwasserschutz, → Infobox 4)?

Ein vorsorgendes Risikomanagement dient in diesem Kontext der Identifizierung von Gefahren und Vulnerabilitäten sowie der Einschätzung der raumplanerisch relevanten Risiken und der Betroffenheit von Schutzgütern gegenüber raumplanungsrelevanten Bedrohungen. Dabei geht es im Sinne des § 1 Abs. 1 bzw. § 8 Abs. 6 ROG um Risiken bzw. Gefährdungen, die aufgrund ihrer räumlichen Auswirkungen eine überörtliche und überfachliche Betrachtung erfordern. Ein entscheidender Beitrag der Raumplanung besteht darin, unterschiedliche Risikoquellen und Risikogebiete einerseits und die vorhandenen Kritischen Infrastrukturen andererseits räumlich zu überlagern. Auf diesem Weg können Wechselwirkungen bzw. kumulative Gefahrenlagen erkannt und planerisch berücksichtigt werden.

Um Herangehensweisen an neue raumplanerische Problemstellungen zu entwickeln und zu erproben, hat sich die Durchführung von „Modellvorhaben der Raumordnung“ (MORO) bewährt. Unterstützt durch das BMI und betreut durch das Bundesinstitut für Bau-, Stadt- und

Raumforschung (BBSR) im Bundesamt für Bauwesen und Raumordnung (BBR) wurde innerhalb dieses Aktionsprogramms im Jahr 2013 auch ein Forschungsfeld „Vorsorgendes Risikomanagement in der Regionalplanung“ ins Leben gerufen. In einem ersten Modellvorhaben mit der Bezirksregierung Köln wurden die Potenziale der Regionalplanung zur Risikovorsorge unter besonderer Berücksichtigung der Belange Kritischer Infrastruktur untersucht (vgl. BMVI/BBSR 2015). Dazu wurde gemeinsam mit Trägern der Regionalplanung ein Ansatz für ein integriertes Risikomanagement im Sinne der räumlichen Risikovorsorge entwickelt, der bei der Fortschreibung bzw. Neuaufstellung von Regionalplänen Anwendung finden soll. Es wurden Empfehlungen hinsichtlich dessen erarbeitet,

- welche Informationsgrundlagen zur räumlichen Verteilung von Gefahren und verletzlichen Schutzgütern, insbesondere Kritischer Infrastrukturen, bei der Aufstellung eines Regionalplans herangezogen werden können,
- wie Risikobelange systematisch im Abwägungsprozess Berücksichtigung finden können,
- welche Instrumente sich für die Formulierung raumordnungsrechtlicher Festlegungen zur Kritischen Infrastruktur eignen und
- wie Träger öffentlicher Belange zu beteiligen sind (vgl. Abbildung 8).

Die von der räumlichen Situation ausgehende Herangehensweise an das Risikomanagement eröffnet dem Schutz Kritischer Infrastrukturen eine sektorenübergreifende Perspektive: Es wird nicht nur die Lage einzelner Infrastrukturen zu diversen raumplanungsrelevanten Gefahren sichtbar, sondern auch die Lage der einzelnen Infrastrukturen zueinander. Da gerade die Bündelung unterschiedlicher Infrastrukturen in gefährdeten Gebieten das Risikopotenzial enorm erhöhen kann, ist diese Betrachtungsweise besonders wichtig. Die separate Anwendung einzelner, branchenspezifischer Sicherheitsvorschriften könnte in solchen Fällen zu kurz greifen oder der Suche nach einer ganzheitlichen Lösung im Weg stehen. Hierbei bietet die Raumordnung mit ihrer querschnittsbetonten, überfachlichen und ausgleichenden Funktion die Möglichkeit, eine rein sektorale Sichtweise zu durchbrechen und die durch Infrastrukturbündelung entstehenden Konflikte zu lösen. Es bedarf – dies war eine grundlegende Erkenntnis aus dem Modellvorhaben – systematisierter Informationen bezüglich der Kritikalität von Infrastrukturen, um diese in der Raumordnung angemessen thematisieren und deren Resilienz erhöhen zu können (→ Kapitel 2.1.2).

Durch eine Ausweitung auf zwei weitere Modellregionen, die Regionen Stuttgart und Schleswig-Holstein/Planungsraum I, wurde in einem Anschlussvorhaben inzwischen ein breiteres Spektrum an sowohl regionalplanerischen Organisations- und Rechtsformen, als auch räumlichen, risikobezogenen Problemkonstellationen abgedeckt. Die bei der Ausweitung des Konzeptes auf diese Modellregionen gewonnenen Erkenntnisse sollen zum Abschluss in eine Überarbeitung des Leitfadens einfließen.

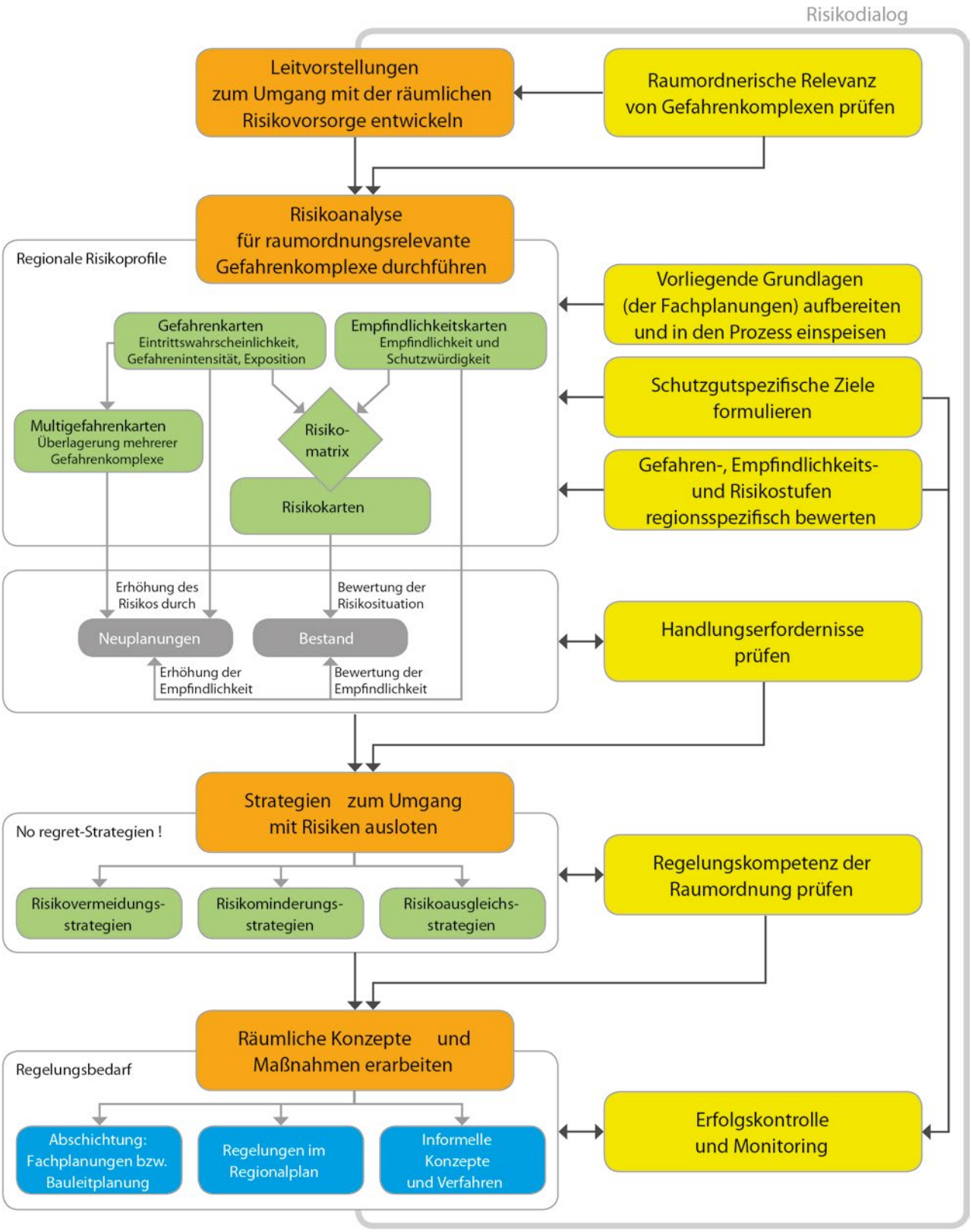
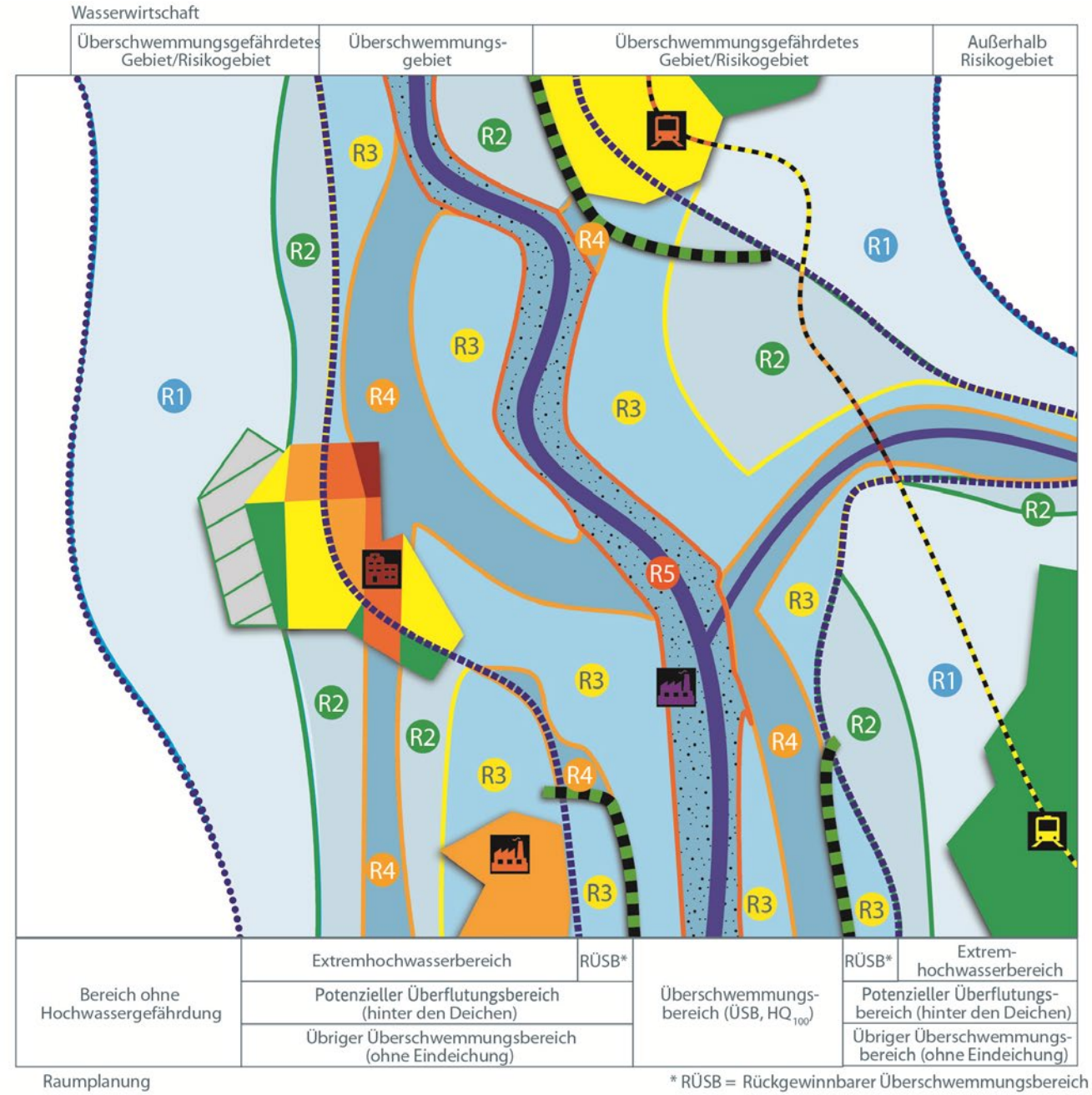


Abbildung 8: Fahrplan für ein integriertes Risikomanagement im Sinne der räumlichen Risikovorsorge in der Regionalplanung (Quelle: agl/prc, in: BMVI/BBSR 2015, S. 139; siehe hierzu auch ARL 2011, Pohl/Zehetmair 2011).

Infobox 4: Raumordnerische Hochwasservorsorge mit neuem Risikoansatz?!

Im Kontext der BBSR-Forschungsprojekte zu einem möglichen „Bundesraumordnungsplan Hochwasserschutz“ nach § 17 Abs. 2 ROG wird auch das Erfordernis einer stärkeren Risikoorientierung der Raumordnung diskutiert. Der Risikoansatz eröffnet die Möglichkeit, multiple raumbezogene Risiken, zum Beispiel Wechselwirkungen im Falle großräumiger Flutkatastrophen, einzuschätzen. Durch diese systematische Verortung und Priorisierung entsteht der Vorteil, dass Maßnahmen zur Reduzierung des Risikos gezielter ergriffen werden können. In diesem Zusammenhang wurde ein praxisorientiertes Handbuch zur Ausgestaltung innovativer Ansätze für die Landes- und Regionalplanung erarbeitet (vgl. BMVI 2017). Besonders hervorzuheben ist der darin vorgestellte differenzierte Ansatz zur raumordnerischen Risikobewertung, wonach die Verwundbarkeit bzw. die Empfindlichkeit von Schutzgütern – z. B. Kritischen Infrastrukturen – aus einer integrierenden Perspektive kartographisch aufbereitet und in einer Risikomatrix nach mehreren Empfindlichkeits- und Hochwassergefahrenstufen bewertet werden kann (vgl. Abbildung 9).

Im Handbuch sind die Überlegungen zum Umgang mit Kritischen Infrastrukturen in der raumordnerischen Risikovorsorge in zwei exemplarische Plansätze eingeflossen. Der erste besagt, dass die Errichtung und der Ausbau Kritischer Infrastrukturen in überschwemmungsgefährdeten Gebieten möglichst unterlassen werden bzw., falls das nicht umsetzbar sein sollte, Objektschutzmaßnahmen vorgeschrieben werden sollen. Es soll also bestenfalls vermieden werden, dass die Kritischen Infrastrukturen einem Hochwasser ausgesetzt sein könnten – wenn das nicht gelingt, sollen sie zumindest keinen Schaden nehmen. Dem zweiten Plansatz zufolge soll in überschwemmungsgefährdeten Gebieten, sofern bauliche Maßnahmen keinen ausreichenden Schutz erlauben, vom „Bündelungsgebot“ abgewichen werden. In den meisten Fällen ist die räumliche Bündelung von Infrastrukturen ein probates Mittel der Raumplanung, um Natur und Landschaft zu schützen – wenn aber gleich mehrere Kritische Infrastrukturen von demselben Hochwasser betroffen sein könnten, würde eine ausgesprochen ungünstige Situation entstehen. Im Handbuch wird betont, dass dem Planungsträger bekannt sein muss, welche Infrastrukturen als kritisch einzustufen sind, um den Schutz Kritischer Infrastrukturen bestmöglich berücksichtigen zu können. Die Identifizierung von Kritischen Infrastrukturen (→ Kapitel 2.1.2) ist also aus Sicht der Autoren des Handbuchs ein sehr wichtiger Planungsschritt.



Risikostufen

Die Risikostufen werden für Siedlungsbereiche und kritische Infrastrukturen flächig dargestellt, für alle weiteren Bereiche mit Symbolen gekennzeichnet.

Risikomatrix	Empfindlichkeitsstufe 1	Empfindlichkeitsstufe 2	Empfindlichkeitsstufe 3
Hochwasser-Gefahrenstufe 1	R 1	R 2	R 3
Hochwasser-Gefahrenstufe 2	R 2	R 3	R 4
Hochwasser-Gefahrenstufe 3	R 3	R 4	R 5
Hochwasser-Gefahrenstufe 4	R 4	R 5	R 6
Hochwasser-Gefahrenstufe 5	R 5	R 6	R 7

Abbildung 9: Raumordnerischer Risikoansatz in der Hochwasservorsorge – Systemskizze zur Risikoeinstufung beim Gefahrenkomplex Flusshochwasser (Quelle: agl/prc, in: BMVI 2017, S. 48).

2.2

Kapitel

Quelle: Christine Müller / Westend61 / Getty Images

Der Handlungsrahmen für den Schutz Kritischer Infrastrukturen

Der Staat, so heißt es im Leitbild zur KRITIS-Strategie „steuert primär moderierend, nötigenfalls normierend, die Maßnahmen zur Sicherung und zur Sicherstellung des Gesamtsystems sowie der Systemabläufe“ (BMI 2009, S. 2). Diesem Leitgedanken entsprechend lag und liegt der Schwerpunkt beim Schutz Kritischer Infrastrukturen auf nichtregulativen Instrumenten. Ein übergreifendes „Gesetz zum Schutz Kritischer Infrastrukturen“ gibt es in Deutschland nicht. Allerdings wurden im Lauf der Zeit einzelne Aspekte des Schutzes Kritischer Infrastrukturen in Fachgesetzen festgeschrieben (→ Kapitel 2.2.1), sei es um Vorgaben von europäischer Ebene in deutsches Recht zu überführen oder um auf nationaler Ebene erkannten Regelungsbedarf zu decken. Die rechtlichen Regelungen mit explizitem Bezug zum Schutz Kritischer Infrastrukturen haben unterschiedliche Formen und Funktionen: Sie formulieren teilweise abstrakte Zielsetzungen, schreiben Befugnisse von Behörden fest oder machen konkrete Vorgaben für Betreiber. Insbesondere das 2015 in Kraft getretene *IT-Sicherheitsgesetz* hat als Artikelgesetz Spuren in vielen Fachgesetzen hinterlassen. Es hat den Bedarf ausgelöst, Aspekte seiner Umsetzung per Verordnung untergesetzlich zu regeln, und zudem die Entwicklung von Standards zur rechtssicheren Umsetzung in Gang gesetzt. Anhand des *Energiewirtschaftsgesetzes* lässt sich nachvollziehen, wie der allgemeine Rechtsrahmen zum Schutz Kritischer Infrastrukturen mit bereichsspezifischen Regelungen verknüpft wird (→ Infobox 5).

Normen und Standards werden zur Konkretisierung gesetzlicher Vorgaben genutzt, insbesondere hinsichtlich des abstrakten „Stands der Technik“, auf den Gesetze häufig Bezug nehmen. Diese Funktion erfüllen sie auch im Kontext des Schutzes Kritischer Infrastrukturen (→ Kapitel 2.2.2): Sie kommen in der einen oder anderen Form in allen Sektoren Kritischer Infrastrukturen zur Anwendung, enthalten technische Spezifikationen, beschreiben Verfahrensweisen oder organisatorische Abläufe. Viele Normen und Standards haben ganz generell zuverlässige und sichere Abläufe zum Ziel, manche beziehen sich aber auch ganz ausdrücklich auf den Schutz Kritischer Infrastrukturen. Doch nicht nur die fertigen Normen und Standards entfalten Wirkung: Bei ihrer Erarbeitung werden mitunter neue Themen in einem strukturierten Prozess von Expertenseite beleuchtet und gemeinsame Positionen gefunden.

Lange bevor sich der Politikbereich Schutz Kritischer Infrastrukturen etablierte, wurde die Aufrechterhaltung zentraler Versorgungsleistungen in definierten Krisensituationen Gegenstand gesetzlicher Regelungen (→ Kapitel 2.2.3): Die Vorsorgegesetze enthalten Regelungen zur Bewältigung von Versorgungsengpässen in Friedenszeiten, während die Sicherstellungsgesetze auf Versorgungskrisen im Spannungs- oder Verteidigungsfall ausgelegt sind (Art. 80a oder 115a GG). Die in diesen Gesetzen adressierten Versorgungsbereiche korrespondieren zu einem gewissen Grad mit den Sektoren Kritischer Infrastrukturen. Ein Beispiel für eine Rechtsnorm, die Versorgungskrisen sowohl in Friedenszeiten als auch im Spannungs- und Verteidigungsfall adressiert, ist das 2017 novellierte *Ernährungsvorsorge- und -sicherstellungsgesetz* (→ Infobox 6).

2.2.1 Schutz Kritischer Infrastrukturen in der Gesetzgebung des Bundes

Ende 2008 wurde die Richtlinie über die *Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern* (RL 2008/114/EG) verabschiedet und trat Anfang 2009 in Kraft. Damit wurde von europäischer Ebene ein erster Impuls an alle Mitgliedsstaaten gegeben, Aspekte zum Schutz explizit *kritischer* Infrastrukturen in gesetzliche Regelungen zu überführen (→ Kapitel 2.6.1). Gegenstand der Richtlinie sind *europäische* kritische Infrastrukturen, verstanden als „in einem Mitgliedstaat gelegene kritische Infrastruktur[en], deren Störung oder Zerstörung erhebliche Auswirkungen in mindestens zwei Mitgliedstaaten hätte“ (Art. 2b RL 2008/114/EG). Die Implementierung der Richtlinie setzte in Deutschland ein erstes Identifizierungsverfahren in den Sektoren *Verkehr und Energie* in Gang und bewirkte eine Änderung im *Energiewirtschaftsgesetz* (EnWG, → Infobox 5).

Auf nationaler Ebene machte fast zeitgleich das *Raumordnungsgesetz* (ROG) den Anfang. Bei einer umfangreichen Novellierung des Gesetzes

Ende 2008 wurde der Passus „dem Schutz kritischer Infrastrukturen ist Rechnung zu tragen“ (§ 2 Abs. 2 Nr. 3 ROG) in die Grundsätze der Raumordnung aufgenommen. Seitdem sind die Belange des Schutzes Kritischer Infrastrukturen in Abwägungs- und Ermessensentscheidungen im Kontext raumbedeutsamer Planungen und Maßnahmen zu berücksichtigen (vgl. § 4 ROG). Die Raumordnung soll sich, vereinfacht gesprochen, mit den ihr zur Verfügung stehenden Mitteln am Risikomanagement bezogen auf Kritische Infrastrukturen beteiligen (→ Kapitel 2.1.4 und Infobox 4).

Kurz darauf, im Jahr 2009, wurden Aspekte des Schutzes Kritischer Infrastrukturen ins *Zivilschutz- und Katastrophenhilfegesetz* (ZSKG) aufgenommen. Das Gesetz regelt die Befugnisse des BBK, Daten über Kritische Infrastrukturen zu erheben und zu verarbeiten (§ 17 Abs. 1 Nr. 3 ZSKG) und konkretisiert mit seiner Definition auch die Schwerpunktsetzung des Bevölkerungsschutzes: Es geht dem Gesetz nach um „Infrastrukturen, bei deren Ausfall die Versorgung der Bevölkerung erheblich beeinträchtigt wird (kritische Infrastrukturen)“ (§ 17 Abs. 1 Nr. 3 ZSKG). Weiterhin gibt das *Zivilschutz- und Katastrophenhilfegesetz* dem Bund auf, die Länder beim Schutz Kritischer Infrastrukturen zu beraten und zu unterstützen (vgl. § 18 Abs. 2 ZSKG).

Im Jahr 2015 trat das *IT-Sicherheitsgesetz* (IT-SiG) in Kraft. Es hat zum Ziel, die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit von IT-Systemen zu verbessern, insbesondere von IT-Systemen, die beim Betrieb von Kritischen Infrastrukturen eingesetzt werden. Im Klartext: Kritische Infrastrukturen sollen besser gegen Gefahren gewappnet sein, die sich über IT-Systeme ausbreiten oder auswirken. Als Artikelgesetz führte das *IT-Sicherheitsgesetz* zu Änderungen in vielen weiteren Gesetzen, u. a. im *Energiewirtschaftsgesetz* (→ Infobox 5), vor allem aber im *Gesetz über das Bundesamt für Sicherheit in der Informationstechnik* (BSIG). Es erteilt dem BSI seitdem weitere Aufgaben und Befugnisse und legt den Betreibern Kritischer Infrastrukturen zusätzliche Pflichten auf (z. B. Meldepflichten für IT-Sicherheitsvorfälle oder die Auflage, die eigenen Systeme nach dem „Stand der Technik“ abzusichern und dies auch nachzuweisen (→ Kapitel 2.2.2).

Dazu musste verbindlich bestimmt werden, welche konkreten Anlagen als Kritische Infrastrukturen „im Sinne des Gesetzes“ betrachtet werden. Es bedurfte also einer Identifizierung jener „Einrichtungen, Anlagen oder Teile davon, die (1) den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und (2) von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden“ (§ 2 Abs. 10 BSIG) . Das Identifizierungsverfahren für die sieben regulierten Sektoren der Kritischen Infrastrukturen wurde in der *BSI-Kritisverordnung* (BSI-KritisV) geregelt (→ Kapitel 2.1.2, Kapitel 2.4.2 und Infobox 16).

Als die im Jahr 2016 auf europäischer Ebene verabschiedete *Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen* (die sogenannte „NIS-Richtlinie“, RL 2016/11487/EU) in deutsches Recht überführt werden musste, war mit dem IT-Sicherheitsgesetz bzw. dem BSIG bereits eine Grundlage geschaffen worden. Mit einem Umsetzungsgesetz wurden die Befugnisse des BSI den Vorgaben der Richtlinie entsprechend erweitert. Inzwischen wird das BSIG bzw. die BSI-KritisV auch herangezogen, um den Adressatenkreis weiterer Rechtsnormen zu bestimmen. So räumt die *Außenwirtschaftsverordnung* (AWV) seit einer Novelle Ende 2018 dem Bundesministerium für Wirtschaft und Energie (BMWi) die Option zur Prüfung von Unternehmensbeteiligungen an Betreibern Kritischer Infrastrukturen gemäß BSIG bereits ab einer von 25% auf 10% abgesenkten Eingriffsschwelle ein (vgl. § 55 AWV).

Einen etwas anderen Weg geht das *Telekommunikationsgesetz* (TKG). Es wurde mit dem Gesetz zur Erleichterung des *Ausbaus digitaler Hochgeschwindigkeitsnetze* (DigiNetzG) im Jahr 2016 geändert und enthält nun insbesondere in einem Unterabschnitt zur „Mitnutzung öffentlicher Versorgungsnetze“ eine Reihe von Ausnahmen im Interesse des Schutzes Kritischer Infrastrukturen. So kann z.B. auf die Aufnahme bestimmter Informationen in den von der Bundesnetzagentur (BNetzA) geführten „Infrastrukturatlas“ verzichtet

werden, wenn „Teile einer Infrastruktur betroffen sind, die durch Gesetz oder aufgrund eines Gesetzes als kritische Infrastrukturen bestimmt worden und nachweislich besonders schutzbedürftig und für die Funktionsfähigkeit der kritischen Infrastruktur maßgeblich sind“ (§ 77a Abs. 4 Nr. 3 TKG). Die offene Formulierung „durch Gesetz oder aufgrund eines Gesetzes“ schließt das BSIG und die BSI-KritisV ein, aber auch das *Energiewirtschaftsgesetz* (→ Infobox 5; vgl. BT-Drs 18/8332, S. 41). Falls in Zukunft weitere Gesetze Kritische Infrastrukturen in ihrem Sinne bestimmen sollten, ist im *Telekommunikationsgesetz* bereits eine Schnittstelle dafür angelegt.

Infobox 5: Schutz Kritischer Infrastrukturen auf Basis des *Energiewirtschaftsgesetzes*

Zweck des *Energiewirtschaftsgesetzes* ist „eine möglichst sichere, preisgünstige, verbraucherfreundliche, effiziente und umweltverträgliche leitungsgebundene Versorgung der Allgemeinheit mit Elektrizität und Gas, die zunehmend auf erneuerbaren Energien beruht“ (§ 1 Abs. 1 EnWG). Die Sicherheit der Versorgung wird also gleich zu Beginn der Rechtsnorm ganz grundsätzlich als ein Ziel formuliert und im Gesetz an vielen unterschiedlichen Stellen konkretisiert. Man kann mit anderen Worten sagen, dass die Interessen des Schutzes Kritischer Infrastrukturen vielfach im EnWG mitgedacht worden sind, ohne dass es hierzu einer ausdrücklichen Bezugnahme bedarf. Überdies kann anhand des EnWG nachvollzogen werden, wie der allgemeine Rechtsrahmen zum Schutz Kritischer Infrastrukturen mit bereichsspezifischen Regelungen verknüpft wird.

Mit der Umsetzung der 2008 verabschiedeten RL 2008/114/EG in nationales Recht hat sich zunächst der Schutz *europäisch* Kritischer Infrastrukturen ins EnWG eingeschrieben (→ Kapitel 2.6.1): § 12g EnWG enthält nun Bestimmungen bezogen auf „Anlagen oder Teile von Anlagen des Übertragungsnetzes, deren Störung oder Zerstörung erhebliche Auswirkungen in mindestens zwei Mitgliedstaaten der Europäischen Union haben kann (europäisch kritische Anlage)“. Alle zwei Jahre wird durch die BNetzA als Regulierungsbehörde bestimmt, welche konkreten Anlagen als solche zu verstehen sind und welche Betreiber infolge dessen die hier formulierten Auflagen erfüllen müssen.

Auch das im Jahr 2015 erlassene *IT-Sicherheitsgesetz* hat seine Spuren im EnWG hinterlassen (→ Infobox 16). So adressieren § 11 Abs. 1b und 1c EnWG die Betreiber von Energieversorgungsnetzen und von solchen Energieanlagen, „die durch Inkrafttreten der Rechtsverordnung gemäß § 10 Absatz 1 des *BSI-Gesetzes* als Kritische Infrastruktur bestimmt wurden“. Das EnWG verpflichtet die Betreiber, einen angemessenen Schutz gegen Bedrohungen für die von ihnen eingesetzten Telekommunikations- und elektronischen Datenverarbeitungssysteme zu gewährleisten (vgl. § 11 Abs. 1b EnWG). Die dabei von den Betreibern zu erfüllenden Anforderungen sind in den sogenannten Sicherheitskatalogen näher beschrieben, die von der BNetzA im Benehmen mit dem BSI erarbeitet worden sind. Nach § 11 Abs. 1c EnWG müssen die Betreiber überdies erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit von IT-Systemen, Komponenten und Prozessen an das BSI melden.

