



Bundesministerium  
für Bildung  
und Forschung

# Forschung für die zivile Sicherheit

Programm der Bundesregierung



HIGHTECH-STRATEGIE

Ideen zünden!

## Impressum

### Herausgeber

Bundesministerium für Bildung und Forschung (BMBF)  
Referat Öffentlichkeitsarbeit  
11055 Berlin

### Bestellungen

Schriftlich an den Herausgeber  
Postfach 30 02 35  
53182 Bonn  
oder per  
Tel. : 01805 - 262 302  
Fax: 01805 - 262 303  
(0,14 Euro/Min. aus dem deutschen Festnetz)  
E-Mail: [books@bmbf.bund.de](mailto:books@bmbf.bund.de)  
Internet: <http://www.bmbf.de>

### Redaktion, Autor der Beispielgeschichten

Dr. Mathias Schulenburg, Köln

### Gestaltung

Suzy Coppens, Köln  
[www.bergerhof-studios.de](http://www.bergerhof-studios.de)

### Druckerei

Druckhaus Locher, Köln

Bonn, Berlin 2007

### Bildnachweis

BergerhofStudios, Suzy Coppens

Seite(n) 04 oben, Mitte; 13 oben; 18; 22;  
25 links; 27-29; 31; 33; 48

Bosch

Titel; Seite 17; 21; 23 oben; 43 rechts; 46 unten

California Inst. of Technology,

Seite 44

Fei-Fei et al.

Seite 04 unten; 10; 11 Mitte; 19 unten

Deutsche Bahn AG

Seite 12; 34

Deutsche Telecom AG

Seite 16 rechts; 19 oben; 38 rechts; 40 unten

EADS

Seite 32

ESA/DLR

Fraunhofer Inst. für Silizium-  
technologie, ISIT

Seite 41

Hamburg, Oberfinanzdirektion

Seite 37 unten

Hafen Hamburg Marketing e.V.,

Seite 30

Achim Sperber

Seite 39

IKONOS, Space Imaging

Seite 25 rechts

Kölnarena GmbH

Seite 45

microdrones GmbH

Seite 06; 08; 16 links; 24; 35; 36 links;

Siemens AG

36 rechts; 40 oben; 42; 43 links; 46 oben

Technisches Hilfswerk

Seite 10 unten; 11 rechts; 13 unten; 15; 26;

University of California,

38 links

Mark Hoemmen

Seite 23 unten

U.S. Customs and Border Protection,

Seite 37 Mitte

Gerald L. Nino

Seite 20

VDI TZ



Bundesministerium  
für Bildung  
und Forschung

# Forschung für die zivile Sicherheit

**Programm der Bundesregierung**

# Vorwort



Deutschland gehört heute zu den sichersten Ländern der Welt. Dies soll und muss auch in Zukunft so bleiben. Der weltweit zunehmende Terrorismus und die organisierte Kriminalität stellen uns aber ebenso wie Naturkatastrophen und technische Großunfälle vor Herausforderungen und Bedrohungen ganz neuer Art, denen wir begegnen müssen. Unsere moderne, stark vernetzte Gesellschaft ist gegenüber solchen Bedrohungen besonders anfällig. Ein Ausfall der Infrastrukturnetze kann die Sicherheit der Menschen ebenso gefährden wie direkte Angriffe und Naturkatastrophen. Deshalb mobilisieren wir die Forschung. Wir brauchen weiterführende, intelligente Lösungen, die uns Sicherheit bieten, aber unsere Kultur der Freiheit nicht beeinträchtigen. Wir brauchen neues Wissen, weil wir nicht einfach alte Lösungen auf neue Herausforderungen übertragen können. Die Bundesregierung legt deshalb erstmals ein Forschungsprogramm zur zivilen Sicherheit vor.

Die Sicherheitsforschung ist eines der zentralen Innovationsfelder im Rahmen der umfassenden Hightech-Strategie für Deutschland. Das Programm bildet eine Plattform, auf der Wirtschaft und Behörden, Forschung und Anwendung strategisch zusammen arbeiten können. Es richtet sich ebenso an die Betreiber von sicherheitsrelevanten Infrastrukturen wie Verkehr, Wasser, Energie wie an Unternehmen, die innovative Sicherheitslösungen entwickeln. Die Entwicklung von Sicherheitsprodukten und –systemen ist ein wichtiger Faktor in einem weltweit expandierenden Markt. Die Verfügbarkeit über Sicherheitstechnologien bestimmt auch über die technologische Leistungsfähigkeit und die internationale Wettbewerbsfähigkeit der deutschen Unternehmen.

Dabei geht es immer um die Sicherheit von Menschen. Dialog und Transparenz sind gerade in der Sicherheitsforschung unverzichtbare Voraussetzungen für den Erfolg des gesamten Programms. Der Einsatz von hochtechnischen Sicherheitssystemen, der Umgang mit Sicherheitstechnologien und deren Akzeptanz müssen von vornherein mit bedacht und berücksichtigt werden. Die Geistes- und Sozialwissenschaften sind bei der Entwicklung innovativer Sicherheitslösungen deshalb ebenso gefragt wie die Natur- und Ingenieurwissenschaften. Ethische, juristische und sozialwissenschaftliche Aspekte der Sicherheitsforschung müssen wir in einem breiten gesellschaftlichen Dialog thematisieren. Ziel der Sicherheitsforschung ist der Schutz der Bürgerinnen und Bürger. Es gilt, die Sicherheit, aber auch den Wohlstand und die Freiheit in unserem Land zu erhalten.



Dr. Annette Schavan, MdB  
Bundesministerin für Bildung und Forschung

# Inhalt

|   |           |
|---|-----------|
| Zusammenfassung   | 5         |
| <b>Teil I: Strategische Ausrichtung der Sicherheitsforschung</b>            | <b>7</b>  |
| Ziele der Sicherheitsforschung  | 8         |
| Ausgangslage  | 9         |
| Leitlinien  | 10        |
| Stärkung der ressortübergreifenden Zusammenarbeit                           | 10        |
| Orientierung auf Endnutzer und Märkte                                       | 11        |
| Verknüpfung technologischer und gesellschaftlicher Fragestellungen          | 13        |
| Europäische Zusammenarbeit und internationale Forschungsallianzen           | 14        |
| Ultrabreitband-Funk für die Rettung von Menschen                            | 15        |
| <b>Teil II: Förderprogramm</b>  | <b>17</b> |
| Ziele der Förderung   | 18        |
| Der Agendaprozess zur Vorbereitung des Programms                            | 20        |
| Die Programmlinien der Förderung  | 21        |
| Programmlinie 1 „Szenariorientierte Sicherheitsforschung“                   | 21        |
| Programmlinie 2 „Technologieverbünde“                                       | 21        |
| Szenariorientierte Sicherheitsforschung                                     | 22        |
| Schutz und Rettung von Menschen   | 22        |
| Evakuierungstechniken   | 25        |
| Sprengstoffdetektion  | 27        |
| Schutz von Verkehrsinfrastrukturen  | 28        |
| Falsch gefühlte Sicherheit – wie sicher ist sicher?                         | 31        |
| Schutz vor Ausfall von Versorgungsinfrastrukturen                           | 32        |
| Schutz vor Kaskadeneffekten   | 35        |
| Sicherung der Warenketten   | 36        |
| Technologieverbünde   | 38        |
| Integrierte Schutzsysteme für Rettungs- und Sicherheitskräfte               | 38        |
| Feuerwehr der Zukunft   | 39        |
| Multi-Sensorsysteme für CBRNE-Gefahren                                      | 40        |
| Nanotechnologien gegen Bioterror  | 41        |
| Mustererkennung   | 42        |
| Biometrie zur Identifizierung von Personen                                  | 43        |
| Aufklärungsroboter  | 45        |
| Biometrie   | 46        |
| Umsetzung des Förderprogramms   | 47        |
| Förderinstrumente   | 47        |
| Programmlaufzeit und Fördermittel   | 47        |
| Anhang  | 49        |
| Laufende Aktivitäten der Bundesregierung mit Bezug zur Sicherheitsforschung | 49        |
| Glossar   | 57        |



# Zusammenfassung

**Deutschland ist eines der sichersten Länder der Welt.**

**Die großen Konfrontationen des Kalten Krieges sind verschwunden, Deutschland ist vereint und von Verbündeten umgeben.**

Es sind allerdings neue Bedrohungsszenarien entstanden, die nur zum Teil auf mögliche Einwirkungen von außen zurückgehen. Die moderne Industriegesellschaft ist dicht mit Infrastrukturnetzen überzogen, die Mobilität, Energie und Informationsflüsse bereitstellen und so das effiziente Wirtschaften in Deutschland ermöglichen. Diese Netze bieten auch kritische Stellen, dann zumal, wenn sie an den Grenzen ihrer Kapazität betrieben werden. An diesen könnten Anschläge mit vergleichsweise geringen Mitteln große Wirkungen erzielen.

Auch die mittlerweile globale Mobilität hat ihren Preis: Viren können heute per Flugzeug innerhalb von Stunden um die Erde reisen, ein Umstand, der von Epidemiologen mit Sorge gesehen wird. Die Spanische Grippe von 1918 konnte schon mit den im Vergleich bescheidenen Verkehrsmitteln der Zeit Verheerungen anrichten. Die erhöhte Mobilität hat eine wachsende Zahl von Großveranstaltungen zur Folge – Weltmeisterschaften, Jugendtreffen – die schon der großen Menschenzahlen wegen ihre eigene Gefährdungsdynamik entfalten und auf die die Fernsehkameras der Welt gerichtet sind, was solche Veranstaltungen wiederum für Anschläge attraktiv macht.

Die technische Gesellschaft hat überdies zusammen mit ihren Annehmlichkeiten neue Möglichkeiten geschaffen, Waffen mit großer Wirkung auch für kleine Gruppen verfügbar zu machen, die damit großen politischen Druck aufbauen könnten. Anthrax ist ein Beispiel – biologische Techniken sind weithin verfügbar –, auch ist als Hinterlassenschaft des Kalten Krieges eine Vielzahl zweifelhaft gesicherter radioaktiver Stoffe übrig geblieben.

Naturkatastrophen und große technische Unfälle können in einer dicht vernetzten Welt ebenfalls große Folgeschäden auslösen.

Die Bundesregierung will diesen und anderen Bedrohungen der zivilen Sicherheit mit dem vorliegenden Forschungsprogramm begegnen. Es ist fest in die Hightech-Strategie für Deutschland eingebunden, die erstmals eine gemeinsame

Innovationspolitik aller Ressorts anstrebt. Das Sicherheitsforschungsprogramm ist überdies auf eine enge Zusammenarbeit mit den Mitgliedsstaaten im Rahmen der EU angelegt, darüber hinaus werden strategische Forschungsallianzen mit außereuropäischen Staaten aufgebaut, die in Sicherheitsfragen besondere Stärken aufweisen.

In der Folge des Programms werden innovative Lösungen erwartet, die die Sicherheit der Bürgerinnen und Bürger verbessern, ohne ihre Freiheit einzuschränken. Sicherheit ist nicht allein durch Technologie erreichbar. Technologische und gesellschaftliche Fragestellungen werden verknüpft, neue Sicherheitslösungen von einem gesellschaftlichen Dialog begleitet.

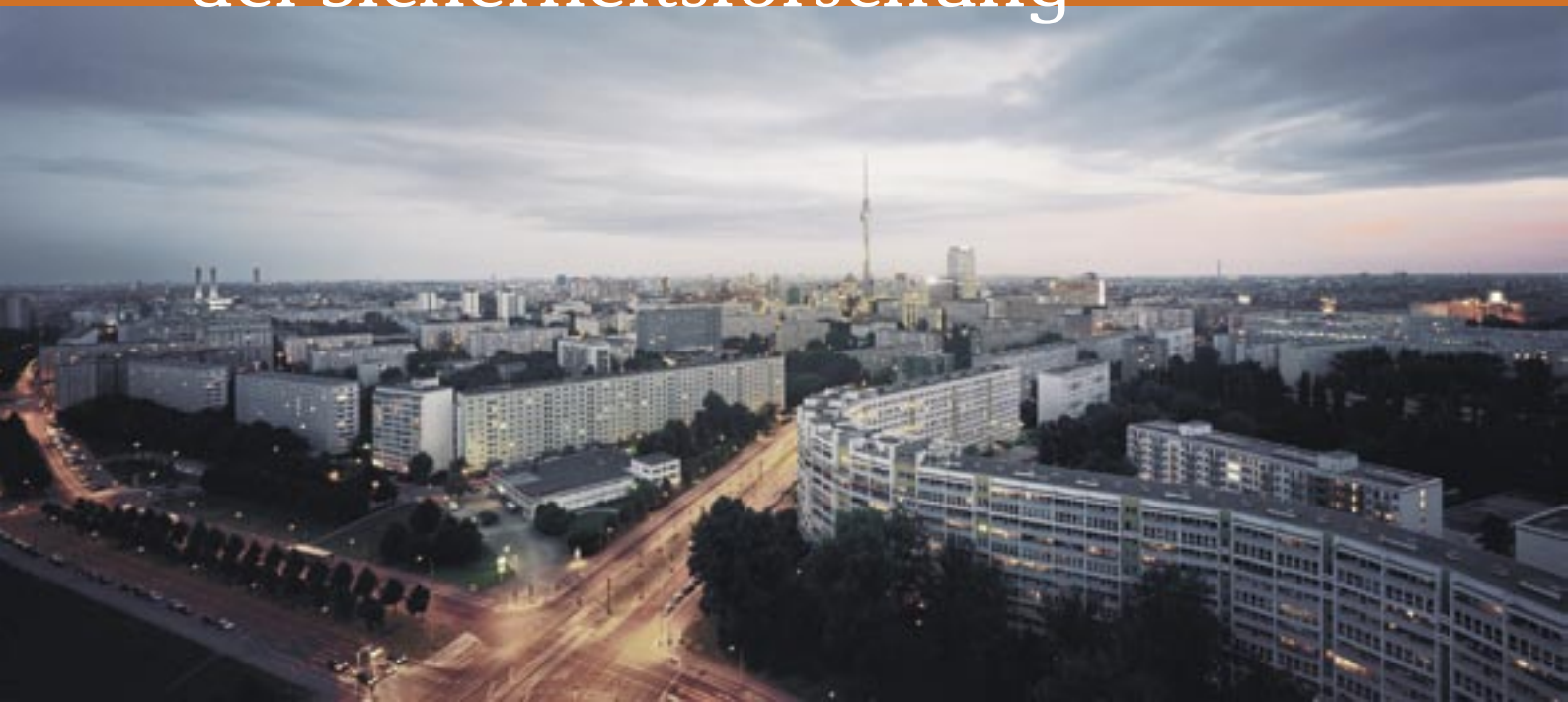
Das Programm ist auch marktorientiert. Der Markt für Sicherheitstechnik und –dienstleistungen belief sich in Deutschland 2005 auf 10 Milliarden Euro, sein weltweites Wachstum beträgt jährlich 7 bis 8%. Deutschland ist durch seine effiziente, vielfältige und zeitgemäße Forschung (Mikrosystemtechnik, optische Technologien, Sensorik u.a.) sehr gut gerüstet, diesen Markt zu bedienen. Mit der engen Einbindung in Europa schafft das Programm die Voraussetzungen für wirtschaftliche Erfolge über Deutschland hinaus.

Die Förderung wird in zwei Programmlinien konzentriert. Programmlinie 1 umfasst die „Szenariorientierte Sicherheitsforschung“ aus der Problemlösungsperspektive der Endnutzer und ist u.a. auf die Verbesserung der Zusammenarbeit zwischen Behörden und privaten Betreibern sicherheitsrelevanter Infrastrukturen angelegt. Kernelemente der Förderung sind: Schutz und Rettung von Menschen; Schutz von Verkehrsinfrastrukturen; Schutz vor Ausfall von Versorgungsinfrastrukturen; Sicherung der Warenketten. Im Vordergrund stehen nicht technologische Einzelergebnisse, sondern die Formierung der Akteursgemeinschaft.

Programmlinie 2 zielt auf die Erforschung von Querschnittstechnologien in „Technologieverbänden“ ab, die in vielen Szenarien benötigt werden, z.B. Techniken zur schnellen und sicheren Personenidentifikation, zur schnellen Erkennung von Gefahrstoffen usw.

Die erste Förderperiode des Programms von 2007 bis 2010 bildet zugleich die Grundlage für eine langfristig ausgerichtete, flexible Förderpolitik. Für die Jahre 2007-2010 stehen – zusätzlich zu den Haushaltsmitteln für die Sicherheitsforschung der Ressorts – rund 123 Millionen Euro zur Verfügung.

# Strategische Ausrichtung der Sicherheitsforschung



Die Bundesregierung hat in ihrem Zweiten Periodischen Sicherheitsbericht vom November 2006 auf die gute Sicherheitslage und das hohe Sicherheitsniveau in Deutschland hingewiesen. Sie hat zugleich festgestellt, dass die Bedrohung durch Terrorismus oder extremistische Angriffe groß ist.

Vorrangige Bedrohungen der modernen Gesellschaft sind darüber hinaus die Verbreitung von Massenvernichtungswaffen, regionale Konflikte, der Zusammenbruch von Staaten und die organisierte Kriminalität, wie sie auch in der Sicherheitsdoktrin der Europäischen Union genannt werden. Die Bedrohungen gehen zumeist von kleinen Gruppen ideologisch oder kriminell motivierter Täter aus, können aber eine Vielzahl von Menschen treffen. Im Extremfall könnte durch Angriffe auf lebenswichtige Infrastrukturen wie die für Energie, Versorgung, Informationstechnik, Telekommunikation, Verkehr, Gesundheitsversorgung oder das Finanzsystem die ökonomische und gesellschaftliche Stabilität eines Landes gefährdet werden. Möglich ist das durch die Existenz und Verfügbarkeit von Waffen und gefährlichen Stoffen, aber auch die Komplexität der vernetzten und globalisierten Gesellschaft, die zahlreiche neuralgische Punkte bietet, an denen sich mit kleinen Mitteln große Wirkungen erzielen lassen. Die Bevölkerung zu schützen, die Verwundbarkeit des Landes zu reduzieren und die Ursachen des Terrorismus zu bekämpfen sind daher wichtige Ziele der deutschen

Sicherheitspolitik. Die Entwicklung geeigneter Technologien und Handlungsstrategien im Rahmen der zivilen Sicherheitsforschung soll die Erreichung dieser Ziele unterstützen. Sicherheitsforschung muss auch Lösungen entwickeln, die die gesellschaftlichen Auswirkungen von Naturkatastrophen oder Großunfällen minimieren, sei es im Gesundheits- und Agrarbereich, bei Trinkwasser und Lebensmitteln, auf dem Energiesektor oder bei anderen lebenswichtigen Infrastrukturen. Die zunehmende Konzentration der Bevölkerung in Ballungszentren, die wachsende Vernetzung unterschiedlichster Lebensbereiche und die Entwicklung zur globalen Informations- und Dienstleistungsgesellschaft haben eine neue Qualität der Verwundbarkeit zur Folge. Schutz- und Sicherungsmaßnahmen können deshalb nur noch bedingt mit vertrauten Techniken und Organisationsformen realisiert werden. Neue Bedrohungs- und Gefahrenpotentiale auch durch neue Verwundbarkeiten der Gesellschaft erfordern neue Sicherheitsansätze, neue Kompetenzen und Qualifikationen sowie neue Technologien.

Die Bundesregierung verankert ihr Sicherheitsforschungsprogramm als einen Schwerpunkt in der nationalen Hightech-Strategie. Dieser Rahmen bietet die Möglichkeit, durch Forschung und Innovation die Wettbewerbsfähigkeit der beteiligten Unternehmen und die Marktfähigkeit der von ihnen erarbeiteten sicherheitstechnischen Lösungen zu fördern, Sicherheit als nationalen Standort- und Wirtschaftsfaktor zu etablieren und Gestaltungsspielräume auf europäischer Ebene zu eröffnen. Auch die Europäische Union hat die Herausforderungen angenommen und ein eigenes Sicherheitsforschungsprogramm aufgelegt.

## Ziele der Sicherheitsforschung

**Forschung und Innovation werden der zivilen Sicherheitspolitik neue Mittel in die Hand geben, unser demokratisches Staatswesen und seine Menschen vor Bedrohungen zu schützen. Sicherheitsforschung hat die Aufgabe, Risiken für unsere Gesellschaft zu analysieren und neue Lösungen zu deren Minderung oder Vermeidung zu entwickeln.**

Im Mittelpunkt des Sicherheitsforschungsprogramms steht die Verbesserung des Schutzes der Bürgerinnen und Bürger in Deutschland vor alten und neuen Gefahren. Die Abwehr besonders der neuen Gefahren erfordert hoch entwickelte Technologien in neuen Sicherheitssystemen und damit verbunden neue Handlungsstrategien.

Die angestrebten innovativen Sicherheitslösungen sollen dazu beitragen, die Sicherheit der Menschen zu erhöhen ohne dadurch ihre Freiheit einzuschränken. Im Gegenteil: Handlungsspielräume, die durch Bedrohung bereits eingeschränkt wurden, können durch verbesserte Sicherheitssysteme zurück gewonnen werden, z.B. durch optimierte und innovative Detektionstechnologien in Flughäfen. Die notwendigen Abwägungen bezüglich der Folgen des Umgangs mit den neuen Sicherheitssystemen und ihrer Akzeptanz können nur im öffentlichen gesellschaftlichen Dialog bestimmt werden. Ziel ist es deshalb auch, diesen Dialog anzustoßen.

Sicherheitsforschung kann nur im internationalen, mindestens im europäischen Kontext wirksam erfolgen. Internationale Forschungsallianzen, die europäische Forschungszusammenarbeit und die Mitgestaltung der europäischen Sicherheitsarchitektur sind deshalb weitere Ziele des Sicherheitsforschungsprogramms.

