Schriften zur Zukunft der Öffentlichen Sicherheit

Das Undenkbare denken

Zukunftsforum Öffentliche Sicherheit

„Seit Menschengedenken ist dies das erste Mal, dass die Welt so einen komplexen Notfall erlebt, der einen Tsunami, ein Erdbeben und eine nukleare Krise beinhaltet. Obwohl dieses Szenario noch nie da gewesen ist, könnte es sein, dass es kein Einzelfall bleibt. Denn ein Anstieg dieser komplexen Art von Katastrophen ist fast sicher.

Um uns zu schützen, müssen wir das Undenkbare denken. Wir müssen große Investitionen im Bereich der Katastrophenbereitschaft tätigen, Risiken reduzieren – eingeschlossen nukleare Risiken – und den Gemeinden helfen, sich selbst zu schützen. Das ist Vorsorge. Die einzige Antwort auf solch eine Tragödie ist schließlich wechselseitige Hilfe und ein Geist der Gemeinschaft – in meinem Land, in Ihrem Land und in allen Ländern – und eine Entschlossenheit, uns besser vorzubereiten, damit wir im Angesicht dieser brutalen Katastrophen Leben schützen können.“

Aus einem offenen Brief von Tadateru Konoé,
Präsident des Japanischen Roten Kreuzes[1]

[1] Quelle: www.drk.de/news/meldung/5691-japan-eine-herausforderung-fa14r-die-vorstellungskraft-ein-appell-an-das-gewissen.html

Seite

Vorwort

Der Mensch ist fehlbar, aber lernfähig

Dr. Konstantin von Notz ist Mitglied des Deutschen Bundestages von BÜNDNIS 90/DIE GRÜNEN und in diesem Jahr Beiratsvorsitzender des ZOES.

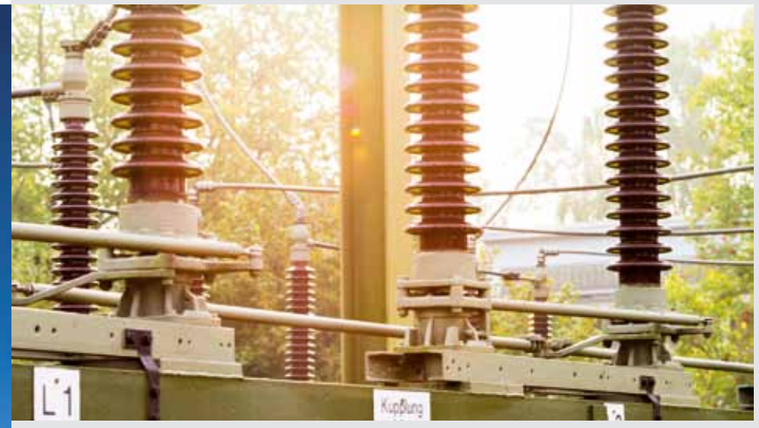
In unserer hoch technologisierten Welt treffen Naturereignisse auf Kritische Infrastrukturen, deren Schädigung ihrerseits katastrophale Folgen nach sich ziehen kann. Naturereignisse erscheinen zwar unausweichlich, doch wie sich unsere Gesellschaft gegen Katastrophen wappnet, ist planbar. Vor dem Hintergrund des Klimawandels erscheinen allerdings gehäuft auftretende Extremwetterereignisse durchaus nicht mehr als rein natürliche Phänomene, sondern bis zu einem gewissen Grad auch als menschengemacht. Es verlangt daher einen klaren politischen Willen, um zu beeinflussen, was sich wirklich beeinflussen lässt.

Unsere Verletzlichkeit steigt in dem Maße, wie die Technologisierung unserer Alltagswelt und die Interdependenz von kritischen Infrastrukturen zunehmen. Politik im Dienste der öffentlichen Sicherheit muss stets im Auge behalten, dass der Mensch und alles Menschengemachte fehlbar sind und dass Technologien immer so ausgelegt sein müssen, dass sie keine unabsehbaren, katastrophalen Folgen nach sich ziehen. Das ist der Grund dafür, warum der Deutsche Bundestag mit breiter Mehrheit beschlossen hat, aus der Atomenergie auszusteigen.

Auch bei neuen Technologien gilt es, mögliche Risiken vorauszusehen, die Fehlbarkeit von Systemen und technologischen Mechanismen im Auge zu behalten und Sicherheit von vornherein als integralen technologischen Bestandteil zu konzipieren. Folgekosten, die beispielsweise aus einer klimaunverantwortlichen Energiepolitik resultieren, müssen, so weit sie auch in der Zukunft liegen mögen, in Wirtschaftlichkeitsberechnungen einfließen. Eins muss klar sein: Nur sichere Technologien sind wirklich ausgereift.

Föderalismus und effizienter Bevölkerungsschutz: ein Widerspruch?

Deutschland mit seinen zahlreichen Hilfs- und Rettungsorganisationen hat durchaus sehr positive Seiten im Bevölkerungsschutz zu verzeichnen. Die durch Ehrenamt und Hauptamt geprägte Struktur bei den Rettungsdiensten, THW und Feuerwehren ist grundsätzlich gut und sollte erhalten werden. Wir müssen aber auch klar sehen, dass unsere föderale Struktur, die viele unbestrittene Vorteile hat, sich im Bevölkerungsschutz als limitierender Faktor auswirken kann: bei Schadensfällen durch Naturereignisse, die häufig überregional wirken, können sich Zuständigkeitsprobleme auftun, die sich auf der kommunalen und Kreisebene fortsetzen und letztlich auch bei der internationalen Zusammenarbeit von Rettungsdiensten relevant werden können. Sich einfach mit dieser Situation zufrieden zu geben, ist keine Lösung. Sind wir für den Fall vorbereitet, dass auch wir einmal Hilfe benötigen werden? Ich sehe da einen dringenden Nachholbedarf, denn Deutschland ist nicht unverletzlich. So gut eine dezentrale Gefahrenabwehr ist: Je größer die Schadenslage, desto wichtiger ist ein zentrales übergeordnetes Krisenmanagement.



Bewältigungsfähigkeiten verbessern, Infrastrukturen robuster machen

Wir sollten meines Erachtens katastrophenvorbeugende Maßnahmen ganz oben auf die politische Agenda setzen. Dazu gehört auch, unsere Infrastrukturen robuster zu machen. Schon ein scheinbar trivialer Stromausfall würde in Deutschland nach wenigen Stunden große, nach wenigen Tagen massivste Sicherheitsprobleme hervorrufen. Der Verbesserung unserer Bewältigungsfähigkeiten dient auch die Modernisierung des Stromnetzes. Nun werden allenthalben Bedenken laut, dass die notwendigen Maßnahmen nur gegen hohe Widerstände von Seiten der Bürger durchzusetzen sein werden. Ich finde, da wird manches in der Diskussion überzeichnet. Die Verantwortlichen müssen sich in die Menschen hineinversetzen, die sagen: Wir wollen keine Starkstromleitung über unserem Kopf haben. Dann müssen Leitungen dort, wo es problematisch ist, unter die Erde verlegt werden, auch wenn das etwas teurer ist. Der Ausbau des Stromnetzes und seine Anpassung an erneuerbare Energien ist eine Zukunftsinvestition: sie wird sich über viele Jahrzehnte auszahlen und ist jede politische und wirtschaftliche Anstrengung wert.

Noch ein Wort zum so genannten Wutbürger, vor dem sich einige politische Vertreter zu fürchten scheinen: Dass Menschen sich darum kümmern, was in ihrer Region geschieht, ist zuallererst Ausdruck einer bürgerschaftlichen Wachheit und insofern etwas Positives. Menschen wollen Einfluss nehmen auf die Gestaltung ihrer Lebenswelt. Das ist ihr gutes Recht. Politik muss in einen Dialog treten und versuchen, solche Prozesse zu moderieren und die Menschen zu beteiligen. Zum Wutbürger wird nur derjenige, der das Gefühl bekommt, es wird über ihn hinweg regiert.

Bei allen Innovationen den Bürgerrechtsgesichtspunkt mitdenken

Ein ähnlich hoher Dialogbedarf mit den Menschen wird sich im Bereich des Smart Metering ergeben: Wenn es darum geht, die Stromversorgung mit Internettechnologie leistungsfähiger zu machen, sehe ich den Datenschutz als die Voraussetzung dafür, dass sich der Standort Deutschland in diesem Punkt weiterentwickelt. Wenn wir die fortschreitende Digitalisierung in der Energieversorgung wollen, so ist Datenschutz kein Hemmschuh, sondern die conditio sine qua non für einen Erfolg dieser verbesserten Technologien. Wir müssen smarte Infrastrukturen grundrechtskonform gestalten, damit sie ihr volles Potenzial für die Energieeffizienz entfalten und eine sichere, umweltschonende Stromversorgung gewährleisten können. Der Staat muss auf der einen Seite Sicherheit gewährleisten, auf der anderen Seite müssen sämtliche Maßnahmen der Sicherheitsgewährleistung rechtsstaatlich geerdet sein.

Dr. Konstantin von Notz, MdB
Berlin, im Januar 2012

Portraitfoto: von-notz.de, Foto Umspannwerk: Verband kommunaler Unternehmen e.V. (VKU)

Geleitwort des Vorstands

Das Undenkbare denken

Die Katastrophenkaskade in Japan hat Menschen auch hierzulande – von den Bürgern an den Bildschirmen bis zu den Verantwortlichen in Politik und den öffentlichen und privaten Institutionen des Bevölkerungsschutzes – verunsichert, zumindest aber nachdenklich gemacht:

- **Wie würden wir in einer Situation reagieren, die niemand für möglich gehalten hat?**
- **Wären unsere Einsatzkräfte ausreichend geschult und belastbar, um Katastrophen eines solchen Ausmaßes zu bewältigen?**
- **Wie ist es um die Selbsthilfefähigkeit unserer Bevölkerung bestellt?**
- **Welche Konsequenzen müssen in Deutschland aus den Ereignissen in Japan gezogen werden?**
- **Wie steht es allgemein um die Beherrschbarkeit von systemischen Risiken in einer immer komplexeren Welt?**

Wir haben unter dem Eindruck der Ereignisse nicht starr an unserem Jahresprogramm festgehalten, sondern die vorgenannten Überlegungen in unseren Foren widergespiegelt. Besonders im 13. Forum, das der vorliegenden Jahrespublikation seinen Namen geliehen hat: Das Undenkbare denken. Dabei haben wir bei der Auswahl der Vortragenden wiederum auf den bewährten Zusammenklang aus Politik und Behörden sowie Wirtschaft und Wissenschaft gesetzt. In den Beiträgen der Experten wurde deutlich: Hilflos sind wir nur, wenn wir uns vor dem Denken drücken, die Risiken ausblenden statt sie zu analysieren und zu bewerten. Es stehen Methoden und Techniken zur Verfügung, sich auf das „Undenkbare“ planerisch vorzubereiten, von der Szenarioentwicklung und Risikoanalyse, über szenariobasierte Übungen bis hin zu Computersimulationen. Dass im Rahmen der Risikoanalyse des Bevölkerungsschutzes auch die Interdependenzen von Kritischen Infrastrukturen stärker in den Blick genommen und mögliche kaskadierende Effekte mit bedacht werden müssen, darauf hat bereits das Grünbuch Öffentliche Sicherheit mit Nachdruck hingewiesen. Hinter diese Erkenntnis dürfen diejenigen, die sich in Sachen Bevölkerungsschutz engagieren, sei es öffentlich oder privat, gemeinnützig oder unternehmerisch, nicht zurückfallen.

Wir sehen in diesem Heft davon ab, weitere Katastrophenszenarien zu entwickeln. Wir fragen also nicht: Was könnte alles schiefgehen? Sondern wir fragen: Was geht, wenn gar nichts mehr geht? Welche Ersatzsysteme, Redundanzen und Systemverstärkungen müssten noch geschaffen werden? Welche Bewältigungspotenziale stehen uns heute bereits zur Verfügung? Welche können mit wenig Aufwand, ggf. allein durch mehr und klügere Kooperation der öffentlichen und privaten Akteure geschaffen werden?

Im ersten Teil der Publikation schildern wir drei Beispiele von Verwundbarkeit unserer hochtechnisierten Gesellschaft und loten Möglichkeiten zu deren Bewältigung aus: Leben in schädlicher Umwelt, Leben ohne Strom, Leben mit dysfunktionaler IKT. Flankiert werden die Problembeschreibungen von erhellenden Statements, die den Vorträgen unserer Forumsredner des Jahres 2011 entnommen sind oder am Rande der Veranstaltungen aufgefangen wurden.

Für den zweiten Teil haben wir nicht nur Akteure der öffentlichen Sicherheit um eine Stellungnahme zum „Undenkbaren“ gebeten, sondern auch Vertreter aus Wirtschaftsverbänden, ihre Sicht auf Bewältigungsmöglichkeiten in krisenhaften, für die öffentliche Sicherheit relevanten Situationen darzulegen. Die hohe Bereitschaft, sich zu diesem Thema zu äußern, werten wir als Ausdruck dafür, dass die öffentliche Sicherheit in zunehmendem Maße ganzheitlich wahrgenommen wird.

Der Gewinn, den wir uns aus der Jahrespublikation erhoffen, ist: sowohl Vertretern der Politik und der öffentlichen und gemeinnützigen Institutionen des Bevölkerungsschutzes die Problemlösungskompetenz in der Wirtschaft nahezubringen, als auch die Entscheider in der Wirtschaft noch stärker als bisher für die Belange der öffentlichen Sicherheit zu sensibilisieren. Sofern das vorliegende Heft dazu beiträgt, einem breiten Gedankenaustausch praktische Verbesserungen der öffentlichen Sicherheit folgen zu lassen, sehen wir das als ein gutes Ergebnis an.

Berlin, im Januar 2012

Prof. Dr. Hermann J. Thomann
Vorstandsvorsitzender

Axel Dechamps
Stellvertr. Vorstandsvorsitzender

Clemens Graf von Waldburg-Zeil
Schatzmeister

Dr. Sandra Schulz
Programmvorstand

Portraitfotos: ZOES

Das Undenkbare denken

Verwundbarkeiten und Bewältigungsmöglichkeiten in komplexen Lagen

Marie-Luise Beck,
Projektkoordinatorin
Forschungsforum
Öffentliche Sicherheit

Dr. Clemens Gause,
Geschäftsstelle Zukunftsforum
Öffentliche Sicherheit

von Marie-Luise Beck und Dr. Clemens Gause

Die klassische Risikobestimmung richtet sich nach Eintrittswahrscheinlichkeit und Schadensausmaß. Diese rein quantitative Methode kann dazu verführen, Risiken mit geringer Eintrittswahrscheinlichkeit als vernachlässigbar zu bewerten, ohne Parameter wie Ungewissheit oder ein gesellschaftlich nicht tolerierbares Schadensausmaß zu berücksichtigen. Die Folge ist, dass das Auftreten solcher „schwarzer Schwäne" als undenkbar gilt und eine Auseinandersetzung mit den Folgen und Bewältigungsmöglichkeiten unterbleibt. Sich eher mit Bewältigungsstrategien für einfache und bekannte Ereignisse zu beschäftigen, erhöht zwar das Gefühl der Kontrolle über die Zukunft, bedeutet aber auch, besonders hart von unvorhergesehenen Ereignissen getroffen zu werden. Das Zukunftsforum Öffentliche Sicherheit hat aus einer theoretisch unendlichen Zahl möglicher Ereignisse drei gewählt, in denen komplexe, unvorhergesehene Lagen neue Wege der Bewältigung erfordern.

Bei einer gleichzeitigen Bewältigung mehrerer Schadensereignisse kommen alle Rettungssysteme sehr schnell an ihre Leistungsgrenzen. Deshalb muss die genaue Leistungsfähigkeit und Ausdauer aller Schutzsysteme geprüft und erprobt werden.

Ralph Stühling, Feuerwehrverband

Leben in schädlicher Umwelt

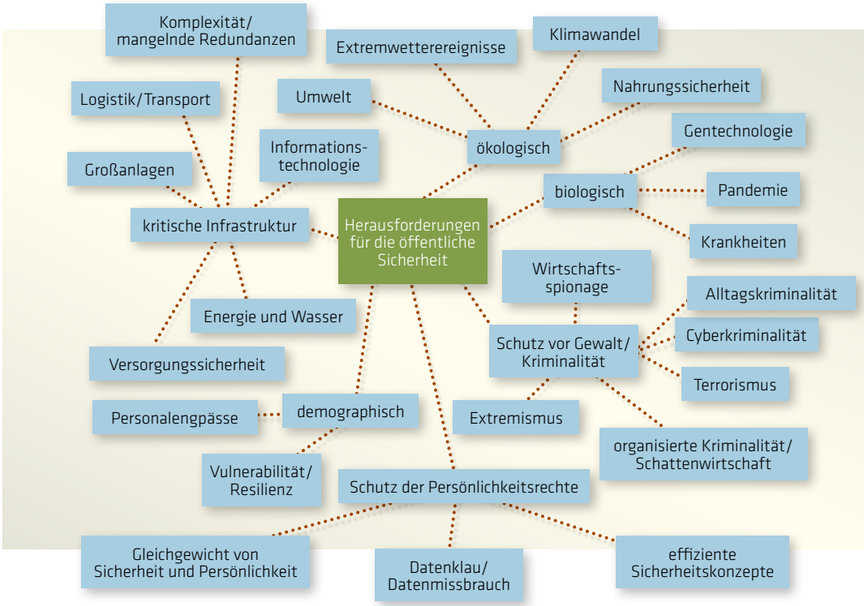
Nach dem schweren Erdbeben, der Flutwelle und den Reaktorschäden in Fukushima hat das Zukunftsforum Öffentliche Sicherheit nach den Konsequenzen für den Bevölkerungsschutz und die öffentliche Sicherheit in Deutschland gefragt. Es ging nicht um die Bewertung der Risiken eines Kernkraftwerkes, sondern um die Diskussion der Bewältigungspotenziale des Bevölkerungsschutzes in Deutschland. Die zentrale Herausforderung in einem solchen Schadensfall liegt in der kurzfristigen Evakuierung einer großen Anzahl von Menschen und ihrer Unterbringung sowie – sobald, wie im Falle von Fukushima, die Dimension der Kontamination bekannt ist – in der langfristigen Unterbringung der Evakuierten. Die Zweifel daran, dass die Bevölkerung einer Großstadt oder Mega-City evakuiert und untergebracht werden kann, sind groß. Eine Warnung an die Bevölkerung kann man aber nur verantworten, wenn eine Evakuierung überhaupt machbar ist um Massenpaniken und zusätzliches Chaos zu vermeiden.

