Bräuninger, Michael et al.

Research Report

Sicherheitsindustrie. HWWI (Teil A): Sicherheit – eine volkswirtschaftliche Perspektive. Berenberg Bank (Teil B): Die Sicherheitsindustrie – Geburt eines Wachstumsmarktes

Strategie 2030 - Vermögen und Leben in der nächsten Generation, No. 7

Provided in Cooperation with:
Hamburg Institute of International Economics (HWWI)

Suggested Citation: Bräuninger, Michael et al. (2008) : Sicherheitsindustrie. HWWI (Teil A): Sicherheit – eine volkswirtschaftliche Perspektive. Berenberg Bank (Teil B): Die Sicherheitsindustrie – Geburt eines Wachstumsmarktes, Strategie 2030 - Vermögen und Leben in der nächsten Generation, No. 7, Berenberg Bank und Hamburgisches WeltWirtschaftsInstitut (HWWI), Hamburg

This Version is available at:
https://hdl.handle.net/10419/102544

Hamburgisches
WeltWirtschafts
Institut

HWWI

SICHERHEITS-INDUSTRIE

Strategie 2030

Vermögen und Leben in der nächsten Generation.
Eine Initiative
des Hamburgischen
WeltWirtschaftsInstituts
und der Berenberg Bank

Privatbankiers gegründet 1590

BERENBERG BANK

Joh. Berenberg, Gossler & Co. KG

Hamburgisches
WeltWirtschafts
Institut

HWWI

Sicherheitsindustrie

HWWI (Teil A)
Sicherheit – eine volkswirtschaftliche Perspektive

Berenberg Bank (Teil B)
Die Sicherheitsindustrie – Geburt eines Wachstumsmarktes

Strategie 2030

Vermögen und Leben in der nächsten Generation.
Eine Initiative des Hamburgischen WeltWirtschaftsInstituts und der Berenberg Bank

Privatbankiers gegründet 1590

BERENBERG BANK

Joh. Berenberg, Gossler & Co. KG

»Berenberg Bank · HWWI: Strategie 2030 – Sicherheitsindustrie«
ist eine gemeinsame Studie der
Berenberg Bank · Neuer Jungfernstieg 20 · 20354 Hamburg und des
HWWI Hamburgisches WeltWirtschaftsInstitut · Heimhuder Straße 71 · 20148 Hamburg

Autoren:
PD Dr. Michael Bräuninger, Julia Freese und Dr. Alkis Henri Otto (Teil A)
Cornelia Koller, Wolfgang Pflüger, Dr. Jörn Quitzau (Teil B)
Stand: Juli 2008

Bezug über:
Berenberg Bank · Unternehmenskommunikation
Neuer Jungfernstieg 20 · 20354 Hamburg
Telefon (040) 350 60-710 · Telefax (040) 350 60-907 · E-Mail: presse@berenberg.de

Strategie 2030 –
Vermögen und Leben in der nächsten Generation

**»Es kommt nicht darauf an, die Zukunft richtig vorherzusagen,
sondern auf sie vorbereitet zu sein.«**

(PERIKLES, ATHENISCHER STAATSMANN, 493–429 V. CHR.)

Die Welt steht vor einer Zeitenwende. Große makroökonomische und geopolitische Trends werden das Leben und Wirtschaften der Menschheit in der nächsten Generation verändern!

Dazu zählen die neue Dimension religiös motivierter terroristischer Bedrohung westlicher Demokratien, die mit der Erweiterung der Europäischen Union verbundene Einführung des Euro als nationalstaatlich übergreifende Gemeinschaftswährung, die Entstehung neuer wirtschaftlicher Schwergewichte in Asien (Volksrepublik China, Indien) mit unausweichlichen Folgen für Rohstoff- und Kapitalmärkte, die Herausforderungen einer rapide alternden Bevölkerung in vielen Industrienationen mit all ihren Konsequenzen für Staatsfinanzen, Sozialsysteme, Arbeitsorganisation, Standortentscheidungen etc. oder der Klimawandel.

Dies alles vollzieht sich vor dem Hintergrund fortgesetzter Technologiesprünge in einer sich globalisierenden Wirtschaft. In der Folge finden politische, gesellschaftliche, technologische und wirtschaftliche Veränderungen immer rascher statt. Mehr noch: Sie beeinflussen sich wechselseitig – mal verstärkend, mal aber auch bremsend – und werden so in der Wahrnehmung der Menschen immer komplexer, auch im Sinne von weniger greifbar. Dies gilt umso mehr, als sie weit in die Zukunft reichen, im Fall des demografischen Wandels sogar generationenübergreifend wirken.

Trotz aller Unsicherheit – eines ist klar: Politiker, unternehmerisch Handelnde und Privatpersonen müssen sich diesem tief greifenden Wandel planerisch und gestalterisch stellen.

So dürfte es ein lohnendes Unterfangen sein, nach Orientierung gebenden Wegweisern zu suchen, sie als solche zu identifizieren und mögliche Wegstrecken sowie Zielorte zu beschreiben. Diesem Versuch dient die gemeinsam vom Hamburgischen WeltWirtschaftsInstitut (HWWI) und der Berenberg Bank getragene Schriftenreihe »Strategie 2030 – Vermögen und Leben in der nächsten Generation«. Sie vereint die Expertise von über unsere Landesgrenzen hinaus anerkannten Konjunkturforschern mit den umfassenden Erfahrungen eines führenden in der Vermögensverwaltung tätigen Privatbankhauses.

Wir wünschen den Lesern eine anregende und nützliche Lektüre!

Inhaltsverzeichnis

Teil B: Die Sicherheitsindustrie – Geburt eines Wachstumsmarktes

Teil A

Sicherheit – eine volkswirtschaftliche Perspektive

HWWI

Zusammenfassung

Menschen sind in ihren Lebensumständen und hinsichtlich ihrer Vermögensausstattung von Risiken verschiedener Art und unterschiedlichen Ausmaßes bedroht. Dabei können Risiken zum Teil versichert und zum anderen Teil vermieden werden, wobei beide Optionen mit Kosten verbunden sind. Die Vermeidung von Risiken kann sowohl durch individuelle Sicherheitsmaßnahmen oder Verhaltensformen als auch auf staatlicher oder gesellschaftlicher Ebene erfolgen. Die optimalen Investitionen in Sicherheit werden dabei durch das individuelle Verhalten und durch gesellschaftliche Gegebenheiten und Prozesse bestimmt.

So führt beispielsweise eine größere finanzielle Ungleichheit tendenziell zu einem erhöhten Gefährdungspotenzial durch Kriminalität. Dieses kann aber durch eine erhöhte Vorsicht ausgeglichen werden. Darüber hinaus beeinflussen private und staatliche Investitionen in Sicherheit wiederum das Gefährdungspotenzial. Dabei können gesellschaftliche Maßnahmen in Teilen individuelle ersetzen. In jedem Fall gilt, dass die Vermeidung von Risiken individuelle und gesellschaftliche Kosten verursacht. Eine fehlerhafte Einschätzung der Bedrohungslage führt zu überhöhten Sicherheitsmaßnahmen, die Zusatzkosten verursachen. Die Studie untersucht Kriminalität, Terrorismus und Datensicherheit als ausgewählte Risiken.

Die Hintergründe und Ursachen für Kriminalität sind vielfältig. Ob zukünftig mehr oder weniger Kriminalität beziehungsweise eine Verschiebung der Bedeutung einzelner Deliktarten zu erwarten ist und wie sich insgesamt die Kosten für die Gesellschaft entwickeln, hängt somit von einer Reihe von Faktoren ab: von der demografischen und wirtschaftlichen Entwicklung, aber auch von der zukünftigen Bedeutung sozialer Normen und nicht zuletzt von der Entwicklung der Aufklärungsraten und der Entwicklung des Strafrechts sowie der öffentlichen Wahrnehmung. Zwei internationale Trends deuten darauf hin, dass die Kriminalität zukünftig steigen könnte. Zum einen ist dies eine Zunahme der Ungleichheit innerhalb und zwischen den Nationen, mit der auch die Anreize für kriminelle Handlungen zunehmen. Zum anderen ist dies die zunehmende Konzentration der Bevölkerung in Städten. Beiden Trends kann durch erhöhte Vorsichts- und Sicherheitsmaßnahmen begegnet werden, sodass nicht notwendig ein Anstieg der Kriminalität folgen muss.

Das Thema Terrorismus hat in den letzten Jahren verstärkt Aufmerksamkeit erfahren. Dabei haben die in jüngster Zeit zu verzeichnenden Anschläge mit islamistischem Hintergrund den Eindruck erweckt, religiöse oder ethnische Motive würden zu den maßgeblichen Triebfedern des Terrors zählen. Daneben ist die Ansicht verbreitet, ein niedriges Einkommensniveau unterstütze tendenziell das Auftreten terroristischer Aktivitäten. Neuere Studien zeigen jedoch, dass das Einkommensniveau beziehungsweise religiöse oder ethnische Unterschiede nur mit Einschränkungen zur Erklärung des Terrorismus herangezogen werden können.

Die Kosten einzelner terroristischer Anschläge können erheblich sein. Beispielsweise wurden die direkten Schäden, die sich infolge der Anschläge des 11. Septembers in New York ergaben, auf rund 0,35 % des US-amerikanischen Bruttoinlandsproduktes (BIP) beziffert. Gesamtwirtschaftlich betrugen die Kosten in Folge der Krise noch im gleichen Jahr schätzungsweise 0,75 % des amerikanischen BIPs. Darüber hinaus ergaben sich auch im internationalen Umfeld erhebliche Kosten. Letztlich sind die volkswirtschaftlichen Kosten aber noch deutlich höher als die direkten Kosten. So können die indirekten Kosten durch präventive Maßnahmen und die Folgen von Unsicherheit sowie damit einhergehende Verhaltensänderungen der Wirtschaftsakteure weit höher liegen als die direkten Kosten.

Über die letzten drei Jahrzehnte hat die elektronische Datenverarbeitung stark an Bedeutung gewonnen. In der Zukunft wird eine immer größere Zahl von Geräten vernetzt. So werden immer mehr Haushalte ans Internet angeschlossen, und neue Endgeräte werden angebunden. Mit der wachsenden Bedeutung der IT und einer zunehmenden Verbreitung in sicherheitsrelevanten Bereichen wachsen auch die Anreize, die IT-Systeme anzugreifen, um diese zu beschädigen oder auszuspionieren. Die Folge ist eine rasant wachsende Zahl von Schadensprogrammen. Diesen stehen aber auch neue Technologien gegenüber, mit denen die Datensicherheit verbessert werden kann. Inwieweit dies zu einer erfolgreichen Bekämpfung von IT-Kriminalität führt, hängt wesentlich davon ab, wer für die Schäden haftet. Die Haftung sollte aus ökonomischer Sicht bei denjenigen angesiedelt sein, die die geringsten Vermeidungskosten haben.

1. Einleitung

Nach den Anschlägen des 11. Septembers 2001 soll der amerikanische Vizepräsident Dick Cheney die Devise ausgegeben haben, dass selbst im Falle einer Wahrscheinlichkeit eines weiteren Anschlages von nur einem Prozent man diesen behandeln solle, als ob die Wahrscheinlichkeit 100 % betrage. Diese als *one per cent doctrine* in die politische Debatte eingegangene Devise stellt eine radikale Position dar und wirft eine interessante Frage auf: Wenn ein Schaden groß, die Wahrscheinlichkeit dafür jedoch relativ klein ist, sollte der Staat tatsächlich buchstäblich alles dafür tun, diesen Schaden abzuwenden? Man mag im Falle des Terrors der Position Cheneys zugeneigt sein, zumal die Folgen weiterer Anschläge, das Ausmaß möglicher Schäden für Leib und Leben unabsehbar sind. Gleichwohl hieße, alles dafür zu tun, dass ein bestimmtes Ereignis nicht eintritt, dass man vieles nicht mehr tun könnte. Totale Sicherheit geht mit hohen Kosten einher und fordert somit einen hohen Preis: einen Verlust an individueller Freiheit, hohe Kosten für die Sicherheitsapparate und damit weniger Ressourcen für andere Ziele wie Infrastruktur oder Bildung und damit langfristig Kosten in Form entgangenen Wirtschaftswachstums.

Gleichwohl spielt Sicherheit für fast alle Menschen eine wichtige Rolle und stellt ein Grundbedürfnis dar. Kriminalität und Terror stellen die Bürger und den Staat daher vor die schwierige Herausforderung, eine richtige Abwägung zwischen Prävention und Abschreckung auf der einen Seite und Freiheit und ökonomischer Vernunft auf der anderen Seite vorzunehmen. Die Schwierigkeiten sind dabei vielfältiger Natur. Risiken und Kosten sind häufig schwer zu messen oder einzuschätzen. Zudem verändert sich das Umfeld, in dem Bürger und Sicherheitsbehörden agieren, stetig. Technische Entwicklungen wie PCs und das Internet bieten große Vorteile und Wohlstandsgewinne, gleichzeitig ergeben sich dadurch neue Bedrohungen für Haushalte und Unternehmen durch die Cyber-Kriminalität. Doch auch bereits bekannte Bedrohungen aus den Bereichen der Kriminalität und des Terrorismus ändern im Zeitablauf ihr Gesicht und gewinnen teils an Bedeutung.

Die vorliegende Studie erläutert, warum Sicherheit ein wertvolles Gut darstellt und welche Handlungsmöglichkeiten zum Umgang mit Risiken die ökonomische Theorie bietet. Danach werden die Entwicklungen der Vergangenheit, zukünftige Trends, Handlungsoptionen und ihre ökonomische Relevanz für ausgewählte Risiken diskutiert.

2. Das Bedürfnis nach Sicherheit

Tagtäglich fällen Menschen Entscheidungen, die für ihre Zukunft bedeutsam sind, obwohl ihnen wichtige Informationen zu den Rahmenbedingungen in der Zukunft und über die Handlungen der Mitmenschen unbekannt sind. Entscheidungen werden unter Unsicherheit gefällt, Chancen und Risiken können ex ante nicht in vollem Umfang abgesehen werden. Ex post, nachdem sich die

einstige Zukunft offenbart hat, werden gute und schlechte Entscheidungen, Erfolge und Misserfolge und die ihnen zugrunde liegenden Ursache- und Wirkungsmechanismen sicht- und verstehbar.

Obwohl oder gerade weil diese Unsicherheit prinzipiell unumgänglich zu sein scheint, ist sie eine stete Quelle des Unbehagens. Wenngleich der Mensch Unsicherheit ertragen muss, kann er jedoch anstreben, die Unsicherheit zu reduzieren oder zumindest die Konsequenzen unvorhergesehener Ereignisse zu begrenzen.

Risiken weisen ganz unterschiedliche Charakteristika auf. Sie unterscheiden sich bezüglich der Eintrittswahrscheinlichkeit, der Art und der Höhe des Schadens und bezüglich des Personenkreises, der zu den Risikoträgern zählt. Wie man mit Unsicherheit umgeht, hat daher zuerst etwas mit der Art des Risikos zu tun. Dabei ist zunächst zwischen materiellen und immateriellen Konsequenzen zu unterscheiden. Erstere meinen hier vor allem finanzielle Risiken, während Letztere eher emotionale oder gar existenzielle Risiken bezeichnen. Dabei ist durchaus denkbar, dass ein und derselbe Schadensfall materielle wie immaterielle Verluste verursacht. So ist der Diebstahl eines Schmuckstücks finanziell, das heißt materiell kompensierbar. Schwieriger wird es jedoch, wenn es sich beim Diebesgut um ein Erbstück oder ein Geschenk, das einen emotionalen Wert hat, handelt. Ähnlich verhält es sich bei Gefahr für Leib und Leben: Zwar ist der materielle Schaden, zum Beispiel der Einkommensverlust für die Hinterbliebenen, bei Versehrtheit oder Tod des Einkommensbeziehers ersetzbar, nicht jedoch der persönliche Verlust. Als Folge dieser unterschiedlichen Verlustarten ergeben sich für risikoaverse Personen zwei Möglichkeiten, mit der Unsicherheit umzugehen: Sie können einerseits versuchen, spezifische Risiken zu vermeiden und die Wahrscheinlichkeit eines Schadensfalles zu verringern, oder sie können andererseits einen eventuellen Schaden versichern, indem sie einem Versicherer eine Prämie für die Übernahme des Risikos zahlen. Obwohl beide Strategien bei materiellen wie immateriellen Risiken angewendet werden können, dürften bei vorwiegend immateriellen Risiken vor allem Risikovermeidung und Prävention den Umgang mit dem Risiko charakterisieren. Da materielle Schäden finanziell erstattet werden können, bietet sich hier oftmals die Versicherung an.

2.1 Strategien im Umgang mit Unsicherheit

2.1.1 Versicherung und Diversifikation von Risiken

Während die Vermeidung bestimmter Risiken – insbesondere bei Aktivitäten, die die Gefahr für Leib und Leben erhöhen – recht einleuchtend ist, sind die Zusammenhänge, die zu Versicherungen führen, weit weniger intuitiv. Experimente haben gezeigt, dass bei den meisten Menschen die Freude, 500 Euro zu finden, bei Weitem durch den Ärger übertroffen wird, der auftritt, wenn man 500 Euro verliert. Glück und Leid sind bei den meisten Menschen asymmetrisch verteilt. Doch woran liegt das? Warum verursacht der gleiche Betrag mehr Leid bei Verlust als Freude beim Fund? Tatsächlich liegt dies darin begründet, dass mehr Geld oder mehr Einkommen das Wohlbefinden

zwar erhöht, dieser Effekt jedoch mit steigendem Einkommen oder Vermögen abnimmt – ein Sättigungseffekt tritt ein. Dieser Sättigungseffekt kann nicht nur für Geld, sondern auch für andere Güter und Dienstleistungen beobachtet werden. Wenn eine Person, die zur Gruppe der Geringverdiener zählt, die 500 Euro fände, so erhöhte dieser Betrag ihr Glück sehr wahrscheinlich mehr, als wenn die Person ein Spitzenverdiener wäre. Umgekehrt wird das Leid bei Verlust umso größer, desto geringer das verfügbare Einkommen ist.

