DStGB
DOKUMENTATION Nº 66

Bessere Koordination und Kommunikation

Zusammenfassung zur DStGB-Sicherheitskonferenz in Berlin 2006

DStGB
Deutscher Städte- und Gemeindebund
www.dstgb.de

Sicherheitskommunikation für Städte und Gemeinden

Sicherheit ist in den Städten und Gemeinden ein wichtiges Thema und gewinnt immer mehr an Bedeutung. Bilder von Bedrohungen, die für alle Ebenen des öffentlichen Lebens alarmierend sind, sind uns allgegenwärtig. Beispielhaft seien genannt die Bedrohungen durch den internationalen Terrorismus und verheerende Katastrophen. Immer wieder verunsichern Meldungen über (Natur-)Katastrophen die Menschen: Überschwemmungen, Wirbelstürme, Erdbeben in aller Welt, aber auch in Deutschland. Experten gehen davon aus, dass aufgrund von Klimaveränderungen derartige Katastrophen in den nächsten Jahrzehnten zunehmen werden.

Die Bevölkerung vor Gefahren aller Art zu schützen und ihr ein Höchstmaß an Sicherheit zu bieten, ist zentrale Aufgabe des Staates und seiner Behörden. Aber perfekte Sicherheit gibt es nicht in freien Gesellschaften, immer wird ein Rest Unsicherheit bleiben. Das gilt insbesondere für die Sicherheit im öffentlichen Raum. Bei allen Gefahrenlagen ist es besonders wichtig, dass die Organe der Gefahrenabwehr, die Hilfsorganisationen und auch die Bevölkerung im Rahmen ihrer Möglichkeiten zusammenwirken: die Behörden und Organisationen aufgrund ihres Auftrages und ihres Leistungsspektrums, die Bürgerinnen und Bürger durch richtiges Verhalten im Rahmen von Selbstschutz und Nächstenhilfe. Dazu müssen die Einsatzkräfte vor Ort personell und mit Sachmitteln bestmöglich ausgestattet sein.

Ein wesentlicher Baustein eines erfolgreichen Krisenmanagements ist die örtliche Informations- und Kommunikationsstrategie, wobei den Städten und Gemeinden eine wichtige Rolle zukommt. Das Unglück in Bad Reichenhall im Winter 2005/2006 hat gezeigt, welche bedeutsame Rolle der Koordination der Rettungskräfte, aber auch einer professionellen Medienarbeit zukommen.

Aus gutem Grund steht bei unserer Konferenz die „Sicherheitskommunikation" im Mittelpunkt. Sicherheitskommunikation umfasst dabei weit mehr als die üblicherweise mit dem Begriff verbundene Kommunikation über abgesicherte Kanäle. Es geht in erster Linie um die Kommunikation zwischen Behörden mit Sicherheits- und Ordnungsaufgaben. Zwischen diesen müssen die technischen Voraussetzungen dafür geschaffen werden, damit Kommunikation stattfinden kann. Darüber hinaus muss die Ausfallsicherheit der Informations- und Kommunikationsinfrastrukturen sichergestellt werden und schließlich müssen die organisatorischen Voraussetzungen dafür geschaffen werden, dass der Informationsfluss gewährleistet und ein koordiniertes Vorgehen der beteiligten Akteure möglich ist.

Zur Bewältigung von Großschadensereignissen ist ein leistungsfähiges Funksystem unerlässlich, das ein Zusammenarbeiten aller Hilfskräfte ermöglicht. Die Erfahrungen der Flutkatastrophe des Jahres 2002 haben gezeigt, wie wichtig die funktionierende Kommunikation zwischen den Einsatz-

kräften, aber auch zwischen den Hilfeleistungsorganen ist. Wir wissen sehr genau, in welche Gefahren sich einzelne Hilfetrupps befunden haben, weil die Kommunikation nicht funktionierte. Wie es mit der Einführung des Digitalfunks weiter geht, darüber wird im Einzelnen auf dieser Tagung zu sprechen sein. Auch die Finanzierungsfrage spielt für die Kommunen eine große Rolle.

Sicherheit ist in modernen Gesellschaften eine komplexe Angelegenheit. Neben äußeren Bedrohungen oder Katastrophen verstärkt der zunehmende Einsatz von Informationstechnologien den Grad der Verwundbarkeit. Denken Sie nur an die vielen Computerviren, die weltweit durch die Datennetze geschleust werden.

Wirtschaft, Gesellschaft und Staat sind immer mehr auf moderne Informations- und Kommunikationssysteme angewiesen. Viele Verkehrsampeln werden inzwischen über den Computer gesteuert. Auch für die Ausstellung von Pässen sind elektronische Systeme unabdingbar. Für Banken und Logistikunternehmen oder Fluggesellschaften, die ständig ihre Flotte online warten, ist die IT sogar existenzentscheidend. Einer sicheren Informations- und Kommunikationsinfrastruktur kommt daher größte Bedeutung zu, ja sie wird immer mehr zu einem wichtigen Standortfaktor.

Auf kommunaler Ebene brauchen wir Sicherheitskonzepte, die im Zusammenspiel mit Behörden und Einrichtungen ständig aktualisiert werden müssen und alle Bereiche möglicher Gefährdungen umfassen. So genannte Sicherheitsbeauftragte sollten jährlich einmal über den Status den Verantwortlichen berichten.

Sicherheit in Städten und Gemeinden ist darüber hinaus weit mehr als eine Frage der geeigneten Technik für die Sicherheitskommunikation. Die Weichen müssen neu gestellt werden. Dies gilt zum Beispiel für die Finanzierung von Feuerwehren und einer erweiterten Katastrophenvorsorge. Auch die Bürgerinnen und Bürger sind gefordert. Sicherheit ist keine Einbahnstraße. Wir alle sind aufgerufen, unseren Beitrag dazu beizutragen. Das kann über ehrenamtliche Tätigkeiten bis hin zur Stärkung des Selbstschutzes gehen.

Das Thema „Sicherheitskommunikation für Städte und Gemeinden" ist ein komplexes Themenfeld. Es bedarf der Vernetzung und der Zusammenarbeit zwischen Bund, Ländern und Gemeinden. Von daher freuen wir uns, dass es gelungen ist, Vertreter aller Ebenen auf unserer Sicherheitskonferenz referieren zu lassen. Die hier vorliegenden Beiträge spiegeln den Verlauf der Tagung wider und sollen es allen Interessierten ermöglichen, sich durch die Schriftfassungen der Vorträge über die verschiedenen Aspekte von Sicherheitskommunikation zu informieren. Wir danken allen Referenten herzlich für Ihre Vorträge während der Tagung und für die ausgearbeiteten Fassungen ihrer Beiträge.

Dr. Dieter Klumpp
Alcatel SEL Stiftung

Franz-Reinhard Habbel
Deutscher Städte- und Gemeindebund

Zusammenfassung

Von Ulrich Mohn

Am 31. Mai und 1. Juni 2006 veranstalteten der Deutsche Städte- und Gemeindebund (DStGB) und die Alcatel SEL Stiftung die Fachkonferenz „Sicherheitskommunikation für Städte und Gemeinden" in der Berliner Vertretung des Landes Nordrhein-Westfalen beim Bund.

In seinem Grußwort führte DStGB-Sprecher Franz-Reinhard Habbel in die Thematik der Tagung ein, die sich schwerpunktmäßig mit dem Thema Sicherheitskommunikation, aber auch mit anderen für Städte und Gemeinden aktuellen Sicherheitsfragen befasste. Bei allen Gefahrenlagen sei es wichtig, dass die Organe der Gefahrenabwehr, die Hilfeleistungsorganisationen, aber auch die Bevölkerung im Rahmen ihrer Möglichkeiten zusammenwirken: Behörden und Organisationen aufgrund ihres Auftrages und ihres Leistungsspektrums, Bürgerinnen und Bürger durch richtiges Verhalten im Rahmen von Selbstschutz und Nächstenhilfe. Dies unterstreiche, wie wichtig es ist, die Einsatzkräfte vor Ort personell und sächlich gut auszustatten. Habbel hob besonders die kommunalen Kräfte im deutschen Sicherheitssystem hervor und erinnerte an die Finanzverantwortung des Staates für die Finanzierung von Feuerwehren und einer erweiterten Katastrophenvorsorge.

Digitaler Sprechfunk

Der Berliner Innensenator Dr. Ehrhart Körting ging davon aus, dass die Einführung des digitalen Sprechfunks unmittelbar bevorsteht. Kernpunkt für einen sicheren Betrieb des digitalen Sprechfunks sei ein bundeseinheitlich bereitgestelltes Netz. Sensible Bereiche nicht zu vernetzen und Insellösungen zu wählen, wäre laut Körting ein Rückschritt. Für einen „System-Flickenteppich" sei schlicht kein Geld vorhanden. Wichtiger Punkt in der Diskussion um die Einführung des Digitalfunks sei immer wieder die Kostenfrage. Hier müsse oft zwischen Ressourcenschonung und Risikoabsicherung entschieden werden. Kritiker müssten aber bedenken, dass möglicher Schaden durch Betriebsstörungen bei veralteter Technik meist weitaus kostenintensiver ausfallen könne als die Investition in moderne und sichere Kommunikationssysteme.

Mit Blick auf die aktuelle Bundespolitik sagte Körting: „Der Bund darf nicht mehr Kompetenz bei der Sicherheit verlangen und sich gleichzeitig aus der Finanzverantwortung ziehen." Welcher Aufwand für digitale Kommunikationssicherheit eingeplant werde und wer ihn letztlich zahle, sei aktuell die entscheidende Frage. Berlin investiere 40 Millionen Euro in die Umstellung auf den Digitalfunk. Auf Nachfrage räumte Körting ein, dass der Digitalfunk in der Erreichbarkeit noch technische Defizite habe. So wäre zum Beispiel ein großflächiger und kompletter Stromausfall wie letzten Winter im Münsterland für die Digitalfunktechnik nicht unproblematisch. „Für bestimmte Situationen kann man keine Vorsorge treffen", so der Berliner Innensenator.

Der frühere Leiter der Berliner Feuerwehr und jetzige Leiter der Bundesanstalt Technisches Hilfswerk (THW), Albrecht Broemme, führte als langjähriger Praktiker in die Strukturen des deutschen Sicherheitssystems ein und referierte insbesondere über die Organisation der nicht-polizeilichen Gefahrenabwehr. Gut ergänzt wurde dieser Vortrag durch den Präsidenten des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe, Christoph Unger. Er berichtete ausführlich über die Angebote des Bundes an Länder und Kommunen zur Kommunikation und Verbesserung der Strukturen im Bevölkerungsschutz. Dabei empfahl er die Lektüre der DStGB-Dokumentation „Sichere Städte und Gemeinden", die auf der Tagung verteilt wurde und auch auf der Internetseite des Deutschen Städte- und Gemeindebundes (www.dstgb.de) unter Brennpunkt „Sicherheit und Kommunen" kostenlos herunter geladen werden kann.

Abgerundet wurde der erste Veranstaltungstag von weiteren Beiträgen von Karl Peter Brendel, Staatssekretär im Innenministerium des Landes Nordrhein-Westfalens, Alf Henry Wulf, Vorsitzender BDI-Ausschuss Multimedia und Kommunikationspolitik sowie stellvertretender Vorstandsvorsitzender der Alcatel SEL AG, Oliver Apfelt, Vorstandsmitglied bei der mit dem Digitalfunknetz-aufbau zunächst beauftragten DB Telematik GmbH, Dirk Borchardt, Direktor des BOSNET-Programms von EADS Secure Networks , und die Dinnerspeech von Rolf Tophoven, Leiter des Instituts für Terrorismusforschung und Sicherheitspolitik.

IT-Sicherheit

Vor allem am zweiten Tag kam mit der IT-Sicherheit ein weiteres Top-Thema der Tagung zu Sprache. Dass Datenmissbrauch und Onlinekriminalität zunehmen wurde ebenso deutlich wie die Forderung nach sicheren Prozeduren und Security-Standards – Fragen mit denen sich auch die für E-Government zuständigen Verantwortlichen in den Kommunen befassen müssen. Dies konnte der Präsident des Bundesamtes für Sicherheit in der Informationstechnik, Dr. Udo Helmbrecht, an vielen praktischen Beispielen den Teilnehmern plastisch vorführen.

Dass im Sicherheitsbereich die technischen, aber auch die organisatorischen Strukturen noch optimiert werden können, zeigten die Beiträge von Carsten Smago, Programmdirektor bei Alcatel SEL, Professor Dr. Walter Gora, Geschäftsführer der Valora Management Group, und Professor Dr. Klaus Lenk vom Hochschulkolleg für E-Government.

Forum zu Sicherheitsfragen

Am Nachmittag des zweiten Konferenztages wurde in einem „DStGB-Forum“ die Gelegenheit gegeben, Fragen der öffentlichen Risikovorsorge und der verschiedenen technischen und organisatorischen Optionen zur besseren Befriedigung der gesellschaftlichen Sicherheitsbedürfnisse zu vertiefen. Hierzu kamen Fachleute von Firmen zu Wort, die in diesem Bereich auch für die Städte und Gemeinden gedachte Angebote unterbreiten.

Für die Microsoft Deutschland GmbH informierte Matthias Dörfel über die vom DStGB unterstützte Initiative „Deutschland sicher im Netz“, die unter www.sicher-im-netz.de wichtige Verbrauchertipps für die IT-Sicherheit bereitstellt. Volker Hartwein von der FREQUENTIS GmbH trug Gedanken eines integrierten Leitstellenkonzeptes vor, in dem die einzelnen BOS-Leitstellen hin zu einem Systemverbund „Innere Sicherheit“ aufgebaut werden könnten. Ebenso präsentierten Dr. Bernhard Escherich von der SAP Deutschland AG & Co. KG, Olaf Lohmann von der der Firma Motorolla und Werner Wirdemann von der Oracle Deutschland GmbH die Sicherheitslösungen ihrer Häuser für Kommunen.

Nachdem das deNIS II plus-Krisenmanagement-System des Bundes bereits im Vortrag des Präsidenten des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe, Christoph Unger, kurz angeschnitten worden war, wurde es in dem DStGB-Forum vertieft dargestellt. Hierzu führte Satish Jha in den gegenwärtigen Stand der Entwicklung dieses Systems ein. Er ist der „Division Manager Government“ der Firma PRO DV Software AG, die das System maßgeblich konstruiert hat. Es dient zur Unterstützung des Krisenmanagements bei großflächigen Gefahrenlagen. Unter der Bezeichnung deNIS II werden Daten zum Bevölkerungsschutz zusammengefasst, aufbereitet und bestimmten Entscheidern in übersichtlicher und variabel darstellbarer Form zur Verfügung gestellt.

Ulrich Mohn leitet das Referat „Recht und Verfassung“ in der Berliner Hauptgeschäftsstelle des beim Deutschen Städte- und Gemeindebundes

Grußwort

Karl Peter Brendel

Staatssekretär im Innenministerium des Landes Nordrhein-Westfalen

Ich freue mich sehr, Sie hier in Berlin, in der Vertretung des Landes Nordrhein-Westfalen beim Bund, begrüßen zu dürfen und möchte Sie zu dieser Fachkonferenz des Deutschen Städte- und Gemeindebundes und der Alcatel SEL Stiftung herzlich willkommen heißen. Thematisch befasst sich diese Fachkonferenz mit der höchst aktuellen Frage nach der Sicherheit der Kommunikation für Städte und Gemeinden. Trotz der in der Verfassung unseres Landes NRW festgelegten kommunalen Selbstverwaltung bedarf es einer umfassenden Betrachtung der Sicherheitsarchitektur über die kommunalen Grenzen hinaus. Ausdrücklich sind hier Behörden und Organisationen des Landes bzw. des Bundes mit einzubeziehen, eine effiziente und effektive Einheitlichkeit der öffentlichen Hand auch auf diesem Feld zu erreichen bzw. diese zu verbessern. Einbezogen werden müssen auch Externe, die z.B. als qualifizierte Systemlieferanten oder Dienstleister hinzugezogen werden und die technischen Voraussetzungen einer modernen Sicherheitsarchitektur wesentlich mitgestalten.

Lassen Sie mich einige Beispiele nennen:

Die Landesregierung misst der Informations- und Kommunikationstechnik sowie dem E-Government als Teil der Verwaltungsmodernisierung eine große Bedeutung zu. Wir werden die Möglichkeiten von E-Government zur Optimierung und Neugestaltung von Verwaltungsprozessen und damit auch zur Verbesserung des Wirtschaftsstandortes Nordrhein-Westfalen zielgerichtet nutzen.

Der Weg dahin ist aber bei allen damit verbundenen Vorteilen auch mit Risiken behaftet. Die elektronisch übermittelten Daten müssen sicher sein vor unbefugtem Zugriff oder Manipulation. Auch müssen Kommunikationswege sicher gestaltet werden.

TESTA-Netz als geschlossenes Netzwerk der europäischen Verwaltungen

So nutzt die Landesverwaltung und die Polizei schon seit langer Zeit jeweils ein geschlossenes Netz zur Kommunikation der Behörden untereinander. Diese Sicherheitsphilosophie des geschlossenen Netzes wurde ebenso bei der Kommunikation mit der Kommunalverwaltung umgesetzt. Basis bildet dabei für die Landesverwaltung das TESTA-Netz, welches als geschlossenes Netzwerk die europäischen Verwaltungen miteinander verbindet. Es freut mich, dass im vergangenen Jahr durch gemeinsame Anstrengungen des Innenministeriums, der kommunalen Spitzenverbände und der kommunalen IT-Dienstleister die vollständige Vernetzung zwischen Landesverwaltung und den Kommunen und Kreisen in NRW erreicht wurde.

Diese Idee wird genauso im neuen Aktionsplan Deutschland Online verfolgt, der den Aus- und Aufbau einer abgestimmten Deutschland-weiten Kommunikationsinfrastruktur vorsieht. Deren Verfügbarkeit, Sicherheit und Qualität wird sich an den besonderen Anforderungen einer leistungsfähigen Öffentlichen Verwaltung ausrichten. Die gemeinsame Federführung bei diesem Vorhaben haben das Land Hessen und der Bund. Ich selbst werde der Lenkungsgruppe der Staatssekretäre angehören, die den Prozess steuert. Es ist meine Überzeugung, dass der Weg über eine sichere Kommunikationsinfrastruktur die beste Voraussetzung für eine IT-basierte Modernisierung der Verwaltungsprozesse darstellt.

Mit der vollständigen Vernetzung von Landesverwaltung und Kommunalbereich in Nordrhein-Westfalen verfügen wir bereits jetzt über eine geeignete Infrastruktur, um vielfältige Anwendungen aus den verschiedenen Fachbereichen zwischen Verwaltungen aufsetzen zu können. Derzeit gibt es über 30 Verfahren zwischen Land und Kommunen, die elektronisch in wirtschaftlicher Weise abgewickelt werden können. Darunter sind beispielsweise die Verfahren „GSL.net – IT-Unterstützung bei größeren Schadenslagen und „Informationssystem Gefahrenabwehr NRW“. Weitere Anwendungen sind in Vorbereitung.

In engem Zusammenhang dazu steht der Aufbau einer entsprechenden Sicherheitsinfrastruktur, da beispielsweise an die Übertragung sensibler Meldedaten hohe Datenschutz- und Sicherheitsanforderungen zu stellen sind. Die Aufwände für Sicherheitsvorkehrungen machen in vielen Verfahren mittlerweile einen erheblichen Teil der Gesamtkosten aus. Das Land hat den notwendigen Aufbau der Sicherheitsmaßnahmen im Kommunalbereich unterstützt – und dieses auch mit finanziellen Mitteln.

Anwendung Governikus beim Einsatz von qualifizierten elektronischen Signaturen bei der Übertragung sensibler Daten

Die vom Land befristet finanzierte Pflege der Software Governikus bietet dem Kommunalbereich die Möglichkeit, neben dem Meldewesen auch Verfahren und die Kommunikation mit Ihren Kunden unter Einsatz von qualifizierten elektronischen Signaturen rechtsverbindlich und sicher zu gestalten. Ich denke, wir haben damit alle Hindernisse aus dem Weg geräumt, die dem Aufbau einer geeigneten Infrastruktur im Wege standen. Damit die Kommunen im Rahmen des Meldewesens den

gesetzlichen Vorgaben zur elektronischen Rückmeldung fristgerecht nachkommen werden, sind aber noch einige Anstrengungen erforderlich.

Bei denjenigen Angeboten, die sich an die Bürgerinnen und Bürger sowie die Wirtschaft richten, erfolgt die Kommunikation zwangsläufig über das Internet. Von Anfang an wurde in der Landesverwaltung der Auf- und Ausbau dieser Angebote von aufwändigen Sicherheitsmaßnahmen begleitet. Die Entwicklung eines mehrstufigen Sicherheitskonzeptes und die Einrichtung eines zentralen Übergangspunktes zum Internet, der nach dem neuesten Stand der Technik gesichert ist, sollen hier nur beispielhaft genannt werden. Nach wie vor werden erhebliche Investitionen getätigt, um mit modernster Technologie den Schutz der Daten in der Landesverwaltung sicherzustellen.

Die intensive fachliche Kooperation, die wir bisher bei E-Government mit dem kommunalen Bereich sowie anderen Bundesländern und der Bundesverwaltung eingegangen sind, muss ebenso auf dem Gebiet der Sicherheit von IT-Infrastrukturen stattfinden. Die heutige Veranstaltung stellt einen sichtbaren Schritt in diese Richtung dar. Auch wird die Zusammenarbeit zwischen Land und Kommunen einen Schwerpunkt des Aktionsplanes 2009 der Landesverwaltung darstellen, der zur Zeit unter Federführung des Innenministeriums erstellt wird. Er beinhaltet die wesentlichen E-Government-Aktivitäten der Landesverwaltung bis zum Jahr 2009. Verwaltungsprozesse durch Einbindung moderner Technologien schneller und effizienter zu gestalten, ohne dass dieses zu Lasten der Datensicherheit geht, ist für mich eine der wichtigsten Voraussetzungen beim E-Government. Denn ohne diese Sicherheit werden die Bürgerinnen und Bürger den neuen Möglichkeiten nicht vertrauen und sie nicht nutzen.

Einführung des Digitalfunks für die Behörden und Organisationen mit Sicherheitsaufgaben (BOS)

Die seit Jahren laufenden Bemühungen, ein bundesweit einheitliches digitales Funknetz für die BOS zu schaffen, gehen Ende Juni 2006 mit der Auftragsvergabe an den günstigsten Bieter in eine neue Phase. Für die Beschaffung und den laufenden Betrieb dieses Netzes investiert allein das Land NRW bis zum Jahre 2020 nach derzeitigem Stand mindestens 208 Millionen Euro. In der zweiten Jahreshälfte 2006 kann in NRW mit dem Roll-Out begonnen werden, sofern nicht Rechtsmittel unterlegener Bieter gegen die Entscheidung des Beschaffungsamtes des BMI Zeitverzögerungen bewirken. Das Land NRW wird dieses Digitalfunknetz nach den laufenden Planungen im Jahre 2010 landesweit flächendeckend allen hier tätigen BOS -also auch den Kommunen und den übrigen nichtstaatlichen Trägerschaften (z.B. DRK)- kostenfrei zur Verfügung stellen. Damit sind wir bundesweit in der Lage, über kommunale, staatliche oder organisatorische Grenzen hinweg ein einheitliches Funknetz zu betreiben. Zusätzlich stellt das Land NRW in den nächsten drei Jahren alleine zur Beschaffung von Endgeräten (auch Leitstellen) für die Polizei mindestens 40 Millionen Euro bereit.

Wir haben gemeinsam die Aufgabe, bis zum Jahre 2010 sowohl polizeiliche als auch nichtpolizeiliche Behörden und Organisationen in die Lage zu versetzen, dieses Netz auch gemeinsam zu nutzen. Da werden also Polizei, Bedienstete der Feuerwehr sowie der Hilfs- und Rettungsdienste Digitalfunkgeräte in Betrieb nehmen wollen. Aufgabe auch der Städte und Gemeinden wird es sein, bis dahin in zeitlicher Übereinstimmung mit den Planungen des Landes, Vorsorge zur Ausstattung mit der neuen Technik zu treffen. Sicherlich eine große Aufgabe, die von allen Beteiligten engagiert angegangen werden muss!