Die Lebensmittelversorgung ist gut, flexibel und im Alltag sicher. Sie kann aber durch ihre extreme Abhängigkeit von der Infrastruktur und wegen der Unterschiedlichkeit der Akteure im Katastrophenfall schnell kritisch werden.

Dr. Helmut Grimm, Tengelmann

Es gibt einen dringenden Bedarf, die Wechselwirkungen zwischen Infrastrukturen zu verstehen. Hierfür ist sowohl ein Ausbau der Modellierungs-, Simulations- und Analyse-Kapazitäten erforderlich als auch eine systematische, umfassende und fortdauernde Daten erhebung über KRITIS-Ausfälle und Kaskaden in Deutschland.

Dr. Erich Rome, Fraunhofer IAIS



Um die Potenziale und Fähigkeiten eines westlichen Industrielandes zu beleuchten, wurden folgende Fragen durch die Expertenbeiträge und die anschließende Diskussion bearbeitet:

1. Durch welche Maßnahmen ist sichergestellt, dass Menschen unverzüglich, gezielt und verständlich gewarnt werden können?
2. Sind wir auf einen Massenanfall von sehr vielen und eventuell kontaminierten Verletzten ausreichend vorbereitet? Stehen genügend Dekontaminations- und Behandlungskapazitäten zur Verfügung?
3. Sind die in Großschadenslagen eingesetzten Kräfte und Krankenhäuser ausreichend ausgestattet und qualifiziert?
4. Welche Vorsorge ist für eine möglicherweise notwendige langfristige Evakuierung der Bevölkerung getroffen worden?
5. Welche Vorsorgemaßnahmen müssen für das Krisenmanagement über einen längeren Zeitraum bereitgehalten werden?
6. Wie kann die Fähigkeit der Bevölkerung, sich selbst und anderen auch in lang anhaltenden Schadenslagen zu helfen verbessert werden?

Wenn wir uns heute, 10 Jahre nach dem 11. September 2001 und auch aus Anlass der Ereignisse in Japan und angesichts geänderter Rahmenbedingungen fragen, wie wir einen modernen und zukunftsfähigen Bevölkerungsschutz erhalten und voranbringen können, müssen wir die europäische Dimension und eine immer stärkere Vernetzung der Mitgliedstaaten mit berücksichtigen. In der Vergangenheit haben wir uns noch zu wenig die Frage gestellt, wo wir selbst im Bevölkerungsschutz von der EU profitieren können.

Norbert Seitz, BMI

Wir sollten, weg von Institutionen, mehr über die Betroffenen in einer Katastrophe sprechen. Wie können sie sich selbst helfen? Sie müssen eigenständig das Richtige tun. Dies setzt eine Schärfung des Risikobewusstseins und eine Verbesserung der Selbsthilfefähigkeiten voraus.

Clemens Graf von Waldburg-Zeil, Deutsches Rotes Kreuz

Braucht es (...) erst Katastrophen, um die Richtung zu ändern? Und ist die Richtung nach Katastrophen „richtiger", oder entscheidet sich „Richtigkeit" nur entlang der Zeit, in der Katastrophen ausbleiben?

Prof. Dr. Wolf R. Dombrowsky, Steinbeis-Hochschule Berlin

Portraitfoto Beck: FOES, Portraitfoto Gause: ZOES

Von einer Sensibilisierung des Energierechts speziell für die Problematik „Kritische Infrastrukturen“ kann nur ansatzweise gesprochen werden.

Prof. Dr. Johann-Christian Pielow, Ruhr-Universität Bochum

Leben ohne Strom

Die zunehmende Abhängigkeit moderner Gesellschaften von funktionierenden Infrastrukturen treibt die Entwicklung von Smarten Infrastrukturen voran. Über die technische und informatorische Vernetzung können beispielsweise die heterogen verfügbaren erneuerbaren Energien effizienter genutzt und das erklärte gesellschaftliche Ziel der Unabhängigkeit von fossilen Energieträgern realisiert werden. Der Preis ist jedoch eine erhöhte Vulnerabilität durch Komplexität und Koppelung der Systeme sowie eine Vervielfältigung der Akteure.

Die zentralen Prozesse einer modernen Gesellschaft – Information und Kommunikation, Verkehr und Logistik, Notfall- und Rettungswesen – sind ohne Energieträger, vor allem ohne Strom, nicht realisierbar. Fallen diese Kritischen Infrastrukturen aus, so trifft das nach und nach die ganze Gesellschaft in ihren Kernbereichen. Das zu erwartende immense Schadensausmaß macht den großräumigen und langfristigen Stromausfall wegen seiner gestiegenen Eintrittswahrscheinlichkeit zu einer ernsthaften Bedrohung.

Der Betrieb von Notstromanlagen kann, bedingt durch die Versorgungsknappheit mit Treibstoff, nur zeitweise erfolgen, aber auch die Notstromgeräte selbst wären schon ein extrem knappes Gut. Es besteht ein hohes Risiko für Menschen, Staat und Wirtschaft: Ein unmittelbar existenzielles zum Beispiel für Kranke, die zu Hause an mobilen Beatmungs- oder Dialysegeräten versorgt werden. Ebenso lebensbedrohlich können Versorgungsausfälle, verursacht durch Lieferunterbrechungen, sein; aber auch Sachschäden, Verdienst- und Umsatzausfälle aller Art müssen antizipiert werden. Die Versorgung mit Bargeld wäre ebenfalls gestört. Industriebetriebe, Dienstleister wären massiv betroffen und mittel- bis langfristig auch die Landwirtschaft, Viehhaltung und Ackerbau. Die für eine Krise typische Suche nach den Ursachen bzw. den Verantwortlichen könnte zu einem Vertrauensverlust der Bevölkerung in Staat und Wirtschaft führen. Je länger ein Stromausfall dauert, desto deutlicher werden die Folgen und Folgefolgen sichtbar: immer mehr andere stromabhängige Infrastrukturen würden zusammenbrechen. Es würde zunehmend schwierig bis unmöglich, sensible technische Anlagen in der Chemie- oder der Stahlproduktion wieder hochzufahren. Es kann beispielsweise zum Durchschmelzen von Hochöfen und zu Bränden kommen. Die Folgewirkungen reichten in jedem Fall über das Ereignis hinaus.

Die geschilderte Lage – ein überregionaler Stromausfall – ist angesichts zunehmenden Stromhandels, der natürlichen Schwankungen erneuerbarer Energieressourcen, deren dezentraler Einspeisung und der Abschaltung von Kernkraftwerken nicht mehr so undenkbar wie noch vor 15 Jahren. Um die Vulnerabilität zu senken, ist es unerlässlich, den Netzausbau voranzutreiben. Flankierend dazu muss in der Bevölkerung für Verständnis geworben werden, dass die gesellschaftlich akzeptierte Energiewende nur mit einem der Energieerzeugung angepassten Netz und Regulation im Strommarkt bewerkstelligt werden kann.

Die Sicherstellung eines bedarfsgerechten Ausbaus der Stromübertragungsnetze ist eine der wesentlichen Aufgaben zur langfristigen Gewährleistung der Versorgungssicherheit in Deutschland.

Iris Henseler-Unger, Bundesnetzagentur

Ein weiteres Innovationsfeld, für die gesellschaftliche Akzeptanz erst noch hergestellt werden muss, ist die Verbindung der Elektrizitätsverteilernetze mit moderner IKT (Smart Grids). In die Planung eines bundesweiten Smart Grids ebenso wie bei der Einführung von Smart Metering müssen Sicherheitsüberlegungen von Anfang an integriert und gesetzgeberisch begleitet werden. Hier gilt es, den Zielkonflikt im Energiewirtschaftsrecht zwischen Sicherheit/Ausfallsicherheit auf der einen und Umweltschutz sowie Wirtschaftlichkeit auf der anderen Seite aufzulösen.

Das derzeitige Vertrauen in die Verbrauchsmesstechnik darf nicht verspielt werden. Die Anforderungen an Datenschutz und Datensicherheit sind deshalb sehr hoch anzusiedeln und zuverlässig umzusetzen. Beides muss vor der Einführung von Smart Metering sichergestellt und einer breiten Öffentlichkeit verständlich kommuniziert werden.

Dr. Michael Arzberger, Power Plus Communications

Leben mit dysfunktionaler IKT

Die moderne Informations- und Kommunikationstechnologie ist zu einem unverzichtbaren Bestandteil von Wirtschaft und Gesellschaft geworden. In einigen Branchen wie dem Telekommunikations- oder dem Finanzbereich ist IKT mittlerweile fast alleiniges Betriebsmittel. Nachdem diese Technik zunächst vor allem Effizienzgewinne und Renditen bescherte, rücken zunehmend Fragen der Sicherheit in den Vordergrund. Zum einen weil Kriminelle das „Renditepotenzial“ des Internet für sich entdeckt haben, zum zweiten weil die Verwundbarkeitspotenziale der IKT auch das Interesse von Staaten geweckt haben, und zum Dritten weil aufgrund der gestiegenen Komplexität gepaart mit Intransparenz des Systems und unzureichenden Sicherheitsstandards technisches Versagen wahrscheinlich ist. Mit welchen Risiken wir jetzt schon leben und welche weiteren Risiken sich abzeichnen ist dabei alles andere als klar.

Fest steht: die fortschreitende Digitalisierung und informationelle Vernetzung birgt neben großartigen Möglichkeiten zunehmend beängstigende und für den Wirtschaftsstandort Deutschland hoch relevante Risiken und Gefahren. Neben einer fortwährenden Bestandsaufnahme gilt es, neue Strategien im Umgang mit der Unsicherheit in der digitalen Welt aus dem Bereich der Politik und Verwaltung, der Wirtschaft und der Wissenschaft zum Thema IKT-Sicherheit und Internet zu entwickeln.

Die hohe Abhängigkeit von IKT wird in den kommenden Jahren weiter steigen. Damit werden Störungen – insbesondere bei kritischen Prozessen – zunehmend intolerabel. Die eingesetzten IKT-Architekturen werden gleichzeitig komplexer. Damit sind sie tendenziell fehleranfälliger und störungsempfindlicher. Die Herausforderung für die kommenden Jahrzehnte besteht in einer Nachjustierung auf folgenden Ebenen: Zum einen muss es zu einer Debatte um Schutzziele kommen, beispielsweise hinsichtlich der Ausfallsicherheit des Notrufs. Zum zweiten müssen wirtschaftliche Anreizsysteme für Sicherheit geschaffen werden; nicht nur Preis, Geschwindigkeit oder Komfort, sondern auch Sicherheit muss ein klarer Wettbewerbsvorteil sein. Zum Dritten müssen diese Sicherheitsgewinne durch Aufklärung, Gütesiegel oder Zertifizierung auch für Nicht-Experten (und das ist fast jeder) erfahrbar und transparent gemacht werden. Und schließlich muss sich Politik, Wirtschaft und Gesellschaft mehr Gewissheit über das Ausmaß der Schäden verschaffen. Während die Sicherheitsindustrie oder auch die Medien die Risiken tendenziell übertreiben, scheinen andere Unternehmen sie eher zu untertreiben.

Michael Hange
Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

Statement Michael Hange, BSI

Vertrauen ist der Pfeiler, auf dem Kritische Infrastrukturen ruhen: Auch das Internet

Bedrohungen im Cyber-Raum sind deshalb so tückisch, weil sie im Gegensatz zu den Gefahren der realen Welt unsichtbar sind und daher oft unterschätzt werden. Das senkt die Bereitschaft vieler Internetnutzer, sich dagegen zu wappnen. Tatsache ist: Die Bedrohungen aus dem Internet, die viele schon als eine Art systemimmanente Belästigung hinnehmen, wird andauern und zunehmen. Die Motivation der Cyber-Kriminellen – das vergleichsweise einfach und risikoarm zu erbeutende Geld – ist zu hoch.

Aus der IT-Perspektive können wir heute anhand der technologischen Entwicklungen antizipieren, was uns an Bedrohungen in zwei bis drei Jahren erwartet und uns entsprechend vorbereiten. Verschiedene methodische Herangehensweisen wenden wir hierzu an: Die Entwicklung von Szenarien sowie szenariobasierte Übungen, wie zuletzt die Bund-Länder-übergreifende LÜKEX, die Analyse der Gefährdungslagen, die Frühwarnung und schließlich die Prävention. Gerade bei der Prävention können alle Akteure der Informationsgesellschaft – Unternehmen, Organisationen sowie Bürgerinnen und Bürger – ihren Beitrag leisten. Allein die Reaktion greift zu kurz. Sicherheitsgestaltung darf nicht erst dann einsetzen, wenn IT-Sicherheitsvorfälle bereits geschehen und Schäden zu verzeichnen sind.

Es wird auch in Zukunft darum gehen, Vertrauen in die für unsere Gesellschaft wichtige Infrastruktur Internet aufzubauen und zu erhalten. Vergleichen wir dies mit der Verkehrsinfrastruktur: Als Autofahrer tue ich das meine, um mich sicher im Straßenverkehr zu bewegen und um andere nicht zu gefährden: ich sorge dafür, dass mein Auto verkehrstüchtig ist, schnalle mich an, halte mich an die Verkehrsregeln. Aber ich vertraue auch darauf, dass die anderen Verkehrsteilnehmer sich an die Regeln halten, dass die Ampeln richtig funktionieren und die Straßen in gutem Zustand sind.

Damit die Dienstleistungsangebote im Internet weiterhin vertrauensvoll genutzt werden können, müssen alle Beteiligten dazu beitragen, dieses Vertrauen zu rechtfertigen. Das kann geschehen, indem Sicherheitsmaßnahmen transparent gemacht werden und Anbieter ihre Dienste zertifizieren lassen. Dies gilt auch für neue technologische Innovationen in der IT oder neue Geschäftsmodelle wie das Cloud Computing.

Portraitfoto: ZOES, Klaus Dombrowsky

Sicherheitsforschung ist Grundlagenforschung. Die drei Bereiche Sicherheit, Virtualisierung und zuverlässige Handhabbarkeit der Geräte und Plattformen müssen als Einheit begriffen werden. Nur mittels eines solchen holistischen Ansatzes lassen sich verlässlichere Sicherheitsarchitekturen schaffen.

Prof. Dr. Jean-Pierre Seifert, TU Berlin

Mit einer Plattform „Dialog Sicherheit im Netz" sollte die Grundlage für eine themenorientierte Kooperation von Wissenschaft, Staat und Wirtschaft mit strategischer Ausrichtung geschaffen werden.

Lutz Diwell, Staatssekretär a. D.

Die Mittel der Wahl wären Forschung aber auch eine Veröffentlichungspflicht von Ereignissen, wie sie mit dem Cyber Incident Disclosure diskutiert werden.

Auf technischer Ebene gilt es Software, Hardware und IKT-Architekturen so weiterzuentwickeln, dass sie ein verlässliches Instrument zur Prozessunterstützung darstellen bzw. bleiben. Eine Strategie liegt in der Entnetzung besonders sensibler Bereiche. Gleichzeitig muss sichergestellt werden, dass IKT auch bei Störungen handlungsfähig bleibt. Hierzu sollten IKT-Infrastrukturen verstärkt redundant ausgelegt sein. Zusätzlich sollten möglicherweise alte proprietäre Technologien bei Bedarf gestuft reaktiviert werden können. Der Mix unterschiedlicher Funktionalität, verschiedener Stofflichkeit, bei gleichem Produktionsergebnis, macht ein System relativ robust. Zu beachten ist aber, dass jede Redundanz ihre eigenen Schwächen und Angriffspunkte hat. Auch durch eine echte Redundanz (also einem funktional und, wenn möglich sogar örtlich und stofflich anders aufgebautem System) kann die Verletzbarkeit nur bedingt eingedämmt werden. Nur in Grenzen kann ein System als zumindest vergleichsweise oder relativ robust charakterisiert werden. Zudem verliert es im Rückfall stets Fähigkeiten, jedoch muss dies nicht notwendigerweise mit einem vollständigen Informations- oder Fähigkeitsverlust einhergehen, sofern die Redundanz die Fähigkeiten zumindest teilweise aufrechterhalten oder mit etwas Zeitverzug partiell wieder zusammensetzen oder rekonstruieren kann.

Aufgrund dessen sind Systeme bereits im jeweiligen Planungsprozess gegen unterschiedlich wirkende Störfaktoren mehrfach echt redundant anzulegen. Unter Umständen können dadurch auch bisher nicht vollständig wahrgenommene und erfasste Pfadabhängigkeiten aufgedeckt, das Ausfallrisiko durch die Anlage energetisch und technisch anders abhängiger Strukturen breiter gestreut und damit minimiert werden. Breite Aufstellung bildet einen wesentlichen Schlüssel.