In der Realität sehen ökonomische Risiken zumeist etwas anders aus als die Modell- und Laborfälle in der ökonomischen Forschung, doch die experimentell gewonnenen Erkenntnisse über das Verhalten und Empfinden der Menschen sind übertragbar. Ein realistisches und sehr bedeutendes Beispiel für Risiken des alltäglichen Lebens sind beispielsweise Einkommensschwankungen der Haushalte. Die jährlichen Einkommen sind zwar zumeist stabil, Wirtschaftswachstum und beruflicher Erfolg sorgen für Einkommenssteigerungen, aber gleichwohl werden Stetigkeit und Wachstum durch Risiken wie Krankheit, Arbeitsplatzverlust oder geschäftliche Misserfolge bedroht. Das jährliche Einkommen gleicht daher einer Lotterie. Um zu entscheiden, wie bedrohlich die Risiken beziehungsweise wie verheißungsvoll die Chancen sind, müssen ihre materiellen und immateriellen Konsequenzen mit ihrer Wahrscheinlichkeit gewichtet werden. Im Ergebnis erhält man dann den Erwartungswert des Einkommens, also das zu erwartende durchschnittliche jährliche Einkommen. In guten Jahren liegt das tatsächliche Einkommen über diesem Erwartungswert, in schlechten Jahren – beispielsweise in Jahren der Krankheit oder des wirtschaftlichen Misserfolgs – unterhalb des Erwartungswerts. Da aufgrund des Sättigungseffektes Einkommensverluste schwerer wiegen als Einkommensgewinne in gleicher Höhe, bereiten schlechte Jahre den meisten Menschen mehr Kummer, als die guten Anlass zur Freude geben. Es wäre daher eine Erleichterung für sie, wenn sie die Unsicherheit über die Höhe des aktuellen Jahreseinkommens mindern oder besser ganz eliminieren könnten. Nicht selten besteht daher die Bereitschaft, für eine derartige Entlastung auch Geld in Form einer Risikoprämie zu bezahlen – insbesondere dann, wenn die Risiken dauerhafte oder gar permanente negative Konsequenzen beinhalten. Sicherheit wird damit zu einer käuflichen Dienstleistung. Käufer dieser Leistung werden als risikoscheu oder risikoavers bezeichnet.

Die Anbieter einer Risikoübernahme sind zumeist Versicherungsgesellschaften, doch zählen auch Investmentfonds, die die Risiken bei Kapitalanlagen bündeln und verteilen, im Prinzip zu dieser Gruppe der Finanzdienstleister. Die Geschäftsidee der Versicherungen besteht darin, ein Risiko, das für einen Haushalt allein ruinöse Folgen hätte, auf viele Schultern zu verteilen und – dem Gesetz der großen Zahl folgend – darauf zu vertrauen, dass die zu erwartenden Schadensfälle nicht häufiger als üblich innerhalb der Gruppe der Versicherten auftreten. Der einzelne Versicherte zahlt dann als Preis eine Prämie, die über dem durchschnittlich zu erwartenden Schaden der Personen innerhalb der Versicherungsgemeinschaft liegt. Die Differenz fließt der Versicherung zu. Gleichsam sorgt die Versicherungsprämie dann dafür, dass die versicherten Personen letztlich ein geringeres Einkommen zur Verfügung haben, als wenn sie den Erwartungswert der Lotterie erhalten würden.

Dafür haben sie jedoch Sicherheit erworben. Wenngleich Versicherungen Schutz vor Unsicherheit bieten, ergibt sich häufig das Problem, dass bestimmte Risiken nicht versichert werden. Diese Nichtexistenz von spezifischen Versicherungsmärkten liegt jedoch nicht unbedingt darin begründet, dass manche individuelle Risiken zu speziell und damit nicht bündelbar wären. Hierfür gibt es spezialisierte Versicherungsgesellschaften, die auch außergewöhnliche Risiken verbriefen und auf Finanzmärkten anbieten. Eine wichtige Ursache für die Nichtversicherbarkeit mancher Risiken liegt darin, dass die Informationen über den Eintritt des Schadensfalles ungleich über potenzielle Versicherungen und Kunden verteilt sind. Im Falle einer solchen Informationsasymmetrie müssen Versicherungen befürchten, dass für eine gegebene Prämienhöhe vor allem diejenigen Personen Versicherungsschutz suchen, die eine besonders hohe Wahrscheinlichkeit für einen Schadensfall haben. Eine Bündelung dieser schlechten Risiken wäre dann jedoch nicht profitabel für die Versicherungsgesellschaft. Gleichzeitig besteht für gewinnorientierte Versicherungen ein Anreiz, vor allem gute Risiken im Portfolio zu haben, sodass vergleichsweise selten Schadensfälle auftreten. In beiden Fällen spricht man von adverser Selektion. Die zum Teil vorliegende asymmetrische Informationsverteilung hat daher den Effekt, dass bestimmte Risiken gar nicht versichert werden. Somit kommt es zu einem Marktversagen. Einer der bekanntesten Versicherungsmärkte, der in diesem Kontext genannt werden kann, ist der Markt der Krankenversicherung. Sein Bestehen ist zu einem großen Teil darauf zurückzuführen, dass es eine gesetzliche Versicherungspflicht und Kontrahierungszwang gibt.

Ein zweiter Grund für das Fehlen bestimmter Versicherungsmärkte besteht darin, dass bei Abschluss eines Versicherungsvertrages Versicherte unter Umständen fahrlässiger handeln, als sie es vor Abschluss des Versicherungskontraktes getan haben. Zum Problem wird dieses Moral Hazard genannte Verhalten dann, wenn es der Versicherung mangels Information nicht oder nur sehr schwierig möglich ist, Fahrlässigkeit gegebenenfalls nachzuweisen. Auch hier ist die ungleiche Verteilung von Informationen letztlich verantwortlich dafür, dass bestimmte Risiken nicht versichert werden.

Neben den Informationsasymmetrien, die zu Marktversagen führen können, hat das Versicherungsprinzip aber auch auf funktionierenden und intakten Versicherungsmärkten seine Grenzen. Diese sind vor allem dann erreicht, wenn sich systemische Risiken materialisieren. Systemische Risiken liegen vor, wenn ein bestimmtes Ereignis zu Schadensfällen bei einer sehr großen Zahl oder gar bei allen Versicherten führt. In diesem Fall versagt das Gesetz der großen Zahl, und die Zahl der Versicherungsansprüche übersteigt die Zahlungsfähigkeit der Risikogemeinschaft. Versicherungen können daher lediglich individuelle Risiken absichern. Beispielsweise bietet die Arbeitslosenversicherung einzelnen Versicherten Schutz vor den finanziellen Konsequenzen unverschuldeter Arbeitslosigkeit. Kommt es jedoch zum Beispiel aufgrund einer allgemeinen schlechten Wirtschaftsentwicklung zu Massenarbeitslosigkeit, gerät die Arbeitslosenversicherung – je nach Ausmaß der Arbeitslosigkeit – in finanzielle Nöte. Ganz ähnlich bietet der Kauf von Anteilen eines Investmentfonds Schutz vor einer negativen Entwicklung einer einzelnen Aktie, die man alternativ hätte

halten können. Gleichwohl bringt die Risikodiversifikation nichts, wenn der gesamte Aktienmarkt und damit der gesamte Aktienfonds von einem Kursverfall betroffen ist. Ganz generell gilt daher, dass systemische Risiken nicht versichert werden können. Der einzige Ausweg, der bei Existenz substanzieller systemischer Risiken bleibt, ist, die Versichertengemeinschaft um Versicherungsnehmer zu erweitern, die nicht von den gleichen systemischen Risiken bedroht werden. So sollten die Versicherungsnehmer eines hurrikangefährdeten Landstrichs beispielsweise Versicherungsteilnehmer aus möglichst weit entfernten Landstrichen in die Risikogemeinschaft aufnehmen.

2.1.2 Risikovermeidung und Gefahrenabwehr

Drohen systemische Risiken oder immaterielle Schäden, insbesondere Gefahr für Leib und Leben, so ist eine Versicherung häufig nicht möglich oder nicht zweckmäßig. Zumeist erhalten bei derartigen Risiken Strategien den Vorzug, die, statt Schadensfälle grundsätzlich zu akzeptieren und zu versichern, die Wahrscheinlichkeit eines Schadensfalles zu begrenzen versuchen. Erkennbare Risiken werden dann gemieden. Auf individueller Ebene können beispielsweise risikoträchtige Aktivitäten vermieden oder durch Sicherheitsvorkehrungen Gefahren abgewendet werden. Risikoscheue Individuen vermeiden daher unter Umständen Reisen in Krisengebiete, betreiben keine Extremsportarten, fliegen ungern oder nutzen in den Abend- oder Nachtstunden nicht das öffentliche Verkehrssystem und zahlen lieber ein Taxi. Die hiermit verbundenen Einschränkungen oder Maßnahmen stellen Kosten dar, die im Falle der nächtlichen Taxifahrt offensichtlich, in einer Vielzahl der Fälle jedoch nur in verdeckter Form auftreten, sodass ihre Bedeutung häufig unterschätzt wird.

Für eine andere Risikoart, Kriminalität und Terror als von Menschen gemachte Risiken, kommt aber vor allem dem Staat eine besondere Bedeutung zu. Zwar sind bestimmte Risiken im Bereich der Kriminalität wie beispielsweise Diebstahl versicherbar, und auch der private Erwerb von Sicherheitstechnik oder Sicherheitsdiensten mindert das Risiko, Opfer einer Straftat zu werden, doch spielen hier Prävention und Gefahrenabwehr staatlicherseits auch aus Gerechtigkeitserwägungen und aufgrund des Gewaltmonopols des Staates eine wichtige Rolle.

Unabhängig davon, ob Sicherheit durch private oder staatliche Maßnahmen erhöht werden soll, ist die Organisation dieses Vorhabens Widrigkeiten ausgesetzt. Die Probleme liegen vor allem darin begründet, dass Sicherheit oftmals den Charakter eines öffentlichen Gutes hat. Dies bedeutet, dass, sobald Sicherheit hergestellt ist, auch Individuen an dieser teilhaben, die finanziell nicht beitragen wollten beziehungsweise nicht beigetragen haben. Damit ergibt sich ein Spielraum für taktisches Verhalten, wenn es um die private Finanzierung und Bereitstellung von Sicherheit geht. Die Mitglieder eines Kollektivs haben einen permanenten Anreiz, ihr wahres Sicherheitsbedürfnis nicht offenzulegen. Sie werden dabei von der Hoffnung geleitet, die übrigen Mitglieder würden Sicherheit erstellen und die Kosten dennoch übernehmen. Als Folge dieses taktischen Verhaltens kommt es daher häufig zu Marktversagen, was bedeutet, dass Sicherheit, obwohl sie von einer größeren Zahl gewünscht wird, nicht privatwirtschaftlich bereitgestellt wird. Aus diesem Grund kann eine

Ausgaben für die öffentliche Ordnung und Sicherheit im internationalen Vergleich, 2005

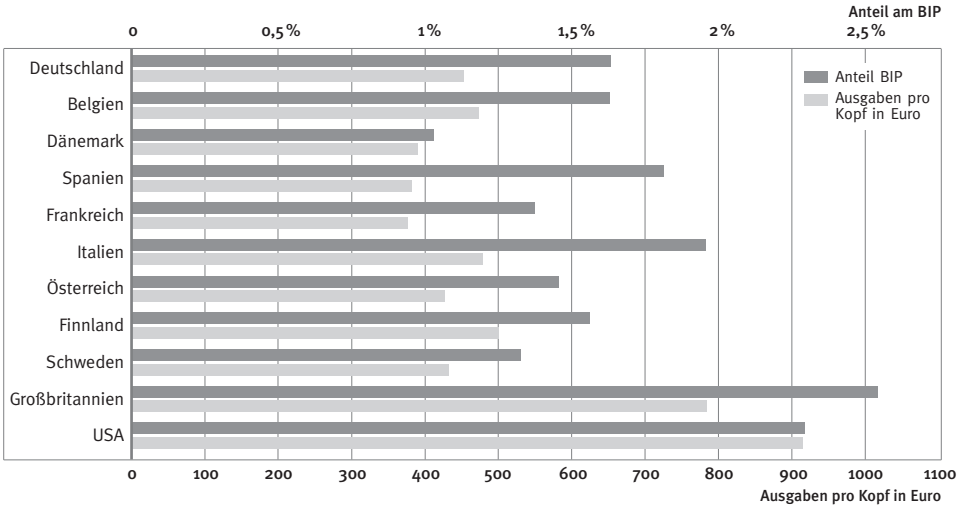

Abb. 1

Quellen: Eurostat (2008); Berechnungen des HWWI.

höhere öffentliche Sicherheit zumeist nur auf staatliche Initiative realisiert werden. Ein prominentes Beispiel ist hier der Bau eines Deiches zum Schutz vor Hochwasserkatastrophen, der prinzipiell auch von privater Hand finanziert und errichtet werden könnte. Einen ähnlichen Charakter haben auch die Landesverteidigung oder die Innere Sicherheit, die, wenn einmal die Grenzen gesichert sind oder kriminelle Strukturen zurückgedrängt werden, allen Inländern, ob zahlungsbereit oder nicht, zugutekommen.

Da dem Staat somit eine wichtige Rolle bei Prävention und Gefahrenabwehr zukommt, stellt sich die politisch relevante Frage, in welchem Umfang Sicherheit hergestellt werden soll oder genauer: welcher Mittelaufwand betrieben und welche Maßnahmen durchgeführt werden sollen. Die als Ergebnis eines politischen Abstimmungsprozesses resultierende Sicherheitspolitik ist jedoch bestenfalls ein Kompromiss, da einerseits die Risikobewertungen und andererseits die im Schadensfall resultierenden Reaktionen der Wähler – und damit ihr Sicherheitsbedürfnis – divergieren. Einigen wird daher zu viel Sicherheit, anderen zu wenig Sicherheit bereitgestellt. Für Letztere ergibt sich ein über die staatliche Grundversorgung hinausgehender Bedarf an Sicherheit, der die Basis für die Nachfrage nach privaten Sicherheitsdienstleistungen und Sicherheitstechnik bildet. Gleichermaßen kann aber ein Zuviel an Sicherheit zu zusätzlichen Kosten führen, da hohe Sicherheitsbestimmungen, starke Kontrollen oder Genehmigungsverfahren die Mobilität und Aktivität der Bürger über den Nutzen der zusätzlichen Sicherheit hinaus hemmen können. Ökonomisch gesprochen nehmen in diesem Fall die Transaktionskosten – Kosten gesellschaftlicher und wirtschaftlicher Interaktion – zu, und es bestehen zudem Opportunitätskosten, da ein Zuviel an Sicherheit Ressourcen bindet, die auch anderweitig eingesetzt werden könnten. Abbildung 1 zeigt, dass Staaten höchst unterschiedlich in Sicherheit investieren. Dies kann darauf zurückzuführen sein, dass die Bürger in verschiedenen Ländern staatliche Sicherheit in unterschiedlichem Maße wertschätzen oder dass sich die Verteilung zwischen staatlichen und privaten Sicherheitsmaßnahmen unterscheidet. Letztlich kann auch das gesellschaftliche Umfeld in den Staaten verschieden sein, sodass unterschiedliche Maßnahmen notwendig sind, um das gleiche Maß an Sicherheit herzustellen.

3. Ausgewählte Risiken

3.1 Kriminalität in Deutschland

Kriminalität ist in ihrer Erscheinungsform und ihren Ursachen ein höchst komplexes Phänomen. Unterschiedlichen Delikten kommt nicht nur eine unterschiedliche empirische Relevanz zu, auch bezüglich der Schwere der Delikte ergeben sich erhebliche Differenzen, sodass das Phänomen Kriminalität kaum allgemeingültig diskutiert und analysiert werden kann. Allein die Erfassung der einzelnen Delikte unterliegt erheblichen methodischen Problemen. So wird im Grunde nur die polizeilich registrierte Kriminalität erfasst; kriminelle Handlungen, die zu keiner Anzeige führen, bleiben im Dunkelfeld verborgen. Die Entwicklung der registrierten Kriminalität im sogenannten Hellfeld ist hingegen Gegenstand zahlreicher kriminologischer Untersuchungen, deren wesentliche Ergebnisse und ökonomische Relevanz im Folgenden kurz dargestellt werden sollen.

3.1.1 Entwicklung der Kriminalität

Die statistisch erfasste Kriminalität hat im langfristigen Vergleich deutlich zugenommen. Im Jahr 1976 wurden 3 063 271 Fälle verzeichnet, im Jahr 2006 waren es 6 304 223, also fast das 2,1-fache. Zu berücksichtigen ist dabei allerdings die gestiegene Bevölkerungszahl im entsprechenden Zeitraum. Bezogen auf die Zahl der registrierten Fälle pro 100 000 Einwohner bedeutet das einen Anstieg von 4 980 auf 7 647 (siehe Abbildung 2).[1] Insgesamt beruht der langfristige Anstieg der polizeilich registrierten Kriminalität in erster Linie auf Diebstahlsdelikten, einer Zunahme der Betrugsfälle und der Sachbeschädigungen.

Zwischen 1976 und 1985 sowie Mitte der 90er-Jahre sind dabei für die insgesamt erfasste Kriminalität die größten Steigerungsraten zu verzeichnen. Seit Mitte der 90er-Jahre ist hingegen ein leicht rückläufiger Trend zu erkennen. Gleichwohl können sich auch in Phasen, in denen die Gesamtzahl der Delikte stagniert, erhebliche Veränderungen in der Deliktstruktur ergeben.