Einrichtung gemeinsamer Leitstellen für Polizei und Feuerwehr sinnvoll? (so genannte „bunte“ Leitstellen)

Täglich sehen wir das Erfordernis der Zusammenarbeit von Polizei und Feuerwehr/Hilfs- und Rettungsdiensten an den Einsatzorten. Dabei werden diese Einsatzkräfte von Leitstellen unterschiedlicher Träger geführt. Der damit verbundene Koordinationsaufwand wird in anderen Bundesländern teilweise durch die Einrichtung von gemeinsamen Leitstellen für Polizei und Feuerwehr reduziert. Auch in Nordrhein-Westfalen gibt es Diskussionen über ein solches Modell, bisher ohne konkretes Ergebnis. Hier gilt es, in NRW Wege zu finden, die möglichen Einspareffekte und ablauforganisatorischen Vorteile unter Berücksichtigung aller Interessen und der kommunalen Selbstverwaltung zu erreichen.In dem Zusammenhang beschäftigen wir uns in NRW aktuell mit der Frage, ob jede Polizeibehörde eine eigene Leitstelle benötigt. Ein entsprechender Entschließungsantrag an den Landtag liegt vor.

Mit diesen Überlegungen möchte ich dieser Veranstaltung in jeder Hinsicht einen erfolgreichen Verlauf wünschen und freue mich schon auf weitere Informationen und Anregungen.

Grußwort

Dr. Gerd Landsberg

Geschäftsführendes Präsidalmitglied des DStGB (Berlin)

Ich freue mich, Sie hier in Berlin ganz herzlich zu einer weiteren DStGB-Sicherheitskonferenz für Städte und Gemeinden begrüßen zu dürfen. Mein erster Dank gilt Herrn Staatssekretär Brendel dafür, dass wir Gast in der Vertretung des Landes Nordrhein-Westfalen sein dürfen. Sicherheit ist in den Städten und Gemeinden ein wichtiges Thema und gewinnt immer mehr an Bedeutung. Bilder von Bedrohungen, die für alle Ebenen des öffentlichen Lebens alarmierend sind, sind uns allgegenwärtig. Beispielhaft seien nur genannt die neuen Bedrohungen durch den internationalen Terrorismus und verheerende Katastrophen. Immer wieder verunsichern Meldungen über (Natur-)Katastrophen die Menschen: Überschwemmungen, Wirbelstürme, Erdbeben in aller Welt aber auch in Deutschland, zuletzt das Hochwasser in Bayern im August 2005. Die Bevölkerung vor Gefahren aller Art zu schützen und Ihnen ein Höchstmaß an Sicherheit zu bieten, ist eine zentrale Aufgabe des Staates und seiner Behörden. Die Bandbreite der Gefahren reicht heute vom schweren Unfall über Naturereignisse mit katastrophalen Auswirkungen bis hin zum Anschlag terroristischer Organisationen mit einem Massenanfall von Verletzten. Aber auch die Ausbreitung z.B. der Vogelgrippe zeigt, dass wir auch für diese möglichen Fälle gut aufgestellt sein müssen.

Die Verantwortlichen in den Städten und Gemeinden sind die ersten Ansprechpartner wenn es darum geht, den Bürgerinnen und Bürgern bei Unfällen zur Seite zu stehen. Bei allen Gefahrenlagen ist es wichtig, dass die Organe der Gefahrenabwehr, die Hilfeleistungsorganisationen, aber auch die Bevölkerung im Rahmen ihrer Möglichkeiten zusammenwirken: die Behörden und Organisationen aufgrund ihres Auftrages und ihres Leistungsspektrums, die Bürgerinnen und Bürger durch richtiges Verhalten im Rahmen von Selbstschutz und Nächstenhilfe.

Dies unterstreicht, wie wichtig es ist, die Einsatzkräfte vor Ort personell und sächlich bestmöglich auszustatten. Ich denke dabei natürlich auch besonders an die kommunalen Kräfte im deutschen Sicherheitssystem, speziell an die Feuerwehren. Unsere Kräfte in den Kommunen können bei Katastrophenfällen am schnellsten erste Maßnahmen ergreifen und haben die beste Ortskenntnis, die man für das Krisenmanagement dringend benötigt. Ein wesentlicher Baustein eines erfolgreichen Krisenmanagements wird vor allem die örtliche Informations- und Kommunikationsstrategie sein – und hier kann den Städten und Gemeinden eine wichtige Rolle zukommen.

Aus gutem Grund steht auf dieser Konferenz die „Sicherheitskommunikation“ im Mittelpunkt der Erörterungen. Die Bewältigung von Großschadensereignissen verlangt nach einem leistungsfähigen Funksystem, das ein problemloses – also auch ein nicht durch Kommunikationsprobleme gestörtes – Zusammenarbeiten von Hilfskräften ermöglicht. Die Erfahrungen der Flutkatastrophe des Jahres 2002 haben gezeigt, wie wichtig die funktionierende Kommunikation zu den einzelnen Einsatzkräften aber auch zwischen den Hilfeleistungsorganen ist. Wir wissen zu genau, in welchen Gefahren sich einzelne Hilfetrupps befunden haben, weil die Kommunikation nicht funktionierte.

Vor dem Hintergrund der Fußballweltmeisterschaft, aber auch der von Land zu Land unterschiedlichen Diskussion über die Reorganisation von Leitstellen wird verstärkt über die näher rückende Einführung des Digitalen Sprechfunks gesprochen. Auch im Rahmen dieser Konferenz werden wir uns daher schwerpunktmäßig mit der Frage der modernen Sicherheitskommunikation und insbesondere mit der Einführung eines digitalen Sprech- und Datenfunknetzes im Bereich der Behörden befassen.

Da die für die Kommunen vor Ort relevanten Fragen in diesem Zusammenhang vor allem in den Bundesländern ausgehandelt werden, unterstützt die Berliner Hauptgeschäftsstelle des DStGB diese Verhandlungen der Mitgliedsverbände immer wieder dadurch, dass sie einen Erfahrungsaustausch der für BOS-Digitalfunk zuständigen Referenten der DStGB-Mitgliedsverbände durchführt und die Erörterungen moderiert. Erst am 23. Mai 2006 fand das jüngste dieser Treffen statt. Hierbei geht es insbesondere um Fragen der Einbeziehung der Kommunen und der Finanzlastverteilung, die in diesem Zusammenhang von Land zu Land unterschiedlich betrachtet werden.

Die heutige Konferenz bietet nun erneut vielen Betroffenen die Chance, die Positionen der verschiedenen Seiten zu Fragen im Zusammenhang mit der näher rückenden Einführung des Digitalen Sprechfunks klarer zu verdeutlichen.

Sicherheitskommunikation umfasst mehr als die Kommunikation über abgesicherte Kanäle. Es geht um die Kommunikation zwischen den unterschiedlichen Behörden mit Sicherheits- und Ordnungsaufgaben. Wir brauchen die technischen Voraussetzungen für eine ungestörte Kommunikation zwischen diesen Hilfeleistungsorganen. Ich kann mich sehr genau an ein Erlebnis während meiner Referendarzeit in einem Landkreis erinnern, bei der bereits die theoretische Katastrophenschutzübung mehr als suboptimal verlaufen ist, die praktischen Übung endete mehr oder weniger in einem Chaos, nicht zuletzt

aufgrund mangelnder Kommunikation. Zugegebenerweise fand diese Übung vor ca. 26 Jahren statt, ich bin mir aber sicher, dass noch heute entsprechende Kommunikationsprobleme bestehen.

Es geht aber auch um die Sicherheit der Kommunikationsmittel: Funktionsfähige Kommunikationsmittel sind der Grundstein einer effektiven Aufgabenbearbeitung. Stehen diese Mittel nicht mehr zur Verfügung, wird die Aufgabenbearbeitung erheblich eingeschränkt oder kommt sogar ganz zum Erliegen. Zur Aufrechterhaltung des Betriebes sind daher konzeptionelle Überlegungen zur Sicherung der Kommunikationswege erforderlich. Darüber hinaus müssen Konzepte, die einen Betrieb auch mit erheblich eingeschränkten technischen Kommunikationsmöglichkeiten zulassen, erarbeitet und regelmäßig geübt werden.

Von einem Stromausfall müssen das Mobilfunknetz und das Telefonfestnetz (zunächst) nicht betroffen sein. Neben Mobiltelefonen sind in diesem Fall Endgeräte hilfreich, die für das Festnetz keine eigene Stromversorgung benötigen bzw. eine ausreichende Notstromversorgung der Telefonanlage.

Leitstellen sollten über eine verlässliche Notstromversorgung (Netzersatzanlagen) verfügen. Um den Notbetrieb im Ereignisfall gewährleisten zu können, ist die Funktionstüchtigkeit der Notstromanlagen regelmäßig zu überprüfen und die Bevorratung ausreichenden Betriebsstoffes und dessen Nachlieferung sicherzustellen. Darüber hinaus sollten auch Konzepte für den Leitstellenbetrieb ohne Computerunterstützung bestehen und regelmäßig geübt werden.

Man muss auch vor Ort wissen, dass das THW über Einheiten mit entsprechender technischer Ausstattung verfügt, um im Notfall Kommunikationsstrukturen (wieder) herzustellen. Mit seinen über Deutschland verteilten Fachgruppen Führung/Kommunikation (FGr FK) – insbesondere dem Teil Weitverkehrstrupp (WVTr) – besitzt das THW hervorragende Möglichkeiten, temporäre Telekommunikationsverbindungen und -netze einzurichten und zu betreiben. Eine Inanspruchnahme dieser Einrichtungen im Ereignisfall sollte im Vorfeld mit den Organisationen abgestimmt werden.

In den Städten und Gemeinden ist Vorsorge zu treffen, wohin sich Bürgerinnen und Bürger in einem Notfall wenden können, wenn infolge eines Stromausfalls o.ä. die öffentlichen Telekommunikationsnetze (Festnetz und Mobilfunknetz) nicht zur Verfügung stehen. In einer Gemeinde sollten an zentralen Stellen – am besten geeignet sind Feuer-, Polizeiwachen und/oder Rathäuser – Meldeköpfe bzw. Anlaufstellen für Betroffene zur Entgegennahme von Hilfeersuchen eingerichtet werden. Die Bürgerinnen und Bürger sollten über diese Möglichkeiten informiert sein.

Die Städte und Gemeinden müssen sich auf einen Ausfall der Stromversorgung vorbereiten. Die jeweilige Kommunalverwaltung sollte zu allererst prüfen, welche Bereiche ihrer Verwaltung sowie sonstiger kommunaler Einrichtungen bei einem Stromausfall zwingend weitergeführt werden müssen, um sodann für diese Bereiche eine verlässliche Notstromversorgung zu schaffen. Detaillierte Hilfestellung hierzu gibt der „Leitfaden für Einrichtung und Betrieb einer Notstromversorgung in Behörden und anderen wichtigen öffentlichen Einrichtungen“ der auf der Internetseite des BBK zum Download zur Verfügung steht.

Während der präventiven Phase sollten Krisen- und Einsatzpläne für einen Stromausfall erstellt werden. In dieser Phase sollten Kontakte und Kooperationen mit Versorgungsunternehmen, ggf. dem Land sowie Hilfsorganisationen z.B. dem THW geknüpft und gepflegt werden. Damit die Krisen- und Einsatzpläne im Ereignisfall ein wirksames Hilfsmittel sind, sollten sie regelmäßig aktualisiert und geübt werden.

Das Thema „Sicherheitskommunikation für Städte und Gemeinden“ ist ein komplexes Themenfeld. Es bedarf der Vernetzung und der Zusammenarbeit zwischen Bund, Ländern und Gemeinden. Von daher freue ich mich, dass alle Ebenen heute und morgen auf unserer Sicherheitskonferenz referieren werden.

Wir sind aber auch auf das „know how“ Privater angewiesen. Zur Durchführung dieser Konferenz konnten wir die Alcatel SEL Stiftung als einen leistungsfähigen Partner gewinnen. Zu Fragen der technischen Infrastrukturen für staatliche und kommunale Sicherheitskommunikation bringt sie dieses notwendige Know How in diese Fachkonferenz mit ein. Für die gute Zusammenarbeit im Vorfeld der Konferenz „Sicherheitskommunikation für Städte und Gemeinden“ danke ich in diesem Zusammenhang den Mitarbeitern von Alcatel SEL und richte diesen Dank stellvertretend an Herrn Alf Henry Wulf, Vorsitzender BDI Ausschuss Multimedia und Kommunikationspolitik sowie stellvertretender Vorstandsvorsitzender der Alcatel SEL AG, der im Anschluss an meine Ausführungen das Wort ergreifen wird.

Mein Dank gilt auch den ausgewiesenen Fachleuten, die für unsere Konferenz interessante Referate angekündigt haben!

So begrüße ich in unseren Reihen ganz herzlich den Senator für Inneres des Landes Berlin, Dr. Ehrhart Körting, der das Einführungsreferat unter dem Titel „Vernetzte Sicherheit“ im Anschluss an die Grußworte halten wird. Wer könnte dies besser als der Innensenator eines Stadtstaates, der den Blick auf Land und Kommune hat und zugleich sich den Sicherheitsherausforderungen nicht nur der ständigen Großveranstaltungen in Berlin, sondern auch denen der Bundeshauptstadt stellen muss.

Ein herzliches Willkommen, auch wenn sie noch nicht alle heute anwesen sind, gehen stellvertretend an

- den Präsidenten des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe, Herrn Christoph Unger,
- den Präsidenten des Bundesamtes für Sicherheit in der Informationstechnik, Dr. Udo Helmbrecht sowie
- den künftigen Präsidenten der Bundesanstalt Technisches Hilfswerk, Herrn Albrecht Broemme, den wir noch auf der letzten DStGB- Konferenz zum Thema „Sicherheitskommunikation“ im Oktober 2005 in Kelsterbach als Landesbrandmeister der Feuerwehr von Berlin begrüßen konnten,
- den Vorsitzenden der Geschäftsführung DB Telematik und Vorsitzender der Geschäftsführung DB Systems, Herrn Robert Simmeth sowie
- den Direktor des Bosnet Programms, Herrn Dirk Borchardt.

Neben den Naturkatastrophen und Unglücksfällen mit Massenschäden beschäftigt die Sicherheitsbehörden der Schutz vor terroristischen Anschlägen. Die Bedrohung durch den islamistischen Terrorismus ist sicherlich von besonderer Tragweite. Am heutigen Abend können wir uns auf einen Vortrag zu diesem Thema von Herrn Rolf Tophoven, Institut für Terrorismusforschung und Sicherheitspolitik freuen.

Sicherheit in Städten und Gemeinden ist natürlich weit mehr als eine Frage der geeigneten Technik für die Sicherheitskommunikation.

Spannend wäre sicherlich auch, angesichts der desolaten kommunalen Finanzlage der Städte und Gemeinden über die staatliche Aufgabe der Finanzierung von Feuerwehren und einer erweiterten Katastrophenvorsorge zu sprechen.

Sehr wichtig für die Sicherheit in Städten und Gemeinden wäre auch, über gute Bedingungen für das Ehrenamt im Bevölkerungsschutz zu sprechen oder über die Qualifizierung der Bürgerschaft zum Selbstschutz.

Derartige Themen haben ganz gewiss in der Arbeit des DStGB einen hervorragenden Platz.

Statt langen Ausführungen hierzu bieten wir Ihnen ganz aktuell eine Broschüre mit dem Titel „Sichere Städte und Gemeinden“. Der Deutsche Städte- und Gemeindebund hat in Zusammenarbeit mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe diese Dokumentation erstellt, um kommunalrelevantes Wissen über die Hilfsangebote und Handlungsempfehlungen des Bundes kompakt zur Verfügung zu stellen. Ich möchte an dieser Stelle Herrn Präsidenten Unger meinen herzlichen Dank für die Zusammenarbeit sagen.

Wir haben diese Broschüre bei unserem jüngsten Gemeindekongress vorgelegt und empfehlen nun auch in diesem Kreis den Teilnehmern, sich anhand der Broschüre mit dem Titel „Sichere Städte und Gemeinden“ tiefer in die Fragestellungen einzuarbeiten, die sich gerade Bürgermeisterinnen und Bürgermeister stellen, wenn sie wollen, das ihre Stadt oder Gemeinde besser auf einen Katastrophenfall vorbereitet ist und im Ernstfall im Rahmen ihrer Möglichkeiten optimal vorgeht.

Diese Broschüre „Sichere Städte und Gemeinden“ steht ihnen hier auf dieser Konferenz in der Druckfassung zur Verfügung. Sie können sie aber auch auf der Homepage des Deutschen Städte- und Gemeindebundes im Brennpunkt „Sicherheit“ kostenlos downloaden.

Mit diesem Hinweis beende ich die einleitenden Worte zu unserer Konferenz „Sicherheitskommunikation in Städten und Gemeinden“, wünsche Ihnen einen anregenden Austausch zu diesem Thema und übergebe das Wort dem nächsten Redner, Herrn Alf Henry Wulf von der Alcatel SEL AG.

Vielen Dank für Ihre Aufmerksamkeit!

Grußwort

Alf Henry Wulf

Vorsitzender des BDI-Ausschusses Multimedia und Kommunikationspolitik sowie stellvertretender Vorstandsvorsitzender der Alcatel SEL AG

Seitens des Kuratoriums der Alcatel SEL Stiftung für Kommunikationsforschung darf ich Sie auf das Herzlichste auf dieser Fachkonferenz begrüßen. Mein herzlicher Dank geht auch an die Landesvertretung NRW, die die Räumlichkeiten für diese Veranstaltung zur Verfügung stellt.

Unsere Wissenschaftsstiftung fördert auch ausdrücklich den Austausch zwischen Wissenschaft und Praxis, man kann sogar sagen, dass sie sich vom „wissenschaftlichen Elfenbeinturm" eher fern hält. Unser heutiger Kooperationspartner ist der Deutsche Städte- und Gemeindebund, also eine Institution, die in Bezug auf die Wissenschaft eher als „Bedarfsträger" bezeichnet werden kann. Es ist eine Aufgabe unserer Stiftung, wissenschaftliche Erkenntnisse – etwa in Form von angebotenen Publikationen oder mit Veranstaltungen – auch an die Praxis weiter zu geben. Wir haben gerade von Kommunen dafür immer großen Dank bekommen, weil die Kommunen, anders als die Länder oder der Bund, aber auch die Wirtschaft, nicht so ohne weiteres Zugriff auf das geballte Wissen unserer Hochschulen und anderer Wissenschaftseinrichtungen haben.

Es geht aber immer um mehr als nur den Informationstransfer. Die Kommunen wollen sich auch in die Diskussion um Electronic Government einbringen, sind sie es doch, die sozusagen „direkt an der Bürgerfront" stehen. Deswegen ist unserer Stiftung auch die Aufgabe zugewachsen, eine neutrale Plattform für den Austausch der Praktiker untereinander zu bieten – wir haben in den bisherigen Veranstaltungen die Erfahrung gemacht, dass dies von den Beteiligten als sehr hilfreich angesehen wurde. Es ist für eine gemeinnützige Wissenschaftsstiftung aus durchaus bürokratischen Gründen nicht immer einfach, dieses Thema zu fördern, weshalb wir uns auch heute über Ihren Zuspruch freuen würden.

Das Thema Sicherheitskommunikation ist bereits in mehreren Veranstaltungen der Stiftung thematisiert worden. Das beteiligte Netzwerk der Stiftung verfolgt dabei das Ziel, die Diskussion in diesem Themenfeld inhaltlich-konzeptionell voranzutreiben, neue Entwicklungen und Ideen vorzustellen und vor allem den Erfahrungsaustausch zwischen Wissenschaft und Praxis zu fördern.

Die erste Veranstaltung zur Sicherheitskommunikation fand im August 2004 zum Thema ePolicing in Hamburg statt. Hier wurden neue Anwendungsmöglichkeiten von vernetzten und mobilen Techniken bei der Polizei, der Feuerwehr und Akteuren des Katastrophenschutzes vorgestellt und diskutiert. Im November 2004 folgte in der Bremischen Bürgerschaft die Tagung „Digitale Infrastrukturen für Sicherheit und E-Government", bei der technische Aspekte sowie mögliche Finanzierungsformen für den Aufbau von technischen Infrastrukturen und Anwendungen für Behörden mit Sicherheits- und Ordnungsaufgaben diskutiert wurden. Schließlich gelang es der Stiftung im Februar 2005, die verschiedensten Behörden, die im Schadensfall auf schnelle und direkte Notfallkommunikation angewiesen sind, sowie die Wissenschaft zu einem gemeinsamen Dialog über Anwendungsbereiche und Einsatzmöglichkeiten neuer Technologien zu einer Tagung in Berlin zu versammeln.

Aus den Diskussionen zwischen Wissenschaft und Praxis ist eine Weiterentwicklung des Verständnisses von Sicherheitskommunikation entstanden, über den auf einer Veranstaltung im Juni letzten Jahres in Darmstadt diskutiert wurde. Der Begriff Sicherheitskommunikation umfasst weit mehr als IT-Sicherheit oder Abhörsicherheit. Sicherheit umfasst viel mehr als Technik, so wichtig die Vernetzung der verschiedenen Akteure beispielsweise der verschiedenen Rettungsorganisationen im Katastrophenschutz auch ist. Die Kräfte von Polizei, Feuerwehr und anderen Rettungsdiensten müssen Informationen übermitteln, aus der Vielzahl gleichzeitig eingehender Informationen die jeweils aktuell wichtigsten herausfiltern und die Informationen verarbeiten. Sie brauchen dafür zum einen ein geeignetes Informationsmanagement sowie zum anderen technische Kommunikationskanäle und eingespielte zuverlässige Kommunikationswege, um im Schadensfall koordiniert und wirksam handeln zu können. Zuverlässige und auch im Ernstfall hinsichtlich ihrer Verfügbarkeit belastbare Kommunikationsmittel sind grundsätzlich von anderer Natur als die anderen Kommunikationsmedien. Der Ausfall eines Fernsehsenders ist vielleicht ärgerlich, kein Kanal beim Mobiltelefon oder langes Warten auf eine e-Mail ist möglicherweise schädlich, ein Kommunikationsloch im Katastrophenfall ist schlicht nicht akzeptabel. Weil andererseits aus wirtschaftlichen Gründen nicht alle Kommunikationstechnik

doppelt und dreifach zur Sicherung vorgehalten werden kann, muss nicht über eine betriebswirtschaftlich-technische, sondern über eine gesellschaftspolitische Diskussion der Kompromiss zwischen Finanzierbarkeit und Anforderungen gefunden werden. Und dieser Kompromiss ist ständig aufgrund der Erfahrungen zu überprüfen, wobei auch der technische Fortschritt über der Zeitachse nicht außer Acht bleiben darf.

Gerade auf dem Gebiet des Electronic Government – so viel lässt sich schon heute sagen – werden noch erhebliche Anstrengungen auch in der Technik notwendig sein, um den Ansprüchen einer „Sicherheitskommunikation" gerecht zu werden. Die Bedeutung des Themas ist erkannt und dies zeigt sich auch daran, dass wichtige Vertreter oberster Bundesbehörden – das Technische Hilfswerk, das Bundesamt für Sicherheit in der Informationstechnik und das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe – heute und morgen teilnehmen.

Noch stärker als bisher sollte Sicherheitskommunikation bei den Verantwortlichen im Bund, bei den Ländern und in den Kommunen als Querschnittspolitik wahrgenommen werden. Bisher stoßen Sicherheitsfragen immer erst dann auf Interesse oder erzeugen Handlungsdruck, wenn es gilt, große Ereignisse wie die Fußball-WM vorzubereiten oder wenn große Schadensfälle bereits eingetreten sind. Es darf nicht übersehen werden, dass für die Kommunikationsinfrastrukturen unter der besonderen Anforderung einer Sicherheitskommunikation die Parole „kleiner, leichter, billiger" der Mobilkommunikation gewiss nicht gelten kann. Hier gibt es noch bedeutsame Gestaltungspotentiale und nicht zuletzt Diskussionsbedarf, das derzeit ausgeschriebene Forschungsprogramm des Bundeswirtschaftsministeriums zur „ – Sicheren Anwendung der mobilen Informationstechnik zur Wertschöpfungssteigerung in Wirtschaft und Verwaltung (SimoBIT)" kann trotz der dort ausgelobten 20 Millionen Euro Förderung nur ein Anfang sein.

Wir werden mit unserer Förderstiftung nach Kräften weiter versuchen, das Thema Sicherheitskommunikation zu vertiefen. Heute und morgen haben wir hierzu gute Gelegenheit, und ich darf uns allen einen interessanten und ertragreichen Verlauf der Fachkonferenz wünschen.

Vernetzte Sicherheit – wirksamer Schutz für Bund, Länder und Gemeinden

Ich danke Ihnen für die Gelegenheit, anlässlich der Fachkonferenz des Deutschen Städte- und Gemeindebundes und der Alcatel SEL Stiftung einige einführende Worte halten zu dürfen. Das Thema *„Vernetzte Sicherheit – wirksamer Schutz für Bund, Länder und Gemeinden"* verknüpft die Anforderungen an eine *moderne* Informationstechnologie mit den notwendigen *Sicherheitsbelangen*.