2.2.2 Normung und Standardisierung – ein wichtiger Baustein für die Umsetzung des Schutzes Kritischer Infrastrukturen

Normen und Standards ergänzen rechtliche Grundlagen und legen die allgemein anerkannten Regeln der Technik fest. Sie werden von Normungsinstituten, wie dem Deutschen Institut für Normung e. V. (DIN), herausgegeben. Als eingetragene Vereine dienen sie auf gemeinnütziger Basis als nationale oder internationale Plattformen für die Normung. Darüber hinaus werden normenähnliche Regelwerke von Verbänden mit nationaler Bedeutung herausgegeben, wie z. B. dem Forum Netztechnik/Netzbetrieb (FNN) im Verband der Elektrotechnik Elektronik Informationstechnik e. V. (VDE), dem Deutschen Verein des Gas- und Wasserfaches e. V. (DVGW) oder der Deutschen Vereinigung für Wasserwirtschaft, Abwasser und Abfall e. V. (DWA). Diese Institutionen entwickeln ebenfalls allgemein anerkannte Regeln der Technik. Auch im Kontext des Schutzes Kritischer Infrastrukturen bieten Normen und Standards die Möglichkeit, gesetzliche Vorgaben zu konkretisieren, einheitliche Verfahren und Regelungen für einzelne Branchen festzulegen und damit die Rechtssicherheit für die Betreiber zu erhöhen. Zudem kann die Arbeit an Normen und Standards dazu beitragen, innovative Ansätze zum Schutz Kritischer Infrastrukturen zu diskutieren und somit neue Themen in den Normungsprozess einzubringen. Alle Normen und Standards werden in einem transparenten Verfahren in Expertengruppen unter Einbeziehung der Fachöffentlichkeit erarbeitet. Die enge Zusammenarbeit zwischen Betreibern Kritischer Infrastrukturen, Verbänden sowie Experten aus Behörden, Wirtschaft und Forschung trägt zur Weiterentwicklung der Regelwerke bei und somit auch zum Schutz Kritischer Infrastrukturen.

Normen und Standards können Verfahren beschreiben und vereinheitlichen. Hierbei greifen sie auch für den Schutz Kritischer Infrastrukturen wichtige Themen wie z. B. das Risiko- und Krisenmanagement auf. Beispielsweise befasst sich die DIN ISO 31000:2018-10 „Risikomanagement – Leitlinien“ mit Verfahrensweisen beim Risikomanagement. Die DIN-Spezifikation, DIN SPEC 91390:2019-12 „Integriertes Risikomanagement für den Schutz der Bevölkerung“, greift daraus den Spezialaspekt der Zusammenarbeit von staatlichen und kommunalen Akteuren mit Betreibern Kritischer Infrastrukturen heraus (→ Kapitel 2.4.3 und Infobox 17). DIN-Spezifikationen entfalten keine eigenständig bindende oder verpflichtende Wirkung, sie können aber in einen tatsächlichen Normungsprozess münden. Die meist branchenspezifischen technischen Regelwerke enthalten Vorgaben für Planung, Bau und Betrieb von bestimmten Anlagen. Sie können durch Merkblätter oder Informationen ergänzt werden, die den Fokus beispielsweise auf bestimmte Szenarien wie Extremwetterereignisse oder Stromausfall legen. So wurde z. B. in der Branche Gasversorgung ein neues Merkblatt „Hinweise zur Aufrechterhaltung der sicheren Gasversorgung bei Ausfall der regulären Kommunikation“ erarbeitet (DVGW G 1003). In der Branche Abwasserentsorgung wird aktuell ein Merkblatt erstellt, das sich der Risikoabschätzung und der Bewältigung eines langandauernden, großflächigen Stromausfalls widmet (DWA M 320 „Sicherstellung der Abwasserentsorgung bei Stromausfall“). Das Merkblatt DWA M 551: Audit „Hochwasser – wie gut sind wir vorbereitet“ nimmt die Vorbereitung auf Hochwasser- und Starkregenereignisse in den Blick.

Auch im Bereich der Normung und Standardisierung spielt die europäische Ebene eine große Rolle. Zur Gewährleistung eines sicheren Betriebes der großen europäischen Verbundnetze erstellen z. B. der Verband Europäischer Übertragungsnetzbetreiber für Strom (ENTSO-E) und der Verband Europäischer Fernleitungsnetzbetreiber für Gas (ENTSO-G) für alle Netzpartner verbindliche Regelwerke zum Netzbetrieb, die „Network Codes“. Oft müssen Normungs- und Standardisierungsverfahren auf europäischer und nationaler Ebene miteinander in Einklang gebracht werden. Beispielsweise wurden in der Wasserversorgung zunächst auf nationaler Ebene unter Leitung des DVGW die Hinweise zum Risikomanagement (W 1001) und zum Krisenmanagement (W 1002) in der Trinkwasserversorgung erarbeitet. Nachfolgend wurden diese DVGW-Hinweise auf europäischer Ebene genormt und in die wasserfachlichen Normen DIN EN 15975-1 „Sicherheit der Trinkwasserversorgung – Leitlinien für das Risiko- und

Krisenmanagement – Teil 1: Krisenmanagement“ sowie DIN EN 15975-2 „Sicherheit der Trinkwasserversorgung – Leitlinien für das Risiko- und Krisenmanagement – Teil 2: Risikomanagement“ überführt.

Die steigende Bedeutung der IT-Sicherheit im Kontext des Schutzes Kritischer Infrastrukturen spiegelt sich erwartungsgemäß auch in der Erstellung von Normen und Standards wider. Im Rahmen des IT-Grundschutzes wurden durch das BSI die BSI-Standards erstellt. Sie geben u. a. Hinweise zum Verfahren der Risikoanalyse sowie zum Notfallmanagement (vgl. BSI-Standard 200-2 „IT-Grundschutz-Methodik“). Für Betreiber Kritischer Infrastrukturen im Sinne von § 2 Abs. 10 BSIG gelten besondere Anforderungen an die IT-Sicherheit (→ Kapitel 2.2.1): Sie sind gemäß § 8a Abs. 1 BSIG verpflichtet, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Der dabei einzuhaltende Stand der Technik kann in „branchenspezifischen Sicherheitsstandards“ (B3S) konkretisiert werden (→ Infobox 16). Als Beispiel sei das von DVGW und DWA herausgegebene Merkblatt 1060 „IT-Sicherheit – Branchenstandard Wasser/ Abwasser“ genannt. In einigen Fällen wurden die im *IT-Sicherheitsgesetz* formulierten Anforderungen in Fachgesetze integriert, in das *Energiewirtschaftsgesetz* und das *Telekommunikationsgesetz*. Hierbei konkretisieren „IT-Sicherheitskataloge“ die Anforderungen an die Betreiber (BNetzA 2015; BNetzA 2016; BNetzA 2018). Die IT-Sicherheitskataloge zum *Energiewirtschaftsgesetz* wurden von der BNetzA im Benehmen mit dem BSI erstellt, der IT-Sicherheitskatalog zum *Telekommunikationsgesetz* im Einvernehmen mit dem BSI und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI).

Normen und Standards, die zum Schutz Kritischer Infrastrukturen und zur Versorgungssicherheit der Bevölkerung beitragen, werden ständig in den jeweiligen Expertengremien, in denen zumeist auch Vertreterinnen und Vertreter der zuständigen Fachbehörden ihre Perspektive einbringen, weiterentwickelt und an die sich wandelnden Herausforderungen angepasst.

2.2.3 Gesetzliche Grundlagen zur Bewältigung von Versorgungskrisen

Schon bevor sich ab Ende der 1990er-Jahre der Schutz Kritischer Infrastrukturen etablierte, war die Aufrechterhaltung von zentralen Versorgungsleistungen eine wichtige staatliche Aufgabe. Dazu wurde seit den 1960er-Jahren sukzessive eine Reihe von Gesetzen für definierte Krisensituationen verabschiedet (vgl. Tabelle 4). Einige dieser Gesetze beziehen sich auf Versorgungsengpässe in Friedenszeiten, die *Vorsorgegesetze*; andere sind ausdrücklich mit den Artikeln 80a oder 115a des Grundgesetzes verknüpft und damit konkret für den Spannungs- oder Verteidigungsfall gedacht, die *Sicherstellungsgesetze*. Um die Gesetze anwenden zu dürfen, muss in der Regel die Bundesregierung formal den Anwendungsfall feststellen oder sogar das Parlament einen entsprechenden Beschluss fassen. Davon ausgenommen sind nur Regelungen zu Vorsorgemaßnahmen, die bereits im „Normalzustand“ umzusetzen sind (z.B. bauliche Maßnahmen oder die Vorhaltung bestimmter Ressourcen).

Die Vorsorge- und Sicherstellungsgesetze sollen gewährleisten, dass die Grundversorgung mit Gütern und Dienstleistungen sowohl für die Zivilbevölkerung als auch für die Streitkräfte gesichert ist (→ Kapitel 2.3.2). Dazu regeln sie beispielsweise innerhalb einiger Sektoren (→ Infobox 2), wie knappe Ressourcen in der Krise zu verteilen sind. Beispielsweise können auf Grundlage des *Energiesicherungsgesetzes* Regelungen zur Erzeugung und Verteilung von Strom getroffen werden, um in einer Mangelsituation den lebensnotwendigen Energiebedarf decken zu können. Das *Arbeitssicherstellungsgesetz* ermöglicht es, bestimmte Personengruppen in benötigte Arbeitsverhältnisse zu verpflichten, wobei die meisten KRITIS-Sektoren ausdrücklich als Anwendungsfall genannt sind. Für die Details verweisen die Vorsorge- und Sicherstellungsgesetze häufig auf – ggf. unter Beteiligung des Bundesrates – zu erstellende oder bereits vorhandene Rechtsverordnungen.

KRITIS-Sektor	*Vorsorge- und Sicherstellungsgesetze*
Energie	*Energiesicherungsgesetz* (EnSiG) *Erdölbevorratungsgesetz* (ErdölBevG) *Wirtschaftssicherstellungsgesetz* (WiSiG)
Informationstechnik und Telekommunikation	*Post- und Telekommunikationssicherstellungsgesetz* (PTSG)
Transport und Verkehr	*Verkehrsleistungsgesetz* (VerkLG) *Verkehrssicherstellungsgesetz* (VerkSiG)
Wasser	*Wassersicherstellungsgesetz* (WasSiG)
Ernährung	*Ernährungssicherstellungs- und -vorsorgegesetz* (ESVG)
Finanz- und Versicherungswesen	*Wirtschaftssicherstellungsgesetz* (WiSiG)
Bezug zu allen Sektoren	*Arbeitssicherstellungsgesetz* (ASG) *Bundesleistungsgesetz* (BLG)

Tabelle 4: Vorsorge- und Sicherstellungsgesetze mit Bezug zu Kritischen Infrastrukturen (Zusammenstellung: BBK).

Es ist nicht überraschend, dass sich viele der Vorsorge- und Sicherstellungsgesetze auf die Bereitstellung von Gütern und Dienstleistungen beziehen, die auch beim Schutz Kritischer Infrastrukturen eine Rolle spielen (vgl. Tabelle 4). Letztlich ist der Schutz Kritischer Infrastrukturen eine permanente Aufgabe und soll dazu führen, dass die Versorgung jederzeit gewährleistet ist. Die Vorsorge- und Sicherstellungsgesetze ergänzen in einigen Bereichen und für definierte Krisenzeiten die rechtlichen Grundlagen, sodass knappe Ressourcen in Versorgungskrisen bestmöglich genutzt werden können. Dazu können sie z. B. auch marktwirtschaftliche Mechanismen außer Kraft setzen.

Damit die in den Vorsorge- und Sicherstellungsgesetzen vorgesehenen Maßnahmen bestmöglich zur Bewältigung von Krisen beitragen können, müssen sie bei den entscheidenden Akteuren präsent gehalten werden. Sie sind daher immer wieder Gegenstand von Übungen. Die Anwendung des *Energiesicherungsgesetzes* wurde beispielsweise im Rahmen der „LÜKEX 2018“ beübt (BBK 2019b; → Kapitel 2.4.4). Die Sicherstellungsgesetze werden zudem im Rahmen der Umsetzung der „Konzeption Zivile Verteidigung“ (BMI 2016b; → Kapitel 2.3.2) auf ihren Novellierungsbedarf geprüft. Das *Post- und Telekommunikationssicherstellungsgesetz* sowie das *Ernährungssicherstellungs- und -vorsorgegesetz* (→ Infobox 6) wurden in den letzten Jahren bereits überarbeitet. In beiden Fällen wurden ursprünglich getrennte Gesetze für den Spannungs-/Verteidigungsfall einerseits und für friedenszeitliche Krisen andererseits zu einem übergreifenden Gesetz zusammengeführt. Dies sollte u.a. dazu führen, dass unterschiedlichen Ursachen normativ mit gleichen Mitteln begegnet wird und dadurch Ressourcen effektiver eingesetzt werden können. Das *Wassersicherstellungsgesetz* (WasSiG) dient primär der Vorsorge im Verteidigungsfall (§ 1). Nach § 8 WasSiG ist allerdings mit Zustimmung der zuständigen Behörden die Nutzung von Anlagen, die aufgrund von Verpflichtungen nach § 2 WasSiG erbaut wurden, grundsätzlich auch zu Zwecken jenseits der Wassersicherstellung im Verteidigungsfall möglich (Doppelnutzen).

Infobox 6: Die Novellierung des *Ernährungssicherstellungs- und -vorsorgegesetzes*

Vor 2017 war die Ernährung in Krisenzeiten über das *Ernährungssicherstellungsgesetz* und das *Ernährungsvorsorgegesetz* geregelt. Ersteres war für den Spannungs- und Verteidigungsfall, letzteres für sonstige Versorgungskrisen gedacht. Beide enthielten jedoch teils unterschiedliche Regelungen und waren nicht mehr zeitgemäß. Das Bundesministerium für Ernährung und Landwirtschaft (BMEL) setzte daraufhin mehrere Forschungsvorhaben auf, die unterschiedliche Aspekte einer Umgestaltung der Regelungen beleuchteten. Unter anderem wurde die Rechtslage zur Ernährungsnotfallvorsorge analysiert, Defizite wurden dargelegt und Änderungsvorschläge aufgezeigt. Zudem wurden im Projekt „Neue Strategien der Ernährungsnotfallvorsorge“ (NeuENV), gefördert durch das Bundesministerium für Bildung und Forschung (BMBF) im Programm „Forschung für die zivile Sicherheit“ (→ Kapitel 2.3.3), Handlungsempfehlungen für neue Strategien der Ernährungsnotfallvorsorge erarbeitet. Die Perspektiven aller relevanten Akteure – der Unternehmen der Lebensmittelkette, der politischen Entscheider, der Hilfsorganisationen und auch der Bevölkerung – wurden bei der Erarbeitung berücksichtigt.

Schließlich wurden im Jahr 2017 beide Gesetze zum *Ernährungssicherstellungs- und -vorsorgegesetz* (ESVG) zusammengeführt. Das ESVG deckt seitdem sowohl die verteidigungsbezogene Sicherstellung als auch die friedenszeitliche Vorsorge ab. Die Anwendung des ESVG ist an die Bedingung der Feststellung einer Versorgungskrise durch die Bundesregierung geknüpft. Es enthält aber auch Regelungen zur Vorsorge vor Feststellung der Versorgungskrise. Zum Beispiel verpflichtet es Bund und Länder, den Selbstschutz der Bevölkerung vor den Folgen einer Versorgungskrise zu stärken und über private Vorsorgemaßnahmen zu informieren (vgl. Abbildung 10). Dies geschieht z. B. über ein von der Bundesanstalt für Landwirtschaft und Ernährung (BLE) bereitgestelltes, spezielles Internetportal (www.ernaehrungsvorsorge.de) und einen Informationsstand bei der „Internationalen Grünen Woche“ in Berlin.

Abbildung 10: Beispielhafter Notvorrat für die Bevölkerung (Quelle: Lechner / BBK).

2.3

Kapitel

Quelle: Volker Pape / EyeEm / Getty Images

Schutz Kritischer Infrastrukturen als inhaltliches Querschnittsthema

Der Schutz Kritischer Infrastrukturen hat vielfältige Berührungspunkte mit anderen Politikbereichen. Aus diesem Grund finden sich Teilaspekte des Schutzes Kritischer Infrastrukturen auch in weiteren politischen Strategiedokumenten wieder und werden dort kontextspezifisch aufgegriffen (→ Kapitel 2.3.1). Beispielsweise fokussieren einige der betreffenden Strategien auf Ausschnitte aus dem Gefahrenspektrum; andere konzentrieren sich auf einen Sektor oder eine Branche. Einen besonders großen Rahmen spannt das „Sendai Rahmenwerk für Katastrophenvorsorge" (NKS 2019): Es deckt das gesamte All-Gefahrenspektrum ab und fasst den Schutz Kritischer Infrastrukturen als Beitrag zur gesamtgesellschaftlichen Katastrophenvorsorge auf.

Die „Konzeption Zivile Verteidigung" (BMI 2016b) bildet den zivilen Teil der Gesamtverteidigung ab, fokussiert also auf Gefahren, die im Zusammenhang mit bewaffneten Konflikten und hybriden Bedrohungslagen auftreten können (→ Kapitel 2.3.2). Aspekte des Schutzes Kritischer Infrastrukturen sind integraler Bestandteil der Konzeption und treten dementsprechend auch an mehreren Stellen zutage. Beispielsweise können Vorgaben zur Aufrechterhaltung von Staats- und Regierungsfunktionen als gefahrenspezifische Maßnahmen für den Schutz Kritischer Infrastrukturen im Sektor *Staat und Verwaltung* aufgefasst werden (→ Infobox 11).

Um gezielt den wissenschaftlichen Erkenntnisgewinn zum Nutzen des Schutzes Kritischer Infrastrukturen fördern zu können (→ Kapitel 2.3.3), ist eine Säule des Rahmenprogramms „Forschung für die zivile Sicherheit" (BMBF 2018) diesem Themenfeld gewidmet. In allen Forschungsprojekten werden Anwender wie Behörden und Organisationen mit Sicherheitsaufgaben oder Infrastrukturbetreiber eng einbezogen, um die Praxistauglichkeit der entwickelten Lösungen sicherzustellen. Zudem werden gesellschaftliche, rechtliche oder ethische Fragen von vornherein berücksichtigt. Im Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit werden Forschungsvorhaben mit Bezug zum Schutz Kritischer Infrastrukturen gefördert, die spezifisch auf IT-Sicherheit ausgerichtet sind.

2.3.1 Schutz Kritischer Infrastrukturen in politischen Strategien

Der Schutz Kritischer Infrastrukturen adressiert gesellschaftswichtige Infrastrukturen in neun Sektoren bzw. 29 Branchen (→ Infobox 2) und verfolgt dabei einen All-Gefahren-Ansatz, demzufolge keine Gefahrenart grundsätzlich ausgeklammert werden kann (→ Kapitel 1.2). Diesen breiten Gegenstandsbereich teilt sich der Schutz Kritischer Infrastrukturen mit einer ganzen Reihe weiterer Politikbereiche. Das kommt u. a. darin zum Ausdruck, dass Strategiedokumente aus anderen Politikbereichen Teilaspekte des Schutzes Kritischer Infrastrukturen aufgreifen, etwa indem sie sich mit einem Ausschnitt aus dem All-Gefahren-Spektrum vertieft auseinandersetzen oder sich besonders intensiv mit einer Auswahl der Sektoren oder Branchen beschäftigen.

Zu den „gefahrenspezifischen" Strategien mit engem Bezug zum Schutz Kritischer Infrastrukturen gehört z. B. die „Cyber-Sicherheitsstrategie für Deutschland" (CSS, BMI 2016a), die Gefahren aus dem Cyber-Raum in den Blick nimmt. Diese Gefahren können sich über informationstechnische Systeme ausbreiten und auswirken, wie sie in allen Sektoren Kritischer Infrastrukturen verbreitet eingesetzt werden (→ Infobox 7). Im Kontext der „Deutschen Anpassungsstrategie an den Klimawandel" (DAS, BReg 2008) spielt eine ganze Palette unterschiedlicher Phänomene aus dem Naturgefahrenspektrum eine Rolle (→ Infobox 8). Einerseits haben CSS und DAS hinsichtlich des Gefahrspektrums einen schmaleren Fokus als die KRITIS-Strategie (BMI 2009). Andererseits sind die Kritischen Infrastrukturen nur ein Ausschnitt des gesamten Gegenstandsbereichs von CSS und DAS. Es gibt also eine gewisse inhaltliche Schnittmenge zwischen allen drei Strategien, gleichzeitig gehen sie alle in einer jeweils unterschiedlichen Weise über diese Schnittmenge hinaus.

Die „Sicherheitsstrategie für die Güterverkehrs- und Logistikwirtschaft" (BMVI 2014) ist ein Beispiel für ein branchenspezifisches Strategiedokument, das sich direkt auf den Schutz Kritischer Infrastrukturen und die KRITIS-Strategie bezieht. Es konkretisiert, was der Schutz Kritischer Infrastrukturen für die Güterverkehrs- und Logistikwirtschaft bedeutet. Der Gegenstandsbereich der

KRITIS-Strategie „umschließt“ den der „Sicherheitsstrategie für die Güterverkehrs- und Logistikwirtschaft“, die KRITIS-Strategie kann allerdings mit ihrer sektorübergreifenden Perspektive die Belange einer einzelnen Branche nicht in der hierbei erreichten Tiefe beleuchten (→ Infobox 9).

Das „Sendai Rahmenwerk für Katastrophenvorsorge 2015-2030“ der Vereinten Nationen (UN ISDR 2015; NKS 2019) „umschließt“ den Schutz Kritischer Infrastrukturen. Wie die KRITIS-Strategie verfolgt auch das Sendai Rahmenwerk einen All-Gefahren-Ansatz. Gleichzeitig beschränkt sich das Rahmenwerk nicht auf die Aufgabenbereiche des Schutzes Kritischer Infrastrukturen: Es fasst den Schutz Kritischer Infrastrukturen als *einen* Aspekt der gesamtgesellschaftlichen Katastrophenvorsorge neben einer Reihe weiterer auf. Der Schutz Kritischer Infrastruktur erscheint aus dieser Perspektive als ein Baustein auf dem Weg zu einer resilienten Gesellschaft (→ Infobox 10).

Infobox 7: Die „Cyber-Sicherheitsstrategie für Deutschland“

Erste Weichen für eine Cyber-Sicherheitsstrategie wurden 2005 mit dem „Nationale Plan zum Schutz der Informationsinfrastrukturen“ (NPSI; BMI 2005b) gestellt, wobei der Fokus noch dezidiert auf dem Schutz der Informationstechnik und den Informationsinfrastrukturen lag (→ Kapitel 1.1). Der NPSI stellte den Beitrag sicherer Informationsinfrastrukturen zur Inneren Sicherheit Deutschlands heraus und nahm Staat und Wirtschaft in die Pflicht, zur Verbesserung des IT-Sicherheitsniveaus beizutragen. Zwei Umsetzungspläne begleiteten den NPSI. Der erste richtet sich an die Bundesverwaltung, der „Umsetzungsplan Bund“ (aktuelle Fassung: BMI 2017). Der zweite, der „Umsetzungsplan KRITIS“ (BMI 2007a), adressiert in erster Linie die Betreiber Kritischer Infrastrukturen, aber letztlich auch deren Fachverbände und die zuständigen Behörden. Daraus ging der UP KRITIS als Kooperation zwischen Staat und Wirtschaft hervor (→ Kapitel 2.4.2).

Der NPSI wurde 2011 durch die „Cyber-Sicherheitsstrategie für Deutschland“ (CSS, BMI 2011b) abgelöst. Wie schon im NPSI wurden mit dem „Schutz kritischer Informationsinfrastrukturen“ und der „Stärkung der IT-Sicherheit in der öffentlichen Verwaltung“ KRITIS-Betreiber und staatliche Stellen explizit angesprochen und der Adressatenkreis um kleine und mittlere Unternehmen erweitert. Organisatorisch wurde die Cyber-Sicherheitsarchitektur ergänzt: um das Cyber-Abwehrzentrum, eine Kooperationsplattform der mit Cyber-Sicherheit befassten Bundesbehörden, und um den Nationalen Cyber-Sicherheitsrat, dem sieben Ressorts und das Bundeskanzleramt angehören. Erstmals wurde auch die Prüfung regulativer Instrumente in Erwägung gezogen, die 2015 im *IT-Sicherheitsgesetz* mündete (→ Kapitel 2.2.1 und Infobox 16).

Die CSS wurde 2016 vor dem Hintergrund der qualitativen und quantitativen Entwicklung der Digitalisierung fortgeschrieben (BMI 2016a). Sie verfolgt das Ziel, die Handlungsfähigkeit und die Souveränität Deutschlands im Zeitalter der Digitalisierung zu gewährleisten, Chancen und Potenziale der Digitalisierung zu nutzen und die damit verbundenen Risiken zu beherrschen. Dazu werden vier Handlungsfelder definiert und mit strategischen Zielen und Maßnahmen hinterlegt:

1. Sicheres und selbstbewusstes Handeln in einer digitalisierten Umgebung

2. Gemeinsamer Auftrag von Staat und Wirtschaft

3. Leistungsfähige und nachhaltige gesamtstaatliche Cyber-Sicherheitsarchitektur

4. Aktive Positionierung Deutschlands in der europäischen und internationalen Cyber-Sicherheitspolitik

Der Schutz Kritischer Infrastrukturen wird in der CSS als „gemeinsamer Auftrag von Staat und Wirtschaft“ im gleichlautenden Handlungsfeld adressiert. Dem Ausbau der engen und vertrauensvollen Zusammenarbeit auf allen Ebenen, wie sie bereits der NPSI vorgezeichnet hatte, werden Präventionsmaßnahmen, u. a. die Erarbeitung und Umsetzung von Mindeststandards, sowie Reaktionspflichten wie die Festlegung von Meldewegen zur Seite gestellt.

Infobox 8: Die „Deutsche Anpassungsstrategie an den Klimawandel“

Es zeichnet sich bereits deutlich ab, dass der Klimawandel Auswirkungen auf das Leben in Deutschland hat und auch weiterhin haben wird. Um sich darauf einzustellen, Verwundbarkeiten zu reduzieren und Anpassungsmöglichkeiten zu nutzen, hat die Bundesregierung im Jahr 2008 die „Deutsche Anpassungsstrategie an den Klimawandel“ (DAS) beschlossen (BReg 2008). Aufgrund der zentralen Bedeutung, die Infrastrukturen und die mit ihrer Hilfe bereitgestellten Dienstleistungen für die Gesellschaft haben, verwundert es nicht, dass viele Handlungsfelder der DAS mit Sektoren Kritischer Infrastrukturen korrespondieren, z.B. die Wasserwirtschaft, die Energiewirtschaft oder die Finanzwirtschaft. Der Bevölkerungsschutz wird – ebenso wie die Raum-, Regional- und Bauleitplanung – seiner vielfältigen Bezüge zu den unterschiedlichen Handlungsfeldern wegen in der DAS als Querschnittsthema betrachtet.

Im Zuge des Klimawandels zeichnen sich Veränderungen in einem breiten Spektrum unterschiedlicher Naturgefahren – von Hitzewellen bis Starkniederschlägen – ab. Maßnahmen zur Steigerung der Widerstandsfähigkeit Kritischer Infrastrukturen gegenüber diesen Gefahren tragen also gleichermaßen zur Anpassung an den Klimawandel *und* zum Schutz Kritischer Infrastrukturen bei. Diese Synergien zu erkennen und zu nutzen, bringt beide Prozesse voran – zu diesem Ergebnis kommt auch der Fortschrittsbericht zur DAS (BReg 2015). Aus diesem Grund lohnt sich auch für alle, die sich mit dem Schutz Kritischer Infrastrukturen befassen, ein Blick in das „Deutsche Klimavorsorgeportal“ (www.klivoportal.de), das Angebote von Bund und Ländern zur zielgerichteten Anpassung an die Folgen des Klimawandels bündelt. Viele der hierin zu findenden Angebote können wichtige Beiträge zum Risikomanagement von Kritischen Infrastrukturen liefern. Weitere Informationen zur Umsetzung der DAS stellt das Bundesministerium für Umwelt, Naturschutz und nukleare Sicherheit (BMU) sowie das Kompetenzzentrum Klimafolgen und Anpassung (KomPass) des Umweltbundesamtes (UBA) zur Verfügung.

Infobox 9: Die „Sicherheitsstrategie für die Güterverkehrs- und Logistikwirtschaft“

Die KRITIS-Strategie fasst die Ziele und den politisch-strategischen Ansatz des Bundes zum Schutz Kritischer Infrastrukturen insgesamt zusammen. Mit der „Sicherheitsstrategie für die Güterverkehrs- und Logistikwirtschaft“ (BMVI 2014) hat das Bundesministerium für Verkehr und digitale Infrastruktur (BMVI) den Grundstein zu deren Umsetzung im Sektor *Transport und Verkehr* gelegt (→ Infobox 2). Die Sicherheitsstrategie verfolgt das Ziel, längerfristige infrastrukturseitige Störungen und Ausfälle durch externe Einwirkungen, die mit schwerwiegenden Unterbrechungen der Güterversorgung für die Bevölkerung und die Wirtschaft einhergehen, möglichst zu verhindern bzw. im Ereignisfall durch ein effektives Krisenmanagement schnell und angemessen zu bewältigen.

Die Sicherheitsstrategie greift viele in der KRITIS-Strategie für den Schutz Kritischer Infrastrukturen als Ganzes aufgeführte Ansätze und Umsetzungsbausteine in branchenspezifischer Perspektive auf. Beispielsweise gehören die Fortsetzung und der Ausbau der Zusammenarbeit zwischen staatlichen und privatwirtschaftlichen Akteuren zu den maßgeblichen Zielsetzungen der Sicherheitsstrategie. Der schon im Vorfeld zur Strategieentwicklung ins Leben gerufene Arbeitskreis „Sicherheit in der Logistik“ bringt diese Akteursgruppen zusammen, begleitet die Umsetzung der Strategie und entwickelt sie fortlaufend weiter. Er ist eng mit dem Branchenarbeitskreis *Transport und Verkehr* des UP KRITIS verbunden (→ Kapitel 2.4.2). Darüber hinaus wird z. B. die Bedeutung von Übungen unter Beteiligung von staatlichen Stellen und Betreibern hervorgehoben und auch ein Engagement von Akteuren aus dem Sektor *Transport und Verkehr* im Rahmen der Übungsreihe LÜKEX angestrebt (→ Kapitel 2.4.4).

Infobox 10: Das „Sendai Rahmenwerk für Katastrophenvorsorge“

Nationale Kontaktstelle für das Sendai Rahmenwerk Deutschland

Auf der dritten Weltkonferenz zur Reduzierung von Katastrophenrisiken der Vereinten Nationen im März 2015 in Sendai (Japan) haben 187 Staaten das „Sendai Rahmenwerk für Katastrophenvorsorge 2015-2030“ angenommen (vgl. NKS 2019). Durch dessen Umsetzung wollen Staaten die Auswirkungen von Katastrophen weltweit bis zum Jahr 2030 substanziell verringern. Ziel ist es, bestehende Risiken und Vulnerabilitäten zu reduzieren, neue Katastrophenrisiken zu verhindern und die Resilienz der Bevölkerung gegenüber natürlichen oder vom Menschen verursachten Gefahren zu stärken.

