acatech DISKUTIERT

# > SICHERHEITSFORSCHUNG – CHANCEN UND PERSPEKTIVEN

PETRA WINZER/
ECKEHARD SCHNIEDER/
FRIEDRICH-WILHELM BACH (Hrsg.)

Prof. Dr.-Ing. Petra Winzer
Bergische Universität Wuppertal
42097 Wuppertal

Prof. Dr.-Ing. Eckehard Schnieder
Technische Universität Braunschweig
38106 Braunschweig

Prof. Dr.-Ing. Friedrich-Wilhelm Bach
Leibniz Universität Hannover
30823 Garbsen

acatech – Deutsche Akademie der Technikwissenschaften, 2010

Geschäftsstelle
Residenz München
Hofgartenstraße 2
80539 München

T +49(0)89/5203090
F +49(0)89/5203099

acatech Hauptstadtbüro
E-Werk
Mauerstraße 79
10117 Berlin

T +49(0)30/206309610
F +49(0)30/206309611

E-Mail: info@acatech.de
Internet: www.acatech.de

ISBN 978-3-642-04980-4 e-ISBN 978-3-642-04981-1

DOI 10.1007978-3-642-04981-1

Mathematics Subjects Classification 92-xx

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.



Redaktion und Koordination: Vera Lohel
Layout-Konzeption: acatech
Satz/Layout: Fraunhofer-Institut für Intelligente Analyse- und Informationssysteme IAIS, Sankt Augustin
Einbandgestaltung: klink, liedig werbeagentur gmbh

Gedruckt auf säurefreiem Papier

springer.com

acatech DISKUTIERT

# > SICHERHEITSFORSCHUNG – CHANCEN UND PERSPEKTIVEN

PETRA WINZER/
ECKEHARD SCHNIEDER/
FRIEDRICH-WILHELM BACH (Hrsg.)

# > INHALT

# > EINFÜHRUNG

PETRA WINZER/ECKEHARD SCHNIEDER/FRIEDRICH-WILHELM BACH

Sicherheit ist ein Grundbedürfnis der Menschen und somit der Gesellschaft. Wissenschaft und Technik dienen dazu, dieses Grundbedürfnis zu befriedigen. Der Begriff der Sicherheit wird jedoch sehr heterogen verwendet. Diese Heterogenität setzt sich in den Modellen und Lösungskonzepten zur Gewährleistung von Sicherheit fort und demzufolge ist das Themenfeld Sicherheit durch ein breites Spektrum von Gegenständen und Fragestellungen gekennzeichnet. Ziel des Themennetzwerks Sicherheit von acatech – Deutsche Akademie der Technikwissenschaften ist es, eine Brücke zwischen der Safety- und Security-Forschung zu schlagen. Dazu ist es zunächst erforderlich, die unterschiedlichen wissenschaftlichen Auffassungen sowie die vielfältigen Aktivitäten systematisch zu bündeln.

Vor dem Hintergrund der wachsenden gesellschaftlichen Bedeutung des Themas Sicherheit hat acatech ein Themennetzwerk zum Querschnittsthema Sicherheit ins Leben gerufen. Das Themennetzwerk wird übergreifende Fragen der zivilen Sicherheitsforschung stellen und Handlungsempfehlungen erarbeiten. Im Juni 2008 fand die Auftaktsitzung des acatech Themennetzwerks Sicherheit statt. Dem Themennetzwerk gehören ausgewiesene Vertreter aus den Bereichen Safety und Security an. Um der Vielfältigkeit des Themas Sicherheit gerecht zu werden, haben sich die Mitwirkenden des Themennetzwerks zu folgenden Unterarbeitsgruppen zusammengefunden:

- Arbeitsgruppe zum Thema „Sicherheitsbegriff/Taxonomie" unter der Leitung von Prof. Dr.-Ing. Eckehard Schnieder (Braunschweig)
- Arbeitsgruppe zum Thema „neue Technologien" unter der Leitung von Prof. Dr. Klaus Thoma (Freiburg)
- Arbeitsgruppe zum Thema „Systemtheorie/Systems Engineering" unter der Leitung von Prof. Dr.-Ing. Jürgen Beyerer (Karlsruhe)
- Arbeitsgruppe zum Thema „Risikoforschung und Sicherheitskulturen" unter der Leitung von Prof. Dr. Ortwin Renn (Stuttgart)
- Arbeitsgruppe zum Thema „Bildung und Kompetenz" unter der Leitung von PD Dr. Wolfram Risch (Chemnitz)

Die Arbeitsgruppe zum Thema „Sicherheitsbegriff/Taxonomie", die von Prof. Dr.-Ing. Schnieder geleitet wird, verfolgt das Ziel, auf der Grundlage eines interdisziplinären methodischen Ansatzes ein konsistentes Begriffsgebäude für den Begriff „Sicherheit" zu entwerfen. Dies wollen Wissenschaftler und Wissenschaftlerinnen verschiedenster Fachdisziplinen durch die integrative Verknüpfung von zuvor terminologisch stringent formulierten und formalisierten Teilbegriffssystemen erreichen. Als Ergebnis wird ein Begriffsgebäude entstehen, welches die Brücke zwischen „Safety" und „Security" schaffen kann. Dies bildet die Basis für die Weiterarbeit im acatech Themennetzwerk Sicherheit.

Die Diskussion in den verschiedenen Workshops des Themennetzwerks zeigte, dass ein gemeinsames Denkmodell erforderlich ist, um transdisziplinär mit Ingenieuren, Geistes-, Sozial- und Naturwissenschaftlern neue Lösungsansätze gemeinsam zu entwickeln, die gleichzeitig sowohl Security- als auch Safetyaspekte berücksichtigen. Ob und wie dies gelingen kann, daran arbeitet die Arbeitsgruppe unter Leitung von Prof. Dr.-Ing. Beyerer. Ihr Ziel ist es, mittels des „Systems Engineering" neue Denk- und Vorgehensmodelle zu entwickeln, die von Wissenschaftlern verschiedenster Fachdisziplinen genutzt werden können, um technische und soziotechnische Systeme ganzheitlich sicherheitsgerecht zu gestalten.

Die Arbeitsgruppe zum Thema „neue Technologien" unter der Leitung von Prof. Dr. Thoma hat zum Ziel, die Anforderungen zu ermitteln, die zukünftige Technologien aus der Sicht der ganzheitlichen Sicherheit erfüllen müssen. Kann sie ihr Ziel umsetzen, dann könnten diese in Folgeschritten mit den neuen Systemmodellen umgesetzt werden.

Dabei sind aber zwingend gesellschaftliche Entwicklungen zu beachten. Welche das sein könnten, untersucht die Arbeitsgruppe „Risikoforschung und Sicherheitskulturen" unter Leitung von Prof. Dr. Renn.

Um das komplexe Verhältnis von Sicherheit, Risikoempfinden und Vertrauen in Institutionen und neue Technologien näher beleuchten zu können, ist eine Betrachtung der Grundmechanismen der Wahrnehmungsforschung und des Vertrauens erforderlich. Diese wird aber auch beeinflusst durch die Kompetenzen der Menschen in der Gesellschaft. Dazu ist es erforderlich, den Zusammenhang von Sicherheit und Kompetenz sowie seine Bedeutung näher zu beleuchten. Dies hat sich die Arbeitsgruppe „Bildung und Kompetenz" unter Leitung von PD Dr.-Ing. habil. Risch zum Ziel gesetzt. Sicherheit ist eine Kernkompetenz für die Wettbewerbsfähigkeit und die Nachhaltigkeit für Unternehmen und die Gesellschaft. Die ersten Untersuchungen dieser Arbeitsgruppe zur Verzahnung von Aus- und Weiterbildung auf dem Gebiet der ganzheitlichen Sicherheit konnten den Widerspruch zwischen dem Erkennen der Bedeutung von sicherheitsrelevantem Wissen und dem Aufbau eines effizienten Aus- und Weiterbildungsmanagements einschließlich des erforderlichen Forschungsbedarfs verdeutlichen.

Innerhalb dieser Unterarbeitsgruppen werden die jeweiligen Themenschwerpunkte vorangetrieben und diskutiert. Die ersten Ergebnisse aus den einzelnen Unterarbeitsgruppen wurden im Mai 2009 in einem Workshop zusammengeführt.

Jede der Unterarbeitsgruppen hat im Rahmen dieses Workshops ihre Ergebnisse in Form eines gemeinsamen Beitrags präsentiert und zudem Forschungsnotwendigkeiten aus der Perspektive der jeweiligen Unterarbeitsgruppe dargestellt. Ebenso haben ausgewählte Initiativen zum Thema Sicherheit (unter anderem „Deutschland sicher im Netz", DsiN, Kompetenzverbund „Sicherheit und Gesellschaft", Fraunhofer-Verbund „Verteidigungs- und Sicherheitsforschung") an dem Workshop teilgenommen und ihre Sicht auf das Thema Sicherheit sowie den Handlungsbedarf in ihrem Themengebiet bezüglich Sicherheit dargestellt. Diese Initiativen wurden im Vorfeld des Workshops aufgrund ihres Blickwinkels und ihres Arbeitsradius' aus den Ergebnissen einer deutschlandweiten Recherche ausgewählt.