Daraus ergibt sich eine Daueraufgabe der Sicherheitsbehörden des Bundes und der Länder: Das Gesamtsystem aus Kompatibilität, Standardisierung und Netz-Sicherheit bedarf stetiger Verbesserung. Aber: bringt Vernetzung *„mehr"* und wirksameren Schutz? Welche Risiken sind mit der fortschreitenden Vernetzung verbunden? Welcher Aufwand muss betrieben werden und – wer zahlt? Bund? Länder? Gemeinden?

Erlauben Sie mir, Ihnen etwas über den Stand der Aktivitäten auf den Gebieten der IT-Sicherheit in vernetzten Systemen und beim Digitalfunk zu berichten. IT-Sicherheit betrifft nicht nur den Einsatz von *Technik*. Sie betrifft auch Organisation, Personal und Infrastruktur. *Technische* und *organisatorische* Maßnahmen bedingen sich gegenseitig. Jedes IT-System sollte heutzutage mit anderen *vernetzt* sein, zumindest aber vernetzt werden können, so der hohe Anspruch. Vernetzung aber schafft zusätzliche Komplexität und Risiken, weil der Systemverbund grundsätzlich im gesamten peripheren Zugang offen ist für Angriffe und missbräuchliche Nutzungen.

Nehmen wir als Beispiel das Internet: Das Internet ist ein allgemein akzeptiertes, unverzichtbares Arbeitsmittel (privat und beruflich) geworden. Der historischen Entwicklung geschuldet sind dort fast keine oder nur sehr unzureichende Sicherheitsmaßnahmen vorhanden. Die missbräuchliche Nutzung ist sehr einfach. Einige Beispiele dafür sind uns allen präsent und ärgern uns bei der täglichen Nutzung des Mediums: Unerwünschte Mails (SPAM), Viren, die Verbreitung strafbarer Inhalte (Rechtsradikalismus, Pornografie), die Sorge um den Missbrauch von persönlichen Daten, vor allem im Geldverkehr. Im Sicherheitsbereich muss die Kommunikation der zuständigen Behörden natürlich in besonderem Maße geschützt werden. Am einfachsten wäre es, einzelne Teilsysteme zu isolieren, „Inseln" zu schaffen. Das wird in hochsensiblen Bereichen notgedrungen auch gemacht, aber es ist nicht das, was wir im IT-Verbund wollen!

Die Folge von „Insellösungen" ist der Verzicht auf die besonderen Vorteile vernetzter Systeme. Strategisch gesehen ist das ein Rückschritt! Uns stehen zunächst die konventionellen technischen Sicherheitsmaßnahmen zur Verfügung: „Virenschutz" und „Firewall". Dann gilt es, die Sicherheitskonzepte konsequent anzuwenden und damit Verfügbarkeit, Vertraulichkeit, Integrität, Authentizität und Nachweisbarkeit im jeweils erforderlichen Maße sicherzustellen. Die Sicherheitskonzepte sind regelmäßig auf Umsetzung und Wirksamkeit zu prüfen. Der *sichere* IT-Einsatz in einer komplexen, aus vielen unterschiedlichen Systemen bestehenden Umgebung, erfordert aber nicht nur Konzepte sondern auch Standards.

Standards beziehen sich dabei nicht nur auf Standards zur *technischen Zusammenarbeit* unterschiedlicher IT-Systeme, sondern auch auf die jeweiligen *Prozesse*. Dabei sind Sicherheitsmaßnahmen unter Berücksichtigung von *Aufwand* und *Nutzen* auszuwählen: So können *Schulungen* oder die *Sensibilisierung* der Beschäftigten manchmal wirkungsvoller sein als der Einsatz komplexer (und teurer) Technikkomponenten. Hierzu gehört auch die Überlegung, nach dem „Versicherungsprinzip" *„Vorsorge- und Interventionsmaßnahmen"* stärker miteinander zu verknüpfen, um noch unmittelbarer und zielgerichteter auf Sicherheitslücken reagieren zu können. Diese vernetzten Maßnahmen zur so genannten Notfallvorsorge haben große Bedeutung für die Stabilität der Systeme, auf die wir alle angewiesen sind. Regelmäßig werden in der Diskussion um die maximale IT-Sicherheit auch *Kostenargumente* vorgebracht, die den Wettstreit um die richtige Strategie erschweren. In Zeiten knapper Mittel müssen Entscheider ohnehin ständig abwägen: Zwischen Risikoprognose und Ressourcenschonung. Der Bereich der IT-Sicherheit hat in einer solchen Abwägung erhebliches Gewicht; mögliche Folgekosten eines Systemausfalles durch Betriebsstörungen oder sogar Attacken auf unsere Netzsysteme können ungleich gravierender ausfallen.

Mit der Einführung des Digitalfunks wird, da bin ich zuversichtlich, auch das Problem *„Netz-Sicherheit in der Kommunikation"* neue Lösungen erfahren. Ich darf Ihnen kurz die besonderen Sicherheitsmerkmale, die Vorteile und den letzten Stand der Dinge in Sachen Digitalfunk darlegen. Der Bund und die Länder sind sich einig, dass für die Behörden und Organisationen mit Sicherheitsaufgaben (so genannte BOS) auch in technischer Hinsicht mehr getan werden muss. Insbesondere zur besseren Kommunikation *zwischen* den BOS ist eine moderne und sichere *funktechnische* Aufrüstung erforderlich. Um ein Beispiel zu nennen: Nach dem Terroranschlag in London funktionierte die Lagebewältigung auch deshalb so reibungslos, weil die Kräfte vor Ort der Einsatzleitung per Digitalfunk Live-Bilder vom Geschehen schicken konnten. Zu den BOS zählen die Polizeien und Verfassungsschutzbehörden der Länder und des Bundes, der Zoll, das technische Hilfswerk, die Feuerwehren, die Rettungsdienste

und die Katastrophenschutzbehörden. Diese setzen heute zur Einsatzbewältigung im täglichen Dienst und bei Sonderlagen *analoge* Funktechnik ein, um ihren mobilen Kommunikationsbedarf zu decken.

Die analoge Funktechnik hat uns 30 Jahre gute Dienste geleistet. Aber sie wird durch die Industrie perspektivisch nicht mehr angeboten. Wir wissen um die Probleme, die die analoge Funktechnik mit sich bringt: Die Möglichkeiten der Kommunikation zwischen unterschiedlichen Dienststellen, die Sprachübertragungsqualität, die Zuverlässigkeit und der Komfort entsprechen nicht mehr dem Stand der Technik. Die Fortführung des Funkbetriebes mittels analoger Technik kann daher den wachsenden Anforderungen der BOS weder in alltäglichen Lagen noch in Katastrophenfällen gerecht werden.

Die Grenzen der analogen Funktechnik sind erreicht: Jede BOS betreibt ihr eigenes Analogsystem; übergreifende Kommunikationsmöglichkeiten sind in großen Einsatzfällen nicht umfassend gegeben und behindern die Einsatzführung;

- Die Vielzahl der analogen Funksysteme erzeugt einen permanenten Frequenzmangel.
- Übertragene Informationen können nicht vor unberechtigten Mithörern oder gar Manipulationen geschützt werden; Verschlüsselung ist *nicht* möglich.
- Sprach- und Datenübertragung in der gleichen Netzinfrastruktur ist nicht realisierbar.
- Die 1990 im Schengener Abkommen geforderten Möglichkeiten einer grenzüberschreitenden Kommunikation der BOS können nur unvollkommen gewährleistet werden. Schon damals haben die Innenminister der Länder und des Bundes deshalb klargestellt, dass es nur *eine* Lösung für die europäische Zusammenarbeit von Polizei, Zoll und Rettungskräfte gibt: Ein digitales Sprech- und Datenfunknetz auf *einheitlichen Funkfrequenzen!*

Die mobilen öffentlichen Netze sind ebenfalls nicht geeignet als vollwertige Ergänzung zur analogen Funktechnik. Sie werden zwar bei vielen Polizeidienststellen im Dienstbetrieb eingesetzt und gewährleisten eine flächendeckende Funkversorgung der Bundesrepublik Deutschland und der benachbarten Länder. Übertragene Informationen können sogar verschlüsselt werden.

Diesen *Vorteilen* im Vergleich zum heutigen analogen Funknetz stehen jedoch einige gravierende Nachteile in öffentlichen digitalen Funknetzen gegenüber:

- Gerade im Katastrophenfall stehen die öffentlichen mobilen Netze nicht zur Verfügung, sondern versagen wegen Überlastung. Dies haben die Sicherheitskräfte in London und Madrid leidvoll erfahren müssen. Es hat sich herausgestellt, dass im Katastrophenfall auch die Infrastruktur der öffentlichen Mobilnetze nicht stabil genug für die hohe Belastung ist.
- Darüber hinaus können einige Mindestanforderungen der BOS-Funksysteme *nicht* erfüllt werden: Hierzu gehört u.a. die Forderung zum „offenen Sprechverkehr", d.h. jeder hört jeden innerhalb eines Teilnehmerkreises.
- Es ist nicht möglich, dynamische Funkverkehrskreise zu bilden oder Leitstellen in die Funkinfrastruktur mit einzubinden.
- Zusätzliche Versorgungskapazitäten stehen im Bedarfsfall *nicht* oder *nicht* zeitnah zur Verfügung.

Die mobilen öffentlichen Netze können also derzeit nicht die Leistungsanforderungen erfüllen, die für die BOS von essentieller Bedeutung sind. Aus diesem Grunde haben Bund und Länder beschlossen, ein *einheitliches* digitales Funknetz für die BOS aufzubauen.

Die Vorteile des Digitalfunks liegen auf der Hand:

- die Eignung sowohl für Sprach- als auch für Datenübertragung, also ein mobiler Datenfunk und ein möglicher Zugriff auf Datenbanken;
- ein gemeinsam zu nutzendes einheitliches Funknetz für alle Sicherheitsbehörden der Länder und des Bundes;
- die flächendeckende Funkversorgung im gesamten Bundesgebiet für Fahrzeugfunkgeräte und für Handfunksprechgeräte;
- ein Funkbetrieb der Sicherheitsbehörden im Bereich der gesamten Bundesrepublik und der Schengenstaaten, über alle Landesgrenzen hinweg;
- ein *wesentlicher* Punkt, vor allem in der öffentlichen Wahrnehmung, stellt die Verschlüsselung des gesamten Funkverkehrs dar; unbefugtes Abhören wird künftig unmöglich;
- es können zusätzliche taktische und betriebliche Leistungsmerkmale eingerichtet werden, wie z.B. Datenübertragungen oder Konferenzschaltungen;
- wir versprechen uns eine deutlich höhere Sprachqualität und Datenübertragungssicherheit;
- zuletzt, aber wichtig für die Anwendung im Täglichen Dienst: Die Nutzer bekommen kleine, leichte, einfach zu bedienende und preiswertere Handfunkgeräte.

Die Leistungsmerkmale eines digitalen Funknetzes sind festgehalten in dem *„Abschlussbericht der Expertengruppe aus Bund und Ländern"*. Die so definierten GAN-Standards („Gruppe Anforderungen an das Netz") haben Leistungsmerkmale und technische Mindeststandards festgelegt.

Entsprechend den GAN-Standards muss ein Digitalnetz als Basisnetz auch bestimmte Sicherheitsbedingungen erfüllen.

Ich habe die Flächendeckung und die Verschlüsselung bereits genannt. Kernpunkt für einen sicheren Betrieb ein bundeseinheitlich von einem zentralen Netzbetreiber eigenständig betriebenes Netz. Die Funktionalitäten des Digitalfunks sind geeignet, durch vernetzte Sicherheit in Bund, Ländern und Gemeinden einen *wirksameren*, wenn nicht sogar *umfassend wirksamen* Schutz zu bieten.

Wie ist nun der aktuelle Stand der Einführung des Digitalfunks?
Der jahrelange Entscheidungsprozess zur Einführung des digitalen Sprech- und Datenfunks mündete zunächst in eine so genannte Dachvereinbarung zwischen Bund und Ländern. Diese gewährleistet einheitliche Standards und ein einheitliches Vorgehen bei einer bundesweiten Ausschreibung. Mit einem Rahmenvertrag soll das bundesweite technisch einheitliche Netz nach dem GAN-Standard gesichert werden, gleichzeitig aber sind unterschiedliche zeitliche Abläufe und solche bei der Funkversorgungsqualität während des Aufbaus der Teilnetze in den Ländern zugelassen.

Die zeitlichen Planungen für den Aufbau des Netzes sehen Einzelschritte vor. Die ersten Teilnetze sollen in 2007 in Betrieb gehen, das Gesamtnetz bis spätestens 31.12.2010 fertig gestellt sein. Die Dachvereinbarung regelt auch die für Planung und Aufbau des Digitalfunksystems der BOS notwendige Projektorganisation. Diese Projektorganisation wird als „netzwerk-BOS" bezeichnet und ist durch Bund und Länder gemeinsam eingerichtet worden.

Die Projektorganisation gliedert sich in den

- Lenkungsausschuss (Innenstaatssekretäre von Bund und Ländern),
- das Vergabegremium (Bund + Länder),
- den Gesamtprojektleiter (dem Staatssekretär des BMI unterstellt),
- die Projektgruppe (35 Vertreter von Bund + Ländern) sowie
- die Vergabestelle (Beschaffungsamt des BMI).

Darüber hinaus hat jedes Land eine Projektgruppe eingerichtet, die im „netzwerk-BOS" mitarbeitet und dem Gesamtprojektleiter als Ansprechpartner in allen Fragen des Projektes zur Verfügung steht.

Im Frühjahr 2005 haben Bund und Länder beschlossen, gemeinsam den Weg zu einem einheitlichen bundesweiten Digitalfunknetz zu gehen. Der Bund wird ein Rumpfnetz entsprechend des *„Mindeststandards GAN"* für 50 Prozent der Fläche eines jeden Landes sicherstellen. Die Länder werden das Rumpfnetz zu 100 Prozent des Mindeststandards und mit einer höheren Funkversorgungsqualität (GAN + X) ergänzen. Der Bund will die Bahntochter DB Telematik GmbH mit einem Betreibervertrag einsetzen.

Im Ergebnis der Ausschreibung zum Teilnahmewettbewerb im März 2005 sind fünf Unternehmen vom Beschaffungsamt des BMI ausgewählt und zur Abgabe eines Angebots aufgefordert worden. Im August 2005 fand eine „Erste Bieterkonferenz" statt. Auf Antrag der Firmen wurde die Angebotsfrist zur Abgabe eines Angebotes auf Dezember 2005 festgesetzt. Am 1. März 2006 präsentierte das Beschaffungsamt des BMI die Auswertung der Angebote.

Die Angebote wurden nach technischen Kennwerten zur angebotenen Leistung, nach Mindesterfüllungsgraden, Ausschlusskriterien, Gesamterfüllungsgrad sowie nach Kennwerten zu Preis-/ Leistungsdaten vergleichend dargestellt. Das Angebot von EADS/Siemens ist zum Ende des ersten Bewertungsschritts als das wirtschaftlichste bewertet worden. Gemäß den für dieses Vergabeverfahren geltenden Regelungen erfolgen nunmehr Labor- und Feldtests in Berlin und Stuttgart. Die Bindefrist der Angebote läuft bis zum 30. Juni 2006. Es wird mit einem Zuschlag zu diesem Zeitpunkt gerechnet. Im Rahmen der zukünftigen Zusammenarbeit zwischen Bund und Ländern ist eine „BOS-Stelle Digitalfunk" notwendig, in der alle Entscheidungen für den Betrieb des gemeinsamen Digitalfunks einvernehmlich getroffen werden können. Dies soll über eine Bundesanstalt für den Digitalfunk der BOS erfolgen. Das Gesetz zur Errichtung dieser Bundesanstalt wurde bereits im Juni 2005 in den Bundestag zur Abstimmung gebracht und in überarbeiteter Fassung in den kommenden Monaten im Bundesrat beraten. Voraussichtlich wird die BOS-Stelle ihre Arbeit im Herbst 2006 in Berlin aufnehmen.

Ich hoffe, es ist mir gelungen, Ihnen für einen Teilbereich einen Überblick über die Aktivitäten zur Umsetzung einer modernen und sicheren Informations- und Kommunikationsstrategie zu vermitteln. Es ist ein anspruchsvolles Programm, von dem aber im Ergebnis alle Bedarfsträger profitieren. Das gemeinsame Handeln von Bund und Ländern zeigt aber auch: moderne Sicherheit, moderne Schutzsysteme lassen sich gemeinsam, auf breiter Basis der Zusammenarbeit am besten verwirklichen.

Dr. Ehrhart Körting
Senator für Inneres, Berlin

Das Technische Hilfswerk und die Organisation der nichtpolizeilichen Gefahrenabwehr

Die Zuständigkeit und die Verantwortung für die Gefahrenabwehr liegt in der Bundesrepublik bei den Ländern. Im Bereich der nichtpolizeilichen Gefahrenabwehr unterhalten die Länder allerdings keine eigenen Einsatzkräfte und greifen im Bedarfsfall auf kommunale Feuerwehren, Hilfsorganisationen oder auf Einheiten der Bundesanstalt Technisches Hilfswerk zurück.

Sicherheitsarchitektur in Deutschland

Die Sicherheitsarchitektur in Deutschland ist auf vier Pfeiler gebaut. Neben der (1) Bundeswehr bilden (2) Polizei, Bundeskriminalamt (BKA) und Bundespolizei (BPOL) sowie der (3) Bevölkerungsschutz mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, der Bundesbehörde Technisches Hilfswerk, Feuerwehren und Hilfsorganisationen und letztlich die (4) Nachrichtendienste die Säulen für das nationale Sicherheitskonzept in Deutschland.

Gemäß dem deutschen Grundgesetz ist die Gefahrenabwehr wie folgt verteilt: Regionale Katastrophen – und somit der Katastrophenschutz _ fallen in die Zuständigkeit der Länder (Art. 70 Abs. 1 GG). Großflächige Gefahrenlagen im Frieden übernehmen Bund und Länder durch ein gemeinsames Krisenmanagement. Dies geht aus dem Beschluss der Ständigen Konferenz der Innenminister und Innensenatoren der Länder vom August 2002 hervor. Laut Artikel 73. Nr. 1 GG fällt der Verteidigungsfall in die Zuständigkeit des Bundes.

Entwicklung des Katastrophenschutz (KatS)

Nach der Wiedervereinigung der beiden deutschen Staaten wurde der Katastrophenschutz in der Bundesrepublik auf allen Ebenen zurückgefahren. Erst die Terroranschläge in New York und auf Bali haben zu einem Umdenken geführt. Als eine der noch ungeklärten Fragen generierte sich hierbei die Aufhebung der Trennung zwischen dem friedensmäßigen Katastrophenschutz (KatS), der im Bereich der Länder liegt, und dem Zivilschutz im Zuständigkeitsbereich des Bundes. Das THW ist als Einsatz- und Katastrophenschutzbehörde des Bundes wesentlich in die Strukturen des Katastrophenschutzes in Deutschland eingebunden.

Katastrophenschutz in Deutschland

In Deutschland wird der Katastrophenschutz von staatlichen und privaten Institutionen getragen. Zu den staatlichen Einrichtungen gehören neben dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) auch das THW, die Feuerwehren – auf kommunaler Ebene – und Länder, Kreise sowie Gemeinden mit verwaltungs- und administrativen Bereichen.

Zu den Privaten zählen die Sanitätsorganisationen wie das Deutsche Rote Kreuz (DRK), die Johanniter-Unfall-Hilfe (JUH), der Arbeiter-Samariter-Bund (ASB) sowie der Malteser Hilfsdienst (MHD) und die Werkfeuerwehren. Insgesamt engagieren sich in Deutschland rund 1.7 Millionen Menschen ehrenamtlich im Bereich des Zivil- und Katastrophenschutzes.

Zuständigkeiten

Die Zuständigkeiten im Bereich der Gefahrenabwehr verteilen sich auf die Kommunen, die Länder und den Bund mit jeweils unterschiedlichen Aufgabenspektren.

In das Aufgabengebiet den Kommunen fällt die örtliche Vorsorge. Hierzu zählen das Erstellen von Gefahrenanalysen, Einsatz- und Alarmierungsplänen sowie die Zusammenarbeit in der örtlichen Gefahrenabwehr. Die Kommunen übernehmen auch die Ausstattung der KatS-Einheiten, die Ausbildung und die Übungen sowie die Auswertung der Einsätze.

Die Länder koordinieren die Planung und die Abstimmung auf kommunaler und auf Landesebene. Sie erstellen die Gefahrenanalysen und statten die KatS-Organisationen zur Gefahrenabwehr aus.

Der Bund beschäftigt sich mit den Grundsatzfragen, wie der Vorsorgeplanung, der Zusammenarbeit, der Unterstützung von Kommunen, Kreisen und Ländern durch das THW. In den Zuständigkeitsbereich des Bundes fallen außerdem die Konzeption und die Durchführung der Aus- und Fortbildung sowie die Ausstattung im Katastrophenschutz.

Das Technische Hilfswerk (THW)

Für den Katastrophenschutz in Deutschland nimmt das Technische Hilfswerk eine bedeutende Rolle ein. Als die einzige operative Katastrophenschutzorganisation des Bundes ist das THW eine der tragenden Säulen des Zivil- und Katastrophenschutzes. Im Inland leistet es auf Anforderungen der zuständigen Stellen bei der örtlichen Gefahrenabwehr technische Hilfe im Bevölkerungsschutz und im Auftrag des Bundesinnenministeriums sowie auf Ersuchen des Auswärtigen Amtes auch im Ausland. Diesen gesetzlichen Auftrag erfüllt die zu 99 Prozent von ehrenamtlichem Engagement getragene Behörde seit 1950.

Eine Leitung mit Sitz in Bonn, acht Landes- und Länderverbände, 66 Geschäftstellen, 669 Ortsverbände und ein Zentrum für die Aus- und Fortbildung mit zwei Standorten bilden die Struktur der Bundesanstalt. Der modulare Aufbau mit bundesweit über 1.000 Fachgruppen ermöglichen dem THW rasche Hilfeleistungen unterschiedlichster Art. Mit seinen spezialisierten Fachgruppen ist die

Bundesanstalt somit den vielfältigen Anforderungen des Zivil- und Katastrophenschutzes gewachsen. Die Fachgruppen spezialisieren sich auf besondere Aufgaben und sind bundesweit einsetzbar und so verteilt, dass sie in kürzester Zeit eingreifen können. Auf Grundlage von Einsatzerfahrungen und Risikoanalysen wird dieser Aufbau ständig weiterentwickelt und optimiert.

Als moderne Einsatzorganisation ist das THW darum bemüht, sich den neuen Anforderungen, wie etwa den Folgen des internationalen Terrorismus oder den zunehmenden Naturkatastrophen, anzupassen. Durch zeitgemäße Einsatzoptionen, grenzüberschreitende Hilfeleistungssysteme sowie durch weltweite Vernetzungen und Kooperationen mit anderen Hilfsorganisationen bietet das THW den Bürgern einen umfassenden Schutz.

Koordiniert werden die bundesweiten Einsätze des THW durch die Leitung in Bonn, landesweit durch die Landes- und Länderverbände und regional durch die Geschäftstellen. Auf lokaler Ebene schließlich durch die Ortsverbände. Die Einbindung der THW-Ortsverbände in die örtliche Gefahrenabwehr garantiert eine schnelle und effiziente Hilfe auf lokaler Ebene. Auf regionaler und nationaler Ebene, also bei Katastrophen großen Ausmaßes wie der Jahrhundertflut 2002, zieht das THW seine Einheiten aus dem gesamten Bundesgebiet zusammen, um sie länderübergreifend einzusetzen. Die Aufgabenabstimmung innerhalb des THW erfolgt gemäß der Größe und der Bedeutung des Schadensereignisses und wird von der Leitung über die Landes- und Länderverbände und die Geschäftsstellen bis zu den Ortsverbänden delegiert. Diese zentrale Struktur und der bundesweit einheitliche Aufbau des THW sind die Grundvoraussetzung für ein leistungsfähiges System im KatS, da es eine einheitliche Ausbildung und Ausstattung sowie ein flächendeckendes Bereithalten von Einsatzkräften bietet. Die Leistungsfähigkeit im Katastrophenschutz wird dadurch erhöht.

Das THW im Inland

80 000 ehrenamtliche Helfer engagieren sich in ihrer Freizeit zum Wohle der Menschen im THW – ein Engagement ohne das der Zivil- und Katastrophenschutz in Deutschland so nicht denkbar wäre. Im Inland kommt das THW täglich zum Einsatz und untersteht der jeweiligen Einsatzleitung vor Ort. Mehr als eine Millionen Einsatzstunden leisteten die ehrenamtlichen Helfer des THW im vergangenen Jahr. Großeinsätze wie das Hochwasser in Bayern und die Stromausfälle im Münsterland oder der Weltjugendtag in Köln stellen dabei nur eine Auswahl dar. Die Einsätze sind aber nur ein Teil des Engagements der Hilfskräfte. Bevor es dazu kommt, absolviert jeder Helfer Grundlagenlehrgänge. Den Einsatzstunden folgen dann noch zahlreiche Ausbildungsveranstaltungen und Übungen, um im Ernstfall schnell und kompetent handeln zu können. Hierbei legt das THW vor allem auf gemeinsame Ausbildungsveranstaltungen mit anderen Organisationen großen Wert. Denn die enge Verzahnung mit den Feuerwehren, der Polizei und den anderen Organisationen gewährleistet einen entsprechend Schutz der Gesellschaft. Zahlreiche Kooperationsvereinbarungen mit den Partnerorganisationen sind nicht zuletzt ein Garant für eine professionelle und zukunftsfähige Struktur im nationalen Sicherheitskonzept Deutschlands.

Durch die Kombination von universellen Basiskomponenten und spezialisierten Fachgruppen unterstützt das THW sowohl Feuerwehren als auch Polizei und Bundespolizei. Die breite Abdeckung von Einsatzmöglichkeiten, die Ausstattung und das fachliche Wissen der ehrenamtlichen Helfer machen das THW zu einem verlässlichen Partner sowohl der örtlichen Gefahrenabwehr als auch der Sicherheitsstruktur der Bundesrepublik.

Das THW im Ausland

Das THW ist eine international ausgerichtete Organisation und in Belangen der humanitären Hilfe weltweit vernetzt. Als Instrument des Bundes wird es auch im Ausland eingesetzt, um technisch humanitäre Hilfe zu leisten. Die Leistungspalette reicht dabei von der akuten Nothilfe bis zum projektbezogenem Engagement beim Wiederaufbau, wie etwa beim Engagement nach Bürgerkriegen. Die Vereinten Nationen, die Europäische Union sowie Regierungen anderer Nationen gehören neben dem Auswärtigen Amt zu den Auftraggebern des THW. Schnelle Reaktionszeiten, Flexibilität, hohe Ausbildungsstandards und moderne Ausstattung machen die Einsatzteams des THW zu einer gefragten Hilfsorganisation im Ausland. Länderübergreifende Übungen auf europäischer Ebene sind die Grundlagen für eine gemeinsame humanitäre und effiziente Soforthilfe im Katastrophenfall. Daher pflegt das THW die partnerschaftliche Zusammenarbeit mit den Zivil- und Katastrophenschutzorganisationen aller Nachbarstaaten. Neben den gemeinsamen Übungen sind ein regelmäßiger Erfahrungs- und Informationsaustausch sowie die Unterstützung bei der Ausbildung ein wesentlicher Bestandteil der Kooperationen.

Nach schweren Naturkatastrophen wie dem Erdeben im iranischen Bam 2003, dem Tsunami in Süd- und Südostasien 2004 oder den Hurrikans „Katrina“ und „Rita“ in New Orleans 2005 leistete das THW in den vergangenen Jahren akute Nothilfe im Ausland. Logistische Unterstützung und Projektarbeit, wie dem Wiederaufbau, leistet das THW unter anderem in Afrika. Nach der Flutkatastrophe in den Niederlanden leistete die Bundesanstalt 1953 zum ersten Mal technische Hilfe im Ausland. Allein 2005 war das THW in über 30 Staaten als humanitärer Botschafter Deutschlands weltweit im Einsatz.

Das THW ist so nicht nur im Inland ein verlässlicher Partner für Menschen in Not, sondern auch außerhalb der Grenzen jederzeit einsatzbereit, um technische und humanitäre Hilfe zu leisten.

Oliver Hochedez
THW

Das Angebot des Bundes an die Länder und Kommunen zur Kommunikation im Bevölkerungsschutz

Um eine Steigerung der Effektivität und der Effizienz unseres integrierten Hilfeleistungssystems herbeizuführen, hatte sich der Bundesminister des Innern in der Ständigen Konferenz der Innenminister und -senatoren der Länder (IMK) im Juni 2002 mit den Ländern auf eine neue Strategie zum Schutz der Bevölkerung in Deutschland geeinigt.

Diese neue Strategie fordert vor allem ein gemeinsames Krisenmanagement bei außergewöhnlichen, national bedeutsamen Gefahren- und Schadenslagen, bei dem alle Ebenen (Kommunen, Länder, Bund) zusammenarbeiten müssen. Ein Schwerpunkt des Handelns auf dem Weg zu diesem Ziel ist die Entwicklung neuer Koordinierungsinstrumente für ein effizienteres Zusammenwirken des Bundes und der Länder, insbesondere für ein verbessertes Informations- und Ressourcenmanagement. Ich möchte Ihnen an dieser Stelle die Beiträge des Bundes vorstellen, die zu einer stärkeren technischen Informationsvernetzung aller Beteiligten im bundesweiten Krisenmanagement führen sollen. Dies sind das Satellitengestützte Warnsystem, das gemeinsamen Melde – und Lagezentrum und das Deutsche Notfallvorsorge-Informationssystem. Da diese Beiträge nicht ohne das Mitwirken anderer Stellen und Organisationen auskommen können, verstehe ich sie letztlich als Angebote zum Mitwirken der entsprechenden Partner bei der Implementierung und beim Betrieb.

Das Satellitengestützte Warnsystem (SatWaS)

Zu den Grundpfeilern des Bevölkerungsschutzes gehört es, die Bevölkerung angemessen, rechtzeitig, schnell und flächendeckend vor bestehenden Gefahren zu warnen. Das heutige Konzept für die Warnung der Bevölkerung basiert auf der Nutzung verschiedener moderner und zukunftsweisender Technologien. Innerhalb des neuen Warnsystems bildet die Warnung über den Rundfunk einen besonderen Schwerpunkt. Sie bietet die Möglichkeit, nicht nur vor Gefahren zu warnen, sondern zeitgleich gefahrenbezogen Verhaltensregeln an die Bevölkerung weiterzugeben. Am 15. Oktober 2001, also schon gut einen Monat nach den Anschlägen in den USA, hat der Bund ein neues, satellitengestütztes Warnsystem (SatWaS) in Betrieb genommen. Die für die Erfassung von Luftgefahren und die Warnung vor großflächigen radiologischen Gefahren eingerichteten Zivilschutz-Verbindungsstellen, die Warnzentrale Bonn sowie die Lagezentren der Länder wurden mit den notwendigen SatWaS-Übertragungs- und Empfangssystemen ausgestattet.

Die neuen Systeme machen es möglich, sekundenschnell Warnmeldungen und Gefahrendurchsagen mit höchster Priorität über Satellit an die angeschlossenen Medien weiterzugeben. Die Warnmeldungen beinhalten die Aufforderung an den Redakteur, die laufende Sendung sofort zu unterbrechen und den Text der Warnung über den Sender weiter zu geben. Neben den öffentlich-rechtlichen Rundfunkanstalten wurden auch die privaten Betreiber in dieses System einbezogen. 45 überregionale und 80 lokale Anbieter haben sich dem Warnsystem bereits angeschlossen.

Betreibern von Internetportalen wird ebenfalls ein Anschluss an das Satellitengestützte Warnsystem angeboten. Sie können dann Warnmeldungen in ihren Netzen an die Kunden verbreiten. Zur Zeit sind zwei Anbieter, t-online und my-weblife, betriebsbereit an SatWaS angeschlossen. Auch ein Paging-Dienst, e*Message, hat sich an das System angeschlossen und leitet an seine Pager-Kunden Hinweise auf Warndurchsagen weiter.

Durch den Anschluss großer Presseagenturen, beispielsweise DPA und AFP, werden die Warndurchsagen auch an deren Medien- und Pressekunden weitergeleitet. Im Endausbau des SatWaS soll umfassend gewährleistet sein, durch Mitbenutzung einer Vielzahl in der Fläche vorhandener moderner Kommunikations- und Informationsdienste (Rundfunk, Telefon, Internet, Paging, Mobilfunk, Funkuhr) in Gefahrensituationen rasche und lageangepasste Warnungen und Informationen an die Bevölkerung zu übermitteln.

Das Gemeinsame Lage- und Meldezentrum

Ein wesentlicher Bestandteil der Neuen Strategie ist die Einrichtung einer gemeinsamen Interministeriellen Koordinierungsstelle von Bund und Ländern für großflächige Gefahrenlagen, eines gemeinsamen Melde- und Lagezentrums (GMLZ) zu deren Unterstützung sowie die Inbetriebnahme des Deutschen Notfallvorsorge-Informationssystems (deNIS).

Das Zentrum für Krisenmanagement des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe in Bonn betreibt daher seit dem 1. Oktober 2002 auf dieser Grundlage ein gemeinsames Melde- und Lagezentrum von Bund und Ländern (GMLZ). Zweck des GMLZ ist die Sicherstellung des länder- und organisationsübergreifenden Informations- und Ressourcenmanagement bei großflächigen Schadenlagen oder sonstigen Lagen von nationaler Bedeutung im In- und Ausland (Naturkatastrophen und andere Katastrophen). Hierzu ist ein ständiges flächendeckendes, nationales Lagebild der zivilen

Sicherheitslage erforderlich. Die zentrale großflächige Betrachtung, das ständige Monitoring und die Integration von verschiedensten interdisziplinären Gefahrenerfassungsquellen lassen ein frühzeitiges Erkennen komplexer Szenarien zu.

Darüber hinaus wird das GMLZ im Auftrag des Bundesministeriums des Inneren im Rahmen des Gemeinschaftsverfahrens der Europäischen Union zur Förderung einer verstärkten Zusammenarbeit bei Katastrophenschutzeinsätzen tätig.

Die primären Aufgaben des GMLZ sind:

- der Betrieb als Geschäftsstelle der Interministeriellen Koordinierungsgruppe,
- der Betrieb eines ständig erreichbaren Meldekopfs bei großflächigen Gefahrenlagen und Ereignissen von nationaler Bedeutung,
- die Generierung eines jederzeit aktuellen, flächendeckenden Lagebildes der zivilen Sicherheitslage für die interministerielle Koordinierungsgruppe, das Lagezentrum des Bundesministeriums des Innern und andere Bedarfsträger,
- das Erstellen qualifizierter und überprüfter Gefahren- und Schadensprognosen in Zusammenarbeit mit anderen Behörden, Stellen und Institutionen,
- die Vermittlung von Engpassressourcen zur Gefahrenabwehr an nationale und internationale Bedarfsträger,
- Förderung der Zusammenarbeit bei Katastrophenschutzeinsätzen im Rahmen des Gemeinschaftsverfahrens der Europäischen Union.

Hierzu bedient sich das GMLZ sowohl des deutschen Notfallvorsorge-Informations-Systems (deNIS), als auch eines ständig wachsenden Netzwerks von eigenen und externen Experten aus den verschiedensten Einrichtungen und Behörden aus dem Bereich des Bevölkerungsschutzes. Neben 25 wissenschaftlichen Disziplinen die allein im BBK vertreten sind, sind dies z.B.: Robert-Koch-Institut, Paul-Ehrlich-Institut, Bundesamt für Sera und Impfstoffe Bundesamt für Strahlenschutz, Umweltbundesamt, Bundesamt für Verbraucherschutz und Lebensmittelsicherheit, Bundesforschungsanstalt für Viruskrankheiten der Tiere, das Havariekommando, Deutscher Wetterdienst, Bundesamt für die Sicherheit in der Informationstechnik, Wasser- und Schifffahrtsämter, BGS, THW, etc.

Das GMLZ ist mit modernster Hard-, Software und Medientechnik ausgestattet und gehört somit zu den modernsten Lagezentren in Deutschland. Zurzeit befindet es sich in den Räumlichkeiten der AKNZ in Ahrweiler und wird mit Fertigstellung der neuen Liegenschaft des BBK nach Bonn-Lengsdorf umsiedeln.

Insgesamt leistet der Bund mit dem GMLZ einen wichtigen Beitrag zu einem gemeinsamen Bund-Länder-Krisenmanagement. Es gilt deshalb das ressort- und länderübergreifende, interdisziplinäre Netzwerk auszubauen, um frühzeitig Gefahrenentwicklungen erkennen und bekämpfen zu können.

Der Erfolg des GMLZ wird maßgeblich von der aktiven Unterstützung und Mitwirkung aller Beteiligten abhängen.

Das deutsche Notfallvorsorge-InformationsSystem (deNIS)

Bundesinnenminister Otto Schily hatte bereits Mitte 2001 entschieden, ein deutsches Notfallvorsorge-Informationssystem (deNIS) aufzubauen. Er beauftragte die damalige Zentralstelle für Zivilschutz im Bundesverwaltungsamt mit diesem Projekt.

Die Notwendigkeit für die Verfügbarkeit eines solchen Informationssystems hat sich Monate später bestätigt. Obwohl wir über ausreichende Hilfepotenziale verfügen, hat sich bei der Bewältigung des Elbehochwassers gezeigt, dass dringend Verbesserungen beim überörtlichen Ressourcenmanagement geschaffen werden müssen. Defizite bei der Gewinnung, Verarbeitung und Übermittlung von Informationen waren oft Ursache für die aufgetretenen Schwierigkeiten.

deNIS I

Mit deNIS I wurde eine offene Internetplattform geschaffen, um die im Internet verfügbaren Informationen zu Notfallvorsorgemaßnahmen konzentriert anzubieten. Über die Internetadresse stehen heute dem Nutzer mehr als 3.000 Links zu Internetseiten zur Verfügung. Hier findet er Hintergrundinformationen zu Katastrophen, Hinweise für die Bevölkerung über Vorsorgemaßnahmen und Verhaltensregeln bei Gefahren sowie Erfahrungsberichte über Maßnahmen zur Gefahrenabwehr.

deNIS II/deNIS II plus

Ziel dieses Informationssystems ist es, ein Netzwerk im Bereich des Zivil- und Katastrophenschutzes aufzubauen, um das Krisenmanagement bei außergewöhnlichen Gefahren- und Schadenslagen zu unterstützen. Hierzu sollen Daten von Bundesressorts, Ländern, Instituten und internationaler Institutionen zentral zusammengefasst, aufbereitet und berechtigten Bedarfsträgern zur Verfügung gestellt werden. Zu diesen Daten gehören Informationen über personelle, materielle und infrastrukturelle Hilfeleistungspotenziale aber auch über Standorte risikobehafteter Anlagen. Insgesamt soll dadurch die Beurteilung der

Lage hinsichtlich der rechtzeitigen Anforderung weiterer Hilfeleistungspotenziale oder von Engpassressourcen aus Nachbarländern oder des Bundes erleichtert werden.

Da hierbei auch vertrauliche Informationen ausgetauscht werden, steht dieses System nur einem eingeschränkten Benutzerkreis zur Verfügung stehen. Hierbei handelt es sich um Entscheidungsträger bei Bund und Länder, die bei einer großflächigen Gefahrenlage tätig werden. Zu diesem geschlossenen Benutzerkreis zählt die

Interministerielle Koordinierungsgruppe, die aus Vertretern der Bundesressorts und der Länder besteht und nur bei großflächigen Gefahrenlagen zusammentritt. Darüber hinaus haben auch die Lagezentren der Innenministerien der Länder und die obersten Katastrophenschutzbehörden der Länder sowie die Hilfsorganisationen Zugang zu deNIS II erhalten.

Wichtige Informationen zu Hilfeleistung- und Risikopotenzialen sind weit verstreut bei Spezialbehörden vorhanden. Wie bereits erwähnt, ist eine wichtige Aufgabe von deNIS II, diese Daten zentral zusammenzuführen, um sie den Entscheidungsträgern zur Verfügung zu stellen.

Diese Daten müssen für die Unterstützung des Krisenmanagements bei großflächigen Gefahrenlagen aufbereitet werden. Hierzu nutzt deNIS II ein geographisches Informationssystem. Kernelement dieses Systems ist eine interaktive Bildschirm-Lagekarte. Vor einem geographischen Hintergrund werden mit diesem System Informationen über ein Ereignis, über die zur Verfügung stehenden Hilfeleistungspotenziale sowie über weitere Risikopotenziale auf einer Bildschirmlagekarte eingeblendet.

deNIS II plus

Um die Datenbank deNIS II mit Daten zu füllen, werden regelmäßig Abfragen zu Hilfeleistungspotenzialen bei Ländern und Bundes-behörden durchgeführt, die bisher nur als Clients am Bundesserver angeschlossen sind. Hierbei hatte sich herausgestellt, dass auf Ebene der Innenministerien der Länder oft keine Datenbanken vorhanden sind, um diese Daten automatisch in deNIS II zu integrieren. Aus diesem Grund wurde eine Entwicklung in die Wege geleitet, die den Ländern ermöglicht, im Bereich des Katastrophenschutzes auf Basis der deNIS II-Technologie eigene Datenbanksysteme, an die sie wiederum untere Ebenen als Clients anschließen können, aufzubauen. Diese Entwicklung wird als deNIS II plus bezeichnet. Im Unterschied zu deNIS II enthält deNIS II plus Werkzeuge, die eine dezentrale Erfassung von Daten zu Hilfeleistungspotenzialen und einen automatisierten Datenaustausch ermöglicht: Die Erfassung und Aktualisierung von Ressourcedaten ist direkt über Eingabemasken möglich. Daher können die Daten dort erfasst und gepflegt werden, wo sie entstehen. Die Verfügbarkeit über aktuelle Daten wird dadurch wesentlich erhöht, weil die Dateneingabe über Dritte wegfällt. Darüber hinaus enthält deNIS II plus neben dem ohnehin auch schon in der Vorgängerversion integrierten Ressourcenmanagement auch ein Modul „Melde- und Auftragsmanagement“, das sowohl eine Erfassung und Übermittlung von Lagemeldungen auf allen Ebene des bundesweiten Krisenmanagements als auch die Erteilung und die Überwachung von Aufträgen ermöglicht. Ebenso wird die Einsatzplanung unterstützt: man kann schon im Vorfeld eines Einsatzes Absperrkreise, Evakuierungszone usw. in eine Karte eintragen und sie dann im Einsatzfall bei Bedarf abrufen. Das gleiche gilt für Maßnahmenlisten, die nun rollenbezogen im System hinterlegt werden können.

Zusammenfassend ergeben sich für das Informations- und Kommunikationsmanagement aus der bisherigen Entwicklung von deNIS folgende Vorteile:

- Elektronische Unterstützung von Stabsabläufen,
- Ämter und ebenenübergreifende, umfassende rechnergestützte grafische und dynamische Darstellung der Gesamtlage und der zur Verfügung stehenden Ressourcen für alle am Krisenmanagement beteiligten Stellen,
- Windowsähnliche, einheitliche Oberfläche (webbasiert mit implementierter Zugriffshierarchie),
- Einfache Benutzerverwaltung,
- Hohe IT-Sicherheit durch geschützte Netze,
- Dezentrale Datenerfassung und -verwaltung,
- To-do-Listen mit Statusverfolgung und Warnmeldung.

In den weiteren Stufen der Verbreitung bzw. der Weiterentwicklung des Programms sind folgende Features vorgesehen:

- Unmittelbarer Datenaustausch von einer Datenbank zur anderen Datenbank im Rahmen definierter Rechte,
- Einbindung von Gefahrenerfassungssystemen,
- Standardschnittstellen zu anderen Krisenmanagementsystemen, z.B. solchen, die auf der Ebene der Länder schon existieren.

Mit der Weiterentwicklung zu deNIS II plus bietet sich erstmals die Möglichkeit, alle Führungsebenen miteinander zu vernetzen und in Deutschland ein umfassendes Netzwerk im Bereich des Bevölkerungsschutzes aufzubauen.

Zusammenfassend ist festzustellen, dass mit dem deutschen Notfallvorsorge-Informationssystem den Ent-

scheidungsträgern bei Bund und Ländern eine wichtige Plattform für das IT-gestützte Krisenmanagement bereitgestellt wird: deNIS II plus wird durch die Bereitstellung der vernetzten Informationen die Risikoabschätzung und das Ressourcenmanagement auf den jeweiligen Entscheidungsebenen erleichtern.

Insgesamt leistet der Bund mit deNIS einen wichtigen Beitrag zum eGovernment im Bereich des Zivil- und Katastrophenschutzes.

Zum Schluss meiner Rede möchte ich noch kurz auf die politische Aspekte der weiteren Entwicklung im Bereich deNIS eingehen. Ich hatte eingangs erwähnt, dass die im Gefolge der schlimmen Ereignisse der Jahre 2001 und 2002 entwickelte „Neue Strategie" Auslöser für das Engagement des Bundes war: Die Länder hatten den Bund gebeten, zur Unterstützung ihres Krisenmanagements verstärkt Koordinations- und Informationsfunktionen vorzuhalten. Der Bund ist dieser Bitte nachgekommen und hat mit GMLZ, deNIS, SatWaS eine breite Palette an Angeboten unterbreitet. Das an der „Neuen Strategie" orientierte Handeln verlangte nach schnellen, pragmatischen Lösungen für die diagnostizierten Defizite des deutschen Hilfeleistungssystems.

Eine wesentliche Rahmenbedingung für die Verbesserung des Hilfeleistungssystems war die Auffassung, dass sich an den Eckpfeilern unseres Hilfeleistungssystems grundsätzlich nichts ändert, sondern dass durch mehr Kooperation und Koordination vorhandene Sicherheitslücken geschlossen werden. Die geforderte Kooperation und Koordination muss auch auf dem Gebiet der Entwicklung rechnergestützter Informations- und Kommunikationssysteme stattfinden. Nichts wäre schlimmer als ein Nebeneinander nicht interoperabler Systeme, was den Datenverbund verhindert. Die Entwicklung von Standards im Bereich der Interoperabilität scheint dringend geboten. Ebenso abträglich sind schleppende oder gar nicht stattfindende Zulieferungen von Daten. Viele Gespräche werden daher geführt, um bestehende Möglichkeiten der Zusammenarbeit und des Informationsaustausches auszuloten. Dies gilt auch für europäische Projekte. Die Mitarbeit in diesen Projekten soll dazu dienen, europäische Entwicklungen frühzeitig mit nationalen Bestrebungen zu verbinden. Es bleibt abzuwarten, ob diese Bemühungen insgesamt von Erfolg gekrönt sind.

Ich danke Ihnen für die Aufmerksamkeit.

Christoph Unger

Präsident des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe

Datensicherheit – die Grundlage für vertrauensvolles eGovernment

Ich freue mich, Ihnen bei der Fachkonferenz Sicherheitskommunikation für Städte und Gemeinden die aktuellen Entwicklungen der Sicherheit in der Informationstechnik und die Rolle des Datensicherheit beim E-Government vorstellen zu können.

Städte und Gemeinden nehmen in der IT-Sicherheit, wie auch in der allgemeinen Sicherheitspolitik eine herausragende Stelle ein. Sie bilden die Netzknoten nicht nur unserer Informationsgesellschaft. Nach Erhebungen des Statistischen Bundesamtes leben in Deutschland knapp 49 Prozent der Bevölkerung in dicht besiedelten, städtischen Gebieten. Zählt man die mittelstark besiedelten Gebiete hinzu, sind es bereits über 83 Prozent der Bevölkerung. Bezogen auf die IT-Nutzung ergab eine repräsentative Studie von TNS Infratest, dass prozentual die meisten Internet-Nutzer in den großen Städten leben. In den Städten und Gemeinden findet der Großteil der Kommunikation der Bürgerinnen und Bürger, der Wirtschaft und der Verwaltung statt. Hier sind die aktuellen und potentiellen Nutzer der E-Government-Lösungen zu Hause. Gleichzeitig sind dies auch diejenigen, die sich mit ihrer IT-Sicherheit beschäftigen müssen.

Datenbestände und IT-Strukturen von Privatpersonen, Unternehmen und Behörden sind immer wieder Angriffen ausgesetzt. Regelmäßig beobachten wir Angriffe auf die IT- und Datensicherheit. Schadprogramme versuchen Daten auszuspähen oder drohen, die Funktionsfähigkeit von IT-Systeme – z.B. durch massive E-Mail-Attacken – zu beeinträchtigen. Ein aktuelles Beispiel ist ein als WM-Spielplan getarntes Schadpropgramm, das als Dateianhang unerwünschter E-Mails verschickt wird.

Die Autoren von Schadprogrammen arbeiten zunehmend mit psychologischen Tricks und setzten auf das „Social Engineering“. Sie sprechen gezielt das menschliche Verhalten an, im aktuellen Fall das hohe Interesse an der Fussball-WM. Und sie spekulieren auf Unvorsichtigkeiten bei der Herausgabe persönlicher Daten oder dem Öffnen von Dateianhängen. Weitere bekannte Beispiele sind E-Mails mit einem Dateinanhang, der angeblich Informationen zu einem geplanten Klassentreffen enthält. Andere E-Mails sollen den Anschein erwecken, sie stammen aus offizieller Quelle, zum Beispiel dem BKA.

Auch Behörden sind immer wieder von Attacken betroffen. Ende April berichtete die Presse über einen Einbruch in das Rechnersystem des amerikanischen Verteidigungsministeriums. Hacker erbeuteten aus dem Krankenversicherungs-system des Pentagon über 14.000 Kreditkarten- und Sozialversicherungsnummern, die Privatadressen und dienstliche Durchwahlnummern. Im Februar 2006 berichteten die Medien über einen massiven Abhörangriff, bei dem im Olympiajahr 2004 die Mobiltelefone der Mitglieder der griechischen Regierung, von Oppositionspolitikern sowie Botschaftsmitarbeitern belauscht wurden.

Diese Beispiele zeigen, dass aus der zunehmenden IT-Durchdringung unserer Gesellschaft und der globalen Vernetzung neue Gefährdungssituationen resultieren, denen wir wirkungsvoll begegnen müssen. Sie zeigen auch, dass die Sicherheit der IT und die Sicherheit der Daten in einem unmittelbaren Zusammenhang stehen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die nationale Sicherheitsbehörde Deutschlands, die entsprechend des gesetzlich verankerten Auftrags aus dem BSI-Errichtungsgesetz (BSIG vom 17. Dezember 1990) für die IT-Sicherheit zuständig ist. Dabei ist die IT-Sicherheit als integraler Bestandteil der inneren und äußeren Sicherheit zu sehen. Dementsprechend positioniert sich das BSI als IT-Sicherheitsdienstleister des Bundes und arbeitet eng mit den nationalen und internationalen Sicherheitsbehörden zusammen.

Die Grundlage unserer Tätigkeit bildet der Beschluss des Bundeskabinetts vom 13. Juli 2005 zum dem „Nationalen Plan zum Schutz der Informationsinfrastrukturen (NPSI)“. Diese IT-Sicherheitsstrategie für Deutschland wurde im Koalitionsvertrag vom 11. November 2005 bestätigt. Umfassender Schutz unserer IT-Systeme ist nur in einer gemeinsamen Anstrengung zu erreichen. Alle gesellschaftlichen Gruppen tragen hier Verantwortung. Der Nationale Plan richtet sich deshalb an die Verantwortlichen in Verwaltung und Wirtschaft genauso wie an die Bürgerinnen und Bürger. Er benennt Ziele und erste Maßnahmen zur dauerhaften Sicherung der Informationsinfrastrukturen unseres Landes. Für die operative Umsetzung des nationalen Plans ist das BSI verantwortlich.

Dabei verfolgt das BSI drei strategische Ziele:

- Mittels Prävention einen angemessenen Schutz der Informationsinfrastrukturen zu erreichen,
- als Reaktion auf IT-Sicherheitsvorfälle wirkungsvoll und schneller handeln zu können sowie
- durch Nachhaltigkeit die deutsche IT-Sicherheitsindustrie auch auf internationaler Ebene zu stärken und Standards zu setzen.

Mit dem „Bericht zur Lage der IT-Sicherheit in Deutschland“ haben wir im August 2005 die Bedrohungslage systematisch analysiert und Lösungsansätze vorgestellt. Wir haben uns dabei vor allem mit vier Aspekten befasst:

- Wie ist der aktuelle Sachstand? Wodurch wird die IT in Deutschland heute vor allem bedroht?
- Welche Herausforderungen kommen auf uns zu? Welche Veränderungen sind zu erwarten?
- Welche Trends zeichnen sich ab? Welche Motivationen treiben z. B. Programmierer von Schadprogrammen oder Hacker an und wie verändern sich diese Motivationen?
- zeigt der Bericht den bestehenden Handlungsbedarf auf und nennt Möglichkeiten, wo sich die jeweiligen Zielgruppen über die notwendigen Schutzmaßnahmen informieren können.

Ich möchte Ihnen den Lagebericht jetzt nicht im Detail vorstellen. Sie können ihn im Internet-Auftritt des BSI einsehen. Trotzdem möchte ich an dieser Stelle auf ein paar Punkte eingehen, die für die IT-Sicherheit entscheidend sind.

Positiv ist festzustellen, dass alle gesellschaftlichen Gruppen sich der Risiken bei der Nutzung von IT bewußt sind. Jedoch mangelt es in der Wirtschaft und der Verwaltung an der Umsetzung von IT-Sicherheitsstrategien und der dauerhaften Implementierung entsprechender Maßnahmen.

Bei den Bürgerinnen und Bürgern ist die IT-Sicherheitskompetenz ist nur unzureichend verbreitet. Obwohl sie immer mehr von Informationstechnik abhängen – sei es am Arbeitsplatz, beim Zahlungsverkehr, in der Kommunikation oder im E-Commerce – räumen nur wenige sicherer Informationstechnik in der Praxis den erforderlichen Stellenwert ein.

Ähnliches gilt sowohl für die Wirtschaft als auch für die Verwaltung. Hier wird das Thema Sicherheit zu oft erst nach einem Schadensfall ernst genommen. Und das, obwohl wirtschaftlicher Erfolg und auch die Akzeptanz von E-Government-Lösungen heute maßgeblich von funktionierender IT bestimmt werden.

Bei der Analyse der Gefahren für die IT-Sicherheit steht die Verbreitung von Schadprogrammen im Vordergrund. In der zweiten Hälfte des Jahres 2004 wurden mehr als 7.360 neue Viren- und Wurmvarianten registriert. Das ist eine Zunahme von 64 Prozent gegenüber dem ersten Halbjahr.

Allerdings nimmt auch der Faktor Mensch – also Irrtum, Unkenntnis und Nachlässigkeit der Mitarbeiter in Unternehmen, in Verwaltungen und der Privatanwender – ebenfalls einen hohen Stellenwert ein.

Ein weiterer Trend ist zu beobachten: Computerwürmer werden immer seltener dazu programmiert, direkt irreparable Schäden anzurichten. Vielmehr versuchen Angreifer, den befallenen Rechner für einen kontinuierlichen Missbrauch unter ihre Kontrolle zu bringen.

Mit Hilfe Trojanischer Pferde missbrauchen Hacker oft mehrere tausend PCs und vermieten diese sogenannten Bot-Netze für kriminelle Zwecke. Sie dienen als Plattform zur Verbreitung neuer Epidemien von Computerschädlingen, für Denial-of-Service (DoS)-Attacken um Internetserver zu sabotieren oder zum Versand von Spam-Mails. Aus das Ausspähen sensitiver Daten wie z. B. Kontonummer, PIN und TAN durch sogenannte Password-Fishing – kurz Phishing – erfolgt zunehmend über Trojanische Pferde, die wiederum über Spam-Mails verbreitet werden.

Allein im Informationsverbund Berlin-Bonn (IVBB), einem der größten Netzwerke in Deutschland, registrieren wir im Schnitt einen Spam-Anteil von über 60 Prozent. Bei Spam-Wellen steigt der Anteil auf mehr als 90 Prozent.

Wenn Sie mich nun nach den Lehren fragen, die wir aus der Erstellung unseres Lageberichts ziehen konnten, so sind es zwei Punkte, die besonders deutlich geworden sind: Zum einen wird unsere Abhängigkeit von der Informationstechnik weiter zunehmen. Mit „uns“ meine ich in diesem Fall alle gesellschaftlichen Gruppen: Bürgerinnen und Bürger genauso wie die Wirtschaft oder die Verwaltung. Mit der steigenden Nutzung der IT steigen aber auch die Risiken.

Neue Schadprogramme wie Viren und Würmer entstehen täglich. Mit Spam-Mails, den unerwünschten E-Mails, werden sie schnell und massenhaft verbreitet. Dazu werden auch verstärkt Bot-Netzwerke eingesetzt, die aus infizierten, ferngesteuerten PCs argloser Anwender bestehen.

Vor allem hat sich die Motivation geändert. Im Schwerpunkt handelt es sich um organisierte Kriminalität. Diese Cyber-Kriminalität bedient sich zunehmend der Dienste von Hackern. Ich möchte hier kein allzu düsteres Bild zeichnen, doch die Lage ist ernst.

Aber, und damit komme ich zur zweiten Lehre: Noch ist die Lage beherrschbar. Gerade Deutschland – eines der von IT am stärksten durchdrungenen Staaten weltweit – steht im internationalen Vergleich in puncto IT-Sicherheit gut da. Doch um die Vorteile funktionsfähiger IT-Systeme auch künftig in vollem Umfang nutzen zu können, muss die IT-Sicherheit in Deutschland weiter verbessert werden.

Zum Schutz der IT-Netze und Computersysteme des Bundes betreibt das BSI seit fünf Jahren das Computer-Notfall-Team CERT-Bund als zentrale Anlaufstelle für die

Rechner- und Netzwerksicherheit der Bundesverwaltung. Im Falle von IT-Krisensituationen führen wir im nationalen Lagezentrum des BSI alle relevanten Informationen zusammen, werten sie aus und eskalieren sie bei Bedarf. Ein wesentlicher Aspekt ist hierbei ein effizientes Frühwarnsystem. Während der Fußballweltmeisterschaft ist das BSI in das Lagezentrum des Bundesministerium des Innern integriert. Zudem hat CERT-Bund den Auftrag, das nationales Netzwerk von Sicherheitsteams, einen nationalen CERT-Verbund, der derzeit aus rund 30 Sicherheitsteams besteht, auszubauen.

Relevante Informationen zur IT-Sicherheit stellen wir auch weiteren Zielgruppen zur Verfügung. In Kooperationen mit der Industrie – hier arbeiten wir mit Mcert/Deutsche Gesellschaft für IT-Sicherheit und dem Bitkom-Verband zusammen – trägt das BSI zur Steigerung der IT-Sicherheit im Mittelstand bei.

Private PC-Anwender erhalten über den Warn- und Informationsdienst des BSI „Bürger-CERT“ (www.buerger-cert.de) und über unser Bürger-Portal (www.bsi-fuer-buerger.de) wichtige Hilfestellung für den Schutz ihrer Privatsphäre. Mit dieser Sensibilisierung und der Herausgabe handlungsorientierter Informationen ermöglicht das BSI die sichere Nutzung der Informations- und Kommunikationstechnik in unserer Gesellschaft.

Als IT- und Sicherheitsverantwortliche der Städte und Gemeinden können Sie von diesem Angebot direkt profitieren. Zudem können Sie als Service für die Bürgerinnen und Bürger in Ihrer Kommune auf die Angebote „Bürger-CERT“ und „BSI für Bürger“ hinweisen, z.B. durch einen Link auf der Internetseite ihrer Kommune. Damit unterstützen Sie vor Ort die IT-Sicherheit!

Das Leitbild des BSI lautet „Sichere Informationstechnik für unsere Gesellschaft“. Um dies zu erreichen, unterstützen wir Unternehmen und Verwaltungen mit einem umfassen Informationsangebot, das ihnen hilft, ihre IT-Sicherheit zu erhöhen. Erwähnt sei z. B. unser IT-Grundschutzhandbuch – mittlerweile ein Standardwerk – und die Möglichkeit der Zertifizierung von Software-Produkten.

Zudem entwickeln wir in Zusammenarbeit mit der Industrie Systeme und Verfahren, um somit einen Beitrag zur inneren Sicherheit Deutschlands und in Europa zu leisten.

Ein prominentes Beispiel ist der Einsatz biometrischer Technologien bei hoheitlichen Dokumenten, wie dem ePass. Seit November 2005 werden in Deutschland elektronische Reisepässe mit einem ersten biometrischen Merkmal im Chip, dem digitalen Passfoto, ausgegeben. Biometrische Verfahren ermöglichen z.B. die automatisierte Erkennung des Passinhabers als Ergänzung zur herkömmlichen Kontrolle durch die Augen der Grenzbeamten. Neben der erhöhten Fälschungssicherheit durch digitale Signaturen eröffnet der ePass damit eine neue Stufe der Sicherheit: die eindeutige und nicht trennbare Zuordnung eines Dokuments zu seinem Inhaber durch die elektronische Speicherung von Gesichtsbild und Fingerabdruck unmittelbar im Dokument.

Wesentlicher Schritt zu diesem neuen biometriegestützten Grenzkontrollregime sind weltweit einheitliche Standards für Pässe und Lesegeräte.

Aktuell testeten hierzu vom 30. Mai bis 01. Juni 2006 in Berlin Experten aus 38 Nationen mit einem Interoperabilitätstest die wechselseitige Funktionsfähigkeit von elektronischen Reisepässen und Lesegeräten. Das Deutsche Institut für Normung e.V. hat in Zusammenarbeit mit dem Bundeskriminalamt (BKA) und dem BSI die Veranstaltung unter der Schirmherrschaft der Europäischen Kommission, des Französischen Innenministeriums und des Bundesministeriums des Innern organisiert.

An zwei Testtagen wurden mehr als 400 elektronische Reisepässe unterschiedlicher Länder in Kombination mit 50 Lesegeräten verschiedener Hersteller geprüft. Ein abschließender Ausstellungs- und Konferenztag am 1. Juni 2006 dient dem internationalen Austausch über den Einsatz von Biometrie in Dokumenten.

Die Ergebnisse des mit über 450 Teilnehmern sehr gut besuchten internationalen Expertentreffens in Berlin bestätigen eindrucksvoll, dass der elektronische Reisepass sowohl für den hohen Standard der IT-Sicherheit in Deutschland, als auch für die erfolgreiche Zusammenarbeit von Behörden und der Industrie steht.

Diese Kompetenz in der IT-Sicherheitstechnologie wollen wir mit der zweiten Stufe des elektronischen Reisepasses ausbauen. Für 2007 ist die zusätzliche Speicherung der Fingerabdrücke in den ePass-Chips vorgesehen.

Mit BundOnline 2005 startete die Bundesregierung im Jahr 2000 Europas größte E-Government-Initiative. Bis Ende 2005 waren über 400 Dienstleistungen des Bundes online verfügbar. Statistische Daten übermitteln, Renten-Anträge stellen oder Patente anmelden ist heute dank BundOnline über das Internet möglich.

Eine wesentliche Voraussetzung für erfolgreiches E-Government ist die Datensicherheit. Behörden, Unternehmen und die Bürgerinnen und Bürgern darauf vertrauen können, dass Informationen, die auf elektronischen Wege kommuniziert werden, nicht von Unberechtigten eingesehen werden können.

Mit der Virtuellen Poststelle (VPS) des Bundes stellt das BSI die „Basiskomponente Datensicherheit“ zur Verfügung. Sie unterstützt den verschlüsselten und signierten elektronischen Datenverkehr zwischen Bürgern, Unternehmen und Behörden. Durch diese zentrale Lösung werden die Mitarbeiter einer Behörde von komplexen Sicherheitsthemen des elektronischen Schriftverkehrs entlastet.

Eingehende E-Mails und Nachrichten aus Web-Formularen werden erfasst, entschlüsselt und auf schädliche Inhalte überprüft. Der Absender einer Nachricht wird verifiziert, die Nachricht erhält einen Zeitstempel und der Absender eine Empfangsbestätigung. Diese Funktionen erfolgen zentral und automatisiert. Mit der Ende-zu-Ende-Verschlüsselung leistet die VPS sowohl einen Beitrag zu IT-Sicherheit als auch zum Datensicherheit.

Die VPS ist ein Beispiel für die praxisorientierte Umsetzung von IT-Sicherheit. Aktuell wird sie in 17 Behörden in unterschiedlichsten Fachverfahren eingesetzt. Anwender sind z.B. das Luftfahrtbundesamt, das Bundesamt für Finanzdienstleistungsaufsicht und das Bundessozialgericht. 13 weitere Behörden planen den Einsatz der VPS. Die Anzahl der Behörden, die den Einsatz der VPS in prüfen, nimmt stetig zu.

Die sichere und geschützte Kommunikation der Behörden und Organisationen mit Sicherheitsaufgaben (BOS) besitzt einen besonderen Stellenwert. Hier besteht eine große Herausforderung in der Umsetzung des digitalen BOS-Funknetzes. Mit dem vom BSI entwickelte Kryptosystem für BOS-digital leisten wir auch einen wesentlichen Beitrag zur Datensicherheit. Zudem betreiben wir das Trustcenter zur Personalisierung der BOS-Sicherheitskarten.

Die technische Verfügbarkeit der Anwendungen und die Sicherheit der Daten sind Erfolgskriterien für das E-Government. Der Schutz der Informationsinfrastrukturen und damit der Schutz sensibler Daten betrifft uns alle. Denken Sie auch einmal darüber nach, von welchen IT-Systemen Sie selbst, Ihr Behörde oder Kommune abhängig ist. Überlegen Sie weiter, was die Folge sein könnte, wenn Ihre eigenen IT-Systeme gestört sind. Ich denke Sie werden erkennen, wie sehr wir alle von der Informationstechnik abhängen – und wie sehr wir über unsere IT auch voneinander abhängig sind.

Dr. Udo Helmbrecht

Präsident des Bundesamtes für Sicherheit in der Informationstechnik

Organisatorische und technische Perspektiven in Einsatzleitbereichen

1. Einleitung

Der Bereich der Einsatzleitstellen unterliegt einem starken Wandel, wobei die Entwicklung in Deutschland tendenziell noch am Anfang ist. Hierzulande herrscht ein bunter „Flickenteppich" unterschiedlichster Zuständigkeiten, organisatorischer Ausprägungen und technischer Systeme. Insbesondere in der Fläche gibt es unterschiedlichste Strukturen, die unter dem Aspekt der erforderlichen Professionalität in diesem elementaren Bereich kritisch bewertet werden müssen.

Dies bedingt nicht nur erhebliche Kosten, sondern auch qualitative Probleme, insbesondere wenn es darauf ankommt, dass bei Großlagen alle Dienste (Polizei, Feuerwehr, Rettungsdienst) Hand in Hand arbeiten. Wie die Erfahrung zeigt und unzählige Zeitungsberichte deutlich machen, gibt es hier ein erhebliches Verbesserungspotenzial. Dies bedeutet, dass es in diesem Bereich – im Gegensatz zur allgemeinen Verwaltungsmodernisierung mit Hilfe von eGovernment – nicht nur um die Reduktion von Kosten geht, sondern insbesondere auch die Qualität der Aufgabenerledigung und der Steuerung der Einsatzkräfte erheblich verbessert werden kann.

In den 90er Jahren wurden weltweit aufgrund unterschiedlicher Anforderungen bzw. Auslöser wie u.a.

- Geforderte Effizienzsteigerungen in der Notrufannahme und Disposition,
- Verbesserung der Zusammenarbeit von Rettungsdienst, Feuerwehr und Polizei vor allem auch bei Großschadensereignissen (z.B. Enschede in den Niederlanden) und
- Kostenreduzierung bei der Einführung neuer Technologien bzw. der Beschaffung neuer Infrastruktur

die Organisation der Notrufannahme und damit auch der Leitstellen kritisch überprüft. Der Änderungsdruck, der sich für die verschiedenen Leitstellen ergibt ist vielfältig und in der Abbildung dargestellt.

In diesem Beitrag wird beispielhaft ein Überblick über Handlungsoptionen bzw. Strukturmodelle zur verbesserten Zusammenarbeit der einzelnen Dienste (Polizei, Feuerwehr, Rettungsdienst) sowie über entsprechende Entwicklungen bzw. gemachte Erfahrungen im Bereich der Leitstellen anderer Ländern gegeben.

Insbesondere vor dem Hintergrund der für 2006 erwarteten Einführung des einheitlichen Digitalfunkes für Behörden und Organisationen mit Sicherheitsaufgaben (BOS) in Deutschland ergibt sich nicht nur ein elementarer Anpassungsdruck für den Bereich der Einsatzleitstellen, sondern auch die Chance für neue integrative Lösungen. Neben Albanien ist Deutschland das letzte europäische Land, das heute noch für den BOS-Bereich den veralteten Analogfunk nutzt.

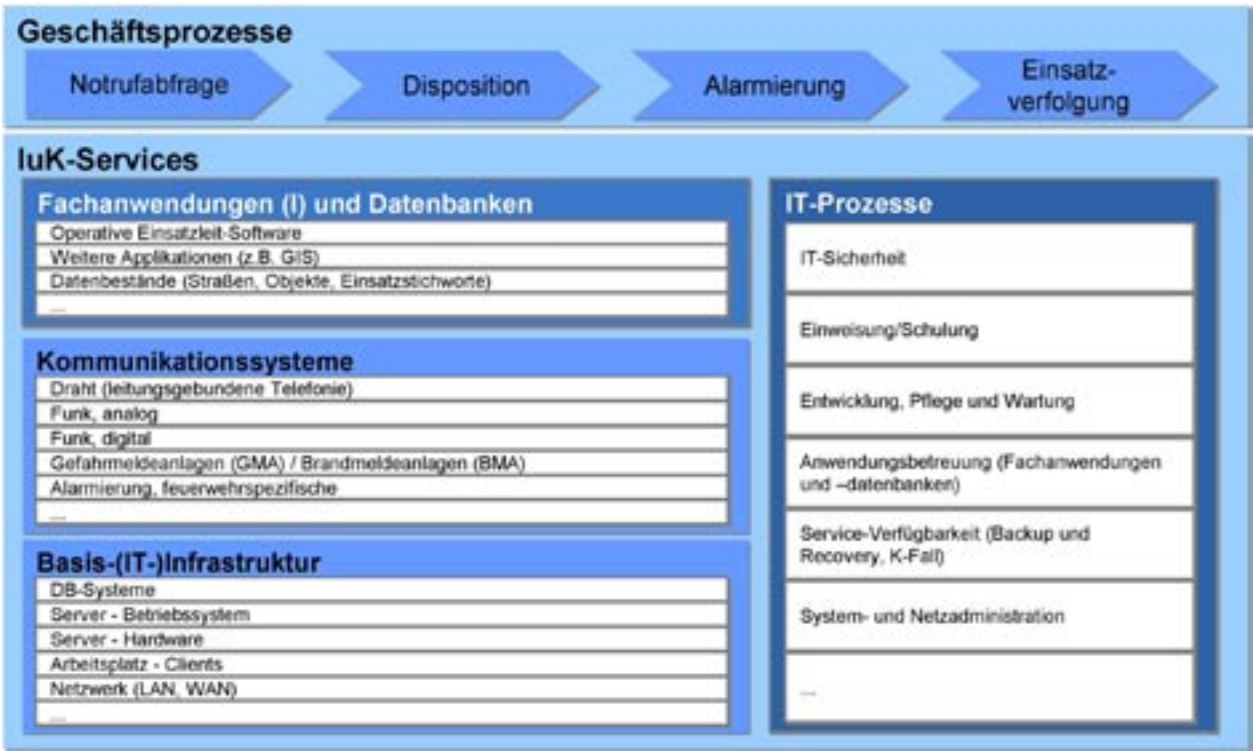
So sind aufgrund der technischen Innovation durch den BOS-Digitalfunk einerseits neue technische Schnittstellen unabdingbar, was bei jeder Leitstelle zu zum Teil erheblichen Investitionen führen wird. Andererseits ergibt sich dadurch auch ein Kostendruck, der vielleicht hilft, autarke organisatorische Lösungen zu vermeiden und im Sinne des Bürgers zu einer verbesserten Vernetzung oder gar Integration der Einsatzleitbereiche der verschiedenen Dienste führt. Erste Entwicklungen sind dadurch auch sichtbar, dass an vielen Stellen bereits die Einsatzleitzentralen von Feuerwehr und Rettungsdienst integriert sind.

2. Handlungsoptionen

In der Abbildung ist das grobe Modell einer Einsatzleitstelle dargestellt, wobei die beiden großen Blöcke „IuK-Services", d.h. Informations- und Kommunikationsdienste bzw. IuK-Systeme/-Lösungen, sowie der Bereich der „Geschäftsprozesse" zu unterscheiden sind. Es stellt sich somit die Frage, ob im Bereich der IuK-Services oder bei den Geschäftsprozessen gemeinsame Lösungen sinnvoll und wirtschaftlich sind.

Die in den Einsatzleitstellen von Polizei, Feuerwehr und Rettungsdienst ablaufenden Geschäftsprozesse Notrufabfrage, Alarmierung, Disposition und Einsatzverfolgung werden mit dem Ziel der Bereitstellung optimaler Dienstleistung bei kürzestmöglicher Reaktionszeit in besonders

Grobstruktur Einsatzleitstelle



starkem Maße durch Informations- und Kommunikationsdienste unterstützt.

Aufgrund der Relevanz der Geschäftsprozesse in der Einsatzleitung ist zur Erfüllung der damit einhergehenden hohen Anforderungen an die Verfügbarkeit der IuK-Services das Thema Ausfallsicherheit (Katastrophenfall Szenarien, redundante Systeme) bei Polizei und Feuerwehr besonders wichtig.

Trotz der heute eigenständigen Einsatzleitstellen und IuK-Bereiche von Polizei und Feuerwehr/Rettungsdienst gibt es bei der Bereitstellung der IuK-Services aufgrund der sehr ähnlichen Geschäftsprozesse deutliche Berührungspunkte und Gemeinsamkeiten.

Für eine erste Differenzierung lassen sich folgende Handlungsoptionen bezüglich einer verstärkten technischen und organisatorischen Integration der einzelnen Einsatzleitbereiche unterscheiden:

1. Gemeinsame Basistechnik für Polizei, Feuerwehr und Rettungsdienst in einer Region
2. Gemeinsame technische Infrastruktur einschließlich einem gemeinsamen Einsatzleitsystem
3. Gemeinsame Notrufannahme für Polizei, Feuerwehr und Rettungsdienst
4. Gemeinsame integrierte Leitstelle für Polizei, Feuerwehr und Rettungsdienst.

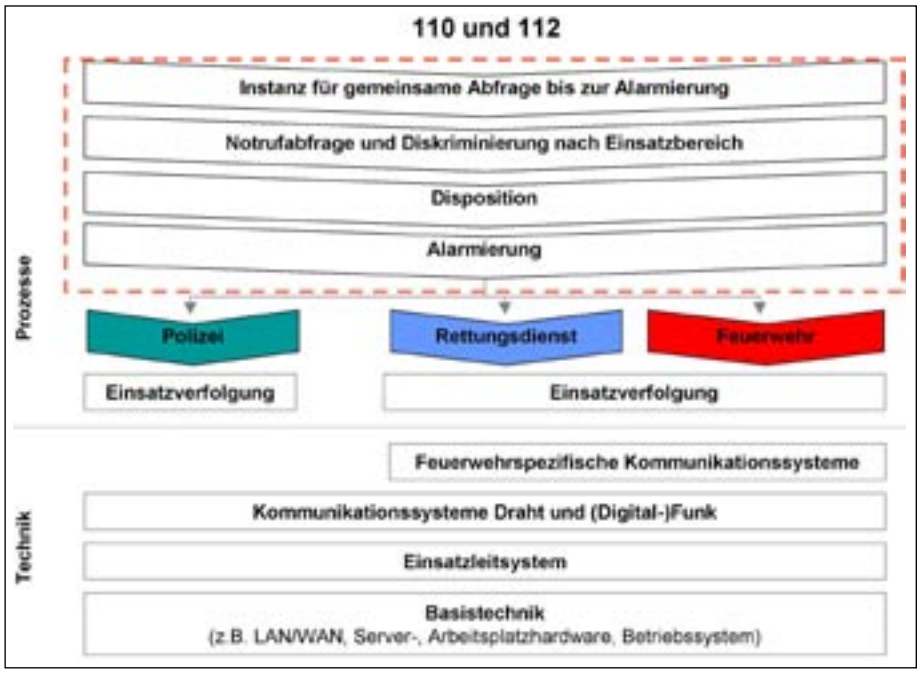
Aufgrund der Relevanz der Geschäftsprozesse in der Einsatzleitung ist zur Erfüllung der damit einhergehenden hohen Anforderungen an die Verfügbarkeit der IuK-Services das Thema Ausfallsicherheit (Katastrophenfall Szenarien, redundante Systeme) bei Polizei und Feuerwehr/Rettungsdienst besonders wichtig.

Die Handlungsoption „Gemeinsame Basistechnik“ fokussiert auf eine Konsolidierung und Vereinheitlichung aller Komponenten der Basis-IT-Infrastruktur und der zugehörigen IT-Prozesse, sowie auf die Einführung einer einheitlichen Digitalfunk-Technologie bei Polizei und Feuerwehr/Rettungsdienst sowie dem (im Rahmen dieses Beitrages nicht berücksichtigten) Katastrophenschutz. Auf Ebene der Fachanwendungen sind durch Polizei und Feuerwehr in eigenständigen Verfahren neue digitalfunkfähige Einsatzleitsystem-Anwendungen auszuwählen und einzuführen. Diese werden auf einer gemeinsamen Infrastruktur betrieben.

Die IT-Support Prozesse können durch die vereinheitlichte und gemeinsam genutzte IT-Infrastruktur vereinfacht werden. Die für Wartung und Betreuung der Basis-Infrastruktur vorgehaltenen Personalkräfte bzw. ggf. eingekauften Dienstleistungen Dritter können konsolidiert und beispielsweise auf einen Dienstleister übertragen werden. Der Support der Fachanwendungen verbleibt bei dem jeweiligen Systemlieferanten.

Die nächste Handlungsoption „Gemeinsame Technologie einschließlich Einsatzleitsystem“ erweitert das hier nur schematisch skizzierte Szenario. Ergänzend zur gemeinsamen Basistechnologie werden die gemeinsame Nutzung von Kommunikationstechnologie und der Einsatz gleicher Fachanwendungen (v.a. Einsatzleitsoftware) betrachtet. Das Einsatzleitsystem und Anwendungen in der Peripherie (z.B. GIS) werden gemeinsam genutzt. Daten werden konsolidiert und gemeinsam gepflegt. Applikationsbetreuung (z.B. Datenpflege, Parametrisierung) und Supportprozesse werden aus einer Hand geleistet. Aufgaben im Bereich des technischen Systemmanagements für den Digitalfunk werden durch eine Stelle zentral wahrgenommen.

Gemeinsame Leitstelle Polizei, Feuerwehr und Rettungsdienst



Auf diese Weise vereinfachen sich bei den IT-Prozessen der Einsatzleitzentralen zusätzlich die Applikationsbetreuung (Datenpflege) und die Supportprozesse (1st und 2nd Level). Die operativen Prozesse der Notrufbearbeitung in den Einsatzleitzentralen von Feuerwehr/ Rettungsdienst und Polizei bleiben bei diesem Szenario immer noch unverändert.

Die Handlungsoption einer gemeinsamen Notrufannahme orientiert sich am Modell der sogenannten „Call Taker“ in den Vereinigten Staaten. In diesem Modell werden alle über 110 und 112 eingehende Notrufe nicht mehr direkt in die Einsatzleitzentralen von Feuerwehr/ Rettungsdienst und Polizei durchgestellt, sondern laufen zunächst in einer rufdiskriminierenden Instanz auf.

Aufgabe der dort tätigen Mitarbeiter ist primär die Unterscheidung der Anrufe in:

1. Notrufe, die an die Polizei gerichtet sind
2. Notrufe, die an die Feuerwehr bzw. den Rettungsdienst gerichtet sind
3. Serviceanfragen von Bürgern ohne Notrufcharakter (z.B. Anfragen über Zuständigkeiten und Öffnungszeiten von Ämtern, Ortsauskünfte, Auskünfte über Verkehrsmittel)
4. Notrufmissbräuche

Zu diesem Zwecke werden die Anrufer primär nach dem Ziel ihres Notrufs (v.a. Feuerwehr, Rettungsdienst oder Polizei) gefragt. Die weitere Bearbeitung der Anrufe richtet sich nach der vorgenommenen Qualifizierung.

Dabei werden Notrufe, die für Feuerwehr/Rettungsdienst und Polizei bestimmt sind, so schnell wie möglich an die zuständige Einsatzleitzentrale weitergeleitet. In der Folge werden die dort eintreffenden Hilfegesuche wie bisher gehandhabt. Notrufabfrage, Disposition, Alarmierung und Einsatzverfolgung verlaufen in den gewohnten Prozessen. Im Rahmen der Notrufabfrage werden die Stammdaten des Notrufs erfasst und ggf. die bereits von der rufdiskrimierenden Schicht erfassten Daten verifiziert. Fehlverbindungen, Notrufmissbräuche und Serviceanfragen werden von dieser Stelle herausgefiltert. Serviceanfragen sollten möglichst fallabschließend beantwortet werden.

Die Option „Gemeinsame Leitstelle Feuerwehr/Rettungsdienst und Polizei“ beschreibt einen Lösungsansatz, bei dem sämtliche eingehenden Notrufe für Feuerwehr/Rettungsdienst, Rettungsdienst und Polizei aus einer Hand bis hin zur Alarmierung bearbeitet werden. Die Abbildung zeigt die prinzipielle Struktur dieses Modells. Lediglich die Einsatzüberwachung und -führung liegt weiterhin in den Händen von „Experten“ aus Feuerwehr, Polizei etc..

Eine gemeinsame Einsatzleitzentrale von Feuerwehr/ Rettungsdienst und Polizei bietet dem Bürger den Vorteil, alle Leistungen in Notfällen aus einer Hand zu erhalten. Unabhängig davon, welche Rufnummer gewählt wird, erhält der Hilfesuchende sofort (ohne Weitervermittlung) schnell und kompetent Hilfe. Die bisher üblichen Weitervermittlungen von Polizei zur Feuerwehr und in Gegenrichtung entfallen. Das Serviceangebot der Einsatzleitzentrale für den Bürger wird damit spürbar verbessert.

Von größter Bedeutung bei dieser Handlungsoption ist die Definition von hinreichenden und zugleich realistischen Anforderungen an die Qualifikation des Personals einer gemeinsamen Leitstelle. Eine solche Festlegung ist allerdings aufgrund der Kompetenzkämpfen zwischen den verschiedenen Diensten kurzfristig in der Regel nicht zu erwarten.

3. Typische Prozesse

Am Beispiel einer Feuerwehr-Einsatzleitzentrale werden typische Abläufe nachfolgend beschrieben.

Die Hauptaufgaben einer Einsatzleitzentrale besteht darin, Notrufe entgegenzunehmen, abzufragen und, wenn erforderlich, die geeigneten Kräfte der Feuerwehr und des Rettungsdienstes oder der Fachdienste zu alarmieren bzw. zu verständigen. Notrufabfrage, Disposition, Alarmierung und Einsatzunterstützung bzw. -lenkung

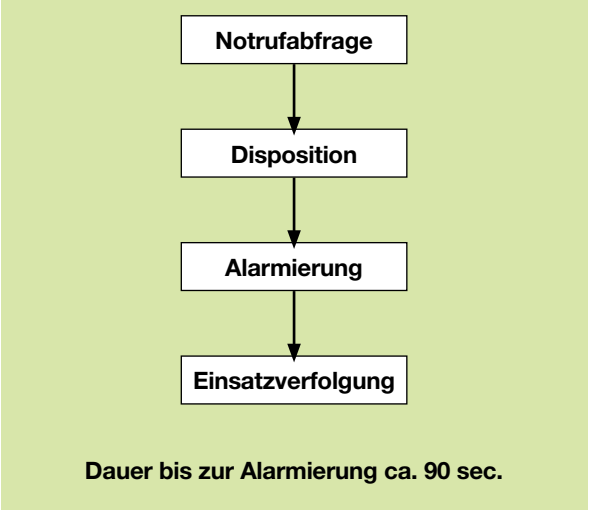


Abbildung 1: Ablauf Notrufbearbeitung

werden in der Einsatzleitzentrale in der Regel aus einer Hand bearbeitet. Sie folgen dem nachfolgend dargestellten Schema.

Notrufeingang und -abfrage

Im Normalfall wird ein Notruf über die bundesweite Feuerwehrnotrufnummer 112 abgesetzt. Eingehende Notrufe werden zumeist strukturiert nach einem weitgehend standardisierten Verfahren bearbeitet:

- Entgegennahme des Gesprächs/Begrüßung
- Strukturierte Abfrage:
  - Wer meldet?
  - Was ist passiert?
  - Wo ist der Einsatzort?
  - Wie viele Verletzte/Erkrankte?
  - Art der Verletzungen/Erkrankungen?
- Gesprächsabschluss
- Qualifikation des Notrufes/Einsatzes durch Vergabe des passenden Einsatzstichwortes (Grundschadensart, Erweiterung, Ergänzung)

Zu den üblicherweise vorhandenen Funktionalitäten eines Einsatzleitsystems zählen u.a.:

- Eingabehilfe für Einsatzart und Erweiterungen (automatische Ergänzung bei Eingabe von Alarmstichworten)
- Eingabehilfe für Einsatzort/Straße über Auswahlliste bzw. automatische Übernahme in Erfassungsformular (bei eindeutiger Angabe)
- Anzeige des Einsatzorts über grafisches Informationssystem
- Abgleich mit bereits existierenden Einsätzen bei identischen Einsatzorten (Straßennahmen) und räumlicher Nähe der Einsatzorte; Entscheidung, ob identischer oder neuer Einsatz vorliegt, ist vom Disponenten zu treffen
- Unterstützung der Disposition der Notarzteinsatzfahrzeuge über ein Fahrzeuglokalisierungssystem auf Grundlage von GPS

Die Bearbeitung von Notrufen genießt oberste Priorität. Fehlverbindungen oder eindeutige Rufmissbräuche werden daher, sofern nicht der Anrufende seinerseits das Gespräch abbricht, um die Rufleitungen für tatsächliche Notrufe nicht zu blockieren, schnellstmöglich durch die Disponenten beendet. Abhängig vom Inhalt der Anfrage und von der aktuellen Auslastung kann die Einsatzleitzentrale in Ausnahmefällen anrufende Bürger in Nicht-Notfällen beraten.

Die durchschnittliche Dauer einer Notrufabfrage beträgt dabei ca. 60 Sekunden.

Die wesentliche Leistung des Disponenten in der Notrufabfrage liegt in einer schnellen und sachgerechten Erhebung von Informationen und der anschließenden sachgerechten Qualifikation des Einsatzes durch Vergabe des entsprechenden Alarmstichwortes.

Gerade bei medizinischen Notfällen, die ca. 85 Prozent des Einsatzaufkommens ausmachen, ist die Zuordnung des geeigneten Rettungsmittels die zentrale Aufgabe des Disponenten. Dabei ist auf Grundlage der abgefragten Informationen zwischen den folgenden Alternativen zu unterscheiden:

- Kein medizinischer Notfall, ggf. Beratung erforderlich
- Kein medizinischer Notfall, Krankenbeförderung erforderlich
- Medizinischer Notfall, kassenärztlicher Bereitschaftsdienst
- Medizinischer Notfall, Rettungswagen
- Medizinischer Notfall, arztbesetztes Rettungsmittel

Gleichzeitig sollte jedem Meldenden der Eindruck vermittelt werden, dass ihm rasch und kompetent geholfen wird. In der Notrufabfrage sind daher neben der fachlichen Qualifikation rhetorische Fähigkeiten und Stresstoleranz ebenfalls von hoher Bedeutung.

Disposition

Wird aufgrund eines Notrufes ein Feuerwehr- bzw. Rettungsdiensteinsatz notwendig, werden die einsatzrelevanten Daten vom Disponenten in den Einsatzleitrechner eingegeben. Dies geschieht im Regelfall bereits während des Meldegespräches.

Unter Berücksichtigung der Örtlichkeit, des betroffenen Objektes, der Verfügbarkeit von Ressourcen und dem gewählten Einsatzstichwort (inkl. Ergänzungen) erhält der Disponent vom Einsatzleitsystem einen Einsatzmittelvorschlag. Dieser enthält die zuständigen Kräfte und die zu alarmierenden Fahrzeuge gemäß Alarm- und

Ausrückeordnung. Der Vorschlag ist vom Disponenten zu prüfen und kann anschließend angenommen oder geändert werden. Dabei können sowohl Fahrzeuge oder Einheiten ergänzt bzw. reduziert als auch alternative Kräfte benannt werden.

Bei unklaren Meldelagen wird zumeist nach dem Grundsatz verfahren, zunächst Kräfte zu alarmieren und auf den Weg zum Einsatzort zu schicken und bei Bedarf den Einsatz im Folgenden weiter zu qualifizieren und weitere Kräfte zu ergänzen oder zurückzubeordern.

Alarmierung

Kommt es zu einer Alarmierung, werden durch das Einsatzleitsystem die angeschlossenen Schnittstellensysteme angesteuert, über die die disponierten Kräfte die erforderlichen Einsatzinformationen erhalten.

Im Grundsatz läuft die Alarmierung nach dem folgenden Muster ab:

- Auslösung des Alarms durch das Einsatzleitsystem
- Ansteuerung der Alarmierungseinrichtungen (z.B. Wachalarm, Alarmdrucker, Alarmfaxe, digitale Meldeempfänger)
- Ausdruck von Alarmdrucken und -faxen auf entsprechenden Endgeräten
- Aussenden von FMS-Telegrammen an Fahrzeuge
- Auslösen der Alarmierungseinrichtungen (Durchsage- und Alarmierungssysteme)
- Anzeige der alarmierten Kräfte im Einsatzleitsystem und auf der Wartenwand
- Anstoß der Fristenüberwachung

Eine Erhebung der Zeit ergibt in der Regel, dass die Prozessschritte Notrufabfrage, Disposition und Alarmierung ca. zwei Minuten je Einsatz beanspruchen.

Einsatzführung

Da Feuerwehreinsätze im Regelfall vor Ort an der Einsatzstelle geführt werden, sind die ELS-Tätigkeiten im Rahmen der Einsatzführung und Kommunikation mit den Einsatzkräften begrenzt. Zu den wesentlichen einsatzbezogenen Aufgaben zählen:

- Überwachung von Fristen und Statusinformationen
- Funkkommunikation mit den Einsatzkräften
- Informationssammlung und -bereitstellung für Einsatzkräfte
- Nachalarmierung von Einsatzkräften
- Vorinformation an Krankenhäuser bei medizinischen Notfällen, Klärung von Verfügbarkeiten in der medizinischen Infrastruktur
- Rückmeldung zur Dokumentation

Abhängig vom Alarmstichwort ist – zumeist bei größeren Einsätzen – vom Disponenten eine durch das Einsatzleitsystem vorgelegte Maßnahmenliste abzuarbeiten. Nach dieser Liste sind z.B. dem Einsatzleiter Einsatzmittelergänzungen vorzuschlagen oder Benachrichtigungen durchzuführen. Benachrichtigungen gehen zum Beispiel an die Polizei, weitere Behörden, Versorgungsunternehmen, Objektbetreiber oder die Presse.

Erhält die Leitstelle neue Erkenntnisse zum Einsatzgeschehen werden diese sofort an den Einsatzleiter weitergeleitet, gegebenenfalls müssen weitere Einsatzkräfte alarmiert und/oder andere erforderliche Maßnahmen ergriffen werden. Dabei ist die Leitstelle bemüht, Informationen, die für die Einsatzkräfte wichtig sind, zu beschaffen. So werden z.B. bei Einsätzen mit Gefahrgut Hinweise aus entsprechenden Datenbanken abgefragt, oder es wird versucht, mit dem Hersteller des Stoffes in Kontakt zu treten, um dort Verhaltensmaßregeln im Umgang mit dem Stoff zu erfahren.

Weiterhin werden z.B. Wetterdaten an den Einsatzleiter weitergeleitet, um die Ausbreitung eventuell vorhandener Gefahrgutwolken besser einschätzen zu können. Nachrückende Kräfte werden von der Leitstelle eingewiesen oder ihnen wird ein Bereitstellungsraum zugeteilt.

Sonstige Aufgaben

Das Personal einer Feuerwehrleitstelle nimmt neben der Abwicklung von Einsätzen eine Reihe weiterer Aufgaben wahr. Dazu zählen unter anderem:

- Erstellen von Einsatzberichten und Einsatznachbearbeitung (zumeist durch Dienstgruppenleiter oder Lagedienstführer)
- Statistische Auswertung des Anruf- und Einsatzaufkommens
- Disposition der bundesweit verfügbaren Verbrennungsbetten
- Kapazitätsnachweis/Erfassen von Beschränkungen der Aufnahmekapazitäten der Kliniken der Stadt Hamburg
- Ausbildung der Reservedisponenten
- Persönliche Aus- und Fortbildung

4. Erfahrungen aus dem Ausland

4.1 Generelle Unterschiede

Die Organisation des Notrufwesens bzw. des Rettungsdienstes ist in allen Ländern historisch gewachsen. Die Unterschiede hinsichtlich der organisatorischen und infrastrukturellen sowie politischen Ausgestaltung der Infrastruktur sind zum Teil erheblich. Neben den politischen Rahmenbedingungen sind geographische, administrative und infrastrukturelle Umstände ein wesentlichen Faktor für Struktur und Organisation des Rettungswesens. Dabei ist die rettungsdienstliche Versorgung im Allgemeinen eine öffentliche bzw. staatliche Aufgabe.

Für die Gestaltung und Organisation der Einsatzleitzentralen gibt es keine „optimale Lösung", die alle Anforderungen erfüllt. Selbst in einzelnen Ländern wie z.B. Australien oder den USA werden verschiedene Modelle von Einsatzleitstellen betrieben. Während der Anrufer in einigen Ländern (z.B. Dänemark und Großbritannien) zunächst eine vorgeschaltete Abrufzentrale erreicht, die ihn dann an die entsprechende Koordinierungsstelle des spezifischen Dienstes (Polizei, Rettungsdienst, Feuerwehr) weitervermittelt, ist in anderen Ländern die Notrufannahme nach wie vor getrennt. Von daher gestalten sich auch die Anforderungen an die Leitstellendisponenten und damit die entsprechenden Qualifikationsanforderungen unterschiedlich. Bis auf wenige Ausnahmen sind aber Annahme- und Dispositionsbereich getrennt.

4.2 Europäische Harmonisierung

Die Weiterentwicklung der Einsatzleitbereiche in Europa wurde insbesondere durch den EU-Beschluss (Richtlinie 98/10/EC, Artikel 7.2) über die Einführung einer europaweit einheitlichen Notrufnummer gefördert. Grundsätzlich hat sich die EU im Vertrag von Amsterdam (1997) geeinigt, den Gesundheitsschutz der Bürger verstärkt zu berücksichtigen, jedoch die Organisation und Finanzierung der Gesundheitssysteme und damit auch der Rettungssysteme in der Kompetenz der einzelnen Mitgliedsländer zu belassen und hier weder eine Harmonisierung der Systeme noch der Politik vorzunehmen.

Alle EU-Staaten verfügen über Leitstellen bzw. Koordinationszentralen, die über eine landeseinheitliche Notrufnummer erreichbar sind. In den meisten europäischen Ländern werden unter der Notrufnummer 112 zumindest die Hilfeleistungen des Rettungsdienstes und der Feuerwehr, teils auch der Polizei vermittelt. Inzwischen haben eine Vielzahl der Mitgliedstaaten die 112 als einzige Notrufnummer eingeführt (z.B. Finnland, Portugal und Irland), unter der der Anrufer alle Hilfeleistungen erreicht.

4.3 Niederlande

Die niederländische Regierung forcierte die Neuorganisation des Notrufbereiches durch die gesetzliche Vorgabe (1996), dass bis Anfang 2004 die Anzahl der Leitstellen auf 25 reduziert werden muss. Grundlage hierfür ist das Zusammengehen von Polizei, Feuerwehr und Rettungsdienst in gemeinsamen Zentralen. Zum Startzeitpunkt gab es 100 Leitzentralen der verschiedenen Organisationen mit unterschiedlichen Grenzen. Es gab keinen direkten Zwang für die Organisationen diese Entwicklung mitzutragen, allerdings müssen die nicht-teilnehmenden Organisationen als „Gegner einer Standardisierung" für künftige Investitionen selbst aufkommen.

Ziel war es, eine bessere Kommunikation zwischen den Organisationen und durch eine Vereinheitlichung der Gebiete eine schnellere Handlungsfähigkeit zu erreichen. Die Schwierigkeiten bei diesem Prozess waren weniger technischer als organisatorischer Art.

Die verschiedenen Organisationen mussten mit ihren jeweiligen Wünschen und Vorstellungen berücksichtigt werden; aufgrund dieser Tatsache ist nicht jede Leitstelle in den Niederlanden gleich. Der größte Teil der Probleme beruhte auf den verschiedenen Kulturen und den „kleinen Königreichen", die erbittert verteidigt wurden.

In den meisten Regionen gibt es inzwischen gemeinsame Leitstellen (Tri-Service-Center), die von einem Gremium, in denen die drei integrierten Bereiche vertreten sind, geleitet werden, wobei jeder Bereich seinen eigenen Leiter hat. Im Vorfeld der gemeinsamen Leitstelle wurden verschiedenen Umorganisationen durchgeführt, bevor zuerst Rettungsdienst und Feuerwehr zusammengelegt wurden und letztendlich auch die Polizei integriert wurde.

4.4 Frankreich

Im Jahr 1996 führte Frankreich die 112 parallel zu den bereits existierenden Notrufnummern ein. Dabei wird die gemeinsame europäische Notrufnummer zu einer Leitstelle je Departement geleitet (in 2/3 der Bereiche zur Feuerwehr ansonsten in die Rettungsleitstelle). Nach und nach sollen die derzeit bestehenden Parallelnummern verschwinden und die Notrufannahmestellen zusammengeführt werden.

In gemeinsamen Arbeitsgruppen werden die Arbeitsabläufe abgestimmt und Möglichkeiten besprochen, eine integrierte Leitstelle mit der entsprechenden Infrastruktur (auch Einsatzleitsystem) zu nutzen. Wobei auch hier eine Unterteilung in Annahme- und Dispositionsbereich erfolgt. Sukzessive werden in den einzelnen Departements

integrierte Leitstellen in neuen Lokationen geschaffen, wobei in einem ersten Schritt die Einsatzzentralen mit ihren Mitarbeitern von Rettungsdienst und Feuerwehr zusammengelegt werden bevor die Integration der Polizeieinsatzzentrale folgt.

4.5 Dänemark

In Dänemark koordinieren insgesamt 11 Leitstellen die landesweite Notrufannahme und organisieren die Rettungsressourcen. Bis auf eine Leitstelle, die von der Kopenhagener Feuerwehr betrieben wird, werden alle Leitstellen von dem dänischen Unternehmen Falck Rettungsdienst als Gesamtdienstleister unterhalten. Das Unternehmen ist Teil des dänischen Konzerns Group 4 Falck, einem der größten Privatunternehmen der Welt im Bereich des Sicherheits-, Feuerwehr- und Rettungsdienstes.

Der dänische Kreistagsverband hat mit dem Unternehmen einen Rahmenvertrag geschlossen, der die allgemeinen Bedingungen und Service- sowie Qualitätsverpflichtungen zusammen mit der Preisliste und -regulierung festlegt. Die jeweiligen Hilfsfristen bzw. Eintreffzeiten sind in Einzelverträgen mit den 14 dänischen Kreisen geregelt.

Allein Kopenhagen hat einen Vertrag mit der Kopenhagener Feuerwehr über den Krankentransport, die Notfallrettung und damit auch den Betrieb einer zentralen Leitstelle abgeschlossen. Diese Leitstelle nimmt alle 112-Anrufe entgegen und fungiert sozusagen als „first point of contact". Bei Meldungen für die Leitstellen der Polizei oder des Rettungsdienstes werden entweder die Daten/Details elektronisch gesendet oder wenn es notwendig ist, wird der Anrufer weiterverbunden. Die Leitstelle ist mit erfahrenen Feuerwehrmitarbeitern besetzt. Grundsätzlich müssen auch die operativen Kräfte regelmäßig 1-monatige Praktika in der Leitstelle absolvieren.

In den von Falck betriebenen Alarmierungszentren spricht der Anrufer mit einem Control Center Operator, der auf Grundlage der erhaltenen Informationen die notwendigen Einsatzmittel disponiert oder die Informationen bzw. den Anrufer an die Polizeileitstellen weiterleitet. Da der Großteil der Leitstellenmitarbeiter bei Falck keine Feuer- oder Rettungsdiensterfahrung hat, arbeiten sie mit einem hochentwickeltem Einsatzleitsystem, dass umfangreiche Unterstützung und Führung bietet.

4.6 Finnland

In Finnland ist die Reformierung der Leitstellen weit fortgeschritten. Dabei ist eine Reduzierung der Anzahl der Leitstellen (Reduzierung bis 2006 auf mindestens 13) verbunden mit einer Vereinheitlichung über eine Zusammenlegung der Leitstellen von Feuerwehr, Rettungsdienst und Polizei das Ziel. Darüber hinaus soll die einheitliche Notrufnummer 112 vollständig eingeführt werden. Um diese integrierten Leitstellen (Emergency Response Centre) aufbauen zu können, werden Zuständigkeitsbereiche vergrößert und angeglichen, bevor die verschiedenen Dienstleister integriert werden. Dabei sollen diese Leitstellen (zukünftig) mit einheitlichen IT-Systemen ausgestattet sein.

Die Notrufe werden von derzeit noch von Annahmebeamten und Disponenten der jeweiligen Dienstleister bearbeitet. Schrittweise sollen aber die „Beamten" der Dienstleister durch eigens für die Leitstellen ausgebildete Mitarbeiter ersetzt werden. Ziel ist es, die zukünftigen 112-Mitarbeiter für die neuen Anforderungen durch entsprechende Ausbildung zu qualifizieren, damit sie in der Lage sind, Anrufannahme und Disposition für die unterschiedlichen Dienstleistungsbereiche (Feuerwehr, Rettungsdienst und Polizei) durchzuführen und die vollständige Ereigniskette in der Leitstelle zu begleiten. Das Training umfasst derzeit 57 Wochen, wobei ein Supervisor als Vorgesetzter weitere 10 Wochen Schulung benötigt. Dieser Zeitraum ist in drei Bereiche unterteilt, die sukzessive durchlaufen werden müssen, um für den Dienst in einer Leitstelle ausgebildet zu sein:

- Allgemeiner Part (Leitstelle, medizinische Priorisierung)
- Besuch des Emergency College
- Besuch der Polizei-Akademie

4.7 Österreich und Schweiz

In der Schweiz und in Österreich gibt es unterschiedliche Organisationsformen der Leitstellen entsprechend der jeweiligen gesetzlichen Regelungen des Kantons bzw. des Bundeslandes. Eine übergreifende Struktur existiert nur in soweit, als die Anbieter von Rettungsdiensten in bundesweiten Dachverbänden organisiert sind. Dabei ist das Rettungswesen in Österreich organisatorisch deutlich von der Feuerwehr getrennt.

Im Gegensatz zu Österreich gibt es in der Schweiz bereits integrierte Leitstellen, in denen Feuerwehr und Rettungsdienst gemeinsam arbeiten. Im Allgemeinen sind die Einsatzzentralen der Polizei getrennt von den Rettungsleitstellen und arbeiten nur eng mit diesen zusammen.

Tendenziell wird in der Schweiz auch verstärkt die Integration der Polizei in gemeinsame Leitstellen angestrebt, wobei in St. Gallen bereits eine gemeinsame Leitstelle von Feuerwehr, Polizei und Rettungsdienst realisiert ist.

4.8 Kanada

In Kanada werden vor allem im Bereich der Städte wie z.B. Toronto und Vancouver integrierte Leitstellen geschaffen, wobei sich die Integration häufig auf die gemeinsame Rufannahme beschränkt, während die Disposition weiterhin von den jeweiligen Organisationen durchgeführt wird.

So wird die Leitstelle für den Distrikt Vancouver durch E-Comm (Emergency Communications for South Western British Columbia Incorporated), eine non-profit Gesellschaft betrieben, in der alle Notrufe des Distriktes auflaufen. Die Mitarbeiter der Leitstelle sind Angestellte der Gesellschaft, obgleich sichergestellt ist, dass von Feuerwehr und Rettungsdienst jeweils ein Mitarbeiter (Uniformed Resource Officer) anwesend ist.

Im Falle eines Notrufes wird vom E-Comm-Mitarbeiter die Art des Notfalls bestimmt. Da nicht alle im Zuständigkeitsbereich liegenden Leitstellen E-Comm Zuständigkeiten übertragen haben, wird entweder der Notruf an die entsprechende Leitstelle weitergeleitet, oder es werden durch den Call Taker die notwendigen Informationen abgefragt, in das Einsatzleitsystem eingegeben und zur Disposition weitergeleitet.

Langfristig sollen alle Organisationen mit dem gleichen Einsatzleitsystem arbeiten, so dass über die Call Taker alle eingehenden Notrufe für Polizei, Feuerwehr und Rettungsdienst angenommen und die Informationen in das System als Grundlage für die Arbeit der Disponenten eingegeben werden können. Die Disposition soll aber weiterhin von Mitarbeitern der entsprechenden Organisationen durchgeführt werden.

In Toronto betreibt die Polizei eine Leitstelle (Toronto Police Services), die die Notrufannahme für Polizei, Feuerwehr und Rettungsdienst übernimmt. Allerdings erfolgt nur die Disposition der Polizeieinsätze in dieser Zentrale durch entsprechende Mitarbeiter, während der Rettungsdienst und die Feuerwehr jeweils eine eigene Leitstelle für die Disposition führen; d.h., dass die angenommenen Rettungseinsätze mit den Informationen entsprechend weitergeleitet werden.

Die Beschäftigten der Einsatzleitzentrale der Polizei sind sowohl Polizeibeamte als auch Zivilisten, die für den Dienst als Call Taker und Disponent trainiert wurden. Dabei obliegt die Leitung der Einsatzzentrale und der jeweiligen Schichten Polizisten. Da die zivilen Mitarbeiter nicht für alle möglichen Dispositionen genügend Erfahrung haben, ist sichergestellt, dass in jeder Schicht auch Polizeibeamte Dienst tun.

4.9 USA

Grundsätzlich ist die Bereitstellung von Notdiensten wie in allen föderalen Staaten auch in den Vereinigten Staaten unterschiedlich organisiert und hängt stark von den lokalen Gegebenheiten ab. In ländlichen Gebieten sind Rettungsdienst und Feuerwehr häufig auf freiwilliger Basis organisiert bzw. zunehmend an kommerzielle Anbieter vergeben. Dagegen gibt es in den Städten schon länger Tendenzen zur Integration der Dienste. Im Allgemeinen ist die Rufannahme in einem Kommunikationszentrum (Public Safety Answering Point) zusammengefasst, so dass der Bürger über eine Notrufnummer alle Notdienste erreicht. Die in einem derartigen Zentrum angestellten Mitarbeiter müssen eine entsprechende Ausbildung zum Dispatcher an einer 911-Schule absolviert haben. Darüber hinaus müssen Disponenten für den Rettungsdienst in einem Großteil der Staaten noch eine zusätzliche Zertifizierung (Emergency Medical Dispatching) nachweisen. Bekanntestes Beispiel aus den Vereinigten Staaten dürfte die Organisation des Notrufdienstes in Chicago sein, das nachfolgend näher erläutert wird.

Im Jahr 1995 wurde das Chicago Emergency Communications Centre in Betrieb genommen, in das die Notrufannahme und Disposition für Polizei, Rettungsdienst und Feuerwehr integriert sind, obgleich jede Organisation ihre spezifischen Vorgehensweisen beibehalten hat. Geleitet wird die Einrichtung durch den zuständigen Polizeibeamten.

Eingehende Notrufe werden von einem Call Taker angenommen, der für die Weiterleitung an die jeweils zuständige Organisation vornimmt und die Fehlanrufe abfängt. Der eingegangene Notruf wird an den entsprechenden Disponenten (Dispatcher) weitergeleitet.

Der Disponent erhebt die benötigten Informationen und erfasst sie computerunterstützt, wobei dies im Rettungsdienst mithilfe eines standardisierten Abfrageprotokolls (Advanced Medical Priority Dispatch System) geschieht. Nach Erhebung der Informationen werden die benötigten Einsatzkräfte alarmiert. U.U. werden bereits erste Verhaltens- und Maßnahmenhinweise an den Notrufenden gegeben. Dabei sind sowohl die notwendigen Fragen als auch die entsprechenden Verhaltenshinweise auf dem Bildschirm des Disponenten sichtbar. Je zwei Disponenten werden durch einen Supervisor, der in kritischen

Situationen eingreifen bzw. unterstützen kann bei der Notrufbearbeitung beaufsichtigt. Daneben gibt es noch Einsatzbetreuer für Feuerwehreinsätze und Mitarbeiter für die Koordination der Rettungsfahrzeuge.

Diese vorgeschaltete Notrufannahme stellt eine bessere Verfolgung der Notrufe für Polizei, Feuerwehr und Rettungsdienst sicher und verkürzt die Antwortzeit der Dienste. Darüber hinaus ermöglicht sie ein besseres Management und Analyse der Notrufdaten. Die Call Taker sind gut ausgebildete zivile Angestellte, während die Disponenten Mitarbeiter der jeweiligen Organisation sind.

5. Erfolgsfaktoren und Ausblick

Es gibt eine Tendenz zu integrierten Leitstellen mit einer gemeinsamen Notrufannahme und einer sich daran anschließenden Disposition, obgleich spezifische Prozesse der Dienstleister häufig in den Händen der jeweiligen Mitarbeiter verblieben sind. Die Wahrnehmung von Notrufannahme und Disposition in Personalunion ist – mit Ausnahme des finnischen Modells – nicht üblich.

Von derartigen Zusammenlegungen werden Vorteile erwartet, wie z.B.:

- Ein Zugang für den Bürger zu den Notfalldienstleistern
- Einsparungen bei der Einführung neuer Technologien in der Leitstelle
- Rationalisierungen bei der Anrufannahme
- Bessere Koordination und Ressourcenverteilung der Dienstleister
- Umfassendere Möglichkeiten für die Entwicklung von (Notfall)Strategien und Diensten durch die übergeordneten Behörden
- Modernisierung der Dienstleistungen der Behörden für den Bürger
- Bessere Reaktionsmöglichkeiten auf steigende Dienst- bzw. Ressourcennutzung

Ausgehend von den Erfahrungen in den anderen Ländern kann man feststellen, dass es ähnliche Widerstände bzw. Hindernisse bei derartigen Integrationen gibt. Grundsätzlich liegen diese weniger im technischen als im kulturellen und organisatorischen Umfeld bzw. der Besitzstandswahrung. So gibt es häufig Unterschiede bei der Entlohnung und den Arbeitsbedingungen zwischen den verschiedenen Organisationen. Auch sind die Prozeduren bzw. Prozesse im Annahme- und Dispositionsbereich von Feuerwehr und Rettungsdienst strukturierter und eignen sich daher besser für eine Automatisierung als die der Polizei, die durch die Verschiedenheit ihrer Aufgaben eine weniger standardisierbare als „frei fließende“ Erledigung der Aufgaben hat. Oftmals haben vor allem Organisationen der Feuerwehr Widerstand gegen eine mögliche Integration geleistet.

Grundvoraussetzung für eine erfolgreiche Umsetzung eines derartigen Projektes ist ein intensives Marketing, um die Akzeptanz der Organisationen zu erreichen. Um den verschiedenen Interessenlagen und den daraus folgenden Argumenten etwas entgegensetzen zu können, ist es notwendig die Eigeninteressen der Dienstleister mit ihren Bestrebungen zur Besitzstandswahrung und dem Erhalt ihrer Traditionen und Routinen zu identifizieren und die Unsicherheit und daraus folgende Ablehnung der Mitarbeiter gegen Veränderungen zu berücksichtigen. Nur mit der Unterstützung der Mitarbeiter aller Organisationen kann ein derartiges Integrationsprojekt erfolgreich umgesetzt werden.

Allerdings sind die Erfahrungen aus anderen Staaten grundsätzlich nicht einfach auf die deutschen Verhältnisse übertragbar. Die Organisation des Notrufwesens und der damit verbunden Dienste bzw. Organisationen hängen stark von den jeweiligen historischen und politischen Rahmbedingungen ab. Zusätzlich spielen noch geographische (z.B. Flächenstaat), administrative und infrastrukturelle (z.B. Bevölkerungsdichte) Faktoren eine wesentliche Rolle.

Die Kosten für die Leitstellen aus den einzelnen Staaten sind bislang keiner vergleichenden Betrachtung zugänglich. Dies liegt zum einen an den erheblichen Unterschieden in der organisatorischen und infrastrukturellen Ausgestaltung der Dienste und der damit verbundenen häufigen Einbindung in andere Systeme und zum anderen an den häufig nicht separat ausgewiesenen bzw. erfassten Kosten.

Literaturverzeichnis

1. Baumann, André-Michael, Die Bedeutung des Meldegesprächs bei der präklinischen Versorgung Schwerverletzter im Rettungsdienst, Berlin 2002
2. Bayerisches Staatsministerium des Innern, Einheitliche Notrufnummer 112 für Feuerwehr und Rettungsdienst in Bayern. Erarbeitung landesweiter Standards für die Errichtung von Integrierten Leitstellen in Bayern. Ergebnisbericht, o.O. 2001
3. Institut für Rettungsdienst des Deutschen Roten Kreuzes (Hg.) Workshop Maria Laach. Leitstelle III. Qualitätsmanagement – Kostenrechnung – Qualifikation, Nottuln 2000
4. Rapp, Günter in „Brand – Die Feuerwehren der Welt", Chronik 8, Moderne Notfallkommunikation Leitstellen heute und morgen, 2000
5. Swedish Rescue Services Agency Fire & Rescue Services Department, Report from Workshop on Effective Handling of Emergency Calls 8-9 March 2002 Rosersberg, Sweden, o.O. 2002
6. Vergeiner, Gernot (Hg.), Leitstellen im Rettungsdienst. Aufgaben – Organisation -Technik, Edewecht, Wien 1999
7. Worrall, Stephen G., Bursary Report 2001.An International Study of Culture in Combined Control, o.O. 2002

Prof. Dr. Walter Gora
Valora Management Group GmbH

Öffentliche Risikovorsorge und gesellschaftliche Sicherheitsbedürfnisse als Gegenstand der Politik

Prof. Dr. Klaus Lenk, Universität Oldenburg und Hochschulkolleg eGovernment der Alcatel SEL Stiftung für Kommunikationsforschung

Vom Titel dieses Vortrags fühlen sich Kommunalpolitiker wahrscheinlich nicht angesprochen. Wir haben es uns angewöhnt, Sicherheitspolitik als Angelegenheit von übergeordneten staatlichen Instanzen und von supranationalen Verteidigungsbündnissen zu sehen. Das wachsende Bedrohungsgefühl und die Einsicht, dass innere und äußere Sicherheit nicht mehr scharf zu trennen sind, haben daran noch nichts geändert. Aber die häufiger werdenden Naturkatastrophen und der internationale Terrorismus wirken sich lokal aus, ebenso wie Alltagskriminalität, Verkehrsunfälle und Feuersbrünste. Die lokale Risikovorsorge ist davon noch nicht sehr beeindruckt. In ihrer Gesamtheit wird sie nicht politisch verantwortet. Sie geschieht spartenweise aus der Sicht der beteiligten Professionen: Notfallmedizin, Feuerwehr, Polizei. Im politischen System „Kommune" findet sie noch keine Ansprechpartner, die eine Gesamtsicht einfordern. Mehr als andere Politikbereiche ist Sicherheit durch reaktives Handeln an Stelle von vorausschauender Planung und Programmatik gekennzeichnet,. Zudem konnte die kommunale Ebene bislang im Windschatten staatlicher Vorkehrungen sich solche Bereiche heraussuchen, in denen lokale Kräfte (z.B. die innerstädtische Kaufmannschaft) besondere Anforderungen stellen, die man politisch nicht ignoriert werden können.

Das heißt nicht, dass darüber hinaus nichts geschieht. Es wird auch auf örtlicher Ebene schwerer, die wachsenden Risiken nicht politisch wahrzunehmen. Aber die Reaktionen sind oft sehr kurz gegriffen. Den Risiken und auch dem in der Bevölkerung zunehmenden Gefühl der Bedrohung begegnet man nicht durch gründliche Analyse und programmatisches Handeln. Vielmehr greift man gern zu neuen technischen Mitteln, kurzfristig Entlastung versprechen. Videoüberwachung von öffentlichen Räumen ist ein markantes Beispiel. Der Einsatz solcher Techniken erfolgt weithin ungeplant, auf Grund vager Vermutungen über ihre Nützlichkeit. Dieser Einsatz, insbesondere von Beobachtungstechniken im städtischen Raum, ist zudem nicht folgenlos. Er hat selbst wiederum Auswirkungen auf das Verhalten der Beobachteten und darüber hinaus auf die Art und Weise, wie Menschen im städtischen Raum miteinander umgehen.

Mit der Fixierung auf technische Lösungen stehen sich Nutzenerwartungen und Risikovermutungen in der Wahrnehmung gegenüber. Politisch wird dieser Gegensatz intensiv verhandelt. Es geht um das Für und Wider bestimmter Maßnahmen, und damit nur indirekt um die Gründe, die dazu führten, dass Maßnahmen wie Videoüberwachung ergriffen werden. Dies kann man wohl kaum als Sicherheitspolitik bezeichnen. Vielmehr schaukeln sich zwei gegensätzliche Perspektiven auf. Bürgerrechtler fürchten staatliche, insbesondere polizeiliche Übergriffe und versuchen sie abzuwehren. Jede Erweiterung des Handlungsarsenals der Polizei oder des Katastrophenschutzes, die am Horizont auftaucht, wird kritisch untersucht. Auf der anderen Seite suchen die Institutionen herauszufinden, was man mit neuen Techniken machen kann. Am Beispiel der Videoüberwachung öffentlicher Plätze lässt sich das gut studieren. Von Seiten der Behörden und Organisationen mit Sicherheitsaufgaben (BOS) weist man oft gar nicht auf den realen Nutzen solcher Vorkehrungen hin, sondern versucht nur, die bürgerrechtliche Kritik zu beschwichtigen. Das weckt auf der anderen Seite wiederum den Verdacht, im Hintergrund werde doch viel mehr geplant als zugegeben wird.

In beiden Perspektiven werden die technischen Möglichkeiten überschätzt. Man hält das Instrumentarium für effektiver und damit auch für bedrohlicher, als es tatsächlich ist. Das eigentliche Diskussionsfeld einer Sicherheitspolitik, die mit effektiven Maßnahmen auf Bedrohungen reagieren will, wird damit nicht erreicht. Vernachlässigt wird die Einbettung der Technik in die Alltagrealität. Damit technische Neuerungen tatsächlich zu Innovationen in organisatorischer und gesellschaftlicher Hinsicht führen, kommt es darauf an, dass sich Verhalten, Prozesse, Strukturen verändern. Nicht die technische Innovation, *sondern die technisch ermöglichte Praxis-Innovation* ist der entscheidende Umstand.

Wenngleich es noch keine explizite städtische Sicherheitspolitik gibt, so hat sich doch Einiges geändert gegenüber der nicht allzu lange zurückliegenden Zeit, als die Kommunen Sicherheitsfragen – vom Straßenverkehr abgesehen – wenig Beachtung schenkten. Ein kürzlich gehaltener Vortrag trug den Titel „Sicherheitstechniken und neue urbane Sicherheitsregimes". Angesprochen wurde in dem Vortrag vor allem die immer weiter anwachsende Menge von Daten, die mit dem Einsatz neuer technischer Mittel zur Beobachtung von Menschen verfügbar wird, durch Videoüberwachung, Zugangskontrollen, Internetnutzung. Ein „Regime" entsteht aus dem Zusammenwirken vieler Akteure mit ihren Strategien. Es hat politische Bedeutung, ist aber nicht gleichzusetzen mit bewusst

gestalteter und verantworteter Politik. Damit wird der gegenwärtige Praxisstand widergespiegelt, wie er sich auch aus der Zusammenschau der Beiträge dieser Tagung ergibt.

Wie lässt sich erreichen, dass eine vorsorgende Sicherheitspolitik auf örtlicher Ebene entsteht, die im Rahmen der staatlichen und internationalen Vorgaben den Schutzbedürfnissen der Bürger gerecht wird und Risikovorsorge betreibt? Wir betrachten zunächst einige Hindernisse, bestimmen dann Gegenstand, Ziele und Instrumente einer solchen Politik und fragen zum Schluss, wie sie am besten etabliert werden kann.

Was hindert eine kommunale Sicherheitspolitik am Entstehen?

Was sind die Gründe dafür, dass Sicherheitspolitik auf kommunaler Ebene immer noch ein Schattendasein fristet? Mindestens vier Umstände sind zu nennen:

- Die schon angesprochene Technikfixierung
- Das Aufrechterhalten von Illusionen
- Gewachsene Organisationsstrukturen, welche Innovationen abwehren oder zumindest erschweren.

Die punktuelle Nutzung technischer Mittel, die angeblich Sicherheit gewährleisten, hat damit zum tun, dass immer wieder Interessenten auf den Plan treten, die solche technischen Mittel anbieten. Sie suggerieren, dass damit die von der Praxis vermuteten, aber selten genau analysierten Probleme gelöst werden können. Wenn Besorgnis über einen Missstand akut wird, sind schnell Lösungsanbieter zur Stelle, die eine gerade fertige oder halbfertige Technikanwendung als Problemlösung darstellen und behaupten, mit ihr seien alle Probleme gelöst. Ein Beispiel für diese kurzschlüssige Argumentationskette liefert die Personenidentifikation. Hier werden gegenwärtig Biometriepässe als eine Lösung gehandelt, mit der alle Probleme beseitigt werden könnten. Es scheint so, als ob manche Technikanwendungen geradezu darauf warten, dass die in der Praxis auftauchenden Probleme so definiert werden, dass der Einsatz fertiger technischer Konzepte als sinnvolle Lösung erscheint.

Die Lösungsanbieter und die Führungsspitzen in Politik und Verwaltung bestätigen sich dabei oft gegenseitig in einer gravierend verkürzten Problemsicht. Beide laufen Gefahr, die tatsächliche Arbeit sowie die Kommunikationsbeziehungen, die es umzugestalten gilt, zu vernachlässigen, weil sie diese nicht (oder nicht mehr) genau kennen. Die Faszination technischer Neuerungen lässt die Notwendigkeit ihrer Einbettung in eine organisch gewachsene Handlungspraxis übersehen. Beispiel: Die Kommunikation in Angsträumen wie z.B. U-Bahn-Eingängen kann nicht allein durch technische Mittel verbessert werden, wenn hinter der Technik kein glaubhaftes Interventionspotenzial steht.

Die Ausblendung der gesellschaftlichen und arbeitsorganisatorischen Realität im Zusammenwirken von Technikverkäufern mit politischem Spitzenpersonal ist auch eine der Ursachen dafür, dass viele technische Großprojekte scheitern oder zu ungeahnten Kostenexplosionen führen. Auf kommunaler Ebene setzt sich also nur fort, was gängige Praxis ist. Die Frage wird gar nicht erst gestellt, wie technische Systeme in organisatorische Strukturen und Praktiken sowie in ein gesellschaftliches Umfeld einzubetten sind, damit sie wirksam werden. Solange sich das nicht ändert, solange der Glaube an die technische Lösungskompetenz der Anbieter ungebrochen ist und die Einbettung der technischen Mittel in die Alltagswelt nicht bedacht wird, ist eine Sicherheitspolitik aus einem Guss erschwert, nicht nur lokal, sondern auch auf Landes- und Bundesebene.

Aufrechterhalten von Sicherheitsillusionen: Sicherheit ist kein populäres Thema. Sicherheitspolitik ist politisch nicht sehr attraktiv, wenn es um die ständigen politischen Spiele um Stimmengewinn geht. Denn sie muss von einem unvoreingenommenen Blick auf das wachsende Risikopotenzial unserer gesellschaftlichen Zusammenhänge getragen sein, das man sich selbst ungern eingesteht. Ein vorausschauender, strategischer Ansatz zu einer Politik der Risikovorsorge auf kommunaler Ebene erfordert zunächst das Eingeständnis, dass Risiken unbekannten Zuschnitts existieren. Nicht nur in der Kommunikation mit der Öffentlichkeit, auch gegenüber sich selbst verdrängen Politiker diese Einsicht. Das mag lange Zeit gut gehen. Handlungsdruck ergibt sich meist erst dann, wenn etwas schief gelaufen ist. Mit Vorbeugung kann man sich schlecht politisch profilieren, und das Eingeständnis der Probleme kommt einem Schlechtreden des eigenen Standorts gleich. Zudem kann es Gefühle der Unsicherheit in der Bevölkerung wecken.

Gewachsene Organisationsstrukturen: Ein weiteres Hindernis kommt hinzu. Als „Newcomer" hat die nunmehr entstehende kommunale Sicherheitspolitik keine Anker im politischen Geschäft und in der Verwaltung. Es fehlen Anknüpfungspunkte in der Verwaltungsgliederung und in der politischen Organisation auf kommunaler Ebene. Das legt es nahe, sie mit der Umweltpolitik zu vergleichen, die sich vor rund zwei Jahrzehnten ebenfalls in der kommunalen Praxis erst ihren Platz schaffen musste.

So wie damals die Umweltpolitik ist Sicherheitspolitik heute dadurch behindert, dass sie Fachgrenzen überschreiten muss. Sie überschneidet sich notwendig mit zahlreichen schon lange verfestigten Fachpolitiken. Auf Zuständigkeiten darf sie dabei keine Rücksicht nehmen. Weder Institutionen wie die Polizei noch deren Aufgabenbereiche dürfen ausgeklammert werden, auch wenn die Kommune nicht oder nur am Rande zuständig ist. Auch insofern bietet sich der Vergleich mit der Umweltpolitik an. Wie die Umweltpolitik muss die Sicherheitspolitik von einem ganzheitlichen Ansatz geprägt sein, der Institutionen und Verwaltungsebenen überschreitet und dabei die verschiedenen professionellen Sichten integriert. Im Falle der Sicherheitspolitik trifft eine große Zahl unterschiedlicher professioneller Sichten zusammen. Ihre Träger sind in vielen öffentlichen und gemeinnützigen Institutionen organisiert, von der Polizei über Schulbildung und Sozialarbeit bis hin zu Feuerwehr, Rettungsdiensten und Notfallmedizin.

Gegenstand und Ziele kommunalen Sicherheitspolitik

Der Ausdruck „Sicherheitspolitik" wird auch dort, wo man die Trennung zwischen innerer und äußerer Sicherheit aufgegeben hat, nicht bezogen auf die Sicherheit im kommunalen Alltag. Und auch im Hinblick auf „Großlagen" und Katastrophen finden sich keine Stimmen, welche die Rolle der kommunalen Ebene hervorheben. Im folgenden soll zwischen der alltäglichen Sicherheit und Ausnahmezuständen nicht getrennt werden. Eine Politik des „Policing" würde sich nur auf Ersteres beziehen, eine Politik der Krisenbewältigung auf Letzteres.

Auszugehen ist von der im Katastrophenschutz üblichen Einteilung in Preparedness, Mitigation, Response und Recovery. Diese Einteilung trifft auch bei der Gewährleistung von „Alltagssicherheit" zu, obwohl sie dort wegen des Ineinandergreifens der Phasen und der bislang gegebenen organisatorischen Konzentration auf die Polizei nicht getroffen wird. Geht man zunächst von (möglichen) Katastrophen und Großschadensereignissen aus, dann hat kommunale Sicherheitspolitik mit allen vier Stadien zu tun. So geht es um das Vorbereitetsein auf akute Gefahrenlagen und Katastrophen wie auch um das Handeln in solchen Lagen (Response), einschließlich des dann erforderlichen Krisenmanagements. Es geht zudem um die Prävention bzw. Abmilderung (Mitigation) möglicher Folgen von Risiken, Großschadenslagen und Katastrophen. An ihre politische Behandlung stellen diese Phasen unterschiedliche Anforderungen. Jedoch muss das Gefahrenpotenzial in jedem Fall realistisch gesehen werden, gleichviel ob aktuelle Krisenbewältigung oder vorbeugendes Handeln gefragt sind. Dieses Gefahrenpotenzial wird mit der Komplexität unserer Lebensumstände und mit globalen Wirtschafts- und Kommunikationsbeziehungen immer vielschichtiger: Neben Naturkatastrophen geht es um soziale und technogene Ereignisse (z. B. Terrorismus, Aufruhr, Freisetzung von radioaktiven, biologischen und chemischen Stoffen u. a.) sowie die Gefährdung und den Schutz so genannter Kritischer Infrastrukturen. Bei alledem müssen die subjektiven Sicherheitsbedürfnisse der Bevölkerung als eigenständiger Gegenstand der Politik gesehen werden, nicht nur als eine lästige Begleiterscheinung objektiver Probleme.

Sicherheitspolitik im erstgenannten Sinne eines Vorbereitetseins auf kleine und große Gefahrenlagen und auf ihre Bekämpfung kann an einige Entwicklungen anknüpfen. Ein kommunales Sicherheitsmanagement wird inzwischen eingefordert. So gilt es hier unter anderem, Selbsthilfepotenziale zu organisieren. Jedoch stellen sich zwei Dauerprobleme, die bislang nicht im Aufmerksamkeitsfeld der Kommunalpolitik lagen: einerseits die mangelhafte Kommunikation zwischen den einzelnen zur Hilfeleistung im Akutfall beitragenden Organisationen sowie andererseits deren gemeinsame operative Führung. Hier sind die Probleme seit langem bekannt (Lenk 1992; ,t Hart 1997), aber Lösungen lassen auf sich warten. Im Gegenteil, jede (Beinah-)Katastrophe oder Krise (Beispiel: an Vogelgrippe verendete Zugvögel werden auf Rügen gefunden) zeigt die Unzulänglichkeit der gegebenen Kommunikationsstrukturen und der mehr oder weniger unreflektierten Reaktionen. Wird die Thematik, wie zu erwarten, demnächst die Aufmerksamkeitsschwelle der Kommunalpolitik überwinden, so kann man zur Frage der Handlungskoordination in einem sich jeweils ad hoc konstituierenden Handlungsnetz weiterführende Beiträge erwarten. Dann könnte auch von Seiten der Wissenschaft her dazu beigetragen werden, dass die überkommenen Führungsstrukturen und -grundsätze der einzelnen BOS bzw. ihres Handlungsgeflechts mit Grundsätzen des Public Management konfrontiert werden (vgl. Lenk 1998).

Noch größere Schwierigkeiten als die Handlungskoordination im Krisenfall wird es bereiten, eine kommunale Sicherheitspolitik auf die Prävention und Mitigation (Abmilderung) von Gefahren und Risiken einzustellen. Hier ist die Akteursvielfalt noch größer als beim Zusammenwirken einzelner BOS und (Laien-)Helfer. Denn es stehen viele Fachbereiche zur Debatte, deren Handeln und Planen Sicherheitsfragen oftmals vernachlässigt und die zur Abmilderung der Risiken viel beitragen könnten. Hier ist ein breites kommunales Handlungsfeld,

denn allzu gern wird übersehen, dass viele Risiken und Gefahren nicht von außen importiert, sondern „hausgemacht“ sind. Aber auch auf von außen kommenden Gefahren wie Terrorismus gibt es lokale Antworten im Sinne z.B. gesellschaftlicher Immunisierungsstrategien und Wachsamkeit. Die Herausforderung gleicht einer Sisyphusarbeit: Beide Typen von Risiken, die importierten und die hausgemachten, sind schlecht beherrschbar, und sie wachsen weiter, als Nebenfolge von Veränderungen in der Gesellschaft, aber auch im kommunalen und staatlichen Handeln selbst.

Vier Zusammenhänge können benannt werden, in denen kommunale Abmilderung von Risiken denkbar ist und politisch durchgesetzt werden könnte.

Der erste dieser Zusammenhänge hat zu tun mit baulichen Arrangements. Parkhäuser, Gewerbegebiete, U-Bahnen haben Auswirkungen, an die bei der Planung selten gedacht wurde. Erdbebensicherheit als Beispiel hängt auch ab von der Siedlungsstruktur. Erst zusammen mit unserer Bauweise werden Erdbeben zur Katastrophe, worauf schon Jean-Jacques Rousseau nach dem Erdbeben von Lissabon 1756 hinwies.

Ein zweiter Aspekt betrifft Folgen des Handlungsstil öffentlicher Institutionen, also (aus kommunaler Sicht) hausgemachte Risiken. Das Streben nach Effektivierung der Erfüllung öffentlicher Aufgaben hat uns einen gravierenden Abbau „nebenbei“ produzierter Sicherheit beschert (Beispiel: Wegfall von Straßenbahnschaffnern). Zusammenhänge wie der zwischen dem Einsparen von Zugschaffnern und zunehmendem Vandalismus wurde lange Zeit ignoriert.

Hinzu kommt drittens die Störanfälligkeit kritischer Infrastrukturen. Diese sind oft im kommunaler Besitz, aber die Notversorgung (z.B. mit Trinkwasser) wurde bislang als übergeordnete Zuständigkeit von Bund und Ländern verstanden.

Der vierte und wohl wichtigste Zusammenhang betrifft den Grad des gesellschaftlichen Zusammenhalts. Auch hier unterliegen die Kommunen Einflüssen, die sie nicht steuern können. Die nachlassende Integrationskraft gesellschaftlicher Institutionen (Schule, Vereinswesen, etc.) beruht auf gesamtgesellschaftlichen Tendenzen, schafft jedoch primär örtliche Probleme. Gravierend ist der gesellschaftliche Wandel, der mit einem Wertwandel und einer Abnahme „zivilen“ Verhaltens, in der Öffentlichkeit wie im eigenen familiären Umkreis, einhergeht. Wir stehen mitten in dem von Jürgen Habermas diagnostizierten allmählichen Abschied von der Arbeitsgesellschaft, wollen dies aber nicht wahrhaben. Die Auswirkungen dieser globalen Entwicklung zeigen sich lokal. Wenn der örtliche soziale Zusammenhalt prekär wird, dann hat das auch damit zu tun, dass jungen Menschen pausenlos ein Schlaraffenland vorgegaukelt wird, gleichzeitig aber bei ihnen die Botschaft ankommt, dass die Gesellschaft sie eigentlich nicht brauche.

Eine Aufkündigung sozialer Solidarität ist die Folge. „The key to survival is to succeed as a neighbour“ formulierte der schwedische Geograph Torsten Hägerstrand (Van Paassen 1981, S.17). Zunehmend sieht man gar nicht mehr die Notwendigkeit, Anstrengungen in diese Richtung zu unternehmen. Den Pflichten, die einem die Pflege der Nachbarschaft auferlegt, kann man mit genügend Geld ausweichen. Wer kann, koppelt sich ab, durch Rückzug in abgeschirmte residential areas. Die Spitze des Eisbergs bilden die gated communities. Soziale Kohäsion wird unter solchen Umständen zu einem Gegenstand der Sicherheitspolitik.

Bezogen auf Prävention und Mitigation folgen aus diesen vier Zusammenhängen Zielsetzungen, die so breit sind, dass sie eine ganze Reihe von Fachpolitiken durchtränken. Damit stellt sich, ganz ähnlich wie in der Diskussion um Nachhaltigkeit, die Frage, ob hier nur ein neues Politikfeld im Entstehen ist, oder ob es sich um Aspekte handelt, die schon existierende Bereiche durchdringen. Wie bei der Umweltpolitik stellt sich damit die Frage, wie viele Elemente in eigenen, neu zu schaffenden Organisationen gebündelt werden sollen (Müller 1986). Wenn es darauf ankommt, sicherheitspolitische Belange stärker in Fachpolitiken wie z.B. Stadtentwicklung und Sozialhilfe zur Geltung zu bringen, dann müssen die Träger dieser Fachpolitiken sensibilisiert werden. Die in Frage stehenden Bereiche sind so verschiedenartig wie kommunale Versorgungsinfrastrukturen und nachbarschaftsbezogene Sozialpolitik. Aber es wäre nicht sinnvoll, über der Beeinflussung dieser Fachpolitiken auf die Herausbildung eines eigenständigen Bereichs „Sicherheitspolitik“ zu verzichten. Die Kommunen müssen auf die Herausforderungen der neuen Situation so reagieren, wie sie es auf die Probleme der Industrialisierung von mehr als einem Jahrhundert getan haben. Sie müssen die Zeichen der Zeit verstehen und neue Strukturen schaffen. Die Ratio der Selbstverwaltung in deutschen Verständnis liegt im „Aufgabenerfindungsrecht“, in der kreativen Antwort auf örtliche Probleme durch neue Politiken und Dienste.

Wege der Institutionalisierung

Ein Vergleich mit der Etablierung der Umweltpolitik auf kommunaler und staatlicher Ebene vor zwei Jahrzehnten

kann einige Lösungswege aufzeigen, um eine für die Entscheidungsträger noch unpopulär erscheinende Querschnittspolitik zu etablieren. Neue Politiken sind zunächst schwach. Im Fall der Umweltpolitik mobilisierten die Träger der Politik im BMI bewusst Bürgerinitiativen, um sich gegen andere Ressorts bzw. Abteilungen durchzusetzen. Auch war die Einrichtung der Umweltverträglichkeitsprüfung (Environmental Impact Assessment) ein Mittel, die eher disparaten und über eine Reihe von Politikfeldern (Bodenschutz, Lärmschutz, Naturschutz, Wasserwirtschaft, etc.) streuenden Umweltbelange zu bündeln und damit ihr Gesamtgewicht in die Waagschale zu werfen. Und wie in der Umweltpolitik sind drei aufeinander aufbauende Schritte von Bedeutung, nämlich Diskurs, Planung und organisatorische Verankerung:

- Diskurs: Die Dinge müssen beim Namen genannt und die gedanklichen Umrisse der Politik müssen etabliert werden
- Planung: Langfristprognosen und Szenarien der Sicherheitsentwicklung müssen erstellt werden, um auf das Unvorhersehbare gefasst zu sein.
- Organisatorische Verankerung: Sicherheitsbelange müssen institutionell gebündelt werden, um ihnen Gewicht zu verleihen, ohne dabei in blinde Überreaktion zu verfallen.

Diskurs:

Interessen, die keine Institutionen als Vertreter haben, sind weniger durchsetzungsfähig. Damit hat es das öffentliche Interesse an Sicherheit schwer. Weil es keine zentralen institutionellen Sprachrohre hat, wird es oft spektakulär „aus gegebenem Anlass" überzogen. Daher rührt dann wiederum ein Misstrauen gegen die politischen Repräsentanten dieses Interesses. Sicherheit stellt in anderer Weise als Datenschutz ein Konglomerat vorwiegend *öffentlicher* Interessen dar, denen gewiss auch Individualinteressen korrespondieren. Datenschutz hingegen bezieht sich viel stärker auf Individualpositionen.

Der Einbezug des Sicherheitsgefühls der Bürger ist wichtig, kann jedoch leicht zu Schieflagen führen, solange die Konfrontation zwischen Sicherheitsbehörden und Öffentlichkeit weiter besteht. Der Einbezug der BOS kann viel bringen. So verfügt die Polizei über viel implizites Wissen über den Zustand der Gesellschaft, das bislang nicht oder nur auf Nebenwegen (z.B. über die Sozialarbeit) kommunal relevant wird.

Planung: Szenarien und Langfristprognosen müssen erstellt werden

Hier geht es um Krisenplanung einerseits und um Prävention bzw. Mitigation andererseits. Bezogen auf die Krisenplanung ist die gegenwärtige Situation der Modernisierung im Bereich der BOS dadurch gekennzeichnet, dass vor allem „aus gegebenem Anlass" gelernt wird. Vielfach führen Eilbedürftigkeit – weil man zu lange nichts getan hat – und emotionale Reaktionen dazu, dass suboptimale Lösungen vorgeschlagen oder einfach technische Pflaster für organisatorische oder gesellschaftliche Probleme gesucht werden. Zu wenig Akteure überblicken sowohl das Potenzial der Informationstechnik als auch die eigenen Arbeitsvollzüge, und sie haben in der Regel keinen ausreichenden Zugang zu den obersten Entscheidungsebenen. Wegen ihrer Überlastung mit Tagesgeschäften sind sie oftmals nur wenig geneigt, längerfristige Überlegungen anzustellen. Die Frage, wie die eigene Arbeit in zehn Jahren aussieht, wird daher aus Gründen der Überlastung gar nicht erst aufgeworfen.

Dies kontrastiert mit dem Vorgehen in vielen anderen Politikfeldern, in denen zum Teil weitaus längerfristige Prognosen angestellt werden. Nun ist es sicher einfacher, den Energiebedarf für das Jahr 2025 vorherzusagen als die Herausforderungen, vor denen die Gewährleistung innerer und äußerer Sicherheit im Jahre 2015 stehen. Es kommt hinzu, dass die Sisyphusarbeit der Gewährleistung innerer Sicherheit reaktiv-stabilisierenden Charakter trägt und daher nicht zu visionären Höhenflügen anregt.

Sicherheitsbelange müssen institutionell gebündelt werden

Es müsste gelingen, das Sicherheitsinteresse rationaler zu behandeln, wenn seine verschiedenen Facetten gebündelt werden. Vorbild hierfür könnte die Umweltverträglichkeitsprüfung sein. Deren Funktion ist es, die verschiedenen umweltbezogenen Gesichtspunkte bei der Planung eines Vorhabens zusammen zu führen und gemeinsam zu bewerten. Beeinträchtigungen von Boden, Wasser, Luft, Naturschutzgebieten mögen je für sich einen geringen Stellenwert haben. Zusammen betrachtet werfen sie jedoch mehr Gewicht in die Waagschale, wenn Wechselwirkungen zwischen den umweltbezogenen Aspekten eines Vorhabens auftreten, welche kumulierende Wirkungen haben.

Die Institutionalisierung nach dem Muster von Umwelt-

ämtern reicht jedoch nicht. Sicherheitspolitik muss in die einzelnen Fachpolitiken (kommunale Sozialpolitik, Bebauungsplanung, Versorgungswirtschaft etc.) hinein wirken. Diese sind zur Kooperation aufgerufen, wofür z.B. die schon vorfindlichen Präventionsräte ein Muster abgeben. Ein weitere Ansatz wäre es, eine Art Sicherheits-Check bei neuen kommunalen Projekten verpflichtend zu machen. Damit würden Sicherheitsinteressen gebündelt. Denn das Sicherheitsinteresse könnte rationaler als durch die üblichen Erörterungen des Für und Wider behandelt werden, wenn seine verschiedenen Facetten nach dem Vorbild der Umweltverträglichkeitsprüfung gebündelt werden.

Literaturangaben:

Lenk, K., Organisationsprobleme des Katastrophenschutzes. In: Notfallvorsorge und Zivile Verteidigung 1992, S. 16-22

Müller, E. Innenwelt der Umweltpolitik. Sozialliberale Umweltpolitik – (Ohn)Macht durch Organisation: Opladen 1986.

,t Hart, P., Krisenmanagement in der öffentlichen Verwaltung. In: Staatswissenschaften und Staatspraxis 8 (1997), S. 31-48.

Van Paassen, C., The Philosophy of Geography: From Vidal to Hägerstand. In: Space and Time in Geography. Essays dedicated to Torsten Hägerstrand, Lund 1981, S.17-29.

Bisher in dieser Reihe erschienen

N° 65	Gemeinden und Unternehmen sagen Ja zu Kindern Standortfaktor Familie	11/2006
N° 64	Rakeling	11/2006
N° 63	Konzessionsverträge und Konzessionsabgaben nach der Energierechtsreform 2005 – Hinweise für die kommunale Praxis	10/2006
N° 62	Basistelefon	7-8/2006
N° 61	Vergaberecht 2006 Aktuelle Neuerungen und kommunale Forderungen	5/2006
N° 60	Sichere Städte und Gemeinden Unterstützungs- und Dienstleistungsangebote des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe für Kommunen	5/2006
N° 59	Für ein starkes Deutschland – Arbeitsplätze und Wachstum in der Fläche – Stärkung der Gemeinden und Mittelstädte unverzichtbar (Nur Online-Version)	4/2006
N° 58	Handlungsempfehlung zur Kostensenkung in der kommunalen Abfallentsorgung Ergebnisse aus dem BMBF-Forschungsverbund zur betrieblichen Kostenoptimierung	4/2006
N° 57	Bildung im Wandel – Schulen ans Netz	4/2006
N° 56	Breitbandanbindung von Kommunen Durch innovative Lösungen Versorgungslücken schließen Grundlagen – Beispiele – Ansprechpartner	1-2/2006
N° 55	Intelligenter Energieeinsatz in Städten und Gemeinden Klimaschutz und Kostensenkung: Gute Beispiele aus dem Wettbewerb „Energiesparkommune“	1-2/2006
N° 54	Mit starken Kommunen Aufschwung und Reformen Bilanz 2005 und Ausblick 2006 der deutschen Städte und Gemeinden	3/2006
N° 53	Gemeinsam für Deutschland – mit Mut und Menschlichkeit Bewertung des Koalitionsvertrages zwischen CDU, CSU und SPD aus kommunaler Sicht	12/2005
N° 52	Mobile Kommunikation Anwendungsbeispiele für Kommunen, Bürger und Wirtschaft (Nur Online-Version)	12/2005
N° 51	Interkommunale Zusammenarbeit – Praxisbeispiele, Rechtsformen und Anwendung des Vergaberechts	10/2005
N° 50	Erfolgreiche Abstimmungsprozesse beim Aufbau der Mobilfunknetze Ergebnisse einer Befragung zur Zusammenarbeit von Kommunen und Netzbetreibern	9/2005
N° 49	Forderungen der deutschen Städte und Gemeinden an die Bundesregierung und den Bundestag – Ohne starke Kommunen keine erfolgreichen Reformen und kein Aufschwung	9/2005
N° 48	Kommunalfinanzen in struktureller Schieflage Datenreport Kommunalfinanzen 2005 Fakten, Trends, Einschätzungen (nur Online-Version)	7/2005
N° 47	Gemeinden sagen Ja zu Kindern – Konzepte und Maßnahmen für mehr Kinder- und Familienfreundlichkeit in Städten und Gemeinden	6/2005
N° 46	Zukunft der Kommunen	5/2005
N° 45	Neustart in der Arbeitsmarktpolitik fortsetzen Bilanz 2004 und Ausblick 2005 der deutschen Städte und Gemeinden“	1-2/2005

DStGB
Deutscher Städte- und Gemeindebund

Marienstraße 6 · 12207 Berlin
Telefon 030.773 07.0 · Telefax 030.773 07.200
E-Mail dstgb@dstgb.de
www.dstgb.de

Verlag WINKLER & STENZEL GmbH
Postfach 1207 · 30928 Burgwedel
Telefon 05139.8999.0 · Telefax 05139.8999.50
E-Mail info@winkler-stenzel.de
www.winkler-stenzel.de