Dazu werden im Sendai Rahmenwerk sieben globale Zielsetzungen vorgegeben. Die Auswirkungen von Katastrophen sollen reduziert werden, indem die (a) Zahl der Todesopfer und (b) der betroffenen Menschen, (c) die wirtschaftlichen Verluste und (d) die „Schäden an kritischen Infrastrukturen und Unterbrechungen der Grundversorgung“ (NKS 2019, S. 13) erheblich gesenkt werden. Zum anderen sollen (e) mehr Staaten über Strategien zur Katastrophenvorsorge verfügen, (f) die internationale Zusammenarbeit gestärkt und (g) die Verfügbarkeit von gefahrenübergreifenden Frühwarnsystemen und von Informationen über Katastrophenrisiken erhöht werden.

Um diese Ziele zu erreichen, setzt das Sendai Rahmenwerk vier Handlungsprioritäten (NKS 2019, S. 15):

1. Das Katastrophenrisiko verstehen

2. Die Institutionen der Katastrophenvorsorge stärken, um das Katastrophenrisiko zu steuern

3. In die Katastrophenvorsorge investieren, um die Resilienz zu stärken.

4. Die Vorbereitungen auf den Katastrophenfall verbessern, um wirksamer reagieren zu können; bei Wiederherstellung, Rehabilitation und Wiederaufbau nach dem Prinzip „besser wiederaufbauen“ vorgehen.

Auch die Bundesrepublik Deutschland hat sich verpflichtet, an der Umsetzung des Sendai Rahmenwerks mitzuwirken. Das bedeutet, nicht nur in der internationalen Zusammenarbeit, sondern auch auf nationaler Ebene zur Erreichung der Ziele beizutragen. Die Steuerung des Umsetzungsprozesses erfolgt im Rahmen einer interministeriellen Arbeitsgruppe. Für die Koordinierung und fachliche Unterstützung in der Umsetzung wurde 2017 die Nationale Kontaktstelle für das Sendai Rahmenwerk (NKS) beim BBK eingerichtet.

Besonders augenfällig sind die Anknüpfungspunkte zwischen den Zielen der KRITIS-Strategie (BMI 2009) und der im Sendai Rahmenwerk festgeschriebenen Zielsetzung einer substanziellen Verringerung katastrophenbedingter „Schäden an kritischen Infrastrukturen und Unterbrechungen der Grundversorgung, einschließlich Gesundheits- und Bildungseinrichtungen“ sowie die „Erhöhung ihrer Resilienz“ (NKS 2019, S 13). Aber auch die Reduzierung der Anzahl von Opfern und Betroffenen von Katastrophen und die Höhe der von ihnen verursachten wirtschaftlichen Schäden hängen vielfach davon ab, wie gut die Versorgung mit Infrastrukturleistungen auch in Katastrophenfällen gewährleistet bleibt bzw. wie schnell sie wieder zur Verfügung steht. Insofern ist der Schutz Kritischer Infrastrukturen ein bedeutender Teilaspekt zur Verminderung von Katastrophenrisiken insgesamt und die KRITIS-Strategie ein wichtiger Baustein der Umsetzung des Sendai Rahmenwerks in Deutschland.

2.3.2 Die Rolle des Schutzes Kritischer Infrastrukturen in der „Konzeption Zivile Verteidigung“

Nach dem in der KRITIS-Strategie (BMI 2009) vertretenen All-Gefahren-Ansatz ist beim Schutz Kritischer Infrastrukturen ein ganzes Spektrum unterschiedlicher Gefahren zu berücksichtigen. Darunter fallen auch solche, die im Zusammenhang mit bewaffneten Konflikten auftreten können. Aus diesem Grund spielt der Schutz Kritischer Infrastrukturen auch eine Rolle in der im August 2016 vom Bundeskabinett beschlosse-

nen „Konzeption Zivile Verteidigung“ (KZV, BMI 2016b). Die KZV enthält Vorgaben zu den in Abbildung 11 dargestellten Bereichen der zivilen Verteidigung: der „Aufrechterhaltung von Staats- und Regierungsfunktionen“, dem „Zivilschutz“, der „Versorgung“ und der „Unterstützung der Streitkräfte“. Zudem werden darin die von der North Atlantic Treaty Organization (NATO) formulierten „sieben Grundanforderungen“ an den Zivilschutz, die sogenannten „Baseline Requirements“ (→ Kapitel 2.6.3), für Deutschland konkretisiert. Die KZV bildet damit das zivile Gegenstück zur „Konzeption der Bundeswehr“ (BMVg 2018) und fußt wie diese auf den Annahmen des „Weißbuchs der Bundeswehr“ (BMVg 2016).

Zivile Verteidigung und militärische Verteidigung stehen als Gesamtverteidigung in einem unauflösbaren Zusammenhang (vgl. Abbildung 11). In diesem Rahmen werden Vorbereitungen zum Schutz der Bevölkerung und zur Verteidigung Deutschlands insbesondere im Spannungs- und Verteidigungsfall (Art. 80a Abs. 1 GG, Art. 115a GG) getroffen sowie die Verpflichtungen Deutschlands im Bündnis- (Art. 5 NATO-Vertrag) und Beistandsfall (Art. 42 Abs. 7 EU-Vertag) berücksichtigt.

Die Verfügbarkeit Kritischer Infrastrukturen spielt letztlich in allen von der KZV adressierten Bereichen der zivilen Verteidigung eine wichtige Rolle. So können die Vorgaben zur Aufrechterhaltung von Staats- und Regierungsfunktionen als gefahrenspezifische Maßnahmen für den Schutz Kritischer Infrastrukturen im KRITIS-Sektor Staat und Verwaltung aufgefasst werden (→ Infobox 11). Im Bereich „Zivilschutz“ geht es maßgeblich um Fähigkeiten des *Notfall- und Rettungswesens* sowie des Sektors *Gesundheit* (z. B. die Krankenhausalarm- und -einsatzplanung; → Kapitel 2.5.4). Der Bereich „Unterstützung der Streitkräfte“ umfasst u. a. die Bereitstellung von Energie, Nahrungsmitteln und Transportdienstleistungen. Im Bereich „Versorgung“ geht es um „die Abwehr und Bewältigung von Ausfällen und Störungen von Versorgungsleistungen“, wobei auf den „vorhandenen friedensmäßigen Strukturen und Krisenvorsorgemaßnahmen“ (BMI 2016b, S. 42) als Basis aller in der KZV beschriebenen Vorsorgeplanungen aufgebaut werden soll. Viele der im Bereich „Versorgung“ adressierten Dienstleistungen weisen deutliche Parallelen zu den KRITIS-Sektoren auf, etwa die medizinische Versorgung, die Energieversorgung oder die (Not-)Versorgung mit Wasser und Lebensmitteln (→ Infobox 6).

Abbildung 11: Bereiche der Gesamtverteidigung und Themenfelder der Konzeption Zivile Verteidigung (Quelle: BBK).

Im Rahmen der KZV werden spezielle Herausforderungen an die Krisenvorsorge betrachtet. Das betrifft etwa den Planungshorizont: Während bei einer kurzfristigen Krise nicht unmittelbar zeitkritische Aufgaben bis zur Abarbeitung der Krise ruhen können, stellt sich im Spannungs- oder Verteidigungsfall möglicherweise ein langfristig veränderter „Normalzustand“ ein. Zudem ist mit außergewöhnlichen Bedrohungen zu rechnen, etwa dem Einsatz von Kriegswaffen und den damit verbundenen Schadensbildern, sowie mit dem gezielten Einsatz von Mitteln der hybriden

Infobox 11: Aufrechterhaltung der Staats- und Regierungsfunktionen

Der Staat muss auch in einer Krisensituation handlungsfähig sein. Dies gilt nicht nur für rein friedenszeitliche Szenarien, sondern auch im Spannungs-, Verteidigungs-, Zustimmungs- oder Bündnisfall. Auch dann müssen Parlamente Gesetze erlassen, Gerichte Recht sprechen und Regierung und Verwaltung ihre Aufgaben erfüllen können. Das ist eine legitime Erwartung an den Staat und so sieht es auch die verfassungsmäßige Ordnung vor. Mit dem Aufgabenbereich „Aufrechterhaltung der Staats- und Regierungsfunktionen“ ist deshalb der KRITIS-Sektor *Staat und Verwaltung* (→ Infobox 2) explizit in der Zivilen Verteidigung verankert. Ziel der Regelungen ist es, auch in besonderen Krisenlagen wie dem Spannungs- oder Verteidigungsfall sicherzustellen, dass die staatlichen Organe ihre Aufgaben und Funktionen weiterhin wahrnehmen können. Die Behörden und Einrichtungen können dabei auf ihre Vorbereitungen für einen zivilen Krisenfall (Notfall-/Krisenmanagement) zurückgreifen, müssen aber die Besonderheiten der Situation berücksichtigen (z. B. die gegenüber friedenszeitlichen Krisen wesentlich längere Dauer der Lage). Daher stellen sich im Kontext der Aufrechterhaltung der Staats- und Regierungsfunktionen u. a. in folgenden Bereichen spezifische Fragen:

1. **Veränderung der Aufgaben**
   Muss die Aufgabenwahrnehmung in qualitativer und/oder quantitativer Hinsicht angepasst werden? Welche Aufgaben kommen ggf. hinzu, die in Friedenszeiten nicht wahrgenommen werden? Welche Aufgaben können ggf. entfallen?

2. **Organisatorische Maßnahmen**
   Müssen Organisations-/Geschäftsverteilungspläne an die veränderte Aufgabenwahrnehmung angepasst werden? Sind die erforderlichen Schnittstellen zu anderen Behörden und die Meldewege definiert? Besteht besonderer Schutzbedarf für kritische Bereiche?

3. **Baulich-technische Maßnahmen**
   Sind besondere Härtungsmaßnahmen der Gebäude erforderlich (z. B. mit Blick auf mögliche Waffenwirkungen)? Müssen besondere Zugangssicherungen eingerichtet werden?

4. **Behördenselbstschutz**
   Sind für verteidigungsfallbezogene Szenarien besondere Schutzmaßnahmen für die Beschäftigten zu ergreifen (u. a. Arbeitsschutz, Brandschutz, Gesundheitsschutz)?

5. **Personelle Maßnahmen**
   Welche Beschäftigten sind als Schlüsselpersonal festzulegen? Steht die Personalplanung für verteidigungsrelevante Bereiche? Müssen Freistellungen oder auch Personalanforderungen nach dem Arbeitssicherstellungsgesetz (→ Kapitel 2.2.3) vorbereitet werden?

6. **Ausweichsitzplanung**
   Müssen ggf. Aufgaben an einem geschützten Standort wahrgenommen werden?

Kriegsführung gegen Kritische Infrastrukturen. Auch im Kontext der Zivilen Verteidigung sind die Infrastrukturbetreiber für die Bereitstellung von Versorgungsleistungen und für die Sicherheit ihrer Einrichtungen verantwortlich, allerdings spielt die staatliche Notfallvorsorge im Sinne der Notversorgung eine größere Rolle: Bis bei Eintritt eines größeren Ausfalls die Versorgung wieder auf normalem Weg gewährleistet werden kann, sollen staatliche Notversorgungsmaßnahmen greifen, für die etwa Vorsorge- und Sicherstellungsgesetze die rechtlichen Grundlagen bilden (→ Kapitel 2.2.3). Gleichzeitig können besonders kritische Einrichtungen durch die Polizeien der Länder, bei Bedarf ergänzt durch Kräfte der Bundespolizei sowie unter bestimmten Voraussetzungen auch durch die Bundeswehr im Rahmen des Objektschutzes, besonders geschützt werden.

Vor diesem Hintergrund gilt: „der fortlaufende Schutz Kritischer Infrastrukturen ist elementare Voraussetzung für die Notfallvorsorge im Rahmen der Zivilen Verteidigung“ (BMI 2016b, S. 42). Die KZV hat in den Jahren seit ihrer Verabschiedung viele Akteure dazu bewogen, sich auch mit außergewöhnlichen Szenarien auseinanderzusetzen. Davon wiederum profitiert auch der „friedensmäßige“ Schutz Kritischer Infrastrukturen.

2.3.3 Forschung zum Schutz Kritischer Infrastrukturen

Wissenschaft und Forschung können wesentlich dazu beitragen, Kritische Infrastrukturen widerstandsfähiger gegen Störungen und Angriffe zu machen sowie Ausfälle schneller zu bewältigen. Das Bundesministerium für Bildung und Forschung (BMBF) fördert daher im Rahmen von Forschungsprogrammen systematisch Projekte, in denen Erkenntnisse und ganzheitliche Lösungen aufgezeigt sowie neue technologische Ansätze entwickelt werden. Fragestellungen mit Bezug zum Schutz Kritischer Infrastrukturen spielen in mehreren Förderprogrammen eine Rolle – besonders einschlägig sind das Rahmenprogramm „Forschung für die zivile Sicherheit“ sowie das Forschungsrahmenprogramm zur IT-Sicherheit „Selbstbestimmt und sicher in der digitalen Welt“.

Das Rahmenprogramm „Forschung- für die zivile Sicherheit“

Das erste zivile Sicherheitsforschungsprogramm (SiFo) wurde 2007 von der Bundesregierung beschlossen, um interdisziplinäre Forschungsprojekte zu fördern, die ganzheitliche Lösungen zur Erhöhung der Sicherheit der Bürgerinnen und Bürger erarbeiten. Inzwischen befindet sich das Programm in seiner dritten Phase. Um die Praxistauglichkeit der entwickelten Lösungen sicherzustellen, werden in allen Forschungsprojekten Anwender wie Behörden und Organisationen mit Sicherheitsaufgaben oder Infrastrukturbetreiber eng einbezogen. Zudem werden relevante gesellschaftliche, rechtliche oder ethische Fragen von vornherein berücksichtigt.

Von den fünf der ersten 2007/2008 im Programm veröffentlichten Förderrichtlinien widmeten sich zwei dem Schutz Kritischer Infrastrukturen. Seitdem wurde das Thema immer wieder in neuen Facetten aufgegriffen und bildet auch im aktuellen Rahmenprogramm der Bundesregierung „Forschung für die zivile Sicherheit 2018–2023“ eine der drei zentralen Säulen (vgl. BMBF 2018; Abbildung 12). In der Programmsäule „Schutz Kritischer Infrastrukturen“ werden Projekte gefördert, die an ganzheitlichen Sicherheitslösungen zur Erhöhung des Schutzes und der Widerstandsfähigkeit Kritischer Infrastrukturen forschen. Die Schwerpunkte liegen auf den Sektoren *Energie*, *Gesundheit*, *Wasser*, *Ernährung*, T*ransport und Verkehr* sowie *Medien und Kultur* (→ Infobox 2).

Seit 2007 hat das BMBF in der Programmsäule „Schutz Kritischer Infrastrukturen“ insgesamt 83 Forschungsprojekte mit einem Volumen von rund 180 Millionen Euro gefördert. Im Folgenden kann nur ein Ausschnitt aus der betrachteten Themenvielfalt dargestellt werden. Ein vollständiger Überblick über die im Rahmen des Programms „Forschung für die zivile Sicherheit“ geförderten Vorhaben ist der Internetseite des BMBF (www.sifo.de) zu entnehmen (vollständige Titel der nachfolgend beispielhaft genannten Forschungsprojekte ab S. 106).

Abbildung 12: Programmsäulen und Querschnittsthemen des Rahmenprogramms „Forschung für die zivile Sicherheit 2018–2023“
(Quelle: BMBF 2018, Forschung für die zivile Sicherheit 2018-2023, S. 5).

Infobox 12: Zentrale Lebensadern sichern: Energie und Wasser

Stromausfälle sind in Deutschland zwar eher selten, doch wenn sie auftreten und länger andauern, können sie Wirtschaft und Bevölkerung unvorbereitet treffen und großen Schaden anrichten. In Forschungsprojekten setzen sich Wissenschaftlerinnen und Wissenschaftler sowie Betreiber Kritischer Infrastrukturen gemeinsam mit der Frage auseinander, was im Ernstfall getan werden muss, wenn über einen längeren Zeitraum kein Strom fließt (→ InfoStrom).

Auch dank der Ergebnisse aus solchen vom BMBF geförderten Forschungsprojekten konnten Rettungs- und Einsatzkräfte im Februar 2019 schneller und effizienter auf einen Stromausfall reagieren, durch den im Berliner Stadtteil Köpenick über 30.000 Haushalte für 30 Stunden ohne Strom waren. Die Berliner Feuerwehr war u. a. durch vorher festgelegte Abläufe besser darauf vorbereitet, den notwendigen Informationsbedarf der Bevölkerung zu decken sowie die Evakuierung von beatmungspflichtigen Patienten bei fehlender bzw. ausgefallener Notstromversorgung durchzuführen (→ AlphaKomm; → Kat-Leuchttürme). Die Feuerwehr setzte dabei ein in einem Forschungsprojekt entwickeltes System zur Überwachung der Treibstoffversorgung ihrer Notstromaggregate erfolgreich in der Praxis ein (→ TankNotStrom).

Die Versorgung mit sauberem Trinkwasser ist für uns selbstverständlich. Damit das so bleibt, hat ein Forschungsteam neue kompakte Sensoren entwickelt, die im Trinkwassernetz ein breites Spektrum von gesundheitsgefährdenden Stoffen – biologischer oder chemischer Natur – schnell und zeitnah detektieren können. Zudem wurden zur Erhöhung der Resilienz in Krisensituationen weitreichende Notfallkonzepte erstellt und Handlungsleitfäden für Trinkwasserversorger und Behörden entwickelt, die im Ernstfall dazu beitragen, dass Einsatzkräfte und Behörden Krisensituationen schneller meistern können (→ AquaBioTox; → STATuS; → ResiWater).

Abbildung 13: (Quelle: Thomas Schelagowski / EyeEm / Getty Images)

Infobox 13: Durchgehende Versorgungsketten gewährleisten: Ernährung und Gesundheit

Wie wird die Versorgung mit wichtigen Gütern wie Lebensmitteln und Medikamenten in Krisensituationen sichergestellt? Ziel der Forschung ist es, für das richtige Handeln in Krisenlagen innovative akteursübergreifende Vorsorge- und Kommunikationsstrategien zu entwickeln. Dazu gehört es beispielsweise, gesundheitsgefährdende Lebensmittelverunreinigungen frühzeitig zu entdecken. Ergebnisse aus der zivilen Sicherheitsforschung ermöglichen es Behörden und Versorgungsunternehmen, schnell und systematisch Krankheitserreger aufzuspüren. Somit kann zeitnah zurückverfolgt werden, an welcher Stelle der Lieferkette die Lebensmittel mit einem identifizierten Erreger verunreinigt wurden, um unmittelbar die passenden Gegenmaßnahmen zu ergreifen (→ SiLeBAT; → NeuENV; → RESCUE IT).

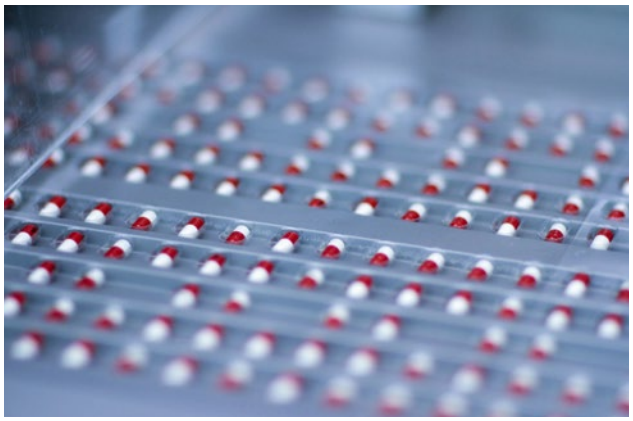


Abbildung 14: (Quelle: Sigrid Gombert / Cultura / Getty Images)

Etwa ein Drittel aller Menschen in Deutschland ist aufgrund chronischer Leiden dauerhaft auf Medikamente angewiesen. Auch in Krisensituationen und Notlagen, wie z. B. bei Pandemien, muss der Bedarf an Medikamenten gedeckt werden. Für solche Fälle haben Wissenschaftler eine Software erstellt, die bereits im Vorfeld mögliche Bedrohungsszenarien für die Medikamentenwarenkette aufdeckt und allen Beteiligten konkrete Präventions- und Schutzlösungen aufzeigt. Da auch die Fälschung von Arzneimitteln eine wachsende Gefahr darstellt, wurde zudem im Rahmen eines Forschungsprojekts ein transportables Gerät entwickelt, mit dem z. B. bei Razzien gefälschte Präparate ohne großen Aufwand erkannt werden können (→ MIME; → SafeMed).

Infobox 14: Grundlagen für sichere Mobilität schaffen: Transport und Verkehr

830.000 Kilometer Straßen, 38.600 km Schienen, 7.300 km Binnenwasserstraßen und 24 Hauptverkehrsflughäfen gewährleisten in Deutschland die Mobilität der Bürgerinnen und Bürger. Zugleich sind sie Voraussetzung für die reibungslose Versorgung von Menschen und Unternehmen mit Lebensmitteln, Gütern und Rohstoffen. Bei Planung und Bau wurde jedoch nicht überall mit der Intensität des heutigen Verkehrsaufkommens gerechnet.

Daher arbeiten Forscherinnen und Forscher an Innovationen, mit denen beispielsweise mithilfe von Drohnen oder hochgenauen Radarmessgeräten der aktuelle Bauwerkszustand von Brücken schnell und umfassend erfasst werden kann (→ AISTEC; → ZEBBRA). Über Computersimulationen können mögliche Alterungsschäden bereits im Entstehen erkannt und deren Verlauf vorhergesagt werden. Neue Technologien sollen auch dabei helfen, die Bausubstanz von Verkehrstunneln echtzeitnah zu überwachen, beispielsweise mithilfe in Betonelementen integrierter Funksensoren. Die gewonnenen Messdaten fließen in Lagebewertungssysteme für Rettungs- und Evakuierungsmaßnahmen ein, sodass im Ernstfall umfassende Informationen zu Schadensausmaß und Bauwerkszustand direkt an die Einsatzkräfte übermittelt werden können (→ AISIS; → AURIS).

Für den Bereich der Fährschifffahrt wurde ein Computerprogramm entwickelt, mit dem für verschiedene Gefahrenszenarien mögliche Sicherheitsschwachstellen auf Fährschiffen oder in Häfen identifiziert und analysiert werden können. Ein aus dem Projekt hervorgegangenes Verfahren zur Risikoanalyse wurde 2014 von allen deutschen Bundesländern mit Hafenanlagen übernommen (→ VESPER; → VESPER^{PLUS}). In einem weiteren Projekt wird simuliert, welche Schadensauswirkungen und Konsequenzen verschiedene Bedrohungsszenarien auf künstliche Wasserstraßen haben. Somit können potenziell kritische Stellen im Wasserstraßennetz sichtbar gemacht und gezielte Schutzmaßnahmen und Krisenpläne entwickelt werden (→ PREVIEW).

Abbildung 15: (Quelle: Abstract Aerial Art / DigitalVision / Getty Images)

Flughäfen sind besonders sensible Knotenpunkte im globalen Reise- und Frachtverkehr und sehr empfindlich gegenüber Störungen. In der zivilen Sicherheitsforschung wurde ein Körperscanner entwickelt, der auf Basis der Millimeterwellen-Technologie potenziell bedrohliche Objekte – egal ob flüssig, metallisch oder nichtmetallisch – detektiert. Das beteiligte Unternehmen brachte den Körperscanner nach Projektabschluss zur Marktreife und erhielt einen Rahmenvertrag über die Ausstattung deutscher Flughäfen mit 300 Körperscannern (→ QPASS).

Moderne Sicherheitslösungen sind auch im Bereich der Luftfracht gefragt. Hierfür wurde ein System entwickelt, mit dem Frachtgüter im gesamten Verlauf der Transportkette berührungslos mithilfe von RFID-Chips überwacht werden können, um z. B. gezielte Manipulationen frühzeitig zu erkennen (→ ESecLog).

Güterverkehrszentren (GVZ) haben als logistische Knotenpunkte eine zentrale Bedeutung für die Warenversorgung in Deutschland. Forscher und Praktiker haben ein Notfallkonzept entwickelt, das im Falle eines Schadenseintritts den Notbetrieb von GVZ ermöglichen soll. Herzstück ist ein digitales Simulationsmodell, über das Schadenslagen und Schadensentwicklungen abgebildet werden können und das den Verantwortlichen eine schnelle automatisierte Entscheidungsunterstützung bietet (→ PREPARED[NET]).

Das Rahmenprogramm „Selbstbestimmt und sicher in der digitalen Welt“

Das Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit (2015 – 2020) bündelt ressortübergreifend die Aktivitäten zur IT-Sicherheitsforschung und fördert die Entwicklung sicherer, innovativer IT-Lösungen für Bürgerinnen und Bürger, Wirtschaft und Staat (BMBF 2015). Das Programm umfasst vier Kernbereiche: Neben der Entwicklung neuer Hightech-Technologien für die IT-Sicherheit stehen sichere und vertrauenswürdige informations- und kommunikationstechnische Systeme, Anwendungsfelder der IT-Sicherheit sowie Privatheit und Schutz von Daten im Fokus. Das Volumen des Rahmenprogramms beläuft sich auf insgesamt 180 Millionen Euro.

Innerhalb des Kernbereichs zu Anwendungsfeldern der IT-Sicherheit wurde der Förderschwerpunkt „IT-Sicherheit für Kritische Infrastrukturen“ angesiedelt, um laufenden Entwicklungen wie der zunehmenden Digitalisierung bzw. rechnergestützten Automation der Prozesse oder dem völlig neuen Grad der Vernetzung der eingesetzten IT-Systeme beim Betrieb Kritischer Infrastrukturen Rechnung zu tragen. Diese Entwicklungen sind wirtschaftlich und technologisch geboten, bergen jedoch durchaus Risiken. Erklärtes Ziel des Förderschwerpunkts ist es daher, zukunftsfähige Sicherheitslösungen für Kritische Infrastrukturen zu entwickeln und dabei auch die Alltagstauglichkeit, Bedienbarkeit und Kosteneffizienz zu adressieren. Die Härtung und Ertüchtigung von Bestandssystemen soll in gleicher Weise gewürdigt werden wie die Anwendbarkeit von Lösungen und Methoden für kleine und mittelgroße Betreiber.

Bis Ende 2018 hat das BMBF insgesamt elf Forschungskonsortien mit dieser Zielsetzung in einem Umfang von 24 Millionen Euro gefördert. Im Rahmen der Förderbekanntmachung „IT-Sicherheit für Kritische Infrastrukturen“ beteiligten

sich 17 Betreiber aus den Sektoren *Gesundheit*, *Energie*, *Transport und Verkehr*, *Wasser*, *Finanz- und Versicherungswesen* sowie *Staat und Verwaltung* (→ Infobox 2). Inhaltliche Schwerpunkte bildeten „Neue Ansätze zur Beurteilung von IT-Sicherheit“ und „Neue Ansätze zur Erhöhung des IT-Sicherheitsniveaus“ von Kritischen Infrastrukturen. Das in den Projekten behandelte Themenspektrum reichte von Werkzeugen für eine schnelle Einschätzung und Verbesserung des vorhandenen Sicherheitsniveaus, insbesondere für kleine und mittlere Betreiber, über die Erforschung neuartiger Anomalieerkennungsverfahren in industriellen Netzen bis hin zur Bewertung der IT-Sicherheit unter Berücksichtigung des Sicherheitsbewusstseins der Nutzer. Eine Gesamtübersicht der Förderprojekte ist der Internetseite des Bereichs „Kommunikation und Sicherheit digitaler Systeme“ des BMBF zu entnehmen.

Infobox 15: Einblicke in den Förderschwerpunkt „IT-Sicherheit Kritischer Infrastrukturen“

Im ersten inhaltlichen Schwerpunkt „Neue Ansätze zur Beurteilung von IT-Sicherheit“ wurden u. a. Sicherheitsschnelltests für kleine Wasserwerke entwickelt (→ AQUA-IT-Lab). Diese Selbsteinschätzungen gestatten eine Analyse des aktuellen Sicherheitsniveaus und setzen diese in Relation zum Branchenstandard und sonstigen regulatorischen Vorgaben. Eine Testumgebung empfindet die IT-Infrastruktur eines typischen Wasserversorgers nach, gestattet Penetrationstests und realitätsnahe Trainingsangebote für das Betreiberpersonal.

Im Rahmen des zweiten inhaltlichen Schwerpunkts „Neue Ansätze zur Erhöhung der IT-Sicherheit“ wurde z. B. eine neuartige Netzwerkkomponente für Großkraftwerke entwickelt (→ INDI). Diese Komponente ist in der Lage, völlig rückwirkungsfrei die Datenkommunikation in sensiblen Bereichen der Prozesstechnik mitzuschneiden und Auffälligkeiten zu analysieren. Das Projekt verband den Einsatz von Systemen zur „Network Intrusion Detection“ (Erkennung von Angriffen) mit maschinellem Lernen und Verfahren zur automatisierten Analyse von industriellen Kommunikationsprotokollen in einem hochkritischen Umfeld.

Querschnittsaspekte des gesamten Förderschwerpunkts, wie etwa Fragen aus den Bereichen Recht, Normung, Aus- und Fortbildung und Innovationprozesse, wurden in einem Begleitforschungsprojekt betrachtet (→ VeSiKi). So wurde z. B. im „IT-Security NAVIGATOR“ eine bis dato einzigartige Zusammenstellung aller relevanten Normen und Gesetze für Anwender aus allen KRITIS-Sektoren veröffentlicht (www.security-standards.de; → Kapitel 2.2.2). Aufgabe des Metaprojekts war es darüber hinaus, die Projektbeteiligten mit dem UP KRITIS zu vernetzen (→ Kapitel 2.4.2), eine übergeordnete Perspektive gegenüber Fragestellungen zur „IT-Sicherheit für Kritische Infrastrukturen“ einzunehmen und den aktiven Ergebnistransfer zu den Betreibern zu unterstützen. Die Ergebnisse des Projekts wurden als Bericht zum „State of the Art“ der IT-Sicherheit Kritischer Infrastrukturen (vgl. Rudel /Lechner 2018) zusammengefasst und im Rahmen der IT-Sicherheitsmesse „it-sa“ symbolisch dem BSI überreicht. Der Bericht zum ist ebenso wie eine praxisorientierte Zusammenstellung von Fallstudien frei zugänglich publiziert (vgl. Lechner et al. 2018). Ein Überblick über die Verbundprojekte im Förderschwerpunkt IT-Sicherheit Kritischer Infrastrukturen sowie weitere Informationen sind der Internetseite der Begleitforschung zu entnehmen (www.itskritis.de;. vollständige Titel der genannten Forschungsprojekte ab S. 106).