1 Vgl. Bundeskriminalamt (2007), S. 28.

Langfristige Entwicklung der registrierten Kriminalfälle, 1976–2006

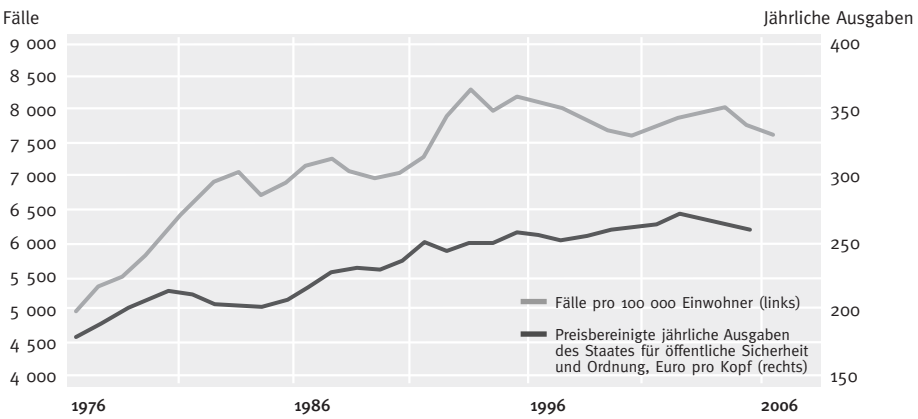

Abb. 2

Quellen: Bundeskriminalamt (2007); Statistisches Bundesamt (2005).

Entwicklung ausgewählter Kriminalitätsbereiche, 1997–2006

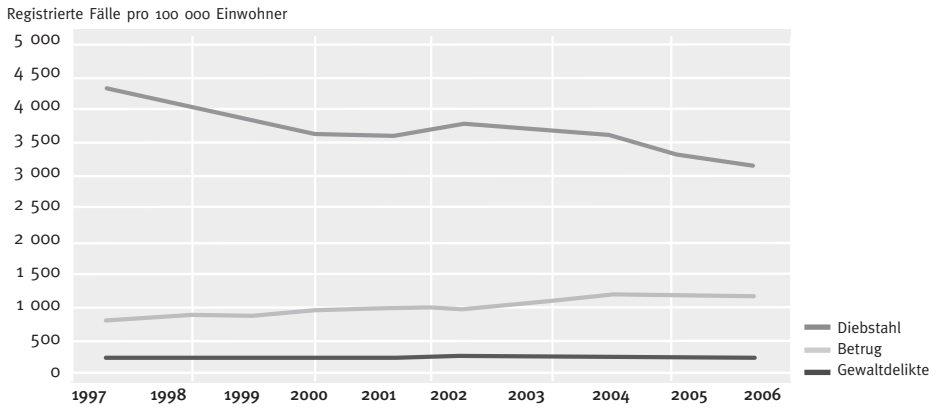

Abb. 3 Quellen: Bundesministerium des Innern, Polizeiliche Kriminalstatistiken (1998-2006).

Gliedert man die Gesamtkriminalität nach einzelnen Bereichen auf, dominieren aktuell wie auch in den Vorjahren die Diebstahlsdelikte, die zu den Eigentums- und Vermögensdelikten zählen. Die statistische Erfassung von Diebstählen ist, stärker als in anderen Deliktbereichen, abhängig von Anzeigen der Opfer. Schwankungen in den registrierten Fällen sind folglich eng mit dem wahrgenommenen Schaden und den Anzeigen der Opfer verbunden. Die registrierten Diebstähle pro 100 000 Einwohner sind in den letzten Jahren entgegen dem langfristigen Trend von 35,4 auf 26 % gesunken. Der Anteil der Betrugsfälle hingegen ist in den letzten Jahren stetig gewachsen. Verglichen mit 1997 ist in 2006 ein Anstieg der Betrugsfälle um knapp 5 % zu verzeichnen, der vor allem auf die Automatisierung des Geldverkehrs und den zunehmenden Warenverkehr über das Internet zurückzuführen ist. Im Jahr 2006 kommen 1 157 Betrugsfälle auf 100 000 Personen. Die Gewaltdelikte sind von 1997 bis 2006 um rund 34 000 auf insgesamt 261 471 Fälle gestiegen, vor allem aufgrund zunehmend gefährlicher und schwerer Körperverletzung sowie Raubdelikten (siehe Abbildung 3).

Der im Folgenden dargestellte Vergleich der Kriminalität in Deutschland zu anderen Ländern unterliegt verschiedenen analytischen Problemen. Insbesondere relevante politische und gesellschaftliche Rahmenbedingungen sowie statistische Erfassungen in Kriminalstatistiken machen internationale Vergleiche sehr schwierig. Möglich ist aber zu untersuchen, ob die nationale Kriminalitätsrate im Zeitablauf erheblichen Schwankungen unterlegen ist, um die Innere Sicherheit eines Landes beziehungsweise einer Region beurteilen zu können, indem politische und gesellschaftliche Veränderungen in die Analyse miteinbezogen werden. Für den Zeitraum von 1990 bis 2002 zeigt sich für die Europäische Union eine relativ stabile Lage der Inneren Sicherheit ohne große Schwankungen. Zwischen den EU-Mitgliedsstaaten sind allerdings erhebliche Differenzen in der Kriminalitätsentwicklung zu erkennen, wobei die Schwankungen keinem erkennbaren Muster folgen. Betrachtet man die Entwicklung der polizeilich registrierten Kriminalität in ausgewählten europäi-

schen Staaten hinsichtlich Rückgang oder Anstieg zwischen 1995 und 2000, so zeigt sich, dass die Kriminalität in Luxemburg in diesem Zeitraum am deutlichsten abgenommen und in Nordirland am deutlichsten zugenommen hat. Deutschland nimmt in diesem europäischen Vergleich eine mittlere Position ein, hier ist von 1995 bis 2000 insgesamt ein Rückgang der registrierten Straftaten um 7 Prozentpunkte zu beobachten.

Durch Opferbefragungen in diversen Weltregionen lassen sich Unterschiede in der registrierten und persönlich wahrgenommenen Kriminalitätsbelastung erheben. Sowohl bei der Gewalt- als auch Eigentumskriminalität schneiden die asiatischen Staaten bei amtlich registrierter und persönlich wahrgenommener Kriminalität am besten ab. Afrika weist nach Bevölkerungsangaben im Ranking von Gewalt- und Eigentumskriminalität in beiden Fällen die höchste Belastung auf. Europa nimmt die zweitgünstigste Position ein. Insgesamt lassen die internationalen Vergleiche den Schluss zu, dass in Europa, verglichen mit anderen Weltregionen, von einer relativ günstigen Lage der Inneren Sicherheit ausgegangen werden kann.[2] Internationale Vergleichbarkeit besteht am ehesten bei Schwerkriminalität, insbesondere bei Tötungsdelikten aufgrund ähnlicher gesetzlicher Definitionen über Landesgrenzen hinweg. Im europäischen Vergleich waren, bezogen auf das Jahr 2000, die Tötungsdelikte pro 100 000 Einwohner in der Schweiz und Spanien am niedrigsten und in Finnland am höchsten. Deutschland nimmt dabei zusammen mit Österreich die zweitbeste Position ein und ist nach Angaben der Weltgesundheitsorganisation (WHO) das Land, bei dem die Entwicklung am deutlichsten nach unten ging.[3]

2 Vgl. Bundesministerium des Innern, Bundesministerium der Justiz (2006), S. 25 ff.
3 Vgl. Heinz (2007), S. 5 ff.

Entwicklung angezeigter und nicht angezeigter Körperverletzung am Beispiel der Stadt Bochum, 1975–1998

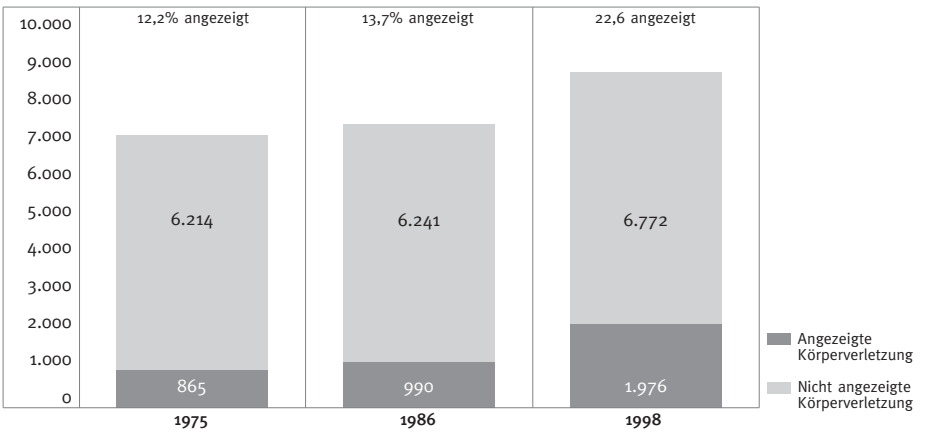

Abb. 4 Quellen: Bundesministerium des Innern, Bundesministerium der Justiz (2006).

Registrierte Kriminalität und Anzeigebereitschaft

Die Daten der Kriminalstatistik bilden nicht die vollständige Kriminalität ab. Dies liegt daran, dass nicht alle anfallenden Straftaten zur Anzeige gebracht werden. Hierfür gibt es unterschiedliche Gründe. Ob eine Straftat angezeigt wird, hängt unter anderem von der Deliktart, dem wahrgenommenen Schaden, der Opfer-Täter-Beziehung und der Einschätzung zur Effektivität polizeilicher Arbeit ab. Aus einem Anstieg der registrierten Kriminalität folgt deshalb nicht zwingend, dass auch mehr Straftaten begangen worden sind. Bei einer geringeren Anzeigequote krimineller Handlungen steigt der Anteil der nicht registrierten Fälle, und die Zahl der statistisch erfassten Kriminalfälle geht zurück, wodurch fälschlicherweise der Eindruck größerer Sicherheit entstehen kann. Somit wird die Bewertung und Einordnung der Daten erschwert, woraus die Notwendigkeit entsteht, Veränderungen der Anzeigeraten in die Interpretation mit einzubeziehen. Bisher gibt es für Deutschland keine kontinuierlich durchgeführten empirischen Studien, die entsprechende Entwicklungen belegen können. Verfügbar sind aber einzelne regionale Opferbefragungen. Dazu gehört die in den Jahren 1975, 1986 und 1998 durchgeführte Bochumer Erhebung mit dem Ziel, Veränderungen der angezeigten und nicht angezeigten Straftaten zu erfassen. Bezogen auf leichte und schwere Diebstahlsdelikte gab es zu allen drei Messzeitpunkten kaum Veränderungen in der Anzeigerate. Anders ist es bei Fällen, die Körperverletzungen betreffen. Während bei den ersten beiden Befragungen die Anzahl der Körperverletzungen insgesamt (angezeigte und nicht angezeigte Fälle) relativ konstant geblieben ist, ist zwischen 1986 und 1998 eine deutliche Zunahme erkennbar (Abbildung 4).

Zwei Drittel der Zunahme von polizeilich registrierten Körperverletzungen in Bochum sind dabei allein auf eine steigende Anzeigerate zurückzuführen. Offensichtlich haben verschiedene Faktoren, wie die Art des Delikts, der wahrgenommene Schaden sowie Einschätzungen über den Erfolg der polizeilichen Arbeit, dazu beigetragen, dass die Quote der nicht angezeigten Fälle in Bochum zurückging und zum Anstieg der erfassten Kriminalität führte. Ob diese Entwicklung auch über Bochum hinaus und auf andere Deliktgruppen anwendbar ist, bleibt fraglich, da entsprechende empirische Untersuchungen fehlen. Ähnliche Ergebnisse zeigt aber auch eine in den Jahren 1998 und 2005 vom Kriminologischen Institut Niedersachsen durchgeführte Schülerbefragung der 9. Jahrgangsstufe in Stuttgart, München und Schwäbisch-Gmünd. Auch hier wurde ein Anstieg der Anzeigebereitschaft von Gewaltdelikten von 17,5 % auf 20,7 % festgestellt. Studien dieser Art sind zwar kein Beleg, wohl aber ein Hinweis darauf, dass der Anstieg der registrierten Kriminaldelikte in den letzten Jahrzehnten jedenfalls zum Teil auf eine höhere Anzeigebereitschaft der Opfer zurückzuführen ist.[4]

Kasten 1

4 Vgl. Heinz (2007).

3.1.2 Ursachen der Kriminalität

Entgegen dem landläufigen Sprichwort, nach dem schon Gelegenheit Diebe mache, geht die ökonomische Theorie der Kriminalität davon aus, dass kriminelle Handlungen (mit Ausnahme von Affekthandlungen) erst in Folge einer bewussten, das heißt rational gefällten Entscheidung begangen werden. Straftäter wägen dabei ab, ob der zu erwartende Nutzen einer Straftat den Nutzen einer alternativen Verwendung von Zeit und Ressourcen übersteigt. Hierzu wird das erzielbare Einkommen aus einer erfolgreich begangenen Straftat den entstehenden Kosten bei Ergreifung gegenübergestellt und unter Verwendung von Wahrscheinlichkeiten das damit zu erwartende Einkommen aus der Straftat ermittelt. Ist es negativ, ist die Straftat in jedem Fall nicht vorteilhaft und unterbleibt. Ist es positiv, so wird das zu erwartende Einkommen der Straftat mit dem zu erwartenden Einkommen einer legalen Tätigkeit verglichen. Erst wenn dieser Vergleich eine Straftat lukrativer erscheinen lässt, wird sie in die Tat umgesetzt. Dieser seitens des Nobelpreisträgers Becker in die Ökonomie eingeführte Ansatz zur Kriminalität beschreibt zwar nicht erschöpfend, warum Individuen Straftaten begehen.[5] Hier spielen nicht zuletzt auch soziale Normen und Werte sowie charakterliche Eigenschaften eine wichtige Rolle, für deren Erklärung Erkenntnisse aus den Bereichen der Psychologie und Soziologie herangezogen werden können. Beckers Ansatz formuliert aber eine notwendige Bedingung für das Begehen einer kriminellen Handlung, in die neben harten ökonomischen und kriminologischen Einflussgrößen auch wichtige weiche Faktoren wie soziale Normen einbezogen werden können.

Basierend auf dem Ansatz Beckers hat es in den vergangenen Jahrzehnten eine Vielzahl von Studien zur Erklärung der Ursachen und Hintergründe für Kriminalität gegeben. Für die Bundesrepublik Deutschland konnten Entorf und Spengler in einer Studie zentrale Hypothesen des Becker'schen Ansatzes bestätigen und zusätzlich weitere sozioökonomische und demografische Hintergründe und Ursachen näher beleuchten.[6] So wirkte sich die Rate der Verbrechensaufklärung in den einzelnen Bundesländern tatsächlich abschreckend auf die Zahl der Delikte pro Kopf aus. Auch das Einkommen hatte signifikant Einfluss auf das Ausmaß der Kriminalität, wobei sowohl das Einkommen der Region als auch die Ungleichverteilung zur Erklärung herangezogen wurden. Hiernach führt ein höheres Einkommen tendenziell zu mehr Kriminalität in einer Region, da sich eine Straftat tendenziell eher lohnt. Gleichzeitig sorgt eine höhere Ungleichverteilung dafür, dass mehr Straftaten begangen werden, da die Möglichkeiten, einen höheren Nutzen aus einer legalen Tätigkeit zu ziehen, geringer sind. Eng hiermit verbunden ist auch die Bedeutung der Arbeitslosigkeit innerhalb einer Region für die Kriminalität. Eine höhere Arbeitslosenquote sorgt nicht nur tendenziell für eine höhere Ungleichverteilung des Einkommens, sie hat auch zur Folge, dass einem größeren Anteil der Bevölkerung schlicht die Zeit zur Verübung von Straftaten zur Verfügung steht. Bemerkenswert ist auch eine Reihe von demografischen Charakteristika, die zum Verständnis der Ursachen der Kriminalität einen Beitrag leisten kann. Ganz offensichtlich und unbestritten spielt das Geschlecht eine wichtige Rolle, da zu einem überwiegenden Teil Männer Straftaten begehen.