*Zentrale im Flughafen München: Komplexe, von vielen Menschen frequentierte Einrichtungen erfordern eine aufwändige Sicherheitstechnik, die sich nicht aufdrängen darf.*



# Ausgangslage

Die Ausgangslage in Deutschland, geprägt unter anderem durch eine vielfältige Forschungsförderung, intensive Forschungstätigkeit an Universitäten und außeruniversitären Forschungseinrichtungen sowie starke Traditionen der Natur- und Technikwissenschaften wie auch der Geistes- und Sozialwissenschaften, bildet eine gute Voraussetzung für die Sicherheitsforschung.

Das Sicherheitsniveau in Bereichen wie Anlagen- und Reaktorsicherheit, Verkehrswegesicherheit, Lebensmittelsicherheit und Chemikaliensicherheit gilt bereits jetzt als vorbildlich, es kann durch gut ausgebaute Basistechnologien weiter optimiert und verfeinert werden.

Die Sicherheitsforschung für die erkannten neuen Herausforderungen benötigt aber neue Qualitäten. Vorhandene Sicherheitslösungen können künftigen Bedrohungen nicht immer gerecht werden. Die Vielzahl der im Sicherheitsbereich tätigen Akteure (Behörden, Infrastrukturbetreiber, Sicherheits- und Rettungskräfte, Anbieter sicherheitstechnischer Lösungen, Forscher) hat derzeit keine gemeinsamen Plattformen, um Fragen nach künftigen Bedrohungen und möglichen Lösungen bundesweit systematisch und koordiniert anzugehen. Mithin findet keine ausreichende Verständigung darüber statt, was als vorrangige Forschung zu gelten hat. Eine den künftigen Herausforderungen angemessene Zusammenarbeit von Bundesforschungseinrichtungen mit anderen öffentlichen Forschungs- und Entwicklungseinrichtungen und der Industrieforschung hat sich bislang nicht etablieren können. Die Landschaft der Nutzer und Anwender von Sicherheitslösungen ist zersplittert, es mangelt an einem abgestimmten Vorgehen.

Diese Situation und die sich daraus ergebenden Chancen und Risiken werden im folgendem zusammengefasst:

Die **Stärken**: Deutschland hat bei einer Reihe von Basistechnologien wie Mikrosystemtechnik, IKT, optischen Technologien, Bautechnik, Biotechnologie und Sensorik eine gute Position. Dazu gibt es eine ausdifferenzierte Forschungslandschaft auch in der Ressortforschung. Bei Störfall- und Unfallsicherheit (z.B. Anlagen- und Reaktorsicherheit, Ver-

kehrswegesicherheit) ist das Niveau bereits jetzt hoch.

Daraus ergeben sich **Chancen**: Bei Gefahrenschutz und Krisenreaktionsfähigkeit kann die Sicherheitstechnik und ihre Interoperabilität verbessert werden; kostengünstige Lösungen könnten zu einer hohen Verbreitung ziviler Sicherheitstechnologien beitragen. Die Förderung der Sicherheitstechnologie bietet deutschen Unternehmen die Aussicht auf eine Erhöhung ihrer Marktanteile und verbesserte Exportchancen. Nationale Industrieunternehmen mit strategisch wichtigen Fähigkeiten für Sicherheitslösungen werden unterstützt. Hochtechnologien aus anderen zivilen Bereichen und der Wehrtechnik können für Anwendungen der zivilen Sicherheit erschlossen werden. Durch gemeinsame Sicherheitslösungen bei Behörden und privaten Nutzern können Synergien gestärkt, europäische Chancen genutzt und Kompetenzen von Technik- und Geistes- und Sozialwissenschaften zusammen gebracht werden.

Zu den **Schwächen** zählt, dass Deutschland bisher kein Forschungsprogramm zur zivilen Sicherheit hatte, das Basistechnologien für Systeminnovationen zur Sicherheit erschließen konnte. Die vorhandene Sicherheitstechnik ist in Teilen veraltet, die Beschaffung unzureichend auf Innovationen ausgerichtet. Die Zusammenarbeit von Ressortforschungseinrichtungen und anderen öffentlichen FuE-Einrichtungen und der Industrieforschung wurde bisher nicht gezielt gefördert. Es gibt bei der zivilen Sicherheit eine Zersplitterung, die Nutzerlandschaft ist heterogen, es gibt zu wenige auf zivile Sicherheit spezialisierte Akteure.

Die **Herausforderungen**: Es liegt in der Natur der Sache, dass die Sicherheitsforschung in Teilen einen gewissen Geheimschutz braucht. Es macht keinen Sinn, sich über Terrorabwehr in einer Weise zu verbreiten, die möglichen Angreifern nutzt. Andererseits würde ein zu rigider Geheimschutz die Breitenwirksamkeit der Forschungsergebnisse einschränken. Eine mangelnde Transparenz der geplanten Aktivitäten und der mit neuen Technologien verbundenen Auswirkungen kann zu Vorbehalten in der Bevölkerung führen. Eine angemessene Begleitforschung muss mögliche nachteilige Auswirkungen auf Bürger- und Freiheitsrechte frühzeitig erkennen.

# Leitlinien

## Stärkung der ressortübergreifenden Zusammenarbeit

Das Sicherheitsforschungsprogramm stützt sich auf die in den jeweiligen Politikbereichen der Ressorts durchgeführten Ursachen- und Sicherheitsanalysen (z.B. zur Radikalisierung in Deutschland, zu Bedrohungspotentialen oder zu Sicherheitslücken in Infrastrukturen). Es bietet darüber hinaus die Möglichkeit, neuartige Bedrohungsursachen und künftige Sicherheitsanforderungen in ressortübergreifenden Vorhaben zu bearbeiten.

Um Mittel zu finden, die als bedeutsam eingeschätzten Bedrohungen zu erkennen und zu neutralisieren, wird die Bundesregierung die in diesem Zusammenhang wichtigen Forschungs- und Entwicklungsaktivitäten auf gemeinsame Ziele ausrichten. Die Zusammenarbeit der Sicherheitsforschung mit anderen Forschungsprogrammen des Bundesministeriums für Bildung und Forschung z.B. im Bereich der Technologieforschung, der Lebenswissenschaften, der Erdsystemforschung oder der Geistes- und Sozialwissenschaften wird verstärkt. Ebenso wird die Kooperation des Forschungsressorts mit den für die jeweiligen Politikbereiche verantwortlichen Ressorts ausgebaut: Dies betrifft insbesondere das für die Innere Sicherheit verantwortliche Bundesministerium des Innern beim Schutz vor Terrorismus und Kriminalität, beim Schutz kritischer Infrastrukturen, beim Bevölkerungs- und Katastrophenschutz, bei der IT-Sicherheit sowie bei der Stärkung der Sicherheits- und Rettungskräfte und das Bundesministerium für Verkehr, Bauen und Stadtentwicklung

*Kontaminationssperre gegen Vogelgrippe auf Rügen - erfolgreiche Zusammenarbeit von Polizei und Bundeswehr im Katastrophenschutz.*



*Die Versorgung des Landes mit Millionen von Gütern ist zu großen Teilen Nachtarbeit zu danken. Blick aus dem Stellwerk in Hamburg-Waltershof auf die Hafen-Gleisanlagen der Deutsche Bahn AG.*

beim baulichen Schutz, beim Satellitennavigationssystem Galileo und bei der Sicherung des Verkehrs- und Transportwesens. Forschungsfragen im Bereich des Umwelt- und Naturschutzes sowie der Störfallsicherheit werden gemeinsam mit dem Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit, in den Bereichen Anlagensicherheit und Luft- und Raumfahrt mit dem Bundesministerium für Wirtschaft und Technologie gefördert. Die Zusammenarbeit im Bereich Bioterrorismus, Seuchen und Pandemien wird mit dem verantwortlichen Bundesministerium für Gesundheit, im Bereich Lebensmittelsicherheit, Tierseuchen, Pflanzen-



schutz und Pflanzengesundheit sowie Agroterrorismus mit dem Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz intensiviert.

Das zivile Sicherheitsforschungsprogramm befasst sich nicht mit militärischer Sicherheitsforschung und ist daher nicht an den Zielen der Verteidigungspolitik ausgerichtet. Die Sicherheitsforschung des Bundesministeriums der Verteidigung orientiert sich an den militärischen Aufgaben Aufklärung, Navigation, Simulation, Waffen, Zielannäherung, militärische Netzwerke, automatische und autonome Plattformen, technischer und medizinischer ABC-Schutz u.a. Dennoch kann das in militärischen Projekten in der Regel industriell erworbene Technologie-Know-how grundsätzlich auch für zivile Anwendungen genutzt werden. Die Zusammenarbeit mit dem Bundesministerium der Verteidigung

wird sich deshalb besonders auf den wechselseitigen Wissenstransfer und die Erschließung neuer Anwendungen beziehen, die für zivile und wehrtechnische Bereiche bedeutsam sind.



*Kriseneinsätze erfordern die reibungslose Zusammenarbeit der verschiedenen Dienste*

Vielfach ist heute nicht mehr die wehrtechnische, sondern die zivile Forschung führend bei der Entwicklung neuer Technologien. Innovative Sicherheitstechnik wird deshalb – vor allem, was kosteneffiziente Lösungen angeht – weit stärker von der zivilen, oft für Massenmärkte einsetzbaren Hochtechnologie profitieren.

### Orientierung auf Endnutzer und Märkte

Um dem Bedarf an Sicherheit möglichst präzise und schnell gerecht werden zu können, sind die Endnutzer in die Durchführung der Projekte eingebunden. Endnutzer sind Behörden und staatliche Sicherheits- und Rettungskräfte (z.B. Polizei, Technisches Hilfswerk, Feuerwehr) sowie staatliche und private Betreiber kritischer Infrastrukturen (Bahn, Energie- und Gesundheitssektor, Telekommunikation, Öffentlicher Nahverkehr, Flughäfen, Logistik u.a.). Da sich etwa 80% aller sicherheitsrelevanten Infrastrukturen in einer privatwirtschaftlichen Trägerschaft befinden, wird die Bundesregierung mit diesem Programm zusätzliche Anreize schaffen, Staat und Privatwirtschaft Hand in Hand arbeiten zu lassen und Zielkonflikte frühzeitig zu minimieren.

Die Nachfrage nach Sicherheit schafft Werte und Arbeitsplätze. Der Markt von Sicherheitstechnik und Dienstleistungen hatte im Jahr 2005 in Deutschland einen Umfang von 10



*Kontrollzentrum Deutsche Telekom AG*

Mrd. Euro, mit Wachstumsraten um 7 bis 8%. Eine Markt-orientierung der Sicherheitsforschung ist aus folgenden Gründen geboten:

- + **Nur kosteneffiziente Sicherheitssysteme finden ausreichend Verbreitung.**
- + **Neue Sicherheitslösungen können neue Arbeitsplätze schaffen und bestehende sichern.**
- + **Internationale Wettbewerbsfähigkeit der Sicherheitstechnik ist nur gewährleistet, wenn industrielle Kernfähigkeiten in Deutschland gehalten und gestärkt werden.**
- + **Der Staat kann als Nachfrager im Bereich der Sicherheitslösungen einen Pioniermarkt schaffen und so Anbietern aus Deutschland die Einführung von neuen Technologien erleichtern. Dadurch entstehen gerade im Bereich der Sicherheit wesentliche Chancen für neue Märkte und Exporte.**

Sicherheitstechnik ist ein für Deutschland immer wichtiger werdender Markt. Sicherheitstechnische Produkte und Dienstleistungen werden nicht nur von staatlichen und privatwirtschaftlichen Endnutzern und Infrastrukturbetreibern in Anspruch genommen, die Nachfrage geht auch von

Unternehmen aller Art sowie zunehmend von einzelnen Verbrauchern aus. Der Bedarf entsteht einerseits durch staatliche Regelung (z.B. Auflagen zur Luftverkehrssicherheit), speist sich aber auch aus rein betriebswirtschaftlichen Überlegungen (z.B. Sichern der Geschäftsprozesse, Maximierung der Verfügbarkeit, Verhindern von Know-how-Abfluss). Konsumenten fragen Sicherheit etwa im Reiseverkehr oder bei der IKT-Nutzung oder im Bereich der Versorgung nach. Neue Technologien sind ein notwendiges, wenn auch nicht hinreichendes Element des Sicherheitsforschungsprogramms. In durchdachte Handlungsstrategien eingebettet sind sie aber ein zentraler Baustein künftiger Sicherheitslösungen:

- + **Modernste Sicherheitstechnologien können den Rettungs- und Sicherheitskräften helfen, neuen Bedrohungen rascher und wirkungsvoller zu begegnen.**
- + **Unsere lebenswichtigen Infrastrukturen sind immer stärker wechselseitig vernetzt. Nur wenn der Fortschritt in diesem Bereich von innovativen Sicherheitstechnologien begleitet wird, können eventuell neu entstehende Sicherheitslücken geschlossen werden.**



*Die Fluggepäckvorschriften werden immer rigider. Automatische Detektionsverfahren für gefährliche Gegenstände und Stoffe werden das ganze Procedere schneller, sicherer und angenehmer machen.*

- + **Durch die Einführung neuer Technologien entstehen neben erwünschten Effekten unter Umständen auch neue Verletzlichkeiten und sogar Missbrauchsmöglichkeiten. Sicherheitsforschung muss deshalb auch im Vorfeld der Einführung neuer Technologien – zum Beispiel der Warenlogistik, der Kommunikation oder**

*Mobile Leitstellen sind auf leistungsfähige Kommunikationsmittel angewiesen.*



**der Einsatzleittechnik – kritische Fragen möglicher Nebeneffekte behandeln.**

### **Verknüpfung technologischer und gesellschaftlicher Fragestellungen**

Sicherheitstechnologien sind Querschnittstechnologien, die Beiträge unterschiedlicher Disziplinen der Technik- und Naturwissenschaften erfordern. Sicherheit ist aber nicht allein mit Technologien erreichbar, sie hängt immer auch vom Handeln der Menschen ab. So kann auch das Verhalten der Bedrohten, z.B. in Paniksituationen, Gefahren potenzieren und nicht selten werden durch menschliches Fehlverhalten – auch und insbesondere im Umgang mit technischen Systemen – Gefahren überhaupt erst akut. Von den potenziellen Nutzern und den zu schützenden Bürgerinnen und Bürgern nicht akzeptierte Sicherheitslösungen wären in ihrer Wirkung beschränkt oder sogar kontraproduktiv. So, wie etwa die Verkehrssicherheit nicht allein durch technische Vorkehrungen oder Regelsetzungen zustande kommt, sondern erst mit deren einvernehmlichem Gebrauch durch die Verkehrsteilnehmer selbst, so müssen auch Sicherheitslösungen zum Schutz vor Bedrohungen jeglicher Art von jedem einzelnen mitgetragen werden.

Technologische und gesellschaftliche Fragestellungen müssen deshalb in der Sicherheitsforschung miteinander verknüpft werden. Von der geistes- und sozialwissenschaftlichen Forschung werden Beiträge insbesondere erwartet

- + **zur Notwendigkeit und Akzeptanz von Sicherheitslösungen, zu deren Wirkungen und Folgen,**
- + **zu Risiken hinsichtlich einer Einschränkung der Freiheit,**
- + **zu Kosten und Nutzen von Sicherheitsmaßnahmen und –strategien,**
- + **zu Bedrohungsursachen einschließlich Terrorismus und Extremismus, den damit verbundenen Radikalisierungspotentialen und daraus entstehenden neuem Sicherheitsbedarf,**
- + **zu Verbesserungsvorschlägen beim Krisenmanagement, d.h. zu Verhalten und Umgang von Einzelpersonen und gesellschaftlichen Gruppen mit Krisen und Katastrophen, zur Beantwortung rechtlicher Fragen und zur Aufklärung der Bevölkerung im Krisen- und Katastrophenfall,**

- + **zu Möglichkeiten der Gestaltung und des Erhalts effektiver Institutionen bei der Krisenvorbeugung und -bewältigung (systemtheoretische und organisations-soziologische Analysen),**
- + **zum Bedarf beim Aufbau von Kompetenzen und Fähigkeiten der Menschen im Umgang mit innovativen Sicherheitslösungen.**

Das Sicherheitsforschungsprogramm soll von einem gesellschaftlichen Dialog begleitet werden, denn sein Ziel ist der Schutz unserer Freiheiten und nicht ihre Einengung. Es wird so transparent wie möglich gestaltet. Die Öffentlichkeit wird eingehend über die Themen der Sicherheitsforschung und die Chancen und Risiken neuer Lösungen informiert.

### **Europäische Zusammenarbeit und internationale Forschungsallianzen**

Die erwarteten künftigen Bedrohungen machen nicht an Grenzen halt, sie sind global und müssen in einem entsprechend großen Maßstab gesehen werden. In Europa ist dafür die enge Zusammenarbeit der Mitgliedsstaaten erforderlich. Die Europäische Union wird in ihrem 7. Forschungsrahmenprogramm (Laufzeit von 2007 bis 2013) erstmals ein Europäisches Sicherheitsforschungsprogramm mit jährlich ca. 200 Mio. Euro fördern. Es ist auf vier so genannte Missionen ausgerichtet:

- + **Schutz vor Terrorismus und Kriminalität,**
- + **Schutz kritischer Infrastrukturen,**
- + **Wiederherstellung der Sicherheit im Krisenfall,**
- + **Grenzsicherung.**

Die Bundesregierung hat sich erfolgreich dafür eingesetzt, dass das Europäische Sicherheitsforschungsprogramm passfähig zur nationalen Sicherheitsforschung angelegt wird. So konzentriert sich das Europäische Sicherheitsforschungsprogramm ebenso wie das deutsche ausschließlich auf zivile Sicherheitslösungen. Beide Programme beziehen die privatwirtschaftlichen Endnutzer ein und setzen auf Wettbewerbsstärkung.

In der Sicherheitsforschung sind wie in vielen anderen Forschungsfeldern Brücken zwischen nationaler und europäischer Forschung zu bauen:

- + **Künftige Sicherheitslösungen sind vielfach nur wirksam, wenn sie in Zusammenarbeit mit den EU-Mitgliedsstaaten europaweit umgesetzt werden.**
- + **Wettbewerbsfähigkeit kann häufig nur erreicht werden, wenn in den jeweiligen Forschungsbereichen europaweit eine kritische Masse geschaffen wird.**
- + **Der Einsatz von neuen Sicherheitslösungen muss von europäischen Standardisierungs- und Normungsinitiativen sowie einer innovationsfreundlichen Gesetzgebung und Regelsetzung begleitet werden.**
- + **Die erfolgreiche Beteiligung deutscher Akteure im Europäischen Sicherheitsforschungsprogramm erfordert eine intensive Vernetzung mit den europäischen Partnern und muss durch geeignete nationale Beratung und Unterstützung der Antragstellerinnen und Antragsteller angestrebt werden.**

Das europäische Programm kann jedoch nationale Programme der Mitgliedstaaten nicht ersetzen. Wie andere EU-Staaten, die ebenfalls eigene Sicherheitsforschungsprogramme planen oder bereits gestartet haben, setzt auch das deutsche Programm eigene Akzente und berücksichtigt spezifische Sicherheitsanforderungen, Standards und Rahmenbedingungen, z.B. seine zentrale Lage in Europa, seine hoch entwickelten Infrastrukturen, seine kulturellen und gesellschaftlichen Besonderheiten und seine besonderen Stärken in der Forschung. Die Teilhabe am europäischen Programm setzt ebenso wie eine Mitgestaltung der europäischen Sicherheitsarchitektur voraus, dass eigene Stärken eingebracht werden können. Dem kommt die Marktorientierung des nationalen Programms entgegen, die auch den eigenen Exportanstrengungen dienlich ist.

Deutschland wird auf dem Gebiet der zivilen Sicherheitsforschung eine aktive Rolle bei der Entwicklung von Lösungsansätzen für globale Herausforderungen wie den internationalen Terrorismus anstreben, auch durch internationale Forschungsallianzen. Dabei wird weltweit verfügbares Wissen zugunsten der nationalen Programmziele genutzt. Die bilaterale Kooperation wird insbesondere mit Staaten aufgebaut, die spezifische Stärken in der zivilen Sicherheitsforschung aufweisen.



Zerstörungen nach dem Erdbeben in Bam, Südiran, Dezember 2003. Mit UWB-Radar lassen sich Lebenssignale (Atmen, Herzschlagen) unter den Trümmern ausmachen.

### Ultrabreitband-Funk für die Rettung von Menschen

Die Computertechnik ist in den letzten Jahren nicht nur unentbehrlich, sondern auch elegant geworden, was selbst Technikmuffel zugeben müssen: Es gibt flache Notebook-Alleskönner mit Displays für brillante, natürliche Farben; flache Scanner, die zum Amateurpreis professionelle Scans liefern; winzige, schnelle Festplatten für den Videoschnitt – nur eines stört die Ästhetik und Mobilität am Arbeitsplatz: Der Kabelsalat. Damit könnte es ein Ende haben, wenn sich neue kabellose Techniken wie WUSB durchsetzen. „Wireless USB“, eine Funkverbindungstechnik, die den sogenannten Breitband-Kurzstreckenfunk UWB (engl. Ultra Wide Band) verwendet. Die UWB-Technik könnte das heimische Ambiente mit einer Art elektronischen Nebels ausfüllen, in den jedes dafür geeignete Gerät – Notebook, Scanner, Kameras, Fernseher usw. – mit Hilfe einer eigenen Funkschnittstelle eintaucht und sich automatisch vernetzt und verständigt. Grund zur Sorge wegen Elektrosmog bestünde nicht, der „elektronische Nebel“ wäre fein verteilt, die verwendeten Ausstrahlungsleistungen würden nur einen Bruchteil, vielleicht ein Tausendstel dessen betragen, was ein Handy ausstrahlt. Im Sommer 2006 wurden in den USA funktionsfähige Wireless-USB-Chips und -Anwendungen vorgestellt. Die Datenübertragungsraten sind mit 480 Mbit/s so hoch, dass auch die Übertragung von High-Definition-TV damit möglich ist, allerdings mit begrenzter Reichweite.

