Bonn International Center for Conversion
B·I·C·C

Bonn International Center for Conversion • Internationales Konversionszentrum Bonn

Innovationen zum Schutz deutscher Flughäfen vor Anschlägen

Sicherheitstechnologien und Arbeitsplätze am Beispiel des Düsseldorfer Flughafens

Ein Projekt der Hans-Böckler-Stiftung

Endbericht

BONN INTERNATIONAL CENTER FOR CONVERSION

B·I·C·C

Innovationen zum Schutz deutscher Flughäfen vor Anschlägen. Sicherheitstechnologien und Arbeitsplätze am Beispiel des Düsseldorfer Flughafens.

Endbericht

abgeschlossen am 5.2.2008

HBS-Projektnummer S-2007-41-1

Dr. Hartmut Küchle (Projektbearbeiter)
E-mail: kuechle@bicc.de
Bonn, 30. Januar 2008
Tel: 0228-91196-60

Inhalt

1. Kritische Infrastrukturen

Die modernen, komplexen Industriestaaten des Westens sehen sich – besonders seit dem 11. September 2001 und den nachfolgenden Anschlägen in Europa – vielfältigen Herausforderungen für die gesamtstaatliche Sicherheit gegenüber: Internationaler Terrorismus, organisierte Kriminalität, Drogen- und Menschenschmuggel, politische und wirtschaftliche Konflikte. Gerade Deutschland als Gesellschaft mit praktizierter Freizügigkeit im Informations-, Personen- und Warenverkehr und als exportorientierte Wirtschaftsnation ist ihnen in besonderem Maße ausgesetzt (Beckstein 2004). Deutschlands politische und wirtschaftliche Strukturen, vor allem aber seine kritische Infrastruktur, sind verwundbarer geworden.

Zur kritischen Infrastruktur zählen Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen einträten. Die Bundesregierung ordnet folgende Sektoren den kritischen Infrastrukturen zu:

- Transport und Verkehr (Luftfahrt, Seeschifffahrt, Bahn, Nahverkehr, Binnenschifffahrt, Straße, Postwesen);
- Energie (Elektrizität, Kernkraftwerke, Mineralöl, Gas);
- Gefahrstoffe (Chemie- und Biostoffe, Gefahrguttransporte, Rüstungsindustrie);
- Informationstechnik und Telekommunikation;
- Finanz-, Geld- und Versicherungswesen (Banken, Versicherungen, Finanzdienstleister, Börsen);
- Versorgung (Gesundheits-, Notfall- und Rettungswesen, Katastrophenschutz, Lebensmittel- und Wasserversorgung, Entsorgung);
- Behörden, Verwaltung und Justiz (staatliche Einrichtungen);
- Sonstiges (Medien, Großforschungseinrichtungen sowie herausragende oder symbolträchtige Bauwerke, Kulturgut) (Bundesministerium des Innern 2005b).

Die vorliegende Studie exemplifiziert sowohl die drohenden Gefahren als auch die technologischen Lösungsmöglichkeiten zur Reduzierung dieser Gefahren anhand von Flughäfen, die zweifelsohne besonders neuralgische Sicherheitszonen darstellen. Das ergibt sich schon aus ihrer ökonomischen Bedeutung, wie das Beispiel des Flughafen Düsseldorf International zeigt, der einer der modernsten in Deutschland ist. Er ist im Jahr 2007 mit fast 18 Millionen Passagieren der drittgrößte im ganzen Land. Er verzeichnet ein überdurchschnittliches Wachstum von 7,5 Prozent bei Passagieren insgesamt und von 17 Prozent im Interkontinentalverkehr und entwickelt sich damit zu einem internationalen Drehkreuz. Die Zahl der Starts und Landungen ist um 6 Prozent auf 228.000 Flugbewegungen gewachsen[1]. Sein Einzugsgebiet ist mit 18 Millionen Menschen der siebtgrößte Wirtschaftsraum der Welt.

[1] Frankfurter Allgemeine Zeitung, 29.12.2007.

Hier werden jährlich 97.000 Tonnen Luftfracht umgeschlagen. 230 Unternehmen haben ihren Sitz auf dem Flughafengelände. Mit 16.000 Beschäftigten ist der Flughafen ein Jobmotor der ganzen Region. Nach einer Faustformel zieht ein Arbeitsplatz am Flughafen mindestens zwei weitere in der Region nach sich. 50.000 Arbeitsplätze in Nordrhein-Westfalen hängen von der Funktionsfähigkeit des Düsseldorfer Flughafens ab. Der Flughafen ist darüber hinaus auch ein Kongress- und Tagungsort und wird täglich von bis zu 70.000 Menschen frequentiert[2]. Ein Anschlag würde zu einer wirtschaftlichen Katastrophe nicht nur in der Landeshauptstadt, sondern in der ganzen Region führen. Folglich ist der Schutz der Flughäfen für eine moderne, hochindustrialisierte Gesellschaft lebenswichtig.

Deshalb ist im Folgenden zu fragen nach den besonderen Bedrohungen bzw. Sicherheitslücken an Flughäfen und nach den technologischen Lösungsmöglichkeiten, um ihnen zu begegnen. Verfügen deutsche Unternehmen über die notwendigen Kernkompetenzen bei diesen Innovationen, um den sich weltweit entwickelnden Markt zu bedienen? Kann die Politik die notwendigen Investitionen in Sicherheitstechnologien nutzen, um dabei den Technologiestandort Deutschland und die Schaffung qualifizierter Arbeitsplätze zu fördern?

2 www.duesseldorf-international.de

2. Sicherheitsrelevante Problembereiche

Die Gefahren für die kritische Infrastruktur im Allgemeinen drohen von unterschiedlicher Seite:

- Natürliche Ereignisse (Extremwetterlagen, Flächenbrände, Epidemien etc.);
- Menschliches und technisches Versagen (Brände, Freisetzung von Gefahrstoffen, Explosionen);
- Terrorismus und kriminelle Handlungen (Drogen- und Menschenschmuggel, Brandstiftung, Flugzeugentführung, Einsatz von Sprengstoff) (Bundesministerium des Innern 2005a).

Hier wird zunächst deutlich, dass der deutsche Sicherheitsbegriff nicht zwischen technischer Sicherheit (s*afety*) und Sicherheit vor Angriffen (*security*) unterscheidet. Beide haben zwar vielfach ähnliche Auswirkungen und erfordern den Einsatz derselben Organisationen wie Polizei und Feuerwehr. Im Mittelpunkt der aktuellen Debatte und dieser Studie steht jedoch der Securityaspekt. Sicherheitsexperten sind u.a. besorgt, dass die Luftverkehrskreuze von Terroristen benutzt werden könnten, um Menschen, Drogen und andere gefährliche Stoffe zu schmuggeln. Außerdem wird befürchtet, dass große Passagierflugzeuge von Terroristen angegriffen und wie am 11. September als fliegende Sprengladung benutzt werden könnten.

Der Schock des 11. September 2001 sitzt immer noch tief im öffentlichen Bewusstsein Amerikas (US General Accounting Office 2007). Dennoch ist es US-amerikanischen Untersuchungen zufolge höchst unwahrscheinlich, dass sich dieser Vorfall so oder ähnlich wiederholen wird. Die größere Gefahr wird vielmehr darin gesehen, dass Verkehrsmaschinen aber auch private und eher kleine Flugzeuge als Transportmittel benutzt werden, um Terroristen und gefährliche Stoffe ins Land zu bringen, wie der Drogenschmuggel aus Lateinamerika schon seit Jahrzehnten demonstriere. Die Sicherheitsstandards seien in den Vereinigten Staaten immer noch zu lax (Carafano 2007).

Als wichtigste sicherheitsrelevante Problembereiche an Flughäfen werden genannt:

- Passagier- und Gepäcksicherheit;
- Frachtsicherheit;
- Infrastruktursicherheit und
- Systemintegration (Zintel 2007).

Experten weisen darauf hin, dass es diese Sicherheitslücken im Prinzip auch schon früher gegeben habe. Da es sich aber bei den Schutzmaßnahmen nicht zuletzt um ein Kosten-Nutzen-Problem handelt, erhielten sie erst durch konkrete, meist spektakuläre Vorkommnisse der letzten Jahre besondere Beachtung und Priorität. So seien im Rahmen der nun verschärften

Kontroll- und Sicherheitsmaßnahmen auch bestimmte Personengruppen, wie Dienstleister, Reinigungspersonal etc., die früher nicht ausreichend überprüft und kontrolliert worden seien, in den Fokus der Sicherheitsspezialisten geraten[3]. Auch mit bestimmten Sprengstoffen oder einer schmutzigen Bombe habe man früher kaum gerechnet, obwohl es sie gab. Die Eintrittswahrscheinlichkeit eines Sprengstoffanschlags sei damals als äußerst gering eingestuft worden. Erst durch die aktuellen Anschläge habe sich die Situation dramatisch geändert, so dass bestimmte Gefahren zentrale Aufmerksamkeit und dafür geeignete Lösungen finanzielle Förderung erhalten.

So ist in Europa am 19. Januar 2003 die Luftsicherheitsverordnung (EG Nr. 2320/2002) in Kraft getreten, und seit dem 11. Januar 2005 gilt das Luftsicherheitsgesetz, in dem die behördlichen Sicherheitsmaßnahmen, die Zuverlässigkeitsüberprüfungen und die Eigensicherungsmaßnahmen der Flughafenbetreiber und Luftfahrtunternehmen geregelt sind. Hier wurden erstmals alle Sicherheitsmaßnahmen für den Luftverkehr in einem Gesetz zusammengefasst, was den Überblick und die Anwendung sehr erleichtert.

Die Airportsicherheit nach §§5 und 8 LuftSiG umfasst:

- Personen- und Handgepäckkontrollen;
- Reisegepäckkontrollen;
- Personal- und Warenkontrollen;
- Identitätskontrollen und
- Objektschutz für Flughafenanlagen.

Zu den Risiken des internationalen Frachtverkehrs gehören neben dem wirtschaftsschädigenden Import von Markenfälschungen und Plagiaten vor allem das verdeckte Einschleusen von Gefahr- und Explosionsstoffen oder Suchtmitteln. Deshalb ist eine genaue Festschreibung der Frachtinformationen bei der Verladung von entscheidender Bedeutung (Bernnat 2004; ;Emery, Werchan und Mowles 2006; ;Klein 2007). Aufgrund des internationalen und transkontinentalen Luftverkehrs ist es außerdem notwendig, den konkreten Flughafen nicht mehr isoliert, sondern in Zusammenhang mit anderen Flughäfen zu betrachten, aus denen die Passagiere oder die Fracht kommen. Nach Auskunft des Flughafens werde heute jeder Wechsel einer Person oder eines Fahrzeugs von der „Landseite auf die Luftseite“ kontrolliert, außerdem natürlich alle Passagiere und das aufgegebene Fluggepäck ohne Ausnahme[4].

Dabei sind allerdings unterschiedliche Sichtweisen zu beachten. Während es bei den notwendigen Kontrollen aus Sicht der Sicherheitsorgane auf hohe Zuverlässigkeit ankommt, um keine Schlupflöcher zu lassen und um Fehlalarme zu vermeiden, die teuer sind und ein Akzeptanzproblem in der Öffentlichkeit schaffen, kommt es aus Sicht der Nutzer auf Komfort und

3 Expertengespräche.

4 Expertengespräche.

Schnelligkeit an[5]. Wenn die Fluglinien und die Flughäfen Geld verdienen wollen, dann müssen sie ihren Kunden diskriminierungsfreie Sicherheit bieten (Rachel 2006) und deshalb in entsprechende Sicherheitstechnologien investieren. Da die Globalisierung der Wirtschaft und der hohe Freizeitanteil zu immer stärkerer Reiseaktivität führen, sind in Zeiten des internationalen Terrorismus und anwachsender organisierter Kriminalität Maßnahmen, Systeme und Prozesse erforderlich, die das Risiko des Reisens so angenehm und so sicher wie möglich machen.

5 Expertengespräche.

3. Technologien

Obwohl unter Experten Einigkeit darüber besteht, dass für ein offenes System, wie es ein Flughafen darstellt, absolute Sicherheit nicht zu garantieren sei6, zeigen sie sich überzeugt, dass Sicherheitstechnik die Gefahrenabwehr sowie Maßnahmen zur Herstellung von Sicherheit und Ordnung in allen Phasen unterstützen könne: Sie kann zur **Analyse von Gefahren- und Bedrohungssituationen** eingesetzt werden und sie kann der **Prävention** dienen. Die **Lagebeurteilung** kann durch technische Systeme erleichtert werden, die **Komplexität von Intervention und Management** bei Schadensereignissen kann handhabbarer gemacht werden und bei der **Rehabilitation von Schadensräumen** wirkt Sicherheitstechnik unterstützend (Floeting 2006).