5 Vgl. Becker (1968).
6 Vgl. Entorf/Spengler (2000).

Gleichzeitig lässt sich zeigen, dass junge Menschen überproportional in den Kriminalstatistiken auffällig werden. Typischerweise steigt dabei die Kriminalitätsbelastung bis zur Altersgruppe der 25-Jährigen und fällt dann wieder ab. Dieses international zu beobachtende Muster gilt in Deutschland bereits seit Jahrzehnten (siehe Abbildung 5), sodass festgestellt werden kann, dass die auffällige Kriminalitätsbelastung Jugendlicher kein alleiniges Phänomen der Gegenwart darstellt. Für die höhere Anfälligkeit der Jüngeren zur Kriminalität gibt es durchaus plausible Erklärungsansätze: Mögliche Gründe hierfür könnten beispielsweise darin liegen, dass junge Menschen sich weniger an soziale Normen gebunden fühlen oder gar dagegen rebellieren, dass sie in geringerem Maße als Ältere im Falle einer aufgedeckten Straftat einen Reputationsverlust in ihren sozialen Netzwerken erleiden oder dass sie sich schwieriger den Sicherheitsbehörden entziehen können und so im Vergleich zu Älteren eher aktenkundig werden. Gleichwohl wäre aber ein bloßes Abstellen auf ein junges Alter zu einfach, um die höhere Kriminalitätsrate in dieser Gruppe zur erklären. Zu berücksichtigen ist auch, dass junge Menschen überdurchschnittlich von Arbeitslosigkeit betroffen sind und tendenziell über niedrigere Einkommen als der Durchschnitt verfügen, sodass eventuell nicht das Alter an sich, sondern mit dem Alter korrelierte Faktoren der eigentliche Grund für die überproportionale Kriminalitätsbelastung dieser Gruppe sind. Hierzu passt insbesondere, dass die Kriminalitätsbelastung eines Jahrgangs zunächst steigt und ab Mitte 20 wieder abnimmt, da mit voranschreitendem Alter und Berufserfahrung auch die legalen Verdienstmöglichkeiten zunehmen.[7]

Wenngleich der ökonomische Ansatz allein Kriminalität nicht erschöpfend erklären kann, so ist er doch von großem Nutzen, wenn es um Lösungsstrategien zur Begrenzung des sozialen Schadens von Kriminalität geht. Denn während psychologisch und soziologisch erklärbare Ursachen der Kriminalität eher langfristige Lösungsansätze aufzeigen, offeriert die ökonomische Theorie einen sehr kurzfristigen Lösungsansatz zur Begrenzung der Kriminalität: Wenn dem Verbrechen eine rationale Entscheidung vorausgeht, so kann Verbrechensbekämpfung darauf abzielen, das Ergebnis dieses Kalküls in die gewünschte Richtung – also in Richtung legalen Handelns – zu beeinflussen. Dies gelingt beispielsweise durch höhere Sicherheitsvorkehrungen und durch Abschreckung. Konkret versucht eine derartige Politik zumeist, das zu erwartende Einkommen aus einer Straftat zu verringern. Durch eine entsprechende Wahl der Abschreckungsvariablen, nämlich der Verurteilungswahrscheinlichkeit und Härte der Strafe, ist die Politik dann in der Lage, Einfluss auf die Kriminalität zu nehmen.[8] Anders als die eher langfristig Erfolg versprechenden kriminalpräventiven Maßnahmen zielt die strafrechtliche Prävention darauf ab, durch die Androhung von Strafen, Strafvollstreckung und Strafvollzug potenzielle Täter von kriminellen Handlungen abzuhalten, strafrechtliche Normen in der Gesellschaft zu bestätigen und den Täter nach begangener Tat zu resozialisieren und von weiteren Straftaten abzuschrecken. Interessant ist dabei vor allem, ob die Höhe der Strafe tatsächlich eine Abschreckungswirkung impliziert, das heißt, ob ein höheres Strafmaß für diverse kriminelle Delikte dazu führt, dass die Zahl der begangenen Straftaten zurückgeht. Wäre dies der Fall, könnte man durch höhere Strafen das Kriminalitätsniveau senken. Dieser Zusam-

7 Vgl. Heinz (2004).
8 Vgl. Entorf/Spengler (1998) und Entorf/Spengler (2000).

menhang ist deshalb auch Gegenstand zahlreicher Studien zum Thema Abschreckungswirkung der Strafverfolgung. Die Ergebnisse der Untersuchungen liefern dazu ein insgesamt differenziertes Bild. Ein Großteil der Analysen für Deutschland kommt zu dem Ergebnis, dass von einer steigenden Strafe für diverse Deliktgruppen keine zunehmende Abschreckungswirkung für potenzielle Täter und Wiederholungstäter ausgeht. Gleichwohl spielt es aber eine wichtige Rolle, dass Strafrecht und strafrechtliche Sanktionierung vorhanden sind. Würde man die strafrechtliche Sanktionierung kurzfristig aufgeben, so wäre ein deutlicher Anstieg der Kriminalität zu erwarten. Dadurch wird deutlich, dass das Strafrecht und die Sanktionierung krimineller Handlungen nicht per se wirkungslos sind, obwohl der Zusammenhang zwischen höherer Strafe und weniger registrierter Kriminalität nicht nachgewiesen werden kann.[9]

Die Bekämpfung und strafrechtliche Prävention verhindert oder begrenzt drohende Schäden kriminellen Handelns. Sie ist jedoch ebenfalls mit Kosten verbunden. Die Strategie erfordert schlagkräftige Ermittlungsbehörden, ein Rechts- und Gerichtswesen und einen Strafvollzug. Dabei ist auch zu berücksichtigen, dass die Kosten, die verurteilten Straftätern entstehen, in einer ökonomischen Betrachtung anzusetzen sind. Wenngleich es wünschenswert erscheint, dass jegliche Kriminalität verhindert würde, ist es aus freiheitlicher und ökonomischer Sicht nicht sinnvoll, Kriminalität durch überdimensionierte Sicherheitsapparate, die zwar die Aufklärungswahrscheinlichkeit erhöhen könnten, oder drakonische Strafen, die die Kosten für verurteilte Straftäter erhöhen würden, vollständig zu verhindern. Vielmehr kommt es darauf an, die Instrumente der Strafverfolgung effizient einzusetzen. Nicht zu unterschätzen ist hierbei die Rolle der gesellschaftlichen Akzeptanz von Kriminalität. Die beispielsweise nicht selten anzutreffende Akzeptanz oder Bagatellisierung von Sozialbetrug, Schwarzarbeit oder Steuerhinterziehung, die häufig als Akt der Notwehr verharmlost werden, trägt tendenziell zu einer größeren Zahl dieser Delikte bei. Eine Stärkung der Bedeutung sozialer Normen kann langfristig relativ kostengünstig zu einer Verbesserung der Kriminalitätssituation beitragen, wenn zusätzlich zur strafrechtlichen Abschreckung auch ein höherer Reputationsverlust abschreckend wirkt. Gleichzeitig gilt es, den Ursachen der Kriminalität zu Leibe zu rücken. Da beispielsweise Arbeitslosigkeit zur Kriminalität beiträgt, stellt eine Verbesserung der Arbeitsmarktchancen ein Mittel zur Kriminalitätsvermeidung dar. Angesichts des unklaren Nutzens einer Verschärfung der strafrechtlichen Sanktionen auf die Kriminalitätsentwicklung kommt den kriminalpräventiven Maßnahmen, die neben pädagogischen und psychologischen Ansätzen auch arbeitsmarkt- und sozialpolitischen Ziele verfolgen, eine wichtige Bedeutung zu.

3.1.3 Volkswirtschaftliche Kosten

Die gesellschaftlichen Kosten der Kriminalität sind nicht allumfassend messbar. Dies liegt nicht zuletzt daran, dass die Kosten zum einen häufig verdeckter Art und zum anderen schlicht, zum Beispiel mangels Anzeige, unbekannt oder selbst bei voller Kenntnis schwer quantifizierbar sind. Ein wesentliches Problem ist dabei, dass die unterschiedlichen Deliktarten zu sehr unterschiedlichen

9 Vgl. Bundesministerium des Innern, Bundesministerium der Justiz (2006), S. 665 ff.

Verurteilte Deutsche je 100 000 Einwohner der gleichen Altersgruppe, 1976–2006

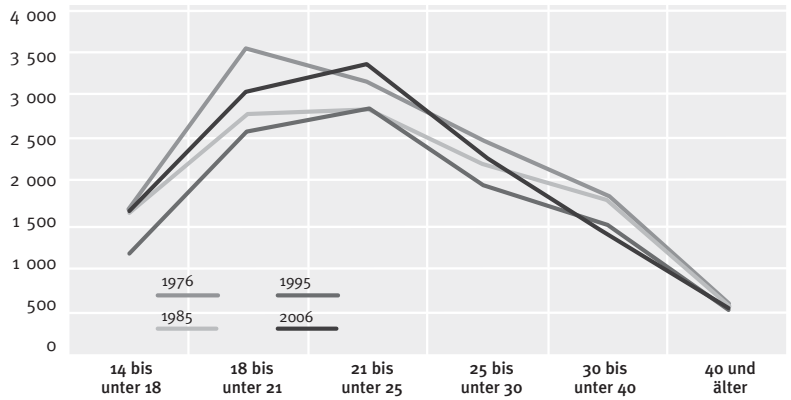

Abb. 5

Quelle: Statistisches Bundesamt (2007).

Schäden führen, die nicht immer in finanziellen Einheiten messbar sind. So lassen sich Gewaltdelikte in Kosten für die medizinische Behandlung, die kriminalistische Aufklärung, Ahndung und mögliche Verdienstausfälle des Opfers bemessen, was im Falle eines Gerichtsverfahrens in Teilen auch geschieht. Weit schwieriger können jedoch die Kosten, die dem Opfer und seinen Angehörigen durch das seelische Leid entstehen, bewertet werden.

Ferner ist es schwierig, die Folgen von Kriminalität zu bewerten, die sich zum Beispiel aus einer Verhaltensänderung ergeben und unter ökonomischen Gesichtspunkten oder im Hinblick auf die Lebensqualität substanziell sein können. Selbst bei Eigentumsdelikten, bei denen das Opfer einen relativ leicht zu bemessenden finanziellen Schaden erleidet, ist die Erfassung der gesamtwirtschaftlichen Kosten überaus schwierig. Im Falle eines Betruges oder eines Diebstahls geht der Vermögensverlust des Opfers mit einem Vermögenszuwachs des Täters einher, sodass in der volkswirtschaftlichen Betrachtung zunächst kein direkter Schaden als Folge dieses illegalen Transfers entstanden ist. Der Schaden bei Eigentumsdelikten ist tatsächlich indirekter Art. Opfer eines Diebstahls oder eines Raubes sind verunsichert oder verängstigt und ändern eventuell ihr Verhalten. Doch selbst potenzielle Opfer sind vorsichtiger, als sie es in einer Gesellschaft ohne Kriminalität wären, und unterlassen Aktivitäten und Transaktionen aus Sicherheitsgründen. Häufig beugen sie auch durch den Kauf von Sicherheitstechnik oder Sicherheitsdiensten Straftaten vor. Daraus wird ersichtlich, dass allein die Furcht vor Kriminalität bereits Kosten erzeugt. Die indirekten Kosten sind jedoch faktisch nicht messbar. Doch selbst wenn sie es wären, könnten sie schwerlich als Kosten der Kriminalität verbucht werden, da Prävention und Vorsorgeausgaben auch das Ergebnis einer falschen beziehungsweise irrationalen Wahrnehmung von Kriminalität und Gefährdung sein können. Insofern sind auch die Ausgaben des Staates für die öffentliche Sicherheit, also für Strafverfolgung und Pflege eines Gerichts- und Strafvollzugswesens, die in erheblichem Maße der Prävention und Aufrechterhaltung der gesetzlichen Ordnung dienen, allenfalls als Indikatoren für die Kosten der Kriminalität aufzufassen. Zusammengefasst lässt sich somit festhalten, dass nicht nur kriminelle H a n d l u n g e n selber gesellschaftliche Kosten hervorrufen. Auch die sinnvolle Prävention und Vorsorge seitens

des Staates und der privaten Haushalte und Unternehmen ist der Kriminalität zuzurechnen. Übertriebene Ausgaben zur Vermeidung von kriminellen Handlungen führen hingegen aufgrund eines ineffizienten Mitteleinsatzes zu zusätzlichen volkswirtschaftlichen Kosten, weil sie nicht auf einer realistischen Beurteilung der Wahrscheinlichkeit und des Ausmaßes krimineller Bedrohung basieren. Daher kommt einer an den Fakten orientierten öffentlichen Debatte über Kriminalität und einem verantwortlichen Umgang mit dem Thema in Politik und Medien eine auch unter ökonomischen Aspekten wichtige Bedeutung zu.

3.1.4 Das Sicherheitsempfinden der Bürger

Wie erläutert, ergeben sich volkswirtschaftliche Schäden nicht nur als Folge krimineller Handlungen. Bereits die Furcht vor Kriminalität führt zu Kosten. Die Einschätzung der Menschen darüber, wie sicher sie sich in einer Gesellschaft oder wie sehr sie sich von der derzeitigen Kriminalitätslage bedroht fühlen, hat zum einen Einfluss auf das Wohlbefinden der Individuen in einer Gesellschaft und zum anderen Einfluss auf die ökonomische Aktivität in einem Land. Aus Angst vor kriminellen Übergriffen kommt es zum Verzicht auf bestimmte Aktivitäten, die aus Sicht der Menschen das Risiko erhöhen, selbst Opfer zu werden. In diesem Fall entstehen Opportunitätskosten oder höhere Transaktionskosten wie Sicherheitsvorkehrungen, um sich gegen kriminelle Bedrohungen zu schützen.

Bei einer Studie im Rahmen des Eurobarometer im Auftrag der Europäischen Kommission wurden Bürger der EU-15-Mitgliedsstaaten zu drei verschiedenen Zeitpunkten zwischen 1996 und 2002 befragt, wie sicher sie sich fühlen, »wenn Sie nach Einbruch der Dunkelheit allein zu Fuß in der Gegend unterwegs sind, in der Sie wohnen«. Über die drei Befragungszeitpunkte hinweg ist ein Anstieg des Sicherheitsgefühls in Deutschland zu beobachten. Während 1996 noch 39 % »etwas« oder »sehr unsicher« waren, waren es im Jahr 2000 nur noch 34 % und 2002 33 %. Damit liegt Deutschland knapp unter dem EU-Durchschnitt von 38 % im Jahr 2002. Außerdem wurden die Bürger im Jahr 2002 gefragt, wie hoch sie das Risiko schätzen, in den nächsten zwölf Monaten selber Opfer eines Raubes zu werden. In Deutschland lag dieses Risiko mit 10 % deutlich unter dem EU-Durchschnitt von 29 %. Im EU-Vergleich bedeutet das die beste Position für Deutschland. Die Befürchtung, Opfer dieser Straftat zu werden, war in Griechenland, zugleich dem Land mit der größten Kriminalitätsfurcht, mit deutlich über 50 % am höchsten.[10]

Zu unterscheiden von dieser individuellen Kriminalitätsfurcht ist die Wahrnehmung der Kriminalität als gesellschaftliches Problem, das heißt, inwiefern Menschen die Innere Sicherheit durch Kriminalität bedroht sehen, sich Sorgen um das Gemeinwesen machen und wie sie die Relevanz der Themen Innere Sicherheit und Kriminalität als Staatsaufgabe beurteilen. Im Rahmen der jüngsten repräsentativen deutschen Befragung bezüglich der wahrgenommenen Entwicklung der polizeilich registrierten Kriminalität wurden den Teilnehmern die erfassten Zahlen aus dem Jahr 1993 für ausgewählte Deliktgruppen vorgelegt und sie aufgefordert, die allgemeine Entwicklung zu beurteilen.

10 Vgl. Zentrum für Umfragen, Methoden und Analysen (2005), S. 6 ff.

Dabei sind 91 % der Meinung, es sei zu einer Zunahme der registrierten Straftaten gekommen, während nur 2 % eine Abnahme unterstellen.[11] Auffällig ist, dass Befragte übereinstimmend in mehreren Studien den Anteil extrem schwerwiegender Delikte am gesamten Kriminalitätsaufkommen extrem überschätzen.

Die im Jahr 1998 durchgeführte Bochumer Opferbefragung bestätigt dieses Phänomen. Der relative Anteil des Mordes an allen Delikten wurde dabei um den Faktor 250, Raub um den Faktor 30 und Körperverletzung um den Faktor zwölf überschätzt. Diese Fehleinschätzung ist auf die enorme Bedeutung von schwerwiegenden Straftaten aus Sicht des Einzelnen und die steigende Medienpräsenz des Themas zurückzuführen, sodass die befragten Personen den schwerwiegenden Straftaten eine überzogene Bedeutung beimaßen und die tatsächliche Kriminalität überschätzten.

Neben der Abnahme der persönlichen Kriminalitätsfurcht, das heißt der Angst, selber Opfer einer Straftat zu werden, ist auch ein Rückgang in der Wahrnehmung der Kriminalität als gesellschaftliches Problem zu beobachten. Die seit 1994 jährlich durchgeführten Umfragen des Sozio-oekonomischen Panels (SOEP) belegen, dass sich die Menschen heute weniger kritisch über die Kriminalitätsentwicklung äußern als noch vor einigen Jahren. Während sich 1997 noch über 60 % der knapp 13 200 Befragten Sorgen um die Kriminalität in Deutschland machten, waren es 2003 nur noch 42,2 % der rund 22 500 Befragten.[12] Folglich empfinden die Menschen die Bedrohung der Gesellschaft durch Kriminalität heute als weniger drastisch als noch vor einigen Jahren. Parallel zu diesem positiven Trend, der sich bei der Einschätzung der Kriminalität als gesellschaftliche Bedrohung zeigt, ist auch in den letzten 15 Jahren eine steigende Zufriedenheit mit der öffentlichen Sicherheit und Kriminalitätsbekämpfung in Deutschland erkennbar (siehe Abbildung 6).