Das muss auch so sein, denn UWB ist eine Funktechnik, die ein sehr breites Band von Frequenzen benutzt, auch von solchen, die schon von anderen Anwendungen besetzt sind. Die UWB-Signale sind aber so schwach, dass andere Anwendungen nicht gestört werden (was vereinzelt bestritten wird). UWB ist deshalb als lizenzfreie Funktechnik vorgesehen, wie z.B. in WLAN-Systemen. Die Technik könnte die Industrie aus ihrer Frequenznot befreien und ist in ihrer Schnelligkeit und Funktionalität auch sonst so verlockend, dass ihr Einzug in den Alltag unvermeidlich scheint. In den Allianzen, die sie durchsetzen wollen, finden sich die Großen der Unterhaltungselektronik.



Nur fürs erste gerettet und versorgt

UWB ist ein typisches Beispiel für Techniken, deren bahnbrechende Einsatzmöglichkeiten und potenzielle Risiken zwei Seiten einer Medaille darstellen. Schon vor 60 Jahren auf Kriegsschiffen für eine störungsarme Sprechfunktechnik erprobt, kann die UWB-Technologie heute zum wichtigen Bestandteil vieler Anwendungen in unserer nächsten Umgebung werden. Zusammen mit RFID-Tags – Funketiketten – lassen sich z.B. dreidimensionale Ortungssysteme realisieren, mit denen die Positionen tausender verschiedener Funketiketten zugleich auf zehn Zentimeter genau bestimmt werden können. Wenn diese Etiketten an Werkzeugen kleben, etwa in einer großen Flugzeugwartungshalle, hat das Suchen ein Ende. In Krankenhäusern lässt sich so der Aufenthaltsort von Patienten und Personal verfolgen, in Raffinerien ist im Katastrophenfall der Verbleib der Mitarbeiter feststellbar.

Das US-Militär hat mittlerweile auch eine Art UWB-Radar, mit dem sich Bewegungen noch hinter dicken Mauern aufspüren lassen. Rettungskräfte könnten das Radar benutzen, wenn Verschüttete unter den Trümmern eines Erdbebens oder dem Schnee einer Lawine gefunden werden müssen: das UWB-Radar ist in der Lage, durch Mauern hindurch Atembewegungen oder sogar das Schlagen eines Herzens auszumachen.

Einsatzfelder für UWB-Sensoren sind neben der Überwachungs- und Sicherheitstechnik in der Bauindustrie, der Lebensmittelindustrie, im Umweltschutz, bei der Produktionsüberwachung und -kontrolle, in der Verkehrs- und Fahrzeugtechnik, aber auch bei der sogenannten humanitären Minensuche gegeben. Im RADIOTECT-Programm der Europäischen Union wird unter anderem die Nutzbarkeit eines UWB-basierten Bodenradars bei der Entdeckung von Minen untersucht.

Einen Massenmarkt wird das UWB-Radar vermutlich zuerst in der zivilen Automobiltechnik finden: als Abstandsradar zur Einhaltung der Sicherheitsabstände auf Autobahnen.

# Förderprogramm





Das Programm der Bundesregierung zur Sicherheitsforschung stellt die Forschung für zivile Sicherheit erstmals in einen Gesamtzusammenhang. Ziel der Förderung ist die Entwicklung innovativer Lösungen – dazu zählen Verfahren, Produkte, Handlungsstrategien und Netzwerke –, die die Sicherheit der Bürgerinnen und Bürger erhöhen. Dabei sind Fragen der Standardisierung und Qualitätssicherung, die Abstimmung der Systemlösungen aufeinander, die Entwicklung von Maßstäben zur einheitlichen Risikobewertung und zur Bewertung der Wirksamkeit von Maßnahmen und Technologien ebenso wichtig wie der begleitende gesellschaftliche Dialog und die Analyse internationaler Entwicklungen.

# Ziele der Förderung

**Die operativen Ziele richten sich auf vier Felder, in denen deutliche Erfolge erwartet werden können:**

**1. Innovative Sicherheitslösungen, um die Verletzlichkeit der lebenswichtigen Infrastrukturen zu reduzieren:**

Zu diesen Infrastrukturen zählen insbesondere Informations- und Kommunikationssysteme, Verkehrsanlagen, Energieanlagen und -netze, Anlagen zur Lebensmittel- und Warenversorgung und -verteilung, Institutionen des Finanzsektors sowie Gesundheits- und Versorgungseinrichtungen. Diese Infrastrukturen hängen immer stärker zusammen. Nur wenn der Fortschritt in diesem Bereich innovative Sicherheitslösungen einschließt, stellen wir sicher, dass das Mehr an Nutzen und Komfort nicht neue Verletzlichkeiten erzeugt.

Sicherheit gerade in diesem Bereich erfordert mehr denn je die Zusammenarbeit von Staat und Wirtschaft. Gerade im

Bereich der Infrastrukturen sind ehemals hoheitliche Aufgaben in großem Umfang privatisiert worden. Die deutsche Industrie ist als Exportweltmeister in besonders hohem Maße auf die Funktionsfähigkeit dieser Infrastrukturen angewiesen. Deutschland ist schon wegen seiner geographischen Lage in der Mitte Europas Standort international agierender Logistikunternehmen und großer transnationaler Versorger. Das Sicherheitsforschungsprogramm enthält Anreize für eine verbesserte Zusammenarbeit der Forschung mit Behörden und privatwirtschaftlichen Infrastrukturbetreibern. Auf diese Weise soll zu der gegebenen hohen technischen Ausfallsicherheit wichtiger Infrastrukturen in Deutschland der Schutz vor Terrorismus, Sabotage und organisierter Kriminalität hinzu kommen.

*Während bei Attacken auf ein Kohlekraftwerk (RWE AG, Weisweiler) der Schaden örtlich begrenzt wäre, könnte die Attacke auf ein Kernkraftwerk sehr weit reichende Folgen haben.*





*Für eine effektive Polizeiarbeit sind moderne Kommunikationsmöglichkeiten dringend erforderlich.*

## **2. Innovative Sicherheitslösungen zur Stärkung der Rettungs- und Sicherheitskräfte:**

Diese Organisationen (Polizei, Feuerwehr, Medizinische Hilfsorganisationen, Technisches Hilfswerk etc.) werden

*Container-Umschlagbahnhof Frankfurt am Main. Die Zahl der gegenwärtig weltweit im Transportwesen eingesetzten Container wird auf rund 100 Millionen geschätzt.*



mit Hochschulen, Instituten und der Industrie Lösungen erarbeiten, mit denen durch Prävention und Reaktion künftigen Bedrohungen wirksam begegnet werden kann. Bei der gegenwärtigen Beschleunigung des Wandels der Bedrohungen und des technischen Fortschritts reicht es nicht aus, die Rettungs- und Sicherheitskräfte von Zeit zu Zeit mit modernerer Technik auszustatten. Im Rahmen der Sicherheitsforschung werden die Voraussetzungen geschaffen, in Zukunft angemessene innovative Lösungen für technische Ausstattung, Organisation und Handlungsstrategien bereitstellen zu können.

## **3. Den Markt für Sicherheitslösungen erschließen:**

Das Sicherheitsforschungsprogramm wird die Wettbewerbsfähigkeit der beteiligten Unternehmen, aber auch die Marktfähigkeit von Sicherheitstechnik allgemein fördern. Nachfrage nach Sicherheit schafft auch Wertschöpfung und Arbeitsplätze. Das Marktpotential neuer Sicherheitslösungen soll auch erschlossen werden, um hoch qualifizierte Arbeitsplätze und industrielle Know-how-Träger in Deutschland zu halten. Es gibt in Deutschland ein breites Spektrum von industriellen Kernfähigkeiten in sicherheitsrelevanten Technologien (z.B. IKT-Technologien, Biometrie, Robotik, Raumfahrt) mit Wurzeln sowohl im Verteidigungsbereich als auch im zivilen Bereich. Diese strategisch wichtige Industrie wird im Rahmen der Sicherheitsforschung Anreize erhalten, ihre Wettbewerbsposition auszubauen. Das Sicherheitsforschungsprogramm wird zudem dafür sorgen, dass Akteure aus Deutschland eine vorteilhafte Wettbewerbsposition für Forschungsk Kooperationen auf europäischer Ebene erreichen. Die Förderung des nationalen Sicherheitsforschungsprogramms wird in der Auswahl der Projekte darauf achten, dass passfähige und europäisch verallgemeinerbare Lösungen erarbeitet werden. Eine Nationale Kontaktstelle zur Sicherheitsforschung wird eingerichtet, die deutsche Akteure durch Beratungsdienstleistungen unterstützt.

# Der Agendaprozess zur Vorbereitung des Programms

Die Ausrichtung des Sicherheitsforschungsprogramms, seine Förderziele und Inhalte wurden gemeinsam mit Wissenschaft und Wirtschaft ermittelt.

Im Rahmen der Vorbereitung wurde ein umfassender Expertendialog, der so genannte Agendaprozess, durchgeführt. Dieser Agendaprozess führte im Rahmen von drei Expertentalkshops von April bis Juni 2006 ca. 250 Expertinnen und Experten aus allen für die Sicherheitsforschung relevanten Bereichen zusammen. Ziel des Agendaprozesses war die Themenfindung und Strategiebildung sowie die Formierung der Fachszene. Vertreten waren:

- + **Wissenschaftlerinnen und Wissenschaftler aus Universitäten, außeruniversitären Forschungsinstituten, Ressortforschungseinrichtungen, Unternehmen und Bedarfsträgern,**
- + **Wissenschaftlerinnen und Wissenschaftler aus Ingenieur- und Naturwissenschaften, Geistes- und Sozialwissenschaften,**

- + **Endnutzer und Anwender (privatwirtschaftliche Infrastrukturbetreiber, öffentliche Bedarfsträger in Bund und Ländern),**
- + **Anbieter von Sicherheitstechnik (Industrieunternehmen).**

Im Rahmen des Agendaprozesses wurden der Forschungsbedarf von Endnutzern und Anwendern ermittelt und Schwerpunkte für die Erforschung und Entwicklung künftiger Sicherheitslösungen identifiziert. Beim Zusammenführen der Bedarfs- und Lösungsperspektive wurden prioritäre Sicherheitsforschungsszenarien entwickelt. Diese Sicherheitsforschungsszenarien skizzieren einerseits den künftigen Bedarf an innovativen Sicherheitslösungen. Andererseits beschreiben sie Bereiche, in denen auf der Basis intensiverer Forschung neue Lösungen erwartet werden können. Ergebnis des Workshops war auch eine Sammlung der technologischen und geistes- und sozialwissenschaftlichen Forschungsthemen, die in den Schwerpunkten berücksichtigt werden.

*Das Sicherheitsforschungsprogramm wurde in einem umfassenden Agendaprozess vorbereitet.*



# Die Programmlinien der Förderung

## Programmlinie 1 „Szenariorientierte Sicherheitsforschung“

In dieser Programmlinie wird die Forschung auf Lösungen für komplexe Sicherheitsszenarien fokussiert. Damit wird die Problemlösungsperspektive der Endnutzer und Anwender von Beginn an in die Forschung eingebracht. Auf der Basis der Szenarien wird gewährleistet, dass alle für die Erarbeitung umsetzungsfähiger Sicherheitslösungen notwendigen Disziplinen aus den Technik-, Natur-, Geistes- und Sozialwissenschaften eingebunden und auf gemeinsame Anwendungsziele ausgerichtet werden. Die Szenarien bieten zudem die Plattform, auf der Behörden und privatwirtschaftliche Akteure als Betreiber und Anbieter von Sicherheitstechnik zusammenwirken. Die Szenariorientierung stellt sicher, dass isolierte Einzelfragen und Einzellösungen zugunsten passfähiger Systeminnovationen vermieden werden. Diese

*Für die Sicherheit von Mensch und Umwelt stehen mittlerweile vielseitige Einbruch- und Brandmeldezentralen, etwa von Bosch, mit zahlreichen Schnittstellen zur Verfügung.*

Systeminnovationen integrieren bestehende und neue Technologien. Sie stützen sich auf Bedrohungsanalysen und berücksichtigen Kosten-Nutzen-Analysen ebenso wie die Einstellungen und das Verhalten von Einzelnen wie auch Gruppen und deren Dynamik: Wie können Bürgerinnen und Bürger in Krisensituationen zur Reduzierung oder Vermeidung von Gefahrenpotentialen besser beitragen? Wie kann Fehlverhalten, z.B. in Paniksituationen, vermieden werden? Auf diese Weise wird die szenariorientierte Sicherheitsforschung dem tatsächlichen Sicherheitsbedarf gerecht und zugleich für eine rasche Umsetzung der Ergebnisse in die Praxis ausgerichtet.

## Programmlinie 2 „Technologieverbünde“

Bestimmte Sicherheitstechnologien werden in allen bzw. vielen Szenarien benötigt. Dazu zählen die Technologien zur schnellen und sicheren Personenidentifikation, Technologien zur raschen und mobilen Erkennung von Gefahrstoffen, Technologien zur Mustererkennung und Technologien zur Einsatzertüchtigung von Sicherheits- und Rettungskräften. Die Technologieverbünde erschließen für die Sicherheitsforschung wichtiges technologisches Basiswissen und entwickeln aus bestehenden und neuen Basistechnologien innovative Technologiesysteme. Sie arbeiten anwendungsnahe durch Einbeziehung der gesamten Innovationskette, von der Forschung über die Industrie bis hin zu den Endnutzern.

In den Technologieverbänden wird eine angemessene Begleitforschung Fragen der Ethik ansprechen, Innovationsanalysen vornehmen und Rechts- oder Technikfolgen untersuchen, um eventuell notwendige Korrekturen oder ergänzende Maßnahmen vorzubereiten.

In beiden Programmlinien werden im Rahmen der Begleitforschung Fragen zur Akzeptanz der Technologieentwicklungen, zu Quellen von Bedrohungen, zum Datenschutz oder zur Auswirkung auf die Menschen- und Freiheitsrechte einen hohen Rang einnehmen. Die Begleitforschung wird besonderen Wert auf den Wissenstransfer in die Öffentlichkeit legen. Publikationen, Workshops und Diskurse unter den Beteiligten verstärken das Bewusstsein für sicherheitsrelevante Fragen und unterstützen die forschungspolitische Willensbildung. Dialog und Transparenz werden als eine wichtige Voraussetzung für einen Erfolg des Ganzen angesehen.



# Szenariorientierte Sicherheitsforschung

## Schutz und Rettung von Menschen

Die Schauplätze von Großveranstaltungen, aber auch schon besonders dicht mit Menschen besetzte öffentliche Räume sind neuralgische Punkte, an denen kleine und sogar ungewollte Störungen katastrophale Wirkungen haben können. Umso dringlicher ist in solchen Fällen der Schutz vor terroristischen Angriffen, dann zumal, wenn sich die Angreifer der Aufmerksamkeit der Medien sicher sein können, denn der durch die Medien multiplizierte Schrecken ist in der Regel Teil des terroristischen Kalküls. Innovative Lösungen für die Prävention und das Krisenmanagement derartiger Ereignisse vermehren auch die Sicherheit eher alltäglicher Situationen, etwa bei Unfällen, medizinischen Notfällen oder kriminellen Handlungen. Auch ist anzunehmen, dass die global weiter steigende Mobilität kritische Verdichtungen, z.B. bei international besuchten Großveranstaltungen, immer wahrschein-

licher macht. Die Personenanzahl kann sich in solchen Fällen selbst in Millionenstädten temporär annähernd verdoppeln.

Im Rahmen dieses Szenarios geht es darum, eine Vielzahl von Menschen zugleich und auf engem Raum zu schützen. Dabei werden innovative Lösungen für die Früherkennung von Störungen benötigt, um eine Krise entweder zu verhindern oder auf ein Minimum zu begrenzen. Eine wirksame Krisenreaktion hat auch präventiven Charakter: Wenn die Wahrscheinlichkeit von Krisen verstärkenden Faktoren wie z.B. Massenpaniken gesenkt wird, werden Großveranstaltungen für Angreifer von vornherein weniger attraktiv. Daher haben Lösungen zum Krisenmanagement und zur Krisenbewältigung bei Großveranstaltungen eine allgemeine Leitfunktion für den Schutz der Bevölkerung an öffentlichen Plätzen. Ziel

*Weihnachtsmärkte - hier der Kölner - sind wiederholt als Ziel für Anschläge genannt worden.*





der Sicherheitsforschung in diesem Szenario ist die Früherkennung von Störungsversuchen, die zeitnahe Einleitung von Rettungs- und Bekämpfungsmaßnahmen sowie die wirksame Notfallversorgung vor Ort.

Relevante Forschungsthemen:

- Sensorik, Detektion, Robotik

- + Bildauswertungssysteme zur echtzeitnahen Auslösung von Reaktionsmaßnahmen,
- + Algorithmen für automatisierte Entscheidungsverfahren,
- + Standardisierte Lagedarstellungen z.B. auf Basis der Galileo-Technologie,
- + Automatische Personenidentifikationsverfahren,

*Bild links: Erfolgreiche Kriminalprävention und Aufklärung von Straftaten durch Videoüberwachung auf dem Münchner Oktoberfest. Mit Hilfe von 12 AutoDome-Kameras von Bosch konnten insgesamt 89 Straftaten aufgeklärt werden.*

*Bild unten: Der Weltjugendtag von 2005 war auch für die Rettungs- und Sicherheitskräfte eine Herausforderung.*



+ Aufklärungs- und Sensortechnik für nicht bemannte Flugzeuge.

- Simulation, Mustererkennung und Datenerfassung

+ Gefahrenidentifikation unterstützt durch Risikobewertungs- und Simulationswerkzeuge sowie Datenbanken,

+ Automatisierte Auswertung auf Basis von Szenariotechniken.

*Allianz-Arena München (unten). Im Hintergrund sorgt Sicherheitstechnik – Zugangskontrolle (rechts, mit RFIDs, Siemens AG) Sicherheits-, Gebäude- und Informationsmanagement, Verkehrszentralen – für einen reibungslosen Ablauf der Veranstaltungen.*





## Evakuierungstechniken

Die Band „Brings“ spielte gerade ihren Dauerbrenner „Superjeile Zick“ (Schöne Zeit), als die dritte Bombendrohung eintraf und die Polizei beschloss, die Kölnarena, in der 8000 Jecken Karneval feierten, räumen zu lassen. Auf Kölsch: Der Moderator unterbrach „Brings“ und forderte das Publikum zur längsten Polonaise der Welt auf, für das Guinness-Buch der Rekorde, und die Menge strömte lachend und tanzend ins Freie, Bürgermeister Jupp Müller vorneweg.

Die auch von Sicherheitsfachleuten bestaunte Aktion vom 20. Februar 2003 – die Bombendrohung war leer gewesen, was man nicht hatte wissen können - wäre außerhalb Kölns vielleicht nicht möglich. Aber immerhin, an Ideen wie diesen sind die Sicherheitsfachleute sehr interessiert, denn die Evakuierung von Massen ist ein heikles Unternehmen. Wenn sich bei den Leuten Platzangst breit macht, ist unter Umständen kein Halten mehr, denn der Mensch, versichert Michael Schreckenberg, Professor am Lehrstuhl der „Physik von Transport und Verkehr“ der Universität Duisburg, schaltet unter starkem Druck automatisch auf uralte Verhaltensmuster um, die in einer dünn besiedelten Steppe tatsächlich auf den nächstgelegenen Baum führen, in einem Fußballstadion aber verheerende Folgen haben können. Die Duisburger erkunden deshalb mit Computerhilfe, nach welchen Gesetzmäßigkeiten sich große Menschenmengen verhalten, um etwa Notausgänge besser gestalten zu können, oder die Evakuierungstechnik großer Kreuzfahrtschiffe. Eine Gesetzmäßigkeit, sagt Michael Schreckenberg, sei, dass sich Menschen im Knubbel wohl abstoßen, auf längere Distanzen aber anziehen: „das, was man als Herdentrieb bezeichnet, ich laufe den anderen hinterher denn die werden schon wissen, was sie tun, aber dann doch wieder Abstoßung auf engem Raum, die aber dann nicht mehr möglich ist.“

Wenn solche Regeln in den Computer eingespeist werden, lassen sich Muster erkennen. Besonders beeindruckend: Das perfekt simulierbare Schwarmverhalten von Vögeln. Es folgt drei einfachen Regeln: Jeder Vogel, erstens, fliegt so schnell er kann, versucht, zweitens, die schützende Mitte des Schwarms zu erreichen ohne dabei, drittens, mit einem anderen Vogel zusammenzustoßen. Ein Computer kann mit diesen Regeln einen überzeugenden Starenschwarm errechnen.

Auch Menschenmassen bilden Muster, die Betreiber der Kaufhäuser wissen das und gruppieren ihre Waren so,

*Die Kölnarena. Als „Lachende Kölnarena“ war das Gebäude 2003 Schauplatz einer mustergültigen Evakuierung.*

dass beim Schlendern Stimmung aufkommt. Mit Hilfe einer Computersimulation – das Fachgebiet heißt „Fußgänger- und Evakuierungsdynamik“ – gelingt es mittlerweile vermeidbare Staus aufzulösen, etwa vor dem Ausgang eines Stadions. Ungesteuerte Fußgänger neigen dazu, am Ausgang erst einmal Luft zu holen und sich umzusehen, was die Menge dahinter zum Stehen bringt. Eine zusätzliche Säule am Ausgang, die die Sicht versperrt und den Menschenstrom auffächert, ausgerechnet ein zusätzliches Hindernis also, schafft Abhilfe.

Als besonders brisantes Studienobjekt gilt unter Fachleuten die jährliche Pilgerversammlung in Mekka. Die Technische Universität Dresden beschreibt die Situation so:

„Der Koran schreibt vor, dass jeder Muslim mindestens einmal in seinem Leben nach Mekka pilgern soll, um ein genau festgelegtes religiöses Ritual zu absolvieren (Hadsch). Insbesondere müssen drei die Versuchung durch den Teufel symbolisierende Säulen (Jamarahs) mit jeweils sieben Steinen beworfen werden. Die Pilger können dieses Ritual ebenerdig oder auf der Jamarat-Brücke vollziehen. In Spitzenstunden drängen sich auf der 80 Meter breiten Brücke bis zu 200.000 Pilger. Das hat in den vergangenen Jahren wiederholt zu tragischen Unglücken geführt, oft mit über 100 Toten. Beim schwersten Unfall kamen sogar über 1.400 Pilger ums Leben.“

Die Dresdener Wissenschaftler untersuchen jetzt, wie insbesondere der Wurfbereich geometrisch zu gestalten ist, um die Situation zu entschärfen: „Wie wirksam könnte der Druck in der Menschenmenge durch eine Art Wellenbrecher gemindert werden, die entlang der elliptischen Wurfbereiche angebracht sind, sich also der Strömungsrichtung nicht entgegenstellen? Oder wie wirksam wären zickzack- oder schlangenförmige Geländer, die den Druck in der Menge herunterbrechen und so den Betroffenen ‚den Rücken freihalten‘ können?“

Die gewonnenen Erkenntnisse lassen sich natürlich auch auf Fußballstadion anwenden. Auch die Unterhaltungsindustrie profitiert von dieser Art Forschung. Die Orkmassen im Film „Der Herr der Ringe“ wären per Hand nicht zu zeichnen gewesen, sie sind Computergeschöpfe mit einer gewissen Teilautonomie, die sich nach Regeln wie denen des Vogelschwarms bewegen und deshalb so überzeugend sind.

+ Systeme zur Modellierung und automatischen Identifikation sozialer Dynamik.

- Informations- und Kommunikationstechnologie

- + Kommunikationssysteme für Einsatzleitstellen und zur Lageinformation,
- + mobile Endgeräte mit flexiblem Zugriff auf Lage- und Einsatzdaten,
- + Systeme zur Unterdrückung der Funkfernauslösung,
- + gemeinsame semantische Basis für Führungssysteme.

- Handlungsstrategien und Organisationsformen zur Prävention und Reaktion

- + Mobilität und Schnelligkeit logistischer Systeme für die Einsatzkräfte und in der Notfallversorgung,
- + Rolle der Medien bei der Wahrnehmung von Bedrohungen und der Verarbeitung von Krisen,
- + Untersuchung von Panikpotentialen,
- + Konzepte zur Vermittlung von Handlungsperspektiven für Gefährdungs- und Katastrophenlagen,
- + Situationsgerechtes Verhalten nach CBRNE - Angriffen.

*Hochwasser – hier in Baden-Württemberg 2006 – sind in Zukunft häufiger zu erwarten und erfordern eine entsprechende Vorbereitung.*



*Gepäckstücke können Sprengstoff verbergen. Für dessen Detektion werden neue Sensoren gebraucht.*



## Sprengstoffdetektion

Die Botschaft auf der Verkehrsanzeige des Autobahnringes M25 um London herum signalisierte am 7. Juli 2005 etwas Apokalyptisches: AVOID LONDON – AREA CLOSED – TURN ON RADIO. Terroristen hatten in der Rush-Hour ab 8 Uhr 50 morgens in kurzer Folge eine Reihe von Bomben gezündet, die das Verkehrssystem trafen: Vier U-Bahn-Züge und einen Doppeldeckerbus. Die Bomben töteten 52 Reisende und die vier Selbstmordattentäter und legten das Transport- und Kommunikationssystem Londons vorübergehend lahm. Im Schrecken erschreckend: Der Terror kam mittels frei verfügbarer Allerweltssubstanzen zustande, die im Sortiment jedes Damenfriseurs enthalten sind: Nagellackentferner und Haarblondierungsmittel. Aus den darin enthaltenen Chemikalien lässt sich mit bescheidenem Know-How ein hochbrisanter Sprengstoff herstellen, Triacetonperoxid, TATP, der allerdings leicht zur Unzeit detoniert.

Wie auch immer: Die modernen Industriegesellschaften verfügen über eine große Zahl von Substanzen und Techniken, die von entschlossenen Menschen ohne wissenschaftliche Vorkenntnisse zur Inszenierung von Verheerungen, zumindest aber zur Auslösung von Medienschocks, genutzt werden können, und die Zahl der Möglichkeiten nimmt ständig zu. Potentiell gefährliche Stoffe aus dem Verkehr zu ziehen wird nur selten möglich sein, dazu sind – wie z.B. im Falle von Kunstdünger – zu viele unentbehrlich. Jedoch war es gerade ein aus Kunstdünger und einem Treibstoffzusatz für Motoren improvisierter Sprengsatz, der beim Anschlag auf das Murrah Federal Building in Oklahoma City im April 1995 zum Einsatz kam, es gab 168 Tote.

Wenn sich staatliche Sicherheitseinrichtungen auf Bedrohungen dieser Art einrichten sollen, müssen sie auch technisch nachziehen. Die wichtigsten in diesem Zusammenhang neu zu entwickelnden Werkzeuge wären Detektoren, die Sprengstoffe verschiedenster Art unter Kleidern, in Gepäckstücken, in Autos und LKWs usf. entdecken können. Solche Detektoren gibt es teilweise schon, ein besonders raffinierter arbeitet nach dem Prinzip der Röntgenrückstreuung („Z Backscatter“).

Bei dieser Methode scannt ein dünner Röntgenstrahl die verdächtigen Areale ab, während ein großflächiger und damit sehr effizienter Detektor die vom bestrahlten Objekt zurück gestreute Röntgenstrahlung registriert. Mit dem Verfahren kann man auch Objekte erfassen, die nur von einer

Seite aus zugänglich sind und bekommt überdies scharfe Bilder in Echtzeit. Der bislang einzige Hersteller solcher Geräte zeigt im Internet einen Lieferwagen mit dem entsprechenden Equipment, der langsam an einer Reihe parkender Autos vorbeifährt, während ein Beifahrer deren Inhalt auf einem Bildschirm betrachtet. Anders als bei konventionellen Röntgenanlagen scheinen aus leichten Elementen wie Kohlenstoff, Stickstoff und Sauerstoff bestehende Sprengstoffe hell auf, eine Schachtel Pralinen allerdings auch, ebenso Menschen. Bei einem Personenscan sei die Strahlenbelastung vernachlässigbar, versichert der Hersteller. Die Technik eignet sich auch zur Erkennung von im Boden vergrabenen Minen.

Um Sprengstoff im Freien, in einer Menschenmenge ausmachen zu können, sind womöglich spektroskopische Methoden von Vorteil. Heute schon werden bei der Gepäckkontrolle im Flughafen von prinzipiell verdächtigen Teilen wie Notebooks Wischproben genommen; die – in einem Analysegerät erhitzt – Dämpfe abgeben, die auf der Stelle auf Sprengstoffspuren untersucht werden, aber die Prozedur ist ortsgebunden. Anders das kürzlich von der Fachhochschule Düsseldorf und dem Fraunhofer-Institut für Chemische Technologien für den Nachweis des typischen Attentatssprengstoff TATP erkundete Verfahren, das Spuren des Stoffes im Prinzip in der über den Köpfen von Marktbesuchern wabernden Luft ausmachen könnte: Mit der „Fourier-Transformations-InfraRot-Spektroskopie“, FTIR, gelingt die Messung verschiedenster Luftverunreinigungen mit Wärmestrahlung berührungslos auf mehreren hundert Meter langen Messstrecken. So kann auch TATP, das schon unter Zimmertemperatur zu verdampfen beginnt, detektiert werden, aber die Idee benötigt noch viel Forschung und Entwicklung.

Aber wer im Gewühl trägt nun den Sprengstoffgürtel? Das wird sich künftig mit elektromagnetischer Strahlung aus dem technisch bislang unerschlossenen Frequenzbereich zwischen Mikrowelle (Herd) und Infrarot (Fernbedienung), mit sogenannter Terahertz-Strahlung feststellen lassen. Ein Terahertz-„Radar“ kann unter die Kleidung sehen und sogar Keramikmesser entdecken, die sich den Metallsuchgeräten entziehen. Ein entsprechend ausgefeiltes Gerät könnte aus der Distanz sogar eine Art chemischer Analyse vornehmen. Die Strahlung ist nicht-ionisierend und damit ungefährlich.

## Schutz von Verkehrsinfrastrukturen

Die Verkehrswege einer modernen Gesellschaft – Straße, Schiene, Luft und Wasser – können ohne Übertreibung als deren Lebensadern bezeichnet werden. Ihre Nutzung ist mittlerweile so fein austariert, dass kleine Störungen weiträumige Beeinträchtigungen und erhebliche Schäden hinterlassen können. Ihre Blockade kann in eine Katastrophe münden und Gesellschaft und Wirtschaft destabilisieren. Die Knotenpunkte der Verkehrssysteme – zum Beispiel Flughäfen, Bahnhöfe, eingedeichte Flüsse und Kanäle, Brücken, Tunnel, Hochgeschwindigkeitsstrecken – sind besonders verletzlich. Der Schutz dieser neuralgischen Stellen ist lebenswichtig. Weiter sind in einer Industriegesellschaft große Mengen potentiell gefährlicher Rohstoffe und kleinere Mengen tatsächlich giftiger Chemikalien unterwegs. Attacken auf solche Transporte – in Städten, auf Brücken, in Tunneln – könnten verheerende Folgen haben. Die schnelle und einfache Analyse der beteiligten Stoffe kann hier über Leben und Tod entscheiden. Daher sind innovative Lösungen für die Sicherung von Verkehrsinfrastrukturen ein besonders wichtiges Ziel der Sicherheitsforschung. Schwerpunkte sind: Prävention, Früherkennung, Redundanzhöhung (Funktionsfähigkeit auch in möglichen Krisenlagen) sowie die Erhöhung der Leistungsfähigkeit der Rettungskräfte im Krisenfall. Die Sicherheitslösungen sollen Wirtschaftlichkeit, Nutzer- und Kundenfreundlichkeit, das Einbeziehen individueller und kollektiver Verhaltensweisen sowie rechtliche Aspekte berücksichtigen.

### Relevante Forschungsthemen:

- Sensorik, Detektion und Robotik

- + Automatische Zugangskontrollen mit integrierten biometrischen Systemen,
- + massensensorgestützte Überwachung von Verkehrssystemen (z.B. für Gefahrguttransporte),
- + Roboter zur Überwachung und zur Gefahrenbekämpfung,
- + automatische Erkennung sicherheitskritischen Verhaltens system- und personenbezogen,





*Deutschland verfügt über eine dichte Verkehrsinfrastruktur, darunter ca. 232 Tausend Kilometer überörtliche Straßen (mehr als die Hälfte der Entfernung zum Mond), 44 Tausend Kilometer Schiene (mehr als der Erdumfang) und 7,5 Tausend Kilometer Wasserstraßen. Durch die Luft über Deutschland werden jährlich 150 Millionen Personen befördert (Quelle: Statistisches Bundesamt). Der Schutz so umfangreicher Infrastrukturen vor den neuen Bedrohungen ist ohne neue Techniken nicht möglich.*

- Simulation, Mustererkennung und Datenerfassung

- + Modellierung von Schädigungen (z.B. zur Brandausbreitung),
- + Simulationsunterstützte Risikoanalysen für Entscheidungsfindungen,

- + Frühwarnsysteme mit Echtzeit-Datenübermittlung,
- + einbeziehen des „Faktors Mensch“ in Simulation und Modellierung.

- Informations- und Kommunikationstechnologie

- + Interoperable IKT-Systeme zur flächendeckenden Überwachung und Sicherung,
- + Simulationssoftware-Lösungen für Krisenübungen.

- Strategien zur Erhöhung der Robustheit von Systemen, Verfahren und Prozessen

- + Bauliche Maßnahmen und sicherheitsbegünstigende Architektur,

- + Mensch-Maschine-Schnittstellen bei Detektions- und Überwachungssystemen,
- + Abschirmung elektronischer Geräte gegen elektromagnetische Felder.

- Handlungsstrategien und Organisationsformen zur Prävention und Reaktion

- + Vernetzte Krisenmanagementsysteme,
- + diskriminierungsfreie Personenkontrollverfahren,

- + Konzepte krisenbezogener Öffentlichkeitsarbeit,
- + Konzepte zur Bürgerbeteiligung bei Krisenprävention und -reaktion.

*Bild unten: Container im Hamburger Hafen. 2004 wurden in deutschen Häfen über 11 Millionen Standard-Container umgeschlagen; das jährliche Wachstum liegt bei 30% (Quelle: Statistisches Bundesamt).*





### Falsch gefühlte Sicherheit – wie sicher ist sicher?

Die Schlüsselübergabe beim Autoverleiher in Valetta, Malta – unvergesslich. Auf die Frage, welche Regeln hier denn außer Linksfahren noch einzuhalten seien, Vorfahrt und so, reißt der Mann beschwörend die Augen auf und schreit mit ausgebreiteten Armen „No rules, absolutely no rules!“ Wenn man nicht weiter wüsste, sollte man einfach anhalten. Was sich so witzig anhört – Südländer eben – ist als Konzept jetzt auch im Norden angekommen. In der niedersächsischen Gemeinde Bohmte wird der Ortskern von Hans Modermann neu gestaltet, einem Niederländer, der nur noch zwei Regeln gelten lassen will: Das Rechtsfahrgebot und die Vorfahrtsregelung „rechts vor links“ (eine Regel mehr als Malta, als Zugeständnis an den Norden). Bohmte hat das Konzept des „shared space“ neu entdeckt, bei dem sich der Verkehr durch die Ungewissheiten der bunt gemischten Teilnehmer so weit verlangsamt, dass sich die Leute in die Augen sehen können. Das reicht, sich zu verständigen. Die Unfallzahlen gehen herunter, die Schilder sind weg, die Leute atmen auf. In einem EU-Projekt werden jetzt sieben europäische Städte das Konzept „mehr Sicherheit durch mehr Unsicherheit“ erproben.

Die Sozial- und Geisteswissenschaften können Modermanns Erfahrungen bestätigen. So existiert – von Individuum zu Individuum verschieden – offenbar eine Risikogrenze, an der man sich unbewusst bewegt. Der durch die Einführung von technischen Systemen erzielte Sicherheitsgewinn wird dadurch nicht selten durch riskanteres Verhalten wieder wettgemacht, der Fachausdruck dafür heißt Risikohomöostase oder „Die Summe aller Laster bleibt gleich“. Umgekehrt erzeugen verstärkt wahrgenommene Risiken ein vorsichtigeres Verhalten.

Dass ein Zuviel an Sicherheitsbemühungen kontraproduktiv sein kann, hat eine tiefenpsychologische Pilotstudie jetzt auch für IT-Arbeitsplätze herausgefunden. Mit einem Computernetzwerk, das absolut dicht hält, verhalte es sich wie mit einem absolut dichten Neubau, kommentiert ein Kundiger. Wenn durch den kein Lüftchen weht, beginnt sich Schimmel zu bilden. Gemeint ist, dass ein Zuviel an Sicherheitsstreben, etwa die ständige Kontrolle des Computerinhalts durch Vorgesetzte oder auch nur die Möglichkeit dazu, die Leute demotiviert.

Versicherungsfachleute wie Rudolf Kreutzer vom Allianz Zentrum für Technik GmbH bestätigen die Regel: „Wer bessere Bremsen hat, fährt dichter auf“. Und: „Der Schutz vor einer Gefahrenquelle muss [...] nicht immer bedeuten, dass die Gefahr langfristig kleiner bleibt. So bewirkt der Bau von Hochwasserdeichen an Flussufern zwar die Senkung der Schadenshäufigkeit. Danach werden aber die vom Wasser mitgeführten Schwemmmaterialien konzentriert im Flussbett abgelagert. Damit erhöht sich der Wasserspiegel, so dass eine laufende Erhöhung der Deiche notwendig wird und das potentielle Risiko hinsichtlich seiner möglichen Schadenshöhe ständig steigt. Dieses konnte in den letzten spektakulären Hochwasserkatastrophen an Oder, Elbe, Po und Mississippi erlebt werden und ist zukünftig auch an Rhein, Donau oder Inn usw. zu erwarten.“

Die Risikowahrnehmung der Allgemeinheit spielt gelegentlich tatsächlich ins Irrationale, gespeist auch vom Zwang der Medien, interessantes Neues liefern zu müssen. So fanden sich bei der letzten BSE-Krise Menschen, die selbst vor Milch und Käse panisch zurückschreckten, aber seelenruhig weiter rauchten. Das Raucherrisiko ist bekanntermaßen groß, aber vertraut, das BSE-Risiko war unbestimmt, aber neu.

### Schutz vor Ausfall von Versorgungsinfrastrukturen

Die Versorgung der Haushalte, Unternehmen und öffentlichen Einrichtungen mit Energie, Wasser, Information und Kommunikation, Finanz- und Gesundheitsdienstleistungen sowie Lebensmitteln stützt sich auf verzweigte, teils europaweit vernetzte Infrastrukturen. Die Versorgungsinfrastrukturen werden immer komplexer, sind immer stärker wechselseitig durchdrungen und voneinander abhängig. Die Störung eines zentralen Infrastrukturelementes, etwa eines Netzknotens, kann über Kaskadeneffekte eine Vielzahl von Menschen auch über Landesgrenzen hinaus treffen. Sein Ausfall kann nach Art eines Dominoeffektes weitere Infrastrukturen in Mitleidenschaft ziehen. Elektrizität ist das Lebenselixier der Moderne und zugleich ihre Achillesferse. Ein lang andauernder Ausfall der Stromversorgung hätte katastrophale Folgen. Die Bahn käme ebenso zum Stillstand wie der Flugverkehr, und auch die Autos würden nicht mehr lange fahren: Ohne Strom funktioniert keine Tankstelle. Sogar die Stromerzeugung selbst könnte dauerhafte Schäden erleiden. Die Kommunikationsnetze würden versagen, das Internet, die Gaspipelines würden kein Gas mehr transportieren und die Gasheizungen in den Haushalten selbst bei intakter Gasversorgung nicht mehr heizen, Kühllhäuser nicht mehr kühlen – nichts ginge mehr. Der Ausfall einer Versorgungsinfrastruktur kann verschiedene Ursachen haben: Gezielte Terroranschläge, kriminelle Handlungen, Industrieunfälle oder Naturkatastrophen wie Erdbeben, Flutkatastrophen, Orkane, starke Schneefälle u.a.). Weil die Netze eine enorme Ausdehnung haben, muss der Schutz wichtiger Infrastrukturen dort ansetzen, wo durch mehrseitige Abhängigkeiten besonders hohe Schäden auftreten können.

Aus der großen Zahl der möglichen Störfaktoren wird deutlich, dass zum Schutz der Versorgungsinfrastrukturen ein großes Spektrum verschiedener Technologien und Handlungsstrategien erforderlich ist. Dabei reicht ein Mehr des Üblichen nicht, es sind echte Innovationen erforderlich. Die Bemühungen um einen Schutz der öffentlichen Sicherheit vor Terrorismus und Kriminalität werden sich schon deshalb bezahlt machen, weil sie zugleich die Stabilität des Gemeinwesens gegenüber Natur- und Unfallkatastrophen verbessern.

In diesem Zusammenhang spielt die Erhöhung der IKT-Sicherheit eine wichtige Rolle. Die Sicherheit aller Infrastrukturen – nicht nur der IKT-Infrastrukturen Telefon, Internet,

Kabel und Funk selbst – ist zunehmend abhängig von der Sicherheit der Informations- und Kommunikationstechnik. Daraus leiten sich besondere Forschungsaufgaben ab. Es muss Vorsorge getroffen werden, dass etwa das erwartete Vordringen der Internettechnologien in Bereiche außerhalb der Kommunikationstechnik, zum Beispiel in Prozessleitsysteme und Finanzsysteme, nicht zu einer neuen Art der Verletzlichkeit führt. Da das Internet eine eigene Versorgungsinfrastruktur mit zunehmender Bedeutung darstellt, muss es besonders vor Anschlägen geschützt werden, bei denen sein Ausfall destabilisierend auf Gesellschaft oder Wirtschaft wirkt. Ziele der Sicherheitsforschung in diesem Szenario sind die Prävention, Früherkennung, Entkopplung und intelligente Bereitstellung von Notfallreserven, die Sicherstellung einer Grundversorgung im Krisenfall und die schnelle Wiederherstellung des ursprünglichen Versorgungszustandes.

*Europa bei Nacht. Das Licht zeichnet die Besiedelungsdichte nach und illuminiert die europaweite Vernetzung.*



*Stromnetze sind die Lebensadern der Industriegesellschaft, ihr reibungsloses Funktionieren ist lebensnotwendig. Achtzig Prozent dieser Art Infrastruktur werden privat betrieben.*





*Schaltzentrum Deutsche Telekom AG. Kommunikationsknotenpunkte wie dieser benötigen besonderen Schutz.*

**Relevante Forschungsthemen:**

- Sensorik, Detektion und Robotik

- + Mobile autonome Multisensorplattformen und Low-Power-Sensorik,
- + verteilte Sensornetzwerke, drahtlose Sensorsysteme, und robuste Sensoriksoftware zur großflächigen Überwachung,
- + systematische Zustandserfassung von Faktoren, die zum flächendeckenden Ausfall von Versorgungsstrukturen führen können,
- + standardisierte interoperable Trägersysteme (z.B. Roboter, unbemannte Flugzeuge, Satelliten).

- Simulation, Mustererkennung und Datenerfassung

- + Nutzung von Geoinformationssystemen für die Erstellung eines „Gefährdungsatlas“,
- + Modellierung von Schadensszenarien, insbesondere von IT-Risikoprofilen,
- + Werkzeuge zur fortlaufenden systematischen Erfassung der Sicherheitslage,
- + systematische Risikoanalyse und Risikobewertung zur Schadensvorhersage,
- + Frühwarnsysteme integriert in kritischen Infrastrukturen,
- + automatischer Lagebildaustausch.

- Informations- und Kommunikationstechnologie

- + Robuste Prozesssteuerungssysteme und entsprechende Testwerkzeuge,
- + Ad-hoc-Netze für Katastrophen- und Notfallmanagement
- + sichere Basis-Plattformen und Betriebssysteme für Prozessleittechnik.

- Strategien zur Erhöhung der Robustheit von Systemen, Verfahren und Prozessen

- + Erforschung von Interdependenzen und systematische Verwundbarkeitsanalysen,
- + Ausfallplanung und Ausfallmanagement,
- + Managementsysteme zur Entscheidungsunterstützung im Krisenfall.

- Handlungsstrategien und Organisationsformen zur Prävention und Reaktion

- + Verbesserte Methoden zur Koordination von Zuständigkeiten,
- + Wechselwirkung von neuen Technologien und Organisationsstrukturen,
- + Analyse künftiger Verwundbarkeit von sicherheitsrelevanten Infrastrukturen,



### Schutz vor Kaskadeneffekten

Ein wesentliches Element für das Versagen komplexer Systeme lässt sich in jeder Kantine studieren, man muss sie lediglich mit einer randvollen Tasse Kaffee und dem eisernen Vorsatz durchqueren, nichts zu verschütten. Wer dabei seinen Blick auf den Kaffeespiegel heftet, wird versucht sein, jedes Schwappen durch eine Gegenbewegung auszugleichen, und das geht bei vielen schief: Fällt die Gegenbewegung nur ein bisschen zu energisch aus, schwappt der Kaffee stärker, wird die Gegenbewegung heftiger – die Hand kommt ins Flattern, der Kaffee schwappt über. Fachsprachlich ist das System Mensch/Kaffeetasse einer Selbsterregung durch positive Rückkopplung zum Opfer gefallen. Vordergründige Ursache kann eine winzige Störung gewesen sein, der Hintergrund ist natürlich: Die Tasse war zu voll.

Ähnliche Mechanismen, das Aufschaukeln von Störungen in einem Netz am Rande seiner Leistungsfähigkeit, darf man als Ursache für viele Blackouts vermuten, wie auch den europaweiten Stromausfall am Abend des 4. November 2006, der Millionen von Europäern betraf. Der oberflächliche Anlass war die Passage des von der Meyer-Werft kommenden Kreuzfahrtschiffes „Norwegian Pearl“ unter zwei Hochspannungsleitungen, die für diesen Zweck vorübergehend ausgeschaltet wurden. Die Last wurde automatisch von anderen Leitungen übernommen, deren Sensorik allerdings Überlast meldete, was zum automatischen Abschalten auch dieser Leitungen führte und so weiter. Nach 30 Minuten war der Strom wieder da. Das verantwortliche Unternehmen machte Versäumnisse zweier Mitarbeiter geltend, die sich der Folgen des Abschaltens der Leitungen über der „Norwegian Pearl“ vorher mittels einer Computersimulation hätten vergewissern müssen, was sie nicht taten. Allerdings hätten diese Leitungen auch aus anderen, unvorhersehbaren Gründen ausfallen können, was im Normalfall nicht zum Zusammenbruch des Systems führen dürfte.

Die Industrienationen sind mittlerweile in einem beunruhigenden Maße von der durchgängigen Verfügbarkeit elektrischer Energie abhängig. Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, BBK, schreibt:

„Ohne elektrischen Strom sind die Großstädte und Metropolregionen moderner Gesellschaften schlagartig lahm gelegt, da fast jede Infrastruktur direkt oder indirekt von der Verfügbarkeit dieser Energie abhängt. Auch extrem kurze

*Für die Versorgung einer Großstadt wie Berlin ist ein riesiges Netzwerk an Infrastruktur notwendig.*

Ausfälle können bereits heftige Auswirkungen auf andere Infrastrukturen, wie beispielsweise der Elektronischen Datenverarbeitung (Computerabstürze), die Verkehrsregelung (Ampelsteuerung) und andere sensible elektronische Systeme haben.“

Auch der moderne Privathaushalt würde von einem länger andauernden Stromausfall schwer getroffen:

„Ohne Strom geht in vielen Haushalten nichts mehr. Im schlimmsten Fall heißt dies: es gibt kein Licht, keine Heizung, kein warmes Wasser, keine Kochmöglichkeit und keine Informations- bzw. Kommunikationsmöglichkeit via Fernsehen, Radio, Telefon oder Computer.“

Störungen des elektrischen Netzes können sich auch in hochsensible Anlagen wie Kernkraftwerke vorarbeiten. Am 25.7.2006 hatte ein Kurzschluss in einer Freiluftschaltanlage vor dem schwedischen Kernkraftwerk Forsmark 1 die automatische Trennung der Anlage vom Hauptnetz zur Folge. Die Umschaltung auf die schließlich erforderliche Notstromversorgung funktionierte nicht planmäßig. Zwei Dieselnostromaggregate sprangen nicht an, weil – so darf man einen Bericht der Gesellschaft für Reaktorsicherheit interpretieren – deren Regeleinheiten von eben den ausgefallenen Stromquellen gespeist wurden, deren Ausfall sie kompensieren sollten. Eine Gashilfsturbine versagte ihren Dienst, weil ein Prozessor defekt war. In der Maschinenhalle trat Dampf aus, der von Rauchmeldern als Rauch interpretiert wurde, was die Zentrale zu Evakuierungsbefehlen veranlasste. Die konnten nicht ans Ziel kommen, weil die Lautsprecheranlage ausgefallen war usf. Dank einer fähigen Bedienungsmannschaft und Glück kam die Anlage wieder unter Kontrolle.

Der Schutz des Stromnetzes ist mithin von höchster Bedeutung. In den USA werden Strommasten mittlerweile mit drahtlosen Störungsmeldern ausgestattet, die über Sensoren für Strom, Temperatur und Luftfeuchte verfügen, und eine kleine Kamera mit einer Software, die große, plötzliche Bewegungen meldet. Der Hauptsinn ist der Schutz des 240.000 Kilometer langen Leitungsnetzes der USA gegen Terrorangriffe. Sinnvoll wäre zweifellos auch eine weitere Erhöhung der Redundanz und eine Erweiterung der Kapazitäten. Denkbar ist auch, dass die Versorgungsnetze unter der Last der Terrordrohung eine andere, weniger verletzliche Form annehmen.

## Sicherung der Warenketten

Eine sichere Warenproduktion, sichere Warentransporte und die Gewährleistung der Integrität von Waren sind für Gesellschaft und Wirtschaft unverzichtbar. Terroristische Attacken könnten das System an vielen Stellen treffen. Die Unterbrechung von Warenlieferungen kann in kürzester Zeit erhebliche wirtschaftliche Schäden verursachen und zum Zusammenbrechen von Unternehmen führen. Auch die Fälschung, Kontamination oder Zweckentfremdung der Waren selbst kann das gesellschaftliche und wirtschaftliche Leben erheblich stören. Eine Beeinträchtigung z.B. der Lebensmittel- oder Medikamentenversorgung kann Auswirkungen auf jeden Bürger und jede Bürgerin haben. Die Sicherung der Warenketten ist für den Export- und Logistikstandort Deutschland von immer größerer Bedeutung. Die Transport-

*Zur lückenlosen Überwachung von Spenderblut hat Siemens zusammen mit Partnern eine umfassende Lösung auf der Basis von RFID entwickelt. Mit der Identifizierung über die Funkchips ist ein Verwechseln von Blutkonserven nahezu ausgeschlossen.*



behälter (zum Beispiel Briefe, Pakete, Kisten, Container, Tanks) können für Anschläge oder kriminelle Absichten missbraucht werden. Das Spektrum für Einzelszenarien ist sehr groß. Mit Verpackungen und Behältern lassen sich verbotene Handlungen vertuschen, Angriffe tarnen und illegale Objekte international verschieben. Produktionsanlagen können gezielt zerstört oder manipuliert werden. In den Warenströmen reisen auch Güter mit, deren Manipulation oder Diebstahl zu einer großen Gefahr werden könnte. Dabei kommt den großen Containertransportsystemen und Logistikzentren eine hohe Bedeutung zu. Innovative Lösungen für deren Sicherheit haben daher für die Sicherung der Warenketten eine herausragende Bedeutung. Ziele der Sicherheitsforschung in diesem Szenario sind die Prävention, die Früherkennung von Bedrohungen ohne Störung oder Verlangsamung des Wirtschaftsverkehrs und die Erhöhung der Leistungsfähigkeit der Einsatzkräfte im Krisenfall sowie die Schadensminimierung.

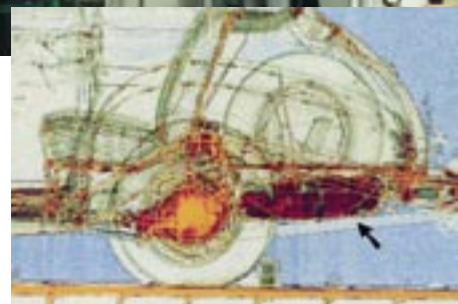
### Relevante Forschungsthemen:

#### - Sensorik und Detektion

- + **Mobile Durchleuchtungsgeräte (z.B. Containerscreening)**
- + **Massensensorsysteme zur Detektion von Schad- und Gefahrenstoffen,**
- + **Nachverfolgung von Gütern über Sensortechnik (auch RFID- und satellitengestützt),**
- + **Hochdurchsatzdetektion.**

*Güteridentifizierung und -verfolgung in der Logistikkette. Dabei werden Daten zwischen dem Objekt und dem RFID-Lesegerät (Siemens AG) ausgetauscht. Um zu vermeiden, dass die ausgetauschten Daten abgehört und manipuliert werden können, sind effektive Sicherheitsmaßnahmen nötig.*





- Simulation, Mustererkennung und Datenerfassung

- + Bildgebende Verfahren,
- + Integration kostengünstiger Überwachungssysteme in Transportcontainern.

- Informations- und Kommunikationstechnologie

- + Integrierte Sicherheitsmerkmale in IKT-Systemen der Logistik,
- + energieeffiziente kryptographische Verfahren für mobile Systeme,
- + sichere elektronische Schlüssel (Token) zum Schutz wichtiger Daten.

- Strategien zur Erhöhung der Robustheit von Systemen, Verfahren und Prozessen

- + Kunden- und Nutzerorientierte Sicherheitsmerkmale und -systeme in Verbindung mit der Qualifizierung der Nutzer,
- + Strategien zur sicheren Koordination von Geschäftsprozessen,
- + Interdependenzen und systematische Verwundbarkeitsanalysen für Schlüsselkomponenten und -produktionen,
- + Ausfallplanung und Ausfallmanagement.

*Mobiles Röntgendurchstrahlungsgerät (oben)*

*Unten: Auch der Zoll im Hamburger Hafen ist mit Container-Röntgengeräten ausgestattet. Das Röntgenbild zeigt einen Oldtimer mit Rauschgift im Tank, in einem Container auf einem LKW.*

- Handlungsstrategien und Organisationsformen zur Prävention und Reaktion

- + Lösungen aus dem Gefahrgutsektor für allgemeine Warentransporte erschließen,
- + Sicherheitskultur im betrieblichen Umfeld,
- + Kosten-Nutzen-Analysen unter Einbeziehung von Haftungsfolgen und Versicherungslasten,
- + präventive Analysen zur Verbreitung von Gefahr- und Kampfstoffen,
- + Modellierung von Schadenslagen zur Aufdeckung von strukturellen und organisatorischen Defiziten.

# Technologieverbünde

## Integrierte Schutzsysteme für Rettungs- und Sicherheitskräfte

Vor dem Hintergrund wachsender Bedrohungspotenziale durch Terrorismus, Natur- und technische Katastrophen, aber auch durch die Zunahme integrierter Einsätze verschiedener Einsatzkräfte, hat sich das Aufgaben- und Einsatzspektrum des Zivil- und Katastrophenschutzes und der Polizei deutlich erweitert. Insbesondere die Ersteinsatzkräfte sind bei der Bekämpfung und Bewältigung katastrophen- oder terror-



Übung mit ABC-Schutzanzügen

bedingter Schadensereignisse mit neuen kommunikativen und organisatorischen Herausforderungen konfrontiert und sehen sich erhöhten psychischen und körperlichen Belastungen ausgesetzt. Ausgehend von dieser veränderten Bedrohungslage wird die Entwicklung integrierter Schutzsysteme, Ausrüstungen und organisatorischer Maßnahmen gefördert, die die Leistungsfähigkeit und Sicherheit der Ersteinsatzkräfte auf Dauer verbessern. Dabei besteht insbesondere Bedarf an zuverlässigen, sicheren und kompatiblen Technologien und Instrumenten für die Kommunikation und Koordination sowie an Ausrüstungen und Hilfsmitteln zum Schutz vor Kampf- oder Schadstoffen. Bei der Entwicklung von leistungsfähigen und robusten Sicherheitssystemen sind insbesondere die Themen Nutzerfreundlichkeit und Mensch-Maschine-Schnittstellen zu berücksichtigen.

Helmmontierte  
Wärmebildkamera mit  
Head-Up-Display und  
Anschluss an Digital-  
funkgerät

Helmintegrierte Hör-/Sprech-  
garnitur für Digitalfunk

Peilsender mit  
Anschluss an Digi-  
talfunkgerät

Digitalfunkgerät (wird  
in Brusttasche getra-  
gen und über große  
Sprechtaste mit Hand-  
schuhen bedient)

Atemschutzüber-  
wachungsgerät-  
mit Anschluss an  
Pressluftatmer und  
Digitalfunkgerät

Schutzanzug der  
EADS Werkfeuerwehr

Das Mehr an Technik darf nicht zu Lasten der Praktikabilität gehen.

*Das World Trade Center nach dem Angriff. Die überraschend große Zahl Überlebender war auch dem selbstlosen Einsatz der Sicherheits- und Rettungskräfte zu danken.*



## Feuerwehr der Zukunft

Am 11. September 2001 wurde gegen 8 Uhr 45 ein voll mit Treibstoff betanktes Flugzeug samt Passagieren von Terroristen in den Nordturm des New Yorker World Trade Center gesteuert, eine Viertelstunde später schlug ein zweites Flugzeug in den Südturm ein. Während der Evakuierungs- und Rettungsarbeiten brachen beide 110-stöckigen Türme zusammen. Etwa 3.000 Menschen verloren ihr Leben, darunter 450 Rettungs- und Sicherheitskräfte.

Die an den Rettungsaktionen Beteiligten wurden – völlig zu Recht – als Helden gefeiert. Erst später fanden Fachleute die Ruhe, herauszufinden, was alles falsch gelaufen war. Das war, wie eine Studie der RAND Corporation öffentlich machte, eine Menge:

Das unmittelbar nach den Terrorangriffen verhängte Flugverbot für alle kommerziellen Flugzeuge hatte zur Folge, dass auch dringend benötigtes Material und Spezialteams nicht eingeflogen werden konnten.

Die Kommunikation war anfänglich katastrophal. Die Mobilfunkanlage für den betroffenen Teil Manhattans hatte sich auf dem Dach des World Trade Center befunden und war mit diesem in die Tiefe gesunken; das Festnetz war ebenfalls demoliert, weil Trümmer der zusammenbrechenden Türme einen Netzknoten getroffen hatten. Die verbliebenen Leitungen waren durch massenhafte Telefonate blockiert.

Die Ausrüstungsteile der Rettungsteams waren nicht immer austauschbar, was etwa die Versorgung mit Atemluftfiltern schwierig machte; die Ausrüstungen der Feuerwehr waren größtenteils nicht für Katastrophen ausgelegt, die einen mehrstündigen Einsatz erforderlich machen, infolgedessen rissen sich die Feuerleute nach einiger Zeit die schweren Helme vom Kopf, so oft sie es konnten. Die Atemschutzmasken schränkten häufig die Sicht zu stark ein, als „beschlagsfrei“ ausgezeichnete Visiere erblindeten im schweißtreibenden Inferno und die akustische Kommunikation, gerufene Kommandos und Warnungen, war so schlecht, dass sich die Männer vereinzelt die Filter von den Masken schraubten. Schließlich hielt selbst schweres Schuhwerk der Hitze des Bodens nicht immer stand, Sohlen schmolzen. An diesen Schwierigkeiten gemessen war die Leistung der Beteiligten nur noch höher einzustufen.

Sicherheitsforscher in aller Welt haben die Lehren aus 9/11 aufmerksam zur Kenntnis genommen. Dem „Feuerwehrmann der Zukunft“, wie ihn sich ein europäischer Techno-

logiekonzern vorstellt, sollte ein großer Teil der in Manhattan zutage getretenen Schwierigkeiten und Gefahren erspart bleiben können: Schutzanzüge aus neuen Materialien ermöglichten einen besseren Schutz vor Feuer, Hitze und mechanischen Verletzungen und böten zugleich einen höheren Tragekomfort. Eine helmmontierte Wärmebildkamera mit Headup-Display würde dem Feuerwehrmann und zugleich der Einsatzleitung ein besseres, dokumentierbares Bild der Gefahrenlage zeigen, etwa vor glühend heißen Teilen warnen. Die Rettungskräfte könnten vor Ort kleine Sende- und Empfangsgeräte verstreuen, die sich selbsttätig zu einem Funknetzwerk zusammenschließen. Das würde der Mann vor Ort mit einem robusten Digitalfunkgerät in der Brusttasche nutzen, das Dank großer Tasten auch mit Handschuhen bedienbar wäre und eine sichere Sprachverbindung zum Trupp, zum Einsatzleiter und zur Leitstelle sicherstellte. Eine ergänzende Spracherkennungsfunktion würde gegebenenfalls die Hände freihalten. Die Verständigung mit den Kollegen über Funk wäre auch bei aufgesetzter Atemmaske problemlos möglich. Die Versorgung mit Pressluft würde elektronisch exakt überwacht und gemanagt. Die verstreuten Sende- und Empfangseinheiten könnten auch als autonome Peilsender dienen und außerdem Sensoren enthalten, die über die aktuelle Gefahrenlage (z.B. Temperaturen) Auskunft geben und in Verbindung mit einem Satellitenpositionierungssystem die Rekonstruktion virtueller Gefahrenräume für den Mann vor Ort gestatten.

Die „Feuerwehr der Zukunft“ wird die Sicherheitsforschung lange beschäftigen. Womöglich ersetzt sie auch das vertraute „Tatü, Tata“ der Löschfahrzeuge, denn deren Sirene ist für Autofahrer zwar leicht zu hören, aber schwer zu orten, so dass es an Kreuzungen immer wieder zu Unfällen kommt. Besser, versichern die Akustiker, sei eine Aufmerksamkeit erregende Tonfolge, die in kurzen Abständen von Rauschimpulsen unterbrochen wird, deren Herkunft für das Ohr gut zu orten ist. Versuche mit solchen Sirenen haben gezeigt, dass sich die Unfallstatistik damit deutlich verbessern lässt. Die Evakuierungszeiten für Schiffskonstruktionen, deren Ausgänge so akustisch „markiert“ wurden, sind in Versuchen um 70% geschrumpft. In den Parkhäusern des Flughafens München sorgen bereits solche „Sound Alert“-Rauschimpulsgeneratoren für mehr Sicherheit. Im Falle eines Brandes sind die Generatoren auch durch dichten Rauch zu orten und überdies für Passagiere jeder Nationalität zu verstehen.

#### Relevante Forschungsthemen:

- + **Medizinische Überwachung durch Sensoren im Einsatz,**
- + **Funktionskleidung für Rettungskräfte mit integrierter Sensor- und Kommunikationstechnik,**
- + **Ortungs- und Navigationssysteme,**
- + **Digitale Kommunikationssysteme für Rettungs- und Sicherheitskräfte,**
- + **Vernetzte Melde-, Warn- und Informationssysteme,**
- + **Service-Roboter für Aufklärung, Hilfe und gefährliche Situationen,**
- + **Innovative ABC-Schutzlösungen,**
- + **Wirkung psychologischer Faktoren und Zusammenwirken von neuen Technologien und Einsatzbedingungen.**

#### Multi-Sensorsysteme für CBRNE-Gefahren

Die Gefahr des Missbrauchs chemischer, biologischer, radioaktiver, nuklearer oder explosiver Schad- und Gefahrstoffe (CBRNE-Stoffe) nimmt zu, da diese Stoffe immer leichter verfügbar sind. Informationen zum Bauen von Waffen, aber auch Bestandteile von Waffen können z.B. über das Internet erworben werden. Die wichtigste technische Voraussetzung für umfassende präventive wie reaktive Schutzmaßnahmen sind hochempfindliche Detektorsysteme für das Aufspüren von CBRNE-Stoffen aller Art. Das Bedrohungsspektrum reicht vom terroristischen Einsatz nicht-konventioneller Sprengstoffe über die Gefahr einer großflächigen Verseuchung der landwirtschaftlichen Produktion und die Beeinträchtigung der Lebensmittel- und Trinkwasserversorgung bis hin zum Einsatz so genannter „Schmutziger Bomben“, die mit konventionellen Sprengstoffen radioaktives Material freisetzen. Das frühzeitige Erkennen und die damit einhergehende Eindämmung derartiger Bedrohungen erfordert sowohl die Entwicklung neuer Sensorkonzepte als auch neuer Scanner- bzw. Durchleuchtungstechnologien mit eingebetteten

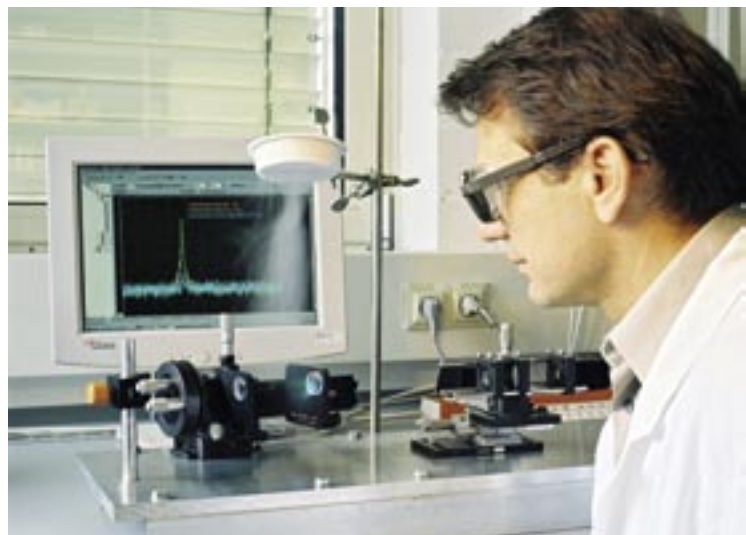
*Bild rechts: Forscher der EADS in München haben auf der Basis eines Ionenmobilitätsspektrometers einen neuartigen Sensor entwickelt (hier ein Laboraufbau), der Drogen und Sprengstoff 30 mal empfindlicher als eine Hundesnase erschnüffelt. Mit der künstlichen Spürnase sollen Flugreisen sicherer und die Polizeiarbeit effektiver werden.*



*RFID-Etiketten machen den Warenumsatz schneller und vor allem sicherer. Für Waren mit hohem Wassergehalt, der die Funksignale stören könnte, kommen Flag-Tags zum Einsatz: Der Transponder steht bei Flag-Tags wie ein kleiner Wimpel von der Verpackung ab.*

oder mobilen Spuren- bzw. Volumendetektoren. Ziel ist die Schaffung von Frühwarnsystemen, die z.B. bei Personen-, Gepäck- oder Güterkontrollen CBRNE-Anschläge verhindern helfen oder die im Krisenfall durch eine frühzeitige Detektion von Kampfstoffen zeitnah die Einleitung von Rettungs- bzw. Evakuierungsmaßnahmen ermöglichen.

Vor diesem Hintergrund sollen in dem Querschnittsthema „Multi-Sensorsysteme für CBRNE-Gefahren“ vorzugsweise



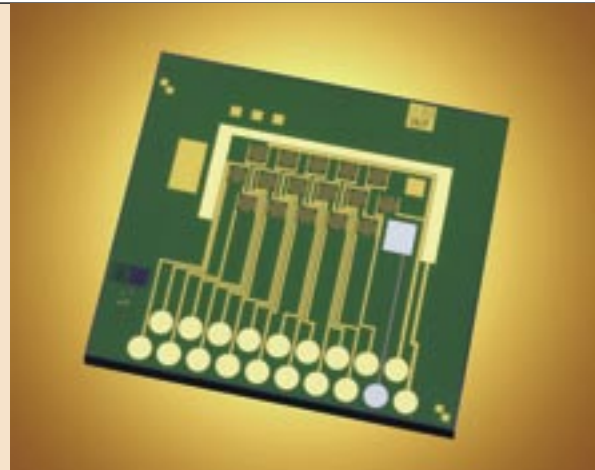
## Nanotechnologien gegen Bioterror

Mit „Grippe“ verbinden die meisten Menschen nur Schnupfen, Husten, Heiserkeit. Das trifft meist auch zu, es gibt allerdings auch sehr aggressive Varianten. Die sogenannte „Spanische Grippe“ von 1918 tötete zwischen 1918 und 1919 2,5 Prozent aller Infizierten, darunter besonders viele jüngere Menschen. Manche Historiker sehen in der Epidemie einen wesentlichen Grund für das Ende des Ersten Weltkrieges. In den USA sank die durchschnittliche Lebenserwartung in der Folge um zehn Jahre. Beunruhigend: Das tödliche Virus von damals lässt sich gentechnisch weitgehend rekonstruieren, was von einer amerikanischen Militärforscherguppe vor wenigen Jahren unter Beweis gestellt wurde. Seither werden erhebliche Mittel für die Entwicklung von Strategien gegen einen Einsatz von Grippeviren als biologische Waffe ausgegeben.

Gefahren dieser Art können nur dann erfolgreich bekämpft werden, wenn sie schnell und präzise genug beschreibbar sind. Das ist unter anderem mit neuen nanotechnologischen Analysegeräten und Sensoren möglich.

Eine besonders vielversprechende Sensorklasse verwendet Nanodrähte aus verschiedenen Materialien, Drähte also, die nur wenige Millionstel Millimeter dünn sind. Wenn an so dünne Drähte eine Fremdsubstanz andockt, verändern sich ihre elektrischen Eigenschaften so drastisch, dass im Prinzip einzelne Viren, sogar einzelne Moleküle nachweisbar werden. Was gemessen wird, bestimmt die Beschichtung des Nanodrahtes; sollte etwa Ammoniak nachgewiesen werden, müsste die Beschichtung bevorzugt Ammoniakmoleküle aufnehmen, möglichst hoch selektiv. Wären bestimmte Viren nachzuweisen, müssten die Drähte mit Antikörpern beschichtet werden, an denen nur diese Viren haften.

Das Nanosensor-Konzept wird durch eine neue Substanzklasse noch attraktiver: iMabs (industrial molecular affinity bodies) sind biotechnisch maßgeschneiderte Moleküle, die aus einem tragenden Körper bestehen, dem eine Affinitätsstelle anhaftet, die sich biotechnisch auf die Bindung mit zahllosen biologischen Substanzen trimmen lässt. Diese Moleküle sind universell und hoch stabil und gelten damit als gute Kandidaten für Nanodrahtsensoren, die pathogene Keime aller Art aufspüren könnten. Auch die Lebensmittelindustrie ist an solchen Sensoren interessiert, die – wenn sie in Massen und billig produzierbar geworden sind – an Lebensmitteln haftend Auskunft über deren Zustand geben könnten.



Mit Chips des Fraunhofer Instituts für Siliziumtechnologie, ISIT, werden schnelle DNA-Sensoren für die Entdeckung pathogener Bakterien und anderer biogener Stoffe entwickelt.

Schnelle, hochempfindliche Sensoren wären auch zur Abwehr von Attacken mit biologischen Kampfmitteln nötig. Eine neue, schnelle, bessere und billigere Biosensorik wird aber auch schon von der fortschreitenden Globalisierung erzwungen: Wenn die Welt durch schnelles, massenhaftes Reisen zum Dorf wird, ist auch die Möglichkeit für eine schnelle Ausbreitung von Epidemien gegeben. Diese einzudämmen könnten den schnellen Spürgeräten künftig nanotechnologische „Labs-on-a-chip“ zur Seite stehen, die etwa den Aufbau eines neuen Grippevirus schnell zu bestimmen gestatten und dessen DNA-Sequenz via Internet schneller verbreiten als das Virus reisen kann. An potentiell betroffenen Orten würden nanotechnologische „Fabs-on-a-chip“ in Windeseile Impfstoffe synthetisieren – ein fernes, aber nicht unrealistisches Ziel. Viele biotechnologische Prozeduren nämlich lassen sich mittlerweile im Chipformat bewerkstelligen; für die Methode der „Polymerase Chain Reaction“, PCR, zur Vermehrung der Erbsubstanz DNA etwa sind exakt temperierbare Reaktionsgefäße nötig, die jetzt mit nanotechnologisch hergestellten thermoelektrischen Kühlfolien im Zehntel-Millimeter-Maßstab realisierbar sind. Diese Art Mikrosystemtechnik wird von einer ständig raffinierter werdenden Nanoelektronik begleitet, zu der jetzt auch nanophotonische Elemente hinzukommen, die z.B. die Integration von spektroskopischen Analysetechniken im kleinsten Maßstab möglich machen.

Die Forschung wird auf diesem Bereich schon aus kommerziellen Gründen voran getrieben, der Beitrag der Sicherheitsforschung hilft, den Weg zum Erfolg zu verkürzen und die biochemische Analytik auf ein neues Niveau zu heben, das eine reale Chance zur Abwehr von gewollten wie ungewollten chemischen, vor allem aber biologischen Bedrohungen bietet.

Ein Projektbeispiel: Das EU-Projekt eBIOSENSE führt eine Reihe von Unternehmen zusammen, um Sensoren zur Analyse gefährlicher Mikroorganismen und mikrobieller Giftstoffe zu konstruieren (Electrical Bio Sensor Arrays for Analyses of Harmful Micro Organisms and Microbial Toxins); das deutsche Fraunhofer Institut für Siliziumtechnologie steuert sein Know-how für den Brückenschlag zwischen Biologie und Elektronik bei.

multimodale und multifunktionale Detektorplattformen, neuartige mobile Sensorkonzepte, aber auch neuartige Sensor- und Datenfusionskonzepte und -verfahren gefördert werden, durch die die Sicherheit am Einsatzort nachhaltig verbessert und Sicherheitskontrollen beschleunigt werden können. Wesentliche Kriterien bei der Entwicklung und Integration multisensorischer Komponenten sowohl für die Nah- als auch für die Ferndetektion von CBRNE-Stoffen sind neben einer hohen Sensitivität, Auflösung und Selektivität vor allem Handhabungsfreundlichkeit, Autonomie, Automatisierungsgrad, Robustheit sowie Fehlalarmfestigkeit und Echtzeitfähigkeit. Adressierte Förderschwerpunkte sind dabei nicht nur neue Detektionsverfahren (z.B. auf Basis der Terahertztechnologie) und Sensortypen (z.B. Self-Reporting-Sensoren), sondern auch Multisensorsystemlösungen, die auf der Kopplung neuer und bewährter CBRNE-Sensoren oder der anwendungsbezogenen Anpassung existierender Detektoriertechnologien (z.B. Biochips oder klinische Diagnoseverfahren) basieren.

#### Relevante Forschungsthemen:

- + **Drahtlose oder verteilte Sensornetzwerke,**
- + **Preisgünstige portable Sensorensysteme mit geringem Energieverbrauch sowie Lab-on-a-chip-Systeme,**
- + **Massendatentaugliche und echtzeitfähige Sensorkommunikation, Datentransfer und Datenfusion mit Entscheidungsfunktion,**
- + **Systeme zur schnellen, automatischen Ferndetektion,**
- + **Markersysteme, Identifikations- und Detektionsmethoden für neue Sprengstoffsubstanzenklassen, Toxine oder Pathogene,**
- + **Hyperspektralsensoren und multispektrale bildgebende Sensorik.**

#### Mustererkennung

Die Fähigkeit, durch eine intelligente und automatisierte Mustererkennung Informationen, Bilder oder Daten, die womöglich aus vielen verschiedenen Quellen stammen, auszuwerten und zeitnah zuständigen Personen, Einrichtungen oder Behörden zugänglich machen zu können, ist ein wesentliches Element zukünftiger Sicherheitssysteme. Im Krisenfall wird diese Fähigkeit die Einsatzplanung und -führung sowie

die notwendige Ermittlungsarbeit erleichtern. Anwendungsschwerpunkte bilden z.B. der automatisierte Schutz von Orten, an denen sich viele Menschen aufhalten, die Erkennung von gefälschten Dokumenten, die automatisierte Unterstützung von Grenzkontrollen oder die Überwachung als gefährlich oder gefährdet eingestuft Objekte.

Dabei sind die Möglichkeiten zur automatisierten Auswertung von multisensoriellen Daten, etwa von Bilddaten, in Verknüpfung mit Ergebnissen von Detektionsverfahren, die zum Beispiel auf Gefahrstoffe ansprechen, in Überwachungs- und Frühwarnsystemen noch stark entwicklungsfähig. Grundlagen für die Realisierung verbesserter Mustererkennungssysteme und neuartiger Techniken zur Datenanalyse und Datenvisualisierung werden unter anderem die äußerst leistungsfähigen Hard- und Softwareentwicklungen aus der Datenbank- und Internettechnologie sein. Dazu kommen informations-, visualisierungs- und sensortechnologische Entwicklungen aus anderen Forschungsfeldern. So können z.B. Algorithmen aus dem Bereich Mustererkennung, die ursprünglich mit dem Ziel entwickelt wurden, Tumore auf Computertomografie-Bildern zu entdecken, in abgewandelter Form auch dazu verwendet werden, im Bereich der Videoüberwachung die Bewegung von Personen zu verfolgen oder verlassene Gepäckstücke auf Bahnhöfen oder Flughäfen zu

*Intelligente Sicherheitskameras erkennen dank ausgeklügelter Software selbstständig, dass ein Gepäckstück abgestellt und herrenlos wird.*





*3D-Gesichtserkennung: Die 3D-Objekterfassung mit Hilfe von Farbstreifen bietet viele Einsatzmöglichkeiten.*

### Biometrie zur Identifizierung von Personen

Menschen sind in der Regel sehr empfindlich, wenn es um Gesichter geht, kleine Abweichungen nur und ein eigentlich vertrautes Gesicht wird als fremd empfunden.

Computer sind da weniger sensibel, sie haben einstweilen ihre liebe Not, ein reales Gesicht mit einem Passfoto zu vergleichen. Das ist für zweidimensionale Abbildungen auch nicht verwunderlich, das Erscheinungsbild im Pass hängt allzu stark vom Lichteinfall bei der Aufnahme oder der Neigung des Kopfes ab. Oder der Tagesform – man will sich häufig ja selbst nicht erkennen. Sicherer versprechen Verfahren zu werden, die ein Gesicht, einen Kopf in drei Dimensionen erfassen. Die Europäische Union hat deshalb 12 Millionen Euro in das Projekt „3D Face“ investiert. Neben Fraunhofer-Forschern arbeiten hier unter anderem die Bundesdruckerei, Cognitec Systems aus Dresden und der französische Rüstungselektronikerhersteller Sagem Defense Securite zusammen. Das Projekt baut auf Erfahrungen in der Produktionstechnik auf, bei der ebenfalls dreidimensionale Formen durch einen optischen Scan möglichst genau erfasst werden müssen. Auf das menschliche Gesicht angewandt, erfasst die Technik auch Feinheiten wie die Krümmung der Wangen, die Knittrigkeit der Ohren, die Dynamik des Kinns. Schlechte Beleuchtung ist bei 3D kein Problem mehr, auch das Altern macht ein Gesicht, Dank vieler neuer Referenzpunkte, für die Maschine nicht unkenntlich.

Seit vor zwei Jahren der Hamburger Chaos Computerclub öffentlich machte, wie einfach sich Kunststoffabdrücke realisieren lassen, die Fingerabdruckscanner überlisten, gilt das Sicherheitsmerkmal Fingerabdruck als ergänzungsbedürftig. Eine Möglichkeit ist die Venenmustererfassung des Handrückens mit einer Infrarotkamera. Der Vorteil: Das typische Muster befindet sich Wärme abstrahlend im Körperinneren. Um es nachzuahmen, müsste man eine Art infrarotaktives Handrückentoupet anfertigen, was sicher nicht unmöglich ist, aber eben auch schwierig. An den Schulen der schottischen Stadt Paisley bezahlen die Schüler so, mit dem Vorzeigen des Handrückens, bargeldlos ihre Schulspeisung. Ein angenehmer Nebeneffekt: Arme Schüler, die nicht zahlen müssen, wiesen sich vor der Einführung des Handrückenscannings durch ein Bändchen um den Hals aus, das sich von dem



*Bosch Sicherheitssysteme hat für die Spielbank Bad Homburg ein anonym arbeitendes Gesichtserkennungssystem installiert. Es erkennt zuverlässig Personen, deren Gesichtsbilder einer freiwilligen Selbstsperrung wegen gespeichert sind. Das Aufsichtspersonal kann so Spielsüchtigen diskret den Zugang verwehren.*

reicherer Mitschüler unterschied – ein Mobbingsignal. Vor dem Handrückenscanner mit Computer sind nun alle gleich, und den Kids macht es Spaß, sie lieben das „Bond-Feeling“. Ihrer Majestät Geheimagent James Bond war nämlich auch in Abenteuer verwickelt, bei dem biometrische Merkmale eine Rolle spielten, in „Sag' niemals nie“ etwa wurde mittels eines Scans der Augen-Iris über die Verfügbarkeit von Atomwaffen entschieden. Das ging nicht gut (am Ende dann doch); den Augenhintergrund, die Netzhaut, hätte man schon auch noch scannen müssen. Und die Handrücken, und die Gesichtsform und ... Die Methoden zur eindeutigen Identifizierung von Zugangsberechtigten erreichen heute schon eine Trefferquote von 98 Prozent. Sie müssen allerdings auch praktikabel sein. Die Lufthansa etwa hat die Venenmustererfassung am Handrücken am Flughafen Johannesburg getestet. Aus den Venenlinien erzeugte ein Check-In-System einen Barcode, der auf die Bordkarte geklebt wurde und beim Boarding zur Identitätsprüfung der Passagiere dienen sollte. Die Passagiere waren mit dem Procedere überfordert.

Aber biometrische Methoden kommen. Das Spielkasino in Bad Homburg etwa hat biometrische Daten von Spielsüchtigen gespeichert – auf deren eigenen Wunsch. Beim Betreten des Casinos werden die Unglücklichen wie alle anderen Besucher auch gefilmt und die Gesichter mit einer biometrischen Datenbank verglichen. Im Erkennensfalle schickt der Computer dahinter per Funk ein Foto an die Taschencomputer der Wachhabenden, ohne Angabe des Namens, und die Ertappten werden im eigenen Interesse hinaus komplimentiert. Ladendiebe können ähnlich abgeschreckt werden.



entdecken. In die Mustererkennung fließen auch Ergebnisse der Geistes- und Sozialwissenschaften etwa zu Verhaltensformen und Organisationsstrukturen terroristischer Akteure ein.

#### Relevante Forschungsthemen:

- + Automatische Bild-, Daten- und Text-Auswertungsverfahren sowie Web-Suchtechnologien,
- + Künstliche neuronale bzw. selbstlernende Netze,
- + Massendatentaugliche und echtzeitfähige automati-

*Testbild, zusammengestellt von L. Fei-Fei, R. Fergus and P. Perona. (California Institute of Technology), an dem Automaten das Kategorisieren erlernen sollen: Was ist ein Insekt, was ein Flugzeug, was ein Mensch, was ein Motorrad?*

#### sierte Informations- und Datenfusion, VR-Technologien,

- + Datenaustauschtechnologien,
- + Maschinelle Übersetzungs- und Spracherkennungstechnologien,
- + Aufspüren und Screening von Radar- und Funksignalen.



*links: Mikrodrohne md4-200 ...*

*rechts: ... und ihre Erbauer, Freunde und Lenker, von der Drohne aus fotografiert. Damit Geräte dieser Art nicht in die Privatsphäre eindringen, wird die begleitende Sicherheitsforschung Regeln für ihre Anwendung finden.*

## Aufklärungsroboter

Der Computer des Apollo-Raumschiffs, das 1969 drei Astronauten zum Mond brachte, hatte einen wiederbeschreibbaren Speicher, RAM, von 4 Kilobyte und einen Takt von einem Megahertz. Das Durchschnittsnotebook von heute liegt vom Speicher her um den Faktor 250.000 darüber und taktet mehr als tausendmal so schnell. Der Vergleich lässt ahnen, was moderne Elektronik und Sensorik heute möglich machen: z.B. ein wagenradkleines „UFO“, das von allein in der Luft stehen bleibt, wenn man die Fernsteuerung aus der Hand legt, selbst wenn es böige Herbstwinde wegblasen wollen.

Besagtes UFO, ein Produkt der microdrones GmbH nahe Siegen, heißt md4-200, wiegt gerade mal 680 Gramm und kann bis zu 200 Gramm Nutzlast tragen, z.B. eine elektronische Kamera. „md“ steht für Micro-Drohne, die 4 für die Zahl der Rotoren und die „200“ für die mögliche Zuladung.

Anders als die schon länger erhältlichen Modellhubschrauber ließe sich die md4-200 schon nach kurzer Zeit auch von völligen Anfängern steuern, versichert der Entwickler Udo Jürss. Das ist möglich, weil die vier Rotoren von raffinierten Elektromotoren angetrieben werden, deren Leistung ein ausgefeiltes Computersystem regelt, das wiederum von zahlreichen Sensoren unterstützt wird. Dazu gehören ein GPS-Empfänger, Luftdruck-, Temperatur- und Magnetfeldsensoren, Dreiachs-Beschleunigungsmesser und mehr. Die Energie für Antrieb und Steuerung liefert ein Lithiumpolymerakku, der das Gefährt ca. 20 Minuten in der Luft halten kann.

Die übliche Nutzlast besteht aus einer Digitalkamera für Videos oder Fotos, die über Funk gesteuert wird und ihre Signale wieder über Funk an die Betreiber sendet. Die steuernde Person kann sich deshalb eine Videobrille aufsetzen und die Drohne so lenken, als säße sie in ihr, hinter der Kamera. Dadurch lassen sich auch Orte anfliegen, zu denen kein direkter Sichtkontakt mehr besteht. Vielleicht, weil die Drohne zu weit entfernt ist, ihre Steighöhe beträgt bis zu 1500 Meter. Es wäre ohne weiteres möglich, die Kugel des Fernsehturms auf dem Berliner Alexanderplatz anzufliegen und durch ein Fenster nachzusehen, was im Turmrestaurant auf den Tellern liegt.

Die md4-200 ist nur eine aus einer Vielzahl von Drohnen, die auf dem Markt zu haben sind, allerdings zeichnet sie sich durch eine Reihe von ungewöhnlichen Eigenschaften aus, wie ihr geringes Gewicht, Dank dessen sie anmeldungsfrei betrieben werden kann. Die Zuladung von 200 Gramm reicht heute für Kameras, die professionelle Bilder liefern.

Drohnen dieser Klasse sind deshalb für Sicherheitsdienste wie Polizei, Feuerwehr, Technisches Hilfswerk usw. hoch interessant, ebenso für Firmen, die Flughäfen, Kraftwerke und Firmengebäude zu bewachen haben. Von einem Satellitennavigationssystem wie GPS oder demnächst GALILEO über ihre Position informiert, können sie computergesteuert vollautomatisch Patrouille fliegen und über Bildauswertungssysteme verdächtige Bewegungen melden. Die Fähigkeit, an einem bestimmten Punkt in der Luft stehen bleiben zu können, machen sie als Ausguck für alle möglichen Großveranstaltungen, wie etwa Fußballspiele, interessant. Die Autobahnpolizei könnte bei Unfällen mit den dazu gehörenden Verkehrsblockaden solche Drohnen vorausschicken, um vorab die Notwendigkeit des Einsatzes eines Rettungshubschraubers oder anderen schweren Geräts abzuschätzen. Die Feuerwehr könnte sich etwa an einem brennenden Hochhaus mit Drohnen ein genaues Bild der Lage verschaffen, ohne das Leben der Einsatzkräfte vor Ort zu riskieren. Brücken wären einfach auf Risse zu inspizieren, große Bauten auf Schäden der Statik.

Natürlich werden auch Paparazzi mit Drohnen auf Bildfang gehen. Ein schwerer wiegender Einwand ist natürlich der, dass auch Terroristen mit frei verfügbaren Drohnen ein neues potentielles Terrormittel in die Hand bekommen, der Phantasie sind hier keine Grenzen gesetzt. Der Staat wird also überlegen müssen, ob diese Technik nicht doch restriktiver zu handhaben ist. Die Sicherheitsforschung kann hier durch intelligente technische Lösungen und sinnvolle Begleitforschung helfen, die richtigen Entscheidungen zu treffen.

## Biometrie

Die Authentifizierung oder Identifizierung von Personen anhand biometrischer Merkmale kann z.B. beim Terrorschutz, bei der Grenzsicherung oder der polizeilichen Strafverfolgung eingesetzt werden. Die Technik gewinnt aber auch im E-Commerce und bei Zutrittskontrollen an Bedeutung. Es gilt unter anderem, biometrische Systeme so zu entwickeln, dass ihr Einsatz etwa bei Grenzkontrollen eine leistungsfähige, überwindungssichere sowie schnelle und komfortable Authentifikation ermöglicht. Neben der Handhabungsfreundlichkeit, Identifikationsgenauigkeit und Robustheit biometrischer Systeme sind unter anderem die Minimierung von Rückweisungs- und Falschakzeptanzraten wichtig. Von hoher Bedeutung für die Weiterentwicklung und Integration biometrischer Komponenten in Sicherheitssystemen ist der Schutz der gespeicherten Referenzdaten sowie die Übertragung der Daten im biometrischen System.

Relevante Technologien sind:

- + Integrierte biometrische Sensorsysteme,
- + Multimodale Biometrie,
- + 3D-Gesichtserkennung,
- + Dezentrale Vertrauensmodelle und –technologien.



*Bosch hat zusammen mit Partnern das Pilotprojekt für die automatisierte biometriegestützte Grenzkontrolle am Frankfurter Flughafen aufgebaut.*

*Bild links: Die Lufthansa hat mit Siemens ein biometrisches Check-in- und Boarding-Verfahren am Frankfurter Flughafen erfolgreich getestet. Demnach können sich Fluggäste künftig mit ihrem Fingerabdruck identifizieren. Das System wandelt die charakteristischen Merkmale des Fingerabdrucks in einen zweidimensionalen Code aus Punkten um und druckt diesen auf die Bordkarte.*

# Umsetzung des Förderprogramms

## Förderinstrumente

Im Vordergrund der Förderung stehen nicht technologische Einzelergebnisse, sondern die Formierung der Akteursgemeinschaft und die Umsetzung von gemeinsam vereinbarten Innovationsstrategien und Zielen. Gerade in der Sicherheitsforschung ist die Mitwirkung der Endnutzer und Anwender mit ihren praktischen Erfahrungen unerlässlich.

Gefördert werden vorrangig Verbundprojekte, die wesentlich an folgenden Kriterien gemessen werden:

- + **Beitrag zur Erhöhung der Sicherheit,**
- + **Innovationshöhe und Erkenntnisgewinn,**
- + **Ganzheitlichkeit und Breitenwirksamkeit des Lösungsansatzes unter Einbeziehung gesellschaftlicher Ziele und Wirkungen,**
- + **Praxistauglichkeit bzw. Marktfähigkeit der angestrebten Lösung sowie deren optimierte volkswirtschaftliche Hebelwirkung.**

Die Verbundprojekte sollen endnutzer- oder industriegeführt sein und alle notwendigen Forschungsdisziplinen einbeziehen.

In der Programmlinie 1 zielen die Verbundprojekte auf Systemlösungen für Sicherheitsszenarien, in der Programmlinie 2 auf szenarienübergreifende Technologiesysteme. Gerade auch für KMU sind Verbundprojekte von besonderem Vorteil. Zum einen kommen die KMU dadurch in unmittelbarem Kontakt zu exzellenten Forschungseinrichtungen, auf der anderen Seite erhalten sie über die im Projektverbund kooperierenden Großunternehmen Zugang zu Schlüsselanwendern und Märkten und damit die Chance, als Zulieferer tätig werden zu können.

Die Vergabe erfolgt im Wettbewerb, d.h. ihr geht in der Regel eine öffentliche Bekanntmachung voraus, in der der jeweilige Themenausschnitt und weitere spezielle Kriterien genannt werden. Der Breite des Themas Sicherheitsforschung entsprechend können die Bekanntmachungen im Zusammenhang mit anderen Forschungsprogrammen und über mehrere Politikbereiche erfolgen.

Um der Breite der Sicherheitsforschung gerecht zu werden, ist, auf thematisch verwandten Verbundprojekten aufbauend, die Einrichtung von Innovationsplattformen vorgesehen. Ziel dieser Innovationsplattformen ist es, alle

beteiligten Akteure an einen Tisch zu bringen. So können etwa Synergien zwischen themenverwandten Forschungsprojekten genutzt werden. Auch der für spätere Entscheidungen, zum Beispiel bei der Beschaffung, wichtige Informationstransfer beginnt auf diese Weise schon im Stadium der Forschung und Entwicklung. Die Innovationsplattformen schaffen die Voraussetzung für eine rasche Umsetzung der Ergebnisse in die Praxis. Die Effizienz wird noch erhöht, wenn die Akteure im Rahmen einer Selbstverpflichtung den Anteil eigener Forschungsaktivitäten vermehren und größere und verbindlichere Verwertungsaktivitäten entfalten als am Standort Deutschland bei einem normalen Fördervorhaben bislang üblich war.

Das Sicherheitsforschungsprogramm wird durch einen Programmausschuss begleitet und gesteuert, dem Expertinnen und Experten aus der Forschung, den Bundesressorts, der Industrie und dem Bereich der Betreiber sicherheitsrelevanter Infrastrukturen angehören. Dieser Programmausschuss wird dazu beitragen, dass die Maßnahmen der Sicherheitsforschung mit den sicherheitspolitischen Aktivitäten der Bundesregierung eng verzahnt werden und eine möglichst nahtlose Umsetzung der Ergebnisse erfolgen kann. Der Programmausschuss hat zudem die Aufgabe, laufend die Zielorientierung zu bewerten, Vorschläge für neue Forschungsthemen und für weitere Innovationsschritte (z.B. Normung und Standardisierung, Regelsetzung, Beschaffung) zu unterbreiten und den Ergebnistransfer in die Anwendung zu verfolgen.

## Programmlaufzeit und Fördermittel

Um aussichtsreiche Sicherheitslösungen und Technologieentwicklungen verfolgen zu können und nachhaltig den Kompetenzaufbau und die Vertrauensbildung der Akteure sicher zu stellen, ist eine auf längere Sicht ausgerichtete Förderung notwendig. Das Förderprogramm bildet den Rahmen für eine solche längerfristig ausgerichtete flexible Förderpolitik. Es ist als lernendes Programm ausgelegt. Die oben beschriebenen Instrumente der Innovationsplattformen und des Programmausschusses zielen unter anderem auf eine kontinuierliche Optimierung und Fortschreibung der Förderung ab.

Das Sicherheitsforschungsprogramm der Bundesregierung ist zunächst auf eine erste Förderperiode bis zum Jahr 2010 angelegt. Es soll am Ende der ersten Programmperiode

evaluiert werden. Der Fortsetzung des Programms über das Jahr 2010 hinaus geht die Festlegung neuer mittelfristiger operativer Ziele voraus.

In den Jahren 2007 bis einschließlich 2010 stellt die Bundesregierung hierfür Haushaltsmittel im Umfang von rund 123 Mio. Euro unter dem Vorbehalt der Bewilligung durch das Parlament bereit. Diese Haushaltsmittel stehen zusätzlich zu der bisher in den Bundesressorts und in entsprechenden Fachprogrammen angesiedelten sicherheitsrelevanten Forschungsförderung zu spezifischen Themen zur Verfügung.

*Nach schrecklichen Auseinandersetzungen und Verirrungen sind schwere innereuropäische Konflikte Vergangenheit. An die Stelle großer äußerer Bedrohungen aber sind kleinteilige, dafür potentiell sehr wirksame getreten, die die Gemeinschaft mit Intelligenz abwehren muss, um in Freiheit zu bewahren, was an Europa schön war und ist - wie der Markusplatz in Venedig, vom Campanile aus gesehen.*



# Anhang

## Laufende Aktivitäten der Bundesregierung mit Bezug zur Sicherheitsforschung

### Auswärtiges Amt (AA)

- Homepage [www.auswaertiges-amt.de](http://www.auswaertiges-amt.de) u. a. mit den Themenbereichen Abrüstung, Rüstungskontrolle, Friedenspolitik, Sicherheitspolitik, Nichtweiterverbreitung von Massenvernichtungswaffen, zivile Krisenprävention, Konfliktlösung und Friedenskonsolidierung, humanitäres Völkerrecht, Zusammenarbeit in EU, NATO, OSZE und VN.
- Sicherheit und Stabilität durch Krisenprävention gemeinsam stärken
- Bericht der Bundesregierung über die Umsetzung des Aktionsplans Zivile Krisenprävention, Konfliktlösung und Friedenskonsolidierung, Mai 2006
- Europäische Sicherheits- und Verteidigungspolitik, Mai 2004
- Jahresabrüstungsbericht, 2005
- EU-Strategie zur Verhinderung der Verbreitung von Massenvernichtungswaffen, Dezember 2003
- EU-Strategie zur Bekämpfung der Anhäufung von Kleinwaffen und dazugehöriger Munition sowie des unerlaubten Handels damit, Dezember 2005

### Bundeskanzleramt (BK)

- Homepage [www.bundeskanzlerin.de](http://www.bundeskanzlerin.de)
- G8-Erklärung zur Terrorismusbekämpfung vom 16. Juli 2006

Behörden und Forschungseinrichtung im Bereich des BK:

### Stiftung Wissenschaft und Politik (SWP)

- Homepage: [www.swp-berlin.org](http://www.swp-berlin.org)
- Forschungsgruppen zu den Bereichen EU-Integration, EU-Außenbeziehungen, Sicherheitspolitik, Amerika, Russland/GUS, Naher Osten und Afrika, Asien, Globale Fragen
- Zahlreiche Studien, Zeitschriftenschauen und Buchreihen zu Sicherheitsfragen

### Bundesnachrichtendienst (BND)

- Homepage: [www.bundesnachrichtendienst.de](http://www.bundesnachrichtendienst.de)
- Aufgaben u. a. im Bereich Risikofrüherkennung durch Aufklärung des Internationalen Terrorismus und der Organisierten Kriminalität. Schnittstelle zu Auslandsnachrichtendiensten

### Bundesministerium der Finanzen (BMF)

- Homepage: [www.bundesfinanzministerium.de](http://www.bundesfinanzministerium.de) u. a. mit den Themenbereichen Zoll und Geldwäsche

### Bundesministerium der Justiz (BMJ)

- Homepage: [www.bmj.bund.de](http://www.bmj.bund.de) u. a. mit dem Themenbereich Kriminalprävention
- Zweiter Periodischer Sicherheitsbericht der Bundesregierung, BMI und BMJ, November 2006

### Bundesministerium der Verteidigung (BMVg)

- Homepage [www.bmvg.de](http://www.bmvg.de) u. a. mit den Themenbereichen Verteidigung, Verhütung und Bewältigung von Krisen und Konflikten und Kampf gegen den internationalen Terrorismus
- Weißbuch 2006 zur Sicherheitspolitik Deutschlands und zur Zukunft der Bundeswehr, Oktober 2006 – gemeinsam mit dem Auswärtigen Amt

Forschungseinrichtungen im Bereich des BMVg:

### Institut für Radiobiologie der Bundeswehr

- E-Mail: [Institutfuerradiologie@bundeswehr.org](mailto:Institutfuerradiologie@bundeswehr.org)

### Institut für Mikrobiologie der Bundeswehr

- E-Mail: [Institutfuermikrobiologie@bundeswehr.org](mailto:Institutfuermikrobiologie@bundeswehr.org)

### Institut für Pharmakologie und Toxikologie der Bundeswehr

- E-Mail: [Institutfuerpharmakologieundtoxikologie@bundeswehr.org](mailto:Institutfuerpharmakologieundtoxikologie@bundeswehr.org)

### Flugmedizinisches Institut der Luftwaffe

- E-Mail: [FlMedInstLtr@bundeswehr.org](mailto:FlMedInstLtr@bundeswehr.org)

### Schiffahrtsmedizinisches Institut der Marine Forschungsanstalt der Bundeswehr für Wasserschall und Geophysik (FWG)

- Homepage: [www.bwb.org](http://www.bwb.org)

### Sozialwissenschaftliches Institut der Bundeswehr (SWInstBw)

- Homepage: [www.sowi-bundeswehr.de](http://www.sowi-bundeswehr.de)

### Wehrwissenschaftliches Institut für Schutztechnologien -ABC-Schutz (WIS)

- Homepage: [www.bwb.org/wis](http://www.bwb.org/wis)

#### **Wehrwissenschaftliches Institut für Werk-, Explosiv- und Betriebsstoffe (WIWEB)**

- Homepage: [www.bwb.org/WIWEB](http://www.bwb.org/WIWEB)

#### **Amt für Geoinformationswesen der Bundeswehr (AGeoBW)**

- E-Mail: [ageobweingang@bundewehr.org](mailto:ageobweingang@bundewehr.org)

#### **Forschungsgesellschaft für Angewandte Naturwissenschaften e.V. (FGAN)**

- Homepage: [www.fgan.de](http://www.fgan.de)
- Anwendungsorientierte Forschung im Bereich Hochfrequenzphysik und Radartechnik; Optronik und Mustererkennung sowie IKT und Robotik.

#### **Fraunhofer-Institute im Geschäftsbereich der BMVg**

- Homepage: Fraunhofer Verbund für Verteidigungs- und Sicherheitsforschung [www.vvs.fraunhofer.de](http://www.vvs.fraunhofer.de)
- FhI für naturwissenschaftlich-technische Trendanalysen (INT)
- FhI für Kurzzeitdynamik, Ernst-Mach-Institut (EMI)
- FhI für Chemische Technologie (ICT)
- FhI für Angewandte Festkörperphysik (IAF)

#### **Bundesministerium des Inneren (BMI)**

- Homepage [www.bmi.bund.de](http://www.bmi.bund.de) u. a. mit den Themenbereichen Bevölkerungsschutz und Katastrophenhilfe, Datenschutz, Kriminalität und Terrorismus, IT-Sicherheit
- Zweiter Periodischer Sicherheitsbericht der Bundesregierung, BMI und BMJ, November 2006
- Nationaler Plan zum Schutz der Informationsinfrastrukturen, Juli 2005
- Schutz Kritischer Infrastrukturen – Basisschutzkonzept, Empfehlungen für Unternehmen, August 2006

Nachgeordnete Behörden des BMI:

#### **Bundesamt für Sicherheit in der Informationstechnik (BSI)**

- Homepage [www.bsi.bund.de](http://www.bsi.bund.de) mit den Themenbereichen Sicherheit in Anwendungen, Kritischen Infrastrukturen und im Internet, Kryptografie und Abhörsicherheit, Zertifizierung,
- Zulassung und Konformitätsprüfungen, Neue Technologien und Veröffentlichung technischer Richtlinien
- Projekte mit Forschungseinrichtungen in den Innovationsfeldern Frühwarnung/Trojaner, Trusted Computing

sowie Biometrie, Pässe, Ausweise

- Lage der IT-Sicherheit in Deutschland, Juli 2005
- IT-Grundschrutkataloge und Leitfaden IT-Sicherheit -IT-Grundschrut kompakt, März 2006
- Risiken und Chancen des Einsatzes von RFID-Systemen, 2005
- Sicherheit von Webanwendungen – Maßnahmenkatalog und Best Practices, Version 1, August 2006
- VoIPSEC -Studie zur Sicherheit von Voice over Internet Protocol, 2005
- Studie Pervasive Computing – Entwicklungen und Auswirkungen (PerCEntA), Oktober 2006
- Studie Integration und IT-Revision von Netzübergängen, Oktober 2006
- Tomcat-Sicherheitsuntersuchung, 2006
- Mobile Endgeräte und mobile Applikationen – Sicherheitsgefährdungen und Schutzmaßnahmen, 2006
- Beispielrichtlinien und Standort-Check für Kritische Infrastrukturen

#### **Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)**

- Homepage [www.bbk.bund.de](http://www.bbk.bund.de) u. a. mit den Themenbereichen Schutz kritischer Infrastrukturen, ABC-Schutz, Krisenmanagement, Forschungs- und Entwicklungsvorhaben im Bevölkerungsschutz
- Rahmenkonzept zur Dekontamination (verletzter) Personen, Bund-Länder-Arbeitsgruppe, September 2006
- Biologische Gefahren – Beiträge zum Bevölkerungsschutz, 2005

#### **Bundesanstalt Technisches Hilfswerk (THW)**

- Homepage: [www.thw.bund.de](http://www.thw.bund.de)
- Aufgaben im Bereich Katastrophenschutzorganisation, Leistung technischer Hilfe im Inland und humanitäre Hilfe im Ausland

#### **Bundeskriminalamt (BKA)**

- Homepage: [www.bka.de](http://www.bka.de)
- Aufgaben u. a. im Bereich Koordinierung der Kriminalitätsbekämpfung auf nationaler und internationaler Ebene, nationale Zentralstelle für Interpol, Europol und das Schengener Informationssystem
- Kriminalistisch-kriminologische Forschung im Kriminalistischen Institut mit den Forschungsstellen für Terroris-

mus/Extremismus, Polizeiliche Kriminalstatistik, Schwere  
Gewaltkriminalität und IuK-Kriminalität, Organisierte  
und Wirtschaftskriminalität, Rechtspolitik und Kriminal-  
prävention

- Beteiligung an Forschungsprojekten u.a. in den Berei-  
chen Gesichtserkennung und Detektionstechnik

#### **Bundespolizei (BPOL)**

- Homepage: [www.bundespolizei.de](http://www.bundespolizei.de)
- Aufgaben u. a. im Bereich Grenzschutz, Bahnpolizei, Luft-  
sicherheit und Schutz von Bundesorganen und Verwen-  
dung im Ausland

#### **Bundesministerium für Bildung und Forschung (BMBF)**

- Homepage [www.bmbf.de](http://www.bmbf.de)  
u. a. mit dem Themenbereichen der institutionellen  
Forschungsförderung und der anwendungsbezogenen  
Projektforschungsförderung

Forschungsorganisationen im Geschäftsbereich des BMBF:

#### **Helmholtz-Gemeinschaft Deutscher Forschungszentren (HGF)**

- Homepage [www.helmholtz.de](http://www.helmholtz.de)  
Arbeiten mit grundsätzlichem Bezug zur Sicherheitsfor-  
schung werden in folgenden HGF-Zentren im Geschäftsbereich  
des BMBF durchgeführt:
- Alfred-Wegener-Institut für Polar- und Meeresforschung,  
Bremerhaven
- GKSS-Forschungszentrum, Geesthacht
- Helmholtz-Zentrum für Infektionsforschung, Braun-  
schweig
- Forschungszentrum Jülich
- Forschungszentrum Karlsruhe
- GeoForschungsZentrum Potsdam
- GSF-Forschungszentrum für Umwelt und Gesundheit,  
Neuherberg
- Helmholtz-Zentrum für Umweltforschung - UFZ, Leipzig-  
Halle

#### **Max-Planck-Gesellschaft (MPG)**

- Homepage [www.mpg.de](http://www.mpg.de)  
Arbeiten mit grundsätzlichem Bezug zur Sicherheitsfor-  
schung werden in folgenden MPG-Instituten durchge-  
führt:

- MPI für ethnologische Forschung
- MPI für Informatik
- MPI für biologische Kybernetik
- MPI für Mikrostrukturphysik
- MPI für Softwaresysteme
- MPI für ausländisches und internationales Strafrecht

#### **Wissenschaftsgemeinschaft Gottfried Wilhelm Leibniz (WGL)**

- Homepage: [www.wgl.de](http://www.wgl.de)  
Arbeiten mit grundsätzlichem Bezug zur Sicherheitsfor-  
schung werden in folgenden WGL-Instituten durchge-  
führt:
- Deutsche Forschungsanstalt für Lebensmittelchemie,  
Garching - DFA
- Deutsches Institut für Wirtschaftsforschung, Berlin - DIW
- Ferdinand-Braun-Institut für Höchstfrequenztechnik,  
Berlin - FBH
- Forschungszentrum Borstel - Leibniz-Zentrum für Medi-  
zin und Biowissenschaften - FZB
- Forschungszentrum Rossendorf, Dresden - FZR (Institut  
für Sicherheitsforschung am FZR)
- Heinrich-Pette-Institut für Experimentelle Virologie und  
Immunologie - HPI
- Institut für innovative Mikroelektronik, Frankfurt (Oder)  
- IHP
- Institut für Geowissenschaftliche Gemeinschaftsaufga-  
ben, Hannover - GGA
- Leibniz-Institut für Altersforschung -Fritz-Lipmann-Insti-  
tut, Jena - FLI
- Leibniz-Institut für Naturstoff-Forschung und Infektions-  
biologie -Hans-Knöll-Institut, Jena - HKI
- Max-Born-Institut für Nichtlineare Optik und Kurzzeit-  
spektroskopie, Berlin - MBI
- Paul-Drude-Institut für Festkörperelektronik, Berlin - PDI
- Wissenschaftszentrum Berlin für Sozialforschung - WZB
- Leibniz-Institut für Pflanzengenetik und Kulturpflanzen-  
forschung, Gatersleben - IPK

#### **Fraunhofer-Gesellschaft (FhG)**

- Strategische Studie zur Aufstellung der FhG Fraunhofer-  
Gesellschaft in der Sicherheitsforschung, März 2005
- Homepage [www.fraunhofer.de](http://www.fraunhofer.de)  
Arbeiten mit Bezug zur Sicherheitsforschung werden in

folgenden Instituten der Fraunhofer-Gesellschaft (FhG) im Geschäftsbereich des BMBF durchgeführt:

- FhI für Offene Kommunikationssysteme (FOKUS)
- FhI für Angewandte Polymerforschung (IAP)
- FhI für Digitale Medientechnologie (IDMT)
- FhI für Experimentelles Software Engineering (IESE)
- FhI für Fabrikbetrieb und -automatisierung (IFF)
- FhI für Grenzflächen- und Bioverfahrenstechnik (IGB)
- FhI für Graphische Datenverarbeitung (IGD)
- FhI für Integrierte Schaltungen (IIS)
- FhI für Informations- und Datenverarbeitung (IITB)
- FhI für Keramische Technologien und Sinterwerkstoffe (IKTS)
- FhI für Lasertechnik (ILT)
- FhI für Molekularbiologie and Angewandte Oekologie (IME)
- FhI für Mikroelektronische Schaltungen und Systeme (IMS)
- FhI für Produktionstechnik und Automatisierung (IPA)
- FhI für Produktionsanlagen und Konstruktionstechnik (IPK)
- FhI für Physikalische Messtechnik (IPM)
- FhI für Siliziumtechnologie (ISIT)
- FhI für Software- und Systemtechnik (ISST)
- FhI für Toxikologie und Experimentelle Medizin (ITEM)
- FhI für Techno- und Wirtschaftsmathematik (ITWM)
- FhI für Zelltherapie und Immunologie (IZI)
- FhI für Zerstörungsfreie Prüfverfahren (IZFP)
- FhI für Zuverlässigkeit und Mikrointegration (IZM)
- FhI für Sichere Informationstechnologie (SIT)

Fachprogramme des BMBF mit Bezug zur Sicherheitsforschung:

**Rahmenprogramm „Werkstoffinnovationen für Industrie und Gesellschaft WING“**

- [www.bmbf.de/pub/rahmenprogramm\\_wing.pdf](http://www.bmbf.de/pub/rahmenprogramm_wing.pdf)

**Programm „Forschung für die Produktion von morgen“**

- [www.bmbf.de/pub/produktionsforschung.pdf](http://www.bmbf.de/pub/produktionsforschung.pdf)
- Fördermaßnahme „Innovationen gegen Produktpiraterie“

**Programm „Optische Technologien“**

- [www.bmbf.de/pub/foerderprogramm\\_optische\\_technologien.pdf](http://www.bmbf.de/pub/foerderprogramm_optische_technologien.pdf)
- Förderung u. a. von Terahertz-Systemen

**Rahmenprogramm „Mikrosysteme 2004-2009“**

- [www.bmbf.de/pub/mikrosysteme.pdf](http://www.bmbf.de/pub/mikrosysteme.pdf)
- Förderung u. a. im Bereich Sensorsysteme und RFID

**Programm „IT-Forschung 2006“**

- [www.bmbf.de/pub/it-forschung\\_2006.pdf](http://www.bmbf.de/pub/it-forschung_2006.pdf)
- Förderung zu Sicherheit und Zuverlässigkeit von IKT-Systemen
- Das Programm IT-Forschung 2006 wird im Jahr 2007 durch das Programm IKT 2020 abgelöst.

**Programm „Gesundheitsforschung“**

- [www.bmbf.de/pub/gesundheitsforschung.pdf](http://www.bmbf.de/pub/gesundheitsforschung.pdf)
- Förderschwerpunkte u. a. im Bereich Infektionsforschung

**Fördermaßnahme „Minendetektionstechnologien für humanitäres Minenräumen“**

- [www.bmbf.de/pub/hintergrundpapier\\_bekanntmachung\\_030327.pdf](http://www.bmbf.de/pub/hintergrundpapier_bekanntmachung_030327.pdf)

**Forschungsprojektförderung der Deutschen Stiftung Friedensforschung**

- [www.bundesstiftung-friedensforschung.de](http://www.bundesstiftung-friedensforschung.de)

**Rahmenprogramm „Forschung für die Nachhaltigkeit“**

- [www.bmbf.de/pub/forschung\\_nachhaltigkeit.pdf](http://www.bmbf.de/pub/forschung_nachhaltigkeit.pdf)
- Förderung u. a. in den Bereichen Klimaschutzstrategien, Hochwassermanagement, Risikovororgestrategien

**Rahmenprogramm „Lebensraum Erde“**

- geplante Veröffentlichung in 2007
- Förderung der System-Erde-Forschung u.a. in den Bereichen Frühwarnsysteme, Erd- und Klimabeobachtung, Risiken des Globalen Wandels. In diesem Kontext steht das laufende Engagement im Bereich Tsunami-Frühwarnung

**Programm „Innovative regionale Wachstumskerne“**

- Projekte zum Thema „Maritime Safety Assistance“ zur

Entwicklung von Sicherheitslösungen entlang der maritimen Transportkette

**Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz (BMELV)**

- Homepage [www.bmelv.de](http://www.bmelv.de) u. a. mit den Themenbereichen Tier- und Pflanzengesundheit, Verbraucherschutz, Ernährungsnotfallvorsorge ([www.ernaehrungsvorsorge.de](http://www.ernaehrungsvorsorge.de)) und Verhinderung von bioterroristischen Angriffen
- *Vulnerabilität von Logistikstrukturen im Lebensmitteleinzelhandel*, BMELV Angewandte Wissenschaft Heft 512, Oktober 2005

Nachgeordnete Behörden und Forschungseinrichtungen des BMELV :

**FLI (Friedrich-Loeffler-Institut)**

- Homepage: [www.fli.bund.de](http://www.fli.bund.de)
- Forschung zu Infektionskrankheiten landwirtschaftlicher Nutztiere

**Bundesinstitut für Risikobewertung (BfR)**

- Homepage: [www.bfr.bund.de](http://www.bfr.bund.de)
- Forschung zur Lebensmittelsicherheit, zum gesundheitlichen Verbraucherschutz, zur Risikobewertung im Rahmen biologischer Sicherheit, zur Expositionsabschätzung und zu Konzepten zur Erkennung und Verhütung absichtlicher alimentärer Kontaminationen

**Bundesamt für Verbraucherschutz und Lebensmittelsicherheit (BVL)**

- Homepage: [www.bvl.bund.de](http://www.bvl.bund.de)

**Biologische Bundesanstalt für Land-und Forstwirtschaft (BBA)**

- Homepage: [www.bba.de](http://www.bba.de)
- Aufgaben des Pflanzenschutzes, der Pflanzengesundheit und der biologischen Sicherheit

**Bundesministerium für Gesundheit (BMG)**

- Homepage: [www.bmg.bund.de](http://www.bmg.bund.de) u. a. zu den Themenbereichen Gesundheitsvorsorge sowie Krankheitsbekämpfung, Risiko- und Sicherheitsforschung u. a. im Bereich der Antibiotika-Resistenz und der Infektionskrankheiten

Forschungseinrichtung des BMG:

**Robert Koch-Institut (RKI)**

- Homepage: [www.rki.de](http://www.rki.de)
- Forschung im Bereich der Erkennung, Verhütung und Bekämpfung von Krankheiten, Erhebung und Aufbereitung von Gesundheitsdaten sowie zur Bewertung von Risiken bei gentechnischen Methoden

**Paul-Ehrlich-Institut (PEI)**

- Homepage: [www.pei.de](http://www.pei.de)
- Forschung im Bereich der Impfstoffvorsorge und der Sicherheit biomedizinischer Arzneimittel

**Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (BMU)**

- Homepage [www.bmu.de](http://www.bmu.de) u. a. mit den Themenbereichen Anlagensicherheit, Chemikaliensicherheit, Strahlenschutz, Radiologischer Notfallschutz
- Vollzugshilfe zur Störfall-Verordnung, 2003
- Leitfaden Maßnahmen gegen Eingriffe Unbefugter, Störfallkommission, 2002
- Reaktorsicherheit und Strahlenschutz, Schriftenreihe
- Berichte der Strahlenschutzkommission, Schriftenreihe
- Radiologische Grundlagen für Entscheidungen über Maßnahmen zum Schutz der Bevölkerung bei unfallbedingten Freisetzungen von Radionukliden, 1999
- Rahmenempfehlungen für den Katastrophenschutz in der Umgebung kerntechnischer Anlagen, 1999

Nachgeordnete Behörden und Ressortforschungseinrichtungen des BMU :

**Bundesamt für Strahlenschutz (BfS)**

- Homepage: [www.bfs.de](http://www.bfs.de)
- Forschung u. a. im gesundheitlichen und physikalisch-technischen Strahlenschutz und zum Nuklearen Teststoppvertrag

**Umweltbundesamt (UBA)**

- Homepage [www.umweltbundesamt.de](http://www.umweltbundesamt.de)
- Aufgaben zu Anlagensicherheit, Sicherheitsmanagement, Risikokommunikation

#### **Bundesministerium für Verkehr, Bau und Stadtentwicklung (BMVBS)**

- Homepage: [www.bmvbs.de](http://www.bmvbs.de) u. a. mit den Themenbereichen Verkehrssicherheit und baulicher Schutz
- Initiative Luftverkehr für Deutschland
- Europäisches Satellitennavigationssystem Galileo

#### **Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung (BMZ)**

- Homepage [www.bmz.de](http://www.bmz.de) u. a. mit den Themenbereichen Friedenssicherung, Armutsbekämpfung und Menschenrechte
- *Krisenprävention, Konfliktbearbeitung, Friedensförderung in der deutschen Entwicklungszusammenarbeit*, BMZ Konzepte 131, 2005
- *Recht -Demokratie -Frieden -Politik für Entwicklung*, BMZ Broschüre, 2003-42
- *Katastrophenvorsorge -Beiträge der deutschen Entwicklungszusammenarbeit*, BMZ Materialien 135, Dezember 2004
- *Der Millennium+5-Gipfel: Weichenstellungen für unsere globale Zukunft - Ein Diskussionspapier des BMZ*, BMZ Diskurs, Juni 2005

Forschungseinrichtung des BMZ:

#### **Deutsches Institut für Entwicklungspolitik(DIE)**

- Homepage [www.die-gdi.de](http://www.die-gdi.de)
- Abteilung III „Governance, Staatlichkeit, Sicherheit“

#### **Bundesministerium für Wirtschaft und Technologie (BMWi)**

- Homepage: [www.bmwi.de](http://www.bmwi.de) u. a. mit den Themenbereichen IT-Sicherheit, Geoinformationswirtschaft, Exportkontrolle, Geheimschutz in der Wirtschaft
- Onlineplattform *Sicherheit in der Wirtschaft*, [bmwi-sicherheitsforum.de](http://bmwi-sicherheitsforum.de)
- *Geheimschutzhandbuch -Handbuch für den Geheimschutz in der Wirtschaft*, November 2004
- *iD2010 -Innovationsstrategie für die Informationsgesellschaft Deutschland 2010*, November 2006
- Sicherheit im Themenbereich Mittelstand -Rubrik E-Business
- Europäische Initiative für globale Umwelt- und Sicherheitsbeobachtung (Global Monitoring for Environment and Security, GMES)

- Im Rahmen des Nationalen Raumfahrtprogramms und der deutschen Beiträge zur Europäischen Weltraumorganisation ESA fördert BMWi sicherheitsrelevante Raumfahrtprojekte (Erderkundungsmissionen TerraSAR-X und Tandem-X, optische Kommunikationssysteme, Umweltsatellit Envisat)

Nachgeordnete Behörden und Forschungseinrichtungen des BMWi:

#### **Bundesanstalt für Materialforschung und -prüfung (BAM)**

- Homepage: [www.bam.de](http://www.bam.de)
- Forschung im Bereich der technischen Sicherheit u. a. im Rahmen des Gefahrstoff-, Gefahrgut- und Sprengstoffrechts, der Zerstörungsfreien Prüfung und der Analytischen Chemie
- Fachportal Öffentlich-technische Sicherheit – Gefahrstoffe/Gefahrgüter TES

#### **Bundesnetzagentur (BNetzA)**

- Homepage: [www.bundesnetzagentur.de](http://www.bundesnetzagentur.de)
- Aufgaben zum Fernmeldegeheimnis, bei der Grundversorgung mit Telekommunikations- und Postdienstleistungen, Strom und Gas, Sicherstellung einer effizienten und störungsfreien Nutzung von Frequenzen, Wahrung der Interessen der öffentlichen Sicherheit sowie im Bereich Eisenbahnen

#### **Helmholtz-Zentrum im Geschäftsbereich des BMWi**

- Homepage [www.helmholtz.de](http://www.helmholtz.de) und [www.dlr.de](http://www.dlr.de)
- Deutsches Zentrum für Luft- und Raumfahrt

#### **Bundesanstalt für Geowissenschaften und Rohstoffe (BGR)**

- Homepage: [www.bgr.bund.de](http://www.bgr.bund.de)
- Forschung u. a. zu geologischen Schadensrisiken, Endlagermaßnahmen und zum Kernwaffenteststoppabkommen
- Seismologisches Zentralobservatorium

# Glossar

**3D Face:** EU-Forschungsprojekt zur Entwicklung dreidimensionaler Gesichtserkennungstechnologien für die automatisierte Grenzkontrolle (Laufzeit bis 31/03/2009).

**ABC-Schutz:** Schutz vor Atomaren, Biologischen und Chemischen Gefahren bzw. ABC-Waffen.

**Anthrax:** Milzbrand. Infektionskrankheit, die meist Paarhufer befällt, aber auch als biologischer Kampfstoff eingesetzt werden kann.

**Biochip:** Trägermaterial, auf dem sich eine große Zahl biologischer oder biochemischer Nachweise oder Tests auf engstem Raum befinden (auch Microarray genannt).

**Biometrie:** Beschäftigt sich mit Messungen an Lebewesen und den dazu erforderlichen Mess- und Auswerteverfahren. Im Bereich Personenerkennung: Automatisierte Erkennung von Individuen, basierend auf ihren Verhaltens- und biologischen Merkmalen.

**Bioterror, Bioterrorismus:** Variante des Terrorismus, bei der biologische Waffen für Anschläge benutzt werden.

**CBRNE-Stoffe:** Chemische, Biologische, Radiologische, Nukleare und Explosive Gefahren- bzw. Kampfstoffe.

**Lab-on-a-chip, Fab-on-a-chip:** Auch Westentaschenlabor genannt. Mikrofluidisches System, das die gesamte Funktionalität eines großen Labors zur Analyse bzw. Synthese von chemischen oder biochemischen Substanzen auf einem nur plastikkartengroßen Kunststoffsubstrat unterbringt.

**FTIR (Fourier-Transformations-InfraRot-Spektroskopie):** Besondere Variante der Infrarotspektroskopie, die die sog. Fourier-Transformation nutzt.

**Galileo:** Europäisches, für zivile Zwecke konzipiertes Satellitennavigationssystem, das Ende 2010 betriebsbereit sein soll.

**Ionenmobilitätsspektrometer:** Gerät zur chemischen Analyse, das sich durch niedrige Nachweisgrenzen, kurze Ansprechzeiten und die Detektierbarkeit unterschiedlicher chemischer Substanzklassen bei Umgebungsdruck auszeichnet.

**Low-Power-Sensorik:** Energieeffiziente bzw. autarke Sensorik bzw. Sensornetzwerke, bei der sich die Sensorknotenpunkte durch einen besonders geringen Stromverbrauch auszeichnen oder der Strom zur Versorgung der Sensorkomponenten direkt aus der Umgebungsenergie gewonnen wird.

**Polymerase Chain Reaction (PCR):** Polymerase-Kettenreaktion. Methode zur Vervielfältigung der Erbsubstanz DNA ohne Zuhilfenahme eines lebenden Organismus. Wird u. a. zur Erkennung von Erbkrankheiten und Virusinfektionen sowie das Erstellen und Überprüfen genetischer Fingerabdrücke eingesetzt.

**RADIOTECT-Programm:** EU-Forschungsprojekt zur Entwicklung von Ultra-Breitband-Technologien für die hochauflösende Detektion von vermissten Personen oder nicht identifizierten Objekten.

**RFID-Tags, Funketiketten:** Radio Frequency Identification. Kleine Transponder, die an Objekten angebracht und deren Dateninhalt berührungslos und ohne Sichtkontakt ausgelesen werden kann.

**(Risiko-)homöostase:** Selbstregulation. Fähigkeit eines Systems, sich durch Rückkopplung selbst innerhalb gewisser Grenzen in einem stabilen Zustand zu halten.

**Schmutzige Bomben:** Radiologische Waffe. Konventioneller Sprengsatz, der bei seiner Explosion radioaktives Material in der Umgebung verteilt.

**Self-Reporting-Sensoren:** Autonome drahtlose zumeist passive Sensoren, die selbsttätig im Ereignisfall ausgelöst werden und bei der die detektierten Signale automatisch an eine zentrale Rechner- bzw. Verarbeitungseinheit weitergeleitet werden.

**TATP (Triacetontriperoxid):** Hochexplosiver Flüssig-Sprengstoff mit der Schlagempfindlichkeit eines Initialsprengstoffs.

**Terahertz-Radar (TADAR):** Elektromagnetische Strahlung im Frequenzbereich zwischen Mikrowellen- und Infrarotstrahlung, mit deren Hilfe Objekte durch Hindernisse (Papier, Textilien etc.) hindurch abgebildet werden können.

**Token:** Hardwarekomponente (meist zum Anschluss an den USB-Port eines Computers), die in der Regel eine Chipkarte enthält, aus der keine Daten herauskopiert oder manipuliert werden können.

**VR-Technologien:** Virtuelle Realität. Mensch-Maschine-Schnittstelle, in der ein Benutzer innerhalb einer vom Computer simulierten audiovisuellen Umwelt agiert.

**WLAN:** Wireless Local Area Network. Kabelloses Lokales Netzwerk.

**WUSB (Wireless USB):** Drahtlose Variante des Universal Serial Bus (USB).

**Z Backscatter:** Röntgenrückstreuung. Verfahren zur Detektion und bildhaften Darstellung verdeckter Objekte, das die materialspezifischen Rückstreueigenschaften bezüglich der aktiv eingestrahlten Röntgenstrahlung ausnutzt.

Diese Veröffentlichung wird im Rahmen der Öffentlichkeitsarbeit vom Bundesministerium für Bildung und Forschung unentgeltlich zur Verfügung gestellt. Sie ist nicht zum gewerblichen Vertrieb bestimmt. Sie darf weder von Parteien noch von Wahlwerberinnen/Wahlwerbern oder Wahlhelferinnen/Wahlhelfern während eines Wahlkampfes zum Zwecke der Wahlwerbung verwendet werden. Dies gilt für Bundestags-, Landtags- und Kommunalwahlen sowie für Wahlen zum Europäischen Parlament.

Missbräuchlich ist insbesondere die Verteilung auf Wahlveranstaltungen und an Informationsständen der Parteien sowie das Einlegen, Aufdrucken oder Aufkleben parteipolitischer Informationen oder Werbemittel.

Untersagt ist gleichfalls die Weitergabe an Dritte zum Zwecke der Wahlwerbung. Unabhängig davon, wann, auf welchem Weg und in welcher Anzahl diese Veröffentlichung der Empfängerin/dem Empfänger zugegangen ist, darf sie auch ohne zeitlichen Bezug zu einer bevorstehenden Wahl nicht in einer Weise verwendet werden, die als Parteinahme der Bundesregierung zugunsten einzelner politischer Gruppen verstanden werden könnte.



Bundesministerium  
für Bildung  
und Forschung