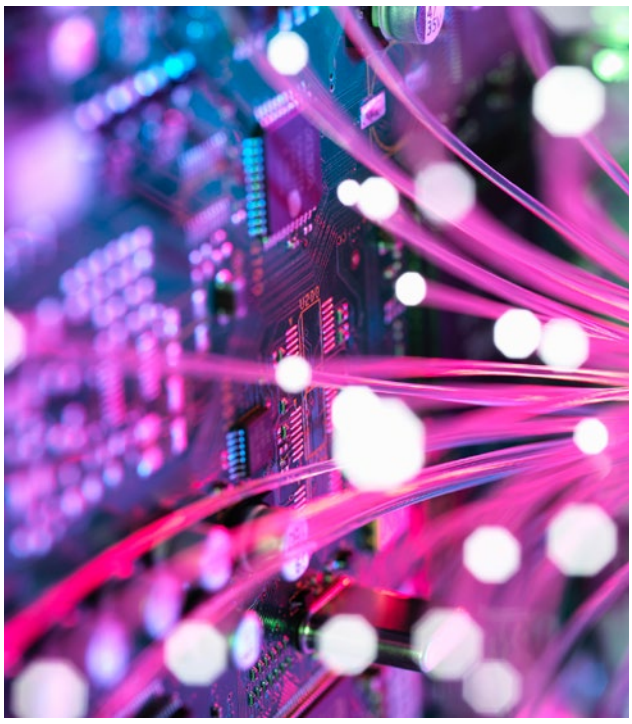


Abbildung 16: (Quelle: Andrew Brookes / Cultura / Getty Images)

2.4

Kapitel

Quelle: Mihajlo Maricic / EyeEm / Getty Images

Schutz Kritischer Infrastrukturen als akteursübergreifende Aufgabe

„Zur Stärkung des Schutzes Kritischer Infrastrukturen bedarf es", so heißt es in der KRITIS-Strategie (BMI 2009, S. 12), „einer intensiven Zusammenarbeit, Abstimmung und Information zwischen und unter den Partnern und Akteuren". Grund dafür ist die ausgesprochen vielfältige Akteurslandschaft, die den Schutz Kritischer Infrastrukturen ausmacht: Verantwortlichkeiten sind zwischen Betreibern und staatlichen Stellen aufgeteilt, fachliche Zuständigkeiten liegen bei mehreren Ressorts, Aufsichtsfunktionen werden von Behörden auf unterschiedlichen administrativen Ebenen wahrgenommen, die Betreiber Kritischer Infrastrukturen sind in diversen Verbänden organisiert, zahlreiche Forschungseinrichtungen widmen sich unterschiedlichen Teilfragen des Schutzes Kritischer Infrastrukturen – und damit sind immer noch nicht alle in der KRITIS-Strategie unter der Überschrift „kooperativer Ansatz" aufgeführten Akteursgruppen genannt (→ Kapitel 1.2). Dem Auftrag zur Zusammenarbeit sind die Beteiligten im Laufe der Zeit in vielfältiger Weise nachgekommen.

Der Schutz Kritischer Infrastrukturen wird als gesamtstaatliche Aufgabe wahrgenommen. Die Zusammenarbeit zwischen Behörden von Bund und Ländern nimmt dabei eine zentrale Stellung ein und die Schaffung entsprechender Strukturen ist ein wichtiger Schritt zur Umsetzung der KRITIS-Strategie (→ Kapitel 2.4.1). Zeitgleich zur Verabschiedung der KRITIS-Strategie wurde der Schutz Kritischer Infrastrukturen in der Fortschreibung (2008/2009) des „Programms Innere Sicherheit" der Innenministerkonferenz verankert (IMK 2009). Auch das Programm bewertet die Intensivierung der Zusammenarbeit aller staatlichen Ebenen als erforderlich. Bereits seit 2012 finden regelmäßig informelle Arbeitstreffen unter Beteiligung der Innenressorts von Bund und Ländern statt. Diese haben sich als Plattform des Austauschs zu ebenenübergreifenden Fragen des Schutzes Kritischer Infrastrukturen bewährt und werden nun stärker an die formale Gremienstruktur der Innenressorts angebunden.

Die partnerschaftliche Zusammenarbeit von staatlichen Stellen und vorwiegend privatwirtschaftlichen Betreibern genießt beim Schutz Kritischer Infrastrukturen einen hohen Stellenwert. Institutioneller Ausdruck dessen ist insbesondere der UP KRITIS (→ Kapitel 2.4.2). Die Zusammenarbeit zwischen Betreibern Kritischer Infrastrukturen, deren Verbänden und den zuständigen staatlichen Stellen im UP KRITIS hat zum einen die Form eines strukturierten Informationsaustauschs über Cyber-Sicherheitsvorfälle, Auffälligkeiten und die aktuelle IT-Bedrohungslage (operativ-taktische Zusammenarbeit). Zum anderen werden branchenspezifische und branchenübergreifende Fragestellungen in Branchen- und Themenarbeitskreisen bearbeitet (strategisch-konzeptionelle Zusammenarbeit).

Bei der Implementierung des *IT-Sicherheitsgesetzes* fungiert der UP KRITIS als Schnittstelle zwischen staatlichen Stellen und den Betreibern Kritischer Infrastrukturen (→ Infobox 16). Diese Funktion erfüllte er u.a. bei der Erarbeitung der Rechtsverordnung zur Identifizierung von Kritischen Infrastrukturen im Sinne des Gesetzes. Die Branchenarbeitskreise des UP KRITIS waren die erste Anlaufstelle, als die Fachexpertise von Behörden- und Betreiberseite in sogenannten „Kernteams" gebündelt werden musste, um die Parameter der Verordnung branchenspezifisch anwendbar zuzuschneiden. Darüber hinaus haben sich die Branchenarbeitskreise des UP KRITIS als ideales Umfeld für die Erarbeitung „branchenspezifischer Sicherheitsstandards" erwiesen. Mit deren Hilfe werden die Vorgaben des IT-Sicherheitsgesetzes zu Sicherheitsvorkehrungen nach dem „Stand der Technik" anwenderspezifisch konkretisiert (→ Kapitel 2.2.2).

Die Zusammenarbeit zwischen Akteuren des Bevölkerungsschutzes und den Betreibern Kritischer Infrastrukturen ist für die Risikominderung bzw. Krisenbewältigung entscheidend. Deshalb ergänzt das Verfahren des sogenannten „Integrierten Risikomanagements" die jeweilige Einzelperspektive der Akteure um eine Gesamtbetrachtung und legt den Schwerpunkt auf die Schnittstellen und den gegenseitigen Austausch von Informationen, Erkenntnissen und Ergebnissen (→ Kapitel 2.4.3). Das inzwischen mehrfach auf seine Praxistauglichkeit getestete Verfahren ist jüngst in Form einer DIN-Spezifikation formalisiert worden. Ein Beitrag zur Entwicklung des Integrierten Risikomanagements wurde im Forschungsprojekt „KIRMin" geleistet (→ Infobox 17).

Das Zusammenspiel von betreiberseitigem und behördlichem Krisenmanagement einzuüben, ist Gegenstand der Länder- und Ressortübergreifenden Krisenmanagementübung (Exercise) „LÜKEX“ (→ Kapitel 2.4.4). Unter der Annahme außergewöhnlicher Krisenszenarien werden Beteiligte aus Behörden und von Betreibern Kritischer Infrastrukturen in ganz besonders fordernde Interaktionssituationen gebracht. Es geht darum, die Fähigkeiten von Mitarbeiterinnen und Mitarbeitern weiterzuentwickeln, Kommunikationswege mit anderen Übungsbeteiligten „einzuschleifen“ und ganz allgemein die Umsetzung von Verfahren des Krisenmanagements gemeinsam zu erproben und zu verbessern.

Ein Szenario, dem in den letzten Jahren besonders viel Aufmerksamkeit von besonders vielen Akteuren entgegengebracht wurde, ist der „großflächige, langanhaltende Stromausfall“ (→ Kapitel 2.4.5). In Deutschland ist nicht nur eine Stelle für die Notfallplanung für Stromausfallszenarien zuständig. Vielmehr setzen eine Vielzahl staatlicher Akteure in Bund, Ländern und Kommunen sowie Betreiber Kritischer Infrastrukturen jeweils in eigener Zuständigkeit Maßnahmen um. Dieses Maßnahmengefüge aus der Vogelperspektive zu betrachten, Wissensstände laufend zu erfassen, Empfehlungen zu erarbeiten und ggf. auch Planungs- und Informationslücken in der Notfallplanung für Stromausfall zu erkennen, ist Sinn und Zweck des „Rahmenkonzepts Notstrom“ mit seinen unterschiedlichen Bausteinen (→ Infoboxen 18, 19, 20 und 21).

2.4.1 Eine gesamtstaatliche Aufgabe: Zusammenarbeit zwischen Bund und Ländern

Die KRITIS-Strategie (BMI 2009) wurde vom Bundeskabinett verabschiedet. Sie richtet sich zunächst an Akteure auf Bundesebene und umreißt die strategische Ausrichtung des Bundes. Zu dieser Ausrichtung gehört allerdings auch, den Schutz Kritischer Infrastrukturen als eine gesamtstaatliche Aufgabe zu betrachten, die eine enge Zusammenarbeit über die administrativen Ebenen hinweg erfordert: Infrastrukturbetreiber sind Adressaten von sowohl von bundes- als auch von landesrechtlichen Regelungen, Aufsichtspflichten liegen auf unterschiedlichen Ebenen, großflächige Ausfälle verlangen nach einem ebenenübergreifenden Krisenmanagement und nicht zuletzt sind auch die Zuständigkeiten im Bevölkerungsschutz auf Bund und Länder verteilt. Aus diesem Grund beschreibt die KRITIS-Strategie die Kooperation von Behörden auf unterschiedlichen Ebenen als grundlegende Voraussetzung zur Umsetzung ihrer Ziele. Im Zusammenhang mit dem kooperativen Ansatz (→ Kapitel 1.2) der Strategie wird die Bedeutung einer intensiven Zusammenarbeit, Abstimmung und Information zwischen und unter allen beteiligten Akteuren betont. Die Behörden von Bund und Ländern nehmen hierbei eine zentrale Stellung ein und die Schaffung entsprechender Strukturen wird als konkreter Schritt im Umsetzungsverfahren benannt.

Zeitgleich zur Verabschiedung der KRITIS-Strategie wurde der Schutz Kritischer Infrastrukturen in der Fortschreibung (2008/2009) des „Programms Innere Sicherheit“ der Innenministerkonferenz (IMK) verankert (vgl. IMK 2009). Der Schutz Kritischer Infrastrukturen wird darin als Handlungsfeld etabliert und die Intensivierung der Zusammenarbeit aller staatlichen Ebenen als erforderlich bewertet. Im Programm wird festgehalten, dass Bund und Länder unter Beibehaltung ihrer Zuständigkeiten die Schaffung ressortübergreifender Strukturen anstreben und dazu koordinierende Stellen einrichten. Schon vorab war durch den für Feuerwehrangelegenheiten, Rettungswesen, Katastrophenschutz und zivile Verteidigung zuständigen Arbeitskreis V der IMK eine länderoffene Arbeitsgruppe damit beauftragt worden, Empfehlungen zur Kooperation von Bund und Ländern beim Schutz Kritischer Infrastrukturen zu erarbeiten.

Zu den vorgelegten Empfehlungen gehörte u. a., den weiteren Austausch in Form regelmäßiger Arbeitstreffen zu strukturieren. Diese Treffen finden seit 2012 unter Beteiligung der Innenressorts von Bund und Ländern statt und haben sich als Plattform für einen vertrauensvollen Austausch zwischen allen Beteiligten und intensive Diskussionen zu ebenenübergreifenden Fragestellungen beim Schutz Kritischer Infrastrukturen etabliert. Ab 2020 wird die bislang informelle Arbeitsgruppe der Koordinierungsstellen für den Schutz Kritischer Infrastrukturen in Bund und Ländern

(AG KOST KRITIS) näher an die Gremienstruktur der Innenressorts heranrücken. Auch hinsichtlich der strategischen Grundlagen zeichnen sich aktuell Entwicklungen ab: Auf Initiative der AG KOST KRITIS haben die Arbeiten an einer gemeinsamen Bund-Länder-Strategie zum Schutz Kritischer Infrastrukturen begonnen. Insbesondere die Einbindung der anderen Fachressorts in die Querschnittsaufgabe Schutz Kritischer Infrastrukturen prägt die laufende Diskussion. Die ressortübergreifende Ausrichtung soll sich auch in der formalen Verabschiedung der Strategie durch die Fachministerkonferenzen bzw. die Ministerpräsidentenkonferenz widerspiegeln.

2.4.2 Der UP KRITIS - Plattform der Zusammenarbeit von Bund und Betreibern

Betreiber Kritischer Infrastrukturen können sowohl öffentliche als auch private Akteure sein. Die weit überwiegende Zahl Kritischer Infrastrukturen wird allerdings von privatwirtschaftlich geführten Unternehmen betrieben. Aus diesem Grund zählt die KRITIS-Strategie „eine vertrauensvolle Kooperation zwischen Staat und Wirtschaft“ (BMI 2009, S. 10) zu ihren Leitprinzipien. Institutioneller Ausdruck dessen ist insbesondere der UP KRITIS, eine öffentlich-private Kooperation zwischen Betreibern Kritischer Infrastrukturen, deren Verbänden und den zuständigen staatlichen Stellen.

Die Anfänge des UP KRITIS liegen im Jahr 2007, als der „Umsetzungsplan KRITIS“ (BMI 2007a) zum zwei Jahre zuvor verabschiedeten „Nationale Plan zum Schutz der Informationsinfrastrukturen“ (BMI 2005b) vorgelegt wurde. Damit reagierte die Bundesregierung darauf, dass informationstechnischen Systemen eine immer größere wirtschaftliche und gesellschaftliche Bedeutung zukam, sich aber gleichzeitig auch die Bedrohungen für diese Systeme immer deutlicher abzeichneten. Der Umsetzungsplan KRITIS wurde von der Bundesregierung in Zusammenarbeit mit Betreibern Kritischer Infrastrukturen erstellt und im Zuge seiner Implementierung auch die Kooperation dieser Akteure beim Schutz Kritischer Infrastrukturen zunächst in Bezug auf IT-Sicherheitsfragen als „UP KRITIS“ institutionalisiert.

Bis 2013 kooperierten im UP KRITIS Betreiber Kritischer Infrastrukturen und die mit dem Schutz Kritischer Infrastrukturen befassten Bundesbehörden in vier Arbeitsgruppen. Hierbei wurde insbesondere zu den in der Roadmap des Umsetzungsplans KRITIS vorgesehenen Themenbereichen Notfall- und Krisenübungen sowie Krisenreaktion und -bewältigung zusammengearbeitet. Um den Austausch zu übergreifenden Themen zu intensivieren, kamen die Arbeitsgruppen regelmäßig zu Plenartreffen zusammen. Als Ergebnis der Zusammenarbeit wurden neben zwei veröffentlichten Empfehlungen (UP KRITIS 2008a; UP KRITIS 2008b; aktuelle Fassungen: UP KRITIS 2014b; UP KRITIS 2014c) auch interne Studien, z. B. zu IT-Abhängigkeiten, erstellt.

Um den Herausforderungen der Digitalisierung und der Zunahme und Professionalisierung von Cyber-Bedrohungen besser begegnen zu können sowie der steigenden Zahl von Teilnehmern gerecht zu werden, wurde 2011 eine Neuaufstellung der Kooperation beschlossen. Es sollten nicht nur Impulse aus der KRITIS-Strategie und der Cyber-Sicherheitsstrategie (BMI 2011b; → Infobox 7) berücksichtigt werden, sondern durch die strategische Neuausrichtung auch möglichst viele Organisationen aus dem Bereich des Schutzes Kritischer Infrastrukturen erreicht werden. Da sich zudem eine getrennte Betrachtung von „physischem Schutz“ und IT-Sicherheitsaspekten als nicht ausreichend gezeigt hatte, wurde ein ganzheitlicher Ansatz mit Schwerpunktsetzung im Bereich der IT in kritischen Prozessen gewählt. Im Februar 2014 verabschiedete das Plenum des UP KRITIS seine neuen Grundlagen und Ziele (UP KRITIS 2014a) und beschloss damit sowohl eine neue strukturelle Aufstellung als auch eine neue inhaltliche Ausrichtung. „UP KRITIS“ ist seitdem ein Eigenname und nicht mehr die Kurzbezeichnung für den o. g. „Umsetzungsplan KRITIS“.

Die Zusammenarbeit im UP KRITIS hat eine operativ-taktische Komponente, die ein schon in der frühen Phase des UP KRITIS bewährtes Modell aufgreift. Dabei geht es darum, einen ständigen Informationsaustausch über Cyber-Sicherheitsvorfälle, Auffälligkeiten und die aktuelle IT-Bedrohungslage zwischen den Teilnehmenden in einer definierten Kommunikationsstruktur zu etablieren. Informationen der Betreiber werden (direkt oder über einen „single point of contact" innerhalb der Branche) zur zentralen Auswertung an das BSI gegeben. Das BSI sammelt, analysiert und bewertet die eingehenden Informationen, ergänzt sie ggf. um Informationen aus anderen Quellen und stellt sie in Form von Lageberichten, Meldungen und (Früh-) Warnungen wieder zur Verfügung. Damit die teilweise hochsensiblen Informationen ausgetauscht werden können, bedarf es neben einer entsprechend abgesicherten technischen Plattform auch klarer Regeln, etwa eines „Traffic Light Protocol" zur Unterscheidung verschiedener Ebenen von Vertraulichkeit (vgl. BSI 2017b).

Die andere Seite ist die strategisch-konzeptionelle Zusammenarbeit in den dafür eingerichteten Gremien, insbesondere in den Branchenarbeitskreisen (BAK) und den Themenarbeitskreisen (TAK). In den BAK arbeiten Betreiber aus einer bestimmten Branche sowie Behörden mit Zuständigkeiten innerhalb dieser Branche zusammen. Beispielsweise spielen die BAK z. B. eine wichtige Rolle bei der Erstellung „branchenspezifischer Sicherheitsstandards" (B3S) zur rechtssicheren Umsetzung von Anforderungen aus dem *IT-Sicherheitsgesetz* (→ Kapitel 2.2.1 und Infobox 16). Die – grundsätzlich zeitlich befristeten – TAK wenden sich Themen zu, die über die Grenzen einzelner Branchen hinaus von Belang sind, z. B. die Sicherheit von industriellen Steuerungssystemen, Anforderungen an Lieferanten und Hersteller, sektorenübergreifende Empfehlungen zur Krisenvorsorge oder die Organisation von Übungen.

An den Plenarsitzungen nehmen die Sprecher der BAK und TAK, der Stab des UP KRITIS, der die Arbeiten zwischen den Plenarsitzungen koordiniert, und die mit Personal des BSI besetzte Geschäftsstelle teil. Beraten wird der UP KRITIS durch einen Rat. Dieser setzt sich aus Vertreterinnen und Vertretern der am UP KRITIS beteiligten Sektoren sowie des BMI, des BSI und des BBK zusammen. Der Rat gibt Impulse für strategische Ziele und Projekte des UP KRITIS. Die Ratsvertreterinnen und -vertreter aus der Wirtschaft bilden den Wirtschaftsbeirat. In den BAK und TAK geht es zwar schwerpunktmäßig, aber nicht mehr ausschließlich, um IT-Sicherheitsfragen: Der sogenannte „physische Schutz" vor weiteren Gefahren aus dem All-Gefahren-Spektrum ist hinzugetreten (→ Kapitel 1.2).

Die Zusammenarbeit im UP KRITIS entwickelte sich zu einem echten Erfolgsmodell. Sie wurde im Lauf der Zeit für immer mehr Teilnehmende interessant. Vor allem seit der Verabschiedung des *IT-Sicherheitsgesetzes* gibt es einen regen Zulauf von Unternehmen aus den KRITIS-Sektoren (→ Infobox 2), wobei nicht alle eine aktive Beteiligung in den Arbeitsgruppen anstreben. Hierbei bewährt sich die neue Struktur mit einer Unterscheidung in „Teilnehmer" und „Mitglieder": Grundsätzlich kann jedes Unternehmen mit Zugehörigkeit zu einem der Sektoren Teilnehmer im UP KRITIS werden. Vertreterinnen und Vertreter eines Unternehmens, die in den Gremien des UP KRITIS aktiv mitwirken, sind Mitglied im UP KRITIS und in den jeweiligen Gremien stimmberechtigt. Neben Betreibern nehmen auch Aufsichtsbehörden wie die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) oder die Bundesnetzagentur (BNetzA) am UP KRITIS teil. Um den Austausch von Bund und Ländern in der Kooperation mit Betreibern zu intensivieren und zu verstetigen, sind seit Ende 2014 auch die Länder in Gremien des UP KRITIS vertreten.

Seit 2017 hat der UP KRITIS über den Wirtschaftsbeirat ein Mandat, d. h. eine „politische Stimme". Er kann seitdem, z. B. im Rahmen von Regulierungsvorhaben zu sektorenübergreifenden Belangen, beteiligt und angehört werden, ohne die nach § 47 der *Gemeinsamen Geschäftsordnung der Bundesministerien* (GGO 2011) vorgesehene, sektorenspezifische Verbändeanhörung vorwegzunehmen. Umgekehrt kann der UP KRITIS nun einfacher die Anliegen der Betreiber gegenüber öffentlichen Stellen vorbringen.

Aktuell (Stand: 12/2019) sind 670 Unternehmen und Behörden als Teilnehmer beim UP KRITIS registriert; derzeit sind 14 BAK und 11 TAK aktiv.

Infobox 16: „Kooperative Rechtssetzung" – Umsetzung des *IT-Sicherheitsgesetzes*

Im Zusammenhang mit dem *IT-Sicherheitsgesetz* wurde der im Schutz Kritischer Infrastrukturen etablierte kooperative Ansatz in ein Rechtssetzungsverfahren übertragen (→ Kapitel 1.2). Die Fachexpertise der Betreiber wurde nicht nur im Rahmen von Anhörungen zum Gesetzesentwurf, sondern auch an weiteren Stellen im Prozess aktiv eingebunden. Dem UP KRITIS als Kooperationsplattform zwischen Behörden und Betreibern kam dabei eine zentrale Rolle zu (→ Kapitel 2.4.2).

Das IT-Sicherheitsgesetz setzt dort an, „wo sich eine moderne Gesellschaft Ausfälle am wenigsten leisten kann: bei den IT-Systemen der Kritischen Infrastrukturen" (BSI 2017a, S. 13). Als Artikelgesetz änderte und ergänzte es eine Reihe bestehender Gesetze, u. a. das *Gesetz über das Bundesamt für Sicherheit in der Informationstechnik* (BSIG). Die Betreiber von Kritischen Infrastrukturen im Sinne von § 2 Abs. 10 BSIG müssen ein Mindestniveau an IT-Sicherheit einhalten und erhebliche IT-Störungen an das BSI melden. Bei der Implementierung des *IT-Sicherheitsgesetzes* fungierte der UP KRITIS an (mindestens) zwei zentralen Stellen als Bindeglied zwischen staatlichen Stellen und Betreibern Kritischer Infrastrukturen.

Das betraf zum einen die Frage, welche konkreten „Einrichtungen, Anlagen oder Teile davon" (§ 2 Abs. 10 BSIG) als Kritische Infrastrukturen im Sinne des BSIG gelten. Dazu sieht das Gesetz das Mittel der Rechtsverordnung vor und macht zu dessen Ausgestaltung in § 10 Abs. 1 BSIG eine Reihe von Vorgaben: Es sind Kritische Infrastrukturen zu identifizieren, die mit einem „als bedeutend anzusehenden Versorgungsgrad" an der Bereitstellung „als kritisch anzusehender Dienstleistungen" innerhalb der vom Gesetz adressierten Sektoren beteiligt sind. Der „als bedeutend anzusehende Versorgungsgrad" ist anhand branchenspezifischer Schwellenwerte zu operationalisieren. Um diese Vorgaben in eine Verordnung zu gießen, die sich innerhalb der adressierten Branchen passgenau umsetzen lässt, wurden sogenannte Kernteams gebildet. In den Kernteams arbeiteten Vertreterinnen und Vertreter des BSI, des BMI, des BBK, der jeweils fachlich zuständigen Bundesressorts sowie von Betreibern Kritischer Infrastrukturen bzw. deren Verbänden zusammen. Erste Anlaufstelle, um geeignete Ansprechpartner für die Kernteams zu gewinnen, waren die BAK des UP KRITIS. Die *BSI-Kritisverordnung* wurde schließlich in zwei „Körben" 2016 und 2017 verabschiedet (vgl. Abbildung 17). Sie ermöglicht es den Betreibern, ihre „Einrichtungen, Anlagen oder Teile davon" dahin gehend zu überprüfen, ob sie „kritisch im Sinne des Gesetzes" sind (vgl. Abbildung 18).

Abbildung 17: Die *BSI-Kritisverordnung* regelt, welche konkreten Infrastrukturen innerhalb der vom *IT-Sicherheitsgesetz* adressierten Sektoren (dunkelgrün) als „kritisch" gelten. Die Verordnung wurde in zwei „Körben" 2016 (gelbe Punkte) und 2017 (rote Punkte) erarbeitet (Quelle: verändert nach BSI 2017a, Schutz Kritischer Infrastrukturen durch IT-Sicherheitsgesetz und UP KRITIS, S. 17).

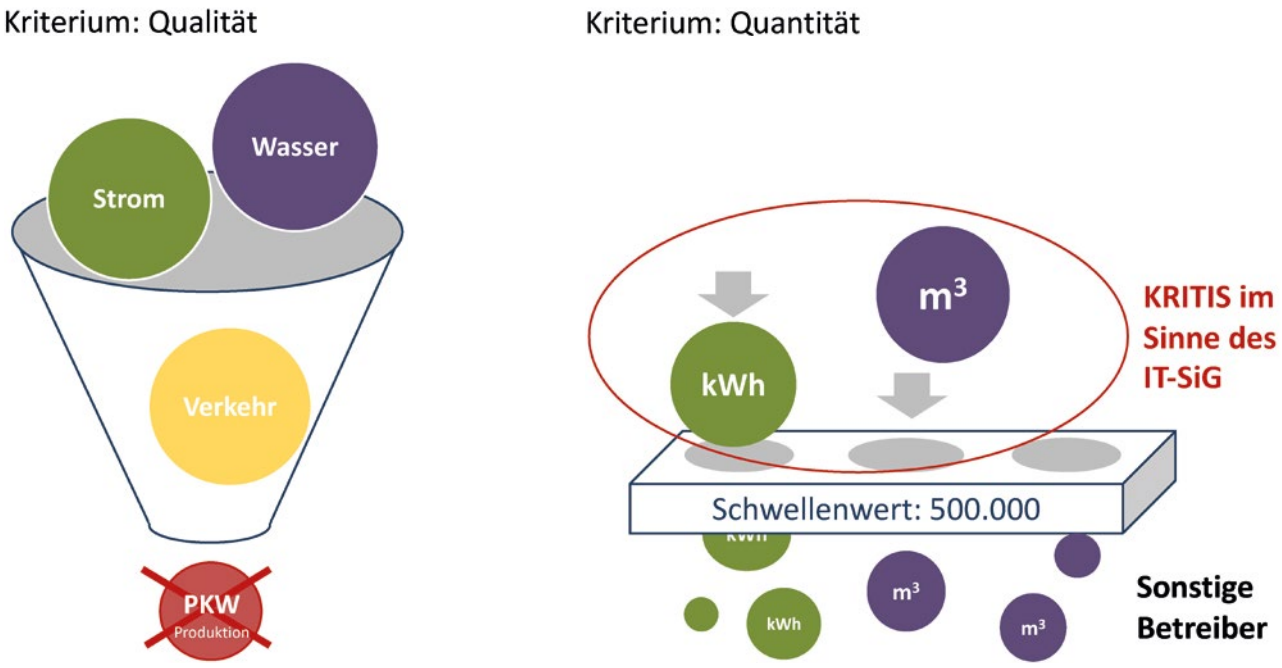


Abbildung 18: Um zu bestimmen, welche Anlagen und Einrichtungen zu den Kritischen Infrastrukturen im Sinnes des *IT-Sicherheitsgesetzes* gehören, wendet die *BSI-Kritisverordnung* eine Kombination aus qualitativen und quantitativen Kriterien an: zum einen die Zugehörigkeit zu einem der adressierten Sektoren, zum anderen den über Schwellenwerte operationalisierten Versorgungsgrad (Quelle: nach BSI).

Eine weitere wichtige Funktion erfüllt der UP KRITIS bei der Konkretisierung von § 8a Abs. 1 BSIG. Danach sind die Betreiber von Anlagen, die nach der *BSI-Kritisverordnung* Kritische Infrastrukturen sind, verpflichtet, die zur Aufrechterhaltung ihrer kritischen Dienstleistungen eingesetzte Informationstechnik nach dem „Stand der Technik" abzusichern. Das Gesetz gibt Betreibern und Branchenverbänden die Option, diesen Stand der Technik in Form „branchenspezifischer Sicherheitsstandards" (B3S) zu beschreiben (vgl. § 8a Abs. 2 BSIG). Auf diesem Weg kann ein passgenauer Standard formuliert werden, der den „Stand der Technik" nicht nur rechtssicher, sondern auch branchenspezifisch beschreibt (→ Kapitel 2.2.2).

Aufgrund ihrer Akteurskonstellation haben sich die BAK des UP KRITIS als ideales Umfeld für die Erarbeitung von B3S erwiesen: Die meisten der inzwischen vorliegenden B3S sind entweder direkt in den BAK oder in enger Abstimmung mit ihnen entstanden. Die Einbindung in die Strukturen des UP KRITIS vereinfachte zudem einen intensiven Austausch über die Branchengrenzen hinaus – dadurch musste das Rad nicht neu erfunden werden, wenn ähnliche Probleme in mehreren Branchen zu lösen waren. Auf Antrag werden alle vorgeschlagenen B3S vom BSI in Zusammenarbeit mit dem BBK und ggf. mit Beteiligung von Aufsichtsbehörden geprüft und, sofern deren Eignung gegeben ist, abgenommen. Die abgenommenen B3S können als Grundlage für den alle zwei Jahre gegenüber dem BSI zu erbringenden Nachweis über die Einhaltung der im BSIG formulierten Sicherheitsanforderungen an die IT herangezogen werden (vgl. § 8a Abs. 3 BSIG).