Bei dieser Befragung wurden die Probanden aufgefordert, auf einer Skala von null bis zehn zu beurteilen, wie zufrieden sie mit der öffentlichen Sicherheit und Kriminalitätsbekämpfung seien. So

11 Vgl. Bundesministerium des Innern, Bundesministerium der Justiz (2006), S. 492.
12 Vgl. Dittmann (2005), S. 6.

Zufriedenheit mit der öffentlichen Sicherheit in Deutschland, 1990–2001

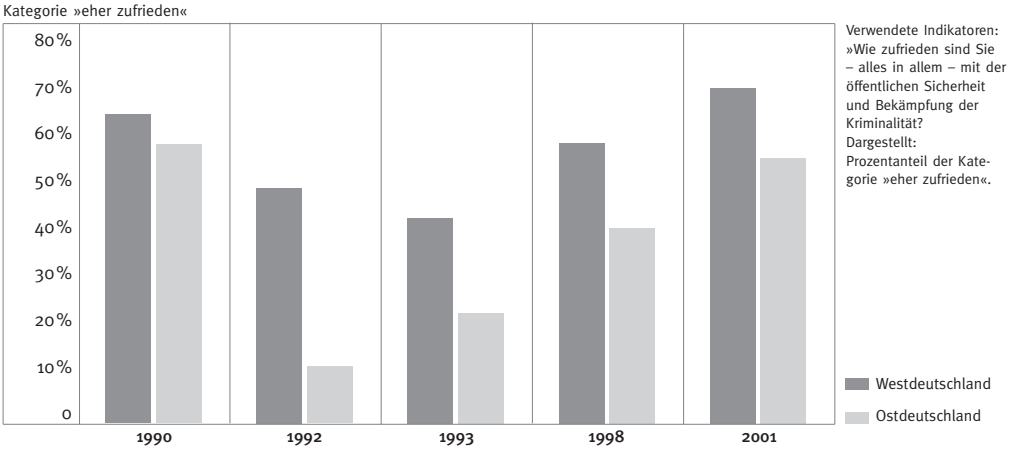

Abb. 6

Quelle: Zentrum für Umfragen, Methoden und Analysen (2001).

zeigt sich für Westdeutschland zwischen den Jahren 1990 und 1993 zunächst ein deutliches Absinken des Anteils der angegebenen Kategorie »eher zufrieden« (sechs bis zehn auf der Skala), wohingegen in den Folgejahren wieder ein deutlicher Anstieg zu beobachten ist. Während 1993 der Anteil der Zufriedenen noch bei 43 % lag, ist er bis 2001 auf 70 % angestiegen. Auch in Ostdeutschland ist ab 1993 eine deutliche Zunahme der Bürgerzufriedenheit mit der öffentlichen Sicherheit zu beobachten. Hier stieg der Anteil von 22 % im Jahr 1993 auf 55 % in 2001. Erkennbar ist aber, dass das Zufriedenheitsniveau in Westdeutschland im gesamten Zeitablauf deutlich über dem Niveau in Ostdeutschland liegt.

Bei der Suche nach Erklärungen für die Veränderungen im Sicherheitsempfinden über die Jahre hinweg ist es wichtig zu klären, inwiefern Änderungen des Sicherheitsgefühls mit der tatsächlichen beziehungsweise registrierten Entwicklung der Kriminalitätsdaten übereinstimmen. Denn es ist nicht selbstverständlich, dass das »gefühlte« und tatsächliche Niveau der Kriminalität immer übereinstimmen. Im Gegenteil, oft nehmen Menschen das Kriminalitätsrisiko als bedrohlicher wahr, als es die statistisch erfassten Zahlen rechtfertigen. Wie oben bereits geschildert, ist diese Überbewertung besonders bei schwerwiegenden Straftaten auffällig, was nicht zuletzt auf die hohe Präsenz der Schwerkriminalität in den Medien zurückzuführen ist. In Ostdeutschland ist das deutlich geringere Zufriedenheitsniveau mit der öffentlichen Sicherheit und der Kriminalitätsbekämpfung nach der Wiedervereinigung aber tatsächlich mit steigenden Kriminalitätszahlen verbunden. Dabei spielte die Umbruchsituation im Osten Deutschlands wohl eine bedeutende Rolle. In den Folgejahren nimmt in West- als auch in Ostdeutschland das persönliche Sicherheitsgefühl deutlich zu, obwohl nur in Ostdeutschland die registrierten Straftaten pro 100 000 Einwohner leicht abnehmen. Auch im europäischen Vergleich schneidet Deutschland gut ab. Für die Bürger anderer Länder, wie zum Beispiel Irland, Dänemark und die Niederlande, gehört das Thema Kriminalität zu den beiden wichtigsten Problemen ihres Landes. Was die Einschätzung betrifft, selber Opfer eines Übergriffs zu werden, liegt Deutschland europaweit im Mittelfeld. Insgesamt ist ab Mitte der 90er-Jahre in Deutschland zu beobachten, dass das Sicherheitsgefühl und die Kriminalitätsbekämpfung immer positiver wahrgenommen werden, die Menschen also weniger der Meinung sind, dass die Gesellschaft in erster Linie durch Kriminalität bedroht werde und die Bekämpfung der Kriminalität zu den relevantesten Staatsaufgaben gehöre. Warum empfinden Menschen das Thema Kriminalität immer weniger als persönliche und gesellschaftliche Bedrohung? Entsprechende Untersuchungen zu verschiedenen Lebensrisiken offenbaren, dass es offensichtlich zu einer Schwerpunktverschiebung gekommen ist. Heutzutage nehmen andere Probleme wie der Anstieg der Lebenshaltungskosten, Terrorismus und die teils individuell, teils konjunkturell bedingte Verschlechterung der Wirtschaftslage die vorderen Plätze ein. Das ist aber nicht der einzige Grund: Zumindest für die neuen Bundesländer kann man seit Mitte der 90er-Jahre tendenziell von einer Gewöhnung an die Kriminalität sprechen und allgemein von einer nachlassenden Präsenz in den Medien ausgehen. Daneben haben auch die kriminalpräventiven Maßnahmen in den letzten 15 Jahren deutlich zugenommen und das Sicherheits-

13 Vgl. Bundesministerium des Innern, Bundesministerium der Justiz (2006), S. 499ff.; Zentrum für Umfragen, Methoden und Analysen (2005), S. 6 f.

3.2 Terrorismus

3.2.1 Entwicklung und Ursachen des Terrorismus

Spätestens seit den Anschlägen auf das World Trade Center hat das Thema Terrorismus verstärkte Aufmerksamkeit erfahren. Der Begriff Terrorismus ist jedoch nicht exakt definiert.[14] Dies liegt nicht zuletzt daran, dass der Begriff Terrorismus nicht konkrete Handlungen benennt, sondern zu einem erheblichen Teil ein Werturteil darstellt und somit von der jeweiligen Perspektive abhängig ist. Je nach Betrachtung kann bei ein und demselben Konflikt im negativen Sinne von Terrorismus oder im positiven Sinne auch von Freiheitskampf die Rede sein. Unter Terrorismus wird hier jedweder gewaltsamer oder unter Androhung von Gewalt ausgetragener Konflikt verstanden, der religiös oder politisch motiviert ist und nicht als feindschaftlicher Akt zweier Staaten oder als Bürgerkrieg verstanden werden kann. Nicht selten spielt bei terroristischen Aktivitäten, im Gegensatz zur Kriminalität, Öffentlichkeitswirksamkeit eine wichtige Rolle. Beim Ansatz der Kosten des Terrorismus wird in dieser Studie lediglich auf die direkten Schäden terroristischer Akte und auf defensive Maßnahmen des Staates und der privaten Haushalte und Unternehmen im Inland abgestellt. Zwar kann und soll nicht ausgeschlossen werden, dass auch militärische Auslandsoperationen wie beispielsweise im Irak oder in Afghanistan der Bekämpfung des Terrorismus dienen, jedoch deuten die Debatten zur völkerrechtlichen Einschätzung solcher Maßnahmen an, die von einem Krieg gegen den Terror bis zum Vorwurf eines Angriffskrieges reichen, welche Grauzone hier betreten wird.

Die Erfassung terroristischer Aktivitäten weltweit wird systematisch durch die RAND Corporation und das National Memorial Institute for the Prevention of Terrorism (MIPT) geleistet. Die statistische Erfassung und Aufbereitung von terroristischen Aktivitäten ist angesichts der definitorischen Unschärfe mit Schwierigkeiten behaftet. Und auch die Erfassung staatlicher Gegenmaßnahmen und Ausgaben ist aufgrund von Abgrenzungsproblemen und angesichts der sicherheitspolitischen Brisanz mit Vorbehalten zu versehen. Wie die Daten des MIPT zeigen, ist der global zu beobachtende Terrorismus zu überwiegenden Teilen ein nationales Phänomen. Die Aktivitäten, bei denen Personen oder Sachvermögen mindestens zweier Länder involviert sind, haben lediglich einen Anteil von etwa 15 bis 20 %. Prominente Beispiele für nationalen Terror sind der Konflikt um das Baskenland, der Tschetschenien-Konflikt oder auch die Konflikte in Afghanistan und im Irak.

Die in jüngster Zeit in westlichen Staaten zu verzeichnenden Anschläge mit islamistischem Hintergrund haben den Eindruck erweckt, religiöse oder ethnische Gründe würden zu den Triebfedern des Terrors zählen. Daneben ist unter vielen wissenschaftlichen Beobachtern und Politikern die Ansicht verbreitet, ein niedriges Einkommensniveau unterstütze tendenziell das Auftreten terroristischer Aktivitäten. Neuere Studien[15] zeigen jedoch, dass das Einkommensniveau beziehungsweise religiöse oder ethnische Unterschiede nur mit Einschränkungen zur Erklärung des Terrorismus herangezogen werden können. Vielmehr kommt es hier auf eine sehr genaue Betrachtung und Differenzierung an. Insbesondere die Bedeutung des Einkommens ist kritisch zu hinterfragen.

14 Vgl. Croissant/Schwank (2006).
15 Vgl. Abadie (2006); vgl. Krueger/Maleckova (2002).

Zunächst ist allein schon die Kausalität von Einkommen und Terror unklar. Führt ein niedriges Einkommensniveau tendenziell zu mehr Terror, oder ist es der Terror, der zu geringerem Wachstum und darüber in armen Ländern zu anhaltend niedrigem Einkommen führt, oder gelten gar beide Kausalitäten, sodass ein Teufelskreis vorliegt? Darüber hinaus zeigt die tiefer gehende statistische Analyse, dass die Terrorgefahr tatsächlich nur oberflächlich betrachtet vom Einkommensniveau abhängt. Vielmehr spielt der Grad politischer Freiheit eines Landes eine wesentliche Rolle, wobei sowohl in besonders autoritären als auch in besonders freiheitlichen Regimen die Terrorgefahr relativ gering ist. Freiheitliche Staaten wie die USA und zahlreiche Staaten Westeuropas haben daher nur geringe terroristische Aktivitäten zu verzeichnen. Autoritäre Regime hingegen unterbinden Terrorismus durch Überwachung und Unterdrückung. Stattdessen ist die Gefahr in Staaten mit einem mittleren Niveau an politischen Rechten und Freiheiten besonders hoch. Dies sind häufig Staaten, die sich von einem einst autoritären Staat in Richtung eines demokratisch verfassten entwickeln. Beispiele hierfür sind Russland oder auch das Spanien der Nach-Franco-Zeit oder aktuell der Irak und Afghanistan.

Auch auf individueller Ebene finden sich kaum Anzeichen, dass die Einkommenssituation und terroristische Aktivitäten in Beziehung zueinander stehen. Die Attentäter des 11. Septembers stammten mehrheitlich aus relativ wohlhabenden Familien. Osama bin Laden entstammt gar einer der reichsten Familien des Nahen Ostens. Auch die Terroristen der Baader-Meinhof-Gruppe oder Mitglieder der Roten Brigaden oder der GAP in Italien, die vom vermögenden Verleger Feltrinelli angeführt wurde, entstammten häufig dem Bürgertum. Wissenschaftliche Studien, die die Hintergründe einer größeren Zahl von Terroristen oder Attentätern untersuchen, untermauern die These, dass zumeist gebildete und wirtschaftlich relativ gut gestellte Personen zum Terror neigen.[16]

Doch auch die Bedeutung religiöser Motive spielt für den weltweiten Terrorismus eine weniger bedeutende Rolle, als für gewöhnlich angenommen wird. Dies liegt daran, dass der weltweit zu verzeichnende Terror zu überwiegenden Teilen nationaler Art ist, sich also infolge beziehungsweise als Ausdruck innerstaatlicher Konflikte ereignet. Staatengrenzen trennen nicht selten auch Religionsgemeinschaften voneinander. Nationaler Terror impliziert daher oftmals Gewalt innerhalb religiöser Gruppen. Das muss nicht zwangsläufig heißen, dass religiöse Motive vollkommen ohne Belang sind, gleichwohl bleibt aber häufig unklar, ob Konflikte zwischen verschiedenen Gruppen der gleichen Religionsgemeinschaft und selbst zwischen Mitgliedern unterschiedlicher Religionsgemeinschaften – wie derzeit beispielsweise im Irak – tatsächlich religiös motiviert sind oder ob religiöse Konflikte lediglich zu anderen Zwecken instrumentalisiert werden. Zwar könnte man Angriffe al-Qaidas auf die westlichen, zumeist christlichen Soldaten als religiös motiviert einstufen. Wie erklärt man aber die Angriffe al-Qaidas auf irakische, meist muslimische Polizisten? Gleichwohl kann nicht ausgeschlossen werden, dass religiöse Motive in den letzten Jahren an Bedeutung gewonnen haben. Hinsichtlich ethnischer Motive lässt sich wiederum zeigen, dass sprachliche Barrieren und Differenzen sehr wohl die Terrorgefahr innerhalb eines Landes erhöhen. Neben dem Grad der politischen

16 Vgl. Krueger/Maleckova (2002).

Freiheit und sprachlichen Differenzen zeichnen sich vom Terrorismus betroffene Staaten häufig durch geografische Gegebenheiten aus. Insbesondere Gebirge und Urwälder kommen Terroristen zu Hilfe. Freilich verursacht die Existenz von Gebirgen oder Urwäldern nicht an sich Terrorismus. Da jedoch Terrorismus in der Regel mit staatlichen Gegenmaßnahmen beantwortet wird, erweisen sich die genannten geografischen Merkmale als nützlich für Terroristen. Sie bieten einerseits Schutz und Deckung vor den staatlichen Sicherheitsorganen und ermöglichen zusätzlich über den Anbau von Drogen illegale Einnahmequellen.

Abbildung 8 zeigt die Zahl der terroristischen Vorfälle in den 25 am stärksten betroffenen Ländern. Dabei ist zu beachten, dass die öffentliche Datenbank des MIPT derzeit lediglich terroristische Vorfälle von 1998 bis einschließlich 2004 erfasst. In diesem Zeitraum spielten sich die meisten terroristischen Aktivitäten im südasiatischen Bereich ab. Die Schauplätze des Terrorismus waren hier vor allem die Dreiländerecke Indien-Pakistan-Afghanistan und Philippinen-Indonesien-Thailand. Seit 2003 jedoch hat der Terror im Nahen Osten dramatisch zugenommen. Insbesondere der hohe Wert des Iraks spiegelt dieses wider, da die hier aufgeführten Terrorakte vor allem in den Jahren 2003 und 2004 stattfanden. Neuere Veröffentlichungen des MIPT legen nun offen, dass die meisten Terrorakte 2005 eindeutig im Nahen Osten und der Golfregion zu verzeichnen waren. Abbildung 7 zeigt die prozentualen Anteile der Weltregionen am Terror für die verfügbaren jüngsten Daten des Jahres 2005. Insbesondere im Bereich des nationalen Terrors ist es im Nahen Osten und der Golfregion zu einem deutlichen Anstieg des Terrors gekommen. 61 % aller nationalen Terroraktivitäten des Jahres 2005 fanden hier statt. Im ersten Quartal 2003 betrug der Anteil der Region noch lediglich 19 %.[17]

Abbildung 9 bildet die Zahl der terroristischen Aktivitäten im Zeitraum 1998–2004 nach Terrorzielen ab. Ganz deutlich zielen die meisten Anschläge auf Privatpersonen und private Besitztümer. Gleichwohl sind auch Staatsrepräsentanten, Regierungseinrichtungen und die Sicherheitsorgane häufiges Ziel terroristischer Handlungen. Dabei befinden sich diplomatische Einrichtungen eher im Mittelfeld, auch religiöse Personen und Einrichtungen sind relativ selten Ziel von Anschlägen.

17 Vgl. Brannan/Chalk/Cragin/Daly (2003).

Anteile der Weltregionen am Terror, 2005

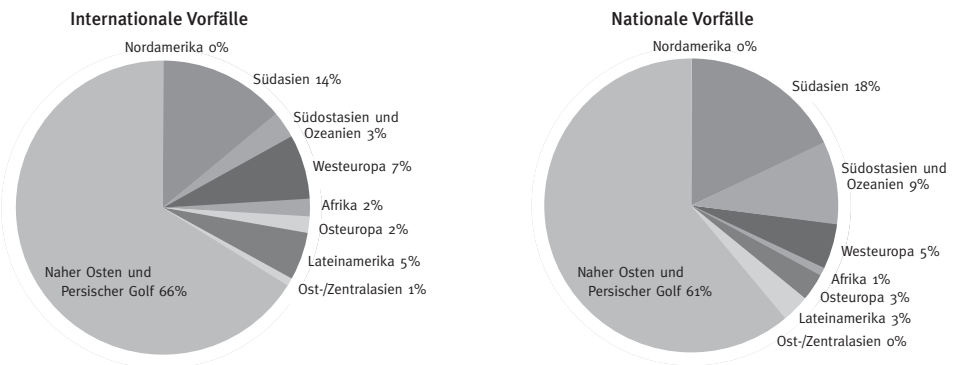

Abb. 7

Quelle: MIPT (2006).