Als Vorteile des Einsatzes von Sicherheitstechnik werden genannt:

- die Programmier- und Parametrierbarkeit von Sicherheitstechnik und damit die Zuverlässigkeit des Funktionierens;
- die Effizienz von Sicherheitstechnik aufgrund der hohen Verfügbarkeit, Dauerhaftigkeit, technischen Wirksamkeit und Genauigkeit;
- die Innovationsorientierung von Sicherheitstechnik;
- die Kosten-Nutzen-Effizienz, die insbesondere unter Berücksichtigung von potenziellen verhinderten Schäden, verminderten Versicherungskosten usw. bewertet werden muss (Floeting 2006).

Die Bandbreite an Technologien, die zum Schutz vor Terrorismus und organisierter Kriminalität eingesetzt werden können, ist groß. Sie reicht von der Sammlung von Telekommunikationsdaten über Videoüberwachung und biometrische Zutrittskontrollen bis zum Durchleuchten von Personen. Dabei lassen sich vier Grundtechnologien unterscheiden, nämlich **Kommunikationstechnologien**, **biometrische Technologien**, **Sensoren** sowie **Datenspeicherung und -auswertung**. Zentrale Elemente dieser Technologien kommen auch beim Schutz der Flughäfen zur Anwendung wie z.B. intelligente Eingangskontrollen, Sprengstoffdetektion, Robotiktechnologien zur Entschärfung von Bomben, vernetzte Aufklärung innerhalb und außerhalb von Gebäuden bis hin zum Schutz der Startbahnen vor Flugkörperbeschuss (Hauschild 2007).

3.1 Detektionssysteme

Bei der Verhinderung von Terroranschlägen auf Flughäfen, zur Abfertigung von Passagieren, Gepäck und Fracht im Luftverkehr sind Detektionssysteme zur Auffindung von Sprengstoffen und toxischen Gasen unverzichtbar. Diese gibt es auf Basis von Röntgenstrahlen, Mikrowellen und Gasabsorption. Eine Entschärferausstattung besteht gegenwärtig aus Bombenschutz-

6 www.fisgmbh.de

anzügen, verschiedenen Fernlenkmanipulatoren, USBV-Röntgengeräten und Wassergewehren etwa zum Öffnen verdächtiger Gepäckstücke (Weisswange 2007). Zum Aufspüren von Gefahrgütern an Flughäfen mussten bisher Spürhunde zu hohen Kosten eingesetzt werden. Die EADS hat nun „künstliche Spürnasen" entscheidend weiterentwickelt. Sie zeichnen sich – basierend auf dem Prinzip der Ionen-Mobilitäts-Spektronomie – durch höhere Genauigkeit, Schnelligkeit und geringere Fehlerquoten aus. Hierzu werden Laser- und spektroskopische Verfahren kombiniert, die es gestatten, schon kleinste Partikelspuren zu erkennen (Hellenthal 2006).

Das Fraunhofer Institut geht bei seiner Suche nach verbesserten Geräten zum Nachweis von Sprengstoffen von zwei verschiedenen Ansätzen aus. Einerseits werden bildgebende Systeme auf der Basis von Röntgenstrahlung oder eine Bestrahlung mit Neutronen eingesetzt. Andererseits versucht man, Spuren nachzuweisen, die der Sprengstoff an die Umgebung abgibt (Fraunhofer Institut 2007a). Dies erreicht man mit der Ionenmobilitäts-spektrometrie und mit der Massenspektrometrie. Bei den Sicherheits-kontrollen von Personen und Gepäckstücken in der zivilen Luftfahrt werden besonders leistungsfähige Systeme benötigt. Die Untersuchung des Gepäcks erfolgt hauptsächlich durch Röntgengeräte, während bei der Personenkontrolle meist Sprengstoffdetektoren eingesetzt werden, die es als tragbare und als feststehende Systeme gibt. Für die Zukunft hofft man, leistungsfähigere Detektionssysteme durch eine Kombination unterschied-licher Nachweisprinzipien in einem System zu erhalten. Durch Nutzung der jeweiligen Vorteile der unterschiedlichen Verfahren könnte es möglich werden, die heute noch häufigen Fehlalarme zu senken. Auch an neuen Nachweismethoden wird gearbeitet. Ein neuer Ansatz wird beispielsweise in der Verwendung von elektromagnetischer Strahlung im Tetrahertzbereich gesehen (Fraunhofer Institut 2007c). Im Bereich Millimeterwellen zur Personenkontrolle wird ebenfalls gearbeitet[7], weil die WTO Geräte auf Röntgenbasis nicht für optimal hält.

Zur Personenkontrolle auf Sprengstoffspuren sind „*Explosive Trace Portals*" entwickelt worden. Hierzu nennt (Davis 2006) folgende Technologien: *Chemical detection paper* sei eine leicht reagierende und gleichzeitig einfache und preiswerte Aufspürtechnik. M256A1 könne Nervengas und Senfgas aufspüren und ihre Konzentration reduzieren. *Colorimetric tubes* von Draeger und RAE Systems benutzen enzymische Techniken, um chemische Stoffe einfach und preiswert zu identifizieren. *Ion mobility spectroscopy* werde benutzt, um Geräte, Oberflächen und Menschen zu scannen, um Kontaminationen zu entdecken. *Infrared radiation detection* werde in vielen Detektoren unterschiedlicher Art verwendet, z.B. in der photoakustischen Spektroskopie, der filterbasierten Infrarotspektroskopie u.a. *Surface acoustic wave* Detektoren könnten viele chemische Stoffe gleichzeitig entdecken und messen. Sie seien billig und fänden deshalb

7 Forschungsinstitut für Hochfrequenzphysik und Radartechnik, Wachtenberg.

gerade im zivilen Bereich Verwendung. Daneben sind Carbon nanotube gas ionization Sensoren zu nennen.

3.2. Videoüberwachung

Eine andere Methode zur Verhinderung von Anschlägen im Flughafen besteht im Einsatz von Überwachungskameras, die sowohl eine präventive als auch eine repressive Wirkung haben. Präventiv wirken sie dadurch, dass ihr Einsatzort bekannt ist, so dass sich potenzielle Täter beobachtet fühlen. Ihre abschreckende Wirkung ergibt sich daraus, dass mithilfe der aufgezeichneten Videos die Täterermittlung unterstützt wird (Geisler 2007). Soll die Videoüberwachung effektiv und effizient sein, muss sie zu einem hohen Grad automatisch arbeiten, weil sonst der Personalaufwand für die Auswertung der Informationsflut zu hoch wäre. Gesucht wird deshalb nach einer Software, die verdächtige Szenen aus der Bilderflut herausfiltert (Lehmann 2006). Eine weitgehend automatische Tätererkennung erfordert die Eingabe biometrischer Täterprofile und/oder eines prognostizierten Verhaltens[8]. Hier müssen intelligente Algorithmen entwickelt werden, um auf Verdachtsmomente aufmerksam zu machen, z.B. auf herrenlose Koffer oder auffällige Bewegungsmuster (Pohler 2007). Verfahren videobasierter Biometrie mittels automatischer Gesichtskontrolle existieren bereits, sie gelten aber nach einem Großversuch im Mainzer Hauptbahnhof noch nicht als verwendungsreif (Geisler 2007). Gearbeitet wird auch an einer Koppelung von Detektion, Videoüberwachung und Anbindung ans Internet, um möglichst schnell zu erkennen, um welchen Giftstoff es sich bei einem Anschlag handelt[9].

Schwerpunkte in der Weiterentwicklung der Videoüberwachungstechnik sind:

- die Personenverfolgung über vernetzte Kameras;
- das Erkennen von als abnorm definiertem Verhalten von Personen;
- die Unterstützung von Bildauswerteverfahren durch eine IT-basierte Systemarchitektur und
- die Verknüpfung der Bildauswertung mit Radar- und anderen Sensortechnologien.

Künftig wird das einzelne Videobild abgelöst werden durch eine intelligentere Aufbereitung von Informationen aus verschiedenen Quellen.

---

8 Die Kombination unterschiedlicher Sicherheitstechniken ermöglicht nicht nur die Entwicklung komplexer Identifikations-, Zugangs- und Überwachungssysteme. Mit zunehmender Erfassung personenbezogener oder personenbeziehbarer Daten und den Möglichkeiten der Verknüpfung von Einzeldaten entstehen auch völlig neue Potenziale der Überwachung. Mit der zunehmenden Vermischung von Aufgaben der Gefahrenabwehr der inneren und der äußeren Sicherheit und dem Wunsch einer möglichst umfassenden informationsbasierten Lagebeurteilung könnte die Verknüpfung von Einzelinformationen verbunden sein, die sich zu einem umfassenden individuellen Datenprofil verdichten lassen (Floeting 2006).

9 Firma smiths detection.

3.3. Verifikationstechnik

Um zu verhindern, dass im Strom der Passagiere aus Krisenregionen unerwünschte Personen mitschwimmen, muss die Verifikation der Berechtigung eines Ausweisinhabers schon in der deutschen Auslandsvertretung, beim Einchecken oder bei der Einreise biometrisch sichergestellt werden[10]. Deshalb wird schon bei der Beantragung eines Visums in der deutschen Auslandsvertretung Biometrie eingesetzt. Geplant ist das Visa-Informationssystem VIS: eine zentrale Datenbank zur Unterstützung der gemeinsamen Visa-Politik der EU-Staaten. So eröffnet die Einführung des biometrischen Passes Möglichkeiten, neuen Reisekomfort mit gesteigerten Sicherheitsanforderungen zu verknüpfen, was für die Abwicklungs- und Logistikprozesse im Flugreiseverkehr von Vorteil ist (Bernnat 2004; ;Emery et al. 2006).

Als eine der Schlüsseltechnologien dieses Jahrhunderts gilt *radio frequency identification* (RFID), das „Internet der Dinge". Damit können grenzüberschreitende Lieferungen von Gütern und insbesondere von Containern abgesichert werden. Dies trägt zur Verhinderung des Imports von Kriminalität und Terrorismus bei. Der sogenannte Smart Container lässt sich zugleich über GPS (*Global Positioning System*) oder mittels Zellenortung durch GSM (*Global System for Mobile Communications*) überall hin nachverfolgen. So ist z.B. die Lufthansa Cargo allein schon durch EU-Recht dazu gezwungen, in Zusammenarbeit mit den Speditionen eine hundertprozentige Prüfung aller Frachtgüter zumindest anzustreben. Deshalb wird jedes Paket, das nicht von einem vom Luftfahrtbundesamt zertifizierten Logistiker angeliefert wird oder von einem Versender, der von einem solchen Logistiker oder einer Airline autorisiert wurde, von Mitarbeitern der Lufthansa-Tochter überprüft. Im Jahr 2006 ergab sich dafür ein Mehraufwand von 36.000 Arbeitsstunden. Bei den Gütern, die von Vertragspartnern angeliefert werden, gehe man davon aus, dass diese Sicherheitsprüfung stattgefunden habe[11]. Bei Frachtgütern könnten heute mit „*objectmetric data*" jene Objektmerkmale erfasst werden, welche einen spezifischen Gegenstand eindeutig beschreiben. Wurde einer einmal versendeten Ware eine eigenständige Objektkennung zuerkannt, lasse sich ihr Weg bis zum Zustellort, ihr aktueller Aufenthaltsort, der jeweils aktuelle Warenzustand sowie jegliche merkmalspezifische Manipulation in Echtzeit nachverfolgen.

Derzeit werden Systeme getestet, die in Fahrzeugen und Containern verborgene Personen aufspüren können. Den größten Erfolg verspricht dabei der Einsatz seismischer Sensoren.

---

10 21 europäische Staaten haben bisher biometrische Pässe eingeführt.

11 Expertengespräch.

3.4. Informationstechnik

Moderne Informationstechnik durchdringt in zunehmendem Maße alle Lebensbereiche. Auch in den Kritischen Infrastrukturen wird immer stärker auf den Einsatz von IT gesetzt, um Prozesse effektiver und effizienter betreiben, steuern und überwachen zu können. Daraus ergeben sich zum Teil hochkomplexe IT-basierte Vernetzungen und Abhängigkeiten (Fraunhofer Institut 2007b). Der Schutz der Kritischen Infrastrukturen erfordert daher auch einen angemessenen Schutz der Informationsinfrastrukturen.