Auch wenn sich die B3S vornehmlich an die Betreiber von Kritischen Infrastrukturen im Sinne der *BSI-Kritisverordnung* richten, weisen sie auch allen anderen Betreibern in den betreffenden Branchen den Weg zu einem IT-Sicherheitsniveau nach dem Stand der Technik. Sie können damit auch über den Regelungsbereich des BSIG hinaus Wirkung entfalten und zum Schutz Kritischer Infrastrukturen beitragen.

2.4.3 Integriertes Risikomanagement – Akteure systematisch zusammen bringen

Im Risiko- und Krisenmanagement zeigt sich in Bezug auf Kritische Infrastrukturen, dass es nicht nur auf die Vorbereitung jedes einzelnen Akteurs ankommt, sondern insbesondere auf die Zusammenarbeit verschiedener Akteure. So wird zum Beispiel die Bewältigung eines Stromausfalls (→ Kapitel 2.4.5) dort am besten gelingen, wo sich Netzbetreiber und Akteure des Bevölkerungsschutzes bereits im Vorfeld über ihre jeweiligen Möglichkeiten ausgetauscht haben.

Die Zusammenarbeit von Akteuren des Bevölkerungsschutzes und häufig privatwirtschaftlichen Betreibern ist beim Schutz Kritischer Infrastrukturen der Knackpunkt, der über eine gelungene Risikominderung bzw. Krisenbewältigung entscheidet. Es hat sich allerdings auch gezeigt, dass hier noch viel zu tun ist: Häufig erstellt jede Organisation ihr eigenes Risikomanagement und arbeitet dabei mit einem eigenen Gefahrenszenario. Wenn die Grenze der eigenen Möglichkeiten erreicht ist, geht man oft automatisch davon aus, dass ein Dritter einspringen würde – etwa die Feuerwehr, das Technische Hilfswerk oder die Polizei. Doch diese Akteure können bei einem größeren Ereignis nicht überall gleichzeitig zur Verfügung stehen. Deshalb rückt beim Schutz Kritischer Infrastrukturen das Verfahren des sogenannten „Integrierten Risikomanagements“ in den Blickpunkt, das staatliche und private Akteure in allen Phasen des Risikomanagements zusammenbringt (vgl. Abbildung 19). Die Perspektive soll von der Einzelbetrachtung jedes Akteurs hin zu einer Gesamtbetrachtung verschoben und der Schwerpunkt auf die Schnittstellen und den Austausch von Informationen, Erkenntnissen und Ergebnissen zwischen den Akteuren gelegt werden. Diese Herangehensweise wird zunehmend praktiziert, nachdem es im Risikomanagement einzelner Einrichtungen bereits große Fortschritte gegeben hat. Die Erkenntnis, dass Zusammenarbeit nötig ist, verbreitet sich und führt dazu, dass sowohl von staatlicher als auch von privater Seite Schritte zu einem gemeinsamen Risikomanagement gemacht werden.

Wichtige Grundlagenarbeit zur Entwicklung und Erprobung des Integrierten Risikomanagements wurde im Rahmen des Forschungsprojekts

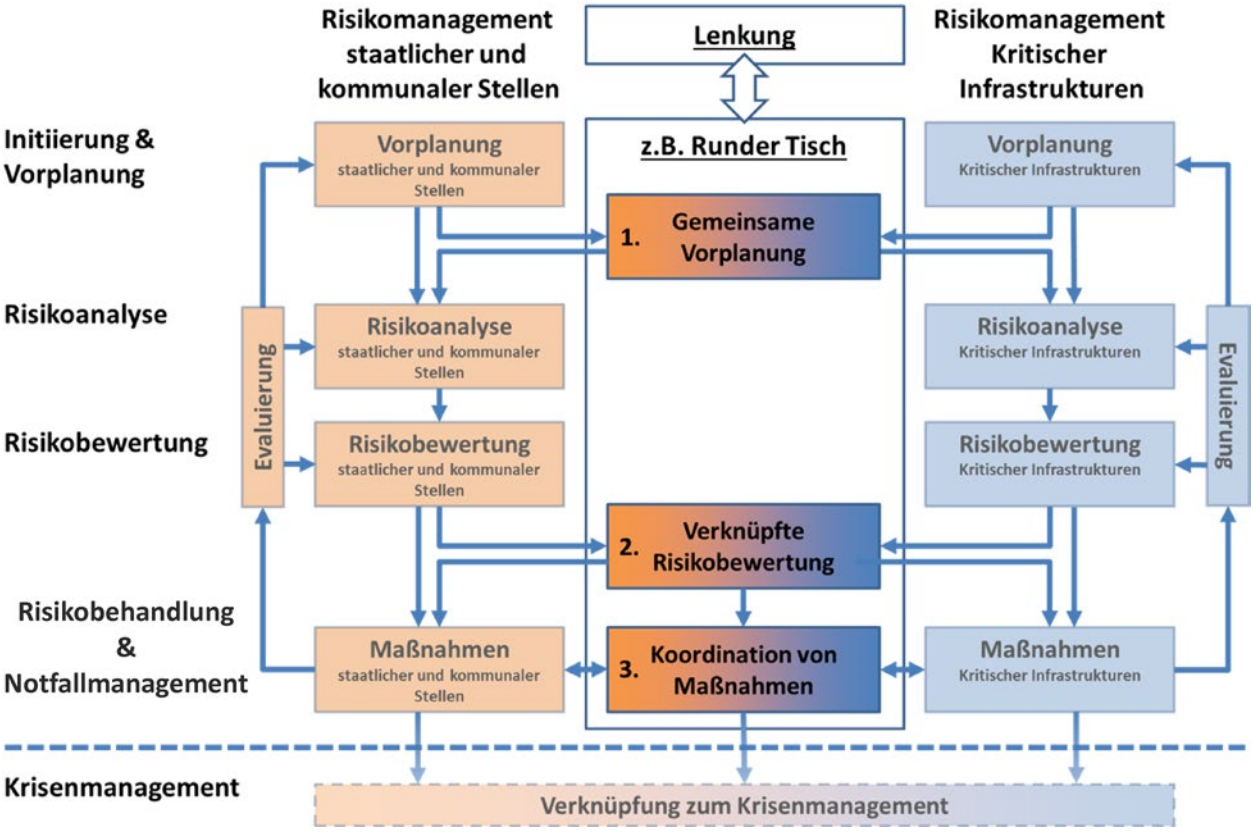


Abbildung 19: Abläufe im Integrierten Risikomanagement (Quelle: DIN SPEC 91390: 2019-12, S. 9; mit freundlicher Genehmigung DIN e. V.).

„KIRMin“ geleistet (→ Infobox 17). Das Verfahren wird in einigen Kontexten bereits erfolgreich angewendet. Die dahinterstehende Idee liegt auch der Zusammenarbeit im UP KRITIS (→ Kapitel 2.4.2) und weiteren Zusammenarbeitsformaten zugrunde. Um das Integrierte Risikomanagement auf allen Ebenen zu etablieren, wird die Vorgehensweise u.a. in Seminaren an der Akademie für Krisenmanagement, Notfallplanung und Zivilschutz (AKNZ) des BBK gelehrt. Zudem wird in Vorträgen und Veröffentlichungen darüber informiert (vgl. BBK 2018a). Dort, wo das Integrierte Risikomanagement praktiziert wird, hilft es den Vorbereitungsgrad aller Beteiligten zu verbessern – das soll in Zukunft überall so sein!

Infobox 17: Forschung zum Integrierten Risikomanagement – das Projekt KIRMin

Das Forschungsprojekt „Kritische Infrastrukturen – Resilienz als Mindestversorgungskonzept“ (KIRMin) wurde im Rahmen des Sicherheitsforschungsprogramms in der Bekanntmachung „Zivile Sicherheit – Erhöhung der Resilienz im Krisen- und Katastrophenfall“ gefördert (→ Kapitel 2.3.3). Das Projekt untersuchte die Abhängigkeiten verschiedener Kritischer Infrastrukturen in Deutschland. Besonders intensiv wurde dabei die Vulnerabilität der Wasserversorgung im Falle eines langanhaltenden und flächendeckenden Stromausfalls analysiert. Auf Grundlage der gewonnenen Erkenntnisse wurde ein Konzept zur Mindestversorgung der Bevölkerung während eines Stromausfalls erstellt. Einblicke in die weiteren Projektergebnisse gibt die Projektbroschüre „Wege zu einem Mindestversorgungskonzept. Kritische Infrastrukturen und Resilienz“ (vgl. Fekete et al. 2019).

Ein Schwerpunkt des Projektes lag darauf, verschiedene Akteure wie Vertreterinnen und Vertreter von Infrastrukturbetreibern, des Katastrophenschutzes, der Wissenschaft sowie der Zivilbevölkerung in einem umfassenden Dialogprozess zur Erarbeitung realitätsnaher Erkenntnisse und praktischer Maßnahmen zur Mindestversorgung zusammenzubringen. Eine besondere Rolle spielte dabei das Verfahren des „Integrierten Risikomanagements“, mit dessen Hilfe das Risikomanagement staatlicher Akteure mit dem Risikomanagement von Betreibern Kritischer Infrastrukturen systematisch verknüpft werden soll. Im Projekt KIRMin wurde das Verfahren konzeptionell weiterentwickelt und die DIN-Spezifikation „Integriertes Risikomanagement für den Schutz der Bevölkerung“ initiiert (DIN SPEC 91390: 2019-12; → Kapitel 2.2.2). Darin werden die Schnittstellen der verschiedenen Risikomanagementprozesse benannt und Potenziale für einen strukturierten Austausch von Informationen zwischen den beteiligten Akteuren aufgezeigt. Als DIN SPEC hat sie weder Norm- noch Gesetzesqualität und entfaltet somit keine eigenständige bindende oder verpflichtende Wirkung. Dennoch ist es gelungen, einen strukturierten Diskussionsprozess einzuleiten, der das Thema in den Fokus gerückt hat und in Zukunft in die Erstellung einer „echten“ Verfahrensnorm münden könnte. Zudem wurden im Projekt KIRMin Instrumente entwickelt, die die Anwendung des Integrierten Risikomanagements insbesondere auf lokaler Ebene unterstützen sollen. Diese Instrumente wurden in Zusammenarbeit mit den Projektpartnern fortlaufend weiterentwickelt und kamen in den Pilotregionen des Projektes – den Städten Köln, Mülheim an der Ruhr und Kerpen sowie im Rhein-Erft-Kreis – zur Anwendung.

2.4.4 Strategische Krisenmanagementübung LÜKEX – niemals ohne KRITIS!

Herausforderungen erkennen, Fortschritt gemeinsam anstoßen, voneinander lernen - diese Punkte treffen in das Herz der Übungsserie LÜKEX. Seit 2004 findet unter diesem Akronym die Länder- und Ressortübergreifende Krisenmanagementübung (Exercise) statt – noch nie ohne Beteiligung von Betreibern Kritischer Infrastrukturen. Während der letzten 16 Jahre ist es gelungen, Unternehmen aus allen KRITIS-Sektoren (→ Infobox 2) als einen Teil der Arbeitsgemeinschaft LÜKEX einzubeziehen und in starker Partnerschaft außergewöhnliche Krisenszenarien zu bewältigen. Die Szenarien sind stets so gewählt, dass eine breite gesellschaftliche Betroffenheit hergestellt wird. Vergangene LÜKEX-Übungen thematisierten beispielsweise Cyber-Angriffe, Stromausfälle, Sturmfluten oder eine Gasmangellage (vgl. Abbildung 20).

Schon in der meist einjährigen Vorbereitungsphase einer jeden LÜKEX entstehen thematische Netzwerke. Probleme und Fragestellungen werden im vertraulichen Rahmen offen adressiert und im Idealfall bereits vor den beiden Hauptübungstagen zu einer Lösung geführt. Die Betreiber Kritischer Infrastrukturen sind dabei intensiv mitübende Partner und gestalten aktiv das fiktive Szenario auf Länderebene oder in der zentralen Projektgruppe des Bundes mit. Die auf diesem Weg entstandenen Netzwerke bleiben auch nach der Übung bestehen, auf die dazugewonnenen Kontakte kann in etwaigen Reallagen zurückgegriffen werden.

Ziel des Übens ist eine verbesserte Vorbereitung auf vergleichbare Ereignisse, z. B. durch spezifisch ausgebildete Mitarbeiterinnen und Mitarbeiter, erprobte Kommunikationswege mit anderen Übungsbeteiligten oder getestete gemeinsame Vorgehensweisen. Die LÜKEX-Szenarien werden dabei so angelegt, dass eine Interaktion zwischen den unterschiedlichen Akteuren zwingend erforderlich wird: Nur durch eine übergreifend abgestimmte Strategie können die fiktiven Krisen bewältigt werden.

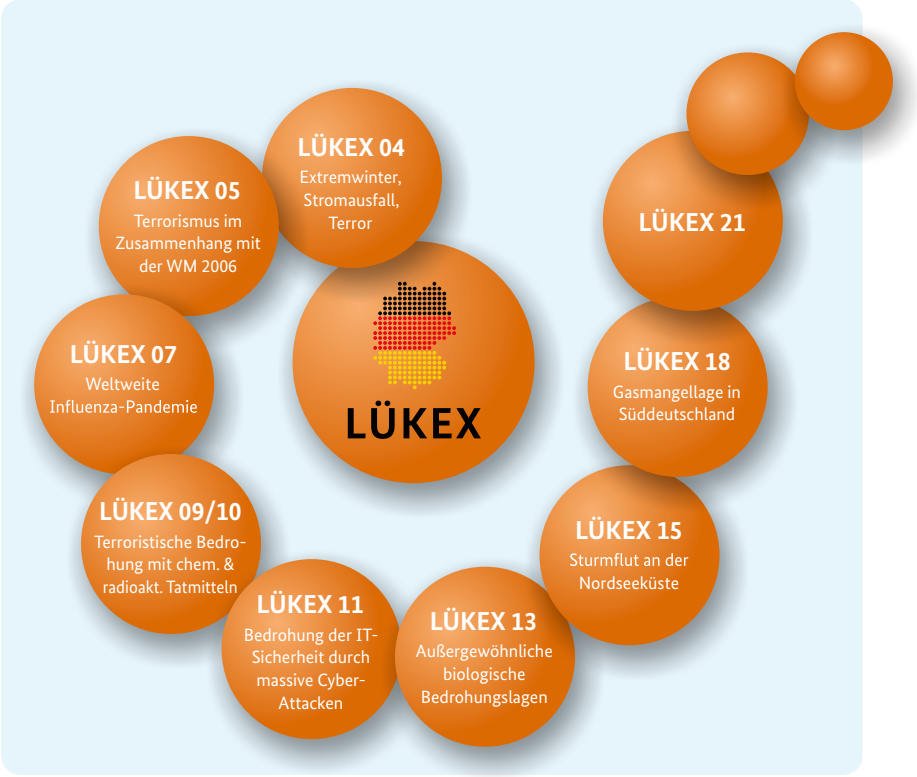


Abbildung 20: Überblick über die bisher durchgeführten Übungen der Reihe LÜKEX (Quelle: BBK).

Ohne die aktive Beteiligung von Unternehmen wäre eine realistische Darstellung vieler relevanter Prozesse nicht möglich und der Erkenntnisgewinn wesentlich geschmälert. Als Beispiel seien aus der LÜKEX 18 (vgl. BBK 2019b) insbesondere die komplexen Melde- und Informationswege genannt, die in einer Gasmangellage relevant werden. Nur mit den echten Betreibern des Gasnetzes konnte eine solche Übung realistisch durchgeführt werden. Bei LÜKEX profitieren also einerseits die öffentlichen Akteure von der Beteiligung der Wirtschaft, andererseits benötigen auch die Unternehmen die staatlichen Stellen, um ihrerseits Fortschritte in der krisenmäßigen Zusammenarbeit erzielen zu können.

Als Teil der Übungsvorbereitung werden Thementage organisiert. Diese fachlich ausgerichteten Veranstaltungen ermöglichen einen Blick über den Tellerrand. Hierbei gewinnen die Übungsplanenden sowie viele weitere Interessierte einen tiefgreifenden Einblick in die Fachwelt des jeweiligen Übungsthemas. Zu jedem Thementag wird ein Tagungsband publiziert, in dem die Fachvorträge der vortragenden Expertinnen und Experten festgehalten sind. Um die Erkenntnisse einer jeden LÜKEX nachhaltig zu fixieren, schließt jede Übung mit einem gemeinsamen Erfahrungsbericht ab. Die Übungsbeteiligten greifen die im Erfahrungsbericht formulierten Handlungsempfehlungen auf und setzen diese in eigener Zuständigkeit und, falls erforderlich, auch in Kooperation mit anderen um. Verbände wirken als Multiplikatoren, um die Erkenntnisse in ihren jeweiligen Branchen zu streuen.

Seit nunmehr 16 Jahren bringen sich Betreiber Kritischer Infrastrukturen aktiv in die Vorbereitung, Durchführung und Auswertung strategischer Krisenmanagementübungen ein. Auch zukünftig wird mit der Übungsserie LÜKEX die Zusammenarbeit von betreiberseitigem und staatlichem Krisenmanagement fortgeführt und weiter ausgebaut werden, denn ohne KRITIS-Betreiber keine LÜKEX! Informationen zur Übungsreihe LÜKEX sowie die im Text genannten Tagungsbände und Auswertungsberichte stellt das BBK zur Verfügung (www.luekex.de).

2.4.5 Gemeinsam planen für den Blackout: Das Rahmenkonzept Notstromversorgung

Das Thema „Stromausfall“ hat in den letzten Jahren zahlreiche staatliche, kommunale und privatwirtschaftliche Akteure beschäftigt. Dabei ist die Stromversorgungsqualität in Deutschland außerordentlich hoch, großflächige und langandauernde Stromausfälle hat es hier bisher nicht gegeben. Würde es allerdings dazu kommen, wären die Auswirkungen in allen Lebensbereichen wie Kommunikation, Gesundheitsversorgung, Mobilität und Lebensmittelversorgung zu spüren. Das Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB) hat sich 2010 intensiv mit dem Szenario eines mehrere Wochen andauernden, großflächigen Stromausfalls beschäftigt und die Folgen dazu ausführlich in einem Bericht dargelegt (vgl. BT-Drs. 17/5672). Der Bericht kommt zu folgendem Ergebnis: „Die Wahrscheinlichkeit eines langandauernden und das Gebiet mehrerer Bundesländer betreffenden Stromausfalls mag gering sein. Träte dieser Fall aber ein, kämen die dadurch ausgelösten Folgen einer nationalen Katastrophe gleich“ (BT-Drs. 17/5672, S. 15).

In Deutschland gibt es nicht die *eine* Behörde, die für die Notfallplanung für Stromausfallszenarien zuständig ist: Staatliche Akteure in Bund, Ländern und Kommunen sowie KRITIS-Betreiber setzen jeweils in eigener Zuständigkeit Maßnahmen um. Dazu zählen so unterschiedliche Aktivitäten wie die Erstellung und Umsetzung von Notfallplänen, die Anschaffung von Notstromaggregaten oder die Teilnahme an Arbeitskreisen und Übungen zu Stromausfallszenarien. Bei der Vielzahl und Vielfalt der von unterschiedlichen Akteuren auf verschiedenen Ebenen und unter Beteiligung mehrerer Ressorts unternommenen Schritte können Planungs- und Informationslücken entstehen, die nicht von den einzelnen Beteiligten aus ihrer jeweiligen Innenperspektive, sondern nur in der „Draufsicht“ erkennbar sind. Im Zuge der Bearbeitung des „Rahmenkonzepts Notstrom“ werden daher beim BBK laufend Wissensstände erfasst und Empfehlungen erarbeitet, die aufzeigen, wie Planungs- und Informationslücken in der Notfallplanung für Stromausfall – bei und zwischen den Akteuren – geschlossen werden können. Planungslücken können sich z. B. bei der Erfassung benötigter Kapazitäten, bei der Priorisierung oder

bei der Festlegung von Zielgrößen und Schwellenwerten unterschiedlicher Art ergeben. Gleichzeitig kann man aber auch genau dort ansetzen: Beispielsweise empfiehlt das BBK für die Aufrechterhaltung der Notstromversorgungen ohne Nachbetankung eine einheitliche Soll-Größe von mindestens 72 Stunden für alle Kritischen Infrastrukturen. Dieses Schutzziel ist mittlerweile in der Fachcommunity etabliert (→ Infobox 18). In einigen Verantwortungsbereichen hat sich die Auslagerung von Treibstoff aus Tanklagern und dessen gezielte Verteilung an die Endverbraucher als eine wesentliche Planungslücke in der Notfallplanung für Stromausfälle herausgestellt (→ Infobox 20).

In den letzten Jahren sind in Deutschland auf allen Ebenen Maßnahmen entwickelt und umgesetzt worden, um die Notfallplanung für Stromausfälle stetig fortzuentwickeln. Die zentrale Herausforderung bleibt dabei die akteursübergreifend notwendige Abstimmung und Zusammenarbeit, da Zuständigkeiten horizontal (über verschiedene Ressorts) und vertikal (über föderale Ebenen) verteilt sind.

Infobox 18: Notstromversorgung für Betreiber und Behörden

Die Problematik einer ausreichenden Notstromversorgung von KRITIS-Betreibern und Behörden ist schon seit der LÜKEX 2004 zum Thema Stromausfall bekannt (→ Kapitel 2.4.4). Denn nur in sehr wenigen Bereichen (z. B. bei Krankenhäusern) gibt es hierzu deutschlandweite, verbindliche Vorschriften. Wo es diese gibt, beziehen sie sich häufig nur auf einige Bereiche und auf sehr unterschiedliche Zeiträume. Deshalb hat das BBK Empfehlungen dazu erarbeitet, wie Einrichtungen ihren Energiebedarf ermitteln und ihre Notstromversorgung aufbauen und sicherstellen können (vgl. BBK 2015a). Die Empfehlungen sind das Ergebnis eines kontinuierlichen Entwicklungsprozesses, in den die Erfahrungen vieler Akteure eingeflossen sind, mit denen das BBK in den vergangenen Jahren zum Thema Notfallvorsorge zusammengearbeitet hat. In den Empfehlungen wird auch ein Richtwert von mindestens 72 Stunden für die Bevorratung von Treibstoff angegeben, um eine Harmonisierung der Notfallvorsorge herbeizuführen. Der Richtwert leitet sich u. a. daraus ab, dass 72 Stunden voraussichtlich genügen, um bei einem länger andauernden Stromausfall die Weiterversorgung mit Treibstoff zu gewährleisten. Die Zielgröße von 72 Stunden wurde im Nachgang in vielen Bereichen übernommen, so z. B. in dem „Merkblatt für die Aufrechterhaltung der sicheren Gasversorgung bei Ausfall der regulären Kommunikation“ des Deutschen Vereins des Gas- und Wasserfaches e. V. (vgl. DVGW G 1003; → Kapitel 2.2.2). Auch zur Lagerung von Treibstoffen wurden ergänzende Empfehlungen erstellt. Wenn Dieselkraftstoff länger unbenutzt gelagert wird, besteht die Gefahr eines mikrobiologischen Befalls. Diesbezüglich müssen wirksame Maßnahmen ergriffen werden, denn nur mit einwandfreiem Treibstoff ist die Notstromanlage im Ernstfall eine Hilfe.

Infobox 19: Bei Stromausfall im Einsatz – Fähigkeiten der Bundesanstalt Technisches Hilfswerk

Das Technische Hilfswerk (THW) ist die operative Einsatzorganisation des Bundes und leistet technische Hilfe nach dem *Zivilschutz- und Katastrophenhilfegesetz*. Auf Grundlage des *THW-Gesetzes* kann das THW bei Schadenlagen größeren Ausmaßes von den für die Gefahrenabwehr zuständigen Stellen angefordert werden – unter anderem, wenn es um die Bereitstellung von Notstromkapazitäten geht (vgl. THW 2014). Hierbei leistet das THW im Bedarfsfall Unterstützung, übernimmt aber nicht die Daseinsvorsorge für die originär zuständigen Stellen.

Grundlage für Auf- und Ausbau von Fähigkeiten des THW ist – nicht nur, aber auch hinsichtlich der Notstromversorgung – das „THW-Rahmenkonzept“. Das Rahmenkonzept sieht unterschiedliche Fähigkeiten in der Notstromversorgung vor. Um die Einsatzfähigkeit des THW oder anderer Einsatzorganisationen zu gewährleisten, ist die Bereitstellung von Notstromkapazitäten in den Leistungsgrößen 13 bis 50 kVA vorgesehen. Diese Fähigkeit hat das THW mit der Fachgruppe „Notversorgung und -instandsetzung“ gestärkt und flächendeckend eingeführt. Zukünftig wird also jeder Ortsverband des THW über diese Fähigkeit

verfügen. Eine andere Größenordnung benötigt man für die Bereitstellung von Notstrom zur Versorgung von größeren Einsatzstellen oder Bereitstellungsräumen im Inselbetrieb. Für diese Zwecke stehen Notstromkapazitäten in der Größenordnung 175 bis 200 kVA bereit. Das THW-Rahmenkonzept sieht für die dafür zuständige Fachgruppe „Elektroversorgung“ eine Fähigkeitserweiterung vor. Diese Erweiterung strebt das THW an, um zukünftig bei der Versorgung einzelner Netzbereiche oder bei der Stützung von teilweise ausgefallenen Netzen noch besser helfen zu können.

Abbildung 21: Notstromkapazitäten des THW im Einsatz (Quelle: THW).

Infobox 20: Treibstoffversorgung bei Stromausfall

Einsatzfahrzeuge und Notstromaggregate benötigen im Ereignisfall die Zulieferung von Dieselkraftstoff. Daher ist die Treibstoffversorgung eine elementare Herausforderung bei der Bewältigung eines langanhaltenden und großflächigen Stromausfalls. In einem ersten Aufschlag haben sich unter Moderation des BBK Akteure aus den Ländern, den Kommunen und der Mineralölbranche intensiv mit der Auslagerung und Verteilung von Treibstoff bei Stromausfall beschäftigt und ihre Ergebnisse in einer Empfehlung zusammengefasst (BBK 2017). Die Lösungsansätze reichen von der Festlegung von notstromversorgten Tankstellen und Tanklagern über die Priorisierung berechtigter Abnehmer im Vorfeld, die Organisation von Transportkapazitäten bis hin zu regelmäßigen Übungen zwischen den beteiligten Akteuren. Zwingend erforderliche weitere Abstimmungen zwischen Bund und Ländern zu Rechtsfragen, Zuständigkeiten, Planung und Organisation sollen u. a. im Rahmen einer durch das federführende Bundesministerium für Wirtschaft und Energie (BMWi) einberufenen Arbeitsgruppe erfolgen.

Abbildung 22: (Quelle: Skitterphoto / pixabay)

Infobox 21: Was tun, wenn der Strom ausfällt? Bürgerinformation zum Thema Stromausfall

Nicht nur für Behörden und KRITIS-Betreiber sondern auch für die Bürgerinnen und Bürger ist es wichtig, beim Ausfall der Stromversorgung gut aufgestellt zu sein. Das gilt ganz besonders für Menschen, die noch stärker als andere auf die Stromversorgung angewiesen sind, beispielsweise Beatmungspatienten oder Familien, die Babynahrung zubereiten müssen. Viele Menschen benötigen aber auch andere Versorgungsdienstleistungen, die bei Stromausfall nicht mehr gewährleistet sein könnten. Wer etwa Essen auf Rädern bezieht oder Pflegeleistungen in Anspruch nimmt, sollte sich mit dem Thema befassen. Letztlich ist jede und jeder Einzelne gefragt, für sich selbst und die Menschen in seinem Umfeld vorzusorgen.

Abbildung 23: (Quelle: Mark Evans / E+ / Getty Images)

Um die persönliche Vorsorge speziell für Stromausfälle zu unterstützen, stellt das BBK Informationen in einer Broschüre (BBK 2019c) und im Video bereit (BBK 2015b). Während zur Vorsorge immer ein Notvorrat an Wasser und Lebensmitteln gehört und auch eine gute Vernetzung innerhalb der Nachbarschaft stets zu empfehlen ist, sollte die Einrichtung einer eigenen Notstromversorgung sorgfältig geprüft werden. Die Möglichkeiten wurden ausführlich in einem Forschungsprojekt zur autarken Notstromversorgung der Bevölkerung untersucht (vgl. BBK 2018b). Wie eine Notstromversorgung für den Eigenbedarf aufzubauen und zu handhaben wäre, wird in o. g. Broschüre und auch im Video (BBK 2015c) beschrieben.

Abbildung 24: (Quelle: Ashok Rodrigues / E+ / Getty Images)

2.5

Kapitel

Quelle: Rico Wasikowski / Moment / Getty Images

Schutz Kritischer Infrastrukturen als sektorale Aufgabe

Beim Schutz Kritischer Infrastrukturen wird der Berücksichtigung sektorenübergreifender Verknüpfungen und Abhängigkeitsbeziehungen viel Bedeutung beigemessen. Dass viele Ansätze und Aktivitäten in diesem Kontext dennoch eine sektorale Ausrichtung aufweisen (→ Infobox 2), steht dazu allerdings nicht im Widerspruch. Vielmehr gibt es einen Bedarf, übergeordnete Herangehensweisen für unterschiedliche sektorale Kontexte zu konkretisieren und grundsätzliche Fragen in einer sektorenspezifischen Weise zu stellen. Deshalb wurden vielfach Methoden zur Anwendung innerhalb eines Sektors, einer Branche oder sogar eines bestimmten Einrichtungstyps zugeschnitten und auch außerhalb des UP KRITIS haben sich sektorale Netzwerke mit Bezug zum Schutz Kritischer Infrastrukturen gebildet.

Unter dem Eindruck folgenschwerer Ereignisse, u. a. dem Brand der Herzogin Anna Amalia Bibliothek (2004) und des Elbehochwassers (2002), begannen im Jahr 2006 – initiiert durch die Konferenz Nationaler Kultureinrichtungen (KNK) – die Arbeiten am „SicherheitsLeitfaden Kulturgut“ (SiLK). Das internetgestützte Beratungs- und Evaluierungsinstrument deckt Themen rund um den Schutz von Kulturgütern ab und richtet sich an Museen, Bibliotheken und Archive als Betreiber wichtiger Einrichtungen im KRITIS-Sektor *Kultur und Medien* (→ Kapitel 2.5.1).

Zur Sensibilisierung und Unterstützung von Betreibern und Behörden hat das BBK zwei Empfehlungen zur Sicherheit der Trinkwasserversorgung herausgegeben (→ Kapitel 2.5.2). Der erste Teil unterstützt die Aufgabenträger der Wasserversorgung in den Kommunen bei der Untersuchung und Bewertung von Risiken, insbesondere im Zusammenhang mit außergewöhnlichen Gefahrenlagen. Der zweite Teil beschreibt die Schritte zur Erarbeitung einer Notfallvorsorgeplanung.

Bei der Ausgestaltung des Risikomanagements im Sektor *Finanz- und Versicherungswesen* nehmen die Rundschreiben der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) eine zentrale Rolle ein. Sie definieren Mindestanforderungen an das Risikomanagement im Kredit- und Finanzdienstleistungswesen oder konkretisieren in den bank-, versicherungs- und kapitalverwaltungsaufsichtlichen Anforderungen auch IT-Sicherheitsaspekte für Betreiber Kritischer Infrastrukturen (→ Kapitel 2.5.3).

Für Krankenhäuser als Kritische Infrastrukturen im Sektor *Gesundheit* wurden methodische Grundlagen zum Risiko- und Krisenmanagement in mehreren Veröffentlichungen adressatenspezifisch zugeschnitten. Unter Beteiligung von Expertenkreisen und Praxispartnern entstand 2008 ein Leitfaden für das Risikomanagement im Krankenhaus. In einem 2013 veröffentlichten Leitfaden werden IT-Sicherheitsfragen im Klinikbetrieb aufbereitet. Das Handbuch zur Krankenhausalarm- und -einsatzplanung wird zu planerischen Maßnahmen anleiten, um Kapazität und Funktionalität von Krankenhäusern in Schadenslagen aufrechtzuerhalten (→ Kapitel 2.5.4).

Im BMVI-Expertennetzwerk werden die Kompetenzen und das Know-how von sieben Ressortforschungseinrichtungen und Fachbehörden im Geschäftsbereich des Bundesministeriums für Verkehr und digitale Infrastruktur (BMVI) gebündelt und auch Fragen des Schutzes Kritischer Infrastrukturen im Sektor *Transport und Verkehr* behandelt. In unterschiedlichen Themenfeldern werden z. B. die aktuellen und in Zukunft zu erwartenden Auswirkungen von klimatisch bedingten Extremereignissen auf unterschiedliche Verkehrsträger untersucht und Anpassungsoptionen entwickelt (→ Kapitel 2.5.5).

2.5.1 Der „SicherheitsLeitfaden Kulturgut“

SiLK
SicherheitsLeitfaden
Kulturgut ein projekt der
konferenz nationaler kultureinrichtungen

Die *Haager Konvention zum Schutz von Kulturgut bei bewaffneten Konflikten* von 1954 (Haager Konvention) hat das Ziel, Kulturgüter bei bewaffneten Konflikten vor Zerstörung, Diebstahl und Plünderung zu schützen und somit zu verhindern, dass Kulturobjekte zum Spielball psychologischer Kriegsführung werden (→ Infobox 3). Deutschland hat den Vertrag und die beiden Ergänzungsprotokolle ratifiziert und die innerstaatliche Aus-

führung dem BMI übertragen (vgl. *Gesetz zu der Konvention vom 14. Mai 1954 zum Schutz von Kulturgut bei bewaffneten Konflikten* vom 11. April 1967). Die Aufgaben werden vom BBK und im Auftrag des Bundes von den Ländern wahrgenommen. Die Umsetzung der *Haager Konvention* ist in Deutschland Teil der „Konzeption Zivile Verteidigung" (BMI 2016b; → Kapitel 2.3.2).

Ein wesentlicher Beitrag zur Umsetzung der *Haager Konvention* ist der „SicherheitsLeitfaden Kulturgut" (SiLK, KNK o.A.), ein internetgestütztes Beratungs- und Evaluierungsinstrument für Themen rund um den Schutz von Kulturgütern. Angesichts der Zerstörung von kulturellem Erbe durch den Brand der Herzogin Anna Amalia Bibliothek (2004) und durch das Elbehochwasser (2002) wurde das Projekt im Jahr 2006 von der Konferenz Nationaler Kultureinrichtungen (KNK) ins Leben gerufen. Die Inhalte von SiLK wurden in Kooperation mit zahlreichen Experten erarbeitet und werden stetig weiterentwickelt. Das Instrument dient mit seinen einführenden Texten, seinen interaktiven Fragebögen und seinem Wissenspool der Schärfung des Bewusstseins für das Thema Sicherheit und Kulturgutschutz in Museen, Bibliotheken und Archiven als Betreiber wichtiger Einrichtungen im KRITIS-Sektor Kultur und Medien (→ Infobox 2). SiLK unterstützt die zuständigen Mitarbeiterinnen und Mitarbeiter dabei, Risikoanalysen durchzuführen und den Sicherheitsstand der Einrichtung zu evaluieren, macht auf Defizite aufmerksam und zeigt Handlungsoptionen auf, um die Sicherheit und den langfristigen Erhalt unserer Kulturgüter zu gewährleisten.

Zu den letzten Weiterentwicklungen zählt ein Konzept zur Bergung von Kulturgütern im Falle eines bewaffneten Konflikts, das 2018 bei der alle drei Jahre stattfindenden internationalen SiLK-Fachtagung „KULTUR!GUT!SCHÜTZEN!" präsentiert wurde. Neben dem Betrieb des „SicherheitsLeitfadens Kulturgut" veranstaltet das SiLK-Team Workshops sowie Tagungen und publiziert, berät und referiert zu Themen des Kulturgutschutzes.

SiLK wurde ab 2006 von der Beauftragten der Bundesregierung für Kultur und Medien (BKM) gefördert, bevor im Jahr 2016 das BBK die Finanzierung übernommen hat. SiLK wird auf der Internetseite der KNK zur Verfügung gestellt (www.konferenz-kultur.de).

Abbildung 25: (Quelle: Maik Schuck / Klassik Stiftung Weimar, Museen, A 1580)

2.5.2 Sicherheit der Trinkwasserversorgung – Risikoanalyse und Notfallvorsorgeplanung

Eine zuverlässige Trinkwasserversorgung ist eine wichtige Grundlage des Gesellschafts- und Wirtschaftssystems. Aufgrund der ausgesprochen hohen Versorgungssicherheit erscheint die ständige Verfügbarkeit von Wasser in bester Trinkwasserqualität und in gewünschter Menge in Deutschland vielen wie eine Selbstverständlichkeit. Sie ist allerdings auch das Ergebnis vorausschauender und vorsorgender Planung und kontinuierlicher Verbesserung von Sicherheitsvorkehrungen. Auf die Notwendigkeit dieser Vorgehensweise weisen außergewöhnliche Ereignisse immer wieder hin. So wurde in den letzten Jahren zunehmend deutlich, dass nicht nur der Klimawandel in Form von Hochwasser, Starkregen und Trockenheit die Versorgungssicherheit vor neue Herausforderungen stellt. Auch Cyber-Gefahren und Bedrohungen mit terroristischem oder kriminellem Hintergrund sind für den Sektor Wasser von solch großer Relevanz, dass sie von Unternehmen und Behörden in die Risikobetrachtungen einbezogen werden müssen. Zur Sensibilisierung und Unterstützung von Unternehmen und Behörden hat das BBK zwei Empfehlungen zur Sicherheit der Trinkwasserversorgung herausgegeben (vgl. auch Abbildung 26).

„Teil 1: Risikoanalyse“ (BBK 2019d) unterstützt die Aufgabenträger der Wasserversorgung in den Kommunen bei der Untersuchung und Bewertung von Risiken durch Naturgefahren, technisches oder menschliches Versagen, Kriminalität, Terrorismus oder auch kriegerische Auseinandersetzungen. Der Schwerpunkt liegt auf der strukturierten Analyse von Risiken und Verwundbarkeiten außergewöhnlicher Schadenslagen. „Teil 2: Notfallvorsorgeplanung“ (BBK 2019e) beschreibt die notwendigen Schritte zur Erarbeitung einer Planung zur Ersatz- und Notwasserversorgung. Das bedeutet u. a., sich mit den rechtlichen und organisatorischen Rahmenbedingungen proaktiv vertraut zu machen und aus der Analyse der identifizierten Versorgungsarten und den vorhandenen Ressourcen den zusätzlichen Ressourcenbedarf abzuleiten.

Abbildung 26: Einordnung der Inhalte der Fachinformationen „Sicherheit der Trinkwasserversorgung“ (BBK 2019d; BBK 2019e) in den Kontext des Risiko-und Krisenmanagementkonzepts des BMI (→ Kapitel 2.1.1; Quelle: BBK).

Beide Empfehlungen zielen im Sinne des Integrierten Risikomanagements auf die Zusammenarbeit aller Aufgabenträger der Wasserversorgung wie Wasserversorger, Gesundheitsämter und Akteure des Katastrophenschutzes ab (→ Kapitel 2.4.3). Zahlreiche Pilotprojekte haben die Praxisnähe und Umsetzbarkeit der in Anlehnung an die allgemein anerkannten Regeln der Technik empfohlenen Methoden zur Risikoanalyse und Notfallvorsorge bestätigt (→ Kapitel 2.2.2). Die Veröffentlichungen zur Sicherheit der Trinkwasserversorgung sind Grundlage von Lehrveranstaltungen an der Akademie für Krisenmanagement, Notfallplanung und Zivilschutz (AKNZ) des BBK.

2.5.3 Anforderungen an Risikomanagement und IT-Sicherheit im Finanz-und Versicherungswesen

Maßnahmen zum Risikomanagement im KRITIS-Sektor *Finanz- und Versicherungswesen* (→ Infobox 2) sind Gegenstand von Rundschreiben der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), der Fachaufsicht über Banken und Finanzdienstleister, Versicherer und den Wertpapierhandel in Deutschland (Aufsichtsobjekte). Mit den betreffenden Rundschreiben werden die gesetzlichen Anforderungen an die Aufsichtsobjekte konkretisiert. Dies betrifft auch Anforderungen an die IT der Aufsichtsobjekte sowie deren IT-Dienstleister, die teilweise einen direkten Bezug zum Schutz Kritischer Infrastrukturen haben.

Dazu zählt etwa das Rundschreiben zu den „Mindestanforderungen an das Risikomanagement“ (MaRisk) im Kredit- und Finanzdienstleistungswesen (Rundschreiben 09/2017, BaFin 2017). Zwar denkt man in diesem Anwendungskontext zunächst an finanzielle Risiken, deren Management auch tatsächlich den größten Raum in den Ausführungen zu den MaRisk einnimmt. Allerdings geht das Modul „Anforderungen an die Risikosteuerungs- und -controllingprozesse“ auch auf die sogenannten operationellen Risiken ein. Operationelles Risiko ist gemäß Art. 4 (52) der *Verordnung über Aufsichtsanforderungen an Kreditinstitute und Wertpapierfirmen* (Verordnung-EU Nr. 575/2013) das Risiko von Verlusten, die durch die Unangemessenheit oder das Versagen von internen Verfahren, Menschen, Systemen oder durch externe Ereignisse verursacht werden, einschließlich Rechtsrisiken. Die Institute müssen u. a. gewährleisten, dass die entsprechenden Risiken jährlich identifiziert und beurteilt, Schadensfälle erfasst und deren Ursachen analysiert werden sowie Maßnahmen, zu denen auch Katastrophenschutzmaßnahmen gehören können, im Rahmen der Risikosteuerung umgesetzt und überwacht werden.

Ebenfalls im Jahr 2017 veröffentlichte die BaFin ihr Rundschreiben „Bankaufsichtliche Anforderungen an die IT“ (BAIT), um den Geschäftsleitungen der Institute die Erwartungen der Bankenaufsicht an eine sichere Ausgestaltung der IT-Systeme sowie die Anforderungen an die IT-Governance transparent zu machen (Rundschreiben 10/2017, aktualisierte Fassung: BaFin 2018a). Die BAIT ist der zentrale Baustein für die IT-Aufsicht über den Bankensektor in Deutschland. Im September 2018 wurde die BAIT zur erleichterten Umsetzung der Anforderungen des § 8a Abs. 3 BSI-Gesetz in Abstimmung mit dem BSI um ein neues Modul „Kritische Infrastrukturen“ ergänzt (vgl. BaFin 2018b; → Kapitel 2.2.1 und Infobox 16). Dieses spezielle Modul gilt ausschließlich für diejenigen Unternehmen in der Bankenbranche, die gleichzeitig KRITIS-Betreiber nach den Kriterien der *BSI-Kritisverordnung* sind. Die Erreichung von KRITIS-Schutzzielen – hier die Sicherstellung der Grundversorgung der Bevölkerung mit Zahlungsdienstleistungen auch im Krisenfall – ist somit elementarer Bestandteil der Bankenaufsicht.

Im Juli 2018 ist auch das Rundschreiben „Versicherungsaufsichtliche Anforderungen an die IT“ (VAIT) in Kraft getreten (Rundschreiben 10/2018, aktualisierte Fassung: BaFin 2019a). Vergleichbar den BAIT für den Bankensektor sind die VAIT der zentrale Baustein der IT-Aufsicht im Versicherungsbereich. Sie enthalten mittlerweile ebenfalls ein Modul „Kritische Infrastrukturen“, das für diejenigen Versicherungsunternehmen gilt, die zugleich auch KRITIS-Betreiber nach den Kriterien der *BSI-Kritisverordnung* sind. Im Oktober 2019 hat die BaFin zudem das Rundschreiben 11/2019 „Kapitalverwaltungsaufsichtliche Anforderungen an die IT“ (KAIT, BaFin 2019b) veröffentlicht.

2.5.4 Das Krankenhaus als Kritische Infrastruktur des Gesundheitswesens

Krankenhäuser gehören zu denjenigen Einrichtungen, deren Leistungen im Alltag und insbesondere bei größeren Schadenslagen mit einer Vielzahl von Verletzten oder Kranken dringend gebraucht werden. Kann ein Krankenhaus seine kritischen Dienstleistungen nicht aufrechterhalten, kann dies zu einer Gefährdung von Gesundheit und Leben der Patienten führen. Die nachfolgend beschriebenen, 2008 und 2013 erschienenen sowie für 2020 geplanten Veröffentlichungen befassen sich alle mit dem Krankenhaus als Kritische Infrastruktur im Sektor *Gesundheit* (→ Infobox 2). In allen Veröffentlichungen wurden methodische Grundlagen (→ Kapitel 2.1) für die Anwendung in Krankenhäusern aufbereitet und auf die spezifischen Herausforderungen dieses Adressatenkreises zugeschnitten. Sie stehen nicht unverbunden nebeneinander, sondern in einem bestimmten Verhältnis zueinander. Die Veröffentlichungen verbindet zudem, dass sie nicht im sprichwörtlichen „stillen Kämmerlein", sondern in interdisziplinären Arbeitsgruppen und Projektkonsortien entstanden sind.

Damit Krankenhäuser ihre Funktionsfähigkeit auch in Krisenlagen aufrechterhalten und die Folgen für Patientinnen und Patienten, Angehörige sowie Mitarbeiterinnen und Mitarbeiter möglichst klein gehalten werden können, ist ein umfassendes Risikomanagement unabdingbar. Um den methodischen Zugang zur Etablierung eines Risikomanagements in Krankenhäusern zu unterstützen, veröffentlichte das BBK im Jahr 2008 den Leitfaden „Schutz Kritischer Infrastrukturen: Risikomanagement im Krankenhaus" (BBK 2008). Er ist das Ergebnis einer Arbeitsgruppe mit Vertreterinnen und Vertretern aus Verwaltung, Fachverbänden und Krankenhausbetreibern. Das im Leitfaden beschriebene Risikomanagementverfahren leitet dazu an, kritische Prozesse eines Krankenhauses zu identifizieren, deren Verwundbarkeiten gegenüber möglichen Gefahren zu erkennen und auf dieser Basis Schutzmaßnahmen abzuleiten. Der Leitfaden zum Risikomanagement im Krankenhaus ist seit über zehn Jahren fester Bestandteil der „Leitfadenfamilie" zum Schutz Kritischer Infrastrukturen und soll in naher Zukunft in einer aktualisierten Neuauflage erscheinen.

Aufbauend auf diesen allgemeinen Ansätzen zum Risikomanagement in Krankenhäusern befasst sich der Leitfaden „Risikoanalyse Krankenhaus-IT" (BSI 2013a) mit den individuellen Herausforderungen, die durch die Abhängigkeit von der Informationstechnik in Krankenhäusern entstehen. Informationstechnik ist aus dem Krankenhausbetrieb nicht mehr wegzudenken – nicht nur die Verwaltungsabläufe, auch die medizinische und pflegerische Patientenversorgung inklusive diagnostischer Maßnahmen wie Laboruntersuchungen oder bildgebende Verfahren werden maßgeblich von IT-Anwendungen unterstützt. Die Technik, die im Alltag die Arbeit erleichtert, kann allerdings auch ausfallen oder missbräuchlich verwendet werden. Aus diesem Grund widmete sich ein vom BSI geleitetes Projekt unter Mitarbeit des BBK, der Senatsverwaltung für Gesundheit und Soziales Berlin sowie des Unfallkrankenhauses Berlin (UKB) dem Spezialaspekt der IT-Sicherheit von Krankenhäusern. Ergebnis der Projektarbeit ist der im Jahr 2013 veröffentlichte Leitfaden „Risikoanalyse Krankenhaus-IT", der für einen schnellen Überblick auch in einer Kurzfassung zur Verfügung steht (vgl. BSI 2013b).

Mithilfe der hier beschriebenen Methode können kritische IT-Abhängigkeiten in einem Krankenhaus und die daraus erwachsenden Risiken schrittweise identifiziert und bewertet werden. Diese Erkenntnisse helfen dabei, begründete Entscheidungen für Maßnahmen zur Erhöhung der Ausfallsicherheit des Krankenhauses zu treffen. Um die Anforderungen an die IT-Sicherheit in Krankenhäusern, die der *BSI-Kritisverordnung* unterliegen, zu konkretisieren, wurde im Branchenarbeitskreis „Medizinische Versorgung" des UP KRITIS ein branchenspezifischer Sicherheitsstandard erarbeitet und inzwischen in zertifizierter Form vorgelegt (DKG 2019; → Kapitel 2.2.1 und Infobox 16).

Die Sicherstellung der stationären Krankenhausversorgung fällt in den Zuständigkeitsbereich der Länder. Die nach Landesrecht zuständigen Behörden haben nach dem *Zivilschutz- und Katastrophenhilfegesetz* ergänzende Maßnahmen zur gesundheitlichen Versorgung der Bevölkerung im Verteidigungsfall zu planen. Das betrifft auch die Krankenhausalarm- und -einsatzplanung (KAEP), die unter Zivilschutzaspekten bundesweit

möglichst einheitlich aufgebaut sein sollte (→ Kapitel 2.3.2). Aus diesem Grund plant das BBK, 2020 ein Handbuch zur KAEP zu veröffentlichen. Zur Erstellung des Handbuchs wird das in Deutschland an verschiedenen Stellen vorhandene Fachwissen in einer Arbeitsgruppe gebündelt, in der führende Experten für KAEP u. a. von der Deutschen Arbeitsgemeinschaft Krankenhaus-Einsatzplanung e. V. (DAKEP) und der Deutschen Gesellschaft für Unfallchirurgie (DGU) sowie aus den Ländern beteiligt sind. Das mit Beteiligung dieser Arbeitsgruppe entstehende Handbuch greift methodische Aspekte der beiden vorgenannten Veröffentlichungen auf und ergänzt sie zu einer umfassenden Handreichung. Ziel ist es, Krankenhausbetreiber in die Lage zu versetzen, in eigener Zuständigkeit und bezogen auf ihre jeweilige Einrichtung strukturiert und systematisch eine KAEP zu erarbeiten, um die Kapazität und Funktionalität der Krankenhäuser in Schadenslagen aufrechtzuerhalten. Auf diesem Weg sollen auch bei Eintritt eines größeren Schadensfalls reibungslose Abläufe sowohl innerhalb der Krankenhäuser als auch in der Zusammenarbeit mit beteiligten Behörden und Organisationen der Gefahrenabwehr ermöglicht werden. Das Handbuch wird in einer Schriftenreihe des BBK erscheinen und kostenlos bereitgestellt.

Abbildung 27: IT unterstützt in Krankenhäusern u. a. im Bereich bildgebender Verfahren (Quelle: Tom Werner / DigitalVision / Getty Images).

2.5.5 Resilientes Verkehrssystem: Beitrag des BMVI-Expertennetzwerks „Wissen – Können – Handeln“

Das Bundesministerium für Verkehr und digitale Infrastruktur (BMVI) bündelt im BMVI-Expertennetzwerk die Kompetenzen und das Know-how von sieben Ressortforschungseinrichtungen und Fachbehörden (vgl. Abbildung 28). Ziel ist es, durch verkehrsträgerübergreifende Forschung einen Beitrag zu leisten, um das Verkehrssystem gleichzeitig umweltgerecht und resilient gegenüber Extremereignissen zu gestalten. Der Umgang mit Extremereignissen wird im BMVI-Expertennetzwerk interdisziplinär, intermodal und hinsichtlich verschiedener Phasen des Risiko- und Krisenmanagements (Vorbereitung, Schutz, Reaktion etc.) thematisiert.

Die Arbeit des BMVI-Expertennetzwerks ist an mehreren Themenfeldern orientiert, von denen das Themenfeld 1, „Verkehr und Infrastruktur an Klimawandel und extreme Wetterereignisse anpassen“, und das Themenfeld 3, „Verlässlichkeit der Verkehrsinfrastrukturen erhöhen“, einen besonders engen Bezug zu den Zielen des Schutzes Kritischer Infrastrukturen aufweisen. In Projekten aus Themenfeld 1 werden z.B. die Auswirkungen klimatisch bedingter Extremereignisse (Hoch- und Niedrigwasser, Sturm, Hangrutschung, Hitze etc.) auf die unterschiedlichen Verkehrsträger analysiert und in die nahe und ferne Zukunft projiziert. Darauf aufbauend entwickeln die Wissenschaftlerinnen und Wissenschaftler des BMVI-Expertennetzwerks exemplarisch Anpassungsoptionen für Straße, Wasserstraße und Schiene (→ Infobox 8). Im Themenfeld 3 geht es u.a. um die Entwicklung von Methoden zur quantitativen Abschätzung der Auswirkungen von Extremereignissen auf Elemente der Verkehrsinfrastruktur, etwa Tunnel, Brücken oder Schleusen. Weitere Informationen sind der Internetseite des Expertennetzwerks zu entnehmen (www.bmvi-expertennetzwerk.de).

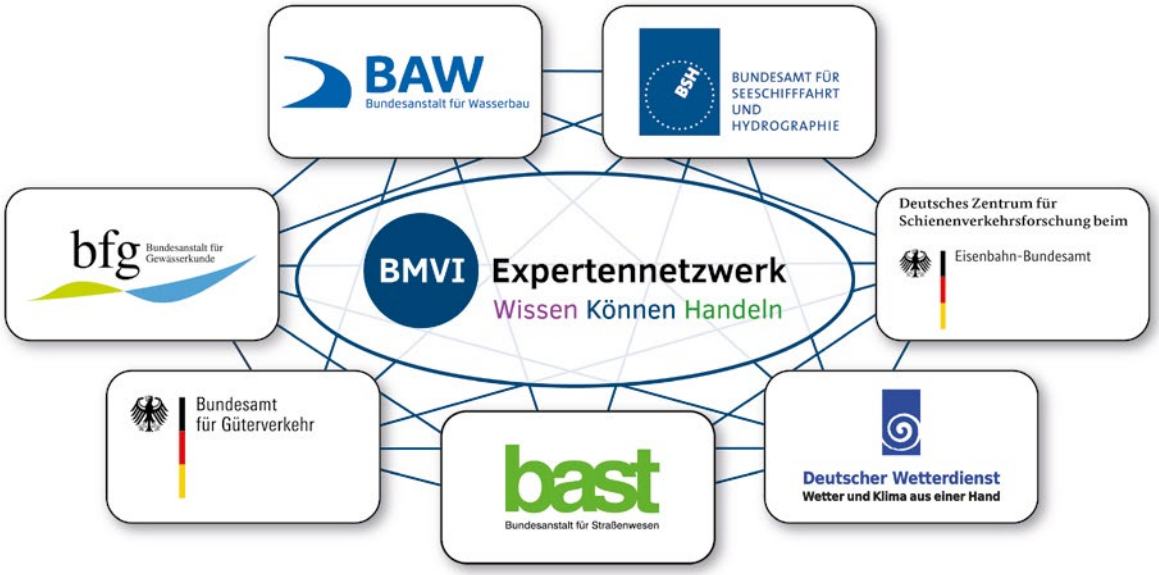


Abbildung 28: Übersicht über die im BMVI-Expertennetzwerk zusammenarbeitenden Ressortforschungseinrichtungen und Fachbehörden (Quelle: BMVI).

2.6

Kapitel

Quelle: Fabian Wentzel / E+ / Getty Images

Grenzüberschreitende Zusammenarbeit beim Schutz Kritischer Infrastrukturen

Weder Gefahren noch Infrastruktureinrichtungen halten sich strikt an nationale Grenzen. Zudem überschreiten Dienstleistungen in einer globalisierten Wirtschaft nationale Wirtschaftsräume. Um grenzüberschreitende Dienstleistungen und Güterströme aufrechtzuerhalten, bedarf es gemeinsamer Sicherungssysteme. Insoweit kommt dem Schutz Kritischer Infrastrukturen auch in grenzüberschreitender Hinsicht stetig wachsende Bedeutung zu.

Die Notwendigkeit einer grenzüberschreitenden Kooperation im europäischen Raum spiegelt sich schon in drei der vier vertraglich vereinbarten Grundfreiheiten des Europäischen Binnenmarktes wider: in der Dienstleistungsfreiheit, dem freien Warenverkehr sowie dem freien Kapital- und Zahlungsverkehr als konstitutionelle Grundlage der Europäischen Union. Um die Funktionsfähigkeit z. B. der Transeuropäischen Verkehrs-, Energie- und Telekommunikationsnetze als Teil des europäischen Binnenmarktes sicherzustellen, ist ein gemeinsames Grundverständnis aller Mitgliedstaaten über Infrastruktursicherheit unverzichtbar. Als Antwort auf die Terroranschläge vom 11. September 2001 auf der einen Seite und die Herausforderungen durch die Digitalisierung auf der anderen Seite entwickelte die Kommission sektorenübergreifende Initiativen zum Schutz europäischer bzw. nationaler kritischer Infrastrukturen und beeinflusste auch die nationale Gesetzgebung (→ Kapitel 2.6.1).

Besonderen Stellenwert hat auch die bilaterale Zusammenarbeit, die sich häufig im Rahmen gegenseitiger Verträge, Abkommen oder Absichtserklärungen vollzieht und in Arbeitsprogrammen konkretisiert wird. Umfang und Intensität der Zusammenarbeit variieren und reichen je nach Vereinbarung von einem Informations- und Erfahrungsaustausch über einzelne konkrete Projekte bis zu mehrjährigen Schulungs- und Ausbildungsprogrammen. In der 2008 begründeten Kooperation im „D-A-CH-Format“ tauschen sich Teilnehmende aus Deutschland, Österreich und der Schweiz zu programmatischen Überlegungen, methodischen Vorgehensweisen und konkreten Umsetzungsmaßnahmen aus und diskutieren über Unterschiede und Gemeinsamkeiten beim Schutz Kritischer Infrastrukturen (→ Kapitel 2.6.2).

Nicht zuletzt ist die Zusammenarbeit in internationalen Organisationen ein wichtiger Baustein, um den Schutz Kritischer Infrastrukturen auch auf nationaler Ebene zu stärken (→ Kapitel 2.6.3). Deutschland ist Mitglied internationaler Organisationen, wie der North Atlantic Treaty Organisation (NATO) sowie der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD), und beteiligt sich auch in diesem Rahmen an der Weiterentwicklung des Schutzes Kritischer Infrastrukturen.

2.6.1 Schutz Kritischer Infrastrukturen in der Europäischen Union

Zwei Meilensteine haben die Zusammenarbeit zum Schutz Kritischer Infrastrukturen auf europäischer Ebene geprägt und auch die nationale Gesetzgebung nachhaltig beeinflusst (→ Kapitel 2.2.1): das „Europäische Programm für den Schutz kritischer Infrastrukturen“ (EPSKI) und die *Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union zur Sicherheit von Netz- und Informationssystemen*, die sogenannte „NIS-Richtlinie“ (RL 2016/11487/EU).

Mit der Veröffentlichung einer Mitteilung der Kommission zum „Schutz kritischer Infrastrukturen im Rahmen der Terrorismusbekämpfung“ (KOM 2004) begann im Jahr 2004 ein intensiver Konsultationsprozess. Dieser setzte sich in einem 2005 vorgelegten „Grünbuch über ein Europäisches Programm für den Schutz kritischer Infrastrukturen“ (KOM 2005) fort und mündete 2006 in eine „Mitteilung der Kommission über ein Europäisches Programm für den Schutz kritischer Infrastrukturen“ (KOM 2006). Als Teil dieses Programms wurde 2008 die *Richtlinie des Rates über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern* verabschiedet, die sogenannte „EPSKI-Richtlinie“ (RL 2008/114/EG).

Die Richtlinie zielt auf die Ermittlung und Ausweisung europäisch kritischer Infrastrukturen (EKI), deren Beeinträchtigung erhebliche Auswirkungen in mindestens zwei Mitgliedstaaten hätte.

Sie bezieht sich nicht auf alle von der Kommission adressierten KRITIS-Sektoren, sondern beschränkt sich auf den Energie- und Verkehrssektor. Die Richtlinie war bis Anfang 2011 in nationales Recht umzusetzen, wobei die Mitgliedstaaten unterschiedlich vorgingen: Während teilweise eigene Umsetzungsgesetze verabschiedet wurden, wählte Deutschland einen ausschließlich fachgesetzlichen Weg durch die Änderung des *Energiewirtschaftsgesetzes* (→ Infobox 5). Gemäß der Richtlinie müssen die Mitgliedstaaten anhand sektorübergreifender und sektorspezifischer Kriterien potenzielle EKI ermitteln und einen Informations- und Konsultationsprozess mit den potenziell von deren Ausfall betroffenen Mitgliedstaaten führen. Betreiber einer EKI müssen Sicherheitspläne aufstellen und einen Sicherheitsbeauftragten benennen. Über den Stand der Umsetzung sowie die Ergebnisse sektorenspezifischer Risiko- und Bedrohungsanalysen haben die Mitgliedstaaten der Kommission regelmäßig zu berichten.

Die Richtlinie ist die einzige verbindliche Maßnahme des EPSKI. Die Kommunikation und der Erfahrungsaustausch auf europäischer Ebene wurden letztlich aber durch dessen nicht verbindliche Elemente beflügelt, etwa regelmäßige Treffen von nationalen Kontaktstellen, die zugleich als Ansprechpartner der Kommission und der anderen Mitgliedstaaten fungieren, die Einrichtung der Informationsplattform „Critical Infrastructure Warning Information Network“ (CIWIN) oder das Forschungsprogramm „Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks“ (CIPS).

Innerhalb Deutschlands führte die EPSKI-Richtlinie durchaus zu Irritationen oder löste doch zumindest Diskussionen aus. Der Bezug der Richtlinie auf *europäisch* kritische Infrastrukturen erschien nicht kongruent mit dem Begriffsverständnis auf nationaler Ebene. Zudem führte die Beschränkung der Richtlinie auf nur zwei Sektoren zu Erklärungsbedarf hinsichtlich des Spektrums der auf nationaler Ebene betrachteten Sektoren (→ Infobox 2). Zum Teil wurde auch die Identifizierung nationaler Kritischer Infrastrukturen mit Hinweis auf die Umsetzung der Richtlinie als „erledigt“ erachtet. Nichtsdestotrotz konnten über die Umsetzung der Richtlinie rechtliche Regelungen explizit zum Schutz Kritischer Infrastrukturen verabschiedet bzw. in anderen Mitgliedstaaten das Thema insgesamt strategisch und rechtlich aufbereitet werden.

Die 2016 erlassene NIS-Richtlinie (RL 2016/11487/EU) wählte einen anderen Zugang zum Schutz Kritischer Infrastrukturen auf europäischer Ebene: Gestützt auf die Regelungskompetenz der Europäischen Union zum Binnenmarkt adressierte sie explizit *nationale* Kritische Infrastrukturen und enthielt Maßgaben zu deren Schutz gegenüber IT- und Cyber-Gefahren. Damit wurde ein einheitlicher Rechtsrahmen für den EU-weiten Aufbau nationaler Kapazitäten für die Cyber-Sicherheit, eine stärkere Zusammenarbeit der Mitgliedstaaten untereinander sowie Mindestsicherheitsanforderungen an und Meldepflichten für Betreiber Kritischer Infrastrukturen sowie bestimmte Anbieter digitaler Dienste wie Cloud-Services und Online-Marktplätze geschaffen.

Die Richtlinie musste von den Mitgliedstaaten bis Mai 2018 umgesetzt werden. Deutschland war insoweit vorbereitet, als bereits am 25. Juli 2015 das *IT-Sicherheitsgesetz* verabschiedet worden war (→ Kapitel 2.2.1). Es enthielt bereits viele auch von der Richtlinie vorgesehene Maßnahmen und wurde mit der *BSI-Kritisverordnung* um ein Instrument zur rechtsverbindlichen Identifizierung Kritischer Infrastrukturen ergänzt (→ Infobox 16). Nicht erfasste Regelungsbestände der NIS-Richtlinie, insbesondere zu digitalen Diensten, wurden 2017 durch das *Gesetz zur Umsetzung der europäischen Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit* umgesetzt.

Nicht als Gestaltungelement der NIS-Richtlinie, wohl aber als Baustein des Politikfelds IT-Sicherheit wurde bereits 2013 die sogenannte „NIS-Plattform“ ins Leben gerufen (ENISA o.A.). In diesem Forum tauschen sich Akteure des öffentlichen und des privaten Sektors auf europäischer Ebene zu Themen der Netz- und Informationssicherheit aus, u. a. zu Anreizen für ein angemessenes Risikomanagement, zur Einführung von Sicherheitsnormen (Mindeststandards) oder zu freiwilligen, EU-weiten Zertifizierungsregelungen. Eingerahmt wird das Politikfeld in der EU durch die 2013 von der Kommission vorgelegte „Cybersicherheitsstrategie der Europäischen Union“ (KOM 2013).

2.6.2 Blick zu den Nachbarn: Trilaterale Zusammenarbeit mit Österreich und der Schweiz (D-A-CH)

Seit Mitte 2008 finden im zwei- bis dreijährigen Abstand gemeinsame Arbeitstreffen zum Thema Schutz Kritischer Infrastrukturen zwischen Behörden aus Deutschland, Österreich und der Schweiz statt. Dieser Blick zu den Nachbarn, die sich nicht nur in sprachlicher Hinsicht verbunden fühlen, sondern auch in der föderalen Struktur Gemeinsamkeiten aufweisen, hat sich immer mehr als lohnend erwiesen.

Ziel der Zusammenarbeit war und ist es, Unterschiede und Gemeinsamkeiten beim Schutz Kritischer Infrastrukturen speziell in den föderalen Systemen auszuloten, Methoden und Projekte vorzustellen und sich über Beispiele guter Praxis, aber auch über Herausforderungen auszutauschen und auf diese Weise voneinander zu lernen. Grundsätzlich kommen Vertreterinnen und Vertreter der koordinierenden Stellen zusammen, für Deutschland insbesondere aus dem BMI, dem BBK und dem BSI. Für Österreich nehmen das Bundesministerium für Inneres, das Bundeskanzleramt und das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung teil, für die Schweiz das Bundesamt für Bevölkerungsschutz. Es sind aber weitere fachlich betroffene Ämter und Ministerien willkommen und haben die Runde themenspezifisch erweitert.

Inzwischen haben vier jeweils zweitägige Arbeitstreffen stattgefunden. Das erste Treffen diente insbesondere der Standortbestimmung und der Vorstellung aktueller Arbeitsstände. Auf der Tagesordnung der nachfolgenden Treffen standen u. a. die nationalen Programme, Vorgehensweisen bei der Identifizierung Kritischer Infrastrukturen sowie die Themen Risikoanalyse, Krisenkommunikation und Resilienzindikatoren. Die Treffen hatten von Anfang einen Werkstattcharakter: Es werden schwerpunktmäßig aktuelle Projekte vorgestellt und methodische Ansätze der einzelnen Staaten miteinander verglichen und hinsichtlich ihrer Übertragbarkeit diskutiert. Besonders interessante Diskussionen ergab die Frage, ob sich der Schutz Kritischer Infrastrukturen in Deutschland und Österreich aufgrund der zwingenden Umsetzung von EU-Recht anders entwickelt als in der Schweiz – was letztlich nicht der Fall ist. Die Ergebnisse der letzten beiden Treffen wurden mit Unterstützung des Center for Security Studies der Eidgenössischen Technischen Hochschule Zürich ausführlich dokumentiert (Herzog/Roth 2014; Maduz/Roth 2018).

2.6.3 Schutz Kritischer Infrastrukturen in internationalen Organisationen

Die Zusammenarbeit in internationalen Organisationen ist ein wichtiger Baustein, um den Schutz Kritischer Infrastrukturen auch auf nationaler Ebene zu stärken. Deutschland ist Mitglied internationaler Organisationen wie der North Atlantic Treaty Organization (NATO) und der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD). Auch in diesem Rahmen beteiligt sich Deutschland an der Weiterentwicklung des Schutzes Kritischer Infrastrukturen – wobei im Sprachgebrauch von NATO und OECD von der „Resilienz“ Kritischer Infrastrukturen die Rede ist.

In der NATO stand der Schutz Kritischer Infrastrukturen frühzeitig auf der Agenda und fand seinen Niederschlag beispielsweise bereits 2001 in der Einrichtung einer „Ad hoc Working Group on Critical Infrastructure Protection“. Auch wurden im Rahmen des seit den 1990er-Jahren bestehenden Programms „Partnerschaft für den Frieden“ (NATO 2017), einer Zusammenarbeit zwischen NATO- und Nicht-NATO-Staaten, Erfahrungen zum Schutz Kritischer Infrastrukturen ausgetauscht und Best-Practice-Beispiele geteilt. Verbindlicheren Charakter erhielt das Thema allerdings durch die Beschlüsse des NATO-Gipfels in Wales 2014 (NATO 2014), die sich unter dem Eindruck des Konflikts in der Ukraine auch auf die zivile Notfallplanung und den Zivilschutz bezogen.

Die im Jahr 2016 verabschiedeten Resilienz-Richtlinien der NATO definieren sieben Grundanforderungen zur Bereitstellung kritischer Dienstleistungen, die „Baseline Requirements“ (NATO 2016). Diese müssen von den Mitgliedsstaaten der NATO zur Gewährleistung ihrer Aufgaben jederzeit zur Verfügung gestellt werden – z. B. im Zusam-

menhang mit dem „Host Nation Support“, der Unterstützung von alliierten oder befreundeten Streitkräften im eigenen Land. Die Grundanforderungen definieren zudem Leitlinien und Kriterien, anhand derer die Mitgliedsstaaten ihre Maßnahmen zur Vorbereitung bewerten können.

Die NATO formuliert Grundanforderungen hinsichtlich

- einer gesicherten Kontinuität der Regierung und kritischer staatlicher Dienstleistungen,
- einer resilienten Stromversorgung,
- der Fähigkeit zum Umgang mit der unkontrollierten Bewegung großer Menschenmengen,
- resilienten Nahrungs- und Wasserressourcen,
- der Fähigkeit zum Umgang mit einem Massenanfall von Verletzten,
- resilienten zivile Kommunikationssystemen und
- resilienten zivile Verkehrssystemen.

(NATO 2016; NATO 2018; Übersetzung: BBK)

Die von der NATO formulierten Grundanforderungen beziehen sich demnach ganz explizit auf sieben der insgesamt neun in Deutschland betrachteten KRITIS-Sektoren (→ Infobox 2). Sie setzen dadurch Impulse für den Schutz Kritischer Infrastrukturen auf nationaler Ebene und die Notfallvorsorge im Rahmen der Zivilen Verteidigung (→ Kapitel 2.3.2). Experten aus den NATO-Mitgliedsstaaten haben in themenbezogenen Arbeitsgruppen (z. B. in der „Joint Health Agriculture and Food Group“) die in den Grundanforderungen formulierten Bedarfe an die Mitgliedsstaaten konkretisiert.

Die OECD bringt regelmäßig Vertreterinnen und Vertreter aus den zuständigen Fachbehörden ihrer Mitgliedsstaaten im „High Level Risk Forum“ zusammen. Aus dieser Zusammenarbeit ist ein 2019 veröffentlichtes „Policy Toolkit“ hervorgegangen, eine Zusammenstellung von Empfehlungen und Politikinstrumenten mit dem Titel „Good Governance for Critical Infrastructure Resilience“ (OECD 2019) – frei übersetzt: Gutes Regierungs- und Verwaltungshandeln für die Resilienz Kritischer Infrastrukturen. Das Policy Toolkit erläutert, wie die Resilienz Kritischer Infrastrukturen in einer dynamischen Risikolandschaft erhöht werden kann, und stellt sieben Schritte vor, die zur Stärkung der Resilienz Kritischer Infrastrukturen auf nationaler Ebene beitragen können. Dazu gehören so unterschiedliche Aspekte wie die Etablierung einer sektorübergreifenden Herangehensweise, der Aufbau einer Vertrauensbasis zwischen Behörden und Betreibern oder die Berücksichtigung grenzüberschreitender Herausforderungen. Viele dieser Schritte wurden in Deutschland beim Schutz Kritischer Infrastrukturen schon umgesetzt oder initiiert – das heißt allerdings nicht, dass es nicht noch einiges von anderen zu lernen gäbe. Daher bietet die OECD eine Plattform für den Austausch zwischen den Mitgliedsstaaten, bei der Best-Practice-Beispiele aus verschiedenen Staaten besonders im Fokus stehen. Möglichst viele sollen von den Erfahrungen der anderen Mitgliedsstaaten profitieren und anderswo bereits erprobte Konzepte auf die Situation „zu Hause“ anpassen können.

3

Kapitel

Quelle: Yuji Kotani / DigitalVision / Getty Images

Ausblick

Die in Kapitel 2 zusammengefassten Einblicke in die Umsetzung der KRITIS-Strategie belegen, dass der Schutz Kritischer Infrastrukturen seit dem Jahr 2009 einen großen Schritt vorangekommen ist. Wie wird es von hier aus weitergehen? Was wird den Schutz Kritischer Infrastrukturen in den nächsten fünf bis zehn Jahren maßgeblich prägen? Es lassen sich bereits einige Themenfelder ausmachen, die in der nahen Zukunft eine große Rolle spielen werden. Eines ist klar: Die Welt ist im Wandel und mit ihr der Schutz Kritischer Infrastrukturen!

Globale Trends bringen Chancen – und Risiken.

Mit dem zunehmenden Einsatz von Informationstechnik im Zuge der Digitalisierung sowie von innovativen Technologien wie z. B. der Künstlichen Intelligenz werden enorme Erwartungen verknüpft: von der Alltagserleichterung über wissenschaftlichen Fortschritt und Effizienzsteigerungen in vielen Wirtschaftsbereichen bis hin zur Schonung natürlicher Ressourcen. Die damit allerdings auch zu erwartenden neuen Abhängigkeiten zwischen Infrastruktursystemen und Verwundbarkeiten der Versorgung mit kritischen Dienstleistungen im Blick zu behalten, wird eine immer wichtigere Aufgabe des Schutzes Kritischer Infrastrukturen. Es gilt, die wünschenswerten Aspekte des technischen Fortschritts zu nutzen und zugleich potenzielle Risiken zu erkennen und zu minimieren.

Zu den globalen Entwicklungen, die schon jetzt und in Zukunft umso mehr die Aufmerksamkeit aller in den Schutz Kritischer Infrastrukturen eingebundenen Akteure erfordert, gehört auch der Klimawandel. Dieser wird voraussichtlich nicht nur hierzulande Anpassungsmaßnahmen erforderlich machen, sondern eine weit vernetzte „Infrastrukturwelt“ auch auf globaler Ebene herausfordern. Zudem bleiben Veränderungen des internationalen Sicherheitsumfelds nicht ohne Folgen für den Schutz Kritischer Infrastrukturen: Gefahren aus dem Cyber-Raum und hybride Bedrohungen haben in den letzten Jahren deutlich an Bedeutung gewonnen und es weist nichts darauf hin, dass sich daran bald etwas ändert.

In Bezug auf die hier genannten (und möglicherweise noch hinzutretenden) Entwicklungen gilt: Die Fähigkeiten, Veränderungen früh zu erfassen, Prognosen abzuleiten und „Frühwarnungen“ hinsichtlich dynamischer Risiken für die Versorgung mit kritischen Dienstleistungen auszusprechen, müssen sukzessive ausgebaut werden.

Die Resilienz von Systemen rückt zunehmend in Fokus.

Mit der Resilienz Kritischer Infrastrukturen tritt die Fähigkeit, unterschiedlichen Gefahren zu widerstehen bzw. flexibel darauf zu reagieren in den Vordergrund. Das gilt sowohl für einzelne Anlagen oder Einrichtungen als auch für ganze Infrastruktursysteme und die darin ablaufenden Prozesse. Insbesondere im Zusammenhang mit den bereits beschriebenen technologischen Entwicklungen und der allgegenwärtigen Digitalisierung ist von einer weiteren Zunahme der Abhängigkeitsbeziehungen zwischen Kritischen Infrastrukturen auszugehen. Die Bereitstellung einer kritischen Dienstleistung beruht auf immer mehr ineinandergreifenden Prozessbausteinen und Infrastrukturkomponenten. Aufgrund dieser Entwicklungen wird der Schutz Kritischer Infrastrukturen im Interesse einer zuverlässigen Bereitstellung kritischer Dienstleistungen verstärkt die Resilienz von Infrastruktursystemen in den Blick nehmen.

Mit einer stärkeren Systembetrachtung stellen sich auch erneut Fragen danach, welche Dienstleistungen und Infrastrukturen als kritisch zu bewerten sind. So haben z. B. satellitengestützte Dienste in mehreren Branchen Kritischer Infrastrukturen kontinuierlich an Bedeutung gewonnen. Die im Jahr 2011 verabschiedete Sektoren- und Brancheneinteilung steht daher auf dem Prüfstand und ist bedarfsgerecht fortzuschreiben. In die darüber zu führenden Diskussionen werden zunehmend Erkenntnisse einfließen, die auf Ebene von Ländern und Kommunen gewonnen werden.

Die horizontale und vertikale Vernetzung staatlicher Akteure wird weiter ausgebaut.

Für den Schutz Kritischer Infrastrukturen ist die Zusammenarbeit von Akteuren aller Verwaltungsebenen und mit fachlicher Zuständigkeit für unterschiedliche Sektoren von essentieller Bedeutung. Es besteht noch großes Potential, im Rahmen der behördlichen Zusammenarbeit rechtsgebietsübergreifend zu planen und zu entscheiden und auf diese Weise ein gemeinsames Verständnis vom Schutz Kritischer Infrastruktur als Querschnittsaufgabe zu entwickeln.

Kritische Infrastrukturanlagen befinden sich „physisch" in Kommunen und unterliegen vielfach der kommunalen Aufsicht. Gleichzeitig aber erstrecken sich Infrastruktursysteme über administrative Grenzen und die Bereitstellung kritischer Dienstleistungen ist von einem ebenenübergreifenden Geflecht fachgesetzlicher Regelungen durchzogen. Neben der horizontalen Kooperation ist daher auch die vertikale Zusammenarbeit zwischen Behörden von Bund, Ländern und Kommunen essentiell. Nur im Zusammenwirken können Behörden auf allen Ebenen die Rahmenbedingungen für eine resiliente Bereitstellung kritischer Dienstleistungen gestalten.

Wesentliche Impulse für die Weiterentwicklung der strategischen Grundlagen beim Schutz Kritischer Infrastrukturen gehen derzeit von der Arbeitsgruppe der Koordinierungsstellen für den Schutz Kritischer Infrastrukturen in Bund und Ländern aus. Diese wird ihre Arbeit zukünftig mit einer stärkeren Anbindung an die Gremienstruktur der Innenressorts fortsetzen und hat sich zum Ziel gesetzt, eine gemeinsame Bund-Länder-Strategie zum Schutz Kritischer Infrastrukturen zu erarbeiten. Es zeichnet sich demnach ab, dass die bundesseitige KRITIS-Strategie demnächst durch eine gesamtstaatliche strategische Grundlage abgelöst werden könnte. Deren Erarbeitung und ebenen- sowie ressortübergreifende Abstimmung bildet dementsprechend einen wichtigen Arbeitsschwerpunkt in den kommenden Jahren.

Integriertes Risiko- und Krisenmanagement: Die Zusammenarbeit staatlicher und nichtstaatlicher Akteure bleibt zentraler Auftrag.

Darüber hinaus wird die Zusammenarbeit zwischen staatlichen und nichtstaatlichen Akteuren – bereits heute ein Kernaspekt des Schutzes Kritischer Infrastrukturen – in Zukunft weiter an Bedeutung gewinnen. Nur ein systematischer Austausch von Informationen und Erkenntnissen wird alle Beteiligten in die Lage versetzen, bestmöglich zur Stärkung der Resilienz Kritischer Infrastrukturen beitragen zu können. Auch die im Zuge des *IT-Sicherheitsgesetzes* gewählte Form der kooperativen Rechtsetzung hat sich in der Zusammenarbeit von Staat und Wirtschaft bewährt und soll, wo sinnvoll, fortgeführt werden.

Viele der in Kapitel 2 beschriebenen Aktivitäten lassen sich unter dem Begriff „Integriertes Risiko- und Krisenmanagement" subsumieren. Ganz im Sinne des kooperativen Ansatzes gehören dazu sowohl Maßnahmen, die seitens des Staates umgesetzt werden, als auch Maßnahmen der Betreiber Kritischer Infrastrukturen. Die Erfahrungen der vergangenen Jahre haben gezeigt, wie wichtig es ist, dass Betreiber und staatliche Akteure in allen Phasen zwischen Prävention und Reaktion im Risiko- und Krisenmanagementprozess zusammenwirken. Die Weiterentwicklung dieses integrierten Ansatzes und seine Anwendung auf allen Ebenen sind Aufgaben für die nächste Dekade.

Kooperieren heißt auch kommunizieren (können) – daher wird es in den nächsten Jahren ganz praktisch darum gehen, die Kommunikation insbesondere zwischen Sicherheitsbehörden und dem Bevölkerungsschutz sowie Betreibern Kritischer Infrastrukturen auszubauen. Dabei wird einerseits die Gewährleistung der technischen Kommunikationsmöglichkeit eine Rolle spielen, andererseits die Abstimmung von Abläufen und die Klärung von Differenzen in der Sprachkultur unterschiedlicher Akteure.

Wesentliche Instrumente zur Strukturierung der Zusammenarbeit und Verstetigung eines vertrauensvollen Austauschs zwischen unterschiedlichen Akteuren sind Kooperationsformate, wie Gesprächsplattformen und Runde Tische.

Als zentrale Plattform zur Zusammenarbeit von Bundesinstitutionen und Betreibern Kritischer Infrastrukturen hat sich der UP KRITIS etabliert, es werden allerdings auf allen Ebenen mehr und mehr Kooperationsformate eingerichtet. Diese und die neu hinzukommenden gilt zu stärken und weiter auszubauen. Als Impulsgeber dazu kann in den kommenden Jahren auch das Sendai Rahmenwerk für Katastrophenvorsorge wirken – sowohl auf nationaler Ebene als auch darüber hinaus.

Der Schutz Kritischer Infrastrukturen muss auf internationaler Ebene gestaltet werden.

Die EU wird auch künftig erheblichen Einfluss auf den Schutz Kritischer Infrastrukturen in den Mitgliedstaaten und damit im Staatenverbund insgesamt nehmen. Dies zeichnet sich schon durch Vorschläge für weitere Legislativakte zum Schutz Kritischer Infrastrukturen bzw. zur Netz- und Informationssicherheit ab. Diese Initiativen sind von deutscher Seite aktiv zu begleiten und mitzugestalten. Ergänzend wird sich Deutschland auch in die Zusammenarbeit der Mitgliedstaaten untereinander und mit der EU einbringen, sei es im Zuge der Weiterentwicklung des „Europäischen Programms zum Schutz Kritischer Infrastrukturen“ oder in der Verknüpfung von Themen des Katastrophenschutzes und des Schutzes Kritischer Infrastrukturen. Diese Verknüpfung wird voraussichtlich auch in dem „Wissensnetzwerk“ angelegt sein, das im Rahmen des Katastrophenschutzverfahrens der EU angedacht ist.

Der Schutz Kritischer Infrastrukturen tritt zunehmend auch auf Ebene der Vereinten Nationen, der OECD und der NATO in den Vordergrund. Diese Organisationen formulieren mit unterschiedlich hoher Verbindlichkeit Anforderungen an ihre Partner. Vielfältige Anknüpfungspunkte wird in den kommenden Jahren die in vielen Staaten laufende Umsetzung des „Sendai Rahmenwerks für Katastrophenvorsorge“ der Vereinten Nationen bieten: Die Reduzierung von Ausfällen Kritischer Infrastrukturen ist im Rahmenwerk explizit als Zielsetzung aufgeführt. Die Anforderungen der NATO werden in Deutschland im Rahmen der Konzeption Zivile Verteidigung adressiert, deren Umsetzung sich auch deshalb auf absehbare Zeit in Aktivitäten zum Schutz Kritischer Infrastrukturen in Deutschland niederschlagen wird.

4

Kapitel

Quelle: Philippe Turpin / Getty Images

Verzeichnisse

Abkürzungsverzeichnis

Abs.
Absatz

AG KOST KRITIS
Arbeitsgruppe der Koordinierungsstellen für den Schutz Kritischer Infrastrukturen in Bund und Ländern

AG KRITIS
Arbeitsgruppe Kritische Infrastrukturen

AKNZ
Akademie für Krisenmanagement, Notfallplanung und Zivilschutz

Art.
Artikel

ASG
Arbeitssicherstellungsgesetz

AWV
Außenwirtschaftsverordnung

BaFin
Bundesanstalt für Finanzdienstleistungsaufsicht

BAIT
Bankaufsichtliche Anforderungen an die IT

BAK
Branchenarbeitskreis (im UP KRITIS)

BBK
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

BBR
Bundesamt für Bauwesen und Raumordnung

BBSR
Bundesinstitut für Bau-, Stadt- und Raumforschung

B3S
branchenspezifischer Sicherheitsstandard

BfDI
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit

BKM
Beauftragte der Bundesregierung für Kultur und Medien

BLG
Bundesleistungsgesetz

BMBF
Bundesministerium für Bildung und Forschung

BMI
Bundesministerium des Innern
ab 2018 Bundesministerium des Innern für Bau und Heimat

BMU
Bundesministerium für Umwelt, Naturschutz und nukleare Sicherheit

BMVI
Bundesministerium für Verkehr und digitale Infrastruktur

BMWi
Bundesministerium für Wirtschaft und Energie

BNetzA
Bundesnetzagentur

BSI
Bundesamt für Sicherheit in der Informationstechnik

BSIG
Gesetz über das Bundesamt für Sicherheit in der Informationstechnik

BSI-KritisV
BSI-Kritisverordnung

BT-Drs.
Bundestagsdrucksache

bzw.
beziehungsweise

CIWIN
Critical Infrastructure Warning Information Network

CIPS
Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks

CSS
Cyber-Sicherheitsstrategie für Deutschland

D-A-CH
Deutschland-Österreich-Schweiz

DAKEP
Deutsche Arbeitsgemeinschaft Krankenhaus-Einsatzplanung e. V.

DAS
Deutsche Anpassungsstrategie an den Klimawandel

DGU
Deutsche Gesellschaft für Unfallchirurgie

d. h.
das heißt

DigiNetzG
Gesetz zur Erleichterung des Ausbaus digitaler Hochgeschwindigkeitsnetze

DIN
Deutsches Institut für Normung e. V.

DIN SPEC
DIN-Spezifikation

DL
Dienstleistung

DKG
Deutsche Krankenausgesellschaft e. V.

DVGW
Deutschen Verein des Gas- und Wasserfaches e. V.

DWA
Deutschen Vereinigung für Wasserwirtschaft, Abwasser und Abfall e. V.

EKI
europäisch kritische Infrastruktur(en)

ENISA
European Union Agency for Cybersecurity

EnSiG
Energiesicherungsgesetz

ENTSO-E
European Network of Transmission System Operators for Electricity
(Verband Europäischer Übertragungsnetzbetreiber für Strom)

ENTSO-G
European Network of Transmission System Operators for Gas
(Verband Europäischer Fernleitungsnetzbetreiber für Gas)

EnWG
Energiewirtschaftsgesetz

EPSKI
Europäisches Programm für den Schutz kritischer Infrastrukturen

ErdölBevG
Erdölbevorratungsgesetz

ESVG
Ernährungssicherstellungs- und -vorsorgegesetz

etc.
et cetera

EU
Europäische Union

FNN
Forum Netztechnik/Netzbetrieb im VDE

GG
Grundgesetz

ggf.
gegebenenfalls

GGO
Gemeinsame Geschäftsordnung der Bundesministerien

IMK
Ständige Konferenz der Innenminister und -senatoren der Länder (Innenministerkonferenz)

ISO
International Organization for Standardization

IT/IT-
Informationstechnik/informationstechnisch

IT-SiG
IT-Sicherheitsgesetz

KAIT
Kapitalverwaltungsaufsichtliche Anforderungen an die IT

KAEP
Krankenhausalarm- und -einsatzplanung

km
Kilometer

KNK
Konferenz Nationaler Kultureinrichtungen

KomPass
Kompetenzzentrum Klimafolgen und Anpassung im UBA

KRITIS
Kritische Infrastruktur(en)

KRITIS-Betreiber
Betreiber Kritischer Infrastrukturen

KRITIS-Sektoren
Sektoren Kritischer Infrastrukturen

KRITIS-Strategie
Nationale Strategie zum Schutz Kritischer Infrastrukturen

kVA
Kilo Volt-Ampere

KZV
Konzeption Zivile Verteidigung

LÜKEX
Länder- und Ressortübergreifende Krisenmanagementübung (Exercise)

MaRisk
Mindestanforderungen an das Risikomanagement (im Kredit- und Finanzdienstleistungswesen)

MORO
Modellvorhaben der Raumordnung

NATO
North Atlantic Treaty Organization

NKS
Nationale Kontaktstelle für das Sendai Rahmenwerk für Katastrophenvorsorge

NPSI
Nationaler Plan zum Schutz der Informationsinfrastrukturen

Nr.
Nummer

OECD
Organisation for Economic Cooperation and Development
(Organisation für wirtschaftliche Zusammenarbeit und Entwicklung)

o. g.
oben genannt

PG KRITIS
Projektgruppe Kritische Infrastrukturen

PTSG
Post- und Telekommunikationssicherstellungsgesetz

RL
Richtlinie

S.
Seite

Schutz KRITIS
Schutz Kritischer Infrastrukturen

SiFo
Sicherheitsforschungsprogramm

SiLK
SicherheitsLeitfaden Kulturgut

TAB
Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag

TAK
Themenarbeitskreis (im UP KRITIS)

THW
Bundesanstalt Technisches Hilfswerk

THWG
THW-Gesetz

TKG
Telekommunikationsgesetz

vgl.
vergleiche

u. a.
unter anderem

UBA
Umweltbundesamt

UKB
Unfallkrankenhaus Berlin

UNESCO
United Nations Educational, Scientific and Cultural Organization
(Organisation der Vereinten Nationen für Bildung, Wissenschaft und Kultur)

UN ISDR
United Nations International Strategy for Disaster Reduction

UP KRITIS
bis 2014 Umsetzungsplan KRITIS (zum NPSI); seitdem Eigenname ohne Langform

VAIT
Versicherungsaufsichtliche Anforderungen an die IT

VDE
Verband der Elektrotechnik Elektronik Informationstechnik e. V.

VerkLG
Verkehrsleistungsgesetz

VerkSiG
Verkehrssicherstellungsgesetz

WasSiG
Wassersicherstellungsgesetz

WiSiG
Wirtschaftssicherstellungsgesetz

Y2K
Year 2 Kilo (Jahr-2000-Problem)

z. B.
zum Beispiel

ZSKG
Zivilschutz- und Katastrophenhilfegesetz

Quellenverzeichnis

Verzeichnis zitierter Publikationen und Onlinequellen

ARL 2011 - Akademie für Raumforschung und Landesplanung (Hrsg., 2011): Zukünftige Ausgestaltung des Risikomanagements in der Raumplanung. Positionspapier aus der ARL Nr. 86. Hannover.

BaFin 2017 - Bundesanstalt für Finanzdienstleistungsaufsicht (2017): Mindestanforderungen an das Risikomanagement (MaRisk). Rundschreiben 09/2017 (BA) vom 27.10.2017.

BaFin 2018a - Bundesanstalt für Finanzdienstleistungsaufsicht (2018a): Bankaufsichtliche Anforderungen an die IT (BAIT). Rundschreiben 10/2017 (BA) in der Fassung vom 14.09.2018.

BaFin 2018b - Bundesanstalt für Finanzdienstleistungsaufsicht (2018): Kritische Infrastrukturen: BaFin ergänzt BAIT um KRITIS-Modul. Internetmeldung vom 14.09.2018.
Abrufbar unter: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2018/meldung_180914_Ueberarbeitung_BAIT.html (09.12.2019).

BaFin 2019a - Bundesanstalt für Finanzdienstleistungsaufsicht (2019a): Versicherungsaufsichtliche Anforderungen an die IT (VAIT). Rundschreiben 10/2018 (VA) in der Fassung vom 20.03.2019.

BaFin 2019b - Bundesanstalt für Finanzdienstleistungsaufsicht (2019b): Kapitalverwaltungsaufsichtliche Anforderungen an die IT (KAIT). Rundschreiben 11/2019 (WA) in der Fassung vom 01.10.2019.

BBK 2005 - Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2005): Problemstudie Risiken für Deutschland (Teil 1 und 2). Bad Neuenahr-Ahrweiler.

BBK 2008 - Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2008): Schutz Kritischer Infrastruktur: Risikomanagement im Krankenhaus. Leitfaden zur Identifikation und Reduzierung von Ausfallrisiken in Kritischen Infrastrukturen des Gesundheitswesens. Bonn.

BBK 2010 - Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2010): Neue Strategie zum Schutz der Bevölkerung in Deutschland. Bonn.

BBK 2012 - Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2012): Schutzkonzepte Kritischer Infrastrukturen im Bevölkerungsschutz. Ziele, Zielgruppen, Bestandteile und Umsetzung im BBK. Bonn.

BBK 2015a - Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2015a): Notstromversorgung in Unternehmen und Behörden. Leitfaden für die Planung, die Einrichtung und den Betrieb einer Notstromversorgung in Unternehmen und Behörden. Bonn.

BBK 2015b - Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2015b): Was tun bei Stromausfall – Vorsorge und Selbsthilfe. (veröffentlicht am: 01.10.2015)
Abrufbar unter: https://youtu.be/VijPkjKVv9I (01.02.2020)

BBK 2015c - Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2015c): Was tun bei Stromausfall – Strom selbst erzeugen. (veröffentlicht am: 29.10.2015)
Abrufbar unter: https://youtu.be/3XCTa1mkAWc (01.02.2020)

BBK 2017 - Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2017): Treibstoffversorgung bei Stromausfall. Empfehlung für Zivil- und Katastrophenschutzbehörden. Bonn.

BBK 2018a - Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2018a): Bevölkerungsschutz. Ausgabe 3/2018. (Themenheft: Integriertes Risikomanagement).

BBK 2018b - Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2018b): Autarke Notstromversorgung der Bevölkerung. Bonn.

BBK 2019a - Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2019a): Schutz Kritischer Infrastrukturen – Identifizierung in sieben Schritten. Bonn.

BBK 2019b - Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2019b): Auswertungsbericht LÜKEX 18. Gasmangellage in Süddeutschland. Bonn.

BBK 2019c - Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2019c): Stromausfall. Vorsorge und Selbsthilfe. Bonn.

BBK 2019d - Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2019d): Sicherheit der Trinkwasserversorgung. Teil 1: Risikoanalyse. Bonn.

BBK 2019e - Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2019e): Sicherheit der Trinkwasserversorgung. Teil 2: Notfallvorsorgeplanung. Bonn.

BBK 2019f - Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2019f): BBK-Glossar. Ausgewählte zentrale Begriffe des Bevölkerungsschutzes. Bonn.

BBK/BSI 2011 - Bundesamt für Bevölkerungsschutz und Katastrophenhilfe; Bundesamt für Sicherheit in der Informationstechnik (2011): Sektoren und Branchen Kritischer Infrastrukturen (Internetmeldung, Stand: 13.5.2011)
Abrufbar unter: https://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/Sektoren/SektorenBBK.html (01.02.2020)

BMBF 2007 - Bundesministerium für Bildung und Forschung (2007): Forschung für die zivile Sicherheit. Programm der Bundesregierung. Bonn.

BMBF 2015 - Bundesministerium für Bildung und Forschung (2015): Selbstbestimmt und sicher in der digitalen Welt 2015-2020. Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit. Bonn.

BMBF 2018 - Bundesministerium für Bildung und Forschung (2018): Forschung für die zivile Sicherheit 2018–2023. Rahmenprogramm der Bundesregierung. Bonn.

BMI 2005a - Bundesministerium des Innern (2005a): Schutz Kritischer Infrastrukturen – Basisschutzkonzept. Empfehlungen für Unternehmen. Berlin.

BMI 2005b - Bundesministerium des Innern (2005b): Nationaler Plan zum Schutz der Informationsinfrastrukturen (NPSI). Berlin.

BMI 2007a - Bundesministerium des Innern (2007a): Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen. Berlin.

BMI 2007b - Bundesministerium des Innern (2007b): Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement. Leitfaden für Unternehmen und Behörden. Berlin.

BMI 2009 - Bundesministerium des Innern (2009): Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie). Berlin.

BMI 2011a - Bundesministerium des Innern (2011a): Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement. Leitfaden für Unternehmen und Behörden. Berlin.

BMI 2011b - Bundesministerium des Innern (2011b): Cyber-Sicherheitsstrategie für Deutschland. Berlin.

BMI 2016a - Bundesministerium des Innern (2016a): Cyber-Sicherheitsstrategie für Deutschland 2016. Berlin.

BMI 2016b - Bundesministerium des Innern (2016b): Konzeption Zivile Verteidigung. Berlin.

BMI 2017 - Bundesministerium des Innern (2017): Umsetzungsplan Bund 2017. Leitlinie für Informationssicherheit in der Bundesverwaltung. Berlin.

BMVg 2016 - Bundesministerium der Verteidigung (2016): Weißbuch 2016 zur Sicherheitspolitik und zur Zukunft der Bundeswehr. Berlin.

BMVg 2018 - Bundesministerium der Verteidigung (2018): Konzeption der Bundeswehr. Berlin.

BMVI 2014 - Bundesministerium für Verkehr und digitale Infrastruktur (2014): Sicherheitsstrategie für die Güterverkehrs- und Logistikwirtschaft. Schutz kritischer Infrastrukturen und verkehrsträgerübergreifende Gefahrenabwehr. Berlin.

BMVI 2017 - Bundesministerium für Verkehr und digitale Infrastruktur (2017): Handbuch zur Ausgestaltung der Hochwasservorsorge in der Raumordnung. MORO Regionalentwicklung und Hochwasserschutz in Flussgebieten. Berlin.

BMVI/BBSR 2015 - Bundesministerium für Verkehr und digitale Infrastruktur; Bundesinstitut für Bau-, Stadt- und Raumforschung (2015): Endbericht zu Modellvorhaben der Raumordnung (MORO) Vorsorgendes Risikomanagement in der Regionalplanung (AZ 10.05.06-13.6).

BNetzA 2015 - Bundesnetzagentur (2015): IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz. (Stand: August 2015).

BNetzA 2016 - Bundesnetzagentur (2016): Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten nach § 109 Telekommunikationsgesetz (TKG). (Stand: Juli 2016).

BNetzA 2018 - Bundesnetzagentur (2018): IT-Sicherheitskatalog gemäß § 11 Absatz 1b Energiewirtschaftsgesetz. (Stand: Dezember 2018).

BReg 2008 - Bundesregierung (2008): Deutsche Anpassungsstrategie an den Klimawandel vom Bundeskabinett am 17. Dezember 2008 beschlossen. Berlin.

BReg 2015 - Bundesregierung (2015): Fortschrittsbericht zur Deutschen Anpassungsstrategie an den Klimawandel. Stand: 16.11.2015. Berlin.

BSI 2004 - Bundesamt für Sicherheit in der Informationstechnik (2004): Jahresbericht 2003. Bonn.

BSI 2013a - Bundesamt für Sicherheit in der Informationstechnik (2013a): Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT. Leitfaden. Bonn.

BSI 2013b - Bundesamt für Sicherheit in der Informationstechnik (2013): Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT. Management-Kurzfassung. Bonn.

BSI 2017a - Bundesamt für Sicherheit in der Informationstechnik (2017a): Schutz Kritischer Infrastrukturen durch IT-Sicherheitsgesetz und UP KRITIS. Bonn.

BSI 2017b - Bundesamt für Sicherheit in der Informationstechnik (2017b): Merkblatt zum sicheren Informationsaustausch mit TLP 17-11. Bonn.

ENISA o.A. –European Union Agency for Cybersecurity (o.A.): NIS-Platform.
Abrufbar unter: https://resilience.enisa.europa.eu/nis-platform (01.02.2020)

Fekete et al. 2019 - Fekete, A.; Neisser, F.; Tzavella, K.; Hetkämper, C. (2019; Hrsg.): Wege zu einem Mindestversorgungskonzept. Kritische Infrastrukturen und Resilienz, Köln.

Herzog/Roth 2014 - Herzog, M.; Roth, F. (2014): Dritter D-A-CH Workshop Schutz Kritischer Infrastrukturen, 4. – 6. Dezember 2013, Magglingen. Zürich.

IMK 2009 - Ständige Konferenz der Innenminister und -senatoren der Länder (2009): Programm Innere Sicherheit. Fortschreibung 2008/2009. Potsdam.

KNK o.A. - Konferenz Nationaler Kultureinrichtungen (o.A.): SiLK – SicherheitsLeitfaden Kulturgut.
Abrufbar unter: http://www.konferenz-kultur.de/SLF/index1.php (01.02.2020)

KOM 2004 - Kommission der Europäischen Gemeinschaften (2004): Mitteilung der Kommission zum Schutz kritischer Infrastrukturen im Rahmen der Terrorismusbekämpfung. KOM(2004)702. Vom 20.10.2004, Brüssel.

KOM 2005 - Kommission der Europäischen Gemeinschaften (2005): Grünbuch über ein Europäisches Programm für den Schutz kritischer Infrastrukturen. KOM(2005)576. Vom 17.11.2005, Brüssel.

KOM 2006 - Kommission der Europäischen Gemeinschaften (2006): Mitteilung der Kommission über ein Europäisches Programm für den Schutz kritischer Infrastrukturen. KOM(2006)786. Vom 12.12.2006, Brüssel.

KOM 2013 - Europäische Kommission (2013): Gemeinsame Mitteilung an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen. Cybersicherheitsstrategie der Europäischen Union – ein offener, sicherer und geschützter Cyberraum. JOIN01. Vom 02.07.2013, Brüssel.

Lechner et al. 2018 - Lechner, U.; Dännert, S.; Rieb, A.; Rudel, S. (2018, Hrsg.): CASE|KRITIS. Fallstudien zur IT-Sicherheit in Kritischen Infrastrukturen. Berlin.

Maduz/Roth 2018 - Maduz, L.; Roth, F. (2018): Vierter Trilateraler Workshop D-A-CH Schutz kritischer Infrastrukturen", 4.-6. Juni 2018 in Bonn. Zürich.

NATO 2014 - North Atlantic Treaty Organisation (2014): Wales Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales. Pressemitteilung (2014/120) vom 05.09.2014.

NATO 2016 - North Atlantic Treaty Organisation (2016): Commitment to enhance resilience. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw, 8-9 July 2016. Pressemitteilung (2016/118) vom 08.07.2016.

NATO 2017 - North Atlantic Treaty Organisation (2017): Partnership for Peace Programme. (Stand: 07.06.2017) Abrufbar unter: https://www.nato.int/cps/en/natolive/topics_50349.htm (18.11.2019)

NATO 2018 - North Atlantic Treaty Organisation (2018): Resilience and Article 3. (Stand: 03.12.2019) Abrufbar unter: https://www.nato.int/cps/en/natohq/topics_132722.htm (01.02.2020)

NKS 2019 - Nationale Kontaktstelle für das Sendai Rahmenwerk beim Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2019): Sendai Rahmenwerk für Katastrophenvorsorge 2015-2030. Bonn.

OECD 2019 - Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (2019): Good Governance for Critical Infrastructure Resilience, OECD Reviews of Risk Management Policies. Paris.

PCCIP 1997 - President's Commission on Critical Infrastructure Protection (1997): Critical Foundations. Protecting America's Infrastructures. The Report of the President's Commission on Critical Infrastructure Protection. Washington.

Pohl/Zehetmair 2011 - Pohl, J.; Zehetmair, S. (2011, Hrsg.): Risikomanagement als Handlungsfeld in der Raumplanung. Arbeitsmaterial der ARL Nr. 357. Hannover.

Rudel/Lechner 2018 - Rudel, S.; Lechner, U. (2018, Hrsg.): IT-Sicherheit für Kritische Infrastrukturen – State of the Art. Ergebnisse des Förderschwerpunkts IT-Sicherheit für Kritische Infrastrukturen ITS|-KRITIS des BMBF. München.

THW 2014 - Bundesanstalt Technisches Hilfswerk (2014): Katalog der Einsatzoptionen des THW (Stand: November 2014). Bonn.

UP KRITIS 2008a - Geschäftsstelle des UP KRITIS (2008a): Früherkennung und Bewältigung von IT-Krisen, Bonn.

UP KRITIS 2008b - Geschäftsstelle des UP KRITIS (2008b): IT-Notfall- und Krisenübungen in Kritischen Infrastrukturen. Bonn.

UP KRITIS 2014a - Geschäftsstelle des UP KRITIS (2014a): UP KRITIS. Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen. Bonn.

UP KRITIS 2014b - Geschäftsstelle des UP KRITIS (2014b, Fortschreibung): Früherkennung und Bewältigung von IT-Krisen. Bonn.

UP KRITIS 2014c - Geschäftsstelle des UP KRITIS (2014c, Fortschreibung): IT-Notfall- und Krisenübungen in Kritischen Infrastrukturen. Bonn.

Verzeichnis zitierter Rechtsquellen

Aktiengesetz (AktG) vom 6. September 1965 (BGBl. I S. 1089), zuletzt geändert durch Artikel 1 des Gesetzes vom 12. Dezember 2019 (BGBl. I S. 2637).

Arbeitssicherstellungsgesetz (ASG) vom 9. Juli 1968 (BGBl. I S. 787), zuletzt geändert durch Artikel 24 des Gesetzes vom 4. August 2019 (BGBl. I S. 1147).

Außenwirtschaftsverordnung (AWV) vom 2. August 2013 (BGBl. I S. 2865), zuletzt geändert durch Artikel 1 der Verordnung vom 27. Februar 2019 (BAnz AT 06.03.2019 V1).

Bundesleistungsgesetz (BLG) in der im Bundesgesetzblatt Teil III, Gliederungsnummer 54-1, veröffentlichten bereinigten Fassung, zuletzt geändert durch Artikel 5 des Gesetzes vom 11. August 2009 (BGBl. I S. 2723).

Energiesicherungsgesetz (EnSiG) 1975 vom 20. Dezember 1974 (BGBl. I S. 3681), zuletzt geändert durch Artikel 324 der Verordnung vom 31. August 2015 (BGBl. I S. 1474).

Energiewirtschaftsgesetz (EnWG) vom 7. Juli 2005 (BGBl. I S. 1970, 3621), zuletzt geändert durch Artikel 1 des Gesetzes vom13. Mai 2019 (BGBl. I S. 706).

Erdölbevorratungsgesetz (ErdölBevG) vom 16. Januar 2012 (BGBl. I S. 74), zuletzt geändert durch Artikel 127 des Gesetzes vom 29. März 2017 (BGBl. I S. 626).

Ernährungssicherstellungsgesetz (ESG) in der Fassung der Bekanntmachung vom 27. August 1990 (BGBl. I S. 1802), zuletzt geändert durch Artikel 359 der Verordnung vom 31. August 2015 (BGBl. I S. 1474), außer Kraft getreten am 11. April 2017 durch das Gesetz zur Neuregelung des Rechts zur Sicherstellung der Ernährung in einer Versorgungskrise vom 4. April 2017.

Ernährungssicherstellungs- und -vorsorgegesetz (ESVG) vom 4. April 2017 (BGBl. I S. 772).

Ernährungsvorsorgegesetz (EVG) vom 20. August 1990 (BGBl. IS. 1766), zuletzt geändert durch Artikel 362 der Verordnung vom 31. August 2015 (BGBl. I S. 1474), außer Kraft getreten am 11. April 2017 durch das Gesetz zur Neuregelung des Rechts zur Sicherstellung der Ernährung in einer Versorgungskrise vom 4. April 2017.

Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz, BSIG) vom 14. August 2009 (BGBl. I S. 2821), zuletzt geändert durch Artikel 1 des Gesetzes vom 23. Juni 2017 (BGBl. I S. 1885).

Gesetz über das Technische Hilfswerk (THW-Gesetz, THWG) vom 22. Januar 1990 (BGBl. I S. 118), zuletzt geändert durch Artikel 5 des Gesetzes vom 11. Juni 2013 (BGBl. I S. 1514).

Gesetz über den Zivilschutz und die Katastrophenhilfe des Bundes (Zivilschutz- und Katastrophenhilfegesetz, ZSKG) vom 25. März 1997 (BGBl. I S. 726), zuletzt geändert durch Artikel 2 Nummer 1 des Gesetzes vom 29. Juli 2009 (BGBl. I S. 2350).

Gesetz über die Errichtung des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe vom 27. April 2004 (BGBl. I S. 630).

Gesetz zu der Konvention vom 14. Mai 1954 zum Schutz von Kulturgut bei bewaffneten Konflikten vom 11. April 1967 (BGBl. 1967 II S. 1233), zuletzt geändert durch Artikel 3 des Gesetzes vom 31. Juli 2016 (BGBl. I S. 1914).

Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz, IT-SiG) vom 17. Juli 2015 (BGBl. I S. 1324).

Gesetz zur Erleichterung des Ausbaus digitaler Hochgeschwindigkeitsnetze (DigiNetzG) vom 4. November 2016.

Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union vom 23. Juni 2017 (BGBl. I S. 1885).

Grundgesetz für die Bundesrepublik Deutschland (GG) in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, zuletzt geändert durch Artikel 1 des Gesetzes vom 28. März 2019 (BGBl. I S. 404).

Gemeinsame Geschäftsordnung der Bundesministerien (GGO) mit Stand vom 1. September 2011.

Post- und Telekommunikationssicherstellungsgesetz (PTSG) vom 24. März 2011 (BGBl. I S. 506, 941), geändert durch Artikel 7 des Gesetzes vom 4. November 2016 (BGBl. I S. 2473).

Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern (ABl. L 345 vom 23.12. 2008, S. 75).

Richtlinie 2016/1148/EU des europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.07.2016, S. 1).

Raumordnungsgesetz (ROG) vom 22. Dezember 2008 (BGBl. I S. 2986), zuletzt geändert durch Artikel 2 Absatz 15 des Gesetzes vom 20. Juli 2017 (BGBl. I S. 2808).

Telekommunikationsgesetz (TKG) vom 22 Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch Artikel 12 des Gesetzes vom 11. Juli 2019 (BGBl. I S. 1066).

Verkehrsleistungsgesetz (VerkLG) vom 23. Juli 2004 (BGBl. I S. 1865), zuletzt geändert durch Artikel 15 des Gesetzes vom 26. Juli 2016 (BGBl. I S. 1843).

Verkehrssicherstellungsgesetz (VerkSiG) in der Fassung der Bekanntmachung vom 8. Oktober 1968 (BGBl. I S. 1082), zuletzt geändert durch Artikel 499 der Verordnung vom 31. August 2015 (BGBl. I S. 1474).

Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über Aufsichtsanforderungen an Kreditinstitute und Wertpapierfirmen und zur Änderung der Verordnung (EU) Nr. 646/2012 (ABl. L 176 vom 27.06.2013, S. 1).

Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung, BSI-KritisV) vom 22. April 2016 (BGBl. I S. 958), geändert die durch Artikel 1 der Verordnung vom 21. Juni 2017 (BGBl. I S. 1903).

Wassersicherstellungsgesetz (WasSiG) vom 24. August 1965 (BGBl. I S. 1225, 1817), zuletzt geändert durch Artikel 2 Absatz 20 des Gesetzes vom 12. August 2005 (BGBl. I S. 2354).

Wirtschaftssicherstellungsgesetz (WiSiG) in der Fassung der Bekanntmachung vom 3. Oktober 1968 (BGBl. I S. 1069), zuletzt geändert durch Artikel 262 der Verordnung vom 31. August 2015 (BGBl. I S. 1474).

Zwölfte Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes (Störfall-Verordnung, 12. BImSchV) in der Fassung der Bekanntmachung vom 15. März 2017 (BGBl. I S. 483), zuletzt geändert durch Artikel 1a der Verordnung vom 8. Dezember 2017 (BGBl. I S. 3882).

Verzeichnis zitierter Bundestagsdrucksachen

BT-Drs 15/2286: Gesetzentwurf der Bundesregierung. Entwurf eines Gesetzes über die Errichtung des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe (22.12.2003).

BT-Drs. 17/5672: Bericht des Ausschusses für Bildung, Forschung und Technikfolgenabschätzung (18. Ausschuss) gemäß § 56a der Geschäftsordnung. Technikfolgenabschätzung (TA). TA-Projekt: Gefährdung und Verletzbarkeit moderner Gesellschaften – am Beispiel eines großräumigen und langandauernden Ausfalls der Stromversorgung (27.04.2011).

BT-Drs. 17/12051: Unterrichtung durch die Bundesregierung. Bericht zur Risikoanalyse im Bevölkerungsschutz 2012 (03. 01. 2013).

BT-Drs. 18/208: Unterrichtung durch die Bundesregierung. Bericht zur Risikoanalyse im Bevölkerungsschutz 2013 (16.12.2013).

BT-Drs. 18/3682: Unterrichtung durch die Bundesregierung. Bericht zur Risikoanalyse im Bevölkerungsschutz 2014 (23.12.2014).

BT-Drs. 18/7209: Unterrichtung durch die Bundesregierung. Bericht zur Risikoanalyse im Bevölkerungsschutz 2015 (04.01.2016).

BT-Drs. 18/8332: Gesetzentwurf der Bundesregierung. Entwurf eines Gesetzes zur Erleichterung des Ausbaus digitaler Hochgeschwindigkeitsnetze (DigiNetzG) (04.05.2016).

BT-Drs. 18/10850: Unterrichtung durch die Bundesregierung. Bericht zur Risikoanalyse im Bevölkerungsschutz 2016 (28.12.2016).

BT-Drs. 19/9520: Unterrichtung durch die Bundesregierung. Bericht zur Risikoanalyse im Bevölkerungsschutz 2017 (12.04.2019).

BT-Drs. 19/9521: Unterrichtung durch die Bundesregierung. Bericht zur Risikoanalyse im Bevölkerungsschutz 2018 (12.04.2019).

Verzeichnis zitierter Normen, Standards und Regelwerke

BSI-Standard 200-2 „IT-Grundschutz-Methodik“ (Version 1.0).

DIN EN 15975-1:2016-03 „Sicherheit der Trinkwasserversorgung – Leitlinien für das Risiko- und Krisenmanagement – Teil 1: Krisenmanagement“ (Stand: 03/2016).

DIN EN 15975-2:2013-12 „Sicherheit der Trinkwasserversorgung – Leitlinien für das Risiko- und Krisenmanagement – Teil 2: Risikomanagement“ (Stand: 12/2013).

DIN ISO 31000:2018-10 „Risikomanagement – Leitlinien“ (Stand: 10/2018).

DIN SPEC 91390:2019-12 „Integriertes Risikomanagement für den Schutz der Bevölkerung“ (Stand: 12/2019).

DKG 2019 - Deutsche Krankenausgesellschaft (2019): Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus. Berlin. (Stand 22.10.2019).

DVGW G 1003 (M) Technischer Hinweis – Merkblatt „Hinweise für die Aufrechterhaltung der sicheren Gasversorgung bei Ausfall der regulären Kommunikation“ (Stand: 07/2019).

DVGW W 1060:2017-08 Merkblatt „IT-Sicherheit – Branchenstandard Wasser/ Abwasser“ (Stand: 08/2017).

DWA M 551 Merkblatt Audit „Hochwasser - wie gut sind wir vorbereitet“ (Stand: 12/2010).

DWA M 1060:2017-08 Merkblatt „IT-Sicherheit – Branchenstandard Wasser/ Abwasser“ (Stand: 08/2017).

Verzeichnis genannter Forschungsprojekte

AISIS: Automatisierte Informationsgewinnung und Schutz kritischer Infrastruktur im Katastrophenfall
Projektbeschreibung: https://www.sifo.de/files/SvV_600x800_AISIS.pdf (31.01.2020)

AISTEC: Bewertung alternder Infrastrukturbauwerke mit digitalen Technologien
Projektbeschreibung: https://www.sifo.de/files/Projektumriss_AISTEC.pdf (31.01.2020)

AlphaKomm: Ausfallsichere Lagebildinformationen zur Kommunikation im Krisenfall
Projektbeschreibung: https://www.sifo.de/files/Projektumriss_AlphaKomm(2).pdf (31.01.2020)

AquaBioTox: Onlinefähige Trinkwasserüberwachung mittels eines biologischen Breitbandsensors
Projektbeschreibung: https://www.sifo.de/files/CBRNE_600x800_AquaBioTox.pdf (31.01.2020)

AQUA-IT-Lab: Labor für IT-Sicherheit bei Wasserversorgern
Projektbeschreibung: https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/aqua-it-lab (31.01.2020)

AURIS: Autonomes Risiko-und Informationssystem zur Strukturanalyse und Überwachung sicherheitsrelevanter Bauwerke
Projektbeschreibung: https://www.sifo.de/files/Projektumriss_AURIS_SvV.pdf (31.01.2020)

ESecLog: Erweiterte Sicherheit in der Luftfrachtkette
Projektbeschreibung: https://www.sifo.de/files/Projektumriss_ESecLog.pdf (31.01.2020)

INDI: Intelligente Intrusion-Detection-Systeme für Industrienetze
Projektbeschreibung: https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/indi (31.01.2020)

InfoStrom: Lernende Informationsinfrastrukturen für das Krisenmanagement am Beispiel der Stromversorgung
Projektbeschreibung: https://www.sifo.de/files/Projektumriss_InfoStrom.pdf (31.01.2020)

Kat-Leuchttürme: KatastrophenschutzLeuchttürme als Anlaufstelle für die Bevölkerung in Krisensituationen
Projektbeschreibung: https://www.sifo.de/files/Projektumriss_Kat-Leuchttuerme.pdf (31.01.2020)

KIRMin: Kritische Infrastruktur – Resilienz als Mindestversorgungskonzept
Projektbeschreibung: https://www.sifo.de/files/Projektumriss_KIRMin.pdf (31.01.2020)

MIME: Multimodales Mustererkennungssystem zum Schutz der Bevölkerung vor organisierter Arzneimittelkriminalität
Projektbeschreibung: https://www.sifo.de/files/Projektumriss_MIME.pdf (31.01.2020)

NeuENV: Neue Strategien der Ernährungsnotfallvorsorge
Projektbeschreibung: https://www.sifo.de/files/Projektumriss_NeuENV.pdf (31.01.2020)

PREPARED^{NET}: Agentenbasierte Simulation und Erforschung eines Notfallkonzeptes zum Schutz von sensiblen Logistikknoten
Projektbeschreibung: https://www.sifo.de/files/Projektumriss_PREPAREDNET.pdf (31.01.2020)

PREVIEW: Resilienz kritischer Verkehrsinfrastrukturen am Beispiel der Wasserstraßen
Projektbeschreibung: https://www.sifo.de/files/Projektumriss_PREVIEW.pdf (31.01.2020)

QPASS: Quick Personnel Automatic Safe Screening
Projektbeschreibung: https://www.sifo.de/files/Projektumriss_QPASS.pdf (31.01.2020)

RESCUE IT: IT-Plattform für die lückenlose Sicherung von Lebensmittelwarenketten
Projektbeschreibung: https://www.sifo.de/files/Projektumriss_RESCUE_IT.pdf (31.01.2020)

ResiWater: Innovative, sichere Sensornetzwerke und modellgestützte Bewertungs- und Analyse-Tools zur Erhöhung der Resilienz von Trinkwasserinfrastrukturen
Projektbeschreibung: https://www.sifo.de/files/Projektumriss_ResiWater.pdf (31.01.2020)

SafeMed: Systemgestaltung zur wirtschaftlichen Sicherung der Medikamentenversorgung
Projektbeschreibung: https://www.sifo.de/files/Projektumriss_SafeMed.pdf (31.01.2020)

SiLeBAT: Sicherstellung der Futter- und Lebensmittelwarenkette bei bio und agroterroristischen (BAT)-Schadenslagen
Projektbeschreibung: https://www.sifo.de/files/Projektumriss_SiLeBAT.pdf (31.01.2020)

STATuS: Schutz der Trinkwasserversorgung in Hinblick auf CBRN-Bedrohungsszenarien – Phase 2
Projektbeschreibung: https://www.sifo.de/files/Projektumriss_STATuS.pdf (31.01.2020)

TankNotStrom: Energie- und Kraftstoffversorgung von Tankstellen und Notstromaggregaten bei Stromausfall
Projektbeschreibung: https://www.sicherheit-forschung.de/forschungsforum/zukunftslabor-sicherheit/Projekte_im_zlab/Projektumriss_TankNotStrom.pdf (31.01.2020)

VeSiKi: Vernetzte IT-Sicherheit Kritischer Infrastrukturen (Begleitforschungsprojekt des Förderschwerpunktes IT-Sicherheit für Kritische Infrastrukturen)
Projektbeschreibung: https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/vesiki (31.01.2020)

VESPER: Verbesserung der Sicherheit von Personen in der Fährschifffahrt
Projektbeschreibung: https://www.sifo.de/files/SvV_600x800_VESPER.pdf (31.01.2020)

VESPER^{PLUS}: Verbesserung der Sicherheit von Personen in der Fährschifffahrt
Projektbeschreibung: https://www.sifo.de/files/Projektumriss_VESPERplus.pdf (31.01.2020)

ZEBBRA: Zustandserfassung und -bewertung von Brücken basierend auf Radar-Sensorik in Kombination mit intelligenten Algorithmen
Projektbeschreibung: https://www.sifo.de/files/Projektumriss_ZEBBRA.pdf (31.01.2020)

Abbildungen

Impressum

Herausgeber
Bundesamt für Bevölkerungsschutz
und Katastrophenhilfe
Postfach 1867, 53008 Bonn
Tel. +49 (0)228 99 550-0
www.bbk.bund.de

Redaktion:
Susanne Krings, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Referat II.3

Satz
ORCA Affairs GmbH, Schumannstraße 5, 10117 Berlin

Druck
WM-Druck + Verlag, Römerkanal 52, 53359 Rheinbach

Stand
Februar 2020

Auflage
1000

Bildnachweise
Titelfoto: Anthony Rakusen / Cultura / Getty Images
Seite 6: Mutzberg, BBK

ISBN 978-3-939347-95-8