Sicherheit muss damit als gemeinsame Aufgabe aller Akteure verstanden und geschultert werden. Die Vernetzung des in allen gesellschaftlichen Bereichen vorhandenen Know-hows und der unterschiedlichen Analyse- und Handlungsperspektiven kann dazu beitragen, Konzepte zur Bypassfähigkeit von lebenswichtigen Prozessen einer Gesellschaft zu erarbeiten. Eine Verstetigung und stärkere Institutionalisierung des Dialogs zwischen Politik, Wissenschaft und Wirtschaft – auch das gehört zu den lessons learned der Vergangenheit - ist für alle Beteiligten ein Gewinn und für die öffentliche Sicherheit ein Gebot der Vernunft.

IT-Sicherheit ist unverzichtbar, auch wenn sie Geld kostet. Prävention ist aber auch hier günstiger als der nicht ganz unwahrscheinliche Schadensfall.

Cornelia Rogall-Grothe, BMI

Die Entwicklung des Cybercrime ist durch zunehmende Kommerzialisierung, Internationalisierung, Professionalisierung und womöglich auch politische Radikalisierung gekennzeichnet. Für die wirksame Bekämpfung der neuen Kriminalitätsphänomene im Internet ist eine strategische und konzeptionelle Ausrichtung der Polizei in allen Aufgabenfeldern erforderlich.

Helmut Picko, LKA NRW

Man muss sich darüber klar sein: Es gibt keine perfekte Sicherheit. Sicherheit ist ein Prozess und kein käufliches Produkt: Sicherheit kann nur entstehen, wenn sich Verwaltung, Benutzer, Integratoren und Zulieferer gemeinsam der Sicherheit als einer fortlaufenden Aufgabe stellen."

Dr. Johann Fichtner, Siemens

Albrecht Broemme, Präsident THW

Statement Albrecht Broemme

Unser Credo: Zukunftsbilder entwerfen, um in der Gegenwart das Richtige zu tun

Vom THW wird zu Recht mehr erwartet, als zwischen den Einsätzen einfach nur auf die nächste Katastrophe zu warten. Deswegen gehört es zu unserer Denkweise, auch das Undenkbare zu skizzieren, Szenarien gedanklich durchzuspielen, zu planen und zu üben, und schließlich auch die eigene Leistungsfähigkeit zu bemessen. Zu wissen, was man leisten kann, ist die beste Voraussetzung für erfolgreiche Einsätze. Dazu gehört auch, die eigenen Grenzen zu kennen.

Falsche Erwartungen zu wecken, kann gefährlich sein

Es gibt eindeutige Anhaltspunkte, die zur Bemessung der Leistungsfähigkeit dienen können: Da ist zum einen der qualitative Aspekt (Wie ist der Ausbildungsstand der Einheiten?), zum anderen der quantitative Aspekt (Wie viele Helfer stehen zur Verfügung, gibt es Mehrfachbesetzungen und Kompensationsmöglichkeiten bei Personalmangel? Wie sieht es mit der Geräteausstattung aus?)

Selbst alle mobilen Notstromaggregate des THW zusammengenommen können kein Kraftwerk ersetzen. Wir sind lediglich in der Lage, punktuell und an besonders kritischen Punkten die Stromversorgung aufrechtzuerhalten, wenn andere Ersatzanlagen versagen. Hier gilt die Maxime: Kenne deine Grenzen und kommuniziere sie nach außen. Sonst gibt es falsche Erwartungen nach dem Motto: Großflächiger Stromausfall? Macht ja nichts, das THW wird's schon richten.

Katastrophenschutz ist immer Gemeinschaftsarbeit

Das THW kann nicht alles alleine stemmen. Wir sind auf die Zusammenarbeit mit anderen wichtigen Akteuren der öffentlichen Sicherheit angewiesen.

Nehmen wir das Beispiel einer Unterbrechung der Trinkwasserversorgung in Berlin: Das THW könnte in einer Krisensituation nicht die ganze Stadt mit Trinkwasser versorgen; unser Limit liegt, das wissen wir anhand der Leistungsfähigkeit der einzelnen Fachgruppen, großzügig berechnet bei 400.000 Einwohnern. Dabei läge die Verteilung des Trinkwassers nicht beim THW, sondern würde in Gemeinschaftsarbeit erledigt, beispielsweise durch die Berliner Wasserbetriebe, die im Katastrophenschutzmanagement sehr gut aufgestellt sind.

Das System des Zusammenwirkens baut auf regelmäßigen Gesprächen auf. Man tauscht sich mit den Akteuren aus, lernt ihre Leistungsfähigkeit und die Anforderungswege kennen, weiß um bereitstehende Mittel und erfährt, wie man sich gegenseitig unterstützen kann. Beispielsweise könnte das THW bei Personalengpässen Einsatzkräfte beistellen, die Wasserbetriebe könnten dann die Gerätebeistellung übernehmen. Wenn Akteure des Katastrophenschutzes ihre Visitenkarten erst auf den Trümmerhaufen austauschen, ist etwas massiv schiefgelaufen.

Private Betreiber von KRITIS: Berührungspunkte kennen und nutzen

Zu den privaten Betreibern von kritischen Infrastrukturen ergeben sich Anknüpfungspunkte ganz von selbst, nämlich durch Mitarbeiter dieser Unternehmen, die sich ehrenamtlich beim THW oder bei den Feuerwehren engagieren. Auf diesen Verbindungen bauen wir auf: Das THW hat Vereinbarungen mit der RWE geschlossen und mit E.on vorbereitet, auch einige lokale Energieverteiler sind bereits mit an Bord.

Vereinbart werden zum Beispiel gemeinsame Übungen oder Planbesprechungen, aber wir prüfen auch, ob Mitarbeiter des Energieversorgers im Katastrophenfall eher dort gebraucht oder nützlicher beim THW eingesetzt werden.

Do you speak Denglish? Im Ernstfall sprachlos

Ein Manko sehe ich darin, dass Deutschland noch nicht ausreichend auf den Einsatz ausländischer Hilfskräfte hier vorbereitet ist. Auch das muss geplant und geübt werden. Es darf nicht als unwahrscheinliches Szenario beiseite geschoben werden, dass auch Deutschland einmal Hilfe brauchen könnte. Schon mit Englisch als internationaler Sprache der Katastrophenschützer sieht es in Deutschland eher dürftig aus. Hier würden viele unserer inländischen Helfer schnell keine richtigen Antworten auf wichtige Fragen bekommen – die Kommunikation wäre problematisch.

Portraitfoto: BA THW

Zuverlässige Stromversorgung als eine Säule der öffentlichen Sicherheit

Hildegard Müller, Vorsitzende der Hauptgeschäftsführung des BDEW

Interview mit Hildegard Müller,
Bundesverband der Energie- und Wasserwirtschaft

Frau Müller, die Bürger werden in den Medien auf länger dauernde Stromausfälle eingestimmt. Sind das Schreckensszenarien, die für wohligen Schauer in der Sofaecke sorgen sollen, oder sehen Sie einen konkreten Gefährdungshintergrund?

Zunächst möchte ich betonen, dass Deutschland die zuverlässigste Stromversorgung im weltweiten Vergleich hat. Die deutschen Energieunternehmen tun alles dafür, jeden Tag, rund um die Uhr, diesen hohen Standard zu halten. Denn die sichere Versorgung mit Strom und Gas ist ein wesentlicher Garant dafür, den Erfolg unseres Industriestandortes auch in Zukunft zu gewährleisten. Die Energiewende stellt die Netzbetreiber jedoch zunehmend vor die Herausforderung, das Stromnetz zu stabilisieren. Die Erneuerbaren als zweitwichtigster Energieträger – sie decken bereits einen Anteil von 20 Prozent des Strombedarfs – machen das Stromangebot zunehmend volatiler. Die Ausbeute von Windstrom und Photovoltaik schwankt je nach Witterung. Gleichzeitig muss immer mehr Strom von Nord nach Süd transportiert werden, weil insbesondere an der Küste große Windparks entstehen, deren Strom in den Verbrauchszentren im Süden des Landes gebraucht wird. Die Netzbetreiber müssen aus diesem Grund immer öfter eingreifen, damit Stromangebot und -nachfrage zueinander kommen.

In den kommenden Jahren wird es darauf ankommen, dass sowohl der Gesetzgeber als auch die Regulierungsbehörden die nötigen Rahmenbedingungen schaffen und die Bevölkerung die nötige Akzeptanz für die Infrastrukturprojekte aufbringt: Versorgungssicherheit muss eines der zentralen energiepolitischen Ziele in Deutschland bleiben. Deshalb sollte die Regierung auch die richtigen Investitionsanreize für den Netzausbau setzen. Er ist aktuell die entscheidende Determinante dafür, dass die Energiewende in Deutschland gelingt.

Beim Thema Netzausbau hat der BDEW in den vergangenen Monaten immer wieder einen gestiegenen Handlungsdruck konstatiert. Welche Schritte stehen jetzt darüber hinaus an?

Die Ziele sind klar und werden von der deutschen Energiewirtschaft mitgetragen: an erster Stelle steht der Ausbau der Erneuerbaren Energien zum Leitsystem der Zukunft und deren Integration in das bestehende System. Das wiederum zieht den dringend notwendigen Ausbau der Verteil- und Übertragungsnetze nach sich. Die Energieeffizienz muss gesteigert werden und es gilt, die Forschungsförderung für Speicher und neue Technologien zu verbessern. Auch die Zukunft der konventionellen Erzeugung in Deutschland braucht intensive Diskussion. Die Politik arbeitet aktuell an rund zwei Dutzend Gesetzen und Verordnungen, die im Zuge der Energiewende noch angepasst oder neu verfasst werden müssen. Die Energiewende ist kein Selbstläufer, die Arbeit zur Umsetzung geht jetzt erst richtig los. Es fehlt allerdings noch in einigen Bereichen an einem konkreten Fahrplan. Die Energieversorgung muss sicher und bezahlbar bleiben. Im nächsten Jahr werden die Verbraucher für den Ausbau der Erneuerbaren voraussichtlich die Rekordsumme von 14,1 Milliarden Euro aufbringen. Meines Erachtens müssen wir uns kurzfristig die weiteren Auswirkungen des EEG genau anschauen, bei Fehlentwicklungen eingreifen und die Förderung falls nötig erneut anpassen. Mittelfristig muss es darum gehen, die Verbraucher zu entlasten und die regenerative Stromerzeugung in den Markt zu integrieren. Was wir brauchen, ist ein schrittweiser Systemwechsel und kein Hau-Ruck-Verfahren. Im Moment wird erneuerbarer Strom erzeugt, wann immer es möglich ist. Es muss aber schon bald darum gehen, dass auch die Erneuerbaren den Strom dann liefern, wenn er wirklich gebraucht wird. Falls wir diese Systemverantwortung nicht schaffen, können wir das Ziel, ein tragfähiges Energieversorgungssystem aus Erneuerbaren aufzubauen, nicht erreichen.

Die Energiewende gibt es nicht zum Nulltarif. Wie beurteilen Sie in diesem Zusammenhang die Faktoren für Strompreiserhöhungen?

Ich warne immer davor, schnell Zahlen in den Raum zu werfen, denn es gibt zahlreiche Einflussfaktoren beim Thema Strompreisentwicklung. Im Wesentlichen sind es drei: Zunächst die staatlichen Steuern und Abgaben, deren Anteil am Strompreis liegt mit 46 Prozent für private Haushalte inzwischen auf einem Rekordniveau. Zweitens gibt es die Entwicklungen am Großhandelsmarkt, beim Service und Vertrieb. Dieser Anteil liegt im Durchschnitt bei 34 Prozent. Und drittens liegt der Anteil der Netzentgelte derzeit bei rund 20 Prozent. Durch den Ausbau der Erneuerbaren Energien müssen mehr Netze gebaut werden. Das schlägt sich zum Teil schon jetzt in den Strompreisen nieder. Die Tendenz der Preise ist im Zuge der Energiewende steigend. Aber niemand kann heute seriös sagen, was das am Ende genau kosten wird. Die deutschen Ausbauziele im Bereich der Erneuerbaren Energien haben Auswirkungen auf die gesamte Volkswirtschaft, auf jeden Bürger, dennoch müssen die Verbraucher künftig vor einer Kostenexplosion bewahrt bleiben. Parallel wird entscheidend sein, wie die Politik die Verbesserung der Energieeffizienz gestaltet. Wenn den Bürgern und Industrien geholfen wird, Energie einzusparen, ist das der richtige Weg.

Wie beurteilen Sie die Innovations- und Investitionsbereitschaft der Branche?

Klar ist: Für die erfolgreiche Umsetzung der Energiewende brauchen wir eine Fülle von Innovationen. Denn es werden neue Lösungen in den Bereichen Netze, Erzeugung, Klimaschutz, Effizienz, Mobilität und Speicherung erforderlich sein. Dabei sollten wir jeweils nicht auf eine einzelne Technologie setzen. Aus diesem Grund machen wir uns für eine verbesserte Forschungsförderung stark und begrüßen die Aktivitäten der Bundesregierung in diesem Punkt. Auch im Bereich der Erneuerbaren sollten weitere Technologien erforscht und gefördert werden. Entscheidend für den weiteren Ausbau der Erneuerbaren wird sein, wie schnell es gelingt, sie in das bestehende Versorgungssystem einzubinden. Hierzu stehen in den kommenden Jahren milliardenschwere Investitionen an. Eine Studie des Bundesverbandes der Energie- und Wasserwirtschaft hat bereits im vergangenen März einen Investitionsbedarf von bis zu 27 Milliarden Euro allein beim Netzausbau ermittelt. Alles muss einhergehen mit der Modernisierung des konventionellen Kraftwerkparks.

Ist in der Bevölkerung ausreichend Verständnis für notwendige Infrastrukturmaßnahmen vorhanden?

Wir sehen in der gesellschaftlichen Akzeptanz ganz klar einen Schlüsselfaktor für die Energiewende. Fakt ist: Das Gesicht unseres Landes wird sich verändern. Die Energieerzeugung wird sichtbarer. Am stärksten deutet sich das durch die großen Windparks an, die überall entstanden sind. Die Zahl der Anlagen hat sich in den letzten zehn Jahren weit mehr als verdoppelt. Vielerorts haben sich Bürgerinitiativen gebildet, die gegen eine „Verspargelung" der Landschaft oder neue Stromtrassen aufbegehren. Eine tiefgreifende Infrastrukturskepsis ist hier zu beobachten: Energiewende ja, aber nicht vor meiner Haustür. An dieser Stelle muss das gemeinsame Gespräch gesucht werden. Der BDEW und seine Mitgliedsunternehmen setzen sich dafür ein, Konflikte zu benennen, Branchenlösungen zu erarbeiten und alle Interessengruppen an der Umsetzung des Energiekonzeptes zu beteiligen.

Die Stromversorgung ist Kritische Infrastruktur, deren Schutz das besondere Augenmerk des Staates und der Öffentlichkeit gilt. Wie bringt sich der BDEW in die Diskussion um den Schutz Kritischer Infrastrukturen ein?

Die Energiewirtschaft steht insbesondere zum Thema Cyberabwehr im engen Kontakt mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI). Konkret geht es um die Themen Sicherheit der IT-Infrastruktur und Datenschutz. Neben den datenschutzrechtlichen Fragen geht es auch um die Umsetzung eines wirksamen Schutzkonzeptes für die IT-Infrastruktur zukünftiger intelligenter Messsysteme, so genannter „smart meter". Das BSI erarbeitet derzeit hierzu verbindliche Sicherheits- und Datenschutzanforderungen. Der BDEW begleitet dieses Vorhaben intensiv, um die Anforderungen der Branche und den bestmöglichen Schutz der Kundendaten und der IT-Infrastruktur zu gewährleisten.

Portraitfoto: BDEW

Informations- und Kommunikationstechnologie als Beitrag zur öffentlichen Sicherheit

Prof. Dieter Kempf,
Präsident BITKOM

von Prof. Dieter Kempf,
Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien

Informations- und Kommunikationstechnologien sind innerhalb von knapp zwei Jahrzehnten zu häufig unverzichtbaren Bestandteilen kritischer Infrastrukturen in hochentwickelten Industriegesellschaften geworden. Ausfälle oder umfassende Störungen, Sabotage und Missbrauch der IT für kriminelle Zwecke bergen erhebliche Risiken für die öffentliche Sicherheit. In einer immer stärker vernetzten Welt potenzieren sich diese Bedrohungen – insbesondere, wenn keine echten Redundanzen zum Auffangen möglicher Fehlfunktionen zur Verfügung stehen. Wenn die IT von Kritischen Infrastrukturen versagen würde, könnte dies in der Tat innerhalb weniger Stunden zu einer ernsten Bedrohung für die Bevölkerung werden. Szenarien, die noch vor wenigen Jahren undenkbar erschienen, nähmen dann realistische Konturen an. Zweifellos gilt: Wir müssen uns mit den Risiken der Abhängigkeit von Informations- und Kommunikationstechnologien auseinandersetzen. Und wir müssen diese Risiken beherrschen lernen. Dennoch darf die Beschäftigung mit den Risiken nicht dazu führen, dass wir die Chancen, die uns die vernetzte Welt bietet, aus den Augen verlieren. Die vertrauenswürdige digitale Vernetzung ist mittlerweile selbst eine vielfach unverzichtbare und damit kritische Ressource. Dessen werden wir uns oft erst bewusst, wenn es mit der Vernetzung Probleme gibt – egal welche Ursache den Problemen zugrunde liegt. Aber wollen wir deshalb wirklich die Nutzung der Informationstechnologie in Frage stellen? Sollen wir uns ernsthaft nach Zuständen zurücksehnen, in denen wir die effizienzsteigernde und leistungsverbessernde Unterstützung durch moderne Informations- und Kommunikationstechnologie und die darauf aufbauenden Dienstleistungen noch nicht kannten? Mir erscheint eine solche Haltung absurd. Sie offenbart einen gefährlichen Fortschrittspessimismus.