Zahl der terroristischen Vorfälle in den 25 am meisten betroffenen Ländern, 1998–2004

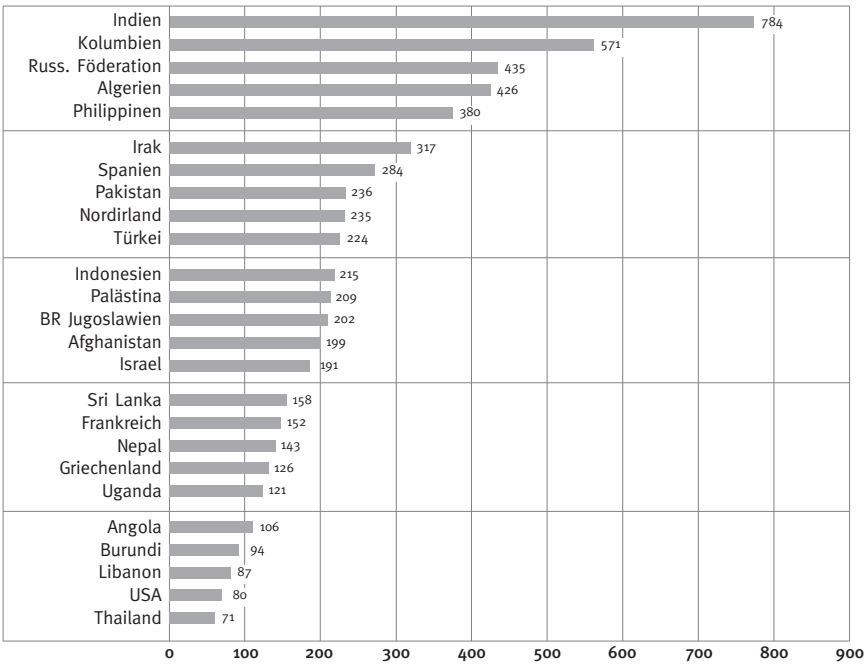

Abb. 8 Quelle: MIPT (2006).

3.2.2 Volkswirtschaftliche Kosten

Ab einer gewissen Bedrohungslage muss davon ausgegangen werden, dass Terrorismus neben individuellen Kosten auch volkswirtschaftliche Kosten verursacht. Diese Kosten sind unterschiedlicher Art. Zum einen können bei einer Vielzahl von terroristischen Attacken direkte Kosten infolge der Zerstörung wichtiger Infrastruktur oder aufgrund des Verlustes von Menschenleben auftreten. Zum anderen ergeben sich aber auch, ganz ähnlich wie bei der Kriminalität, indirekte Kosten, die in einer Lähmung der wirtschaftlichen Dynamik und damit des Wirtschaftswachstums zum Ausdruck kommen. Beispielsweise wurden die direkten Schäden, die sich infolge der Anschläge des 11. Septembers in New York ergaben, auf rund 0,35 % des US-amerikanischen BIP beziffert. Gesamtwirtschaftlich betrugen die Kosten in Folge der Krise noch im gleichen Jahr schätzungsweise 0,75 % des amerikanischen BIPs. Auch weltweit ergaben sich erhebliche Kosten.

Schließlich entstehen auch durch präventive Maßnahmen direkte und indirekte Kosten. Von größerer Bedeutung sind die indirekten Kosten, die sich als Folge von Unsicherheit und damit einhergehenden Verhaltensänderungen der Wirtschaftsakteure ergeben. Hierzu zählen beispielsweise Kursverluste auf den Finanzmärkten infolge von Unsicherheit oder veränderten Standortbewertungen. Ganz allgemein führt eine höhere Unsicherheit auf den globalisierten Finanzmärkten dazu,

Zahl der terroristischen Vorfälle nach Art des Ziels, 1998–2004

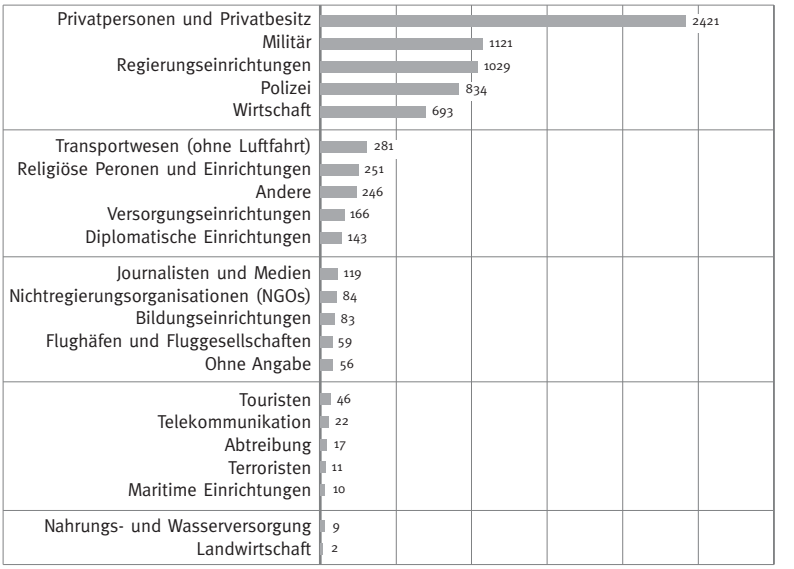

Abb. 9

Quelle: MIPT (2006).

dass weniger Kapital ins Inland fließt beziehungsweise Kapital tendenziell in andere Länder abfließt. Damit steht jedoch weniger Kapital für die Produktion zur Verfügung, sodass das Einkommen permanent sinkt. Wollte das vom Terror bedrohte Land diesen Nettokapitalabfluss abwenden, müsste es über den internationalen Kapitalmarktzins hinaus eine Risikoprämie an die Kapitalgeber zahlen. Aktuelle Studien[18] belegen derartige Reaktionen der Kapitalmärkte auf Terror für ausländische Direktinvestitionen. Doch nicht nur die Reaktion auf den Kapitalmärkten senkt die Produktion. Ganz allgemein sorgt eine höhere Unsicherheit für schlechtere Zukunftserwartungen und diesbezüglich geringere Konsumausgaben oder auch eingeschränkte Unternehmensaktivitäten. Die Kosten, die sich aus diesen direkten wie indirekten Konsequenzen des Terrors ergeben, sind beträchtlich. Tabelle 1 listet exemplarisch die Kosten für unterschiedliche Länder und unterschiedliche Konflikte auf.

Die hier dargestellten Schätzungen zeigen für unterschiedliche Länder durchschnittlich jährliche Kosten von 0,5 bis 2 % des jeweiligen Bruttoinlandsproduktes. Für die Region des Baskenlandes schätzten Abadie und Gardezabal für den Zeitraum 1980 bis 2000 Kosten in Höhe von 10 % des Bruttoinlandsproduktes. Das BIP im Jahr 2000 wäre also ohne Terror 10 % höher ausgefallen.[19]

18 Abadie/Gardezabal (2007).
19 Abadie/Gardezabal (2003).

Terroristische Konflikte und volkswirtschaftliche Kosten

Land	Konflikt	Zeitraum	Kosten in % des BIP
USA	9/11	2001	0,75
Welt	9/11	2002	1
Baskenland	ETA	1980–2000	10
Israel	Intifada	2000–2001	4

Tab. 1

Quellen: Abadie/Gardezabal (2003); Nanto (2004); IMF(2001); Weltbank (2002).

Die wirtschaftlichen Folgen der Anschläge vom 11. September

Die Anschläge des 11. Septembers und insbesondere die Zerstörung der zwei Türme des World Trade Centers dürften sich wie nur wenige Ereignisse in das Bewusstsein eingebrannt haben. Tatsächlich stellen die Angriffe auf die Hochhäuser, die 2 774 Menschen das Leben kosteten, gemessen an der Zahl der Opfer, den bisher bei Weitem größten Terroranschlag dar. Auch finanziell ergaben sich auf unterschiedlichen Ebenen hohe Kosten. Der Verlust von Menschen bedeutete auch wirtschaftlich einen Verlust, der anhand der zu erwartenden Lebenseinkommen der Verstorbenen geschätzt werden kann. Zu diesen fast acht Milliarden US-Dollar müssen zudem Einkommensrückgänge für Überlebende und sonstige Betroffene in den umliegenden Gebäuden oder mittelbar betroffenen Geschäftsbereichen addiert werden, die sich auf 3,6 bis 6,4 Milliarden US-Dollar belaufen. Schließlich fielen für die zerstörten Türme und die Aufräumarbeiten am Ground Zero, Reparaturen an umliegenden Gebäuden und der Infrastruktur weitere 21,6 Milliarden US-Dollar an, sodass die direkten finanziellen Konsequenzen zwischen 33 und 36 Milliarden US-Dollar rangieren.[20]

Dies entsprach in etwa einem drittel Prozent des US-amerikanischen Bruttoinlandsproduktes 2001. Neben der Verunsicherung der Bürger und verschiedenen Unannehmlichkeiten, wie zum Beispiel den deutlich verstärkten Sicherheitsmaßnahmen an den US-Grenzen, ergaben sich auch für die gesamte amerikanische Volkswirtschaft substanzielle Kosten. Auch wenn eine exakte Zurechnung der Terroranschläge auf die US-Konjunktur angesichts anderer konjunktureller Einflussfaktoren schwerlich vorgenommen werden kann, muss für die USA von nicht unerheblichen Konsequenzen ausgegangen werden. Nach Schätzungen des Internationalen Währungsfonds (IMF) betrugen die Gesamtkosten für die USA im Jahr 2001 etwa 0,75 % des BIP. Damit würden die indirekten Kosten bereits im Jahr des Anschlages die direkten Kosten übertroffen haben. Zudem setzten die Anschläge Schockwellen frei, die weltweit Wirkung zeigten. Die ohnehin aufgrund der Dot-com-Blase gefährdeten Finanzmärkte gerieten in Schwierigkeiten, und eine Rezession der Weltwirtschaft folgte. Global wurden die makroökonomischen Effekte, die aufgrund des geringeren Wirtschaftswachstums und der geringeren internationalen Handelsaktivitäten eintraten, für das Folgejahr 2002 von Beobachtern in der Spitze auf bis zu 1 % des Welt-BIP geschätzt. Dies entsprach 2002 rund 300 Milliarden US-Dollar.[21]

Kasten 2

20 Vgl. Bram/Orr/Rapaport (2002).
21 Vgl. Nanto (2004).

Der ISPS-Code zur Sicherung der Häfen

Die Zunahme der internationalen Warenströme im Rahmen der Globalisierung bringt auch erhöhte Sicherheitsrisiken mit sich. Dabei stellen insbesondere die Häfen, die die Schnittstellen des internationalen Warenaustausches darstellen, die Sicherheitsbehörden vor große Herausforderungen. Neben dem Schmuggel haben in jüngster Vergangenheit auch Menschenschmuggel und vor allem die Gefahr terroristischer Anschläge an Bedeutung gewonnen. Zur Sicherung der Häfen wurde daher der International Ship and Port Facility Code (ISPS-Code) weltweit eingeführt. Er gilt für Häfen und die sie anlaufenden Schiffe und beinhaltet eine Reihe von Sicherheitsvorschriften, die terroristische Aktivitäten erschweren sollen. So sind die Hafenanlagen eingezäunt und dürfen nur nach erfolgter Personenkontrolle betreten werden. Schiffszugänge werden nach Anlegen durch Posten gesichert, und es finden Prüfungen der Spediteure und Zulieferer statt. Die Herstellung von Sicherheit bleibt jedoch angesichts der gewaltigen Volumina der in den Häfen umgeschlagenen Waren auch mit dem ISPS-Code eine große Aufgabe. Allein in Hamburg, dem größten Hafen Deutschlands, wurden 2007 knapp zehn Mio. Containerstandardeinheiten (TEU) umgeschlagen.

Kasten 3

3.3 IT-Sicherheit

3.3.1 Gefährdung von Daten

Die elektronische Datenverarbeitung hat über die letzten drei Jahrzehnte immer weiter an Bedeutung gewonnen. Dabei waren die 1980er-Jahre durch die Dezentralisierung der Datenverarbeitung geprägt: Großrechner wurden durch flexible Personalcomputer ersetzt. Mit Beginn der 1990er-Jahre wurde die Entwicklung der Informationstechnologie durch die Vernetzung der Computer über das Internet bestimmt. Im letzten Jahrzehnt haben dann die drahtlose Vernetzung der Computer untereinander sowie mit mobilen Endgeräten, wie Handys und PDAs (Personal Digital Assistants), und die interaktive Nutzung des Internets die Entwicklung bestimmt. Mit diesen Entwicklungen hat die Datenverarbeitung stetig an Bedeutung gewonnen. Inzwischen hat sie im Sinne einer echten Querschnittstechnologie alle Lebens- und Wirtschaftsbereiche erfasst. So sind Versorgungsbetriebe der Elektrizitäts-, Gas- und Wasserwirtschaft ebenso wie Industriebetriebe und die Unternehmen aus Dienstleistungen und Verwaltung auf die Informations- und Kommunikationstechnik angewiesen.

Besonders offensichtlich ist die Bedeutung der Informationstechnologie bei den Versorgungsunternehmen. Ein Ausfall der Strom-, Gas- oder Wasserversorgung legt Haushalte und Industrieunternehmen lahm. Darüber hinaus könnte auch der gesamte Bereich der Infrastruktur zusammen-

Ranking über die verschiedenen Gefahrenquellen von Daten, 2004/2005

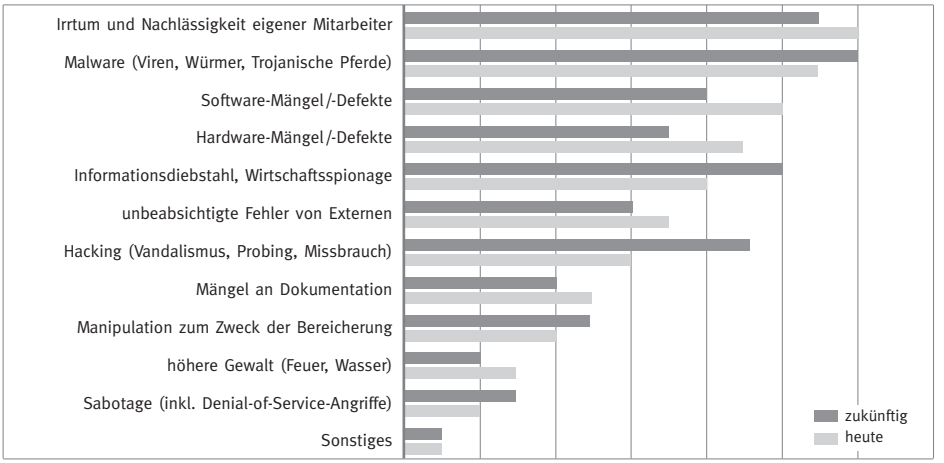

Abb. 10

Quelle: KES (2006).

brechen. Bei immer weiteren Netzen können sowohl Produktionsspitzen als auch der Ausfall von einzelnen Kraftwerken sofortige Reaktionen bei anderen Kraftwerken erforderlich machen. Fehlende oder zu langsame Reaktionen können Netzausfälle vergleichbar mit denen in den USA oder in Nordrhein-Westfalen verursachen. 50 Millionen Menschen waren betroffen, als im Nordosten der USA und Kanada der Strom am 14. August 2003 für mehrere Tage ausfiel. Dadurch entstanden Kosten von 6 Mrd. US-Dollar.[22] In Nordrhein-Westfalen fiel im Herbst 2005 der Strom für 250 000 Haushalte bis zu vier Tage aus. Die Kosten dieses Ausfalls lagen bei 100 Mio. Euro.[23]

In Industrieunternehmen wird sowohl die Produktion als auch die Distribution und Lagerhaltung elektronisch gesteuert. Dabei hat in den letzten Jahrzehnten die Arbeitsteilung zwischen Unternehmen – national wie auch international – stark zugenommen. Die genaue Abstimmung von Produktions- und Lieferungsprozessen erlaubt es, die Lagerhaltung zwischen Produktionsstufen und auch zwischen Produktion und Endabnahme auf ein Minimum zu reduzieren. Diese Just-in-time-Produktion ist ausgesprochen kostensparend, verursacht jedoch erhebliche Probleme, sofern Fehler bei der Abstimmung zwischen den Produktionsstufen entstehen. Der nahtlosen korrekten Datenverarbeitung kommt dabei eine erhebliche Bedeutung zu.

Sowohl die öffentliche Verwaltung als auch die privaten Dienstleistungen wären ohne elektronische Datenverarbeitung nicht mehr funktionsfähig. Besonders deutlich wird dies bei Banken und Versicherungen. Konten werden nicht mehr manuell geführt, sondern liegen nur noch elektronisch vor. Deshalb würde ein Ausfall des elektronischen Zahlungsverkehrs das gesamte Wirtschaftsleben lahmlegen. Folgerichtig gehört die Informations- und Kommunikationstechnik der Banken ebenso wie die der Versorger in den Bereich der Kritischen Infrastruktur, für die das Bundesamt für Sicherheit in der Informationstechnik (BSI) besondere Richtlinien herausgibt.

22 Vgl. U.S.-Canada Power System Outage Task Force (2004).
23 Vgl. Deutscher Wetterdienst (2005).
24 Vgl. X-Force (2007).

Mit der steigenden Bedeutung der Datenverarbeitung hat auch die Datensicherheit in den letzten Jahren immer mehr an Bedeutung gewonnen. Dabei werden die Daten durch Fehler der Nutzer, durch Fehler von Soft- und Hardware und auch durch Angriffe von außen gefährdet. Abbildung 10 zeigt das Ergebnis einer Befragung von 135 Unternehmen zur Bedeutung der einzelnen Risikofaktoren für die Datensicherheit. Derzeit sehen die Unternehmen ihre Daten vor allem durch Fehler von Mitarbeitern gefährdet. Erst an zweiter Stelle steht Schad-Software. Es wird allerdings erwartet, dass sich diese Reihenfolge zukünftig ändert. So ist davon auszugehen, dass Hacking und die bewusste Manipulation von IT-Systemen zukünftig in ihrer Bedeutung steigen werden. Dafür nimmt die Bedeutung von Fehlern durch externe Benutzer, Software oder Dokumentation ab.