Auch Flughäfen können durch digitale Kommunikationsmittel sicherer und effizienter gemacht werden. Da die ersten analogen Systeme das Ende ihrer Lebensdauer erreicht haben, stellen Großflughäfen derzeit weltweit auf digitale Kommunikationssysteme wie z.B. Bündelfunknetze um, die mehr Sicherheit bieten.

Hinsichtlich seiner Komplexität lässt sich ein Großflughafen mit einer Massenveranstaltung wie der Europameisterschaft oder den Olympische Spielen mit Service 'Rund-um-die-Uhr' gleichsetzen. Es gibt weltweit keine Einrichtung mit so vielen Teilnehmern auf einer so geringen geografischen Fläche und mit einer derartigen Anrufdichte. Zusätzlich wird ein typischer Großflughafen innerhalb eines Radius von 30-40 km über Funkerfassungssysteme für sämtliche Flughafenbereiche, einschließlich Tiefgaragen, Gepäck- und Frachtanlagen sowie Flugzeughangars für Instandsetzung und Wartung verfügen.

Mitte der 1980er Jahre war die Abhörsicherheit flughafenseitiger Funksysteme lediglich ein Randthema. Daher waren operative Sicherheitsaspekte bei der generellen Bewertung solcher Systeme nicht entscheidungsrelevant. Nach dem 11. September haben sich die Anforderungen hinsichtlich der Lieferung eines kurzfristig umzusetzenden hohen Sicherheitsstandards für den operativen Flughafenbetrieb sprunghaft erhöht. Obwohl digitale PMR-Lösungen mit hochwertigen Verschlüsselungssystemen ausgelegt werden können, sind bereits die in einem Basis-System angewandten Kodierverfahren für kurzfristige Sicherheitsvorkehrungen auf einem Flughafen als durchaus ausreichend anzusehen.

Typische Nutzergruppen digitaler Funksysteme von Flughäfen sind:

- Tower und Vorfeldkontrolle;
- Bodenabwicklungsdienste;
- Lotsenfahrzeuge (*Follow-Me*);
- *Push-Back*;
- Sicherheitspersonal;
- Feuerwehr- und Rettungsdienste;
- Fluglinien;
- Catering;
- Technische Dienste[12].

[12] www.eads.com

Im Falle einer Katastrophe am Flughafen müssen viele verschiedene Institutionen, nämlich Polizei, Zoll, Verfassungsschutz, Feuerwehr, Rettungsdienste, private und kommunale Katastrophenschutzeinrichtungen und ihre Mitarbeiter schnell und effizient koordiniert werden. Integrierte Leitstellen, um alle Akteure einzubinden, sind deshalb entscheidend für erfolgreiche Gegenmaßnahmen. Dafür bieten sich Lösungen der Informations- und Kommunikationstechnologie an, mit denen das Wissen verschiedener Organisationen zusammengeführt und verdichtet werden kann. So entsteht ein detailliertes und interdisziplinäres Lagebild, das eine zuverlässige Entscheidungs- und Führungsgrundlage für den Krisenfall bildet. Auch bei der Steuerung der Einsatzkräfte und bei der Krisenprävention leisten diese Technologien wertvolle Dienste. Die globale Dimension der heutigen Gefahren ist ein weiteres Argument für Lösungen der Informations- und Kommunikationstechnologien. Ohne sie lassen sich grenzüberschreitende Konzepte, hochkomplexe Aufgaben, Koordination, Synchronität, Vertraulichkeit und Zuverlässigkeit nicht herstellen (Bernnat 2004; ;Emery et al. 2006).

Die größte Herausforderung ist wahrscheinlich nicht die Informationsgewinnung, sondern die Informationsauswertung sowie die Bereitstellung, der Austausch und die Weitergabe von Erkenntnissen in Echtzeit (Hellenthal 2006). Die Informationen müssen in mehreren Schleifen auf ihre Verlässlichkeit überprüft werden, um Fehlalarme auszuschließen[13]. Große Bedeutung kommt der Systemintegration zu, denn netzwerkzentrierte Systemlösungen sind prädestiniert dafür, einen nachhaltigen Sicherheitsmehrwert zu generieren.

Viele dieser Technologien wurden aus militärischen Gründen entwickelt. Da aber in jüngster Zeit die terroristischen Gefahren, die der Zivilgesellschaft drohen, in den Vordergrund getreten sind, müssen diese Technologien angepasst werden, da sich die zivile Nutzung vielfach von der militärischen unterscheidet (Davis 2006).

Experten versichern, es gäbe kaum wirklich neue Technologien. Die Kunst der Flughafensicherungskonzepte sei vielmehr, aus vorhandenen Technologien, wie z.B. Fingerprintsysteme oder Videobewegungsmelder, geeignete Elemente herauszusuchen und miteinander zu verknüpfen. So sei die Installation von Sensorsystemen nur der erste Schritt. Der zweite und wichtigere Schritt sei dann der Zugriff auf die dahinterliegenden Datenbanken. Auch elektronische Spürnasen, Tracken und Scannen seien technologisch nichts Neues. Sie hätten aber früher kaum Abnehmer und folglich hohe Stückpreise gehabt. So habe es Fingerprintsysteme früher nur im Hochsicherheitsbereich der Atomkraftwerke gegeben. Neu sei, dass es jetzt dafür einen weltweiten Markt gibt, der es erlaubt, vorhandene

[13] Expertengespräch

Technologien weiterzuentwickeln und zu verbilligen. So kosten leistungsfähige Videosensoren heute nur noch 8.000 Euro[14]. Ein Metaziel der Entwicklungsingenieure sei es, die Komplexität zu reduzieren und zu beherrschen.

[14] Expertengespräch.

4. Unternehmen

Experten versichern, dass die industriellen Kernkompetenzen in Deutschland weitgehend vorhanden seien, um die zum Schutze der Flughäfen erforderlichen Technologien zu entwickeln und herzustellen. Zunächst sind hier die großen Unternehmen wie Siemens, Bosch und EADS zu nennen, die einen großen Teil des technologischen Spektrums abdecken und vor allem komplexe, in sich geschlossene Systemlösungen anbieten. Hierbei handelt es sich um Gesamtpakete, die Planung, Errichtung und Betreibung umschließen und langfristig auch für den Kunden Vorteile bieten. Beispiele für solche Gesamtlösungen sind die Sicherheitskonzepte für die Flughäfen in Katar und Sevilla und für den im Bau befindlichen Großflughafen Berlin Brandenburg International (BBI), aber auch Atomkraftwerke und Gefängnisse. Die finanzielle Dimension der Sicherheitstechnologien innerhalb solcher Systemlösungen konnte bei Expertengesprächen nicht beziffert werden, weil sie von zu vielen Parametern abhänge.

Den großen Nachfrageschub gebe es jedoch hauptsächlich im privaten Bereich und bei Unternehmen, die durch die aktuellen Ereignisse sensibilisiert worden sind. Hier profitieren vor allem die kleinen und mittleren Unternehmen[15], die einzelne Technologien beherrschen und sich in kleinen Teilmärkten positionieren. Dabei gibt es Hunderte von Anbietern etwa für Videoüberwachung wie beispielsweise die Vitracom AG. Aber auch die traditionellen Hersteller wie Sony und Philipps sind auf diesem Gebiet aktiv.

Eine Zuordnung einzelner Unternehmen und ihrer Produkte zu einem bestimmten Sektor der Kritischen Infrastruktur erwies sich als unmöglich. Das liegt gerade an den vielfältigen Einsatzmöglichkeiten sicherheitstechnologischer Lösungen. Videoüberwachung beispielsweise ist nicht nur auf Flughäfen, sondern darüber hinaus auch zur Überwachung von Seehäfen und Bahnhöfen, aber auch von Gefängnissen, Kernkraftwerken und Staatsgrenzen einsetzbar und kann sowohl von Polizei, Militär, Feuerwehr und Katastrophenschutzeinrichtungen eingesetzt werden.

Allein in Nordrhein-Westfalen konnten rund 60 Unternehmen festgestellt werden, die sich mit sicherheitstechnologischen Lösungen beschäftigen und die auf diesem Gebiet über Kernkompetenzen verfügen. Dazu gehören etwa zehn größere Unternehmen, darunter auch die führenden Rüstungsunternehmen Rheinmetall und Diehl. Die meisten dieser Sicherheitsfirmen sind jedoch relativ kleine und teilweise auch junge Unternehmen mit oft nur 10 bis 40 Beschäftigten. Dennoch entwickeln gerade diese kleinen Spezialisten durchaus interessante Lösungen oder haben sich als Nischenanbieter bewährt. Da diese Firmen jedoch nicht publizitätspflichtig sind, ist die Informationslage schlecht. Im Internet sind nur spärliche Informationen

15 Expertengespräche.

erhältlich, die sich allenfalls auf die Produktpalette beziehen, aber keine näheren Angaben zu Umsatz und Zahl der Beschäftigten enthalten.

Im Folgenden werden drei Unternehmen vorgestellt, die im Hinblick auf Größe und Technologiespektrum als typisch angesehen werden können.

4.1. EADS

Als Beispiel für ein sicherheitstechnologisches Großunternehmen möge die *European Aeronautic Defence and Space Company* (EADS) dienen. Sie definiert die Aufgaben beim Schutz kritischer Infrastrukturen wie folgt:

- Identitätsprüfung und Kontrolle des Personen-, Waren- oder Frachtverkehrs zwischen den einzelnen Standorten;
- Schutz von Standorten und kritischen Infrastrukturen;
- Lieferung von IT-Lösungen und Schutz von Kommunikationsnetzwerken;
- Schutz gegen Bedrohungen durch Terrorismus und organisierte Kriminalität[16].

Die EADS bietet vor allem integrierte Lösungen mit kosteneffizientem Sicherheitsmanagement für unterschiedliche Standorte. Das Portfolio beinhaltet:

- Sicherheitssysteme (Abbildung 1): Schutz kritischer Standorte wie z.B. Industrieanlagen, Flug- und Seehäfen, Energieanlagen, Öl-, Gas-Anlagen / Offshore-Plattformen, Regierungsgebäude und –gelände, Denkmäler und Wahrzeichen;
- Videoüberwachung: CCTV, intelligente Videosysteme, Nummernschilderkennung, Überwachung von Menschenansammlungen, Identifizierung der ID-Nummer von ISO-Containern, Überwachung von Verkehrsknotenpunkten;
- Nicht zerstörende Prüfungen: Personen, Fracht, Kfz und Gepäckstücke, *Screening*, Detektion von Sprengstoffen, Metallen, CBRN, Drogen.
- Sicherheit von Verteilernetzwerken: Schutz von Pipelines, Wasserkraftwerken, Energieanlagen;
- Cybersicherheit: Informationssysteme und Datennetzwerke bilden die zentrale Infrastruktur der Wirtschaft. Die Abwehr von Cyberkriminalität und der Schutz von Systemen und sensiblen Daten zählen zu den kritischsten Themen, mit denen sich Sicherheitsorganisationen befassen müssen. Geheimhaltungspflichtige Daten von Regierungen und privaten Sicherheitsorganisationen müssen gegen illegale Aktivitäten geschützt werden. Die EADS integriert und entwickelt komplexe Sicherheitsprogramme zum Schutz von IT-Systemen und Daten.

16 www.eads.com

Abbildung 1: Sicherheitssysteme der EADS

Quelle: www.eads.com

Durch maßgeschneiderte Subsysteme, die in größere kohärente Systeme integriert werden können, soll ein Maximum an Sicherheit erreicht werden. Größe und Zusammensetzung derartiger Systeme sind abhängig von den zu sichernden Einrichtungen, operativen Kundenprozessen und der erwarteten Bedrohung. Die sich daraus ergebende optimale Kombination aus Technik, Personalressourcen und Organisationssteuerung bietet laut Firmenprospekt ein Höchstmaß an Sicherheit bei gleichzeitiger Kosten- und Risikosenkung. Der EADS-spezifische Ansatz besteht darin, von vorne herein schlüsselfertige und auf den jeweiligen Kunden- und Einrichtungsbedarf maßgeschneiderte Sicherheitssysteme in enger Zusammenarbeit mit dem Kunden zu entwickeln. Diese basieren auf einem breiten Angebot an Konzepten für Beobachtungs- und Überwachungssysteme, um jederzeit und in jeder Situation hochwertige Informationen zu liefern[17].