Mehr Sicherheit durch IT

Klar ist: Wir profitieren im Privatleben und in der Wirtschaftswelt von zahlreichen Verbesserungen durch moderne IT-Infrastrukturen. Wir sollten auch die Chancen ergreifen, die in einem spezifischen Einsatz von IT für Sicherheitszwecke liegen. Richten wir also unseren Blick auf die Erfolge und Fortschritte im Sinne eines modernen Bevölkerungsschutzes und einer öffentlichen Sicherheit, die mit IT-gestützten Methoden arbeitet, beispielsweise in der polizeilichen Bekämpfung der Organisierten Kriminalität oder in Prozessen und Services zur Steuerung und Sicherung der Verfügbarkeit Kritischer Infrastrukturen. Ein Beispiel ist die Einführung des Digitalen Behördenfunks: ging sie anfangs durch die Grenzen des Föderalismus nur sehr stockend voran, nimmt sie jetzt zum Wohle von Behörden und Organisationen mit Sicherheitsaufgaben und der Bevölkerung Fahrt auf. Beim Digitalen Behördenfunk handelt sich um eines der größten technischen Modernisierungsvorhaben der vergangenen Jahre; nach Fertigstellung wird Deutschland über das weltweit größte auf TETRA beruhende Funknetz verfügen, das aufgrund seiner Leistungsfähigkeit im internationalen Kontext seinesgleichen sucht.

Zukunftsfähig bleiben mit IT

Behalten wir aber auch im Hinterkopf, welche Herausforderungen in der öffentlichen Sicherheit noch vor uns stehen: In dem Maße, wie die Verstädterung zunimmt, stehen wir vor der Aufgabe, urbane Räume mit Hilfe der IT zu „Smart Cities“ zu machen. Es gilt darüber hinaus, spezifische Sicherheitsprobleme von Großstädten zu bewältigen. Die IT kann dazu beitragen, zu einem effizienteren Sicherheitsmanagement komplexer, urbaner Infrastrukturen zu gelangen. Das betrifft das Wassermanagement ebenso wie effiziente Energieversorgung oder die intelligente Verkehrssteuerung bis hin zur Orchestrierung von Rettungs- und Hilfskräften bei Großeinsätzen.

Zum Schluss möchte ich an die Empfehlungen des BITKOM erinnern, wie sie im „Leitfaden Krisenmanagement und Bevölkerungsschutz“ zusammengefasst sind. Der Leitfaden ist vor gut drei Jahren erschienen. Darin wird für ein ganzheitliches Sicherheitsdenken geworben. Diese Forderung hat nichts an Aktualität eingebüßt. Wir haben damals Empfehlungen für einen gut aufgestellten, IT-verstärkten Katastrophenschutz gegeben. Was ist davon bis heute umgesetzt worden? Wir haben aufgezeigt, welche Effizienzgewinne sich im Bevölkerungsschutz durch organisatorische Interoperabilität erzielen lassen. Die Vielfalt von öffentlichen und privaten Organisationen macht die Stärke des Bevölkerungsschutzes in Deutschland aus, kann aber die Abstimmung bei der Rettung von Menschenleben auch zeitaufwändiger machen. Und Zeit ist beim Krisenmanagement einer der kritischen Erfolgsfaktoren. Eine echte IT-gelenkte Verzahnung und Synchronisierung von Rettungsmaßnahmen lässt noch auf sich warten. Wir brauchen aber eine gesamtstaatliche Sicherheitsarchitektur, die es ermöglicht, auch in einer Großschadenslage rasch Verantwortlichkeiten zuzuweisen, Hilfsbedarfe sowie -potenziale zu identifizieren und zusammenzubringen. Deshalb sollten wir unsere Intelligenz und unseren Ideenreichtum weniger für möglichst umfängliche Darstellung von Horrorszenarien bezüglich unserer IT-Abhängigkeit nutzen, sondern beides zur Lösung der anstehenden Aufgaben einsetzen – für einen Bevölkerungsschutz, der auch zukünftig jedem weltweiten Vergleich standhält.

Portraitfoto: BITKOM

Versicherungswirtschaft und öffentliche Sicherheit

Das Undenkbare berechenbarer machen

Dr. Bernhard Gause, Mitglied der Hauptgeschäftsführung des GDV

von Dr. Bernhard Gause, Gesamtverband der Deutschen Versicherungswirtschaft

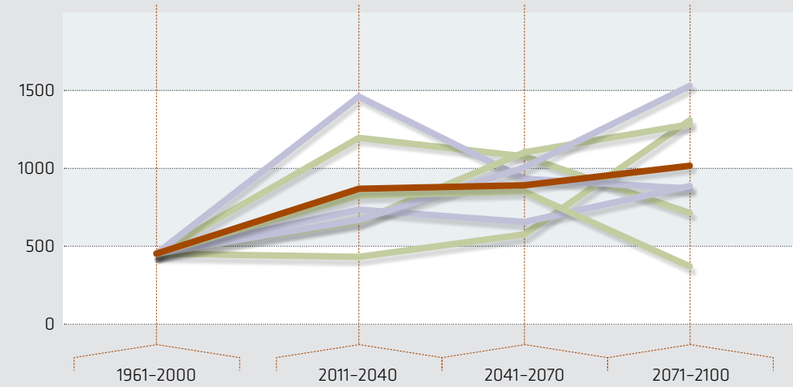
Versicherer brauchen keine Kristallkugel, um in die Zukunft zu schauen, sie arbeiten mit Expertenwissen, umfangreicher Schadenerfahrung und mathematischen Berechnungen. Diese Qualifikationen versetzen sie in die Lage, eine Vielzahl von Ereignissen aus der Vergangenheit abzubilden und daraus Folgerungen für die Zukunft hinsichtlich möglicher Schadenhöhen und der Wahrscheinlichkeit ihres Eintretens abzuleiten.

Zu diesem Zweck greift die Versicherungswirtschaft auf ihre umfangreichen statistischen Datenbanken mit detaillierten Angaben zu Schadenerfahrungen zurück, sie analysiert die Daten, gleicht sie mit wissenschaftlichen Erkenntnissen ab und vermag so schon frühzeitig deutschlandweit Trends zu erkennen, so beispielsweise bei der Zunahme von Extremwetterereignissen.

Expertise potenzieren

Die Versicherungswirtschaft ist eine Branche, die mit ihren Mitarbeitern über eine äußerst breite Expertise aus den unterschiedlichsten Wissensbereichen verfügt. Neben Mathematikern und Spezialisten für Photovoltaik, Windkraft, Brennstoffzellen oder Wasserstofftechnologie werden auch Meteorologen oder Geologen und andere Fachleute für die Risikoeinschätzung eingesetzt. Und das ist nur eine kleine Auswahl der Fachdisziplinen. Darüber hinaus ziehen wir externe Experten zu Rate, um die Schärfeneinstellung für den Blick in die Zukunft noch zu verbessern. So geschehen bei der großen Klimastudie des GDV, deren Ergebnisse im Mai 2011 vorgestellt wurden. Die Studie stellt eine weltweit einzigartige und sehr fruchtvolle Zusammenarbeit der Versicherungswirtschaft mit renommierten wissenschaftlichen Instituten[1] dar: Mit unseren Schadendaten haben wir die beteiligten Klimaforscher in die Lage versetzt, Klimadaten aus der Vergangenheit mit den aufgetretenen Schäden zu verknüpfen und die Auswirkungen der Klimaentwicklung für die kommenden Jahrzehnte zu prognostizieren. Die Erkenntnis: Die Menschen in Deutschland müssen sich in Zukunft auf häufigere, heftigere Wetterextreme einstellen – und mit ihnen auch sämtliche Verantwortliche der öffentlichen Sicherheit.

Hochwasserschadenmodell des Potsdam-Instituts für Klimafolgenforschung

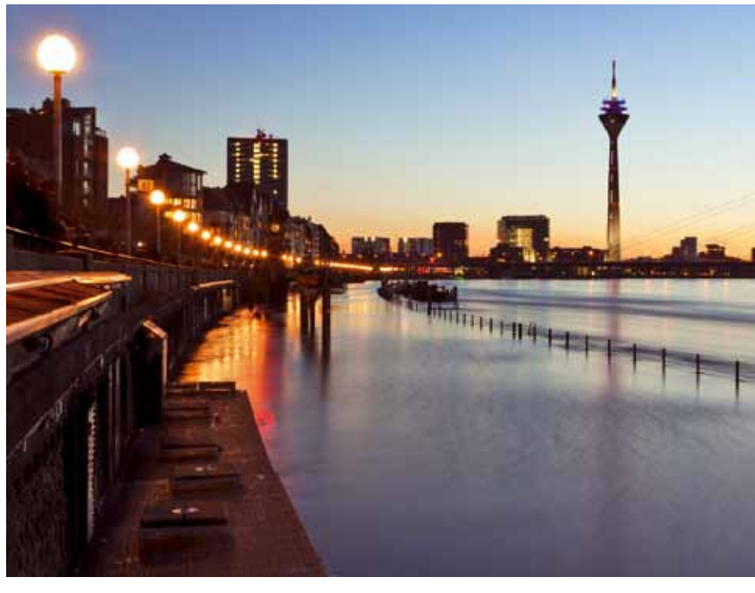


Entwicklung des langjährigen Schadenniveaus: hydrologische Modellierungen in verschiedenen Szenarien basierend auf CCLM- bzw. REMO-Klimadaten. Werte in Mio. EURO

Quelle: GDV

Geburtshelfer für Innovationen

Ingenieure kommen in der Versicherungswirtschaft auch zum Einsatz, wenn es um die Chancen von Technologien geht, die sich noch in der Entwicklungsphase befinden. Es ist wichtig, dass Versicherer so früh wie möglich an der „Werkbank“ dabei sind, denn der Aspekt der Versicherbarkeit muss in die jeweiligen Wirtschaftlichkeitsberechnungen natürlich stets mit einfließen. Die Versicherungswirtschaft kann somit als Geburtshelfer von zukunftsträchtigen technologischen Innovationen fungieren. Unsere Aufgabe besteht aber auch darin aufzuzeigen, ob eine neue Technologie ein nur in sehr engen Grenzen oder gar nicht versicherbares Risiko darstellt, beispielsweise für die öffentliche Sicherheit.



[1] An der Studie waren Forscher des Potsdam-Instituts für Klimafolgenforschung, der Freien Universität Berlin und der Universität Köln beteiligt. Weitere Informationen unter www.gdv.de.

Portraitfoto: GDV

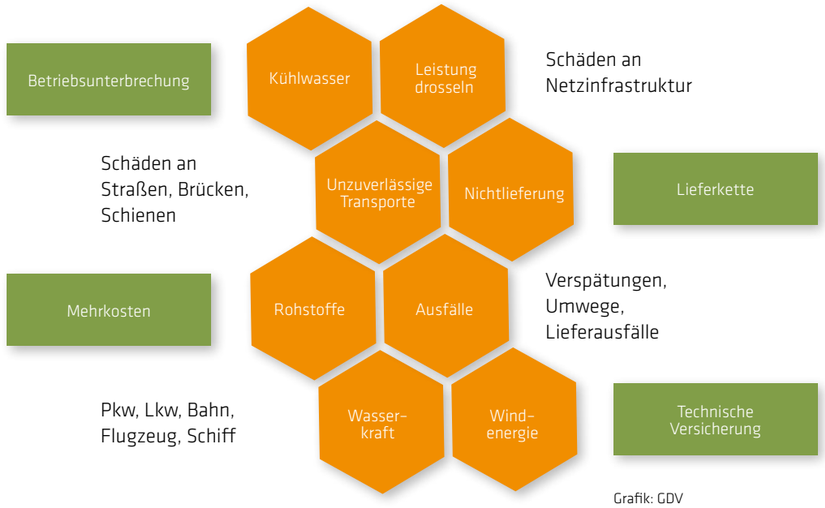
Der öffentlichen Sicherheit verpflichtet

Wenn wir etwas für die öffentliche Sicherheit tun können, dann tun wir das gerne – Schadenprävention ist seit jeher ein elementares Anliegen der Versicherungswirtschaft und stellt Versicherbarkeit oftmals erst her. Bis zum Jahresende werden wir eine öffentliche Version unseres Geoinformationssystems ZÜRS Geo im Internet zur Verfügung stellen: ZÜRS Public wird Hausbesitzern eine Einschätzung des Risikos ermöglichen, mit dem eigenen Haus Opfer einer Überschwemmung zu werden. So lassen sich rechtzeitig Vorkehrungen für den Schutz von Hab und Gut, von Leib und Leben treffen. Ein Service, der unbedingt vor dem Kauf von Bauland in Anspruch genommen werden sollte. Generell können wir sagen: gerade Starkregen und die damit in Zusammenhang stehenden Überschwemmungen werden immer noch unterschätzt. ZÜRS Public ist nur ein Beispiel dafür, wie sich aus Berechnungen der Versicherungswirtschaft Handlungsempfehlungen ableiten lassen – für die Bevölkerung und Bevölkerungsschützer gleichermaßen.

Naturgefahren in Deutschland – nicht nur Hochwasser

Grafik: GDV

Naturgefahren schaffen neue Versicherungsbedürfnisse



Grafik: GDV

Miteinander von Staat und Privat: Terrorrisiken gemeinsam bewältigen

Für Risiken, die zwar als Bedrohung real sind, aber sich in Deutschland nicht in größerem Ausmaß verwirklicht haben, liegen keine Schadenerfahrungen vor. In diese Reihe gehören Terroranschläge, deren Eintrittswahrscheinlichkeit nicht kalkulierbar ist und deren Schadenhöhen derart verheerend sein können, dass sie die Grenzen der Versicherbarkeit überschreiten. Da bei Terrorschäden die versicherungstechnischen Kapazitäten von Erst- und Rückversicherern begrenzt sind, haben sich der Staat und die private Versicherungswirtschaft zur gemeinschaftlichen Deckung der Risiken entschieden. In Sachversicherungen ist bis zu einer Versicherungssumme von 25 Millionen Euro das Terrorrisiko generell mitversichert. Für darüber hinausgehende Schäden bietet der Spezialversicherer EXTREMUS Schutz vor finanziellen Verlusten bei Sach- und Betriebsunterbrechungsschäden durch Terroranschläge. Dort decken die Versicherer Gesamtschäden mit einer Jahreskapazität bis 2 Milliarden Euro ab, daran schließt sich eine Haftungsstrecke des Bundes mit 8 Milliarden Euro an. Dieses PPP-Modell der Terrorversicherung ist ein gelungenes Beispiel für eine punktuelle öffentlich-private Zusammenarbeit in der Risikoabsicherung. Auch in anderen Industrieländern, wie z. B. den USA, England, Frankreich, Spanien und den Niederlanden existieren in Zusammenarbeit von Staat und privater Versicherungswirtschaft Lösungen zur Absicherung von Schäden durch Terrorismus.

Kreditwirtschaft und öffentliche Sicherheit

Dr. Ibrahim Karasu, Geschäftsführer Retail Banking und Banktechnologie des BdB

von Dr. Ibrahim Karasu,
Bundesverband deutscher Banken

Bankdienstleistungen kommen in ihrer Bedeutung für das öffentliche Gemeinwesen einer Kritischen Infrastruktur gleich. Doch die Kreditwirtschaft ist auch angewiesen auf ein reibungsloses Funktionieren anderer Kritischer Infrastrukturen wie Energieversorgung oder Internet. In Krisensituationen, die relevant sind für die öffentliche Sicherheit, arbeitet die Kreditwirtschaft mit Vertretern der anderen Wirtschaftszweige im Umsetzungsplan „Kritische IT-Infrastrukturen" – kurz UP KRITIS – der Bundesregierung zusammen. Hier werden Prozesse und Maßnahmen zur Krisenreaktion und Krisenbewältigung entwickelt oder auch Krisenszenarien tatsächlich geübt.

Die Kreditwirtschaft ist bereits seit 2006 im UP KRITIS sehr aktiv. Da die Kreditwirtschaft ein nicht physisches Produkt anbietet – nämlich Finanzdienstleistungen – sind IT-Infrastrukturen die Basis für das gesamte Bankgeschäft. Der Schutz und der sichere Betrieb dieser IT-Infrastrukturen steht daher schon immer im Fokus einer Bank – ganz unabhängig von der aktuellen wirtschaftlichen und politischen Lage.

Die Bankenbranche zeichnet sich traditionell durch ein gutes Geschäftskontinuitätsmanagement aus. Diese Expertise, die einzelne Bankgesellschaften zum Schutz vor Umsatzeinbußen und Reputationsschäden aufgebaut haben, ist selbstverständlich auch von Nutzen, um die Kritische Infrastruktur „Kreditwirtschaft" als Ganzes zu schützen. Eine sichere IT-Infrastruktur ist Grundvoraussetzung für den Geschäftserfolg einer jeden Bank. Und Sicherheit muss dabei ganzheitlich gesehen werden: Die IT-Struktur muss ständig verfügbar und widerstandsfähig sein. Integrität, Authentizität und Vertraulichkeit sind wichtige Merkmale. Insofern trägt jedes einzelne Kreditinstitut mit seiner individuellen Expertise und seinen hohen Qualitätsanforderungen an die eigene IT-Struktur dazu bei, dass in Krisenfällen die Sicherheit der gesamten Finanzwirtschaft gewährleistet ist.