3.3.2 Schwachstellen und Bedrohungen von IT-Systemen

In Softwareprodukten kommen regelmäßig Fehler vor, die zu Sicherheitslücken führen und es externen Nutzern erlauben, den Computer anzugreifen. Im Jahr 2006 entdeckte ein Sicherheitsunternehmen 7 247 neue Schwachstellen.[24] Über die Hälfte dieser Schwachstellen erlaubte den Angreifern, Benutzer- oder Administratoren-Rechte auf dem Computer zu erlangen. Nach Angaben des Bundesamts für Sicherheit in der Informationstechnik benötigen Hacker durchschnittlich nur noch drei Tage, um ein Programm zur Ausnutzung der Sicherheitslücken (Exploit) zu erstellen. Eine mögliche Begründung für den starken Anstieg bei der Ausnutzung von Sicherheitslücken liegt darin, dass Cyber-Kriminalität große Gewinne ermöglicht.[25]

Die häufigste Form der Angriffe gegen IT-Systeme bilden Computerschadensprogramme. Diese werden meist über E-Mail-Anhänge verschickt oder werden über Webseiten verbreitet. Bis vor einigen Jahren waren Viren die häufigste Form der Schadensprogramme. Entsprechend den Angaben des BSI 2007 haben heute jedoch Trojanische Pferde mit einem Anteil von 56 % und Würmer mit 34 % eine deutlich größere Bedeutung als Viren mit 10 %. Zum Teil dient die Schad-Software zerstörerischen Zwecken, zunehmend jedoch dem Ausspionieren des Rechners. So werden E-Mails mitgelesen und Tastatureingaben überwacht. Kennworte und Benutzernamen können dann über das Internet an die Angreifer übermittelt werden. Die gewonnenen Informationen werden dann entweder für kriminelle Aktivitäten oder aber auch »nur« für gezielte Werbeeinblendungen genutzt.

Ein weiteres Ziel der Angriffe auf einzelne Computer sind auch größere Attacken auf IT-Systeme. So werden mithilfe von Schadensprogrammen Rechner zu Bot-Netzen (Kurzform von Robot) zusammengeschlossen, um diese für weitere Aktivitäten wie den Versand von unerwünschten E-Mails oder zu DoS-Angriffen zu missbrauchen. Bei DoS-Angriffen (Denial-of-service-Angriffen) wird versucht, ein IT-System lahmzulegen. Häufig wird dieses dazu mit unnützen Daten überschwemmt. Ziele solcher Attacken sind insbesondere die Online-Angebote großer Unternehmen. E-Mails sind inzwischen ein zentrales Kommunikationsinstrument in und zwischen Unternehmen geworden. Unerwünschte E-Mails (Spam) verursachen unnötige Netz- und Serverbelastungen und führen zum Arbeitszeitausfall. Da diese Nachrichten inzwischen einen Anteil von

25 Vgl. Bundesamt für Sicherheit in der Informationstechnik (2007).
26 Vgl. Symantec (2008).

über 70 % am Gesamtaufkommen der E-Mails haben,[26] werden in der Regel Filter eingesetzt, um die Flut des Spams zu reduzieren. Dennoch berichten etwa 10 % von Firmen und Organisationen 2006, dass sie keine Spam-Filter einsetzen.[27] Da diese Filter nicht mit absoluter Sicherheit funktionieren und zum Teil auch erwünschte Nachrichten herausfiltern, erhöht der Spam die Unsicherheit in der Kommunikation und verursacht damit indirekt Kosten, die weit über die direkten hinausgehen können.

Mit der Bedeutung der vernetzten Datenverarbeitung ist es zunehmend notwendig, sich elektronisch zu identifizieren. Die dazu notwendigen Benutzernamen und Passwörter bieten die Gewähr, dass Fremde nicht auf eigene Daten zugreifen können. Dies ist natürlich besonders relevant, wenn es sich um sensible Daten wie Bankverbindungen oder Online-Bezahlsysteme handelt. Die KES-Befragung zeigt, dass bei den 154 befragten Firmen Verlust oder Diebstahl mobiler Systeme oder Einbrüche die häufigste Ursache von unbefugtem Datenzugriff sind. Nur ein kleiner Teil der Unternehmen war sich sicher, durch Phishing (Password Harvest Fishing) über Online-Angriffe unbefugt Zugriffe erfahren zu haben. Allerdings waren sich fast 60 % über diese Tatsache nicht sicher. Hier zeigen sich große Unsicherheiten, die bezüglich der Netzwerksicherheit bestehen. Dies hat zur Folge, dass Gegenmaßnahmen getroffen werden und dass bestimmte Anwendungen vermieden werden.

In der Vergangenheit fand Phishing im Wesentlichen über gefälschte E-Mails statt. In diesen wurden die Empfänger aufgefordert, ebenfalls gefälschte Webseiten zu besuchen und dort Daten über Identität und Bankverbindungen abzugeben. Obwohl die gefälschten E-Mails und Webseiten immer professioneller werden, hat die Zahl der erfolgreichen Betrugsfälle in dieser Form abgenommen. Hier zeigt sich die Wirkung von diversen Aufklärungsmaßnahmen von Banken, Behörden und Medien. Nach Angaben von Banken sind von den im Jahr 2006 eingetretenen Schadensfällen nur noch 10 % auf E-Mail-Betrugsfälle zurückzuführen. 90 % der Fälle wurden durch Trojaner verursacht.

Als direkte Kosten für IT-Sicherheit werden im Folgenden die Kosten durch Schäden und durch Sicherheitsmaßnahmen verstanden. Betrachtet werden zunächst die Kosten durch Schäden. Für ihre Abschätzung wird die Unternehmensbefragung von KES herangezogen.[28] Ähnliche Daten finden sich für Großbritannien in BERR.[29] Von den in KES befragten Unternehmen berichten 78 %, dass in ihrem Unternehmen mindestens ein Angriff durch Schadsoftware pro Jahr erfolgt. Die durchschnittliche Zahl von Infektionen lag bei 38 und, sofern um einen Ausreißer (mit mehr als 1 000 Infektionen) bereinigt wird, noch bei 28 Infektionen. Die Kosten einer durchschnittlichen Infektion wurden auf 18 000 Euro geschätzt. Entsprechend ergeben sich durchschnittliche Kosten durch Infektionen von Schadensprogrammen von 684 000 Euro. Der durchschnittliche Umsatz der befragten Unternehmen lag bei 2,6 Mrd. Euro. Damit betrug der Schaden, bezogen auf den Umsatz, im Durchschnitt nur 0,03 %. Für einzelne Unternehmen hat die Schadensumme jedoch erhebliche Ausmaße angenommen. Darüber hinaus müssen die Kosten zur Verhinderung von Schäden

27 Vgl. Bundesamt für Sicherheit in der Informationstechnik (2007).
28 KES (2006).
29 BERR Department for Business Enterprise & Regulatory Reform (2008).

Ursache und Häufigkeit von Entwendungen vertraulicher Daten, 2004/2005

Unbefugter Zugriff durch	Sicher ja	Vermutlich ja	Vermutlich nein	Sicher nein
Verlust oder Diebstahl mobiler Systeme	27%	9%	18%	46%
Einbruch in Gelände	17%	1%	18%	64%
Missbrauch/Weitergabe durch Berechtigte	3%	15%	66%	16%
Verlust oder Diebstahl von Speichermedien	7%	5%	32%	56%
Abhören von Kommunikation	1%	8%	76%	15%
Online-Angriff (Hacking, Systemeinbruch)	2%	4%	59%	34%
Sonstiger Weg	2%	1%	11%	5%

Tab. 2 Quelle: KES (2006).

Schwarzmarktpreise illegaler Informationen, 2007

Güter und Dienstleistungen	Prozentsatz	Preisspanne
Bankkonten	22%	10–1000 US-Dollar
Kreditkarten	13%	0,40–20 US-Dollar
Identitäten	9%	1–15 US-Dollar
Online-Auktionskonto	7%	1–8 US-Dollar
Betrügerische Webseiten	7%	2,50–50 US-Dollar je Woche für Bereitstellung
		25 US-Dollar für Entwurf
Mailer	6%	1–10 US-Dollar
E-Mail-Adresse	5%	0,83–10 US-Dollar je MB
E-Mail-Passwort	5%	4–30 US-Dollar
Zugriffe auf Bestellsysteme	5%	10 % – 50 % der Internet-Bestellungen
Server-Zugänge	5%	1,50–30 US-Dollar

Tab. 3 Quelle: Symantec (2008).

berücksichtigt werden. Die befragten Unternehmen beschäftigten durchschnittlich etwa 4 000 Mitarbeiter. Von diesen waren etwas unter 10 % im IT-Bereich tätig. Von IT-Mitarbeitern haben sich zwischen 2 und 15 % mit der Sicherheit von Information beschäftigt. Die Ausgaben für Informationssicherheit dürften somit zwischen 0,2 und 0,5 % des Umsatzes liegen.

Vieles spricht dafür, dass die kriminellen Aktivitäten im Cybernetz künftig zunehmen werden. Schon heute hat der Schwarzmarkt ein erhebliches Ausmaß angenommen. Tabelle 3 zeigt die Schwarzmarktpreise für illegal erworbene Daten. Nach Schätzung von Gartner lag die Zahl der Phishing-Attacken in den USA im Jahr 2007 bei 3,6 Mio. In 3,3 % der Fälle führten diese Attacken zu Schäden und verursachten einen Schaden von 3,6 Mrd. US-Dollar.[30]

Für die zukünftige Entwicklung stellt sich die Frage, wer an welcher Stelle und in welchem Umfang in Maßnahmen zur Datensicherheit investiert. Dabei müssen kontinuierlich Investitionen

30 Vgl. PC-WELT (2007).

vorgenommen werden, da auch das Angriffspotenzial stetig steigt. Ökonomische Erwägungen zeigen, dass die Investitionen in Datensicherheit in der Tendenz zu gering ausfallen. Jeder Nutzer wägt zur Bestimmung seiner optimalen Investitionen in Datensicherheit die Kosten dieser Investition gegen deren Nutzen ab. Dabei besteht der Nutzen in einer Reduktion des Risikos von Datenverlusten und der damit verbundenen Kosten. Der gesellschaftliche Nutzen der Investition geht aber über den individuellen Nutzen hinaus. Indem man sich vor Schadensprogrammen schützt, verhindert man auch deren Weiterverbreitung über den eigenen Rechner, und man vermindert die Anreize zur Erstellung solcher Programme. Die Nichtberücksichtigung dieses externen Nutzens aus den Sicherheitsmaßnahmen führt insgesamt zu geringen Sicherheitsausgaben. In anderen Sicherheitsbereichen finden in solchen Fällen staatliche Maßnahmen statt. Diese können entweder in Vorschriften für die Individuen bestehen oder aber in direkten staatlichen Sicherheitsmaßnahmen. Da das Internet grenzenlos ist, haben nationale Staaten hier nicht die Möglichkeit, regelnd einzugreifen. Insofern fehlt hier die Koordinationsfunktion. Es stellt sich die Frage, ob andere Institutionen bereit und in der Lage sein könnten, diese Funktion zu übernehmen. Die einzige Möglichkeit scheinen dabei die Netzbetreiber zu sein.

Potenziell könnten diese Maßnahmen von den Netzbetreibern oder von den Anwendern durchgeführt werden. Da bei der derzeitigen Organisation des Internets die Netzbetreiber nicht für Inhalte verantwortlich sind, übernehmen sie auch keine Haftung. Die Anreize, in Datensicherheit zu investieren, ergeben sich aus der Frage, wer im Fall von Schäden für diese haftet. Anderson führte einen internationalen Vergleich von Betrugsfällen bei Geldautomaten durch.[31] In den USA müssen im Zweifelsfall die Banken den Fehler des Kunden nachweisen. Im Gegensatz dazu müssen in den Niederlanden und in Großbritannien die Kunden nachweisen, dass der Fehler nicht von ihnen zu verantworten ist. Als Folge dieser unterschiedlichen Nachweispflichten gab es in den USA eine sehr viel geringere Zahl von Betrugsfällen bei Geldautomaten und dies, obwohl die Sicherheitsausgaben deutlich geringer waren.

Häufig sind Sicherheitslücken in der Software die Ursache für mögliche Angriffe im Netz. Auch hier sind die Konsequenzen von Fehlern nicht von den Software-Firmen als deren Urhebern zu tragen. Anderson spricht von der Microsoft-Philosophie »we'll ship on Tuesday and get it right by version 3«. Er argumentiert, dass diese Philosophie aufgrund von Netzwerkeffekten entsteht. Diese machen es sinnvoll, der Erste am Markt zu sein, um damit Standards zu setzen. Dabei führen Sicherheitsmaßnahmen zu Verzögerungen und machen zugleich die Programmierung von Anwendungen für die Systeme komplexer. Gerade die schnelle Entwicklung von Anwendungen ist aber notwendig, um zum Standard zu werden. Eine weitere Ursache für relativ schwache Sicherheitssysteme ist, dass diese zur Produktdifferenzierung missbraucht werden. So werden einfache Varianten ohne Sicherheitsstandards ausgeliefert, obwohl professionelle Varianten mit Sicherheitsstandards vorhanden sind. Da die Grenzkosten für beide Produktvarianten gleich sind, dient der höhere Preis ausschließlich der Produktdifferenzierung.

31 Anderson (2001).

4. Trends

4.1 Kriminalität

Wie die bisherigen Ausführungen gezeigt haben, sind die Hintergründe und Ursachen für Kriminalität sehr vielfältig. Ob zukünftig mehr oder weniger Kriminalität beziehungsweise eine Verschiebung der Bedeutung einzelner Deliktarten zu erwarten sind und wie sich insgesamt die Kosten für die Gesellschaft entwickeln, hängt somit von einer Reihe von Faktoren ab: von der demografischen und wirtschaftlichen Entwicklung, aber auch von der zukünftigen Bedeutung der sozialen Normen und nicht zuletzt von der Entwicklung der Aufklärungsraten und der Entwicklung des Strafrechts sowie der öffentlichen Wahrnehmung. Zu den gesellschaftlichen Rahmenbedingungen, deren Entwicklung sich relativ gut vorhersehen lässt, zählt die demografische Entwicklung. In den kommenden Jahrzehnten wird die Bevölkerungszahl abnehmen und gleichzeitig der Anteil Älterer zunehmen. Wie beschrieben, sind die Kriminalitätsraten der Altersgruppen im Zeitablauf relativ robust. Angesichts der zukünftig geringeren Bedeutung der stärker kriminalitätsbelasteten jüngeren Altersgruppen dürfte daher, rein demografisch betrachtet, die Kriminalität pro Kopf im Jahr 2030 insgesamt geringer als gegenwärtig ausfallen. Außerdem könnte der veränderte Altersaufbau der Gesellschaft zu einer anderen Struktur der Delikte führen. So stammen beispielsweise die Täter im Bereich der Drogendelikte oder bei kleineren Diebstählen vornehmlich aus jüngeren Altersgruppen. Mit zunehmendem Alter nimmt hingegen das Spektrum der Delikte zu, sodass aufgrund der zukünftig steigenden Bedeutung älterer Altersgruppen für die Gesamtkriminalität für einzelne Deliktarten wie Betrug oder Fälschung, die eher von Älteren begangen werden, auch Zunahmen beobachtet werden könnten.

Gleichwohl greift eine Betrachtung der demografischen Entwicklung als alleinerklärende Variable für Kriminalität zu kurz. Wie gezeigt, sind andere ökonomische Größen wie die Einkommensentwicklung (Einkommenshöhe und Ungleichverteilung) und die Arbeitslosenquote ebenso von Bedeutung. Wie im Kapitel 3.1 diskutiert, steigen mit zunehmender Ungleichheit die Anreize zur Kriminalität. Deshalb ist es interessant, die Häufigkeit von kriminellen Handlungen zwischen Ländern mit unterschiedlichen Einkommensverteilungen zu vergleichen. Dabei ergibt sich das Problem, dass kriminelle Handlungen in den verschiedenen Ländern unterschiedlich definiert sind und deshalb auch unterschiedlich erfasst werden. Deshalb unterscheiden sich Kriminalitätsstatistiken von Land zu Land sehr stark. Am ehesten vergleichbar sind Tötungsdelikte, da ihnen ein ziemlich eindeutiges Kriterium zugrunde liegt. Abbildung 11 zeigt den Zusammenhang zwischen dem Gini-Index, als Maß für die Ungleichheit in einem Land, und der Zahl der Tötungsdelikte für einen Querschnitt von 54 Ländern. Ein Indexwert von 0 zeigt eine totale Gleichverteilung, ein Wert von 100 eine totale Ungleichverteilung des Einkommens an. Dabei wird der positive Zusammenhang zwischen Einkommensungleichheit und der Zahl der Tötungsdelikte deutlich.

Derzeit ist Deutschland ein Land mit einer im internationalen Vergleich relativ hohen Gleichverteilung des Einkommens.[32] Sollten die im Zuge der Globalisierungs- und Internationalisierungs-

32 Vgl. United Nations Development Programme (2007).

Gini-Koeffizient verschiedener Länder gegen die Anzahl der Tötungsdelikte

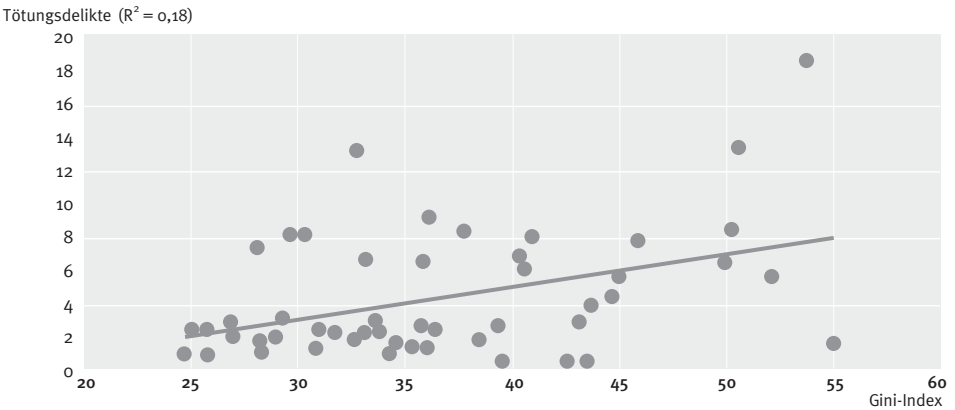

Abb. 11

Quelle: United Nations Development Programme (2003); United Nations Office of Drugs and Crime (2004).