Die genannten Standpunkte aus dem Themennetzwerk und den Initiativen wurden ausführlich im Workshop diskutiert und gehen im Ergebnis in diesen Band ein. Der vorliegende Band aus der Reihe „acatech diskutiert" ist damit ein erstes Diskussionsergebnis des Themennetzwerks Sicherheit. Die Beiträge veranschaulichen die Vielschichtigkeit des Begriffs „Sicherheit" sowie die entsprechenden Denkmodelle und Lösungsansätze. Alle Beiträge gehen davon aus, dass die begriffliche und wissenschaftliche Trennung von „Security" und „Safety" überwunden werden muss.

Die Notwendigkeit für diese Forderung kann anhand des Beispiels „Konzeptionierung eines Kinderplatzes" veranschaulicht werden. Bei der Neuanlage von Kinderspielplätzen treffen aus verschiedenen Richtungen Anforderungen für Safety und/oder Security aufeinander: Die Eltern der Kinder, die dort spielen sollen, legen Wert darauf, dass die Spielgeräte sicher sind, um das Verletzungsrisiko für die Kinder möglichst gering zu halten. Des Weiteren sollte aus ihrer Sicht der Spielplatz idealerweise von jedem Ort auf dem Spielplatz vollständig einsehbar sein, um eine Beaufsichtigung der Kinder zu erleichtern und es potenziellen Entführern oder anderen Verbrechern möglichst zu erschweren, unbemerkt in die Nähe der Kinder zu gelangen. Die an der Anlage des Spielplatzes beteiligte Kommune ist ebenso wie die Eltern daran interessiert, sichere Spielgeräte zur Verfügung zu stellen, um eventuellen Schadensersatzansprüchen und schlechter Publicity aus dem Weg zu gehen und den gesetzlichen Vorschriften Genüge zu tun. Der Gesetzgeber wiederum hat neben den eben erwähnten Sicherheitsanforderungen bezüglich der spielenden Kinder auch Anforderungen, die die Sicherheit der für den Aufbau und die Wartung der Geräte sowie der Grünflächen des Spielplatzes zuständigen Personen betreffen (Arbeitssicherheit). Neben den eben dargestellten Sicherheitsanforderungen können beispielsweise noch vonseiten der Passanten oder Autofahreren,

die Sorge haben, sie bzw. ihre Fahrzeuge könnten durch geworfene Bälle oder andere Spielgeräte gefährdet sein, oder diversen anderen Seiten vielfältige, sicherheitsrelevante Anforderungen eine Rolle spielen. Wie das Beispiel verdeutlicht, trennen die einzelnen Anforderungsquellen (Eltern, Passanten etc.) nicht zwischen „Safety"- und „Security"-Politik. In den Wissenschaften ist diese Trennung hingegen gängige Praxis, was eine ganzheitliche Betrachtung der Sicherheit des Systems deutlich erschwert. Eine solche Betrachtungsweise ist allerdings notwendig, um ein möglichst hohes Niveau an Sicherheit zu gewährleisten.

Sowohl bei der Entwicklung von neuen Technologien oder Produkten als auch bei der Erstellung von Gebäuden, Organisationen oder anderen Einrichtungen müssen also sowohl Safety- als auch Security-Aspekte berücksichtigt werden. Unternehmen der Zukunft benötigen infolgedessen eine Kernkompetenz auf dem Gebiet der Sicherheit. Dabei ist „Sicherheit" im umfassenden Sinne gemeint, sowohl als Sicherheit des Arbeitsschutzes als auch des Datenschutzes und des Personenschutzes, um nur einiges zu nennen. Während die Praxis schon nach dieser Integration der verschiedensten Schutzziele sucht, ist die Förderpolitik getrennt auf „Security" und „Safety" ausgerichtet. Dies muss überwunden werden.

Im vorliegenden Band sind eine Reihe von Forschungsansätzen skizziert, die dazu beitragen könnten, die Bereiche von „Safety" und „Security" zu überbrücken. So kann zum Beispiel die Taxonomie, basierend auf dem Systems Engineering oder neuen gesellschaftlichen Konzepten, die auf zu entwickelnden Kompetenzen sowie zu erstellenden Sicherheitskulturen basieren, neue Sicherheitsmodelle schaffen.

Neue Sicherheitskonzepte erfordern eine entsprechende Kommunikation, Motivation, Kompetenzentwicklung sowie das Schaffen gesellschaftlicher Voraussetzungen. Auf dieser Basis können dann Zukunftstechnologien durch eine Systemanalyse und ein Systemdesign mehr Sicherheit garantieren – wie dies gegenwärtig in der Praxis bereits umgesetzt wird. Welche offenen Fragestellungen bestehen bleiben, wird im letzten Abschnitt „Zur Umsetzung von Sicherheit in der Praxis" veranschaulicht.

Die Mitglieder des Themennetzwerks Sicherheit beabsichtigen, mit der Veröffentlichung dieser Beiträge in dem vorliegenden Band Vertreter aller gesellschaftlichen Schichten anzuregen, mit uns gemeinsam die zu lösenden Aufgaben im Themenfeld Sicherheit zu lokalisieren und in einem Folgeschritt zu priorisieren. Ziel ist es, darauf aufbauend als Ergebnis einer breiten nationalen und internationalen Diskussion Empfehlungen für die Verbesserung bestehender Sicherheitskonzepte entwickeln zu können, die ein gesellschaftliches Grundbedürfnis darstellen.

# > THEMATISCHE UND BEGRIFFLICHE STRUKTURIERUNG DER AKTUELLEN SICHERHEITSFORSCHUNG

# 1 ZUKUNFTSTECHNOLOGIEN IN DER SICHERHEITSFORSCHUNG

KLAUS THOMA/BIRGIT DREES/TOBIAS LEISMANN

## 1.1 EINLEITUNG: SICHERHEITSFORSCHUNG – WARUM?

Sicherheit ist nicht nur für jeden Menschen ein hohes persönliches Gut, das die Lebensqualität maßgeblich bestimmt; Sicherheit nimmt auch eine Schlüsselrolle in der politischen Stabilität und Rechtsstaatlichkeit eines Landes ein. Zuverlässig funktionierende Infrastrukturen wie Versorgungsketten, Verkehrswege, Kommunikations- und Bankensysteme bilden die Basis der modernen Industriegesellschaften. Die zunehmende Konzentration der Bevölkerung in Ballungszentren, die wachsende Vernetzung unterschiedlichster Lebensbereiche und -funktionen sowie der Übergang zu einer global vernetzten Informations- und Dienstleistungsgesellschaft vergrößern dabei die Verwundbarkeit durch Naturkatastrophen, Angriffe und Störungen vielfältiger Art.[1]

Sicherheitsforschung zielt darauf ab, diese Verwundbarkeiten zu erkennen, zu analysieren und Vorschläge bzw. Technologien zur Minderung oder Vermeidung der Risiken zu entwickeln, ohne in die Freiheit oder die Rechte des Bürgers einzugreifen. Dem Bericht des European Security Research Advisory Board (ESRAB) folgend, wird „Sicherheitsforschung" hier als Forschungsaktivität verstanden, die einen Beitrag zum Schutz vor ungesetzlichen oder vorsätzlich schädigenden Handlungen gegenüber Menschen, Infrastrukturen oder Organisationen leistet. Dazu zählt auch die Minimierung der Schädigungen, die sich aus solchen aktiven Eingriffen, aus Naturkatastrophen oder als Folge von Industrieunfällen ergeben. Strategien und Verfahren zur zeitnahen Wiederherstellung der normalen Funktion des Systems oder der Infrastruktur nach einer Störung sind ebenso Thema der Sicherheitsforschung.[2] Übergeordnetes und langfristiges Ziel muss der Aufbau einer widerstandsfähigen, fehlertoleranten und robusten Infrastruktur sein. Bisher ist die Sicherheitsforschung (noch) nicht als eigenständige Forschungsrichtung etabliert. Wissen und Kompetenzen aus Ingenieurs- und Naturwissenschaften sowie Geistes- und Sozialwissenschaften müssen systematisch zusammengeführt werden, um zu koordinierten Lösungen von Sicherheitsproblemen zu gelangen.[3]

Da die Sicherheitsforschung ein sehr breites wissenschaftliches und politisches Querschnittsthema darstellt, sind zu ihrer Entwicklung neue Ansätze notwendig. Während anfangs eine technologieorientierte Herangehensweise vorherrschte, die einzelne grundlegende Technologien für die Sicherheitsforschung losgelöst voneinander entwi-

1 Reichenbach et al. 2008.
2 European Communities 2006.
3 Beyerer 2007.

ckelte und erst im Engineering des Endprodukts zusammenführte und nutzbar machte („bottom-up"), setzt sich zunehmend ein szenarienorientierter Ansatz durch, der von Bedrohungs- und Gefährdungsszenarien ausgeht („top-down"). Dieser zweite Ansatz soll zu systematischen, sicherheitsrelevanten Gesamtkonzepten führen und, basierend auf Risikoanalysen, die Angreifbarkeit und Verwundbarkeit der betrachteten Systeme minimieren.[4] Wie im Folgenden dargestellt, kommt dem letztgenannten Ansatz sowohl auf europäischer Ebene als auch in der nationalen Umsetzung der Sicherheitsforschung eine große Bedeutung zu.