Anders als die klassischen KRITIS, wie Energie, Wasserversorgung, Lebensmittelversorgung, ist die Bankeninfrastruktur geographisch gut verteilt und erscheint insofern weniger anfällig für regionale Naturkatastrophen. Bei Pandemien als „natürlichem" Risiko haben Banken gute Voraussetzungen, die Funktionsfähigkeit ihrer Services sicherzustellen:

Eine gute IT-Infrastruktur ermöglicht beispielsweise auch Tele- bzw. Online-Arbeitsplätze oder nutzt Ausweichrechenzentren, sodass die Mitarbeiter einen von einer Pandemie betroffenen Standort gar nicht aufsuchen müssen. Allerdings braucht eine gute IT auch leistungsfähige, gesunde Mitarbeiter. Bei außerordentlich vielen Krankheitsfällen könnte der Produktionsprozess leiden oder müsste teils eingestellt werden – nicht nur in der Kreditwirtschaft.

Bei einem überregionalen Stromausfall ist es wichtig, die Versorgung mit Bargeld sicherzustellen. Für größere Stromausfälle sind ausreichend viele Filialen mit Notstromaggregaten ausgestattet.

Banken und ihre Kunden sind seit Jahren das Ziel von Cyberkriminellen, die an Prozeduren des Onlinebanking ansetzen, um das schnelle Geld zu machen. Das Tatmotiv für Online-Banking-Kriminalität ist und bleibt in erster Linie die Bereicherung. Wir konnten nicht feststellen, dass sich am Motiv der Angreifer substanziell etwas ändert. Gegen diese Formen der Bedrohung entwickelt die gesamte deutsche Kreditwirtschaft ihre Sicherheitssysteme ständig weiter.

Gezielte, organisierte Attacken auf die Kreditwirtschaft, mit dem Ziel, die globalen Finanzmärkte zu unterminieren, haben wir nicht beobachtet. Doch wir bleiben wachsam. Der UP KRITIS, in dem die Kreditwirtschaft aktiv mitwirkt, ist auch Teil der Cyber-Sicherheitsstrategie der Bundesregierung. Das Beispiel Estland hat gezeigt, dass man gezielte Angriffe auf die IT von ganzen Wirtschaftszweigen oder gar Staaten nicht ausschließen kann. Aus diesem Grund behandelt der UP KRITIS verschiedene Angriffs- und Abwehrszenarien, um alle kritischen Sektoren – und damit die IT-Struktur Deutschlands – bestmöglich zu schützen.

Portraitfoto: BdB

Sicherheit ist unser Geschäftszweck

Dieter Kaden,
Vorsitzender der
Geschäftsführung
der DFS

von Dieter Kaden,
DFS Deutsche Flugsicherung

Es ist nicht nur gute Tradition, sondern auch gelebte Selbstverständlichkeit, dass die DFS Deutsche Flugsicherung GmbH (DFS) die Sicherheit an die erste Stelle setzt. Dieses Bestreben beschränken wir nicht nur auf die Sicherheit des Luftraums. In allen Unternehmensbereichen handeln wir nach der Maxime, Fehlentscheidungen systematisch zu erfassen und auszuwerten, um sie künftig zu vermeiden. Wir sind daher für verschiedene Arten von Sicherheitsvorfällen außerordentlich gut gewappnet.

Uns wären daher auch im Fall eines überregionalen Stromausfalls nicht die Hände gebunden. Die DFS verfügt über mehrfach ausgelegte Redundanzen für die Stromversorgung: Neben dem Zugang zum öffentlichen Stromnetz haben wir in unserer Hauptniederlassung in Langen ein Kraftwerk, in dem wir unseren eigenen Strom produzieren. Alle anderen Niederlassungen halten dieselbetriebene Stromgeneratoren vor. Eine weitere Redundanzstufe bietet unsere Unterbrechungsfreie Stromversorgung (USV), deren Hauptaufgabe im Normalbetrieb darin besteht, für einen gleichmäßigen, schwankungsfreien Strom zu sorgen. So können unsere Flugsicherungssysteme zuverlässig arbeiten. Darüber hinaus dient die USV dazu, bei einem Stromausfall einen Notbetrieb für etwa zwei Stunden aufrecht zu erhalten.

Die DFS ist somit, was die Stromversorgung anbelangt, bis zu einem gewissen Grad autark, wenn auch zeitlich begrenzt. Wenn also das „Undenkbare" eintritt, kann mit Hilfe unserer Reservesysteme der Flugverkehr abgearbeitet werden. In diesem Zeitfenster werden in der Luft befindliche Flugzeuge zur Landung gebracht oder zu störungsfreien Flughäfen weitergeleitet, falls erforderlich ins benachbarte Ausland. Schließlich stehen als vierte Redundanz an jedem Fluglotsenplatz batteriebetriebene Funksprechgarnituren zur Verfügung – fiele im äußersten Notfall auch der strombetriebene Sprechfunk aus, könnten unsere Fluglotsen dennoch mit den Piloten kommunizieren, ihnen Anweisungen geben oder sie zu sicheren Flughäfen umleiten.

Neue Flugzeuge würden in dieser Zeit keinesfalls starten oder in den Luftraum hineingelassen werden. Hier geben wir der Sicherheit absoluten Vorrang vor Wirtschaftlichkeitserwägungen.

Das bedeutet aber: Nachdem diese zwei Stunden verstrichen sind, wird der Flugverkehr in dem betroffenen Gebiet zum Erliegen kommen. Ein dauerhaftes funktionales Äquivalent zu unseren stromabhängigen Flugsicherungssystemen existiert nicht. Bei der Komplexität des heutigen Flugverkehrs ließe sich die Kontrolle ohnehin nicht mehr von Hand bewerkstelligen.

Die Deutsche Flugsicherung ist jedoch nur ein Akteur im Verbund aller am Flugverkehr beteiligten Unternehmen und Organisationen. Im Falle eines überregionalen Stromausfalls wären gleichermaßen die Flughafengesellschaften, die Airlines und andere Leistungserbringer rund um die Luftfahrt wie Bundespolizei und Sicherheitsunternehmen betroffen. Der Flugverkehr würde also ohnehin zum Erliegen kommen, weil keine Buchungen mehr getätigt, keine Passagiere mehr abgefertigt, kein Gepäck mehr eingecheckt und die Sicherheit an den Flughäfen nicht mehr gewährleistet werden könnte.

Krisensituationen werden im Rahmen der Ausbildung bei der DFS regelmäßig durchgespielt. Darüber hinaus bereiten wir uns auf verschiedene sicherheitsrelevante Ausnahmesituationen in Übungen vor. Dazu gehört beispielsweise, dass wir übungsweise nachts die Stromversorgung unterbrechen, um die Zuverlässigkeit der Notsysteme zu prüfen.

Wie in Notfällen verfahren wird, ist in den Towern und Kontrollzentralen der DFS mithin nicht dem Zufall überlassen. Die DFS verfährt wie alle Flugsicherungsorganisationen weltweit nach den Vorschriften der Internationalen Zivilluftfahrtorganisation ICAO. Nach diesen Grundsätzen wird gehandelt, im Normalbetrieb wie im Notfall.

Wir sind gegenwärtig gut aufgestellt, doch schauen wir auch in die Zukunft: Schon jetzt müssen wir für die anspruchsvolle Tätigkeit des Fluglotsen permanent werben. Wie wird sich die demographische Entwicklung auf die Rekrutierung von Fluglotsen auswirken? Dass sich Nachwuchsprobleme verschärfen und schließlich Auswirkungen auf die Betriebssicherheit unserer Einrichtungen haben könnten, sehen wir derzeit noch nicht. Das Phänomen des Bevölkerungsrückgangs verbunden mit einem Fachkräftemangel wird Deutschland in der Breite treffen, so viel ist sicher. Das wird die Volkswirtschaft insgesamt betreffen, nicht nur die Flugsicherung isoliert.

Fotos: DFS Deutsche Flugsicherung

LÜKEX – das „Undenkbare“ denken und üben

Christoph Unger,
Präsident des BBK

von Christoph Unger,
Bundesamt für Bevölkerungsschutz
und Katastrophenhilfe

„Das Undenkbare denken“ – und dennoch realistisch bleiben: Dieser Leitsatz steht auch über den Szenarien für die LÜKEX-Übungen, die sich grundsätzlich an „worst-case-Szenarien“ orientieren und dadurch gelegentlich Kritik auf sich ziehen, über die Realität hinauszuschießen. Mittlerweile ist die Kritik leiser geworden, da z. B. ein Jahr nach dem 2004 gewählten Stromausfallszenario ein großflächiger Stromausfall im Münsterland die bei der Übung simulierten Effekte fast deckungsgleich hervorrief. Auch bei der jüngsten Übung LÜKEX 11 zum Thema IT-Sicherheit haben im Vorfeld reale Hackerangriffe auf als sicher geltende IT-Systeme gezeigt, dass das gewählte Szenario der Wirklichkeit sehr nahe kam.

Der Begriff LÜKEX steht für „Länder übergreifende Krisenmanagement-Übung/Exercise“ und bezeichnet eine Übungsserie im strategischen Krisenmanagement, die seit 2004 von Bund und Ländern im zweijährigen Rhythmus gemeinsam geplant, vorbereitet und durchgeführt wird. Die Übungen gehen auf Beschlüsse der Innenministerkonferenz aus dem Jahr 2002 zurück, als die Minister im Rahmen einer „Neuen Strategie des Bundes und der Länder zum Schutz der Bevölkerung in Deutschland“ für „außergewöhnliche Gefahren- und Schadenslagen“ eine gemeinsame Verantwortung von Bund und Ländern feststellten. Im Rahmen der Krisenvorbereitung sollten auch gemeinsame strategische Übungen stattfinden, die unter Wahrung der gesetzlichen Zuständigkeiten die überwiegend operativ-taktisch ausgerichteten Übungsvorhaben der Länder ergänzen. Mit der Planung, Vorbereitung und Durchführung der LÜKEX-Übungen wurde das 2004 neu eingerichtete Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) beauftragt, das 2009 im § 14 des Zivilschutz- und Katastrophenhilfegesetzes (ZSKG) dazu einen gesetzlichen Auftrag erhielt.

LÜKEX-Übungen finden zu wechselnden Themen / Szenarien und mit darauf abgestimmter Beteiligung statt. Den bisherigen Übungen lagen folgende Szenarien zugrunde:

- LÜKEX 04: winterliche Extremwetterlage mit Hochwasser und großflächigem Stromausfall;
- LÜKEX 05: terroristische Anschläge und Anschlagsdrohungen im Zusammenhang mit der Fußball-Weltmeisterschaft 2006;
- LÜKEX 07: weltweite Influenza-Pandemie;
- LÜKEX 09/10: terroristische Bedrohung mit Androhung und Durchführung von Anschlägen mit konventionellen Sprengstoffen, chemischen und radioaktiven Tatmitteln („schmutzige Bombe“);
- LÜKEX 11: Bedrohung bzw. Störung der IT-Strukturen und -systeme. Und da nach der Übung bei uns vor der Übung ist, hat der Zyklus für
- LÜKEX 13 bereits begonnen; diese Übung wird sich mit Fragen der Lebensmittelsicherheit befassen.

Eine der wesentlichen Prämissen von LÜKEX ist, dass Bevölkerungsschutz die intensive und partnerschaftliche Zusammenarbeit zwischen den behördlichen Akteuren in Bund und Ländern und mit – größtenteils privaten – Betreibern gesamtstaatlich wichtiger Infrastruktureinrichtungen erfordert. Ziel ist eine verstärkte Auseinandersetzung mit Fragen der Früherkennung und Frühwarnung sowie der Risikoanalyse. Ebenso ist die Risiko- und Krisenkommunikation mit Medien und Bürgern integraler Bestandteil eines professionellen strategischen Krisenmanagements.

Grafik: BBK

Der Zyklus einer LÜKEX-Übung dauert etwa 2 Jahre. Er gliedert sich in die vier Phasen Planung, Vorbereitung, Durchführung und Auswertung. Die ca. 18monatige Phase der Übungsvorbereitung ist für das Erreichen der Übungsziele von besonderer Bedeutung. Schon hier sollen sich die Übungsbeteiligten in themenbezogenen Workshops, Diskursen und Arbeitssitzungen intensiv mit den Übungsinhalten auseinandersetzen, Schwachstellen in der eigenen Organisation erkennen und möglichst vor Übungsbeginn beseitigen. In dieser Phase wird das Drehbuch als wichtigste Übungsgrundlage erstellt und abgestimmt. Wissenschaftliche Gutachten zu Fachfragen werden eingeholt und vermittelt. Aufgrund der intensiven Zusammenarbeit aller für das Krisenmanagement Verantwortlichen von Bund, Ländern, gesellschaftlichen Organisationen und Unternehmen entstehen „Kooperations-Netzwerke“, die wesentlich dazu beitragen, über die Übung hinaus die Funktionsfähigkeit des Hilfeleistungssystems in realen Krisensituationen zu gewährleisten.

Die Übungsdurchführung ist Höhepunkt des Übungszyklus und zugleich „Lackmustest“ für den Erfolg langer, vertrauensvoller Zusammenarbeit. In dieser Phase wirken bundesweit bis zu 3.000 Personen in den Krisen- bzw. Verwaltungsstäben der Bundes- und Landesressorts bzw. den sonstigen für das Krisenmanagement zuständigen Stellen mit.

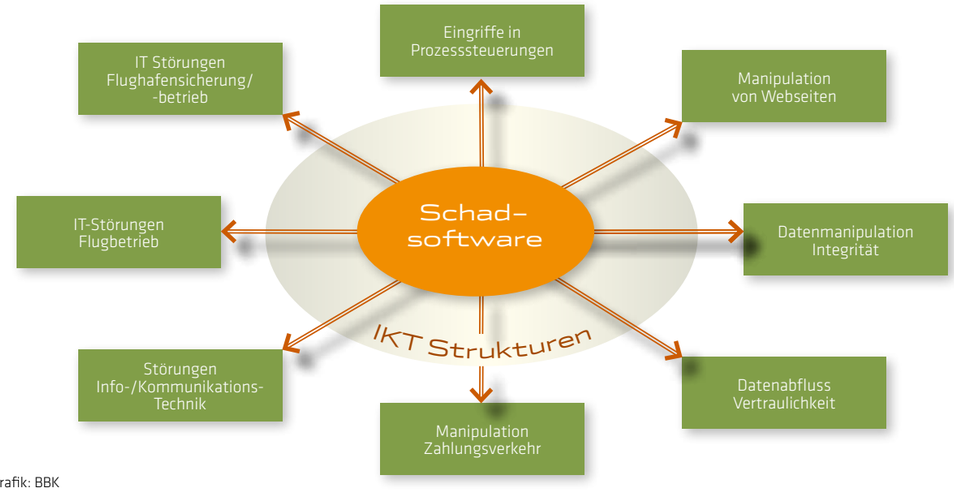
Portraitfoto: BBK

„LÜKEX 11“ – IT-Sicherheit auf dem Prüfstand

Die letzte Übung ihrer Art, die LÜKEX 11, wurde am 30. November und 1. Dezember 2011 bundesweit und unter Beteiligung zahlreicher Bundesländer durchgeführt. Übungsthema war diesmal IT-Sicherheit. Ziel der Übung war es, dafür zu sensibilisieren, dass der Befall mit „Malware“, der Abfluss vertraulicher Daten und Integritätsverletzungen von IT-Systemen zur existentiellen Bedrohung für Behörden und Unternehmen werden können. An der Übung waren wichtige, für die IT-Sicherheit und das allgemeine Krisenmanagement im Bevölkerungsschutz relevante Stellen von Bund und Ländern beteiligt, ebenso Unternehmen der Kritischen Infrastrukturen (KRITIS) aus den vier Sektoren Staat und Verwaltung/Behörden mit Sicherheitsaufgaben (BOS), Informations- und Kommunikationstechnologie (IKT), Banken und Versicherungen, Transport und Verkehr sowie gesellschaftliche Organisationen und Verbände. Die Übung, die wegen der hohen Aktualität des Themas große öffentliche Aufmerksamkeit und Medienresonanz erfuhr, verlief nach den derzeit vorliegenden, noch nicht vollständigen Auswertungsergebnissen erfolgreich. Insbesondere ist die Sensibilisierung der Übungsbeteiligten für Fragen der IT-Sicherheit und die Integration des IT-Krisenmanagements in das allgemeine Krisenmanagement gelungen. Darüber hinaus fand das erstmalig durchgeführte, zweitägige Fachforum, das für über 150 Gäste die Übung mit Expertenvorträgen aus dem In- und Ausland begleitete, großen Anklang. Ganz im Sinne des Vernetzungsgedankens der Übungsserie LÜKEX ermöglichte das Begleitforum zur LÜKEX 11 nicht nur einen intensiven, sektorübergreifenden fachlichen Austausch, sondern bot auch einen passenden Rahmen für die Intensivierung bestehender Netzwerke und die Knüpfung neuer fachlicher Kontakte auch auf dieser Ebene.