Urbanisierung der Weltbevölkerung, 2007–2050

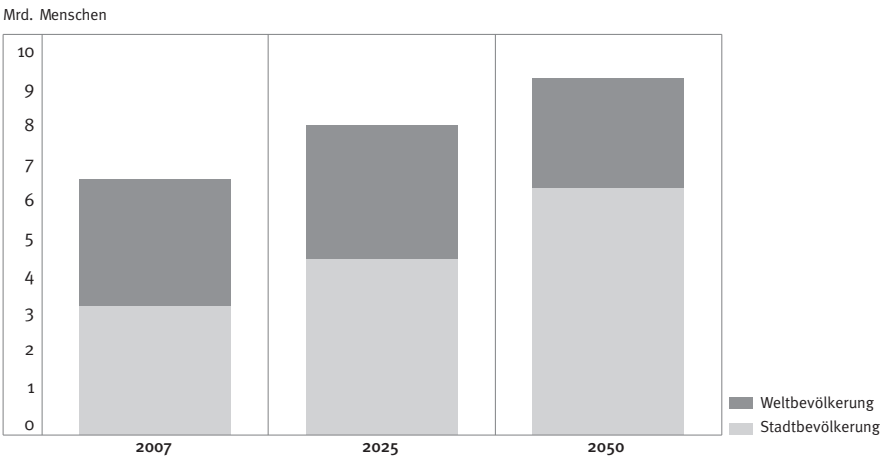

Abb. 12

Quelle: World Urbanization Projects (2007).

prozesse der Wirtschaft bestehenden Tendenzen zu einer größeren Ungleichverteilung des Einkommens beziehungsweise zu einer Teilung der Gesellschaft in Globalisierungsgewinner und -verlierer auch zukünftig anhalten, drohen infolge der Einkommensspreizung und der drohenden Arbeitslosigkeit einzelner Teile der Gesellschaft höhere Anreize für Kriminalität. Im Allgemeinen ist die Kriminalität in großen Städten höher als in sehr kleinen Städten oder auf dem Land. Abbildung 12 zeigt die UN-Prognose zur Bevölkerungsentwicklung und Urbanisie-rung. Es wird deutlich, dass die Urbanisierung in den kommenden Jahrzehnten weiter voranschreiten wird. Aufgrund der höheren Kriminalitätsraten in Städten könnte dies zu mehr Kriminalität führen.

4.2 Terror

Mit den Anschlägen des 11. Septembers und den folgenden Anschlägen in London und Madrid hat der internationale Terrorismus eine für die westlichen Staaten neue Dimension und Form angenommen. Wie es scheint, ist Terrorismus ein bisher noch unzureichend verstandenes Phänomen. Bisherige Erklärungsansätze wie wirtschaftliche Unterentwicklung oder religiöse Motive können, wie neue Studien zeigen, nur begrenzt die terroristischen Aktivitäten erklären. Auch die zukünftige Entwicklung ist daher höchst ungewiss.

Da durch Terror in erheblichem Maße immaterielle Risiken, insbesondere der Verlust von Menschenleben, auf dem Spiel stehen, kommt der Prävention eine besondere Bedeutung zu. Diese wird jedoch dadurch erschwert, dass die Ursachen unzureichend verstanden werden und die Verhaltensmuster der Terroristen und Terrororganisationen höchst unterschiedlich und unkonventionell ausfallen, sodass einheitliche Handlungsrichtlinien in der Regel nicht weiterhelfen. Zwar bleiben konventionelle Gegenmaßnahmen, wie die Zerschlagung der Finanzierungsquellen des Terrors, ein probates Mittel, gleichzeitig zeigen aber die Anschläge in Madrid und London, dass auch mit vergleichsweise geringen finanziellen Mitteln terroristische Aktivitäten möglich sind. Angesichts dieser neuen Bedrohungslage wird vonseiten der Sicherheitsexperten eine neue Art der Kooperation von Polizei und nationalen wie internationalen Geheimdiensten für notwendig erachtet, um effektiv gegen den internationalen Terror vorzugehen.[33]

Auch wenn der Sicherheit vor Terror und dem Schutz von Menschenleben Priorität einzuräumen ist, sollte aber nicht vergessen werden, dass ein hohes Maß an Sicherheit nicht nur hohe direkte Kosten für stärkere Sicherheitsapparate und Sicherheitstechnologien mit sich bringt, sondern zusätzlich auch hohe indirekte und damit schwer messbare Kosten induzieren kann. Das Beispiel der USA zeigt, welche Art von Kosten bei einer Präventionsstrategie auftreten kann. Nach Berechnungen der Federal Reserve Bank in New York stiegen die Ausgaben für die Landessicherheit (homeland security) von 56 Mrd. US-Dollar in 2001 auf 99,5 Mrd. US-Dollar im Jahr 2005.[34] Dies entsprach immerhin einer Zunahme von einem viertel Prozentpunkt des BIP. Nicht eingerechnet dabei und schwieriger zu schätzen sind jedoch die Kosten, die sich durch längere Wartezeit bei der Ein- und Ausreise oder auch die verminderte Bereitschaft ausländischer Fach- und Spitzenkräfte, zum Beispiel in der Wissenschaft, in den USA tätig zu werden, ergeben und langfristig Wirkung zeigen könnten. Freiheit und Offenheit sind nicht nur wesentliche Charakteristika der westlichen Demokratien, sie sind auch Schlüsselfaktoren der erfolgreichen wirtschaftlichen Entwicklung dieser Staaten. Daher ist aus einem ökonomischen Blickwinkel darauf zu achten, dass die Bekämpfung des Terrors, ähnlich wie die Bekämpfung der Kriminalität, mit Realismus und Augenmaß betrieben und nicht übertrieben wird, um sonst entstehende Fehlallokationen und ein langfristig niedrigeres Wirtschaftswachstum zu vermeiden.

33 Vgl. Crenshaw (2007).
34 Hobijn/Sager (2007).

4.3 Datensicherheit

Für die Zukunft der Datensicherheit sind verschiedene technische Entwicklungen bedeutsam. Das Gefährdungspotenzial wird durch eine immer größere Zahl von vernetzten Geräten steigen. Gleichzeitig stehen aber auch neue Technologien zur Verfügung, mit denen die Datensicherheit verbessert werden kann. Diesen stehen aber immer auch neue Technologien für Schadensprogramme gegenüber.[35] In den nächsten Jahrzehnten wird die Vernetzung der Computer weiter zunehmen. In den Industrieländern sind schon heute nahezu alle Unternehmen und ein großer Anteil von Haushalten ans Internet angeschlossen. Dennoch gibt es international große Unterschiede. Abbildung 13 zeigt für die OECD-Länder den Anteil der ans Internet angeschlossenen Haushalte. Für die weit entwickelten Länder zeichnet sich ein Schwellenwert ab: Hier sind etwa 35 % der Haushalte an das Netz angeschlossen. Damit haben über 80 % der Bevölkerung Zugang zum Internet. Geht man davon aus, dass Deutschland bis 2030 eine ähnliche Verbreitung des Internets erreichen wird, wird die Netzgröße noch um fast 50 % zunehmen.

Anzahl der Breitband-Anschlüsse pro 100 Einwohner im internationalen Vergleich, 2007

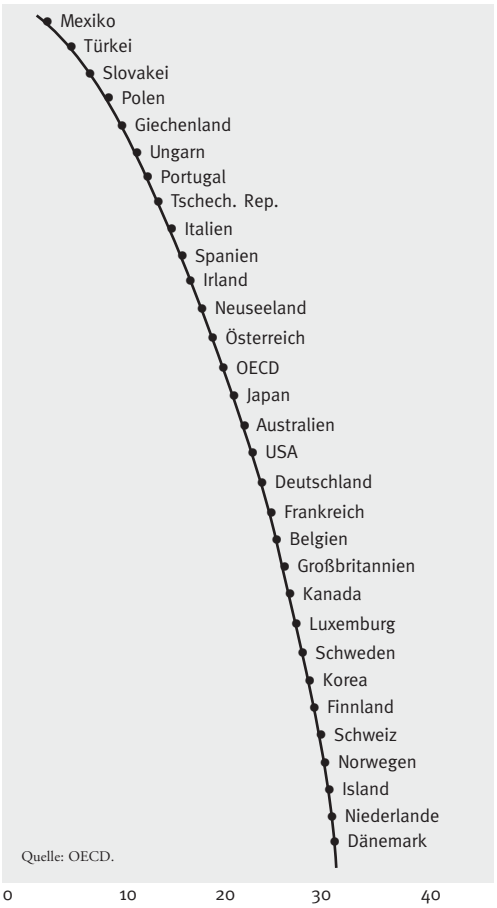

Abb. 13

Über die reine Netzausweitung hinaus wächst die Reichweite des Internets durch die steigende Zahl von mobilen Endgeräten. Insbesondere die Zahl der Smartphones und der PDAs wird deutlich steigen. Da diese über Bluetooth oder W-LAN mit Computern verbunden sind, bilden sie Einstiegspunkte ins Internet und damit Einfallstore für kriminelle Anwendungen. Viren-Scanner und Firewalls sind für diese Geräte zwar vorhanden, aber bisher kaum im Einsatz. Dies gilt insbesondere für Systeme, in denen mobile Endgeräte im Zahlungsverkehr eingesetzt werden.

Eine wesentliche Erweiterung von vernetzten Technologien und Prozessen werden RFID-Systeme (Radio Frequency Identification) darstellen. Solche Systeme bestehen aus einem Transponder und einem Lesegerät. Dabei sendet der Transponder auf Abruf Daten an das Lesegerät. Die

35 Vgl. Bundesamt für Sicherheit in der Informationstechnik (2007).

Informationen werden mittels Radiowellen ausgetauscht und können dann computergestützt weiterverarbeitet werden. Dies erlaubt eine elektronische Identifikation mit kontaktloser Datenübertragung. Heute gängige Anwendungen sind automatische Eingangskontrollen und die lückenlose Verfolgung von Produktionsketten. Beispiele hierfür sind Tieridentifikationen oder die Überwachung von Kühlketten.

Die seit 2007 in Deutschland ausgegebenen elektronischen Pässe speichern biometrische Daten auf einem RFID-Chip und verbessern so die Fälschungssicherheit. Gleichzeitig beschleunigen sie Passkontrollen beispielsweise an Flughäfen. Die zukünftigen Möglichkeiten dieser RFID-Technologie gehen weit über die derzeitigen Einsatzbereiche hinaus.[36] So ist vorstellbar, dass mit dieser Technologie vollautomatische Logistiksysteme, wie sie heute im Containerverkehr eingesetzt werden, für Einzelprodukte Anwendung finden. Außerdem könnte RFID dazu beitragen, dass der selbst nachbestellende Kühlschrank Wirklichkeit wird.

Es ist davon auszugehen, dass zukünftig vermehrt personenbezogene Daten auf Chips gespeichert werden und drahtlos übertragen werden. Diese Daten können von biometrischen Merkmalen über individuelle Krankheitsgeschichten bis hin zu Bewegungs- und Einkaufsverhalten reichen. Verschiedenste Kriminelle könnten Interesse an solchen Daten haben und deshalb versuchen, Schwächen in den Systemen auszunutzen. Insofern trägt die RFID-Technologie zum einen zu einer erhöhten Sicherheit bei, zum anderen erlaubt die Technologie neue Anwendungen, die Angriffe in die Systeme interessanter und attraktiver machen.

Eine weitere Neuentwicklung zur Verbesserung der Sicherheit ist das Trusted Computing. Hier erlaubt ein in PCs oder Endgeräte wie Mobiltelefone eingebauter Chip die gegenseitige Authentisierung der Geräte. Dabei misst der Chip mittels kryptografischer Verfahren die Integrität von Software-Datenstrukturen und Hardware. Die Werte werden nachprüfbar abgespeichert, sodass sie mithilfe des Betriebssystems oder aber auch mit geeigneten Anwendungsprogrammen überprüft werden können. Dadurch entsteht ein Markt für Sicherheitszertifikate. Software-Hersteller und Anbieter von Webseiten können sich zertifizieren lassen, Anderson und Moore sehen darin allerdings den Versuch der großen Software-Hersteller, Markteintrittsbarrieren aufzubauen.[37] Darüber hinaus kann sich auf einem Markt für Zertifikate eine Abwärtsspirale ergeben. Für dubiose Unternehmen ist der Wert eines Sicherheitszertifikates größer als für seriöse. Edelman zeigt, dass es tatsächlich zu einer adversen Selektion dieser Art kommt: Während insgesamt 3 % der Webseiten infiziert sind, sind 8 % der von großen Anbietern zertifizierten Seiten infiziert.[38]

Neben den Neuentwicklungen bei der Hardware kann es auch durch Software-Entwicklungen zu Änderungen im Gefahrenpotenzial kommen. Hier sind insbesondere innovative Anwendungen im Rahmen des Web 2.0 zu nennen. Diese erlauben es, inaktive Inhalte in bestehende Webseiten nachzuladen. Damit wird es möglich, desktopähnliche Anwendungen über das Internet anzubieten. Dies wird vom BSI kritisch bewertet, da für diese Anwendungen die Browser für die Ausführung aktiver Inhalte freigeschaltet werden müssen.

36 Vgl. Oertel/Wölk (2006).
37 Vgl. Anderson/Moore (2006).
38 Vgl. Edelmann (2006).

Teil B

Die Sicherheitsindustrie – Geburt eines Wachstumsmarktes

Berenberg Bank

»Freiheit ist die unverzichtbare Garantie der Sicherheit oder auch nur des Gefühls von Sicherheit.«

(Charles de Montesquieu, französischer Rechts- und Geschichtsphilosoph, 1689–1755)

1. Einleitung

Selten schien das Streben nach Sicherheit ausgeprägter als zu Beginn des Jahres 2008. Große Besorgnis herrschte über den Zustand der öffentlichen/Inneren Sicherheit. Die so empfundene Bedrohung terroristischer Elemente bestand fort. Erinnert sei zudem an die Vorgänge in Tibet und verschärfte Kontrollen im Vorfeld der Fußball-EM sowie der Olympischen Sommerspiele in der VR China. Vielerorts reagierten die Regierungen mit erhöhten Anforderungen an Sicherheitschecks im Waren- und Personenverkehr und vermehrten Überwachungssystemen an öffentlichen Plätzen, Flug- und Seehäfen, Bahnhöfen und Sportstätten. Das schnelle Zusammenwachsen von Informations- und Kommunikationstechnologien sowie digitalisierte Steuerungsprozesse etwa von Kraftwerken und industriellen Produktionsabläufen erhöhten die Aufwendungen von Unternehmen und Privatpersonen für Maßnahmen des Datenschutzes, gegen Wirtschaftskriminalität und Industriespionage.

So ist der Markt für Produkte und Dienstleistungen der Sicherheitsindustrie aktuell von einer hohen Wachstumsdynamik, aber auch von einem ständigen Wandel gekennzeichnet. Kaleidoskopartig vermischen und überlagern sich Teile des Ganzen und führen zu immer neuen Produkten, Anwendungen, Teilbereichen. Konventionelles und Avantgarde beziehungsweise Old und New Economy treffen aufeinander. Anforderungen an die Innere und Äußere Sicherheit wachsen zusammen. Der klassische Gebäude- und Personenschutz wird durch Entwicklungen in der Verteidigungsindustrie, IT- und Kommunikationstechnologie, der Nanotechnologie, Mikroelektronik, Biosensorik oder Robotik erweitert und/oder ergänzt.

Das Ergebnis ist ein faszinierendes, für Unternehmen und Investoren gleichermaßen interessantes Geschäftsvehikel, das wenigstens für die kommenden zehn bis 15 Jahre überdurchschnittliche Expansions- und Ertragschancen birgt.

1.1 Was ist Sicherheit?

Qualitativ: Ein Gefühl des Unbedrohtseins, das aus vorhandenen Schutzvorrichtungen und/oder nicht vorhandenen Gefahren(quellen) resultiert.

Quantitativ: Es gibt etwas, das zwischen völlig sicher und komplett unsicher liegt. Das über Eintrittswahrscheinlichkeiten messbare Risiko vermittelt Anhaltspunkte für mögliche Schadenshöhen. Das Streben nach Sicherheit zählt genauso wie Essen und Trinken zu den Grundbedürfnissen des Menschen. Erst wenn sie erfüllt sind, entsteht (materieller) Raum, um sublimeren Genüssen (Lesen, Musik, Reisen etc.) nachgehen zu können (Maslowsche Bedürfnispyramide).

1.2 Die Entstehung/Entwicklung der Sicherheitsindustrie

Es ist zu beobachten, dass mit steigendem Wohlstand die Bereitschaft zunimmt, diesen sichern beziehungsweise schützen zu wollen. Daraus entstand das klassische Feld der »Sicherheitsindus-

trie«, nämlich der Schutz von Menschen und Objekten. Kollektivschutz war Aufgabe des Staates (Armee, Grenzschutz, Polizei etc.), Individualschutz unterlag der Eigeninitiative. Eine Trennung der Aufgaben und Tätigkeiten war klar und einfach vorzunehmen.

In den vergangenen 15 Jahren, insbesondere nach den Anschlägen des 11.9.2001 auf das World Trade Center in New York, hat sich mit hoher Dynamik ein rapider Marktwandel vollzogen. