Dieses Autorenmanuskript ist korrigiert erschienen als: Fekete, A. (2012) Ziele im Umgang mit „kritischen“ Infrastrukturen im staatlichen Bevölkerungsschutz. In: Stober, R. et al. (eds.). Managementhandbuch Sicherheitswirtschaft und Unternehmenssicherheit, Boorberg Verlag, Stuttgart: 1103-1124.

Ziele im Umgang mit „kritischen“ Infrastrukturen im staatlichen Bevölkerungsschutz

Dr.-Ing. Alexander Fekete

A. Teil I: Begriff und Verständnis kritischer Infrastrukturen

I. Einleitung - Was heißt hier kritisch?

Wohl kein Unternehmen und auch keine staatliche Einrichtung möchten gerne als „kritisch“ gelten. Kritisch ist im Deutschen ein auf den ersten Blick überwiegend negativ besetztes Wort. Man denkt an Kritik, kritische Situationen und, in Verbindung mit dem Wort Infrastruktur, vermutlich an technische Einrichtungen mit potentiell gefährlichen Eigenschaften. Dieses Kapitel möchte aufklären, was dieser Begriff, „kritische Infrastruktur“, genau bezeichnet und, wie er im Umfeld staatlichen Bevölkerungsschutzes gegenwärtig verwendet wird.

Der Begriff „kritische Infrastruktur“ ist bislang vorwiegend Experten ein Begriff, insbesondere im Bereich Risiko- und Krisenmanagement, beispielsweise in der Konzernsicherheit. Dies gilt gerade für Großunternehmen, die mit regionalen, staatlichen, oder gar europäischen bis internationalen Sicherheitsbehörden im Austausch sind. Doch auch in den Medien kann man den Begriff kritische Infrastruktur finden, im Zusammenhang z.B. mit Themen wie etwa Cyberangriffen, Auswirkungen von extremen Wetterereignissen oder dem Ausbau und Wandel der Energieversorgung.

Der Begriff kritische Infrastruktur ist in Deutschland auf staatlicher Seite durch Behörden der inneren Sicherheit eingeführt worden.[1] „Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.“[2]

„Infrastrukturen gelten dann als „kritisch“, wenn sie für die Funktionsfähigkeit moderner Gesellschaften von wichtiger Bedeutung sind und ihr Ausfall oder ihre Beeinträchtigung nachhaltige Störungen im Gesamtsystem zur Folge hat. Ein wichtiges Kriterium dafür ist die Kritikalität als relatives Maß für die Bedeutsamkeit einer Infrastruktur in Bezug auf die Konsequenzen, die eine Störung oder ein Funktionsausfall für die Versorgungssicherheit der Gesellschaft mit wichtigen Gütern und Dienstleistungen hat.“[3]

Die Gesellschaft verlässt sich auf das alltägliche Funktionieren der Versorgung durch Infrastrukturen, hat aber auch implizite Erwartungen, dass sich die Qualität des Lebens dadurch steigern lässt, private Vermögen halten, und gar ökonomisches Wachstum gefördert

[1] Der Begriff wurde in Deutschland, unter dem Bundesministerium des Innern (BMI), zuerst durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) und, nach der Neugründung, durch das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) eingeführt.

[2] Bundesministerium des Innern (BMI): Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie), Berlin 2009, S. 3.

[3] Ibidem, S. 5.

Dieses Autorenmanuskript ist korrigiert erschienen als: Fekete, A. (2012) Ziele im Umgang mit „kritischen“ Infrastrukturen im staatlichen Bevölkerungsschutz. In: Stober, R. et al. (eds.). Managementhandbuch Sicherheitswirtschaft und Unternehmenssicherheit, Boorberg Verlag, Stuttgart: 1103-1124.

werde.[4] Die folgende Abbildung weist jene Infrastrukturen aus, die von staatlicher Seite gegenwärtig als „kritisch“ eingestuft werden.

Tabelle. KRITIS-Sektoren[5]

Energie	**Gesundheit**	**Staat und Verwaltung**
Elektrizität Gas Mineralöl	Medizinische Versorgung Arzneimittel und Impfstoffe Labore	Regierung und Verwaltung Parlament Justizeinrichtungen Notfall-/ Rettungswesen einschließlich Katastrophenschutz
Ernährung	**Transport und Verkehr**	**Wasser**
Ernährungswirtschaft Lebensmittelhandel	Luftfahrt Seeschifffahrt Binnenschifffahrt Schienenverkehr Straßenverkehr Logistik	Öffentliche Wasserversorgung Öffentliche Abwasserbeseitigung
Finanz- und Versicherungswesen	**Informationstechnik und Telekommunikation**	**Medien und Kultur**
Banken Börsen Versicherungen Finanzdienstleister	Telekommunikation Informationstechnik	Rundfunk (Fernsehen und Radio), gedruckte und elektronische Presse Kulturgut Symbolträchtige Bauwerke

Der Begriff Kritische Infrastruktur ist nicht ganz einfach zu erklären, da er aus verschiedenen Bedeutungen zusammengesetzt ist. Zum einen ist kritisch negativ besetzt; gefährdet, brisant. Durch die negative Konnotation wird der Begriff ungern von Betreibern von Infrastrukturen benutzt. Zum anderen hat „kritisch“ eine positive Komponente; wichtig, bedeutend, relevant. Weiterhin wird der Begriff auch im Zusammenhang mit „kritischer Masse“ benutzt, um die nötige Anzahl für eine Kernreaktion zu beschreiben. Dies ist interessant, da dieser Begriff eng mit der technischen Welt verbunden ist, eine Sicht, unter die Infrastrukturen allgemein zugeordnet werden.
Nach der dargestellten Terminologie bedeutet kritisch hier zweierlei; zum einen bedeutsam, zum anderen gefährlich. Bedeutsam, da sie für die Versorgung einer großen Anzahl der Bevölkerung wichtig ist. Gefährlich, wenn eine bestimmte Situation entsteht, in der die Versorgung mit einem Gut oder Dienstleistung nicht mehr erfüllt werden kann. Allgemein formuliert ist jede Infrastruktur an sich bedeutsam, aber wenn sie einen kritischen Schwellenwert eines wesentlichen Merkmals erreicht, wird ihre „Kritikalität“ deutlich.
Der Begriff Infrastruktur beschreibt eine Struktur, also etwas das geordnet wahrnehmbar ist und das anderen Prozessen als Unterbau dient. Das weist bereits auf ein wesentliches

[4] Vom Autor übersetzt aus: Boin, Arjen; McConnell, Allan: Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience. In: Journal of Contingencies and Crisis Management, Jg. 15, H. 1, 2007, S. 50.

[5] Einteilung der KRITIS-Sektoren als Ergebnis einer Bund-Länder-Arbeitsgruppe und eines intensiven Abstimmungsprozesses auf Bundesebene. Stand 2011. www.kritis.bund.de, abgerufen am 6.12.2011.

Dieses Autorenmanuskript ist korrigiert erschienen als: Fekete, A. (2012) Ziele im Umgang mit „kritischen“ Infrastrukturen im staatlichen Bevölkerungsschutz. In: Stober, R. et al. (eds.). Managementhandbuch Sicherheitswirtschaft und Unternehmenssicherheit, Boorberg Verlag, Stuttgart: 1103-1124.

Merkmal von Infrastrukturen hin, sie werden meist als nahezu selbstverständlich wahrgenommen. Das gilt für die Bevölkerung wie auch für Organisationen, die sich ganz selbstverständlich darauf verlassen, dass bestimmte Güter und Dienstleistungen, wie z.B. Wasser, Elektrizität oder Telkommunikation ununterbrochen verfügbar sind
Typisch für Infrastrukturen ist aber, dass in einer Gesellschaft historisch große gemeinschaftliche Anstrengungen unternommen werden, um die Versorgung durch eine Infrastruktur zu erstellen und zu gewährleisten. Infrastrukturen sind also auch Ausdruck der Organisationsfähigkeit einer Gemeinschaft und ein gemeinschaftliches Gut, selbst wenn es von einer einzelnen Institution hergestellt oder besessen wird.
Kritische Infrastrukturen sind ein Schnittstellenthema zwischen den Zuständigkeiten von Behörden die sich mit Sicherheitsrisiken befassen und den Betreibern von Infrastrukturen. Einsatzorientierte Kräfte wie etwa die Polizei, Feuerwehr und Technisches Hilfswerk (THW), Behörden mit planerischen Aufgaben im Bereich der Katastrophenvorsorge wie etwa das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), oder die Betreiber und die Kunden von Infrastrukturdienstleistungen haben alle einen unterschiedlichen Zugang zu diesem Thema. Daher umfasst dieses Thema sowohl Fragen der Gefahrenabwehr, der technischen Härtung von Infrastrukturanalysen als auch von anderen Sicherheitskonzepten, die mehr auf Risikominimierung im Vorfeld und Erhöhung der Resilienz setzen.

II. Entstehungsgeschichte des Schutzes Kritischer Infrastrukturen

Der „Schutz Kritischer Infrastrukturen“ ist ein Begriff aus den USA. In den 1980ern waren Infrastrukturen in der Politik der USA noch ein rein wirtschaftliches Entwicklungsthema.[6] In den 1990ern folgte ein Anschauungswandel durch eine unter Präsident Clinton eingesetzte Kommission zum Schutz Kritischer Infrastrukturen.[7] Hintergrund war das neue Bedürfnis nach Fähigkeiten zum Schutz vor Anschlägen. The … „United States shall have achieved and shall maintain the ability to protect the nation’s critical infrastructures from intentional acts“.[8] Unter diesem neuen Paradigma bündeln sich sicherheitspolitische Bereiche und Zuständigkeiten. Zusätzlich ist der private Sektor in die Verantwortung eingebunden. In den 1980ern wurden zunächst Transportwesen, Wasserversorgung und Wasserbehandlung als Infrastrukturen von nationalem Interesse betrachtet. Nebengeordnet wurden auch Schulen, Krankenhäuser, Gefängnisse und die Industrie, auch die Abfallwirtschaft einbezogen. Unter dem neuen Begriff *„critical infrastructure“* und unter neuen Sicherheitsanforderungen z.B. zur *cyber-security* kamen die Sektoren Telekommunikation, Energie, Banken und Finanzwesen hinzu. Die Bush-Regierung strukturierte auch unter dem Eindruck der Anschläge vom 11.9.2001 die Behörden fortwährend um und prägte eine neue Anschauung der Sicherheit - der *„homeland security“*. Auch das Thema *critical infrastructures* wurde in einer neuen nationalen Strategie erfasst, welche den physischen Schutz von Infrastrukturen und Schlüsselelementen (*key assets*) hervorhob.[9] Diese *„key assets“* umfassen nukleare

[6] Koski, Chris: Committed to Protection. Partnerships in Critical Infrastructure Protection. In: Journal of Homeland Security and Emergency Management, Vol.8 (1) 2011, S. 2.
auch: Moteff, J.: Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences. Washington, DC: Congressional Research Service, Library of Congress 2004.
[7] US Government: The President’s Commission on Critical Infrastructure Protection (PCCIP), executive order 13010, Washington DC 1996.
[8] Ibidem.
[9] US Office of the President: The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets. Washington DC, February 2003.

Dieses Autorenmanuskript ist korrigiert erschienen als: Fekete, A. (2012) Ziele im Umgang mit „kritischen“ Infrastrukturen im staatlichen Bevölkerungsschutz. In: Stober, R. et al. (eds.). Managementhandbuch Sicherheitswirtschaft und Unternehmenssicherheit, Boorberg Verlag, Stuttgart: 1103-1124.

Einrichtungen, Landwirtschaft, Verteidigung, Chemische Industrie, Postwesen, Schifffahrt, Nationale Monumente und andere Schlüsselindustrien.[10]

Tabelle. KRITIS in den USA[11]

Agriculture and Food	Banking and Finance	Chemical
Commercial Facilities	Communications	Critical Manufacturing
Dams	Defense Industrial Base	Emergency Services
Energy	Government Facilities	Healthcare and Public Health
Information Technology	National Monuments and Icons	Nuclear Reactors, Materials, and Waste
Postal and Shipping	Transportation Systems	Water

Dieser Hintergrund hilft zu verstehen, wie dieses Thema in Deutschland aufgegriffen wird. So firmiert das Thema gegenwärtig unter dem Begriff „Schutz Kritischer Infrastrukturen“ in Anlehnung an den insbesondere im Nordamerikanischen Sprachgebrauch verwendeten Begriff *Critical Infrastructure Protection (CIP).* In Bezug auf die Entstehungsgeschichte und Begriffswahl der Regierungen der USA erklärt sich der Fokus der Arbeiten von deutschen Behörden des Bevölkerungsschutzes auf den Schutzaspekt, der Bezug auf (terroristische) Anschläge, Cybersicherheit, der besondere Bezug auf physischen Schutz und physische Elemente, sowie auf die Kooperation mit dem privaten Sektor und die Veränderung des Verständnisses von Innerer Sicherheit.

III. Das Thema Kritische Infrastrukturen in Deutschland

Infrastrukturen sind ein Leitthema für den Bevölkerungsschutz, da Infrastrukturen wie Lebensadern die Versorgung der Bevölkerung mit lebenswichtigen Gütern wie Wasser und Energie gewährleisten.[12] Infrastrukturen sind als Prioritätsthema für den Bevölkerungsschutz prädestiniert, da sie als neuralgische Punkte bei einem Ausfall große Bevölkerungsanteile empfindlich beeinträchtigen können. Weiterhin sind Infrastrukturen relativ leichter erfassbar als vergleichsweise „weiche“ Faktoren wie etwa Risikowahrnehmung oder soziale Verwundbarkeit. In Deutschland werden sie unter dem Begriff „Kritische Infrastrukturen“ (auch abgekürzt als KRITIS) vom Bundesministerium des Innern (BMI), dem Bundesamt für Sicherheit in der Informationstechnologie (BSI) und dem Bundesamt für Bevölkerungsschutz und Katastrophenvorsorge (BBK) geführt. Das BMI hat in Zusammenarbeit mit dem BBK in der nationalen KRITIS-Strategie Definitionen und Ziele des Themas dargelegt.[13] BMI und BBK haben eine Reihe von Leitfäden zur Umsetzung und Anleitung von Risikoanalysen im Bereich KRITIS erstellt.[14] Das Thema Infrastrukturen ist für den Bevölkerungsschutz

[10] Koski 2011, S. 3 & 4 gibt in einer Tabelle einen Überblick über diverse critical infrastructures oder auch key resources, wie sie sowohl vom Department of Homeland Security (DHS) als auch von anderen Behörden in den USA eingeordnet werden.
[11] Department of Homeland Security: Critical Infrastructure Sectors, http://www.dhs.gov/files/programs/gc_1189168948944.shtm, abgerufen am 06.12.2011.
[12] BMI 2009, KRITIS-Strategie S. 2.
[13] Ibidem.
[14] Bundesministerium des Innern (BMI): Schutz Kritischer Infrastrukturen – Basisschutzkonzept. Empfehlungen für Unternehmen. Berlin 2005.
BMI: Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement. Leitfaden für Unternehmen und Behörden. Berlin: Bundesministerium des Innern 2007, Neuauflage 2011.

besonders interessant, da es sowohl im Alltagsfall (z.B. Notfall- und Rettungswesen, *Business Continuity Management*) als auch im Krisenfall relevant ist.[15] Damit schlägt das Thema eine Brücke für eine breite Anzahl von einzubeziehenden Akteuren, vom Rettungswesen, der Wirtschaft, diversen staatlichen Behörden bis hin zur Bevölkerung selbst.
Als Eigenheit des Verständnisses, was eine KRITIS ist, gilt in Deutschland, aber auch in vielen anderen Ländern, dass man den Fokus auf die Auswirkungen durch den Ausfall von Infrastrukturen richtet. Das bedeutet, dass die Beeinträchtigung durch Versorgungsausfälle im Mittelpunkt für den Bevölkerungsschutz steht. Gefährdungen durch die Nutzung der Infrastrukturen oder durch primäre Einwirkungen z.B. von Terroranschlägen stehen dagegen gegenwärtig weniger im Vordergrund. Die gefährdende Seite von Infrastrukturen wurde eine Zeitlang noch unter dem Sektor „Gefahrstoffe“ geführt, inzwischen werden jedoch keine „kritischen“ Eigenschaften der Infrastrukturen hinsichtlich eines inhärenten eigenen Gefahrenpotenzials im BBK mehr betrachtet. Das liegt zum einen daran, dass mit einer Vielzahl von Sektoren[16] und Branchen eine sehr große Fülle von Aufgabenfeldern bereits für den Bevölkerungsschutz besteht. Dadurch empfiehlt es sich, eine Priorisierung vorzunehmen. Auch liegen die Zuständigkeiten für bestimmte Infrastrukturen oder Sektoren bei anderen Behörden, z.B. bei kerntechnischen Anlagen, oder bei den Auswirkungen auf die Umwelt.

IV. Infrastruktur – das ist mehr als nur die Technik

Eine Infrastruktur ist die für die Versorgung der Bevölkerung genutzte Struktur, die aus physischen und nicht-physischen Bestandteilen besteht. Eine Infrastruktur besteht aus einem System, das aus kleineren Systemen zusammengesetzt ist, die wiederum aus einer Vielzahl von Kleinteilen bestehen.
Bei einer Infrastruktur denkt man zunächst an die technischen Bestandteile. Dazu gehören physisch vorhandene Elemente wie Gebäude, Leitungen und Ähnliches. Als Bestandteile eines Systems müssen jedoch insgesamt alle Bestandteile des Infrastruktursystems betrachtet werden, sofern sie die Funktionsfähigkeit der Infrastruktur aufrechterhalten. Eine Infrastruktur besteht demnach sowohl aus physisch greifbaren Strukturen, als auch aus weniger greifbaren Elementen und „weichen Faktoren“ die die Funktion der Infrastrukturen bestimmen. Dazu gehört beispielsweise die Qualität des Wassers, die maßgeblich die Funktionalität der Infrastruktur „Wasserversorgung“ beschreibt. Funktionieren beispielsweise noch alle technischen Wasserleitungssysteme, ist aber das Trinkwasser (angeblich) verunreinigt, so nützt die technische Funktionsfähigkeit allein recht wenig.
Die Vielzahl der Funktionen und Elemente einer Infrastruktur kann man mithilfe von Organisationsprozessen erfassen. Prozesse umfassen oft mehr als die physischen Bestandteile allein, z.B. sind Handel und Vertrieb nicht allein durch technische Teile oder Gebäude beschreibbar. Auch der Mensch oder ein anderer Akteur sind als systemsteuerndes Element ein wesentlicher Bestandteil eines Infrastruktursystems. Zur technischen Dimension kommt also noch der Faktor Mensch hinzu. Weiterhin gehören die Umwelt als Standortfaktor und die natürlichen Ressourcen, z.B. Rohstoffe untrennbar zu einer Infrastruktur. Auch ein natürlicher Fluss ist eine Infrastruktur, z.B. als Trinkwasserressource und als Verkehrsweg.

BBK: Schutz Kritischer Infrastruktur: Risikomanagement im Krankenhaus. Praxis im Bevölkerungsschutz, 2, Bonn 2008.
BBK: HEIKAT – Handlungsempfehlungen zur Eigensicherung der Katastrophenschutz- und Hilfsorganisationen bei einem Einsatz nach einem Anschlag. Berlin 2009.

[15] Fekete, Alexander: Weitgehende Abhängigkeiten. Funktionierende Infrastrukturen sind wichtig im Alltag wie im Katastrophenfall. In: Bevölkerungsschutz Magazin, Jg. 3., 2010.

[16] BMI 2009: KRITIS-Strategie, S. 5.

Dieses Autorenmanuskript ist korrigiert erschienen als: Fekete, A. (2012) Ziele im Umgang mit „kritischen“ Infrastrukturen im staatlichen Bevölkerungsschutz. In: Stober, R. et al. (eds.). Managementhandbuch Sicherheitswirtschaft und Unternehmenssicherheit, Boorberg Verlag, Stuttgart: 1103-1124.

Infrastrukturelemente

Die verschiedenen KRITIS-Sektoren und Branchen bestehen aus völlig unterschiedlichen Elementen; von Stromübertragungsnetzen, IT-Software, Steuerungsprozessen bei Behörden, bis hin zu Vertrauensaspekten im Finanzwesen. Eine reine Betrachtung von physisch-technischen Infrastrukturelementen und Knotenpunkten ist hierbei nicht ausreichend. Daher werden im Rahmen eines Projekts am BBK namens KritisKAT[17] Infrastrukturen in folgende Elemente untergliedert:[18]

- Physisch-technische Elemente
- Prozesse / organisatorische Strukturen der Steuerung (Regelwerke, Schaltpläne, etc)
- Personal / steuernde Akteure (Herstellungs-, Leitungs-, Überprüfungs-, Trainings-, Reparaturpersonal)
- Umwelt- und Standortfaktoren

Gerade für ein ganzheitliches Risikomanagement ist es unerlässlich, neben technischen Elementen auch das Personal, wesentliche Prozesse und Standortfaktoren zu integrieren. Personal ist funktionsrelevant – ob als Prozesssteuerung oder als Reparaturteam. Bestimmte Gefahren, beispielsweise eine Epidemie, wirken selektiv auf das Personal ein, und nicht auf technische Bestandteile.

V. Risikomanagement im BBK im Bereich KRITIS

Kritische Infrastrukturen werden im BBK unter dem Blickwinkel der mittel- bis langfristigen Planung im Vorfeld einer Krise untersucht. Damit unterscheidet sich dieser Arbeitsbereich von anderen Aufgaben des BBK und auch des Technischen Hilfswerks (THW), welche sich mehr mit Krisenreaktion und Gefahrenabwehr, also dem operativen Einsatz in und nach einer Krise, befassen.
Das Ziel des KRITIS-Programms des BBK ist die Aufrechterhaltung der Funktionsfähigkeit der Versorgung der Bevölkerung insbesondere bei außergewöhnlichen Notfällen. Diese Einwirkungen sind nicht-regelmäßige Störungen und unterscheiden sich damit von alltäglichen Einwirkungen und den hiefür bereits vorhandenen technischen Standards. Diese Einwirkungen sind z.B. sog. Naturgefahren, technisches oder menschliches Versagen oder auch bewusste Störungen wie etwa Sabotage.
Diese Bandbreite an Einwirkungen wird auch als All-Gefahren Ansatz bezeichnet.[19] Hintergrund des All-Gefahren Ansatzes ist weniger der Anspruch, möglichst alle Gefahren zu erfassen oder gar zu minimieren. Vielmehr möchte man allgemeine Erkenntnisse ableiten, die eine Risikominderung gegenüber möglichst vielen Gefahren bewirken können. Zu dieser Überlegung führt auch die Erkenntnis, dass weder eine Erkennung oder Eindämmung aller möglichen Gefahren, noch ein vollständiger Schutz der Bevölkerung gegenüber seltenen oder extremen Risiken möglich ist. Daher werden zunehmend spezielle Untersuchungsmethoden der Risikoforschung auch im Risikomanagement von Unternehmen angewendet, z.B.

[17] Projekt KritisKAT: www.bbk.bund.de; auch: http://www.bbk.bund.de/DE/AufgabenundAusstattung/KritischeInfrastrukturen/Projekte/KritisKat/KritisKat_Startseite.html?nn=1899916, abgerufen am 06.12.2011.
[18] Fekete, Alexander: Common Criteria for the Assessment of Critical Infrastructures. In: Int. J. Disaster Risk Sci. 2011, 2 (1), S. 15–24.
[19] All-hazard approach: Federal Emergency Management Agency (FEMA): SLG 101, Guide for All-Hazard Emergency Operations Planning, Washington DC 1996.

Dieses Autorenmanuskript ist korrigiert erschienen als: Fekete, A. (2012) Ziele im Umgang mit „kritischen“ Infrastrukturen im staatlichen Bevölkerungsschutz. In: Stober, R. et al. (eds.). Managementhandbuch Sicherheitswirtschaft und Unternehmenssicherheit, Boorberg Verlag, Stuttgart: 1103-1124.

Einschätzungen der Verwundbarkeit und Resilienz. Durch diese Methoden werden weniger die Gefahren an sich betrachtet, als die Fähigkeiten der Menschen oder der KRITIS selbst, auf die Gefahren zu reagieren.

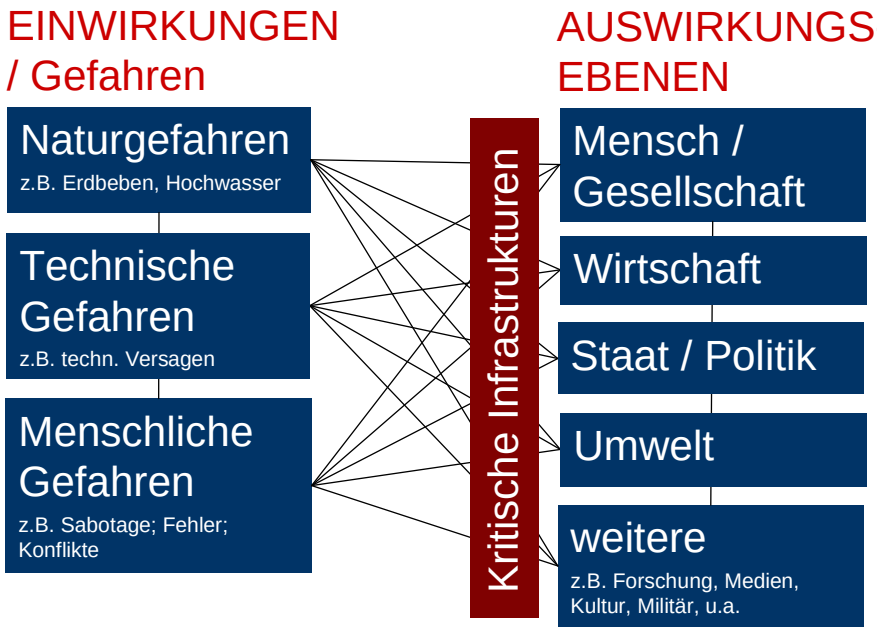


Abb. Gefahren und Auswirkungsebenen (Eigener Entwurf)

Das BBK ist mit Vertretern der privaten Wirtschaft im Dialog, in Form eines kooperativen statt eines regulierenden Ansatzes. Da etwa 80% der Infrastrukturen heutzutage in privater Hand sind, möchte das BBK gerne das Bewusstsein für die Verantwortung im Bevölkerungsschutz auch auf Seiten der Wirtschaft vermitteln. In Gesprächen wurden einerseits unterschiedliche Ziele deutlich, zum anderen wuchs der Bedarf nach einer gemeinsamen Zielgröße, bis zu der ein Schutzniveau vernünftig realisierbar ist. Weiterhin wurde eine belastbare Grundlage gefordert, aus der ersichtlich wird, welche Grenzwerte oder Schutzniveaus erreicht werden sollen. Das BBK hat zu diesem Zweck eine Reihe von Projekten in verschiedenen Sektoren gestartet, die wissenschaftliche Grundlagen und Expertenwissen verbinden, um die Kritikalität bestimmter Infrastrukturen zu erfassen. Darin geht es um die Erfassung von unternehmenswichtigen Prozessen und Elementen, und um die Einschätzung von Versorgungsausfällen und ihren Auswirkungen auf die Gesellschaft. Im Bereich Elektrizität ist das z.B. das Projekt GRASB (2009-2012), im Bereich Gas- und Mineralöl das Projekt KritisGM (2009 – 2011) und im Bereich Straßenverkehr das Projekt SKRIBT (2008 - 2011).
Das Projekt KritisKAT ist hingegen ein sektorübergreifendes Projekt, das Grundlagen, ein gemeinsames Konzept und allgemeine Kriterien zur Ermittlung der Kritikalität von allen Sektoren von Infrastrukturen im BBK, erstellt (2009 – 2012). Ein Kern der Untersuchungen ist einerseits die Relevanz, die eine bestimmte Infrastruktur oder ein Bestandteil der Infrastruktur für die Versorgung der Bevölkerung innehat. Zum anderen werden Schwellenwerte untersucht, also kritische Zeitpunkte oder die Anzahl von ausfallenden Knotenpunkten, ab denen es kritisch wird.[20] Diese Ergebnisse eignen sich als Grundlage zur Diskussion um gesamtgesellschaftliche Schutzziele für großflächige und lange andauernde Versorgungsausfälle.

[20] Fekete, A. 2011: Common Criteria.

Dieses Autorenmanuskript ist korrigiert erschienen als: Fekete, A. (2012) Ziele im Umgang mit „kritischen“ Infrastrukturen im staatlichen Bevölkerungsschutz. In: Stober, R. et al. (eds.). Managementhandbuch Sicherheitswirtschaft und Unternehmenssicherheit, Boorberg Verlag, Stuttgart: 1103-1124.

B. Teil II: Schutzziele für Kritische Infrastrukturen

VI. Der Bedarf an Schutzzielen im Risikomanagement

Ein Manager einer bekannten Computerfirma soll sich einmal gefragt haben, wie er noch mehr Personal Computer verkaufen könne. Als er sich über die lange Startzeit seines Computers ärgerte, rief er seine Techniker an und ordnete an, die Startzeit zu verkürzen. Er erklärte ihnen, wenn sie die Startzeit um 10 Sekunden verkürzten, würden sie allein beim einmaligen Hochfahren von 5 Millionen dieser Computer der Menschheit 50 Mio. Sekunden Lebens- und Arbeitszeit schenken. Fortan wurden alle Aktivitäten der Techniker diesem strategischen Ziel untergeordnet. Man kennt dieses Prinzip in der Wirtschaft auch unter dem Begriff „strategisches Management“.
In ähnlicher Weise und mit ähnlich umfassender Bedeutung gibt es auch im Bevölkerungsschutz strategische Ziele, z.B. Schutzziele. Als Schutzziel wird im Folgenden ein gesamtgesellschaftliches Übereinkommen von Zielvorstellungen zum Umgang mit krisen- bis hin zu katastrophenartigen Risiken verstanden. Schutzziele formulieren generell anzustrebende Zustände oder Vorbilder für die Gesellschaft für den Umgang mit Ressourcen und Bedrohungen.

Gegenwärtige Terminologie des BBK[21]

- Schutzziel: angestrebter Zustand eines → Schutzguts, der bei einem Ereignis erhalten bleiben soll
- Schutzgut: alles, was aufgrund seines ideellen oder materiellen Wertes vor → Schaden bewahrt werden soll
- Schaden: negativ bewertete Auswirkung eines → Ereignisses auf ein → Schutzgut
- Bevölkerungsschutz: Summe der zivilen Maßnahmen zum Schutz der Bevölkerung und ihrer Lebensgrundlagen vor den Auswirkungen von → Kriegen, → bewaffneten Konflikten, → Katastrophen und anderen schweren Notlagen sowie solcher zur Vermeidung, Begrenzung und Bewältigung der genannten → Ereignisse.

„Schutzziele“ existieren in ganz unterschiedlicher Weise, für verschiedene Zwecke und Ebenen. Es gibt technische Normen und Schutzziele zur Dimensionierung von Extrembelastungen z.B. an Strommasten oder Gebäuden. Diese Schutzziele legen Grenzwerte (z.B. Stand der Technik, Grenzbelastungen, erwartete Belastungsspitzen) und in gewisser Weise auch den erwarteten Risikobereich fest. Neben technischen Normen werden zunehmend auch Sicherheitskonzepte oder Risikoanalyseprozesse standardisiert und normiert. Die Beratung zu Zertifizierungen im Bereich Sicherheit und Risikomanagement ist ein attraktives und wachsendes Geschäftsfeld, mit Wirtschaft wie Behörden als Zielgruppe.

[21] Interne Definitionen des BBK, Stand 2011.

Dieses Autorenmanuskript ist korrigiert erschienen als: Fekete, A. (2012) Ziele im Umgang mit „kritischen“ Infrastrukturen im staatlichen Bevölkerungsschutz. In: Stober, R. et al. (eds.). Managementhandbuch Sicherheitswirtschaft und Unternehmenssicherheit, Boorberg Verlag, Stuttgart: 1103-1124.

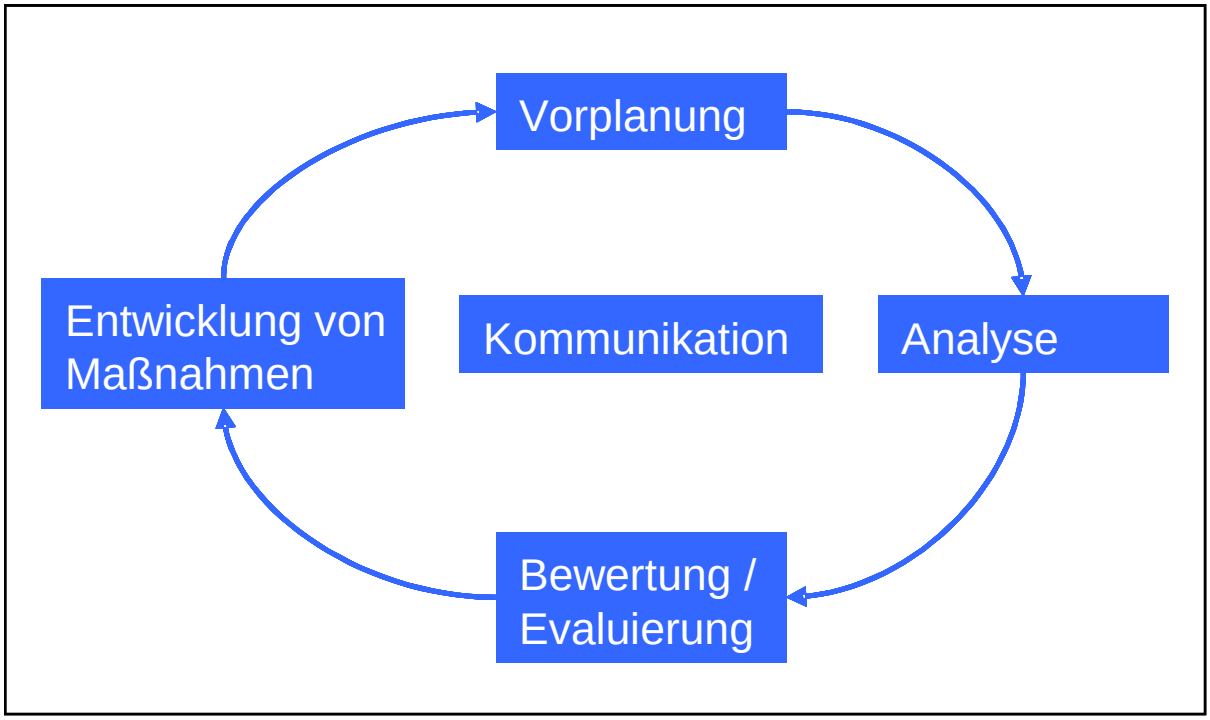


Abb. Risiko- und Krisenmanagement-Zyklus (Eigener Entwurf[22])

Schutzziele durchziehen alle Phasen des Risiko- und Krisenmanagement-Kreislaufs. Als strategisches Element sind Zielvereinbarungen der Anfang jeder Planung. Auch Analysen, und die Entwicklung von konkreten Maßnahmen benötigen Richtlinien oder Richtwerte, an denen sich die Ergebnisse bewerten und einordnen lassen – z.B. ob sie nun ein Risiko als hoch oder niedrig einschätzen. Bei der Bewertung und Kommunikation von strategischen Zielen und den daraus resultierenden Umsetzungsmaßnahmen, z.B. Schutzmaßnahmen, sind Schutzziele ebenfalls ein grundlegender Bestandteil.

VII. Inhalte von Schutzzielen im Bevölkerungsschutz

Der Ruf nach Schutzzielen ist nicht neu und durchdringt viele Expertenvorträge und Fachpublikationen, z.B. im Zusammenhang mit der Zukunft des Bevölkerungsschutzes[23], oder beispielsweise in der Hochwasservorsorge mit der Forderung nach einer gesellschaftlichen Debatte um Schutzziele.[24] Für den Bevölkerungsschutz liegen gesetzliche Regelungen vor, z.B. diverse Sicherstellungsgesetze, Richtlinien oder Normen, die aus unterschiedlichen Bereichen und Sektoren stammen. Auf der Webseite des BBK[25] findet sich eine Zusammenstellung von Sicherstellungs- und Vorsorgegesetzen. Sie nennen konkrete

[22] Vereinfacht und verändert nach: BMI 2011 und diversen andern Quellen, z.B. ISO 31010:2009; IRGC 2009.
[23] Schöttler, Horst: Ist unser Bevölkerungsschutzsystem noch zukunftsfähig? Katastrophenschutz im 21. Jahrhundert: Anspruch, Realität und notwendige Entwicklungslösungen. Bonn: Deutsches Komitee für Katastrophenvorsorge e.V. (DKKV) 2000, S. 15.
[24] Deutsches Komitee für Katastrophenvorsorge e.V. (DKKV): Hochwasservorsorge in Deutschland. Lernen aus der Katastrophe 2002 im Elbegebiet. Bonn: Lessons Learned. Schriftenreihe des DKKV, (29) 2003 Bonn, S. 7,16.
[25] www.bbk.bund.de.

Dieses Autorenmanuskript ist korrigiert erschienen als: Fekete, A. (2012) Ziele im Umgang mit „kritischen“ Infrastrukturen im staatlichen Bevölkerungsschutz. In: Stober, R. et al. (eds.). Managementhandbuch Sicherheitswirtschaft und Unternehmenssicherheit, Boorberg Verlag, Stuttgart: 1103-1124.

Ziele, z.B. die „Deckung des lebensnotwendigen Bedarfs an Trinkwasser“ im Wassersicherstellungsgesetz. Jedoch fehlt es gegenwärtig an viele Stellen und für viele KRITIS-Sektoren an konkreten Schutzniveaus oder Konzepten, wie diese Ziele in einem Risikomanagement zu erzielen sind.
Schutzziele sind ein Kernpunkt des Risiko- und Krisenmanagementkonzepts des BBK.[26] Bei der Frage nach Anpassungsoptionen an den Klimawandel, wie auch in anderen Bereichen, sind Schutzziele jedoch häufig noch nicht bestimmt oder kaum strukturiert. Andere Länder wie etwa die Schweiz haben bereits Grundlagen zur gesellschaftlichen Diskussion um Schutzziele geschaffen.[27] Für den Bevölkerungsschutz in Deutschland wird ein Bedarf, gar ein Fehlen konkreter Schutz- und Interventionsziele festgestellt.[28]
Für den Bevölkerungsschutz und seine Schutzziele lassen sich die unterschiedlichen Konzepte vereinfacht auf vier Kernfragen reduzieren.

Fragen, die das Thema Schutzziele umfassen, sind:

- Wovor soll geschützt werden?
- Was soll geschützt werden?
- Bis zu welchem Grad soll geschützt werden?
- Wie soll dieses Ziel erreicht werden?

Zur ersten Frage können als Zielobjekte sog. Schutzgüter festgelegt werden. Diese Fragen sind teilweise auch gesetzlich fixiert, beispielsweise in den Vorsorgegesetzen. Neben dem reinen Schutzgut oder Schutzobjekt besteht ein Schutzziel noch aus Normen und Werten. Darin besteht ein großer Bedarf, die zu schützenden Objekte und Lebensgrundlagen ähnlich des Models der Daseinsgrundfunktionen[29] grundsätzlich neu zu bestimmen. Damit müssen auch gesellschaftliche Normen und Zielvorstellungen für den Bevölkerungsschutz modernisiert werden und sich nicht mehr nur auf den Kriegsfall beziehen.
Die Frage bis zu welchem Grad geschützt werden soll, enthält Aspekte eines Schutzniveaus, einer Zielerreichungsgröße. Häufig werden Schutzziel und Schutzniveau synonym verwendet. Ein Schutzziel wird hier im Folgenden als übergeordneter Begriff verwendet.
Im Bevölkerungsschutz spielen gegenwärtig weniger kriegerische Handlungen, sondern vielmehr so genannte Naturgefahren, technische, ökologische und menschlich bedingte Risiken eine treibende Rolle. Kennzeichnend für den gegenwärtigen Stand ist der so genannte *all hazard* Ansatz (All-Gefahrenansatz). Er betont die Vielzahl gegenwärtiger Bedrohungen und Gefahren und global wirkender Auswirkungen von Störungen. Dieser Ansatz fördert einen ganzheitlichen Blick auf Aspekte, die für eine Vielzahl von Gefahren ähnlich sind. Damit ist auch die Erkenntnis verbunden, die Betrachtung nicht nur auf die Gefahren, sondern auch auf die Einwirkungen und Fähigkeiten der betroffenen Bevölkerung, Ökosysteme, Einsatzkräfte etc. zu lenken. Für solch einen ganzheitlichen Ansatz, der sich nicht auf spezifische Gefahren und den Aspekt ihrer Abwehr allein bezieht, erfasst der Begriff „Schutzziel“ nur einen Teilaspekt der Fülle möglicher Risikobewältigungsstrategien. Neben

[26] BMI 2007, Neuauflage 2011: Risiko- und Krisenmanagement Leitfaden
[27] Eckhardt Anne (Ed.): Schutzziel-Modell. Nationale Plattform Naturgefahren PLANAT. Bern 2009.
[28] BBK: Neue Strategie zum Schutz der Bevölkerung in Deutschland. Wissenschaftsforum. Band 4. Bonn 2010, S. 36.
[29] Hierarchy of needs: Maslow, Abraham H.: A Theory of Human Motivation. In: Psychological Review, Jg. 50, 1943, S. 370–396.

Dieses Autorenmanuskript ist korrigiert erschienen als: Fekete, A. (2012) Ziele im Umgang mit „kritischen“ Infrastrukturen im staatlichen Bevölkerungsschutz. In: Stober, R. et al. (eds.). Managementhandbuch Sicherheitswirtschaft und Unternehmenssicherheit, Boorberg Verlag, Stuttgart: 1103-1124.

Schutz müssen künftig auch strategische Ziele in Verbindung mit Begriffen wie Vorsorge, Anpassung, Akzeptanz und Toleranz betrachtet werden.
Akzeptanz und Toleranz sind Schlüsselbegriffe für Ziele im Zusammenhang mit Risiken. Im anglophonen Sprachraum wird im Zusammenhang mit Risikoanalysen von *acceptable* oder *tolerable risk levels* gesprochen.[30] Es wird auch darauf hingewiesen, dass es den einen einzigen *risk level* nicht gibt. Stattdessen werden mehrere Ebenen unterschieden; von individueller Akzeptanz, Akzeptanz mehrerer Individuen, system-interner Akzeptanz, gesellschaftlicher Akzeptanz und Experten-Akzeptanz. Toleranzgrenzen wie etwa das ALARA- Prinzip[31] aber auch Begriffe wie “Restrisiko“ beschreiben anzustrebende Ziele oder Grenzwerte. In der Schweiz werden Toleranzgrenzen genutzt, abgeleitet aus Risikobewertungen und Risikomatrizen.[32] Die Zielformulierung der Schweiz ist ein klassisches Beispiel für Risikoreduzierung: „Das Ziel des Schutzes Kritischer Infrastrukturen ist es, die Eintretenswahrscheinlichkeit und das Schadensausmaß einer Störung, eines Ausfalls oder einer Zerstörung der Kritischen Infrastrukturen zu reduzieren, beziehungsweise die Ausfallzeit zu minimieren.“[33] Die Minimierung von Ausfallzeiten, die Verfügbarkeit, Integrität und Vertraulichkeit sind auch Grundwerte oder (Schutz-)Ziele, die Unternehmen kennen, sei es im Bereich IT-Sicherheit[34] oder bei der Einhaltung vertraglicher Liefervereinbarungen, auch als *Service Level Agreements* (SLA)[35] bekannt.
Traditionell werden neben dem Vergleich mit der durchschnittlichen Sterberate im Alltag auch Messgrößen aus *cost-benefit* Analysen (*marginal costs*) genutzt. Alternativ verwendet man auch die Bereitschaft der Bevölkerung, Sicherheitsmaßnahmen zu bezahlen (*willingness to pay*), um Akzeptanzgrenzen zu ermitteln.[36]
Viele Ziele transportieren eine Botschaft, die den Glauben an eine Kontrollierbarkeit von Risiken beinhaltet, z.B. “Schutz”, „Regulierung“ oder „Steuerung“ (*risk governance, risk management*). Andere Zielformulierungen können ethisch brisant werden, wie z.B. ‘*accepted collective suffering*’.[37] Schutzziele formulieren generell anzustrebende Zustände oder Leitbilder für den Umgang mit Ressourcen oder Bedrohungen.

---

[30] Bell, R.; Glade, T.; Danscheid, M.: Challenges in defining acceptable risk levels. In: Ammann, W. J.; Dannenmann, S.; Vulliet, L. (Eds.) Coping with Risks due to Natural Hazards in the 21st Century. Taylor & Francis, London 2006, S. 77-87.
[31] ALARA: *as low as reasonably achievable,* oder auch -*practicable:* ALARP, siehe z.B. Perrow, Charles: Normal Accidents: Living with High-Risk Technologies. Chichester: Princeton University Press, 1999, S. 308.
[32] Hess, Josef Th.: Schutzziele im Umgang mit Naturrisiken in der Schweiz. Doktorarbeit. DISS. ETH Nr. 17956. Zürich 2008.
[33] VBS & BABS: Erster Bericht an den Bundesrat zum Schutz Kritischer Infrastrukturen: Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS & Bundesamt für Bevölkerungsschutz BABS, Bern 2007, S. 7.
[34] Bundesamt für Sicherheit in der Informationstechnik (BSI): Leitfaden Informationssicherheit. IT-Grundschutz kompakt. Bonn, Stand 2011, S. 11.
[35] BSI: BSI-Standard 100-4. Notfallmanagement. Bonn 2008, S. 5.
[36] Bell et al. 2006.
[37] LaPorte, Todd R.: Critical Infrastructure in the Face of a Predatory Future: Preparing for Untoward Surprise. In: Journal of Contingencies and Crisis Management, Jg. 15, 2007, S. 60–64.

Dieses Autorenmanuskript ist korrigiert erschienen als: Fekete, A. (2012) Ziele im Umgang mit „kritischen“ Infrastrukturen im staatlichen Bevölkerungsschutz. In: Stober, R. et al. (eds.). Managementhandbuch Sicherheitswirtschaft und Unternehmenssicherheit, Boorberg Verlag, Stuttgart: 1103-1124.

VIII. Schutzziele als Impulse für den Bevölkerungsschutz

Im Folgenden werden Beispiele für Schutzziele und Schutzniveaus dargestellt. Aus diesen Beispielen sind unterschiedliche Herangehensweisen und Interessensschwerpunkte erkennbar, die durch ihre Vielfalt unterschiedliche Impulse für den Bevölkerungsschutz bieten.

„Null Tote“

Ein gesamtgesellschaftliches Schutzziel ist die „Vision Zero“ im Straßenverkehr. Diese Zielvorgabe ist auf europäischer Ebene ausgerufen[38], in Schweden rechtsverbindlich festgelegt seit 1997[39] und auch in Nordrhein-Westfalen ein offizielles Ziel. Es trägt dem Umstand Rechung, dass der Straßenverkehr noch immer eine der tatsächlich häufigsten und relevantesten Gefahren mit Todesfolge darstellt. Während es in Deutschland 1970 noch 21300 Tote im Straßenverkehr gab, waren es 2010 noch 3648.[40] Mit der „Zielvorgabe Null“ wird auch deutlich, dass dies eine Vision ist, die ggf. gar nicht vollständig zu erreichen ist. Sie soll jedoch inspirieren und Maßnahmen steuern, um die Anzahl der Verkehrstoten wesentlich zu reduzieren. Ein ähnliches Ziel von null Sterblichkeit wird z.B. in der Nahrungsmittelsicherheit verfolgt.[41]

Das Beispiel „Schweinegrippe“ hat jedoch auch gezeigt, wie schwierig der Umgang mit unsicheren Zahlenwerten ist. Bereits ein Toter, der mit der Schweinegrippe assoziiert wurde, hat eine große Medienresonanz erfahren, während es zunächst weniger öffentlich bekannt war, dass es jedes Jahr Tausende Tote allein durch die saisonale Grippe gibt.

„Zwei Grad“

Der Klimawandel wie auch der Bevölkerungsschutz sind Querschnittsthemen, die nicht nur auf einen Sektor oder eine Branche beschränkt sind.[42] Während die genauen Auswirkungen des Klimawandels weiterhin unsicher und umstritten sind, gibt es eine Reihe von Kommunikationsmitteln, die dieses vage und breite Thema anschaulich machen. Insbesondere das vieldiskutierte Ziel, den Temperaturanstieg auf zwei Grad zu beschränken, fixiert einen Zahlenwert, der sich eingeprägt hat in die öffentliche Diskussion. Auch macht ein prognostizierter Meeresspiegelanstieg das Thema Klimawandel erst greifbar und regt damit zu konkreten Handlungen an. Solche Zahlenwerte, unsicher, wie sie sind, stellen eine für alle Akteure vorstellbare Größe, eine Art bildliches Kommunikationsmedium dar.

---

[38] Rieckmann, Tanja: EU-Initiative Vision Zero. Weiter Weg zur Nullnummer. In: Spiegel online, 15. September 2010.

[39] Breitinger, Matthias: Zielgröße Null. In: Zeit online, 20. Juli 2010.

[40] Statistisches Bundesamt: 2010: Unfallreiches Jahr, aber weniger Verkehrstote denn je. Pressemitteilung Nr.252 vom 06.07.2011.

[41] Knight, Andrew J.; Worosz, Michelle R.; Todd, Ewen C. D.; Bourquin, Leslie D.; Harris, Craig K.: Listeria in Raw Milk Soft Cheese: A Case Study of Risk Governance in the United States Using the IRGC Framework. In: Renn, Ortwin; Walker, Katherine (Eds.): Global Risk Governance: Springer 2008, S. 179–220.

42 Fekete, Alexander, Rosen, Klaus-Henning, Goldammer, Johann Georg, Zemke , Julian J.: Analyse der Berücksichtigung des Bevölkerungsschutzes in: Anpassungsstrategien an den Klimawandel. Anforderungen an den Bevölkerungsschutz. Wissenschaftsforum 5. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe Bonn 2010.

Dieses Autorenmanuskript ist korrigiert erschienen als: Fekete, A. (2012) Ziele im Umgang mit „kritischen“ Infrastrukturen im staatlichen Bevölkerungsschutz. In: Stober, R. et al. (eds.). Managementhandbuch Sicherheitswirtschaft und Unternehmenssicherheit, Boorberg Verlag, Stuttgart: 1103-1124.

Risiko 10^7

In der Luftfahrt gibt es weit entwickelte Standards von *security* und *safety* für diverse Gefährdungen für die Luftfahrt (‚*environmental risk*') und Reduzierung von Unfällen (‚*individual risk*'). So beziehen z.B. die sog. *target levels of safety*, auf mindestens seit den 1940ern bestehende Berechnungen der Wahrscheinlichkeit von Unfällen.[43] Ziel ist es, die Luftfahrt nicht gefährlicher als die normale Erwartung von alltäglichen Unfällen zu gestalten. Errechnete Schutzniveaus sind z.B. die Erwartung eines Unfalls pro 10^7 Flugstunden, die Werte variieren jedoch.[44]

Ähnliche Werte gibt es auch im Gesundheitswesen, in dem dann von einer außergewöhnlichen Notfallsituation (*emergency situation*) gesprochen wird, wenn die Sterblichkeitsrate (*crude mortality rate, CMR*) in der betroffenen Bevölkerung nach einer Katastrophe signifikant höher als vor der Katastrophe ist, oder wenn sie höher als ein Todesfall pro 10.000 Betroffene pro Tag oder drei Todesfälle pro 1000 Betroffene pro Monat ist.[45]

In Deutschland hat die Nutzung von Kernenergie zur Entwicklung der wissenschaftlichen und gesellschaftlichen Debatte um technische Risiken stark beigetragen. Anhand von Risikoanalysen wurde der Versuch unternommen, Risiken begreifbar, reduzierbar und auch kommunizierbar zu machen. Die Erfahrung hat jedoch gezeigt, dass auch als sehr niedrig kalkulierte Risikowahrscheinlichkeitswerte (1:1000000) allein kein Sicherheitsgefühl vermitteln konnten. Dennoch hat die grundsätzliche Art, Risiken zunächst zu analysieren, um sie dann beispielsweise in Ampelfarben in Risikomatrizen darzustellen, auch in anderen Gefahrenbetrachtungen eine weiträumige Verbreitung gefunden. Anhand solcher Analysen von Risiken werden konkrete Maßnahmen zur Risikoreduzierung als Ziel abgeleitet (z.B. ‚*disaster risk reduction*'). Ermittelte Risikoskalen oder –margen werden häufig verwendet, um daraus dann technische oder auch gesellschaftliche Toleranzgrenzen zu erreichender Schutz- oder Risikospielräume zu ermitteln.[46]

„Nachhaltigkeit“

Ein Beispiel für die Verlagerung des Blickpunkts weg von einer Beherrschbarkeit und „Zähmung der Natur“[47] und damit auch weg von der Gefahreneindämmung und hin zu vorsorgenden Verhaltensweisen des Menschen ist das Umwelt und Entwicklungsparadigma „Nachhaltigkeit“. Seit der Betonung und Bezugsetzung durch die sog. Brundtland

43 Saldana, M. A. M. Herrero S. G. Del Campo M. A. M. Ritzel D. O. (2003): Assessing Definitions and Concepts within the Safety Profession. In: The International Electronic Journal of Health Education, H. 6, 2003, S. 1–9.

44 Subotic B., Ochieng, W. & A. Majumdar: Equipment failures in ATC. Finding an appropriate safety target. In: The Aeronautical Journal 2005, S. 278, 281.

45 Center for Disease Control and Prevention, 1992; Sphere Project, 2000, wie zitiert in Wisner, B.; Adams, J. (Eds.): Environmental health in emergencies and disasters: a practical guide, World Health Organization, Geneva 2002, S. 13.

46 WBGU - Wissenschaftlicher Beirat der Bundesregierung Globale Umweltveränderungen: Welt im Wandel: Strategien zur Bewältigung globaler Umweltrisiken, Wissenschaftlicher Beirat der Bundesregierung Globale Umweltveränderungen, Springer, Berlin 1998.

47 Blackbourn, D.: The Conquest of Nature: Water, Landscape, and the Making of Modern Germany: Water, Landscape and the Making of Modern Germany, Jonathan Cape, Random House, London 2006.

Kommission[48] ist Nachhaltigkeit ein Leitbild zur Entwicklung unserer „gemeinsamen Zukunft“. Auch wenn der Begriff inzwischen Abnutzungserscheinungen trägt, hat er zum Verständnis globaler Auswirkungen von Umwelteinflüssen durch den Menschen beigetragen. Ein ähnlich qualitativ formuliertes Ziel ist *‚living with risk’*[49], also das Risiko als Teil des Lebens zu akzeptieren.

„8 Minuten“

Schutzziele sind bei Feuerwehren in Brandschutzbedarfsplänen festgelegt. Darin werden die Kapazitäten und Ausstattung der Feuerwehren für eine Gemeinde ermittelt, um eine ausreichend schnelle und umfangreiche Versorgung zu gewährleisten. Interessanterweise wird hier, ähnlich wie beim Vorgehen zur Risikoanalyse von KRITIS im BBK[50] zunächst eine Risikoanalyse durchgeführt, und Schutzziele daraus abgeleitet, um danach die Ausstattung der Feuerwehren zu bestimmen.[51] Als Qualitätskriterien werden zur Schutzzielbestimmung die Zeitdauer zum Erreichen des Einsatzortes (Hilfsfrist, z.B. „8 Minuten“; sie variiert jedoch), die Stärke von Mannschaft und Gerät (Funktions- oder Einsatzstärke), sowie der Erreichungsgrad als Prozent der Fälle, in denen die Feuerwehr den Einsatzort erreichen soll, genutzt.
In ähnlicher Weise werden auch für Rettungskräfte Anforderungen an die Notfallvorsorge ermittelt. Für den so genannten „Massenanfall von Verletzten“ (MANV) sind hierbei Transport- und Betreuungskapazitäten die Kernpunkte der Planung von Personal und Ressourcen. Darin werden so genannte MANV-Stufen 1-4 je nach Betroffenen- oder Verletztenzahl unterschieden.[52]
Wenn es sozusagen schon brennt, oder Risiken und ihre Auswirkungen nicht mehr zu verhindern sind, sind Selbsthilfe und Selbstschutz weitere wichtige Aspekte des Bevölkerungsschutzes. Im anglophonen Raum ist die Stärkung der *community resilience* oder *local level adaptability*, der *livelihoods*, etc. ein vorherrschendes Thema in der Entwicklungszusammenarbeit und insbesondere in der sozialwissenschaftlichen Forschung. Die Ziele sind meist qualitativ und häufig sehr normativ geprägt.

Die Bandbreite an Beispielen zeigt, dass ein gesellschaftliches Ziel des Bevölkerungsschutzes eine Vielzahl an Aspekten integrieren müsste. Oder es eine ganze Reihe an spezifischen Zielen geben müsste: von der Abwehr und Beherrschung von Gefahren bis hin zu Risikoakzeptanz, weiterhin zu verschiedenen Phasen des *disaster cycle*, für verschiedenste Akteure von Betroffenen bis hin zu „Kümmerern“ auf verschiedenen räumlichen und administrativen Ebenen, für eine Vielzahl von Sektoren, für verschiedene Eskalationsstufen vom Notfall bis hin zur Katastrophe.

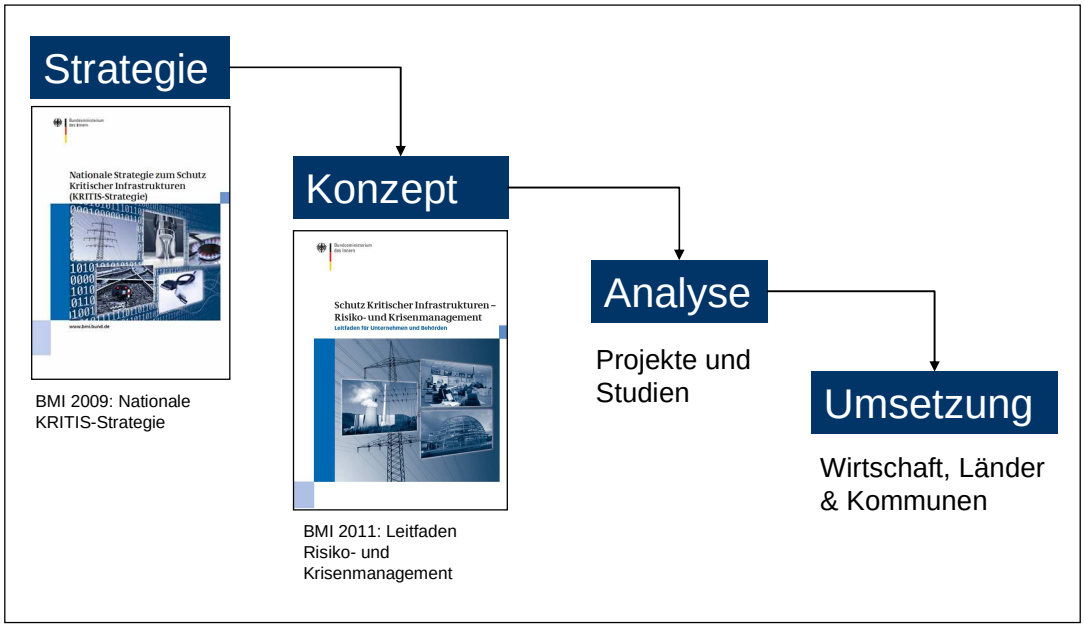
[48] UN: Report of the World Commission on Environment and Development: Our common future 1987.
[49] UN/ISDR: Living with Risk. A global review of disaster reduction initiatives, UN/ISDR - Inter-Agency Secretariat of the International Strategy for Disaster Reduction, United Nations, Geneva 2004.
[50] BMI 2007, Neuauflage 2011: Risiko- und Krisenmanagement Leitfaden
[51] Als Beispiel: Stadt Bonn: Brandschutzbedarfsplan der Bundesstadt Bonn – 1. Fortschreibung 2007 – Stand 30.11.2007.
[52] Sefrin, Peter: Der Massenanfall von Verletzten (MANV). In: Notfallvorsorge 4/2010.

Dieses Autorenmanuskript ist korrigiert erschienen als: Fekete, A. (2012) Ziele im Umgang mit „kritischen“ Infrastrukturen im staatlichen Bevölkerungsschutz. In: Stober, R. et al. (eds.). Managementhandbuch Sicherheitswirtschaft und Unternehmenssicherheit, Boorberg Verlag, Stuttgart: 1103-1124.

Es wird schwierig, wenn nicht unmöglich oder gar unsinnig sein, Schutzniveaus allgemein für alle Gefahren, Branchen oder Verwaltungsebenen festzulegen.[53] Für konkrete Schutzziele gerade hinsichtlich von Katastrophen im Zusammenhang mit dem Ausfall von Kritischen Infrastrukturen herrscht noch großer Forschungsbedarf.

IX. Ziele beim Thema Infrastrukturen für den Bevölkerungsschutz

Beim Thema Kritische Infrastrukturen lässt sich sehr deutlich der Weg von der Strategie bis hin zur Umsetzung verfolgen. Die strategische Zielvorgabe ist im Europäischen Programm zum Schutz Kritischer Infrastrukturen (EPSKI) sehr allgemein formuliert. In EPSKI wird der Bedarf für den Schutz Kritischer Infrastrukturen und für Analysen festgestellt. Um diesen Schutz genauer bestimmen zu können, sollen im Programm EPSKI Kriterien ermittelt werden, welche Infrastrukturen europaweit relevant sind und bei einem Ausfall, der mindestens zwei Nachbarstaaten betrifft, kritisch sein können. Die Ermittlung der Kriterien, und die Analysen werden den Mitgliedstaaten als Aufgabe übertragen. Das EPSKI Programm ist also gleichzeitig eine Strategie und bietet einen Umsetzungsweg an.
In Deutschland lässt sich zum Schutz Kritischer Infrastrukturen der Weg von der Strategie bis zur Umsetzung in Schritten nachverfolgen. Die Nationale KRITIS Strategie[54] formuliert das allgemeine Ziel und Begriffsdefinition. Das Konzept zur Umsetzung bietet ein Leitfaden[55] zum Risiko- und Krisenmanagement, welcher die einzelnen Schritte einer Analyse bis hin zur Entwicklung von Maßnahmen erläutert. Die Analysen werden für jede Infrastrukturbranche in jeder Einrichtung von den Anwendern selbst erstellt. Nur diese kennen sich mit ihrer Infrastruktur aus. Hier erarbeitet der Bund lediglich Empfehlungen und fordert keine Einblicke in konkrete Schwachpunkte o.ä. von Unternehmen. Die Umsetzung von konkreten Maßnahmen obliegt ebenfalls den Unternehmen und Einrichtungen, bzw. den Ländern und Kommunen, je nach Infrastruktur-Branche.



[53] Ergebnis einer Diskussion der Tagung ‚The Future of Critical National Infrastructure - The View to 2015’, Royal United Services Institute (RUSI), London 2010.
[54] BMI 2009: KRITIS-Strategie.
[55] BMI 2007, Neuauflage 2011: Risiko- und Krisenmanagement Leitfaden.

Dieses Autorenmanuskript ist korrigiert erschienen als: Fekete, A. (2012) Ziele im Umgang mit „kritischen“ Infrastrukturen im staatlichen Bevölkerungsschutz. In: Stober, R. et al. (eds.). Managementhandbuch Sicherheitswirtschaft und Unternehmenssicherheit, Boorberg Verlag, Stuttgart: 1103-1124.

Abb. Weg von Strategie zu Maßnahmen im Bereich KRITIS im Bevölkerungsschutz (Eigener Entwurf)

X. Gesamtgesellschaftliche Schutzziele für Kritische Infrastrukturen

Die Erarbeitung von Schutzzielen geschieht im Optimalfall in einem Mehrebenenansatz. Schutzziele, auch im Bereich Kritischer Infrastrukturen, betreffen Behörden auf staatlicher Ebene, auf Länder- und auf kommunaler Ebene[56], sie betreffen die Privatwirtschaft auf allen Ebenen, von Großkonzernen bis zu Kleinen und Mittleren Unternehmen (KMUs), alle Einheiten des Notfall- und Rettungswesens, die Wissenschaft und nicht zuletzt die Bevölkerung selbst. Für eine Vielzahl von Ebenen müssen Akteure an einer Diskussion um Schutzziele beteiligt werden. Im Grunde genommen ist die Schaffung von Diskussionsplattformen nötig, in der gesamtgesellschaftlich das Thema Risiko auch im Zusammenhang mit Infrastrukturen in das öffentliche Bewusstsein gerückt wird. Die „Neue Strategie“ des BBK formuliert als eine Anforderung an den Schutz der Bevölkerung ein strukturelles Gesamtkonzept, zu dem auch politisch zu vereinbarende gesellschaftliche Schutzziele gehören.[57]
Zunehmend wird der Ruf nach „Grenzgängern“ und Übersetzern laut, die fertige Analyseergebnisse und abstrakte Sicherheitskonzepte verständlich und begreifbar machen. Risikokommunikation ist schon lange ein wichtiges Thema in der Regulierung und im Umgang mit Risiken[58], und einige *Risk Governance Frameworks* stellen sie gar als zentral dar.[59] Auch im BBK wird gegenwärtig ein Risikokommunikationskonzept entworfen.
In Schweden wird erwogen, runde Tische mit Anwohnern und Elektrizitätsbetreibern, der Stadtverwaltung und Katastrophenschützern einzuberufen, um öffentlich die Rangliste der Abschaltung von Straßenzügen bei Stromausfall zu diskutieren. Wäre ein solches Vorgehen in Deutschland auch denkbar? Ist Deutschland reif für eine öffentliche Diskussion um Schutz- Vorsorge- oder Verhaltensziele?

Es lassen sich gegenwärtig zwei Wege zur Erstellung von gesamtgesellschaftlichen Schutzzielen im Bevölkerungsschutz erkennen. Der eine Weg führt über die Ermittlung von gemessenen oder beobachteten Grenzen z.B. von Kapazitäten oder Ressourcen zur Erstellung von Schutzzielen. Zum anderen können Schutzniveaus und Schutzziele anhand von Toleranzgrenzen („Null Tote“, Nachhaltigkeit, etc.) vorgegeben werden. Dies kann z.B. durch Gremien (Normung), Institutionen oder durch eine Einbeziehung vieler Akteure (siehe „Stuttgart 21“) vorgegeben werden.
Mit Schutzzielen befassen sich im Zusammenhang mit KRITIS gegenwärtig mehrere Forschungsprojekte. Die Fachhochschule Köln, Institut für Rettungsingenieurwesen und Gefahrenabwehr untersucht in der Studie KRITIS-Kapa einerseits Möglichkeiten zur

[56] John-Koch, Monika; Fekete, Alexander: Der Schutz Kritischer Infrastrukturen – auch eine kommunale Aufgabe. BBK & Deutscher Städtetag (Hg.) Drei Ebenen, ein Ziel: BEVÖLKERUNGSSCHUTZ – gemeinsame Aufgabe von Bund, Ländern und Kommunen. 2010, S. 22-29.
[57] BBK 2010: Neue Strategie, S.45.
[58] United Kingdom Interdepartmental Liaison Group on Risk Assessment (UK-ILGRA): Risk Communication. A Guide to Regulatory Practice. Health and Safety Executive, Risk Assessment Policy Unit, London 1998.
[59] IRGC: An introduction to the IRGC Risk Governance Framework: International Risk Governance Council (IRGC), Geneva, 2008.

Erstellung von Schutzzielen für KRITIS[60]. Zum anderen werden die Grenzen der Notfallfähigkeiten von Akteuren im Bereich Stromversorgung auf den Ebenen staatliche Stellen, Betreiber und Bevölkerung untersucht. Die Grenzen der Notfallfähigkeiten sind ein wichtiger Beitrag zur Ermittlung von Schutzzielen.
Schutzziele sind auch ein Risikokommunikationsmedium, das eine gesamtgesellschaftliche Diskussion über den Umgang mit Risiken und die Grenzen von Schutz antreiben kann. Hierzu werden in mehreren Arbeiten an der Hochschule für Wirtschaft und Recht (HWR) Möglichkeiten für eine Risikokommunikation mit der Bevölkerung untersucht. Die Einbindung der Bevölkerung selbst, sowie moderne Risikokommunikationskonzepte sind ein Thema im Aufbau. Einseitige Informationsversorgungen erst nach Abschluss von Analysen und ohne Beteiligung der Bevölkerung werden zunehmend durch moderne Ansätze der Wissensvermittlung ergänzt.[61]
Anregungen für Schutzziele können gerade auch aus der Erfahrung von Experten gezogen werden. Ein „Faustregel“ für den Zeitpunkt, ab wann von einer Katastrophe ausgegangen werden kann, lautet: wenn zehn Prozent einer Region vier Tage und länger betroffen sind.[62] Interessanterweise gibt es in den USA eine ähnliche Faustregel, von 72 Stunden, bis zu denen sich die Bevölkerung z.B. auf Nuklearangriffe, Erdbeben oder andere Krisen vorbereiten sollte.[63] Die sehr allgemeingültigen Kriterien Zeitdauer und evtl. auch Ausdehnung / oder Betroffenheitsmenge der Bevölkerung bieten eine allgemein akzeptierbare Basis zur Verhandlung von Schutzzielen. Im Gegensatz dazu sind wirtschaftliche Zahlenwerte oder sensible Größen wie die Anzahl von Toten weniger für eine öffentliche Diskussion geeignet, da sie unterschiedlich und kontrovers bewertet werden.
Es verbleiben aber bei jeder Festlegung gerade quantitativer Schutzniveaus weiterhin Restrisiken, welche die einzelnen Bemessungen von zu erwartenden Ereignissen übersteigen. Diese Restrisiken lassen sich nur bedingt für bestimmte Ereignisse und bestimmte (technische) Objekte konkret bestimmen und dimensionieren. Ein gesamtgesellschaftliches Schutzziel, das gegenüber einer Vielzahl von Gefahren die Versorgungssicherheit von Infrastrukturen beschreibt, geht jedoch einen anderen Weg. Es fokussiert auf die Auswirkungen auf die Bevölkerung und die zu erwartende Situation, egal wodurch sie eintritt. Aus diesem Ansatz ergeben sich eine ganze Reihe von Fragestellungen, z.B. ob und wie „Schutz“ oder „Vorsorge“ ohne konkreten Bezug auf einzelne Gefahren überhaupt möglich ist. Auf der anderen Seite ermöglicht dieser Ansatz unter der Bandbreite an Unsicherheiten der Risikovorhersage die Anerkennung der Grenzen der Risikoanalysen und verlässt sich nicht auf historische Bemessungsereignisse. Katastrophen zeichnen sich schließlich dadurch aus, dass sie unerwartet und überraschend eintreten. Die Dimensionierung von Schutz und Vorsorge anhand von Ereignissen wie dem Elbehochwasser 2002, dem Stromausfall im Münsterland 2005 oder generell der bekannten aufgetretenen Orte von Ereignissen und Zeitpunkten, ggf. mit einem Sicherheitsaufschlag, birgt das große Risiko, sich nur auf das

[60] KRITIS-Kapa: http://www.f09.fh-koeln.de/institute/irg/forschung/projekte/01837/index.html, abgerufen am 06.12.2011.
[61] Schweer, Benedikt: Analyse der Möglichkeiten und Grenzen bei der Verwendung von Schutzzielen in der Risikokommunikation zur Vorbereitung auf einen anhaltenden Stromausfall, Bachelorarbeit. Hochschule für Wirtschaft und Recht, Berlin 2011.
[62] Mündliche Auskunft des Präsidenten des THW, Albrecht Broemme, langjähriger Leiter der Berliner Feuerwehr, auf der Veranstaltung "Public Private Security: Schutz Kritischer Infrastrukturen" in Berlin am 21-24.03.2010.
[63] Lucus-McEwen, Valerie: 72 hours of one, three days of another. In: Natural Hazards Observer, H. 1, 2011, S. 9.

Dieses Autorenmanuskript ist korrigiert erschienen als: Fekete, A. (2012) Ziele im Umgang mit „kritischen“ Infrastrukturen im staatlichen Bevölkerungsschutz. In: Stober, R. et al. (eds.). Managementhandbuch Sicherheitswirtschaft und Unternehmenssicherheit, Boorberg Verlag, Stuttgart: 1103-1124.

bereits Bekannte vorzubereiten. Hier sind zukünftig noch sinnvolle Grenzen von Schutzzielen und Schutzniveaus zu ermitteln.

C. Teil III: Umsetzung des Schutzes Kritischer Infrastrukturen

XI. Zusammenarbeit zwischen Bund, Ländern und Privaten

Innerhalb der privaten Wirtschaft möchte nicht jeder Betrieb gerne als „kritisch“ gelten. Da der Gefährdungsaspekt von Infrastrukturen in Deutschland beim Bevölkerungsschutz gegenwärtig nicht vorrangig beachtet wird, könnte man erwägen, künftig nur noch von „Infrastrukturen“ zu sprechen, oder, ähnlich wie in den Niederlanden, von „vitalen“[64], oder besonders wichtigen, essentiellen Infrastrukturen für die Versorgung der Bevölkerung.
Neben der Debatte um Begriffe geht es aber vor allem um die Frage der Verantwortungsübernahme. Für außergewöhnliche Notfälle, Krisen oder Katastrophen muss ein gemeinsames Verantwortungsbewusstsein geschaffen werden. Es ist nicht genug, nur Vorschriften und Gesetzesvorgaben abzuarbeiten, proaktives Denken ist für Krisen notwendig. Krisen wie das Elbehochwasser 2002[65] oder die jüngste Finanzkrise machen deutlich, dass Staat, Wirtschaft und auch die Bürger an ihre Grenzen stoßen. Keiner will den Löwenanteil der Schäden bezahlen, oder die Schulden. Aber es ist auch schwierig, die eigenen Möglichkeiten und Fähigkeiten zu erkennen, eine Krise zu bewältigen. Noch schwieriger ist die korrekte Umsetzung und das Bewusstsein, auch für andere Verantwortung übernehmen zu wollen. Das gilt für die Handlung von Individuen wie für große Organisationen. Ausnahmen und leuchtende Vorbilder gibt es natürlich auch.
Eine große Herausforderung für Unternehmen sind aber besonders die ständigen Veränderungen und Trends. So hört man mitunter auch von großen Unternehmen unter der Hand den Ruf nach staatlichen Vorgaben und Richtlinien. Dies wird dann verständlich, wenn man die inzwischen weltweit agierenden Unternehmenszweige und in Tochterunternehmen ausgelagerte Arbeitsbereiche sich vor Augen führt. *Outsourcing* und *Unbundling* haben zu einer Zersplitterung des davor zentral vorhandenen Wissens über die Unternehmensbereiche geführt. Damit fehlen teilweise ein ganzheitliches Risikomanagement und ein Überblick über Lieferketten, Verflechtungen und Abhängigkeiten, kurz, die ganze Palette an Risikofaktoren. Daher besteht auch in großen Unternehmen Interesse an Leitfäden zu Risikomanagement, *Business Continuity Management* oder Risikoanalysen, Gefahrenkatalogen, zentralen Wissensdatenbanken. Risikomanagement und gerade der Consultingbereich scheint in diesen Bereichen zu boomen. Diese Beratungsfunktion kann die staatliche Seite nur begrenzt im Bereich Bevölkerungsschutz leisten.
Ein Problem in der Zusammenarbeit von Wirtschaft und Behörden sind die Zuständigkeiten, die unübersichtlich sind und wo es verständlich ist, dass die Industrie sich hier klare Ansprechpartner wünscht. *Single Points of Contact (SPOC)* werden daher in einigen Arbeitskreisen mit Vertretern der Wirtschaft gebildet. Das BMI, BSI und auch das BBK haben im Rahmen des Umsetzungsplans KRITIS (UPKRITIS) KRITIS-Verbände bei der Bildung von SPOCs unterstützt. Damit kann der Austausch von Informationen in Krisenzeiten optimiert werden. In regelmäßigen Übungen erprobt, arbeiten hier Behörden und Wirtschaft zusammen. Auch in anderen Arbeitskreisen des BBK, z.B. im Bereich

[64] Luiijf, Eric; Burger, Helen & Klaver, Marieke: Critical Infrastructure Protection in The Netherlands: A Quick-scan. EICAR Conference Best Paper Proceedings 2003.
[65] DKKV 2003: Lessons Learned.

Dieses Autorenmanuskript ist korrigiert erschienen als: Fekete, A. (2012) Ziele im Umgang mit „kritischen“ Infrastrukturen im staatlichen Bevölkerungsschutz. In: Stober, R. et al. (eds.). Managementhandbuch Sicherheitswirtschaft und Unternehmenssicherheit, Boorberg Verlag, Stuttgart: 1103-1124.

Stromversorgung wird der Dialog gesucht, und Kooperation gegenüber einem regulierenden Ansatz bevorzugt.
Bei kleinen und mittleren Unternehmen (KMU) ist die Lage eine andere, hier fehlen Personalressourcen, um sich auch noch mit Risikomanagementthemen zu befassen. Dies ist ein zukünftiges Arbeitsfeld im Bevölkerungsschutz. Das BSI, aber auch einzelne Gesprächskreise und Projekte im BBK, z.B. im Bereich Wasserversorgung treten mit KMU in Kontakt und suchen Wege, zumindest grundlegende Schutzmaßnahmen zu vermitteln. Dieser Grundschutz kann im Bereich IT schon allein die Bewussteisvermittlung beim Personal um Schwachstellen im Internet sein. Die zunehmende Vernetzung mit IT macht KMU wie auch den Bürger selbst genauso verwundbar wie auch große Behörden und Unternehmen. Hier ist ein Ansatzpunkt gegeben, durch eigene, auch einfache Vorsichts- und Vorsorgemaßnahmen die Widerstandsfähigkeit (Resilienz) gegenüber Krisen zu erhöhen. Ein Backup der Daten auf der Festplatte kann nicht schaden, wie auch das Wissen für den Notfall: wer kann mir helfen, wohin kann ich gehen, und was kann ich selbst tun? Dieses Prinzip gilt nicht nur für IT-Ausfälle, sondern auch für ein Hochwasser, Stromausfall oder jede andere Art von Krise.

XII. Kritische Bereiche identifizieren und Maßnahmen entwickeln

Die Erkenntnis, dass ein vollständiger Schutz der Bevölkerung nicht möglich oder finanzierbar ist, macht eine Identifizierung und Priorisierung der Verwundbarkeiten der Infrastrukturen nötig.[66] Die Ermittlung der Kritikalität von Infrastrukturen wird im BBK gegenwärtig im Projekt KritisKAT untersucht, um solche Priorisierungen vornehmen zu können.
Trotz der Definition des Begriffs „Kritikalität“ und „Kritischer Infrastrukturen (KRITIS“ in der Nationalen KRITIS-Strategie[67] und der expliziten Aufnahme in das Risiko- und Krisenmanagement-Konzept zu KRITIS im Leitfaden für Behörden und Unternehmen (BMI 2008), sowie der Anwendung in diversen Projekten und Studien, besteht noch Bedarf an Grundlagen, wie man Kritische Infrastrukturen und ihre kritischen Bestandteile erkennt. Kritikalitätsuntersuchungen sollen die Fülle an möglichen Bereichen für eine Risikoanalyse eingrenzen, um den Arbeitsaufwand zu begrenzen. Aus den Ergebnissen der Risikoanalysen erhofft man sich schließlich möglich konkrete und anwendbare Erkenntnisse, um Gegenmaßnahmen daraus ableiten zu können. Zum einen ist dieser gedachte Ablauf in einem ganzheitlichen Risikomanagementprozess in der Realität sehr umfangreich, personalintensiv und aufwendig. Erfahrungen von Einrichtungen, die den Risiko- und Krisenmanagementleitfaden des BBK angewendet haben, belegen das. Diese Erkenntnisse flossen in die Neuauflage des Leitfadens „Risiko- und Krisenmanagement“ ein[68], und werden auch im Rahmen von Seminaren an der Akademie für Krisenmanagement, Notfallplanung und Zivilschutz (AKNZ) durch das BBK vermittelt. Andererseits lassen sich jedoch bereits aus einfachen Anfangsabschätzungen durch recht einfache Kriterien erste Handlungsschwerpunkte erkennen. Beispielsweise liegt es auf der Hand, dass nur einmal vorhandene Infrastrukturbestandteile, sei es eine technische Spezialeinrichtung oder ein speziell ausgebildeter Angestellter, sehr schwer ersetzbar sind. Gerade in einer Notfallsituation wird das überdeutlich. Ein weiteres Beispiel ist das Kriterium Größe – Unternehmen, die einen großen Marktanteil haben, treffen die ganze Wirtschaft empfindlich.

[66] Apostolakis, George E.; Lemon, Douglas M.: A Screening Methodology for the Identification and Ranking of Infrastructure Vulnerabilities Due to Terrorism. In: Risk Analysis, Jg. 25, H. 2, 2005, S. 361.
[67] BMI 2009: KRITIS-Strategie.
[68] BMI 2007, Neuauflage 2011: Risiko- und Krisenmanagement Leitfaden.

Dieses Autorenmanuskript ist korrigiert erschienen als: Fekete, A. (2012) Ziele im Umgang mit „kritischen“ Infrastrukturen im staatlichen Bevölkerungsschutz. In: Stober, R. et al. (eds.). Managementhandbuch Sicherheitswirtschaft und Unternehmenssicherheit, Boorberg Verlag, Stuttgart: 1103-1124.

Ein reales Beispiel ist ein Hersteller von Computerfestplatten, der in Thailand 2011 vom Hochwasser stark betroffen war. Die Preisanstiege für Festplatten in den folgenden Monaten trafen sowohl Konzerne wie auch Privatpersonen. Solch einfache Kriterien werden auch zur Ermittlung sog. systemrelevanter Banken genutzt; Größe, Substituierbarkeit und Vernetzungsgrad. Daraus lassen sich Gegenmaßnahmen erkennen. Diese sind für jede Branche, für jeden Standort und für jede Unternehmensgröße unterschiedlich. Dennoch gibt es Gemeinsamkeiten, welche das BBK im Projekt KritisKAT erkennen, auswerten und für verschiedene Anwender zur Verfügung stellen möchte. Als Ergebnis werden Empfehlungen zur Entwicklung von allgemein anwendbaren Kriterien für alle KRITIS-Branchen erwartet und für einige beispielhafte Branchen auch konkrete, umsetzbare Kriterien. Während die Maßnahmenvorschläge von so einem generalistischen Projekt ebenfalls allgemein sein werden, befassen sich andere Projekte des BBK mit Partnern aus der Wirtschaft mit der Entwicklung konkreter Ergebnisse du Maßnahmen, z.B. im Bereich Stromversorgung das Projekt GRASB. Auch für den Bereich Lebensmittel wird ein Leitfaden erarbeitet, für Krankenhäuser ist er bereits vorhanden, ebenso für Notstromversorgung (siehe www.bbk.bund.de).
In KritisKAT ergaben sich folgende generell anwendbare Kriterien, um Kritikalität einzuschätzen.[69] Ein Element wird dann kritisch, wenn

- eine kritischer Anteil (z.B. der Leistungsfähigkeit eines Elements)
- eine kritische Zeiteinheit (z.B. Ausfalldauer oder Eintrittsschnelligkeit)
- eine kritische Qualität (z.B. die Wasserqualität)

betroffen sind. Eine kritische Reaktion tritt meist in Kombination von zweien oder allen dreien dieser generischen Kriterien ein. Sie kann sowohl positiv als auch negativ verlaufen. Das Untersuchungsinteresse im Bereich KRITIS bezieht sich auf das *Business Continuity Management (BCM)* und die Versorgungssicherheit. Es geht dabei um mögliche negative Konsequenzen durch Unterbrechungen im Betriebsablauf und daraus entstehenden Versorgungsengpässen.

XIII. Empfohlene Maßnahmen auf Unternehmensebene

Der bereits erwähnte Leitfaden „Schutz Kritischer Infrastrukturen - Risiko- und Krisenmanagement“ ist gezielt zur Anwendung von Unternehmen und Behörden mit Hilfe von Unternehmen entwickelt worden. Er liegt nun in einer überarbeiteten Auflage vor[70] und wird durch eine kurze Einführungsbroschüre und eine Darstellung auf Folien online ergänzt[71]. In die Überarbeitung flossen auch wertvolle Hinweise von Anwendern ein, die bereits Erfahrung mit der Durchführung eines Risikomanagements oder zumindest mit Risikoanalysen nach Vorgabe des Leitfadens gemacht haben. Die Erfahrungen von Anwendern zeigen, dass der Leitfaden umfassend alle kritischen Bereiche zu erfassen hilft, und ein weit reichendes Methodenset enthält. Die folgende Tabelle stellt vereinfacht den

[69] Fekete, Alexander: Common Criteria for the Assessment of Critical Infrastructures. In: Int. J. Disaster Risk Sci. 2011, 2 (1): S. 15–24.
[70] BMI 2007, Neuauflage 2011: Risiko- und Krisenmanagement Leitfaden.
[71] Eine Einführungsbroschüre und eine Einführung mittels Folien zum Leitfaden sind unter den Publikationen zu KRITIS des BBK zu finden: http://www.bbk.bund.de/DE/AufgabenundAusstattung/KritischeInfrastrukturen/Publikationen/Leitfaden_Schutz-Kritis.html?nn=1899920.

Dieses Autorenmanuskript ist korrigiert erschienen als: Fekete, A. (2012) Ziele im Umgang mit „kritischen“ Infrastrukturen im staatlichen Bevölkerungsschutz. In: Stober, R. et al. (eds.). Managementhandbuch Sicherheitswirtschaft und Unternehmenssicherheit, Boorberg Verlag, Stuttgart: 1103-1124.

Ablauf einer Risikoanalyse für KRITIS und die einzelnen Methodenschritte dar[72]. Die genauen Schritte sind im Leitfaden enthalten.

Tabelle: Vereinfachte Darstellung der Phasen einer Risikoanalyse KRITIS

Phasen der Risikoanalyse	**Erläuterung**
1. Vorplanung	An was sollte man denken, wenn man eine Risikoanalyse durchführen möchte?
2. Kritikalitätsabschätzung	Welche Betriebsabläufe sind wichtig und bedürfen einer eingehenden Analyse?
3. Gefahrenabschätzung	Welche Gefahren können die Betriebsabläufe stören?
4. Verwundbarkeitsabschätzung	Gibt es besonders verwundbare Betriebsbereiche?
5. Risikoermittlung	Wie hoch wird das Risiko von Störungen im Betriebsablauf bewertet?
6. Einbindung in das Risiko- und Krisenmanagement	Welche Sicherheitsmaßnahmen sollten untersucht werden?

Es gibt aber auch einige Hürden bei der Implementierung und Durchführung einer Risikoanalyse bzw. eines Risiko- und Krisenmanagements; insbesondere personelle Ressourcen müssen eingeplant werden, auch längerfristig, um nach der Erarbeitung der Ergebnisse der Risikoanalyse daraus auch Maßnahmen ableiten und im Unternehmen einführen zu können. Weiterhin müssen Zuständigkeiten abgefragt werden und nicht zuletzt immer wieder eigene Entscheidungen getroffen werden, denn der Leitfaden gibt nur die Richtung und die Methoden vor. Der Leitfaden enthält daher keine Muster-Anleitungen, da jede Einrichtung unterschiedlich aufgebaut und gesteuert ist, unterschiedliche Produkte herstellt, unterschiedliche Sicherheitsanforderungen hat und mit unterschiedlichen Zulieferern und Kunden in Beziehung steht. Der Leitfaden und die Risikoanalyse ersetzen daher auch nicht Erfahrungen, reale Tests, oder kontinuierliche Überprüfungen des Risikomanagements.

[72] Ibidem. Die Tabelle ist der Einführungsbroschüre entnommen.