Nach den Erfahrungen von nunmehr fünf LÜKEX-Übungen kann man sagen, dass das Übungskonzept inzwischen als bewährte Grundlage für die Anlage strategischer Übungen per se gilt. Über die Erprobung des Krisenmanagements hinaus haben die Übungen zahlreiche Impulse für das strategische Krisenmanagement in der Bundesrepublik insgesamt gegeben, nicht zuletzt auf Grund der Bildung von Kooperations-Netzwerken und vielfältiger spin-off-Effekte für zahlreiche andere Bereiche und Handlungsfelder. LÜKEX ist so Ausdruck eines in die Zukunft gerichteten Prozesses, der wichtige Entwicklungen im strategischen Krisenmanagement im Bevölkerungsschutz in Gang gesetzt hat. Nicht zu Unrecht gilt LÜKEX deshalb heute als anerkanntes Markenzeichen eines vorausschauenden Krisenvorsorgesystems im Bevölkerungsschutz Deutschlands und wird im In- und Ausland auch als solches wahrgenommen.

Die Gefährdung der IT-Strukturen und –verfahren ist komplex



Grafik: BBK

Forschung für zivile Sicherheit

Dr. Wolf Junker,
Leiter Referat 522 – Sicherheitsforschung – im BMBF

Interview mit Dr. Wolf Junker,
Bundesministerium für Bildung und Forschung

Herr Junker, das Sicherheitsforschungsprogramm wird fortgeschrieben. Auf welche Herausforderungen zielt das Programm?

Die Risiken für die zivile Sicherheit werden in einer globalisierten Welt immer vielfältiger. Die Vernetzung internationaler Handels- und Reiseströme, die Gefahren durch Extremwetterereignisse sowie die zunehmende Digitalisierung führen zu neuen Verwundbarkeiten. Weitere Risiken entstehen durch organisierte Kriminalität und einen weltweit operierenden Terrorismus. Diesen Herausforderungen stellt sich das neue Rahmenprogramm „Forschung für die zivile Sicherheit" im Zeitraum von 2012 bis 2017.

Welche neuen Akzente sollen mit dem Rahmenprogramm gesetzt, welche Forschungsschwerpunkte noch stärker gefördert werden?

Mit dem Rahmenprogramm vertiefen wir Schwerpunkte, für die weiterhin Bedarf besteht, wie der Schutz Kritischer Infrastrukturen sowie die Erforschung der gesellschaftlichen Aspekte der zivilen Sicherheit. Gleichzeitig stellen wir uns aktuellen Fragestellungen mit Schwerpunktsetzungen, wie Urbane Sicherheit, Schutz vor Gefahrstoffen und Sicherheit der Wirtschaft.

Der erfolgreiche Ansatz des ersten nationalen Sicherheitsforschungsprogramms besteht aus einem Dreiklang: Interdisziplinarität, Einbeziehung von Industrie und Endnutzern, wie Polizei, Feuerwehr und Rettungskräften, sowie die Analyse gesellschaftlicher Aspekte der zivilen Sicherheit. Innovative Technologien werden in umfassende Sicherheitskonzepte eingebettet, die dem täglichen Bedarf von Anwendern, wie zum Beispiel dem Technischen Hilfswerk (THW), Polizei und Rettungskräften ebenso wie der Gesellschaft insgesamt Rechnung tragen. Diesen erfolgreichen Ansatz setzt das neue Rahmenprogramm für Sicherheitsforschung fort.

Welche Akteure waren an der Fortschreibung des Programms beteiligt?

Um die künftigen Herausforderungen für die zivile Sicherheitsforschung zu identifizieren, hat das BMBF im Herbst 2011 einen offenen Agenda-Prozess initiiert, in dem wir gemeinsam mit Forschern, Endnutzern und Industrie die Herausforderungen der zivilen Sicherheitsforschung und neue Forschungsthemen, wie etwa Urbane Sicherheit, identifiziert haben.

Dem Sicherheitsforschungsprogramm als Teil der Hightech-Strategie liegt die Erkenntnis zu Grunde, dass Innovationen unerlässlich sind, um die zivile Sicherheit zu erhöhen. Welchen Anteil hat das Programm daran, dass der Bereich zivile Sicherheit auch als Treiber von Innovationen wahrgenommen wird?

Sicherheit ist ein wichtiger Standort- und Wirtschaftsfaktor. Mit dem ersten Programm „Forschung für die zivile Sicherheit" hat sich seit 2007 eine Fachszene der zivilen Sicherheitsforschung in Deutschland etabliert, die auch auf europäischer Ebene beachtliche Erfolge zu verzeichnen hat. Es sind zahlreiche innovative Projekte initiiert worden, wie etwa für die schnellere Erstversorgung von Verletzten durch Digitalisierung oder die Überprüfung von grenzüberschreitenden Warenketten durch IT-Plattformen oder auch Organisationskonzepte und -systeme, die die Sicherheit der Besucher von Großveranstaltungen erhöhen sollen. Viele dieser Projekte setzen mit ihren Innovationen erste Standards, die entsprechend in die Normierungen auf nationaler und internationaler Ebene einfließen sollen.

Sicherheitstechnische Produkte tragen zum spezifisch deutschen Kompetenzprofil der Industrie bei. Inwieweit schärft das Sicherheitsforschungsprogramm dieses Profil?

Das Sicherheitsforschungsprogramm setzt auf Austausch und Vernetzung: Der Innovationstransfer zwischen Forschung und Wirtschaft sowie internationale Kooperationen mit den USA, Israel und Frankreich beschleunigen den Informationsaustausch der Akteure über leistungsfähige Hightech-Lösungen und innovative Dienstleistungen. Die Erforschung und Entwicklung konkurrenzfähiger Produkte und Dienstleistungen eröffnen die Chance, Deutschland als Leitanbieter für zivile Sicherheitslösungen zu etablieren.

Ein Leitbegriff der Hightech-Strategie ist neben Ideen und Innovation das Wachstumspotenzial. Inwieweit spielt die zivile Sicherheitsforschung als Wachstumsfaktor bereits eine Rolle?

Zivile Sicherheit ist nicht nur eine wichtige Grundlage für die Freiheit in der Gesellschaft, sondern stellt auch einen zunehmenden Wettbewerbsfaktor dar. Der Markt für zivile Sicherheitstechnologien und -dienstleistungen hatte 2008 ein Gesamtvolumen von gut 20 Mrd. Euro in Deutschland laut einer Studie des BMWI. Aufgrund begründeter Wachstumsannahmen ergibt sich für das Jahr 2015 ein Umsatzvolumen in Deutschland von über 31 Mrd. Euro und ein Wertschöpfungsanteil von etwa 69 % oder 21,5 Mrd. Euro.

Die klassischen Sicherheitsressorts liegen beim BMI bzw. BMVg. Wie wird der Erkenntnistransfer aus dem Sicherheitsforschungsprogramm des BMBF in die zuständigen Ministerien bewerkstelligt?

Im Bereich der zivilen Sicherheitsforschung besteht ein enger Austausch zwischen den Ressorts. Ausdruck dieser Dynamik ist unter anderem der Ressortkreis, in dem etwa BMI, BMWi, BMG, BMELV, BMVBS vertreten sind. Zudem hat das BMI zwei sogenannte One-Stop-Agencies eingerichtet. Eine an der Deutschen Hochschule der Polizei und eine zweite im Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK). Diese dienen als zentrale Koordinierungsstelle für alle Bedarfsträger und erleichtern den Informationsfluss. Hiervon zu unterscheiden ist die wehrtechnische Forschung des BMVg, die als Bestandteil der dortigen Ressortforschung sich auf die für wehrtechnische Anwendungen relevanten wissenschaftlichen Disziplinen bezieht.

Portraitfoto: BMBF

Komplexität, Unsicherheit und Ambiguität – vom mühsamen Umgang mit systemischen Risiken

Marie-Luise Beck,
Projektkoordinatorin
Forschungsforum
Öffentliche Sicherheit

Dr. Lars Gerhold,
wissenschaftlicher Koordinator
Forschungsforum Öffentliche
Sicherheit

von Marie-Luise Beck und Dr. Lars Gerhold, FOES

Wollte man versuchen Risiken und Gefahren für unsere Gesellschaft zusammenzutragen, würde man eine Liste ganz unterschiedlicher Phänomene zusammenstellen können, wie bereits vielfach geschehen: Ausfall kritischer Infrastrukturen, Naturgefahren, Pandemien sowie Terrorismus und (Cyber-) Kriminalität[1]. Die Aufzählung ließe sich problemlos erweitern. Entscheidend ist jedoch, dass die benannten Gefahren und Risiken etwas gemeinsam haben: Sie haben systemischen Charakter. Nach Renn et al. beziehen sich systemische Risiken auf „hochgradig vernetzte Problemzusammenhänge, mit schwer abschätzbaren Breiten- und Langzeitwirkungen, deren Beschreibung, Kategorisierung und Bewältigung mit erheblichen Wissens- und Bewertungsproblemen verbunden sind[2]. Renn et al. machen dies an vier Kriterien fest[3]:

1. Die **Entgrenzung in Zeit, Raum und Schadenskategorie**, welche sich auf die Ausstrahlung oder Ausbreitung eines betroffenen Systems auf andere, vernetzte Systeme, Bereiche oder Sektoren, deren Funktionen oder Leistungen gefährdet oder gestört werden können, bezieht. Während direkte Folgen bei offenkundigen Systemzusammenhängen beobachtbar und steuerbar sind, lassen sich nicht-intendierte Nebenfolgen weder absehen noch regulieren. Ein prominentes Beispiel ist die derzeitige Finanzkrise, die als US-Immobilienkrise startete, auf den Bankensektor übersprang, sich zur Staatenkrise entwickelte und derzeit wieder die Banken in Bedrängnis zu bringen scheint. Als weitere Nebenfolgen wird der Vertrauensverlust der Bevölkerung in das Finanz- und Wirtschaftssystem sowie ein Legitimitätsverlust der Demokratie in den Medien diskutiert.

2. Ein hohes Maß an **Komplexität** und oftmals nicht mehr nachzuzeichnende Ursache-Wirkungs-Bezüge, die in ihren Verästelungen kaum bekannt, geschweige denn beherrschbar sind. Ein Beispiel sind die Interdependenzen von Kritischen Infrastrukturen und ihre kaskadierenden Effekte bei Störungen, aber auch Infektionserkrankungen, bei denen es keinen eindeutigen Dosis-Wirkungs-Zusammenhang gibt und wo durch unterschiedliche Inkubationszeiten die Ursache (Ansteckung) und Auswirkung (Erkrankung) zeitlich extrem auseinander liegen kann.

3. Ein hohes Maß an **Unsicherheit**, das sich oft nicht hinreichend qualifizieren lässt und Formen der Verunsicherung ebenso annehmen kann wie Formen des Nicht-Wissens. Unsicherheit entsteht im Wesentlichen durch Mangel an Kontrolle und Einfluss gegenüber Risiken und Gefahren, deren Eintreten und Auswirkungen nicht eindeutig abschätzbar sind. Beispiele finden sich in der Terroranschlagsgefahr auf Flughäfen und Weihnachtsmärkten oder plötzlich auftretenden Naturgefahren, deren Vorhersage selbst mit einem hohen Maß an Unsicherheit verbunden ist.

4. Ein hohes Maß an **Ambiguität**, das heißt an Mehrdeutigkeit hinsichtlich der zu erwartenden Konsequenzen und ihrer Bewertung. Beispielsweise ist die Frage, ob Atomkraftwerke ein tolerierbares oder nicht-tolerierbares Risiko darstellen, technisch-naturwissenschaftlich nicht eindeutig zu beantworten. Vielmehr liegt ihr eine gesellschaftliche Wertentscheidung zugrunde. Oder das Internet, das einerseits die Welt unsicherer macht, andererseits aber durch Frühwarnfunktionen der Risikominimierung in einer Gesellschaft dient.

Das Forschungsforum Öffentliche Sicherheit hat sich im Jahr 2011 in drei interdisziplinären Workshops mit systemischen Risiken auseinandergesetzt und sich Fragen des Umgangs mit Unsicherheit in nichtbeherrschbaren Systemen anhand der Themen Kriminalität bzw. Cyberkriminalität, biologische Gefahren und Naturkatastrophen gestellt[4]. Themenübergreifend konnte gezeigt werden, dass sich durch die hohe technische wie gesellschaftliche Vernetzung unserer Gesellschaft, die Folgen eines Ereignisses rasant auf unterschiedlichste Systeme ausbreiten können. Besonders soziale, ökonomische und politische Nebenfolgen von ursprünglich technischen Krisenereignissen sind ein Phänomen, das Forscher wie Praktiker beschäftigt. Dabei sind systemische Risiken nicht erst durch moderne Technologien und Lebensweisen entstanden. Als Blaupause systemischer Risiken kann die Ansteckungsdynamik von Infektionserkrankungen betrachtet werden, die schon zuvor – man denke nur an die mittelalterliche Pest oder die Spanische Grippe Anfang des 20. Jahrhunderts – beachtliche Auswirkungen entfalten konnte. Dies spiegelt sich beispielsweise auch sprachlich wider, wenn im Zusammenhang mit der Euro-Krise auf medizinisches Vokabular wie „Ansteckungsgefahr", „infizieren" und dergleichen zurückgegriffen wird. Neu sind heute jedoch zum einen die Dimensionen der gekoppelten Systeme, zum anderen die technische Beschleunigung der Prozesse, die die gesellschaftlichen Strukturen wie das individuelle Reaktionsvermögen zu überfordern scheinen, und zum dritten die zunehmende Abhängigkeit der Menschen von deren reibungslosen Funktionieren.

[1] z. B. Bundesministerium des Innern 2009a: 9–12, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2011: 30, Bundesministerium für Bildung und Forschung 2007: 5, Reichenbach et al. 2008:10

[2] Renn, Ortwin/Schweizer, Pia J./Dreyer, Marion/Klinke, Andreas 2007: Risiko. Über den gesellschaftlichen Umgang mit Risiko, München:176

[3] vgl. Renn et al. 2007:176

[4] State-of-the-Art Studien, die Vorträge und die Workshopdokumentation finden sich unter www.sicherheit-forschung.de

Portraitfotos: FOES, Foto oben: ZOES, Klaus Dombrowsky

Jochen Schiller wies anlässlich eines Expertengesprächs am Deutschen Bundestag auf das Verletzlichkeitsparadoxon hin, das systemische Risiken kennzeichnet: „Kommunikationstechniken funktionieren ‚fast immer'; daraus ergibt sich eine große Erwartungshaltung in der Bevölkerung bis hin zu einem medienwirksamen Aufschrei, wenn z. B. das Mobilfunksystem auch nur teilweise, für nur einen Teil der Nutzer und auch nur für eine relativ kurze Zeit ausfällt. Gerade mit zunehmender Robustheit und eigentlich geringer Störanfälligkeit schleicht sich ein Gefühl der (trügerischen) Sicherheit ein."[5] Folge dieses Phänomens ist, dass derzeit ein unverbundenes Nebeneinander von Ignoranz auf der einen und anekdotischen Horrorbotschaften auf der anderen Seite existiert. Zum einen operieren Mobilfunkbetreiber mit veralteten Sicherheitsstandards, geht Politik der Frage nach wirksamen Anreizsystemen für mehr Sicherheit aus dem Weg, sind (mobile) Netze in der Administration aller Ebenen und Institutionen unersetzbar geworden, fehlt eine ehrliche Kommunikation der Unternehmen über Datenverluste, Spionage oder Sabotage und eine verantwortungsvolle Risikokommunikation der Politik über die grundsätzliche Unsicherheit und Nichtbeherrschbarkeit von Kommunikationsnetzen. Zum anderen konzentrieren sich Medien auf der Suche nach skandalträchtigem Stoff zunehmend auf Cybercrime und wieder andere Unternehmen nutzen reale Sicherheitsvorfälle als Verkaufsargument ihrer sicherheitstechnischen Wunderwaffen.

Und obwohl systemische Risiken immer wieder Gegenstand wissenschaftlicher Analysen sind, mangelt es an der Akzeptanz begrenzter Handlungsräume. Der Wunsch nach Strategien und Sicherheitsmaßnahmen übersieht den Charakter des systemischen Risikos. Das Ziel der Klassifikation und Kartographie systemischer Risiken kann Wissenschaft nur für einzelne Problembereiche erreichen. Allumfassende Lösungsansätze zur vollständigen Sicherung kann es nicht geben; vielmehr bedarf es zukünftig (kreativer) Strategien des Umgangs mit dem Nichtfunktionieren.

Systemische Risiken lassen sich längst nicht mehr allein über die klassischen Komponenten Eintrittswahrscheinlichkeit und Schadensausmaß bewerten. Vielmehr müssen qualitative Faktoren wie wahrgenommenes Katastrophenpotenzial, Unsicherheit, Kontrollierbarkeit, Schrecklichkeit, systemisches Vertrauen und weitere berücksichtigt werden.[6] Die Forschung um qualitative Kriterien der Risikowahrnehmung ist ebenso wie die grundlegenden Erkenntnisse um die Kriterien systemischer Risiken bereits seit den 90er Jahren des vergangenen Jahrhunderts etabliert.[7] Es ist deshalb erstaunlich, dass in Folge des Reaktorunfalls in Fukushima der

Eindruck entstand, als habe die Definition systemischer Risiken vor über 10 Jahren nicht stattgefunden. Nach wie vor werden systemische Risiken wie „einfache Risiken" behandelt[8], als ob sie sich – genügend Zeit und Geld vorausgesetzt – vollständig beherrschen ließen.

Damit ist die Frage nach dem Wissenstransfer als einer der Kernfragen unserer wissensbasierten Gesellschaft berührt. Wie kann sich eine gesellschaftliche Praxis entwickeln, die sensibilisiert ist für unvorhersehbare Ereignisse, dabei eher auf *coping*, als auf *control & command* in eingeübten Routinen setzt? Wo ist der gesellschaftliche Ort, an dem der öffentliche Diskurs über die Chancen und Risiken von komplexen und grundsätzlich unsicheren, dabei aber effizienten, profitablen und für Individuum, Wirtschaft und Gesellschaft eben auch „praktischen" Systemen stattfinden kann?