## 1.2 SICHERHEITSFORSCHUNG IN EUROPA UND IN DEN USA

### 1.2.1 ENTWICKLUNG DER SICHERHEITSFORSCHUNG IN EUROPA

Die immer komplexer verknüpften Strukturen der modernen Industriegesellschaft führen zu einer zunehmenden Verwundbarkeit unseres Lebensraums. Die weltweite Vernetzung der Infrastrukturen macht eine stärkere internationale Zusammenarbeit in der zivilen Sicherheit notwendig.[5] Daher hat die Europäische Union eine umfassende Strategie zum Aufbau einer europäischen Sicherheitsforschung entwickelt.

Als ein entscheidendes Instrument zur Entwicklung einer europäischen Verteidigungs- und Sicherheitspolitik werden Anstrengungen im Bereich der Forschung und Technologie gesehen. Im Auftrag der Europäischen Kommission erarbeitete eine „Group of Personalities" (GoP) Handlungsvorschläge zum Aufbau einer europäischen Sicherheitsforschung. Diese Empfehlungen umfassen unter anderem den Aufbau eines EU-geförderten Sicherheitsforschungsprogramms, das Aufheben der Trennung zwischen ziviler und wehrtechnischer Forschung, um vorhandene Technologien besser zu nutzen, die Schaffung eines European Security Research Advisory Board (ESRAB) zur Entwicklung der Inhalte des geplanten europäischen Sicherheitsforschungsprogramms und die Förderung eines Markts für sicherheits- und wehrtechnische Produkte.[6]

Durch den Start eines mit geringen finanziellen Mitteln ausgestatteten Vorläuferprogramms zum Sicherheitsforschungsprogramm, des „Preparatory Action for Security Research" (2004 bis 2006), konnte sich eine europäische Sicherheitsforschungsszene unter Beteiligung von Industrie, Behörden und Forschungseinrichtungen in Ansätzen entwickeln.[7]

Das ESRAB-Gremium wurde konstituiert und erarbeitete ein umfassendes Konzept für eine europäische Sicherheitsforschung.[8] Basierend auf diesem Konzept wurde das Thema Sicherheitsforschung mit einer Förderung von 1,4 Mrd. Euro für den Zeitraum

4 Beyerer/Geisler 2007.
5 Thoma 2008.
6 European Communities 2004.
7 Eine Beschreibung der 39 PASR-Forschungsprojekte einschließlich der End- und Zwischenergebnisse ist abrufbar unter: http://ec.europa.eu/enterprise/security/articles/article_2007-02-23_en.htm.
8 European Communities 2006.

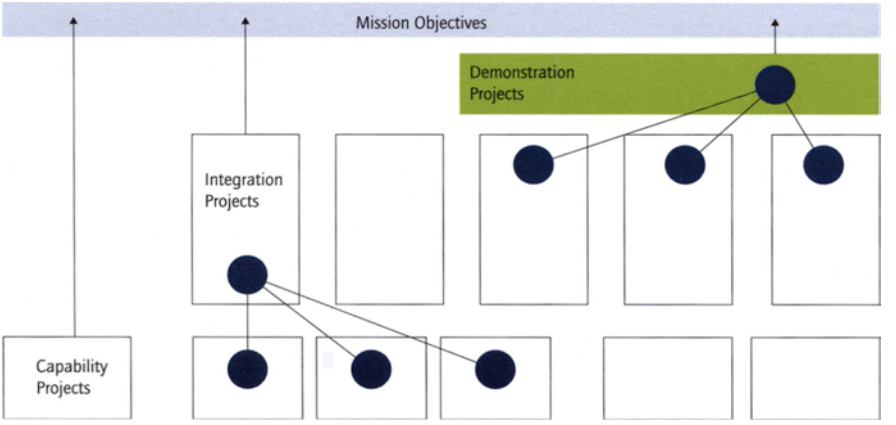
von 2007 bis 2013 als neues Schwerpunktthema im spezifischen Programm „Zusammenarbeit" in das 7. Forschungsrahmenprogramm der Europäischen Kommission aufgenommen.

Auf der Grundlage der Empfehlungen des ESRAB orientieren sich die Forschungsthemen des Rahmenprogramms inhaltlich an den vier Missionen:

- Schutz der Bürgerinnen und Bürger,
- Sicherheit von Infrastrukturen und Versorgungseinrichtungen,
- Schutz und Sicherung der europäischen Außengrenzen,
- Wiederherstellung der Sicherheit im Krisenfall.

Darüber hinaus werden noch die drei Querschnittsaktivitäten Integration und Interoperabilität von Sicherheitssystemen, Sicherheit und Gesellschaft sowie Koordinierung und Strukturierung der Sicherheitsforschung adressiert. Zur Erfüllung dieser Missionen werden bestimmte Fähigkeiten, sogenannte „Capabilities" benötigt. Diese Fähigkeiten sind die Grundbausteine zur Technologiedefinition, denn sie stellen die kleinste Einheit von Technologien und Prozessen dar, die benötigt werden, um eine bestimmte Funktion, Aufgabe oder Operation durchzuführen.[9] Abbildung 1 veranschaulicht den fähigkeitsbasierten Ansatz der Sicherheitsforschung und zeigt unterschiedliche Forschungspfade auf, um die Ziele der Missionen zu erreichen.

Abbildung 1: Forschungspfade des EU-Sicherheitsforschungsprogramms nach ESRAB[10]




9 European Communities 2006.
10 European Commission 2008, S. 6.

Zur Fortführung der mit dem ESRAB begonnenen strategischen und inhaltlichen Ausrichtung des Sicherheitsforschungsprogramms wurde 2007 das European Security Research Innovation Forum (ESRIF) gegründet. In diesem Gremium beraten ausgewählte Experten der Mitgliedsstaaten aus Forschung, Industrie, dem Bereich öffentlicher und privater Endnutzer, der EU-Kommission sowie dem Europäischen Parlament und anderen europäischen Organisationen über die langfristige strategische Planung und die Ausrichtung der Sicherheitsforschung in Europa. Bis Ende 2009 soll das ESRIF eine gemeinsame Agenda für Sicherheitsforschung aufstellen, die Empfehlungen enthalten wird zu den Themen „verbesserte Sicherheit von Infrastrukturen", „Kampf gegen das organisierte Verbrechen und den Terrorismus", „Wiederherstellung der Sicherheit in Krisenzeiten" sowie eine „Verbesserung der Grenzüberwachung und -kontrolle".

### 1.2.2 NATIONALE SICHERHEITSFORSCHUNGSPROGRAMME IM VERGLEICH

#### 1.2.2.1 DEUTSCHLAND

Auch auf nationaler Ebene wird auf die veränderte Sicherheitssituation reagiert. In Deutschland wurde das Thema Sicherheit als eines von 17 Zukunftsfeldern in die Hightech-Strategie der Bundesregierung aufgenommen, um so sicherheitsrelevante Entwicklungen im Bereich Forschung und Technologie schwerpunktmäßig zu fördern.[11] Sicherheitsforschung wird dadurch erstmals als Thema von herausragendem nationalen Interesse definiert. Um die Hightech-Strategie umzusetzen und um die systematische und strategische Forschung für die zivile Sicherheit zu stärken, wurde ein nationales Sicherheitsforschungsprogramm entwickelt, das gleichzeitig mit dem Sicherheitsforschungsprogramm im 7. Rahmenprogramm der EU anlief. In Deutschland wird die Entwicklung von neuartigen Sicherheitslösungen damit erstmals ressortübergreifend, d. h. in Abstimmung mit allen Bundesministerien, gefördert. Das Programm „Forschung für die zivile Sicherheit" ist auf den Schutz der Bürger gegen Bedrohungen durch organisierte Kriminalität, Terrorismus und die Folgen von Naturkatastrophen und Großunfällen ausgelegt. Der Schutz der sogenannten „kritischen Infrastrukturen" wie zum Beispiel Energieversorgungssysteme, Verkehrsnetze und Telekommunikationsstrukturen ist dabei ein zentrales Thema. Für den Zeitraum von 2007 bis 2010 ist dieses Programm mit 123 Mio. Euro ausgestattet.[12] Da es bisher keinen derartigen Forschungsschwerpunkt gab, müssen hier viele Verfahren, Strategien, Ziele und auch Märkte erst entwickelt werden, beziehungsweise vorhandenes Wissen sowie verfügbare Entwicklungen und Technologien müssen für die Sicherheitsforschung genutzt und angewandt werden.

Die Umsetzung erfolgt in Form von Verbundprojekten in zwei Programmlinien. Programmlinie 1 umfasst die „Szenarienorientierte Sicherheitsforschung". Ausgangspunkte sind nicht spezielle technische Problematiken, sondern konkrete Bedrohungssituationen.

[11] BMBF 2006.
[12] BMBF 2007.

Dadurch sollen alle Disziplinen aus Technik, Natur-, Geistes- und Sozialwissenschaften, die für eine Erarbeitung umsetzungsfähiger Sicherheitslösungen notwendig sind, eingebunden werden. Schwerpunkte sind Schutz und Rettung von Menschen, Schutz von Verkehrsinfrastrukturen, Schutz vor Ausfall von Versorgungsstrukturen und Sicherung der Warenketten. In der Programmlinie 2 wird die Erforschung von Querschnittstechnologien in „Technologieverbünden" verfolgt. Innovative Systeme werden aus bestehenden und neuen Technologien anwendungsnah entwickelt. Dazu zählen die Technologien zur raschen und mobilen Erkennung von Gefahrstoffen, zur Unterstützung von Sicherheits- und Rettungskräften, zur Mustererkennung und zur schnellen und sicheren Personenidentifikation durch Biometrie. Integraler Bestandteil des Programms ist die Betrachtung gesellschaftlicher und juristischer Dimensionen der Forschung. Dabei wird unter anderem kritischen Fragen zur Ethik, zur Akzeptanz von neu entwickelten Sicherheitslösungen oder zu deren rechtlichen Grundlagen nachgegangen.

Die Fraunhofer-Gesellschaft hat frühzeitig die Bedeutung der Sicherheitsforschung erkannt. Im Rahmen eines Portfolio-Prozesses wurde die Sicherheitsforschung als eines von zwölf langfristigen Innovationsthemen identifiziert. Die Fraunhofer-Innovationsthemen zeichnen sich durch ein herausragendes Innovationspotenzial, hohen Forschungsbedarf, Marktnähe und Fokussierung auf Fraunhofer-Kompetenzen aus.[13] Als Schwerpunkte wurden die Themen Sicherheit in Information und Kommunikation (Sicherheit durch IT-Systeme, IT-Sicherheit, Kommunikation für mehr Sicherheit), Krisen- und Katastrophenmanagement (Wiederherstellung der Sicherheit im Krisenfall), multisensorische Detektion und Identifikation für Gefahrenaufklärung und Überwachung, Detektion und Monitoring von Gefahrstoffen, Robotik, Schutzsysteme und Werkstoffe sowie Risikomanagement abgeleitet.[13]

Das nationale Sicherheitsforschungsprogramm ist passfähig zum 7. Forschungsrahmenprogramm und stellt daher eine wichtige Umsetzung und Ergänzung der sicherheitsrelevanten europäischen Forschung dar. Durch die Initiierung des nationalen Forschungsprogramms wird den deutschen Akteuren in Industrie und Forschung die Chance geboten, Kompetenzen und Know-how zu erwerben und sich auf dem europäischen und internationalen Markt für Sicherheitsprodukte und -technologien zu positionieren. Als ein zentrales Wissenschaftsforum für die Sicherheitsforschung hat sich die Konferenz „Future Security" etabliert.[14]

#### 1.2.2.2 FRANKREICH

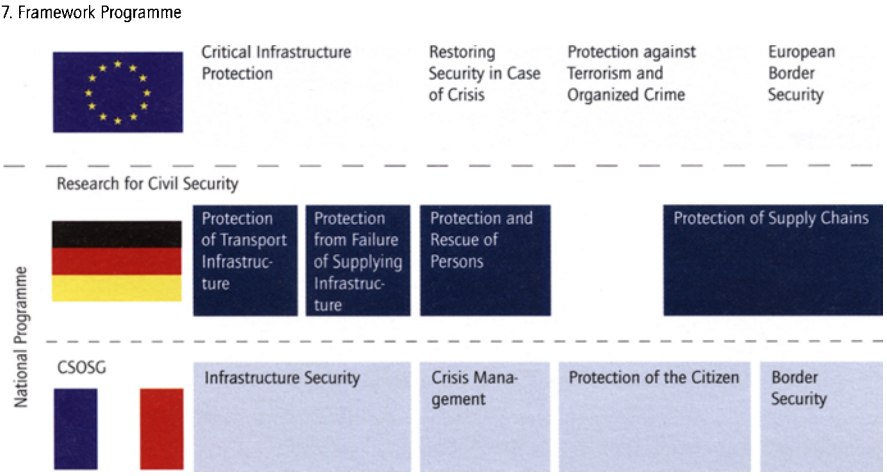
Die französische Sicherheitsforschung wird seit 2006 im Rahmen des nationalen Programms „Concepts, Systèmes et Outils pour la Securité Globale" (CSOSG) gefördert. Dieses Programm soll die Grundlage für die Forschung im Bereich der inneren Sicherheit bereitstellen und beinhaltet eine jährliche Fördersumme von ca. 11 Mio. Euro.[15] Gemein-

[13] Buller/Thoma 2006.
[14] Thoma 2008; siehe auch: www.vvs.fraunhofer.de.
[15] ANR 2009.

schaftlich gesteuert durch das französische Innenministerium (Ministère de l'Intérieur, de l'Outre-Mer et des Collectivités Territoriales), das Verteidigungsministerium (Ministère de la Défense) und die nationale Forschungsagentur (Agence Nationale de la Recherche, ANR) soll sowohl die projektbasierte Entwicklung sicherheitsrelevanter Technologien und Entwicklungen unterstützt als auch die französische Sicherheitsforschung für den europäischen Wettbewerb gestärkt werden.

Die Ausschreibungen zur Projektförderung innerhalb des CSOSG sind thematisch in vier Themengebiete unterteilt: Schutz der Bürger, Schutz von Infrastrukturen und Netzwerken, Grenzsicherheit und Krisenmanagement.[16] Damit lassen sich hier die übergeordneten Missionen, die der Zielformulierung in der europäischen Sicherheitsforschung dienen, klar in der nationalen Umsetzung wiederfinden (vgl. Abbildung 2).

Abbildung 2: Umsetzung der vier Missionen der europäischen Sicherheitsforschung in Schwerpunktthemen des deutschen und des französischen Sicherheitsforschungsprogramms. Die starke Ausrichtung des französischen Programms an dem europäischen wird deutlich.




Die Ausrichtung des französischen Programms an den europäischen Missionen zeigt Wirkung auf den Erfolg französischer Sicherheitsforscher im europäischen Vergleich: Im Jahr 2007 gingen 13 Prozent der Förderverträge (und damit 21 Mio. Euro Fördermittel)

[16] ANR 2009.

des Sicherheitsforschungsprogramms im 7. EU-Rahmenprogramm an französische Partner. Damit lag Frankreich auf dem vordersten Platz vor Großbritannien und Deutschland.[17]

Durch gemeinsame Ausschreibungen in der Sicherheitsforschung wird die Förderung der bilateralen Forschungszusammenarbeit Deutschlands und Frankreichs gestärkt und damit eine Entwicklung hin zu einer stärkeren europäischen Zusammenarbeit vorangetrieben. Beispielhaft zu nennen ist hier die nationale Förderausschreibung zur „Sicherheit der Warenkette" im Jahr 2009, die für bilaterale Verbundprojekte geöffnet wurde.[18]

### 1.2.3 THEMEN DER SICHERHEITSFORSCHUNG IN DEN USA

Ein Blick nach Nordamerika soll exemplarisch zeigen, welche sicherheitsrelevanten Themen außerhalb von Europa von Bedeutung sind. Dazu wird hier eine Studie des Nationalen Forschungsrats der USA zur Rolle von Wissenschaft und Technologie im Kampf gegen den Terrorismus herangezogen, die 2001 aufgrund der gewandelten Bedrohungssituation initiiert wurde.[19]

Der Bericht „Making the Nation Safer" charakterisiert die Spannweite der Bedrohungen der nationalen Sicherheit und benennt wichtige Möglichkeiten, wie durch langfristige Forschung und Entwicklung gegenwärtige und zukünftige Risiken minimiert werden können. Terroristische Anschläge mit nuklearen, radiologischen, toxischen oder explosiven Gefahrstoffen können auf Ziele wie die Gesundheit von Mensch und Tier, Informationstechnologien, Energiesysteme, Transportsysteme, Städte und bauliche Infrastruktur oder komplexe, untereinander verbundene und voneinander abhängige Systeme ausgerichtet sein. Solche Anschläge können auch weitreichende Auswirkungen auf Systeme und Infrastrukturen haben, die in enger Wechselbeziehung zu dem eigentlichen Ziel eines Anschlags stehen.

Aus diesen Bedrohungsszenarien werden Empfehlungen für Forschung und Entwicklung zur Erhöhung der Sicherheit abgeleitet. So sollen Risiko- und Schadensanalysen zu kritischen Infrastrukturen und Versorgungs- bzw. Transportsystemen helfen, sowohl Schwachstellen als auch Interdependenzen zu identifizieren. Dazu gehört auch die Modellierung verschiedener Anschlagsszenarien oder die Untersuchung von Ausbreitungscharakteristika gefährlicher chemischer oder biologischer Substanzen. Ebenso wie in Europa wird das zentrale Ziel verfolgt, robuste Systeme und Infrastrukturen zu entwickeln, die widerstandsfähig gegen terroristische Angriffe jeglicher Art und gegen Naturkatastrophen sind. Eine Schlüsselrolle in der Gefahrenabwehr nimmt auch hier

[17] Intelligence online 2008.
[18] BMBF 2009a.
[19] Committee on Science and Technology for Countering Terrorism 2002.

die Früherkennung von Bedrohungen (zum Beispiel durch versteckte Waffen) und die echtzeitnahe Detektion von Gefahrstoffen ein. Sensoren, die zuverlässig konventionelle Explosivstoffe und unkonventionelle chemische, biologische und radioaktive Stoffe detektieren können, wird auf beiden Seiten des Atlantiks eine entscheidende Bedeutung zugemessen. Auch bei Maßnahmen zur besseren Unterstützung von Rettungs- und Einsatzkräften vor (zum Beispiel durch Simulationssoftware) und während eines Einsatzes (Verbesserung der Informations- und Kommunikationssysteme) wird Entwicklungsbedarf gesehen. Eine schnelle Wiederherstellung von Transport- und Versorgungssystemen soll zur Vermeidung von Kaskadeneffekten beitragen. Forschungsbedarf besteht auch zu Aspekten der Dekontamination nach einem Schadensereignis.

Das Department of Homeland Security hat in einer Broschüre die Technologien zusammengestellt, die aus Sicht des Ministeriums für die zivile Sicherheit dringend erforderlich sind.[20] Diese werden unterteilt in die Bereiche Grenzschutz, Frachtsicherheit, chemische und biologische Abwehr, Internetsicherheit, Verkehrssicherheit, Counter-IED (Improvised Explosive Device), Krisenmanagement, Austausch von Informationen, Infrastruktursicherheit, Zusammenarbeit, maritime Sicherheit und das Screening von Personen. Eine repräsentative Liste der benötigten Technologien gibt Abbildung 3 wieder.

Die Ausführungen zeigen, dass es eine große Überlappung der Schwerpunktthemen im Bereich der Sicherheitsforschung in Europa und den USA gibt.

Abbildung 3: Prioritäre Technologien in der US-Sicherheitsforschung[20]

| | |
|---|---|
| BORDER SECURITY | - Detection, tracking, and classifying of all threats along the terrestrial and maritime border<br>- Improved ballistic protection via personal protective equipment<br>- Non-destructive tools that allow the inspection of hidden or closed compartments<br>- Ability for law enforcement officers to assure compliance of lawful orders using non-lethal means<br>- Ability for law enforcement personnel to quickly identify the origin of gunfire and classify the type of weapon fired<br>- Improved analysis and decision-making tools that will ensure the development and implementation of border security initiatives<br>- Non-lethal compliance measures for vehicles, vessels, or aircraft, allowing safe interdiction by law enforcement personnel |
| CARGO SECURITY | - Improved screening and examination by non-intrusive inspection<br>- Increased information fusion, anomaly detection, Automatic Target Recognition capability<br>- Detect and identify WMD materials and contraband<br>- Capability to screen 100 percent of air cargo |

[20] DHS 2008.

| | |
|---|---|
| CARGO SECURITY | - Track domestic high-threat cargo<br>- Positively ID cargo and detect intrusion or unauthorized access<br>- Reliable container seal security/detect intrusion devices |
| CHEMICAL-BIOLOGICAL DEFENSE | - Improved Chemical-Biological Forensic Analysis capability<br>- Handheld rapid biological and chemical detection systems<br>- Policy net assessments to provide fresh perspectives on fundamental elements of the national biodefense strategy<br>- Detection paradigms and systems for improved, emerging, and novel biological threats<br>- Tools to detect and mitigate animal disease breakouts<br>- National-scale detection architectures and strategies to address outdoor and indoor (for example, highly trafficked transportation hubs) and critical infrastructure<br>- Consequence assessment of attacks on chemical facilities and Chemical-Biological attacks on other critical infrastructure<br>- Integrated CBRNE Sensor Reporting capability<br>- Improved tools for integrated CBRN Risk Assessment<br>- Incident characterization capability for response and restoration<br>- Mechanisms to independently evaluate and validate commercially developed assays for the first-responder community to be public health actionable<br>- Tools for sampling, rapidly detecting, and identifying in the field illegal products, including high-consequence pathogens and toxins that threaten agriculture and the food industry |
| CYBER SECURITY | - Secure Internet protocols, including standard security methods<br>- Improved capability to model the effects of cyber attacks<br>- Comprehensive next-generation network models<br>- Composable and scalable secure systems<br>- Technologies and standards for managing the identities, rights, and authorities used in an organization's networks<br>- Information-system insider-threat detection models and mitigation technologies<br>- Analytical techniques for security across the IT system-engineering lifecycle<br>- Process Control Systems (PCS) security |
| TRANSPORTATION SECURITY | - Technologies to screen people for explosives and weapons at fixed aviation and mass-transit checkpoints<br>- System solutions for explosives detection in checked and carried bags<br>- Capability to detect homemade or novel explosives<br>- Optimized canine explosive detection capability<br>- Technologies for screening air cargo for explosives and explosive devices |
| COUNTER IED | - Capability to detect domestic use vehicle-borne improvised explosive devices (VBIEDs)<br>- Capability to assess, render safe, and neutralize explosive threats<br>- Capability to detect person-borne IEDs from a standoff distance<br>- Capability of inerting common explosives or making them less sensitive to initiation |

| | |
|---|---|
| COUNTER IED | - Techniques to track the origin of explosives and bomb components used in domestic IEDs<br>- Capability to mark explosives material to improve the detection of IED<br>- Low-cost and practical approaches to protect urban structures and occupants from VBIED attacks<br>- Protective measures to reduce damage and prevent catastrophic failure of high-consequence infrastructure assets subjected to IED attacks<br>- Models for the prediction of blast effects that take into account the diversity and variability of construction in urban settings<br>- Affordable blast-, fragment-, and fire-resistant materials<br>- Rapidly deployable blast-mitigation concepts for rapid threat response or temporary protection<br>- Tools to rapidly assess damaged structures<br>- Techniques and tools to stabilize damaged structures and prevent their collapse<br>- Capability to predict the threat of an IED attack<br>- Increased capability at vehicle or pedestrian ports of entry and border crossings to identify person born IED threats<br>- Enhanced capability for local officials to communicate understandable and credible IED warnings and instructions to the public |
| INCIDENT MANAGEMENT | - Integrated modeling, mapping, and simulation capability<br>- Personnel monitoring (emergency responder 3-D locator system) capability<br>- Personnel monitoring (physiological monitoring of firefighters) capability<br>- Incident management enterprise system<br>- Logistics management tool |
| INFORMATION SHARING | - Data fusion from law enforcement, intelligence partners, and other sensors to support the common operating picture (COP)<br>- Management of user identities, rights, and authorities<br>- Distribution of intelligence products<br>- Information sharing within and across sectors on terrorist threats<br>- Improvement of situational awareness and decision support<br>- Situational awareness between U.S. Coast Guard and partners<br>- Predictive analytics<br>- Protection of U.S. citizen personal data<br>- Improved cross-agency reporting of suspicious activity |
| INFRASTRUCTURE PROTECTION | - Analytical tools to quantify interdependencies and cascading consequences as disruptions occur across critical infrastructure sectors<br>- Effective and affordable blast analysis and protection for critical infrastructure, and an improved understanding of blast-failure mechanisms and protection measures for the most vital critical infrastructures and key resources (CI/KR)<br>- Advanced, automated, and affordable monitoring and surveillance technologies<br>- Rapid mitigation and recovery technologies to quickly reduce the effect of natural and manmade disruptions and cascading effects<br>- Critical utility components that are affordable, highly transportable, and provide robust solutions during manmade and natural disruptions |

| | |
|---|---|
| INTEROPERABILITY | – Accelerate the development of Project 25 and Internet Protocol (IP) interfaces<br>– Standardize, pilot, and evaluate emergent wireless broadband data technologies and applications<br>– Develop message interface standards that enable emergency-information sharing and data exchange<br>– Develop complementary test procedures<br>– Provide seamless access to voice and data networks, using a unified communications device<br>– Perform interoperability compliance testing on emergency response communications devices and systems |
| MARITIME SECURITY | – Wide-area surveillance from the coast to beyond the horizon, including port and inland waterways, for detection, ID & tracking<br>– Data fusion and automated tools for command center operations<br>– Improve the capability to continuously track contraband on ships or containers<br>– Develop improved ballistic personal protective equipment for officers<br>– Vessel compliance through less-lethal compliance<br>– Ability for law-enforcement personnel to detect and identify narcotics, chemical warfare agents, toxic industrial chemicals, explosives, and contraband materials |
| PEOPLE SCREENING | – Systematic collection and analysis of information related to understanding a terrorist group's intent to engage in violence<br>– Real-time detection of deception or hostile intent<br>– Capability in real time for positive verification of an individual's identity, using multiple biometrics<br>– Capability for secure, non-contact electronic credentials; contactless readers or remote interrogation technologies for electronic credentials<br>– Mobile biometrics screening capabilities, including handheld, ten-fingerprint-capture, environmentally hardened, wireless, and secure devices<br>– High-speed, high-fidelity ten-print capture capability<br>– Rapid DNA testing to verify family relationships during interviews for the disposition of benefits<br>– Remote, standoff biometrics detection for identifying individuals at a distance |

## 1.3 VOM FORSCHUNGSPROGRAMM ZU MARKTFÄHIGEN TECHNOLOGIEN

Das oberste Ziel aller Bemühungen in der Sicherheitsforschung ist, die Sicherheit der Bürgerinnen und Bürger zu gewährleisten. Es geht also zentral um die Fähigkeit, Bedrohungen und Gefahren abzuwehren oder zu minimieren bzw. Krisen zu bewältigen. Wie oben bereits beschrieben, definieren die nationalen und übergeordneten Programme dafür die wichtigen, zielführenden Themen. Doch mittels welcher konkreten Technologien können diese Fähigkeiten erreicht werden? An welchen Entwicklungen und Forschungsansätzen wird derzeit gearbeitet? Da die Entwicklung von Technologien wesentlich von Marktpotenzialen gelenkt wird, stellt sich auch die Frage, welche Sicherheitstechnologien kommerziellen Nutzen versprechen.

Um der Beantwortung dieser Fragen näher zu kommen, sollen im Folgenden zwei Ansätze verfolgt werden. Zunächst werden, ausgehend von den geförderten Forschungsprojekten, die Schwerpunkte der Technologieentwicklungen aufgezeigt. Daher werden hier hauptsächlich Technologien miteinbezogen, die eigens für den Bereich der zivilen Sicherheit entwickelt werden. Andere Entwicklungen, deren Nutzen für diese Disziplin vielleicht erst nachträglich erkannt wird, bleiben unberücksichtigt. Die zweite Herangehensweise stützt sich auf aktuelle Marktanalysen, die einen Hinweis auf die Entwicklung des Bedarfs an Sicherheitstechnologien geben sollen.

### 1.3.1 GEFÖRDERTE TECHNOLOGIEENTWICKLUNGEN

Der ESRAB-Report benennt eine Reihe von konkreten Technologiefeldern, die von entscheidender Bedeutung sind, um zukünftig den wichtigsten Sicherheitsanforderungen gerecht zu werden (vgl. Abbildung 4). Hierzu zählen viele sogenannte Schlüsseltechnologien, die in viele verschiedene Systeme integriert werden können bzw. müssen, um die Sicherheit in bestimmten Risikoszenarien zu gewährleisten. Einen hohen Stellenwert haben dabei beispielsweise Informations- und Kommunikationstechnologien, Systeme zur Entscheidungsunterstützung und Sensortechnologien. Diese Liste gibt den „top-down"-Ansatz des europäischen Entwicklungsprozesses der Sicherheitsforschung wieder. Die umfangreiche Anzahl der Technologiefelder wird aber nicht weiter priorisiert; dies geschieht erst mit der Veröffentlichung von Ausschreibungen und der nachfolgenden Auswahl von Verbundprojekten zur Förderung.

Abbildung 4: Prioritäre Technologiefelder nach Technologiebereichen (dem ESRAB Report entnommen)[21]

| TECHNOLOGY DOMAIN | PRIORITY TECHNOLOGY AREAS |
|---|---|
| Signal & information technologies | data collection/data classification, image/pattern processing technology, data and information management technology (DB etc.) |
| Artificial intelligence and decision support | text-mining/data-mining, IKBS/AI/expert techniques, knowledge management, modelling and simuation, optimisation and decision support technology |
| Sensor equipment | cameras, radar sensor equipment, CBRN sensors (in particular biological and chemical threat detection technologies), passive IR sensors equipments |
| Sensor technologies | hyperspectral/multispectral sensors, hyperspectral/multispectral processing, IR sensor technologies, Terahertz sensors, acoustic sensors – passive, optical sensors technologies |
| Communication equipment | reconfigurable communications, mobile secured communications, information security, network supervisor, network and protocol independent secured communications, communications network management and control equipment, secured, wireless broadband data links for secured communications, protection of communication networks against harsh environment |
| Human sciences | human behaviour analysis and modeling, population behaviour, human factors in the decision process, teams, organisations and cultures |
| Information security technologies | encryption and key management, data-mining, access control, filtering technologies, authentication technologies, encryption technologies (cryptography) |
| Computing technologies | protocol technology, SW architectures, secure computing techniques, high performance computing, high integrity and safety critical computing, software engineering |
| Information warfare/ intelligence systems | infrastructure to support information management and dissemination, cyber security policy management tools, optimisation, planning and decision support systems |
| Scenario and decision simulation | impact analysis concepts and impact reduction, advanced human behaviour modeling and simulation, simulation for decision making (real time simulation), structures vulnerability prediction, evacuation and consequence management techniques, mission simulation |
| Information systems | infrastructure to support information management and dissemination, cyber security policy management tools, optimization, planning and decision support systems |
| Navigation, guidance, control and tracking | RFID tags, tracking, GPS, radionavigation, direction finding and map guidance, bar code based tracing |
| Forensic technologies – biometry | fingerprints recognition (digital fingerprints), facial recognition, iris/retina, voice, handwriting, signature reconnaissance |

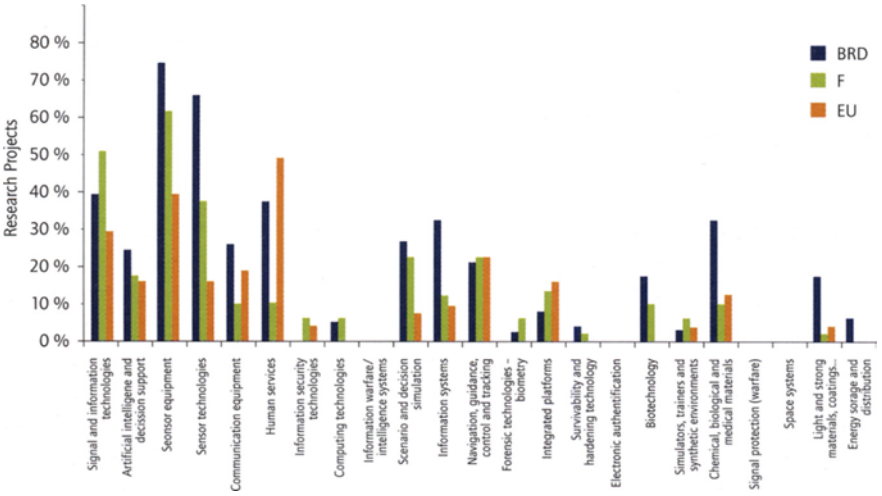
[21] European Communities 2006, S. 50.

| | |
|---|---|
| Integrated platforms | UAVs (air/land/sea), lighter than air platforms, surveillance and navigation satellites |
| Survivability and hardening technology | EMC evaluation and hardening, smart clothes and equipment, anti-blast glasses/concretes, critical buildings specific architectures, blast and shock effects |
| Electronic authentication | electronic tagging systems, smart cards |
| Biotechnology | rapid analysis of biological agents and of human susceptibility to diseases and toxicants, decontamination techniques, water testing and purification techniques, food testing and control techniques |
| Simulators, trainers and synthetic environments | virtual and augmented reality, tactical/crew training systems, command and staff training systems, synthetic environments |
| Chemical, biological and medical materials | chemical and biological detection systems |
| Space systems | earth observation (image and communications) |
| Light and strong materials, coatings... | light materials for human protection, smart textiles, light materials for site protection, self-protective and explosive resistant material technology, corrosion reduction |
| Energy generation storage and distribution | electrical generators, electrical batteries, energy distribution, microenergy technologies |

Um aus der gegenwärtigen Sicherheitsforschung ein Bild über die Technologien der Zukunft zu gewinnen, wurden die laufenden Forschungsprojekte des deutschen, französischen und europäischen Programms den ESRAB-Technologien zugeordnet (Abbildung 5). Dargestellt ist der Anteil der Projekte, die sich mit einer Technologie beschäftigen; ein Projekt kann dabei auch mehrere Technologien erforschen. Daraus ergibt sich ein „bottom-up"-Ansatz zur Priorisierung der Technologiefelder. Wichtig hierbei ist, dass die Grafik lediglich eine erste Momentaufnahme der aktuell geförderten Projekte in den Sicherheitsforschungsprogrammen wiedergibt. Dieser Prozess hat jedoch gerade erst begonnen. Während das Programm „Forschung für die zivile Sicherheit" der deutschen Bundesregierung noch bis 2010 läuft, hat das europäische Sicherheitsforschungsprogramm eine Laufzeit bis 2013. Daher stehen noch zusätzliche Ausschreibungen aus, die weitere wichtige Themenfelder adressieren und entsprechend zukunftsträchtige Technologien generieren werden. Abbildung 5 zeigt dennoch, dass die verschiedenen Forschungsprogramme zu einer ähnlichen Verteilung der Projekte führen, trotz der unterschiedlichen Art, die Ausschreibungen zu gestalten. So ist der Anteil der Projekte, die beispielsweise „Signal and Information Technologies" entwickeln, in Frankreich zwar am höchsten (50 Prozent), aber in Deutschland und der EU mit knapp 40 bzw. 30 Prozent auch nicht unerheblich. Andererseits ist die Entwicklung von „Integrated Platforms" bei allen Programmen mit maximal 15 Prozent der Projekte eher spärlich ausgeprägt.

Wo Themenbereiche in der aktuellen Forschung unterrepräsentiert sind, müssen die Forschungsprogramme nachsteuern, um das gesamte Spektrum der benötigten Entwicklungen abdecken zu können. Zu berücksichtigen ist aber, dass in einigen Themenbereichen bereits vielfältig nutzbare Technologien entwickelt worden sind (zum Beispiel Electronic ID, Smart Cards) und dass auch andere Forschungsprogramme (Informations- und Kommunikationstechnologien, Energie, Weltraum) sicherheitsrelevante Themen und Technologiefelder fördern.

Abbildung 5: Vergleich der projektbasierten Forschungs- und Entwicklungstätigkeiten Deutschlands (39 Verbundprojekte), Frankreichs (49 Projekte) und auf europäischer Ebene (31 Projekte). Die Technologieentwicklungen sind bezogen auf die Gesamtzahl der geförderten Projekte (kategorisiert nach den im ESRAB herausgestellten prioritären Forschungsfeldern, Forschung an mehreren Technologiefeldern in einem Projekt möglich, Stand: 1.3.2009.)




### 1.3.1.1 SENSORTECHNOLOGIEN

Besonders stark werden in allen drei Forschungsprogrammen bisher Sensorausrüstung und -technologien gefördert. Deutschland beteiligt sich an deren Entwicklung in herausragendem Maße: Von den insgesamt 39 vom BMBF geförderten Verbünden beschäftigen sich 29 unter anderem mit diesen Aspekten.[22] Sensortechnologien wird somit eine wichtige Rolle in der Sicherheitsforschung zuerkannt. Grund dafür sind wohl das sehr breite Einsatzspektrum und der erwartete hohe Nutzen durch den Einsatz von automatisierbaren, multisensorischen und mobilen Sensorsystemen.[23] Ein Schwerpunkt

[22] Stand: 1. März 2009.
[23] Thoma in: BMBF 2008.

der gegenwärtigen Sensorforschung liegt, vorangetrieben durch eine Förderbekanntmachung des BMBF im Jahr 2008, bei der Entwicklung von Detektoren von chemischen, explosiven und biologischen Gefahrstoffen.[24] Ein zentrales Forschungsfeld ist die Probenentnahme und die schnelle Detektion und Analyse von Gefahrstoffen vor Ort (auch aus großer Entfernung). Technologische Lösungen zur Detektion von hochtoxischen oder gefährlichen Substanzen in der Luft sind beispielsweise Systeme, mit denen Gasspuren angereichert und mittels gaschromatografischer Trennung über verschiedene Sensoren analysiert werden können. Biologische Breitbandsensoren zur Trinkwasserüberwachung oder portable Diagnostiksysteme mit Spektrometern zum Aufspüren und Erkennen bakterieller Kontaminationen sind Beispiele aktueller Entwicklungsansätze zur Detektion biologischer Gefahrstoffe. In Zukunft sollen Sensortechniken auch deutlich stärker zur Unterstützung von Einsatzkräften genutzt werden. Beispielsweise können energieautarke Funksensornetze Auskünfte über die Resttragfähigkeit von Bauwerken nach einer Explosion geben,[25] sodass Einsatzkräfte einsturzgefährdete Bereiche meiden können. Ein weiteres Forschungsfeld ist die Entwicklung innovativer Schutzanzüge mit integrierten Sensoren, die ein sicheres und zielgerichtetes Handeln der Einsatzkräfte unterstützen, unter anderem durch eine Überwachung der Vitalparameter der Einsatzperson, Messung der Umgebungsbedingungen oder durch integrierte Kommunikationssysteme mit Ortungsmöglichkeiten.[26] Darüber hinaus können Drohnen mit miniaturisierter Onboard-Sensorik zur Lageaufklärung aus der Luft beitragen.

Die gegenwärtige intensive Forschung im Bereich der Sensortechnologien wird in Zukunft einen verstärkten Einsatz von Sensoren in allen Bereichen der Sicherheit ermöglichen. Insbesondere die Nutzung von Multisensorsystemen und von vernetzten Sensorsystemen wird zu vielfältigen neuen Produkten und Anwendungen führen, was man in anderen Bereichen (zum Beispiel in der KFZ-Motorsensorik oder der Unterhaltungselektronik mit Mobiltelefonen voller Sensorik) schon heute beobachten kann.

Zukunftsweisende Technologien und vielversprechende Sicherheitslösungen sind aber auch in vielen anderen, in den Forschungsprogrammen bislang weniger stark berücksichtigten Themenfeldern zu erwarten. Daher ist es von entscheidender Bedeutung, dass die Sicherheitsforschung ebenso intensiv auch an andere prioritäre Forschungsfelder herangeht.

#### 1.3.1.2 RISIKO- UND GEFÄHRDUNGSANALYSEN

Simulationen spielen bei der Abschätzung der Wahrscheinlichkeit und des Ausmaßes eines terroristischen Angriffs oder einer Naturkatastrophe eine grundlegende Rolle. Solche Risiko- und Gefährdungsanalysen sollten Ausgangspunkt für die Einführung von Sicherheitsmaßnahmen sein, um so gezielt und effizient die zivile Sicherheit zu erhöhen. Einige solcher Software Tools und Programme sind bereits im Einsatz und bilden

[24] BMBF 2008.
[25] Riedel/Schäfer 2008.
[26] BMBF 2009b.

in zunehmend größerer Detailtreue die reale Welt ab; damit erlauben sie auch immer genauere Prognosen zu den Folgen beispielsweise eines terroristischen Anschlags mit Sprengstoff.[27]

Forschungs- und Entwicklungsbedarf besteht bei Simulations- und Optimierungsinstrumenten zur Unterstützung von Entscheidungsprozessen im Krisenfall. Nur bei Kenntnis der genauen Gefahren können geeignete Gegenmaßnahmen ergriffen werden. Die Simulation von Schlüsselfaktoren wie die Brand- oder Gefahrstoffausbreitung, Resttragfähigkeit von Gebäuden oder Evakuierungssituationen von Personenströmen trägt maßgeblich zum optimalen Einsatz von Rettungskräften bei. Verfahren zur automatischen Lagebewertung ebenso wie Systeme, die in Gefahrensituationen automatisch optimale Entscheidungen treffen, können die kritische Zeitspanne bis zur Einleitung von Maßnahmen zur Wiederherstellung der Sicherheit entscheidend verkürzen.

#### 1.3.1.3 SCHUTZ KRITISCHER INFRASTRUKTUREN

Die Entwicklung von baulichen Maßnahmen zum Schutz kritischer Infrastrukturen zielt vorrangig auf eine Erhöhung des Schutzes vor terroristischen Angriffen mit Explosivstoffen oder vor natürlichen Extremereignissen. Laufende Forschungsprojekte auf nationaler Ebene adressieren vor allem die Sicherheit von Verkehrsinfrastrukturen. In ihnen wird beispielsweise, basierend auf einer Risikoanalyse, die Implementierung von baulichen Schutzmaßnahmen an Flughäfen analysiert. Als weitere Innovationen sind unter anderem die Verwendung von energieabsorbierenden Materialien zur Ummantelung von Gebäuden, druckwellenbeständige Fassadenelemente oder die Entwicklung brandbeständiger ultrahochfester Betone und deren Verwendung zur Fertigung von Bauteilen zu nennen. Auch im Bereich des baulichen Schutzes sind weitere zukunftsweisende Entwicklungen zu erwarten, da im nächsten Aufruf zum Themenfeld Sicherheit im 7. EU-Rahmenprogramm mit entsprechenden Ausschreibungen zu rechnen ist. Dies betrifft zum einen die umfassende Maßnahmenrealisierung zur Erhöhung der Widerstandsfähigkeit von Verkehrsknotenpunkten (Flughäfen, Bahnhöfe, Häfen etc.) und zur Realisierung der dazugehörigen Infrastruktur im Rahmen eines Demonstrationsprojekts. Zum anderen sollen robuste, widerstandsfähige und gleichzeitig kostengünstige Materialen, Bauteile und Bauweisen für den Einsatz in kritischen Infrastrukturen entwickelt werden.

Eine sichere Energieversorgung ist in unserer technisierten Welt von entscheidender Bedeutung und stellt ein wichtiges Zukunftsthema in der Sicherheitsforschung dar. Sowohl die Informations- und Kommunikationssicherheit kritischer Energieinfrastrukturen als auch der bauliche Schutz, beispielsweise von öffentlichen Gebäuden, sind nicht nur wichtig für die wirtschaftliche Leistungsfähigkeit unserer Gesellschaft, sondern auch für die zivile Sicherheit. Kaskadeneffekte, die sich aus der Störung eines Energieversorgungsnetzes ergeben, könnten verheerende Auswirkungen haben. Somit müssen

[27] Häring/Dörr 2005.

Schutzmaßnahmen entwickelt werden, die einerseits direkt auf die Widerstandsfähigkeit kritischer Infrastrukturen zielen und andererseits auch interdependente Infrastrukturen und Systeme vor schädlichen Effekten bewahren. Eine Ausschreibung sowohl zur Entwicklung von Beurteilungs- und Identifikationsmethoden zur Verwundbarkeit von Kraftwerken und Energieversorgungsnetzen als auch zur Verstärkung solcher Infrastruktureinrichtungen wird für das dritte Arbeitsprogramm zum Thema Sicherheit des 7. Forschungsrahmenprogramms[28] erwartet.

#### 1.3.1.4 INFORMATIONSTECHNOLOGIEN UND BIOMETRIE

Informations- und Kommunikationstechnologien (IKT) haben in vielen Produktions- und Dienstleistungsbereichen eine zentrale Stellung in unserer heutigen Informations- und Wissensgesellschaft. Die Sicherheit von Computersystemen und Netzwerken ist daher auch für die Sicherheit der gesamten Bevölkerung von großer Bedeutung. Vor diesem Hintergrund verwundert es zunächst, dass gegenwärtig nur wenige Sicherheitsforschungsprojekte in den Themenfeldern „Information Systems" und „Computing Technologies" aktiv sind (vgl. Abbildung 3). Erklären lässt sich dies dadurch, dass Entwicklungen im Bereich IKT sowohl auf europäischer als auch auf nationaler Ebene in Parallelprogrammen gefördert werden.[29] Aspekte zur Sicherheit von IKT (zum Beispiel Internet, Datentransfer und -verwaltung, Kontrollsysteme, Software) gegenüber kriminellen Angriffen oder Missbrauch stellen dabei ein zentrales Anliegen dar. Innovative Verschlüsselungstechnologien zur sicheren Datenübertragung und sich selbst überprüfende und anpassende Netzwerke sind nur einige Beispiele für aktuelle Entwicklungen in der IT-Sicherheit. Widerstandsfähige Netzwerke mit einem zuverlässigen Sicherheitsmanagement sind auch Grundlage für die sichere Funktion kritischer Infrastrukturen (unter anderem Versorgungs- und Transportsysteme) und beispielsweise unverzichtbar im Bereich des Krisenmanagements und der Koordination von Einsatzkräften. Einige Projekte, die im Rahmen des IKT-Forschungsbereichs des 7. Forschungsrahmenprogramms derzeit durchgeführt werden, zielen auch auf Technologien, die direkt für die zivile Sicherheit eingesetzt werden können. Beispielsweise gehören hierzu die Entwicklung eines Terahertz-Verstärkers, die Widerstandsfähigkeit von Funksensornetzen oder ad-hoc Personal Area Networks (PAN) und Entwicklungsaspekte von Drohnen und Unterwasservehikeln zur Sicherheitsüberwachung von Objekten. Diese Beispiele zeigen, dass es deutliche Überlappungen zwischen den Forschungsbereichen IKT und Security gibt. Das BMBF hat daher für die IT-Sicherheitsforschung in den nächsten fünf Jahren Fördermittel in Höhe von 30 Mio. Euro vorgesehen.[30] Darüber hinaus untersucht das Bundesamt für Sicherheit in der Informationstechnik (BSI) als zentraler IT-Sicherheitsdienstleister des

[28] Die Ausschreibung ist für den Juli 2009 vorgesehen.
[29] Nationales Forschungsförderungsprogramm: IKT 2020 – Forschung für Innovationen (Laufzeit 2007 bis 2011).
[30] BMBF 2009c.

Bundes mögliche Risiken und Gefahren beim Einsatz von Informationstechnik, entwickelt entsprechende Sicherheitsvorkehrungen und analysiert Entwicklungen und Trends in der Informationstechnik.

Ebenfalls im Forschungsbereich IKT des europäischen Rahmenprogramms werden derzeit Projekte zum Thema Biometrie gefördert. Entwicklungsansätze sind hierbei beispielsweise die multiple biometrische Authentifizierung von Personen oder die Kombination von Kryptografie und Fingerbiometrie, um eine äußerst zuverlässige biometrische Identifikation zu erreichen bei gleichzeitiger Gewähr von Datenschutz und Privatsphäre. Eine Ausschreibung im Bereich Biometrie innerhalb des deutschen Sicherheitsforschungsprogramms ist noch nicht erfolgt, was die geringe Forschungsaktivität zu diesen Themen erklärt (vgl. Abbildung 3). Weitere technologische Innovationen sind hier also noch zu erwarten.

### 1.3.2 MÄRKTE FÜR SICHERHEITSTECHNOLOGIEN

Sicherheitstechnologien dienen nicht nur der Erhöhung der Sicherheit, sie haben auch ein großes wirtschaftliches Potenzial. Der Markt für sicherheitstechnische Produkte und Dienstleistungen hatte 2005 allein in Deutschland ein Umsatzvolumen von 10 Mrd. Euro bei hoher Wachstumsrate. Eine Förderung ziviler Sicherheitstechniken bedeutet daher gleichzeitig eine große Chance für Zukunftsmärkte.[31]

Der Markt für Sicherheitstechnologien und -dienstleistungen ist sehr breit gefächert und umfasst ein Spektrum, das von Überwachungssystemen über biometrische Zugangskontrollen bis hin zu Maßnahmen zur baulichen Verstärkung von Gebäuden reicht. Die prognostizierten Wachstumsraten für verschiedene Sicherheitstechnologien weisen darauf hin, welche Technologien sich auf dem Markt von morgen wahrscheinlich durchsetzen werden. Auf der Grundlage verschiedener Marktstudien können hier nur beispielhaft einige vielversprechende Technologiefelder genannt werden.

Sensorik als Technologie mit einem weiten Anwendungsfeld wird unter anderem in der Flughafensicherheit (Gesamtwachstumsrate von 34,3 Prozent von 2005 bis 2010) und Containersicherheit eingesetzt. Forschung an Technologien zur echtzeitnahen Lokalisierung (RTLS) und automatischen Identifizierung von Gegenständen findet derzeit nur in moderatem Maße statt und zielt unter anderem auf die Integration von RFID-Sensoren in komplexe Systeme. Dem europäischen Markt für RFID-Systeme im Bereich der Containersicherheit wird beispielsweise eine Wachstumsrate von 7,7 Prozent, gemittelt für den Zeitraum 2006 bis 2013, vorausgesagt.[32]

---

[31] BMBF 2006.
[32] Frost/Sullivan 2007a.

Unabhängig von der Einsatzumgebung werden tragbare Gefahrstoff-Detektoren in den kommenden Jahren von steigender Bedeutung sein. Sensortechnologien zur berührungslosen Detektion von CBRNE[33]-Stoffen, zum Beispiel für das Explosivstoff-Screening unbeaufsichtigter Gepäckstücke an öffentlichen Orten, haben hohe Wachstumsaussichten am Markt.[34] Für Explosivstoff-Detektionssysteme an Flughäfen etwa wurde in einer Studie von 2007 eine Wachstumsrate von 52,5 Prozent prognostiziert (im Zeitraum von 2005 bis 2010).[35] Das zeigt, dass Markt und Forschung hier in die gleiche Richtung zielen.

Smart Cards, obwohl in der Forschung nicht mehr stark vertreten, haben dennoch ein globales Marktwachstum von 12 Prozent (von 2007 bis 2012).[36] Innerhalb der Sicherheitstechnologien werden Smart Cards vor allem im Bereich der Zugangskontrollen, insbesondere in Verbindung mit biometrischen Sensoren, eingesetzt. Letzere werden sich in Zukunft immer mehr durchsetzen. Derzeit wird zwar ein Großteil des Markts (44,5 Prozent) für biometrische Technologien immer noch von Regierungsanwendungen bestimmt;[37] Fingerabdruckscanner beispielsweise sind jedoch schon zur Massenware geworden. Auf dem europäischen Markt wird ein starkes Wachstum von über 60 Prozent für biometrische Sensortechnologien erwartet.[38]

Im Forschungsfeld der Videoüberwachung sind bereits viele Technologien verfügbar, die sich in einigen Bereichen fest in der Sicherheitsarchitektur etabliert haben. Der Markt für Videoüberwachungstechnologien (einschließlich CCTV) ist bereits relativ gesättigt. Dennoch wird für die nächsten Jahre von einem geringen Wachstum von 4,6 Prozent (von 2006 bis 2012) ausgegangen.[39] Ein Grund dafür ist die Entwicklung und zunehmende Umrüstung von einfachen, analogen Anlagen hin zu komplexen, vernetzten computergestützten Systemen. Aktuelle Forschungsthemen in diesem Bereich sind unter anderem die optische Detektion und das Tracking von Personen, Fahrzeugen oder Gepäckstücken, intelligente Bewegungsanalysen, die auffälliges Verhalten erkennen, sowie die Kombination der Signale von festinstallierten und tragbaren Überwachungskameras.

Da Faktoren wie Qualität und Zuverlässigkeit gerade auf dem Markt für Sicherheitstechnologien eine wichtige Rolle für den Erfolg eines Produkts spielen, stellt die Entwicklung international einheitlicher Standards eine besondere Herausforderung für die Zukunft dar.

33 Chemical, Biological, Radioactive, Nuclear, Explosives (CBRNE).
34 Frost/Sullivan 2005.
35 Frost/Sullivan 2007b.
36 Frost/Sullivan 2008a.
37 Frost/Sullivan 2009.
38 Frost/Sullivan 2008b.
39 Frost/Sullivan 2007c.