17 www.eads.com

4.2. Robowatch

Als Beispiel für eine junge Firma diene Robowatch Technologies GmbH. Sie ist einer der führenden Anbieter von autonom gesteuerten Robotersystemen (AUGVs - *Autonomous Unmanned Ground Vehicles*), die den Menschen in gefährlichen Situationen rechtzeitig warnen, die Bewachung risikoreicher Zonen oder großer Areale unterstützen und die Aufklärungsarbeit im Bevölkerungs- und Katastrophenschutz optimieren. Mit den autonom navigierenden Überwachungsrobotern OFRO+detect, ASENDRO und AUG-V8 stehen Robotersysteme für Aufklärung, CBRN-Detektion (Erkennung chemischer, radioaktiver und nuklearer Gefahren), Entschärfung und Transport zur Verfügung. Die Roboter MOSRO und OFRO unterstützen die Überwachung sehr großer Hallen, Außenflächen, schwer einsehbarer Areale oder die Zutrittskontrolle für sensible Unternehmensbereiche.

Diese Systeme bündeln verschiedene Elemente bewährter Sicherheitstechnik (Video- und Thermokamera, Bewegungsmelder etc.) auf einer fahrbaren Plattform. Damit entdecken sie Personen, die unerlaubt ein Gelände, Gebäude oder bestimmte Bereiche betreten. Sie können aber auch mit zusätzlichen Sensoren zur Leckage- und Brandfrüherkennung oder zur Detektion von atomaren und chemischen Gefahrstoffen ausgestattet werden. Erkennen die sensiblen Spürnasen auf ihrer Patrouille etwas Außergewöhnliches, alarmieren sie in Sekundenbruchteilen die Sicherheitszentrale und ermöglichen ein schnelles Eingreifen[18].

Die Firma beschäftigt 45 Mitarbeiter, die überwiegend Entwickler, Ingenieure, Informatiker, Programmierer und Designer sind, so dass die Produktion hauptsächlich durch externe Partnerunternehmen erfolgt. Die Kernkompetenzen der Firma sind:

1. Entwicklung mobiler und autonom navigierender Robotersysteme
   - Modulares Plattformdesign;
   - Energiemanagement;
   - Autonome Navigation;
   - Bewegtzielerkennung von Personen;
   - Kommunikation (GSM, UMTS, WLAN).
2. Integration stationärer und semi-mobiler Sensortechnologie
   - Gase (CBRN, Feuer, Toxine);
   - Identifikationssysteme (RFID, Biometrie, Gesichtserkennung);
   - Sensorik (Explosives und metallisches Material)[19].

[18] www.robowatch.de

[19] www.robowatch.de

4.3. Flug- und Industriesicherheit Service- und Beratungs-GmbH

Ein anderes Beispiel für Firmen in diesem Sektor ist die Flug- und Industriesicherheit Service- und Beratungs-GmbH (FIS GmbH). Sie wurde 1988 gegründet und ist spezialisiert auf Sicherheitsdienstleistungen an deutschen Flughäfen. Die FIS GmbH gehört als Tochterunternehmen der ICTS Europe B.V. (*International Consultants on Targeted Security Europe*) dem Fraport-Konzern an.

An elf Flughäfen in Deutschland beschäftigt die FIS GmbH zurzeit über 2.100 Mitarbeiter. Die FIS GmbH konzentriert sich in der Kernkompetenz mit hohen Sicherheitsstandards auf folgende Geschäftsfelder:

- Passagier- und Gepäckkontrollen;
- Dokumentenkontrollen;
- Terminalservices;
- Objektschutz.

Auftraggeber sind hauptsächlich Behörden, Flughafenbetreiber und Luftverkehrsgesellschaften.

Gleichzeitig entwickelt die FIS neue Produkte, die den Abfertigungsprozess im Luftverkehr noch schneller und zuverlässiger gestalten. Als erfolgreiches Pilotprojekt gilt der „*Flying Pass*“, den die FIS zurzeit am Frankfurter Flughafen für die amerikanische Fluggesellschaft Northwest einsetzt. Dabei wird eine Verbindung zwischen Biometrie und einer SmartCard hergestellt, die den Passagier identifiziert und gleichzeitig das Check-in mit der Personenkontrolle verknüpft. Ein zweites, ebenfalls neues Produkt wurde für die Luftfracht entwickelt. Vor dem Hintergrund einer schnellen und effizienten Methode zur Aufspürung von Explosivstoffen, wurde das Detektionsverfahren RASCargOTM entwickelt. Hierbei übernehmen speziell trainierte Hunde aufgrund ihres hochsensiblen Geruchssinns die Analyse der entsprechenden Luftproben.

Die bisherigen Methoden des *Cargo Screening* haben eine Reihe von Nachteilen. So verursachen die Kontrolle durch Röntgendurchleuchtung, die manuelle Durchsuchung und die Prüfung mittels einer Dekompressionseinrichtung einen hohen Material-, Kosten- und Zeitaufwand und führen zu Verspätungen. Bei der Durchführung nach dem RASCO-Ablauf wird eine Luftprobe aus dem Frachtraum entnommen, versiegelt und dem Prüfhund in einer zentralen Analyseeinheit vorgeführt. Das RASCargOTM-System dagegen bietet signifikante Vorteile:

- Erreichte Aufspürquote: über 95 Prozent;
- Geringe Fehlalarm-Quote: geringer als 1 Prozent;
- Unterschiedliche Sprengstoffe können aufgespürt werden;
- Der Hund kann auf mehrere Substanzen hin trainiert werden;
- Der Prüfhund kann bis zu 8 Stunden eingesetzt werden (mit Pausen);
- Leichte Integration in den Betriebsprozess;
- Keine kostspieligen Investitionen erforderlich;

- Sehr schnelle Ergebnisse.

RASCargOTM ist bereits in Großbritannien (nach DTLR) und in Frankreich zertifiziert und im Einsatz[20].

Wegen der starken Nachfrage hat FIS allein am Frankfurter Flughafen in den vergangenen zwei Jahren mehr als 1.000 neue Arbeitsplätze geschaffen; deutschlandweit liegt die Anzahl der Jobs bei über 5.000. In der EU ist der Dienstleister, der im vergangenen Jahr 137 Millionen Euro umgesetzt und dabei einen Gewinn vor Steuern, Zinsen und Abschreibungen von 20 Millionen Euro erzielt hat, an 66 Flughäfen[21] tätig.

Der Sicherheitsdienstleister FIS plant nun, auf dem großen nordamerikanischen Markt aktiv zu werden. Dort wird trotz gewaltiger Investitionen immer noch großer Nachholbedarf gesehen. So sagt der frühere Inspector General des *US Department of Homeland Security*, Clark Kent Ervin, noch immer könnten Personen ungehindert Sprengstoff, Bomben und Waffen an Bord von Flugzeugen schaffen – mehrere Tests bewiesen dies –, außerdem würden nur sechs Prozent der 26.000 Cargo-Container, die täglich in den Vereinigten Staaten vom nahen und fernen Ausland ankommen, wirklich inspiziert. Die öffentliche Sicherheit in den Vereinigten Staaten habe sich kaum verbessert[22].

4.4. Standortförderung durch Clusterbildung

Für den deutschen Standort im Allgemeinen gilt, dass der Nachteil in Form hoher Kosten ausgeglichen werden muss durch Innovationen und Produktivitätssteigerungen. Nur dadurch kann der relative Vorsprung gegenüber ausländischen Konkurrenten gehalten und möglichst ausgebaut werden. Deshalb stellt sich die Frage, wie die technologischen Kompetenzen insbesondere der kleinen, innovativen Firmen gefördert und ihre Innovationen möglichst schnell vermarktet werden können. Ein bewährtes Mittel zu diesem Zweck ist die Bildung von Clustern[23], indem Unternehmen auf ein Netz an spezialisierten Zulieferern in ihrem unmittelbaren Umfeld zugreifen können und ein Pool an hochqualifizierten Mitarbeitern zur Verfügung steht. Unternehmensübergreifende Cluster können helfen, klare Technologieschwerpunkte zu erarbeiten und die vorhandenen Kompetenzen und Fähigkeiten zu bündeln und auf gemeinsame Projekte auszurichten.

Cluster bieten auch Informations- und Kostenvorteile, denn Synergien entstehen nur bei intensiver Kooperation. Durch eine wertschöpfungs-

---

20 www.fisgmbh.de

21 Frankfurter Allgemeine Zeitung, 27.4.2006.

22 www.fisgmbh.de

23 Unter dem aus der Regionalforschung entlehnten Begriff „Cluster“ versteht man ein organisiertes, kreatives Netzwerk aus Wirtschaft und Wissenschaft. Man könnte aber auch von einem „nationalen Innovationssystem“ sprechen.

orientierte, auch interdisziplinäre, Zusammenarbeit der Unternehmen sowie durch Forschungs- und Entwicklungskooperationen entstehen Innovationen, Produktivitätssteigerungen und schließlich wirtschaftliche Erfolge. Dabei muss das wissenschaftliche Potenzial der Hochschulen und außeruniversitären Forschungseinrichtungen für die Wirtschaft besser erschlossen und die Vernetzung innerhalb der Unternehmen dieser Branche verbessert werden. Dadurch könnten Forschungsergebnisse noch schneller als in der Vergangenheit in marktfähige Produkte überführt werden. Ein wechselseitiger Austausch hilft auch der Wissenschaft, die Bedürfnisse der Unternehmen besser zu verstehen und das eigene Forschungsprofil entsprechend zu schärfen. Mit der Einbindung von Unternehmen in Netzwerke werden auch die Bindungskräfte an einen Standort entscheidend erhöht (Bayerisches Staatsministerium für Wirtschaft 2006).

Der Nutzen von Clustern zeigt sich darin, dass sie

- Konkurrenz und Kooperation gleichzeitig erlauben;
- die Größe der Partner erweitern durch gegenseitige Ergänzung;
- die Produktivität steigern und
- Innovationen fördern und die Gründung neuer Unternehmen stimulieren.

Cluster bewirken somit globale Überlegenheit durch lokale Synergien insbesondere bei Produktivität und Innovation. Cluster beugen damit auch der Gefahr vor, dass Arbeitsplätze ins Ausland verlagert werden (müssen).

Neben der unabdingbaren Beteiligung der Großen, die internationalen Marktzugang und eigene Technologiepotenziale haben, muss die Clusterpolitik auch die kleinen Unternehmen und Zulieferer einbeziehen. Die Netzwerkbildung erleichtert gerade den kleinen Betrieben in der Fläche den Zugang zu den für sie relevanten und interessanten Forschungseinrichtungen und Partnerunternehmen und hilft, Standortnachteile auszugleichen. Viele KMU sind international erfolgreiche Anbieter, oft sogar Weltmarktführer. Sie stoßen jedoch oft auf finanzielle Grenzen und personelle Engpässe. Das gilt gerade bei der notwendigen Vernetzung verschiedener Bereiche. Insbesondere brauchen sie verbesserte Zugangsmöglichkeiten zu Forschungseinrichtungen (Küchle 2007).

Die Vernetzung der Potenziale zu organisieren, ist Aufgabe der Clusterplattformen. Sie sind Dienstleister für die Unternehmen der jeweiligen Branche oder des Kompetenzbereichs. Im Vordergrund ihrer Tätigkeit stehen Aufbau und Pflege eines Kontaktnetzes zwischen Unternehmen, Hochschulen, Forschungseinrichtungen, Kammern und Verbänden, Kapitalgebern, Förderinstitutionen, Beratern und anderen Akteuren des jeweiligen Clusters. Das Kontaktnetzwerk soll den Zugang zu leistungsfähigen Lieferanten und Leit-Kunden, zum technischen Know-How von Hochschulen und Forschungseinrichtungen, zu hochqualifizierten Mitarbeitern und zu Kapitalgebern erleichtern. Von diesen Plattformen profitieren insbesondere mittelständische Unternehmen, denen eine abgestimmte Zusammenarbeit mit anderen Unternehmen einen höheren Grad an Spezialisierung ermöglicht und die

so ihre Wettbewerbsposition gegenüber Großunternehmen verbessern (Bayerisches Staatsministerium für Wirtschaft 2006).

4.5. Existierende Netzwerke

Inzwischen gibt es nicht nur eine wachsende Zahl von Unternehmen, die sich auf sicherheitstechnologische Lösungen spezialisieren, sondern auch bereits einige Netzwerke, die man als Vorstufe für sicherheitstechnologische Cluster betrachten kann. Dazu zählen beispielsweise:

Das auf europäischer Ebene aktive **Forschungsnetzwerk *Global Monitoring for Security and Stability* (GMOSS)**, das Synergien zwischen seinen Partnerfirmen und die Kooperation mit anderen sicherheitsorientierten Initiativen fördern möchte. Die Aktivitäten umfassen vor allem:

- Wissenschaftliche Integration;
- Wissenschaftliche Workshops zu m Thema zivile Sicherheit;
- Entwicklung von Datenstandards;
- Austausch von Mitarbeitern und
- Informationsweitergabe.

Die **Gesellschaft der sicherheits- und wehrtechnischen Wirtschaft in Nordrhein-Westfalen e.V.** (GSW) mit über 70 Mitgliedsfirmen (siehe Anhang).

Das **Netzwerk Systeme für integriertes Sicherheitsmonitoring (NESIS)** ist ein seit 2004 bestehender Zusammenschluss erfahrener innovativer, vorwiegend mittelständischer Unternehmen, dessen Ziel es ist, in enger Kooperation der Partner mit deren Produkten und Technologien sowie durch gemeinsame Forschung und Entwicklung schnell und flexibel komplexe Lösungen des Sicherheitsmonitoring sowie des Sicherheitsmanagements nach den spezifischen Erfordernissen der Kunden bereitstellen zu können[24]. Die wichtigsten Netzwerkpartner sind:

- AirRobot: Mini UAV Systeme;
- IABG: Analysen, Konzepte und Strategien;
- Lohse und Schilling: Informationsmanagement und Leitsysteme;
- Robowatch: Robotik;
- Bundesamt für Materialforschung: Forschung, Prüfung und Zertifizierung für Sicherheit in Technik und Chemie;
- Greenway Systeme GmbH: Sicherheit durch verkehrstelematische Systemlösungen;
- Institut für Umwelttechnologien: Detektion chemischer Kampfstoffe, toxischer Gase, Sprengstoffe und Drogen;
- Deutsches Zentrum für Luft- und Raumfahrt: Optische Informationssysteme, Echtzeit-Monitoring;
- Deutsche Risikoberatung GmbH: Risikoanalysen und Sicherheitsmanagement;

[24] www.ne-sis.org

- FM-One Management Services GmbH: Organisation von Gebäude-, Prozess- und Unternehmenssicherheit;
- Optotransmitter-Umweltschutz-Technologie (OUT) e.V.: F&E-Projektmanagement.

Die **German European Security Association e.V. (GESA)** ist ein überparteilicher, von Abgeordneten des Europäischen Parlaments und des Deutschen Bundestages gegründeter Verein. Sein Ziel ist das Bestreben nach mehr Sicherheit in Deutschland und Europa zum Schutz der demokratischen Gesellschafts- und Wertestruktur durch die Förderung des Dialogs auf nationaler und internationaler Ebene zwischen:

- staatlichen und gesellschaftlichen Institutionen;
- der Forschung und Wissenschaft und
- der Industrie.

GESA setzt sich vor dem Hintergrund der hohen sicherheits- und industriepolitischen Bedeutung des entstehenden zivilen Sicherheitsmarktes in Europa dafür ein, Bundesländer übergreifend gemeinsame Interessenlagen, Innovationsstrategien und Projektkooperationen zu identifizieren. Ziel ist es, den Bedarfsträgern kosten- und leistungsoptimierte Produkte anzubieten sowie den Anbietern eine international wettbewerbsfähige Marktposition zu schaffen.

GESA widmet sich u.a. der Flughafensicherheit nach folgenden Leitideen:

- Mehr Sicherheit durch gesellschaftliches Bewusstsein und Akzeptanz;
- Mehr Sicherheit durch Prävention und Kooperation;
- Mehr Sicherheit durch Innovation;
- Mehr Sicherheit durch Finanzierbarkeit (z.B. durch größere Märkte);
- Mehr Sicherheit durch Trendprognosen (gesellschaftlich und technisch);
- mehr Folgeanwendungen im privatwirtschaftlichen Bereich;
- mehr Exportmöglichkeiten[25].

Neben diesen Netzwerken sind hier auch die **Fachverbände** zu nennen, die ihre Mitgliedsfirmen u.a. bezüglich Ausbildung und Qualitätssteigerung beraten:

Der **Fachverband Sicherheitssysteme des ZVEI – Zentralverband Elektrotechnik- und Elektronikindustrie e.V.** in Frankfurt a.M.[26] vertritt seit Januar 2007 auch die Interessen von Fachplanern und Errichtern von Sicherheitssystemen. Insgesamt werden über 1.400 Mitgliedsunternehmen der Elektrotechnik- und Elektronikindustrie mit über 800.000 Beschäftigten und einem Umsatz von knapp 180 Milliarden Euro im Jahre 2006 vertreten (Roeder 2007).

25 www.gesa-network.de

26 www.zvei.org

Der **Bundesverband der Hersteller- und Errichterfirmen von Sicherheitssystemen e.V. (BHE)** ist der übergreifende Fachverband für Unternehmen, die Produkte und Anlagen der vorbeugenden Sicherungstechnik herstellen, planen und/oder installieren. Hier findet sich das gesamte Spektrum der Sicherungstechnik. Der BHE hat über 500 Mitgliedsfirmen, davon sind 80 Prozent Errichter, 18 Prozent Hersteller und 2 Prozent Planer[27].

Die **Arbeitsgemeinschaft Zivile Sicherheit** vertritt die Interessen der führenden deutschen Unternehmen der Sicherheitsindustrie und versteht sich als aktiver Entwicklungs- und Diskussionspartner der Politik und der öffentlichen Hand auf nationaler und internationaler Ebene. Darüber hinaus fördert die Arbeitsgemeinschaft die gemeinsame Forschung und Entwicklung in der Sicherheitstechnologie und die enge Kooperation bei Projekten im In- und Ausland. Der Arbeitsgemeinschaft gehören neben den großen Firmen Bosch und Diehl u.a. die Unternehmen Flug- und Industriesicherheit Service- und Beratungs-GmbH, Hübner, KB Impuls, Smiths und Rohde & Schwarz an.

Die von der EU mit über zwei Milliarden Euro bis 2013 geförderte Entwicklung neuer Sicherheitstechnologien, die auch den Schutz Kritischer Infrastrukturen umfasst, unterstützt ebenfalls die Clusterbildung, da die Einbindung relevanter Partner aus mindestens zwei weiteren EU-Ländern gewünscht wird. Das legt auch die Bildung von Konsortien aus Industrie und Endnutzern auf der Projektebene nahe (Mengel 2007). So hat sich im September 2007 in Brüssel ein Forum zur Koordination der Zusammenarbeit zwischen Sicherheitsbehörden und Industrie gegründet (Peilert 2007).

27 www.bhe.de

5. Arbeitsplatzpotenzial

Sicherheit ist ein weltweit wachsender Markt. In Deutschland wenden Bund, Länder und Kommunen etwa 30 Milliarden Euro jährlich für Innere Sicherheit auf. Der deutsche Markt für sicherheitstechnische Produkte und Dienstleistungen hatte bereits im Jahre 2005 ein Umsatzvolumen von 10 Milliarden Euro, von denen 3,6 Milliarden Euro auf die IT-Sicherheit entfielen – bei hohen Wachstumsraten. Der Markt für Zutrittskontrollen und Videoüberwachungsanlagen ist seit dem 11. September um jeweils ein Drittel gewachsen. Eine Untersuchung des TÜV Nord kommt zu dem Ergebnis, dass allein zu einer vollständigen Abdeckung der Logistikkette Luftfracht in Deutschland 24.000 Unternehmen zu zertifizieren seien[28].

Der ZVEI-Fachverband Sicherheitssysteme hat zusammen mit dem Bundesverband der Hersteller und Errichterfirmen von Sicherheitssystemen (BHE) durch eine Befragung der Mitglieder ermittelt, dass der Gesamtmarkt für elektronische Sicherheitstechnik 2006 gegenüber dem Vorjahr um 7,9 Prozent wuchs. Ein Umsatzanstieg war in allen Teilbereichen – Video, Zutrittskontrolle, Brandmeldetechnik sowie Einbruch- und Überfallmeldetechnik – zu verzeichnen (Abbildungen 2 und 3). Auch 2007 zeichnet sich eine positive Entwicklung von etwa drei Prozent ab (Staimer 2007).

Der europaweite Markt für Sicherheitsdienstleistungen an Flughäfen wird für das Jahr 2006 auf 2,7 Milliarden Euro geschätzt, mit Steigerungsraten von ca. sechs Prozent p.a. für die nächsten Jahre. Der weltweite Markt für Sicherheitstechnik i.H.v. 55 Milliarden US-Dollar wächst gar um acht bis zehn Prozent jährlich (Schulte 2007).

Der Markt für Sicherheitstechnologien wächst aber nicht nur in den Industrieländern mit ihren hockkomplexen Infrastrukturen, auch in den Entwicklungsländern steigt die Nachfrage, so dass sich daraus ein beachtliches Arbeitsplatzpotenzial ergibt. Firmen, die auf diesen heute geforderten Technologiefeldern führend sind, können den europäischen Markt, vielleicht sogar den Weltmarkt bedienen und damit Arbeitsplätze, Einkommen und Steuern generieren. Die Entwicklung neuer Sicherheitstechnologien könnte darüber hinaus von enormer Bedeutung für den Technologiestandort Deutschland, seine internationale Wettbewerbsfähigkeit und seine Arbeitsplätze werden. Deutschland mit seinen starken Basistechnologien und einer vielfältigen Forschungslandschaft bringt gute Voraussetzungen mit, um im internationalen Wettbewerb auf diesem Zukunftsmarkt zu bestehen und sollte diese Chancen zielstrebig nutzen.

28 Flugplatzgesellschaft Schönhagen mbH.

Abbildung 2

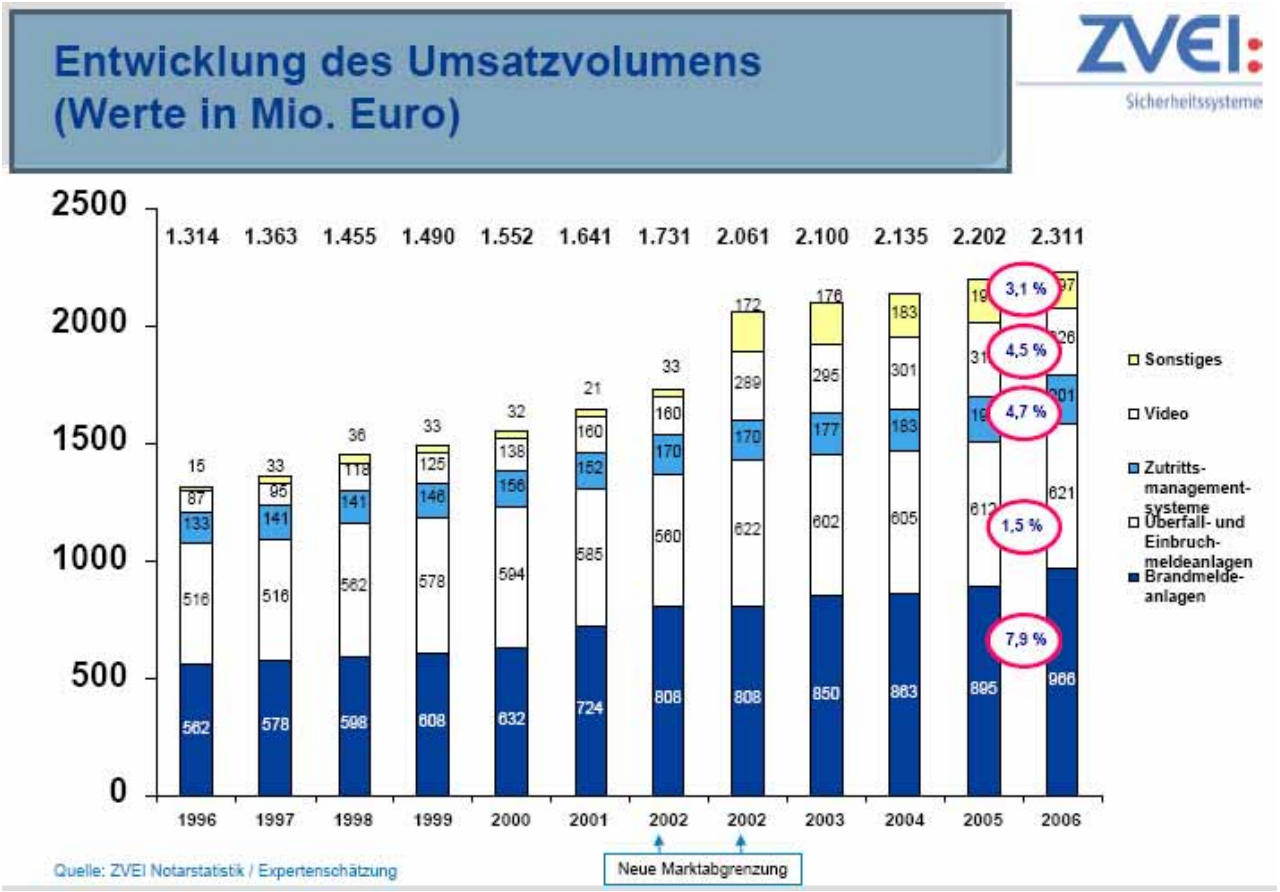
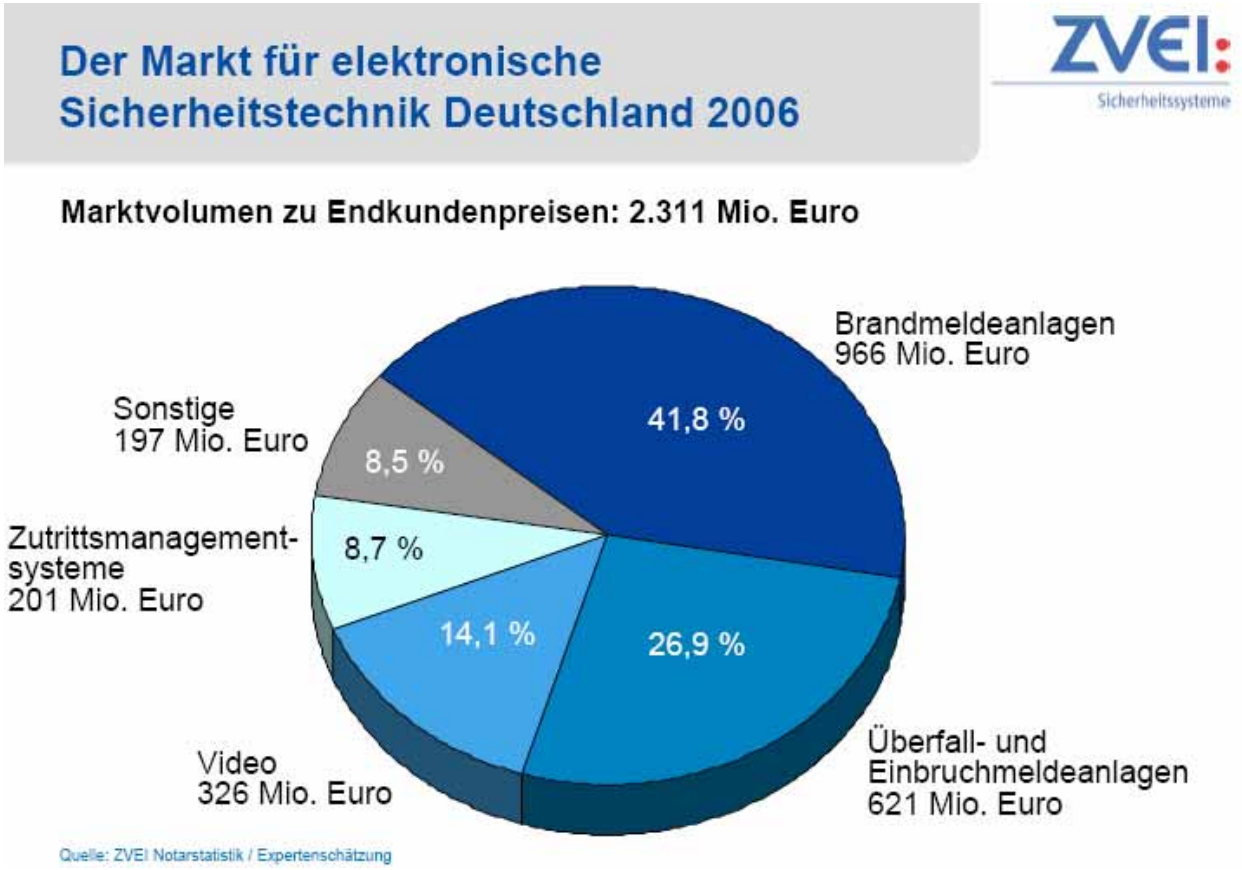

Entwicklung des Umsatzvolumens
(Werte in Mio. Euro)
ZVEI: Sicherheitssysteme
2500
2000
1500
1000
500
0
1.314
1.363
1.455
1.490
1.552
1.641
1.731
2.061
2.100
2.135
2.202
2.311
3,1 %
4,5 %
4,7 %
1,5 %
7,9 %
Sonstiges
Video
Zutritts-management-systeme
Überfall- und Einbruch-meldeanlagen
Brandmelde-anlagen
1996
1997
1998
1999
2000
2001
2002
2002
2003
2004
2005
2006
Quelle: ZVEI Notarstatistik / Expertenschätzung
Neue Marktabgrenzung

Abbildung 3


Der Markt für elektronische Sicherheitstechnik Deutschland 2006
ZVEI: Sicherheitssysteme
Marktvolumen zu Endkundenpreisen: 2.311 Mio. Euro
Brandmeldeanlagen
966 Mio. Euro
41,8 %
Sonstige
197 Mio. Euro
8,5 %
Zutrittsmanagement-
systeme
201 Mio. Euro
8,7 %
14,1 %
26,9 %
Video
326 Mio. Euro
Überfall- und
Einbruchmeldeanlagen
621 Mio. Euro
Quelle: ZVEI Notarstatistik / Expertenschätzung

Experten weisen darauf hin, dass Produkte und Systeme nur „die halbe Wahrheit“ seien. Die Qualität von Sicherheitssystemen werde nämlich zu einem hohen Prozentsatz von den zugehörigen Dienstleistungen bestimmt (Staimer 2007). Deshalb sei es gerade für die Beschäftigungsperspektiven wichtig, dass die Sicherheitsfirmen nicht nur das Gerät allein verkaufen, sondern auch ein umfassendes Sicherheitskonzept und die entsprechende Organisation anbieten. Mit dieser Paketlösung, die von den großen Firmen bereits praktiziert wird, sei es aussichtsreicher, den gesamten europäischen Markt zu bedienen und die Beschäftigung in den deutschen Firmen zu sichern[29].

Auch der Datenschutz, der aufgrund der strengen Vorschriften in Deutschland zunächst als Wettbewerbsnachteil deutscher Unternehmen erscheint, könne zum eigenen Vorteil genutzt werden. Die deutsche Softwareindustrie, die sich gerade aufgrund der strengeren Vorschriften hier einen Vorsprung in Europa erarbeitet habe, sollte dieses zukunftsträchtige Produktmerkmal als strategischen Vorteil nutzen und offensiv vermarkten[30].

In Deutschland arbeiten bereits rund 145.000 Menschen bei privaten Sicherheitsdienstleistern, allein seit Anfang der 1990er Jahre ist deren Zahl um etwa 50 Prozent gestiegen (Floeting 2006). Von den 68.000 Beschäftigten am Frankfurter Flughafen sind derzeit etwa 8.000 Personen im Bereich Sicherheit beschäftigt[31].

Genaue Angaben zur Beschäftigungsentwicklung in den sicherheitstechnologischen Industriefirmen konnten nicht ermittelt werden, u.a. weil die meist kleinen und mittleren Firmen nicht publizitätspflichtig sind. Aber auch bei den großen Konzernen, die komplexe Systemlösungen für Großprojekte erarbeiten, sind genaue Angaben zur Beschäftigung schwierig. Das liegt hier vor allem daran, dass die Gesamtpakete mit einem riesigen Finanzvolumen äußerst umfassend sind. Diese Pakete enthalten z.B. auch Erd- und Betonarbeiten und andere Arbeiten, die von Subfirmen ausgeführt werden[32]. Eine Abgrenzung dieser Arbeiten von der Sicherheitstechnik im engeren Sinne ist schwierig und konnte in der kurzen Bearbeitungszeit nicht geleistet werden. Alle befragten Unternehmen berichten jedoch übereinstimmend von einem zunehmenden Bedarf an Fachkräften auf allen Ebenen (Goericke 2007). Auch die Fachverbände sind nicht in der Lage, Angaben zur Beschäftigung ihrer Mitgliedsfirmen zu machen, bestätigen jedoch ebenfalls einen wachsenden Trend. Es gebe viele Firmenneugründungen, besonders im Softwarebereich, von denen jedoch

---

29 Expertengespräche.

30 Expertengespräche. Für die Sicherheitsindustrien vieler europäischer Länder gebe es bislang noch keinen Anreiz, bei Software den Datenschutz einzubauen (Behörden Spiegel, 2007).

31 www.fisgmbh.de

32 Expertengespräche.

viele nach kurzer Zeit wieder verschwinden. Diejenigen, die sich am Markt durchsetzen, würden oft von großen Unternehmen aufgekauft, sodass es immer wieder zu einer Konsolidierung des Sektors komme[33]. Insgesamt ist davon auszugehen, dass das wachsende Sicherheitsbedürfnis auch zu neuen hochqualifizierten Arbeitsplätzen in diesen Firmen führt.

Dies bestätigt auch der überall laut werdende Ruf nach einer systematischeren Fachkräftequalifizierung. Die Schulung des eingesetzten Personals ist auch bei den Flughäfen ein großes Thema. Da sie jedoch aufgrund der hohen Personalzahl über eigene Ausbilder verfügen, hat der Lieferant von Sicherheitstechnologien die Aufgabe des „train the trainers". Gefordert ist dabei u.a.:

- Eine bereichsübergreifende Ausbildung zur Sicherung eines hohen und standardisierten Basiswissens im Bereich Security-Management und
- eine Spezialisierung in Teilbereichen des Security-Managements und Verknüpfung von Management und IT-Security (Goericke 2007).

33 Expertengespräch.

6. Fazit

Zusammenfassend lässt sich feststellen:

- Flughafensicherheit besteht im Wesentlichen aus den Aspekten Passagier- und Gepäcksicherheit, Frachtsicherheit, Infrastruktursicherheit und Systemintegration. Diese sicherheitsrelevanten Problem- bzw. Aufgabenbereiche sind an sich nicht neu. Es gab sie auch schon früher, sie haben aber seit den jüngsten Anschlägen höchste Priorität erhalten. Vor dem 11. September 2001 lag beispielsweise der Fokus auf der Gepäckkontrolle der Passagiere, jetzt liegt er auf der Gepäck- und Personenkontrolle gleichermaßen.
- Auch die möglichen Maßnahmen sind nicht neu, aber es werden jetzt neue Maßstäbe gesetzt. Es gab beispielsweise eine Kontroverse, ob der Einsatz von Technologien oder menschlichen Kontrolleuren besser sei. Beide haben ihre Vor- und Nachteile. Israelische Erfahrungen zeigen, dass das menschliche Auge in Kombination mit Technologien die beste Sicherheitsplattform bietet (Avihai 2007). Die Frage ist daher, wie man diese beiden Ansätze miteinander verbinden kann und nicht die, welcher der beiden der Vorzug gebührt.
- Die zur Verfügung stehenden Technologien sind ebenfalls nicht neu. Da aber vorbeugende Maßnahmen mit hohen Investitionen verbunden sind, werden sie verständlicherweise erst getätigt, seit sich bestimmte Gefahren konkret abzeichnen. Die Folge ist, dass es jetzt für diese Technologien einen weltweiten Markt mit breitem Einsatzspektrum gibt, sodass sie sich verbilligen und den massenweisen Einsatz ermöglichen. IT-Schlüsseltechnologien sind die Biometrie, die automatisierte und digitalisierte Überwachung von Räumen und die Auswertung von Informationen. Zur Sprengstoffdetektion werden eingesetzt: Röntgenstrahlen, Bestrahlung mit Neutronen, Ionenmobilitätsspektrometrie zum Nachweis von Spuren sowie Massenspektrometrie. Zukünftig wird wahrscheinlich die elektromagnetische Strahlung im Tetraherzbereich an Bedeutung gewinnen. *Radio frequency identification* wird eine der Schlüsseltechnologien dieses Jahrhunderts werden. Neue sicherheitstechnologische Lösungen werden vielfach eine Kombination verschiedener, bereits vorhandener Technologien sein.
- Die genannten Sicherheitstechnologien haben den ökonomischen Vorteil einer sowohl zivilen als auch militärischen Verwendung. Dies verbreitert ihr Einsatzspektrum, erhöht die Stückzahl und ermöglicht deutliche Preissenkungen. Beispielsweise kann die militärische Detektionstechnologie zur Feststellung toxischer Gase und zum Aufspüren radioaktiver, biologischer und chemischer Waffen auch

im zivilen Bereich angewendet werden. Weitere Möglichkeiten für Dual-Use-Arwendungen militärischer Einsatzmittel finden sich in den Bereichen Sensorik und Bildverarbeitung einschließlich Mustererkennung sowie in der Informations- und Datenverarbeitungstechnik einschließlich Datenfusion und *Datamining*[34]. In der Regel ist eine Umrüstung auf den zivilen bzw. militärischen Anwendungsbereich kostensparender als eine Neuentwicklung.

Aufgrund ihres Dual-Use Charakters sind die meisten Sicherheitssysteme gleichermaßen verwendbar für Polizei, Zoll und Grenzschutz, die im Sicherheitskonzept eines Flughafens zusammenarbeiten müssen. Eine strikte Trennung militärischer und ziviler Sicherheitsforschung ist daher weder möglich noch sinnvoll. Eher sollte die Entwicklung von Dual-Use-Technologien gezielt vorangetrieben werden, um *economies of scale* zu erreichen. Eine systematische Nutzung der *spin-on* bzw. *spin-off*-Effekte ergäbe zweifellos erhebliche Einsparpotenziale. Dadurch würde auch die Förderung innovativer Lösungen effizienter, die für den Technologiestandort Deutschland von größter Bedeutung sind. Dies sollte ergänzt werden durch eine aktive Industriepolitik, die alle wichtigen Akteure vernetzt. Wichtige Ansätze zur Clusterbildung sind in Form von Netzwerken bereits gegeben und sollten weiter ausgebaut werden.

- Deutschland zeichnet sich durch starke Basistechnologien und eine vielfältige Forschungslandschaft aus und verfügt über zentrale Kompetenzen im Bereich der zivilen und militärischen Sicherheitstechnik. Damit sind große Chancen auf diese Zukunftsmärkte gegeben, die systematisch genutzt werden sollten. Darüber hinaus gibt es eine Reihe großer und eine Vielzahl kleiner und mittlerer Unternehmen in Entwicklung und Produktion von Sicherheitstechnologien. In allen Bereichen konnte eine steigende Beschäftigung festgestellt werden.
- Befürchtungen hinsichtlich allgegenwärtiger technischer Überwachung und Skepsis gegenüber Sicherheitsversprechen sind gerade in Deutschland weit verbreitet. Viele sehen im Staat eine potenzielle Bedrohung ihrer individuellen Freiheit und möchten deshalb an der Selbstbeschränkung des Staates unbeirrt festhalten, wie sie vor dem 11. September und vor den mörderischen Aktivitäten der Roten Armee Fraktion möglich war. Wenn jedoch wie bei der geplanten Online-Durchsuchung die informationelle Intimsphäre des einzelnen

[34] Allerdings gibt es einen Unterschied zwischen rein zivilen Sicherheitsunternehmen und den wehrtechnischen Unternehmen. Die Wehrtechnik orientiert sich an grundsätzlich anderen Bedrohungsszenarien: großflächige, auf lange Dauer angelegte Angriffe von hoher Intensität, durchgeführt von Verbänden mit einem komplexen Waffenarsenal. Auch das Ziel der Abwehr solcher Angriffe ist anders als beim Kampf gegen Kriminalität und Terrorismus. Das technische Verteidigungsinstrumentarium ist daher noch komplexer, zumeist auch kostspieliger. Die Rüstungsindustrie hat mehr finanziellen Spielraum und dadurch Vorteile im Wettbewerb mit Unternehmen der zivilen sicherheitstechnischen Industrie (Foerster 2007).

den Lebensinteressen anderer bzw. der ganzen Gesellschaft übergeordnet wird, kann das im Falle islamistischer Terroristen dramatische Folgen haben. Deshalb muss geprüft werden, ob die oft diffusen Ängste der veränderten Bedrohungs- und Gefahrensituation wirklich gerecht werden. Freiheit ist ohne Sicherheit nicht realisierbar. Nur in einer von Sicherheit geprägten Umwelt kann Fortschritt stattfinden und Wohlstand gemehrt werden (Hellenthal 2006). Immerhin reichen 44 Prozent der Deutschen die Sicherheitsvorkehrungen gegen Terroranschläge nicht aus (Allensbach-Erhebung). Diese in Deutschland breit und seit vielen Jahren kontrovers geführte Diskussion ist nun durch ein Urteil des Bundesverfassungsgerichts abgeschlossen worden, das die Online-Durchsuchung grundsätzlich erlaubt, aber an strenge Bedingungen knüpft.

Gesprächspartner

- Drescher, Christian R. Sales Manager, Tonbeller Software Consulting, Wien.
- Duschka, Michael. Redakteur „Home and Security“.
- Fischer, Hans-Martin. Geschäftsführer und stellvertretender Vorsitzender ZVEI –Zentralverband Elektrotechnik- und Elektronikindustrie e.V., Fachverband Sicherheitssysteme, Frankfurt a.M.
- Fuhrmann, Astrid. Landespräventionsrat, Polizeipräsidium Düsseldorf.
- Garbers, Jan. Referatsleiter Grundsatzangelegenheiten, Technisches Hilfswerk, Bonn.
- Hellenthal, Dr. Markus. Senior Vice President Global Security, Mitglied des Vorstands EADS Defence and Communications Systems, Unterschleißheim.
- Lüders, Tom. Program Manager Global Security, EADS Defence and Security Systems, Unterschleißheim.
- Pieck, Stefan. Head of Security Services Defence and Communications Systems, EADS Deutschland GmbH, Bonn/Berlin.
- Rehak, Dr. Wolfgang. Projektmanagement Optotransmitter-Umweltschutz-Technologie (OUT) e.V. Berlin.
- Sperber, F.-M. Leiter Sicherheit, Flughafen Düsseldorf GmbH.
- Wasserer, Manfred. Referat Terrorismus, Bundesministerium für Inneres, Wien.
- Wörner, Rainer. EADS Unterschleißheim.

Anhang

1. Hersteller- und Errichterfirmen von Sicherheitssystemen[35]:

- ADT-Sensormatic, Essen
- Axis Communications GmbH, Hallbergmoos
- Dallmeier Electronic GmbH, Regensburg
- Geutebrück GmbH, Windhagen
- HeiTel Digital Video GmbH, Kiel
- Honeywell Security Deutschland, Düsseldorf
- IDS Imaging Development Systems GmbH, Obersulm
- JVC Professional Products GmbH, Friedberg
- MHM Electronic GmbH, Lindhorst
- Mitsubishi Electric Europe GmbH, Ratingen
- Panasonic Deutschland GmbH, Hamburg
- Sanyo Video Vertriebs GmbH + Co., Ahrensburg
- Senstar GmbH, Markdorf
- Werner Industrielle Elektronik, Kreischa

35 www.bhe.de

2. Ausgewählte Unternehmen der GSW

Name des Unternehmens	Jahres-umsatz Mio. €	Beschäftigte	Sicherheitstechnologien /Anwendungsbereiche	Produkte
activ-net GmbH & Co. KG	k.A.	k.A.	IT; Consulting	Core-Switches, Industrial Networking, Installationsswitches, ISDN Konverter, Sensortechnik, Medienconverter, Managementsoftware
AIRMATIC Gesellschaft für Umwelt und Technik mbH	k.A.	k.A.	Ausrüstungen für Katastrophen-schutz; Mechanik; Disaster Control; F&E	Reinigungssysteme; Feuerwehrtechnik; Behäl-tertechnik; Industrieautomation
Aquasun Schutzfolien GmbH	k.A.	k.A.	Mechanik; Disaster Control; Öf-fentliche Sicherheit	Hitzeschutz; Blendschutz; Sichtschutz; Splitter-schutz; UV-Schutz
Atos Origin	592 (Konzern: 5,4 Mrd.)	Meppen: 3.900; Paris: 50.000	IT;	Consulting

Name des Unternehmens	Jahres-umsatz Mio. €	Beschäftigte	Sicherheitstechnologien /Anwendungsbereiche	Produkte
Bollrath GmbH	k.A.	k.A.	Proforce - blast resistant window and facade systems	blast resistant and bullet proof window, door and facade systems; blast and bullet resistant steel, aluminium constructions, curtain and aluminium walls; burglar proof window, door and facade systems break in/out proof; fire resistant constructions; safety rooms; security equipment; PC security controlling systems
Brüggemann GmbH	k.A.		Rettungssysteme	troop parachutes; tactical systems; aerial delivery; air cargo restraint; rescue + emergency; helicopter transport; development
Baumaschinenvertrieb Amling GmbH	k.A.	k.A.	Logistik; Mechanik; Consulting	militärische Kettenfahrzeuge im Bereich Laufwerk, Bremssystem, Getriebe u. Hydraulik für alle Fahrzeuge der Bundeswehr
CAE Elektronik GmbH	k.A.	k.A.	Öffentliche Sicherheit; Logistik; Luft- und Raumfahrtsysteme; IT	Entwicklung, Herstellung u. Betreuung von Simulationssystemen sowie Unified Communications Systemen. Flugsimulationstechnik, Simulatorausbildung
CONET Solutions GmbH	23	200	Consulting, Software-Entwicklung, Informations- u. Kommunikations-technologie	Consulting; IP-basierte Unified Communication Centers (UCC).

Name des Unternehmens	Jahres-umsatz Mio. €	Beschäftigte	Sicherheitstechnologien /Anwendungsbereiche	Produkte
cv cryptovision gmbh	k.A.	k.A.	Öffentliche Sicherheit; IT	security concepts for smartcards and other security tokens; performant implementation of advanced encryption technologies into up-to-date software products & network infrastructures; project consulting
Diehl Remscheid GmbH & Co. KG	k.A.	400	Ausrüstungen für Katastrophenschutz; Logistik; Mechanik; gepanzerte Fahrzeuge	weltweit führender Hersteller von Systemketten für gepanzerte Fahrzeuge: Kettenglieder, Zahnkränze, Leiträder, Laufrollen, Stützrollen
DynITEC GmbH	k.A.	k.A.	Ausrüstungen für Katastrophenschutz; Logistik; Munition	Zünd- u. Anzündmittel, Energetische Materialien, Elektronische Systeme, z.B. Handgranaten- u. Torpedozünder, Sprengstoffe, Funkauslösesysteme
E.I.S. Aircraft GmbH	k.A.	100	Luft- und Raumfahrtsysteme; Rettungssysteme; Mechanik	Entwicklung, Herstellung, Service verschiedener Bauteile, Baugruppen u. Flugzeugbaumuster. luftfahrttechnische Ausrüstungen u. Dienstleistungen (zivil u. militärisch)
ESRI Geoinformatik GmbH	k.A.	150	Rettungssysteme; Luft- und Raumfahrtsysteme; Mechanik; IT; Geoinformatik.	Geographische Informationssysteme (GIS): von Auskunftssystemen im Internet bis zu komplexen raumbezogenen Spezialanwendungen im Simulationsbereich

Name des Unternehmens	Jahres-umsatz Mio. €	Beschäftigte	Sicherheitstechnologien /Anwendungsbereiche	Produkte
ESW	k.A.	k.A.	Anbieter technologisch komplexer, innovativer Produkte und Leistungen in der Zivil- u. Verteidigungstechnik. Fahrzeug- u. Flugzeugausrüstung, Antriebs- und Stabilisierungstechnik, Energiesysteme, Service (militärisch u. zivil)	k.A.
ETEC Gesellschaft für Technische Keramik mbH	k.A.	k.A.	Ausrüstungen für Katastrophenschutz; gepanzerte Fahrzeuge; Mechanik	Verschleiß- u. Korrosionsschutz bei Industrieanlagen, ballistischer Schutz von Personen und Fahrzeugen auf der Basis von Hochleistungskeramiken
Forschungsgesellschaft für Angewandte Naturwissenschaften e.V. (FGAN)	k.A.	520	Sensoren; Simulationen, F&E; IT	Hochfrequenzphysik u. Radartechnik; Optronik und Wärmebildtechnik; Bildverarbeitung und automatische Mustererkennung; Ergonomie/Gestaltung der Mensch-Maschine-Schnittstelle; Kommunikation u. Informationssysteme
Fraunhofer Institut für Naturwissenschaftlich-Technische Trendanalysen	k.A.	k.A.	Öffentliche Sicherheit; F&E	Technologiebeobachtung und -vorausschau, Technologieanalysen, Übergreifende Analysen und Planungsunterstützung, Elektromagnetische Effekte, Nukleare Detektionsverfahren und Sicherheitspolitik, Kernstrahlungseffekte in Elektronik und Optoelektronik, Informationsbeschaffung und -management

Name des Unternehmens	Jahres-umsatz Mio. €	Beschäftigte	Sicherheitstechnologien /Anwendungsbereiche	Produkte
Heggemann AG	k.A.	k.A.	Ausrüstungen für Katastrophen-schutz; gepanzerte Fahrzeuge;	Engineering, Aerospace (Raumfahrt, Luftfahrt, Verteidigung), Automotive
ICOS Gesellschaft für Indus-trielle Communications Systeme mbH	k.A.	k.A.	gepanzerte Fahrzeuge; Luft- und Raumfahrtsysteme; Munition; Ret-tungssysteme	Systemlösungen für industrielle und wehrtechni-sche Anwendungen. gehärtete IT-Komponen-ten zum mobilen und stationären Einsatz für den industriellen und militärischen Markt: Rechner, Server, Laptops, Displays, Netzwerkkomponenten, Software-Lösungen, Visualisierungs- und Kommunikations-anwendungen
IMST GmbH	k.A.	k.A.	Ausrüstungen für Katastrophen-schutz; Öffentliche Sicherheit; F&E; Sensoren; Simulationen; IT	Funksysteme und Mikroelektronik; Auftragsent-wicklung und Lizenzierung von Technologie. Telekommunikation , Automatisierung, Automotive, Medizintechnik, Funk in Hard- und Software, Chips, Schalttechnik, Antennen usw.
Incontrol Enterprise Dyna-mics.com GmbH	k.A.	k.A.	airport & airlines; harbors & ship-ping; production & warehousing; railway systems; supply chain management	k.A.
IABG: Industrieanlagen-Be-triebsgesellschaft mbH	140	1000	Analytische, technische und operationelle Lösungen in Automotive, InfoKom, Verkehr & Umwelt, Luftfahrt, Raumfahrt, Verteidigung & Sicherheit; Sensoren; Simulationen	z.B. Modelbildung u. Simulation, Nachrichten-gewinnung, Transformation

Name des Unternehmens	Jahres-umsatz Mio. €	Beschäftigte	Sicherheitstechnologien /Anwendungsbereiche	Produkte
Ingenieurbüro Hasenau / LPH Engineering	k.A.	k.A.	Sicherheitstechnik, Nachrichten-technik, Elektrotechnik, Ergono-mie, Mensch-Maschine-Interface Optimierung, Medizintechnik	k.A.
Intergraph (Deutschland) GmbH	k.A.	k.A.	Homeland Security, Militär und Nachrichtendienste, Öffentliche Sicherheit	k.A.
ITSS solutions + systems GmbH	k.A.	k.A.	IT-Lösungen und Dienstleistungen	k.A.
LBBZ GmbH	k.A.	k.A.	Öffentliche Sicherheit; F&E; Mechanik; Lasertechnik	k.A.
Logistik-Systembetreuungsge-sellschaft mbH (LOG)	k.A.	k.A.	Öffentliche Sicherheit; IT; Logistik und Informationsmanagement	k.A.
Mayday 24	k.A.	k.A.	IT	Hotline für Notfälle
Metall express GmbH (Cole & Swallow)	k.A.	k.A.	Ausrüstungen für Katastrophen-schutz; Mechanik	Cole & Swallow (UK): e.g. navy; marine & off-shore; aluminium, alloys & aerospace; precision tubing; pneumatic tubes, etc.
nivosta EDV-Systemhaus GmbH	k.A.	k.A.	Öffentliche Sicherheit; Ausrüstun-gen für Katastrophenschutz; IT.	IT-Kozeptlösungen; IT-Dienstleistungen

Name des Unternehmens	Jahres-umsatz Mio. €	Beschäftigte	Sicherheitstechnologien /Anwendungsbereiche	Produkte
R & S Systems GmbH	1,33	6.800 welt-weit	Logistik; gepanzerte Fahrzeuge; Luft- und Raumfahrt.	Test & Measurement; Radiocommunications; Broadcasting; Antennas; IT-Security; Signal Intelligence; Spectrum Monitoring; Trunked Radio; Bündelfunk. microwave; automotive; LAN extension for instrumentation
rola Security Solutions GmbH	k.A.	60	Öffentliche Sicherheit; Logistik; Mechanik; Ausrüstungen für Katastrophenschutz. Telekommunikation u. Logistik	Softwaretechnologien für den Sicherheitsalltag, Polizeiarbeit, Analysemethoden.
Robowatch		45	Ferngesteuerte und autonom navigierende Überwachungs-roboter	ORFRO+Detect, Asendro, MOSRO
Schroth Safety Products GmbH	k.A.	k.A.	Ausrüstungen für Katastrophen-schutz; gepanzerte Fahrzeuge; Luft- und Raumfahrtsysteme; Sensoren	Insassenschutz in Militärfahrzeugen, -flugzeugen und -helikoptern
secunet Security Networks AG	k.A.	k.A.	Öffentliche Sicherheit; Ausrüstun-gen für Katastrophenschutz. Tele-kommunikation und Logistik	IT-Sicherheit; insb. Biometrie/Hoheitliche Doku-mente, Gesundheitswesen, Secure Web Solutions, E-Government, Sicherheitsvalidierung
Serco GmbH	k.A.	40.000 welt-weit	Logistik; IT	k.A.
Sony			Videosensoren	Überwachungskameras

Name des Unternehmens	Jahres-umsatz Mio. €	Beschäftigte	Sicherheitstechnologien /Anwendungsbereiche	Produkte
Spanset GmbH & Co. KG	k.A.	k.A.	Ausrüstungen für Katastrophen-schutz; IT	Hebetechnik, Ladungssicherungstechnik, Höhensicherungstechnik
Technisch-Mathematische Studiengesellschaft mbH (TMS)	k.A.	30	F&E; IT	Berechnung von Schadstoffausbreitungen, Bewertung konventioneller u. intelligenter Flug-körpersysteme
Thomas GmbH	73.000	409	Sicherheitssysteme; Disaster Control, Mechanik	Hoch-/SF-Bau, Straßenbau, Kanalbau, Land-schaftsbau, Recycling, Bauconcept, Zaunbau
Top Security Services	k.A.	k.A.	Öffentliche Sicherheit; Mechanik	k.A.
T-Systems Enterprise Services GmbH	k.A.	k.A.	Öffentliche Sicherheit; Ausrüstun-gen für Katastrophenschutz. IT	k.A.
VCS Engineering AG	k.A.	120	Raumfahrt und Öffentliche Sicherheit	Umwelt- und Erdbeobachtung in Alpinregionen, Ermittlung von Positionsmerkmalen
Vitracom	K.A.	k.A.	Videosensor-Software	SiteView zur automatischen Analyse von Kamerabildern

Literatur

Avihai, Hillel. 2007. "Aviation Security: The Human Eye vs. Detection Technology." *International Institute for Counter-Terrorism (ITC)*, 06/06/2007.

Bayerisches Staatsministerium für Wirtschaft, Infrastruktur, Verkehr und Technologie. 2006. *Allianz Bayern Innovativ: Eckpunkte bayerischer Clusterpolitik*. München, Juni 2006.

Beckstein, Günther. 2004. "Bedrohung internationaler Terrorismus: Was muss Deutschland für die innere Sicherheit tun?" In: J. Vielhaber (Hrsg.), *Homeland Security: Die Bedrohung durch den Terrorismus als Herausforderung für eine gesamtstaatliche Sicherheitsarchitektur*. Berlin: DGAP.

Bernnat, Rainer. 2004. "Herausforderungen einer gesamtstaatlichen Sicherheitsarchitektur am Beispiel Homeland Security." In: J. Vielhaber (Hrsg.), *Homeland Security: Die Bedrohung durch den Terrorismus als Herausforderung für eine gesamtstaatliche Sicherheitsarchitektur*. Berlin: DGAP.

Bundesministerium des Innern. 2005a. *Schutz Kritischer Infrastrukturen - Basisschutzkonzept*. Berlin, Referat Öffentlichkeitsarbeit.

Bundesministerium des Innern. 2005b. *Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen*. Berlin, Referat Öffentlichkeitsarbeit.

Carafano, James Jay. 2007. "Keeping the Skies Friendly: Next Steps for General Aviation Security
" *Backgrounder*, No. 2051.

Davis, Griffin. 2006. "Chemical Detection Equipment for Emergency Response." *Military Technology*, 11/2006, Seiten 54-65.

Emery, Norman; Werchan, Jason und Mowles, Donald G. 2006. "Fighting Terrorism and Insurgery: Shaping the Information Environment." *Milirary Technology*, 11/2006, Seiten 104-110.

Floeting, Holger. 2006. "Sicherheitstechnologien und neue urbane Sicherheitsregime
" *ITA manuscript, Wien*, November 2006.

Foerster, Michael von. 2007. *Homeland Security - Trends, Entwicklung, Technologiethemen. Pressekonferenz des Fachverbandes Sicherheitssysteme*.

Fraunhofer Institut. 2007a. "Künstliche Nasen." *Strategie und Technik*, August.

Fraunhofer Institut. 2007b. "Netzwerksicherheit." *Strategie und Technik*, Juli.

Fraunhofer Institut. 2007c. "Sprengstoffdetektion." *Strategie und Technik*, November.

Geisler, Jürgen. 2007. “Überwachungstechnologie für die zivile Sicherheit.” *Strategie und Technik*, November, Seiten 12-14.

Goericke, Stephan. 2007. *Gründung eines GESA Workshops "Fachkräftequalifizierung". Zweite GESA-Konferenz*. Brüssel.

Hauschild, Elisabeth F. 2007. “Herausforderung Sicherheit.” *Griephan Global Security*, 01, Herbst 2007, Seiten 21-25.

Hellenthal, Markus. 2006. “Sicherheit als Herausforderung. Die technischen Möglichkeiten zum Schutz Kritischer Infrastruktur.” *Homeland Security*, 4/2006, Seiten 10-14.

Klein, Adam. 2007. “The Costs of Terror: The Economic Consequences of Global Terrorism.” *Analysen & Argumente (Konrad-Adenauer-Stiftung)*, 41, Mai 07.

Küchle, Hartmut. 2007. *Die deutsche Heeresindustrie in Europa. Perspektiven internationnaler Kooperationen und industriepolitischer Nachholbedarf*. Düsseldorf: Edition der Hans-Böckler-Stiftung Nr. 200.

Lehmann, Gerd. 2006. "Fahndungshilfe für die Innere Sicherheit. Videoüberwachung in Deutschland." *Behörden Spiegel*, Oktober, S. 44-45.

Mengel, Stefan. 2007. *Sachstand Sicherheitsforschungsprogramme. Zweite GESA-Konferenz*. Brüssel.

Peilert, Andreas. 2007. *Police Private Partnership in der Sicherheitsforschung und in der Entwicklung von Sicherheitstechnik. Zweite GESA-Konferenz*. Brüssel.

Pohler, Andreas. 2007. “Öffentliche Sicherheit. Bewertungen und Lösungsansätze für Deutschland und Europa aus Sicht der IT-Industrie.” *Strategie und Technik*, November, Seiten 8-11.

Rachel, Thomas. 2006. *Sicherheit - eine Frage der Technologie? Forum Neue Technologien des "Security-Kongress" auf der "Security-Messe"* Essen.

Roeder, Eckart. 2007. *Planer und Errichter im ZVEI - Vorstellung der Arge Errichter und ZVEI Akademie für Sicherheitsfragen. Pressekonferenz des Fachverbandes Sicherheitssysteme.*

Schulte, Heinz. 2007. “Macht der Definition.” *Griephan Global Security*, 01, Herbst 2007.

Staimer, Angelika. 2007. *Der Markt für elektronische Sicherheitssysteme in Deutschland 2006 - Daten, Tendenzen, Auswirkungen. Pressekonferenz des Fachverbandes Sicherheitssysteme.*

US General Accounting Office. 2007. *Critical Infrastructure: Challenges Remain in Protecting Key Sectors. Testimony Before the Subcommittee on Homeland Security, Committee on Appropriations, House of Representatives*. GAO-07-626T. Washington D.C., 20. März.

Weisswange, Jan-Phillipp. 2007. "Ausrüstung der Bundespolizei." *Strategie und Technik*, Oktober.

Zintel, Volker. 2007. *Flughafensicherheit. Zweite GESA-Konferenz*. Brüssel.