Diese Fragen sind nicht trivial und nicht simpel durch den Ruf nach „der Politik" zu lösen. Thymian Bussemer fordert in seinem Buch „Die erregte Republik" eine neue Diskursordnung, die die drei wesentlichen Akteure – Bürger, Politiker und Journalisten – besser als bisher zu Problemlösungen befähigt. Dafür müssten sie „die vorherrschenden schwarz-weiß Zeichnungen der Realität durch ein ambivalenteres Bild der Welt ersetzen, ... Alle am öffentlichen Diskurs Beteiligten müssen ... die Welt in ihrer ganzen Kompliziertheit in den Blick ... nehmen."[9]

Das Zukunftsforum Öffentliche Sicherheit am Deutschen Bundestag hat in seinen inzwischen 14 Foren und das vom Bundesforschungsministerium geförderte Forschungsforum in seinen fünf Workshops solche Diskursräume eröffnet. Es wäre gut, solche Ressourcen auszubauen und systematisch weiterzuentwickeln.

Literatur

Bonß, W. (1995). Vom Risiko: Unsicherheit und Ungewissheit in der Moderne. Hamburg: Hamburger Edition.

Buergin, R. (1999). Handeln unter Unsicherheit und Risiko. Eine Zusammenschau verschiedener Zugänge und disziplinärer Forschungslinien. Arbeitsbericht 27-99. Albert-Ludwigs-Universität Feiburg: Institut für Forstökonomie.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (Hrsg.) 2011: Vierter Gefahrenbericht. Schriften der Schutzkommission, Bonn.

Bundesministerium des Innern (o.J.). Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie). http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/Sicherheit/SicherheitAllgemein/kritis.pdf?__blob=publicationFile, S. 9-11.

Jungermann, H. & Slovic, P. (1993a). Charakteristika individueller Risikowahrnehmung. In Bayerische Rückversicherung (Hrsg.), Risiko ist ein Konstrukt. Wahrnehmungen zur Risikowahrnehmung (S. 90-107). München: Knesebeck.

Reichenbach, Gerold/Wolff, Hartfrid/Göbel, Ralf/Stokar von Neuforn, Silke 2008: Risiken und Herausforderungen für die Öffentliche Sicherheit in Deutschland. Szenarien und Leitfragen. Grünbuch des Zukunftsforums Öffentliche Sicherheit, Berlin.

Renn, Ortwin/Schweizer, Pia J./Dreyer, Marion/Klinke, Andreas 2007: Risiko. Über den gesellschaftlichen Umgang mit Risiko, München.

Renn, O. & Zwick, M. (1997). Risiko- und Technikakzeptanz. Berlin: Springer.

[5] Prof. Dr.-Ing. Jochen Schiller, Projektleiter des Forschungsforums, anlässlich des Expertengesprächs zum Thema „Sicherheit im Netz" der Enquete Kommission „Internet und digitale Gesellschaft" des Deutschen Bundestages, siehe http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZustrSi_2011-11-28_oeffentliches_Expertengespraech/PGZuStSi_2011-11-28_Expertengespraech_Stellungnahme_ProfSchiller.pdf

[6] Vgl. Renn/Zwick 1997: 92.

[7] Vgl. Buergin 1999, Bonß 1995, Jungermann & Slovic 1993, Renn & Zwick 1997.

[8] „However, it is a consistent finding that in most of these cases, the risks are treated, assessed and managed as if they were simple. The assessment and management routines in place do not do justice to the nature of such risks. The consequences of this maltreatment ranges from social amplification or irresponsible attenuation of the risk, sustained controversy, deadlocks, legitimacy problems, unintelligible decisionmaking, trade conflicts, border conflicts, expensive rebound measures, and lock-ins." Ortwin Renn, Andreas Klinke, Marjolein van Asselt, "Coping with Complexity, Uncertainty and Ambiguity in Risk Governance: A Synthesis", AMBIO (2011) 40:231–246 DOI 10.1007/s13280-010-0134-0

[9] Thymian Bussemer, Die erregte Republik, Stuttgart 2011, S. 237/238.

Fotos: ZOES, Klaus Dombrowsky

Bevölkerungsschutz in Deutschland – Bilanz und Perspektiven

Norbert Seitz,
Abteilungsleiter Krisenmanagement und Bevölkerungsschutz, BMI

von Norbert Seitz,
Bundesministerium des Innern

Das Jahr 2011 war geprägt vom Überdenken der Strukturen, Stärken und Schwächen unseres Bevölkerungsschutzes. Die Ereignisse in Japan zu Beginn des Jahres führten uns eindringlich vor Augen, dass große Katastrophen und Industrieunfälle mit komplexen Schadenszenarien auch hochmoderne Industrienationen empfindlich treffen können. „Restrisiken“ und Grenzen staatlicher Vorsorge wurden greifbar.

Zugleich war es zehn Jahre nach den Ereignissen des 11. September 2001 an der Zeit Bilanz zu ziehen. Die Terroranschläge in den USA brachten die große Zäsur auch in unserem nationalen Bevölkerungsschutz. Zuvor war der Zivilschutz auf Ebene des Bundes rückläufig. Nach Beendigung des Kalten Krieges erschienen Vorkehrungen, um die Bevölkerung vor verteidigungsbedingten Gefahren zu schützen, obsolet. Aber nach 2001 und den Sommerhochwassern 2002 entstand ein grundsätzlich neues Bewusstsein für Zivil- und Katastrophenschutzfragen. Bund und Länder vereinbarten eine „Neue Strategie für einen modernen Bevölkerungsschutz“, gekennzeichnet durch eine bessere Verzahnung, Abstimmung und partnerschaftliche Zusammenarbeit aller Akteure über föderale Grenzen hinweg und eine stärkere Verantwortung des Bundes zur Unterstützung der Länder bei der Bewältigung von Großschadenslagen.

Als neue Instrumente in der Bund-Länder-Zusammenarbeit wurden das Gemeinsame Melde- und Lagezentrum des Bundes und der Länder, die Datenbank deNIS für das Informations- und Ressourcenmanagement, das satellitengestützte Warnsystem des Bundes und als organisatorischer Schwerpunkt das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe gegründet. Das BBK verknüpft alle Bereiche der zivilen Sicherheitsvorsorge zu einem wirksamen Schutzsystem für die Bevölkerung und ihre Lebensgrundlagen („Bevölkerungsschutz“) und unterstützt mit Ausstattung und Expertise die Länder bei Großschadenslagen („Katastrophenhilfe“).

Die großen Entscheidungen im Bevölkerungsschutz sind damit gefallen. Die „Neue Strategie“ ist – letzter wesentlicher Schritt war das neue Gesetz über den Zivilschutz und die Katastrophenhilfe des Bundes im Jahr 2009 – im Wesentlichen umgesetzt, auch wenn noch einige Punkte abzuarbeiten sind, so die bundesweite Risikoanalyse. Ferner wird das satellitengestützte Warnsystem des Bundes, mit dem wir binnen weniger Sekunden Gefahrenwarnungen und Verhaltensweise über Rundfunk und Fernsehen an die Bevölkerung herausgeben können, jetzt ausgebaut zu einem modularen Warnsystem. Daran können diverse zusätzlich Warnmittel angeschlossen werden – darunter Sirenen, Rauchwarnmelder oder Cell Broadcast. Wichtig ist ein „Weckeffekt“. Neu ist auch eine stärkere regionale Differenzierung: Regionale Leitstellen können

mit eingerüstet werden, und Warnungen können regional begrenzt herausgegeben werden. Die technischen Voraussetzungen hat der Bund bereits geschaffen.

Der medizinische Bevölkerungsschutz war Gegenstand umfassender Diskussionen und Beratungen in einer Bund-Länder-Arbeitsgruppe, die 2012 ihren Abschlussbericht mit Handlungsempfehlungen in verschiedenen Feldern von der Sanitätsmaterialbevorratung bis zur Krankenhausalarmplanung der IMK vorlegen wird.

Insgesamt sind wir heute mit unserem dezentralen Notfallvorsorgesystem, das im Ereignisfall von unten bis ganz oben aufwachsen kann und den nach 2001 für die Bund-Länder-Zusammenarbeit neu installierten Instrumenten gut und richtig aufgestellt. Aber wir dürfen nicht stehen bleiben. Unser Bevölkerungsschutz muss sich wandelnden Rahmenbedingungen anpassen, um zukunftsfähig zu sein.

Seine Stärke und Schlagkraft verdankt unser System den vielen freiwilligen Helfern in Feuerwehren, Hilfsorganisationen und Regieeinheiten. Angesichts einer Vielzahl geänderter Rahmenbedingungen von der Wehrstrukturreform über den demographischen Wandel bis hin zur Fülle konkurrierender Freizeitangebote ist die langfristige Sicherstellung eines flächendeckenden Freiwilligennetzwerkes heute die zentrale Herausforderung für unseren nationalen Bevölkerungsschutz. Hierzu gilt es, laufende Projekte zur Unterstützung und Stärkung des Ehrenamtes weiterzuentwickeln und konsequent umzusetzen, so beispielsweise den Wettbewerb um den Förderpreis „Helfende Hand“ oder die Zusammenarbeit mit Schulen und die Zertifizierung von Ausbildungsabschlüssen beim THW. Zur Entwicklung strategischer Konzepte hat das Bundesministerium des Innern in Absprache mit den Ländern ein umfassendes Forschungsprojekt initiiert. Wichtig ist, dass die ehrenamtlichen Strukturen der heutigen Lebenswirklichkeit gerecht werden. Wenn es dafür neuer Formate wie befristeter oder projektbezogener Engagements bedarf, einer stärkeren Unterstützung durch hauptamtliche Kräfte oder einer organisierten Einbindung spontaner Helfer in akuten Großschadenslagen, müssen wir hierfür Wege schaffen.

Wir müssen eine Idee entwickeln, wie der Bevölkerungsschutz 2020/2030 aussehen kann. Insoweit besteht auch eine hohe Erwartung an das Zukunftsforum und in diesem Sinne wertvolle Beiträge.

Portraitfoto: BMI

Ergebnisbewertung

Chancen für die Sicherheit, Chancen durch Sicherheit

Prof. Dr. Hermann J. Thomann, Vorstandsvorsitzender ZOES

von Prof. Dr. Hermann J. Thomann, ZOES

Wir haben in dieser zweiten Jahrespublikation dem Denken in Extremen einen Vorrang eingeräumt vor dem routinierten Umgang mit Risiken für die öffentliche Sicherheit, denen sich unsere Gesellschaft tagtäglich ausgesetzt sieht. Das Undenkbare zu denken hat im Bevölkerungsschutz seine Berechtigung, weil es von uns abverlangt, die Grenzen unserer Belastbarkeit zu berechnen und unsere Bewältigungsfähigkeiten – zunächst gedanklich – auszubauen.

In den Foren tauchte die Frage auf, ob es nicht letztlich die Extremerfahrungen sind, die eine Änderung von Einstellungen erst herbeiführen und notwendige Richtungswechsel einleiten. Der durch einen Extremtsunami ausgelöste Atomunfall in Fukushima hat diese Annahme bestätigt: Unter dem Eindruck der Katastrophe haben sich einige Regierungen zu einer Neubewertung der Kernenergie bzw. zum Ausstieg entschieden. Diese politische Entscheidung, die im Sinne der öffentlichen Sicherheit und des Umweltschutzes getroffen wurde, beschert uns wiederum neue Risiken, was die Versorgungssicherheit mit Strom anbelangt. Doch stellen sich diese Risiken als das kleinere Übel dar, das auf lange Sicht besser beherrschbar und verantwortbar erscheint.

Unser Ausflug an die Ränder des Vorstellbaren sollte jedoch nicht zu der verzerrten Wahrnehmung führen, das Leben in einer modernen Technologiegesellschaft wie der unseren sei so gefährlich wie nie zuvor. Dies ist sicherlich nicht der Fall. Es gibt wenige Länder auf der Welt, die sich eines so hohen Sicherheitsniveaus in allen Bereichen des Lebens erfreuen können wie Deutschland. Hierzu gehört auch die Erkenntnis, dass technischer Fortschritt wichtig und richtig ist, weil er in der Regel Erleichterungen verschafft und nutzenstiftende Möglichkeiten eröffnet. Manche neuen Technologien bedürfen aber auch einer kritischen Wertung, bevor sie für die allgemeine Nutzung freigegeben werden (Ich denke hier an die pränatale Medizin, an die Erzeugung genveränderter Lebensmittel, an das Klonen von Lebewesen usw.). Die Sicherheitsansprüche der Bürger sind gewachsen, die Risikoperzeption hat sich intensiviert und neue Risiken sind unbestreitbar auf den Plan getreten: Die Beiträge in dieser Jahrespublikation unterstreichen dies.

Risiken in komplexen Systemen verstärken sich gegenseitig. Ereignisse, deren Schadensausmaß relevant ist für die öffentliche Sicherheit, können ihrerseits Folgen nach sich ziehen, die in einer Art Domino-Effekt weitere Schäden provozieren. Unsere modernen Infrastrukturen stellen sich als komplexes Räderwerk aus miteinander verbundenen, interdependenten und adaptiven Systemen dar, von deren störungsfreiem Funktionieren Menschen in ihrem privaten Lebensumfeld, staatliche Institutionen und Wirtschaftsbranchen abhängen. Es ist nicht nur die Verzahnung der Infrastrukturen, die die Analyse der immanenten Risiken zu einem komplizierten Unterfangen macht, sondern auch die Vielzahl der Abhängigkeiten und die Geschwindigkeit von Kaskadeneffekten, die sich durch IT-gestützte Systeme fortpflanzen. Das Problem der Beherrschbarkeit von Risiken verschärft sich dadurch, dass die menschliche Entscheidungsgeschwindigkeit nicht mit der Geschwindigkeit von IT-basierten Systemen Schritt halten kann.

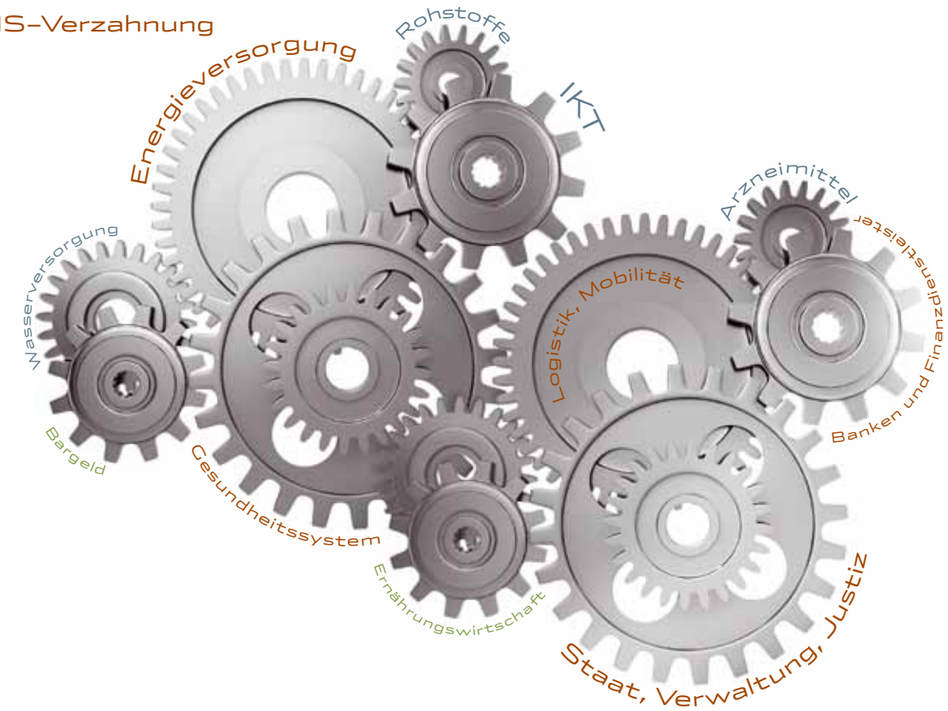
Dass die Nutzung risikobehafteter Technologien jedoch auch enorme Vorteile hat, lässt sich anhand der Internettechnologie am besten verdeutlichen (z.B. rasche Informationsbeschaffung, Nutzung gemeinsamer Plattformen, „informationelle Globalisierung"). Erst wenn das Web gestört ist, kommt uns dies zu Bewusstsein.

Priorisierung von Risiken und Schutzmaßnahmen

In einem sich dynamisch verändernden Risikoumfeld müssen sich auch die Abwehrmaßnahmen dynamisch anpassen. Um klug die Verantwortungsbereiche für die öffentliche Sicherheit zu bemessen, sollten wir womöglich stärker differenzieren zwischen Risiken für das wirtschaftliche Gedeihen, Risiken für das soziale Gefüge und Risiken für Leib und Leben. Letztere – die existenziellen Risiken - erfordern verständlicherweise die intensivste Form der Prävention und im Schadensfall Schutzmaßnahmen, die eindeutig in die Zuständigkeit staatlicher Stellen fallen: Wenn es dabei um Maßnahmen geht, die in die Grundrechte der Bürger eingreifen, dann hat der Staat seine Schutzpflichten nach rechtsstaatlichen Maßstäben zu erfüllen. Wenn es hingegen darum geht, Risiken für das wirtschaftliche Gedeihen abzufedern, dann sind die betroffenen Wirtschaftsakteure – wie beispielsweise Betreiber Kritischer Infrastrukturen - dazu aufgerufen, ihrer Verantwortung für die öffentliche Sicherheit gerecht zu werden. Risiken für das soziale Gefüge schließlich werden am frühesten von den betroffenen Bürgern wahrgenommen: Hier besteht eine kommende Herausforderung darin, die Bürger zur Partizipation zu ermutigen, dazu, Verantwortung für ihren unmittelbaren Lebensbereich zu übernehmen, auch im Sinne der öffentlichen Sicherheit. Inklusionsprojekte in sogenannten sozialen Brennpunkten sind beeindruckende Beispiele dafür, wie die Menschen der zunehmenden Bandenkriminalität und Ghettoisierung wirksam begegnen. Diese positiven Trends gilt es angesichts der zunehmenden Verstädterung zu fördern. Mehr dazu in den kommenden Foren.

Tatsache ist: Wir können nicht sämtliche Risiken auf null reduzieren, oft gelingt es uns nur, deren Eintrittswahrscheinlichkeit herabzusetzen. Künftig wird es im Zukunftsforum auch darum gehen, Risiken nach Wichtigkeit abzustufen und Schutzprioritäten festzulegen. Öffentliche Sicherheit jedoch ausschließlich im Sinne einer Risikobetrachtung und Gefahrenabwehr wahrzunehmen, greift meines Erachtens zu kurz. Es gilt auch, öffentliche Sicherheit im Sinne einer Chancenwahrnehmung zu begreifen. Dass Freiheit und Sicherheit ein Wertepaar sind, sollte dabei Konsens sein.

KRITIS–Verzahnung



Grafik: ZOES

Portraitfoto: ZOES, Klaus Dombrowsky

Nachwort und Ausblick auf das Jahresthema 2012

Demographischer Wandel – Herausforderungen für ländliche Räume, Städte und Deutschland in Europa

Clemens Binninger, Mitglied des Deutschen Bundestages von CDU/CSU und Beiratsmitglied des ZOES

Die Rede vom „demographischen Wandel" ist mittlerweile in aller Munde. Er erscheint regelmäßig wie ein Menetekel in medialen Diskussionsrunden und hinterlässt oft eine Spur der Ratlosigkeit. Denn wie auf die Bevölkerungsentwicklung in Deutschland mit adäquaten politischen Maßnahmen zu reagieren sei, darüber gehen die Meinungen auseinander. Einig ist man sich aber in einem Punkt: Die tiefgreifende Veränderung des Altersgefüges ist aktuelle Herausforderung und Zukunftsthema gleichermaßen. Sie beeinflusst die Lebensplanung für das Alter, die Mobilität, den Arbeitsmarkt und das Berufsleben. Sie wirkt sich schon jetzt auf Produktgestaltung, kulturelle Angebote, Immobilienmarkt und Gesundheitsdienstleistungen aus. Und sie stellt unsere Sozialsysteme vor große Herausforderungen.

Vergleichsweise wenig öffentlich diskutiert wird indes über die Auswirkungen des demographischen Wandels für die Sicherheit in Deutschland. Dabei prägt die Bevölkerungsentwicklung auch und gerade die öffentliche Sicherheit und wirft Fragen auf:

Wie entwickelt sich die Kriminalität in einer alternden Gesellschaft? Gibt es zukünftig andere Straftaten? Wird der abnehmende Anteil von jungen Menschen für einen Rückgang der Kriminalität sorgen? Oder wird umgekehrt die Zuwanderung in urbane Räume kriminelle Milieus anwachsen lassen?

Wie wird sich unsere Gesellschaft verändern? Wird sie ängstlicher, zurückgezogener, risikoaverser werden? Wie werden die Selbsthilfefähigkeiten einer alternden Bevölkerung im Katastrophenfall aussehen?

Wie sind Sicherheitsbehörden, Polizei oder Freiwilligen-Organisationen wie die Feuerwehren, die Rettungsdienste und das Technische Hilfswerk aufzustellen? Wie kann mit einem Personal- und Fachkräftemangel umgegangen werden? Welche technische Ausstattung wird in Zukunft gefragt sein? Sind organisatorische Veränderungen, neue Institutionen oder eine Fokussierung staatlicher Sicherheitsaufgaben notwendig?

Das sind nur einige Aspekte, mit denen sich das Zukunftsforum Öffentliche Sicherheit im Rahmen des Jahresthemas 2012 befassen wird. Dabei wird deutlich: Die mit dem demographischen Wandel verbundenden Herausforderungen werden nicht überall gleich sein. Polizei, Feuerwehr, Rettungsdienste und Katastrophenschutz etwa müssen in dünn besiedelten ländlichen Regionen anderen Anforderungen gerecht werden als in urbanen Ballungsräumen. Deshalb befassen sich im Jahr 2012 zwei Zukunftsforen mit den Perspektiven und Herausforderungen für die öffentliche Sicherheit im ländlichen Raum und in der Stadt, ergänzt durch ein drittes Zukunftsforum, das sich mit übergeordneten Fragestellungen der öffentlichen Sicherheit im europäischen Rahmen beschäftigt.

Es gehört zu den vornehmsten Aufgaben des Staates, Sicherheit für seine Bürger zu gewährleisten. Gerade deshalb stellt die Veränderung in der Altersstruktur der Bevölkerung auch in diesem Bereich eine wichtige politische Gestaltungsaufgabe der kommenden Jahre dar. Dabei kommt es darauf an, die Auswirkungen der demographischen Veränderungen frühzeitig zu erkennen, um gestalten zu können. Es geht darum, Risiken zu identifizieren, um vorbeugen zu können, aber auch darum, Chancen zu begreifen, um sie nutzen zu können. Dazu möchte das Zukunftsforum Öffentliche Sicherheit mit dem Jahresthema „Demographischer Wandel – Herausforderungen für ländliche Räume, Städte und Deutschland in Europa" einen Beitrag leisten.

Clemens Binninger, MdB
Berlin, im Januar 2012

Portraitfoto: Clemens Binninger

Das Zukunftsforum Öffentliche Sicherheit e. V. dankt allen Mitwirkenden für ihren Beitrag zum Gelingen der Jahrespublikation:

Prof. Dr. Gerhard Adrian
Präsident des Deutschen Wetterdienstes

Dr. Michael Arzberger
Vice President Research & Development, Power Plus Communications AG

Michael Bartsch
Manager Marketing & Communications, T-Systems International GmbH

Marie-Luise Beck
Projektkoordinatorin des Forschungsforums Öffentliche Sicherheit

Clemens Binninger
Mitglied des Deutschen Bundestages (CDU/CSU), Mitglied des Innenausschusses

Stephan Boy
Geschäftsführer, KKI GmbH

Bernhard Brinkmann
Mitglied des Deutschen Bundestages (SPD), Mitglied des Haushaltsausschusses

Albrecht Broemme
Präsident der Bundesanstalt Technisches Hilfswerk

Angelika Brunkhorst
Mitglied des Deutschen Bundestages (FDP), Mitglied und Obfrau der FDP-Bundestagsfraktion im Ausschuss für Umwelt, Naturschutz und Reaktorsicherheit

Raimund Bücher
Vorsitzender des Bundesverbandes Betrieblicher Brandschutz/Werkfeuerwehrverband e. V.

Manfred Buhl
Vorsitzender der Geschäftsführung, Securitas Deutschland Holding GmbH & Co. KG

Detlev L. Burgartz
Inhaber, Pro Versicherer

Ernst Burgbacher
Mitglied des Deutschen Bundestages (FDP) sowie parlamentarischer Staatssekretär im Bundesministerium für Wirtschaft und Technologie

Axel Dechamps
Deutsches Komitee für Katastrophenvorsorge e. V., stellvertretender Vorstandsvorsitzender des Zukunftsforums Öffentliche Sicherheit e. V.

Lutz Diwell
Staatssekretär a. D.

Prof. Dr. Wolf Dombrowsky
Lehrstuhl Katastrophen-Management, Steinbeis Business Academy

Sebastian Edathy
Mitglied des Deutschen Bundestages (SPD), stellvertretendes Mitglied des Innenausschusses

Christian Endreß
wissenschaftlicher Mitarbeiter an der Universität Witten/Herdecke

Dr. Johann Fichtner
Corporate Research and Technologies CT T DE, Siemens AG

Michael von Foerster
Bosch Sicherheitssysteme GmbH, Vorsitzender der ZVEI-Landesstelle Berlin

Gabriele Fograscher
Mitglied des Deutschen Bundestages (SPD), Mitglied des Sportausschusses, des Innenausschusses sowie stellvertretendes Mitglied des Verteidigungsausschusses

Dr. Bernhard Gause
Mitglied der Hauptgeschäftsführung des Gesamtverbandes der Deutschen Versicherungswirtschaft e. V.

Dr. Clemens Gause
Geschäftsstelle, Zukunftsforum Öffentliche Sicherheit e. V.

Dr. Lars Gerhold
wissenschaftlicher Koordinator des Forschungsforums Öffentliche Sicherheit

Ralf Göbel
stellvertretender Abteilungsleiter der Bundespolizei im Bundesministerium des Inneren

Dr. Dietmar Gollnick
Vorsitzender der Geschäftsführung, e*Message – Wireless Information Services Deutschland GmbH

Prof. Dr. Dr. René Gottschalk
stellvertretender Amtsleiter des Stadtgesundheitsamtes Frankfurt

Dr. Helmut Grimm
Sonderbeauftragter des Vorstandes, Tengelmann Warenhandelsgesellschaft KG

Michael Hange
Präsident des Bundesamtes für Sicherheit in der Informationstechnik

Michael Hartmann
Mitglied des Deutschen Bundestages (SPD), innenpolitischer Sprecher der SPD-Fraktion

Dr. Iris Henseler-Unger
Vizepräsidentin der Bundesnetzagentur

Dieter Hesse
Leiter Vertriebsregion Ost, Dräger Safety AG & Co. KGaA

Dr. Hans-Dieter Heumann
Präsident der Bundesakademie für Sicherheitspolitik

Dr. Wolf Junker
Referatsleiter für Zivile Sicherheit im Bundesministerium für Bildung und Forschung

Dieter Kaden
Vorsitzender der Geschäftsführung, Deutsche Flugsicherung GmbH

Robert Kamrau
Business Development Executive Public Sector, IBM Deutschland GmbH

Dr. Ibrahim Karasu
Geschäftsführer Retail Banking und Banktechnologie, Bundesverband deutscher Banken

Prof. Dieter Kempf
Vorstandsvorsitzender, DATEV eG, sowie Präsident, BITKOM e. V.

René Kiefer
Leiter Services & Maintenance, Siemens AG

Uwe Kirsche
Leiter Presse- und Öffentlichkeitsarbeit des Deutschen Wetterdienstes

Hans-Peter Kröger
Präsident des Deutschen Feuerwehrverbandes e. V.

Norbert Kronenberg
Referatsleiter beim Deutschen Städtetag

Prof. Dr. Hans-Jürgen Lange
Universität Witten/Herdecke, Fakultät für Kulturreflexion

Peter Lange
Kanzler der Freien Universität Berlin

Benedikt Liefländer
Bereichsleiter Notfallfürsorge des Malteser Hilfsdienstes e. V.

Yitzhak Lifshitz
Direktor Konzernsicherheit, Axel Springer AG

Mauro Lima-Vaz
Niederlassungsleiter und Prokurist, Bosch Sicherheitssysteme GmbH

Wolfgang Lohmann
Vizepräsident des Bundespolizeipräsidiums

Kirsten Lühmann
Mitglied des Deutschen Bundestages (SPD), Mitglied des Ausschusses für Verkehr, Bau und Stadtentwicklung sowie Mitglied des Innenausschusses

Prof. Dr. Wolf-Dieter Lukas
Leiter der Abteilung „Schlüsseltechnologien – Forschung für Innovationen" im Bundesministerium für Bildung und Forschung

Jörg Marks
Leiter Siemens Building Technologies GmbH & Co KG, Siemens AG

Alexander C. Mayer
Vertrieb kommunale Rechenzentren, Cisco Systems GmbH

Patrick Meinhardt
Mitglied des Deutschen Bundestages (FDP), Mitglied des Ausschusses für Bildung, Forschung und Technikfolgenabschätzung

Dr. Horst Miska
Mitglied der Schutzkommission beim Bundesministerium des Inneren

Hildegard Müller
Hauptgeschäftsführerin des Bundesverbandes der Energie- und Wasserwirtschaft

Herbert Nalbandjan
General Manager, 3M Deutschland GmbH

Ortwin Neuschwander
Unternehmensberatung Neuschwander

Dr. Konstantin von Notz
Mitglied des Deutschen Bundestages (BÜNDNIS 90/DIE GRÜNEN), Mitglied des Innenausschusses sowie Mitglied der Enquete-Kommission „Internet und digitale Gesellschaft"

Uwe Osterkamp
Vorstand, ProDV Software AG

Dr. Sigurd Peters
Leiter des Fachbereichs „Katastrophenmedizin National" der Deutsch-Europäischen Kommission für Bevölkerungsschutz e. V.

Helmut Picko
Leiter des Dezernates „Wirtschaftskriminalität und IuK-Kriminalität" beim Landeskriminalamt NRW

Prof. Dr. Johann-Christian Pielow
Geschäftsführender Direktor des Instituts für Berg- und Energierecht an der Ruhr Universität Bochum

Gisela Piltz
Mitglied des Deutschen Bundestages (FDP), Mitglied des Sportausschusses sowie im Ausschuss für Planung und Stadtentwicklung, stellvertretende Vorsitzende der FDP-Bundestagsfraktion

Detlef Raphael
Beigeordneter beim Deutschen Städtetag

Dr. Peer Rechenbach
Vorsitzender des Arbeitskreises V der Landesinnenministerkonferenz, Behörde für Inneres und Sport der Freien und Hansestadt Hamburg

Gerold Reichenbach
Mitglied des Deutschen Bundestages (SPD), Mitglied des Innenausschusses

Cornelia Rogall-Grothe
Staatssekretärin im Bundesministerium des Inneren, Beauftragte der Bundesregierung für Informationstechnik

Dr. Erich Rome
Projektleiter am Fraunhofer-Institut für Intelligente Analyse- und Informationssysteme

Prof. Dr. Jochen H. Schiller
Vizepräsident der Freien Universität Berlin, Projektleiter des Forschungsforums Öffentliche Sicherheit

Bernhard Schneck
Technischer Geschäftsführer, GeNUA GmbH

Dr. Sandra Schulz
Vice President Political Affairs und Leiterin Hauptstadtrepräsentanz Berlin, Thales Deutschland GmbH, Programmvorstand des Zukunftsforums Öffentliche Sicherheit e. V.

Armin Schuster
Mitglied des Deutschen Bundestages (CDU), innenpolitischer Sprecher

Prof. Dr. Jean-Pierre Seifert
TU Berlin und Deutsche Telekom Laboratories, Fachgebiet „Security in Telecommunications"

Norbert Seitz
Abteilungsleiter „Krisenmanagement und Bevölkerungsschutz" im Bundesministerium des Inneren

Joachim Steig
Key Account Director Public Security Marketing & Sales, Thales Deutschland GmbH

Prof. Dr. Jürgen Stock
Vizepräsident des Bundeskriminalamtes

Matthias L. Strate
Fachbereichsleiter „Rettungsdienst und Bevölkerungsschutz" bei der Johanniter-Unfall-Hilfe e. V.

Ralph Stühling
Kreisbrandinspektor, Deutscher Feuerwehrverband e. V.

Frank Tempel
Mitglied des Deutschen Bundestages (Die Linke), Mitglied des Innenausschusses, stellvertretendes Mitglied des Sportausschusses sowie stellvertretendes Mitglied des Ausschusses für Gesundheit

Prof. Dr. Hermann J. Thomann
Globaler Geschäftsfeldleiter Consulting, TÜV Rheinland Group sowie Vorstandsvorsitzender des Zukunftsforums Öffentliche Sicherheit e. V.

Serkan Tören
Mitglied des Deutschen Bundestages (FDP), Mitglied des Ausschusses für Menschenrechte und Humanitäre Hilfe, Mitglied des Innenausschusses

Bernhard Tschöpe
Landesvorsitzender Berlin des Bundesverbandes Betrieblicher Brandschutz/Werkfeuerwehrverband Deutschland e. V., Leiter Standortsicherheit, Bayer Schering Pharma AG

Christoph Unger
Präsident des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe

Clemens Graf von Waldburg-Zeil
Vorstandsvorsitzender des Deutschen Roten Kreuzes e. V., Schatzmeister des Zukunftsforums Öffentliche Sicherheit e. V.

Prof. Dr. Lothar H. Wieler
geschäftsführender Direktor des Instituts für Mikrobiologie und Tierseuchen an der Freien Universität Berlin

Hartfrid Wolff
Mitglied des Deutschen Bundestages (FDP), Mitglied des Innenausschusses sowie Vorsitzender des Arbeitskreises Innen- und Rechtspolitik der FDP-Bundestagsfraktion

Jörg Ziercke
Präsident des Bundeskriminalamtes

Volker Zintel
freier Managementberater Luftverkehr und Sicherheit

IMPRESSUM:

Herausgeber:
Prof. Dr. Hermann J. Thomann
Axel Dechamps
Dr. Sandra Schulz
Clemens Graf von Waldburg-Zeil

V.i.S.d.P.
Dr. Clemens Gause, Berlin

Redaktion:
Dr. Susanne Schubert, Berlin

Lektorat:
Daniela von Treuenfels, Berlin

Gestaltung:
Galasix-Schack, Bodenheim b. Mainz

Druck:
Druckerei Schlesener KG, Berlin

Redaktionsschluss/Auflage:
23. 01. 2012, 1. Auflage/500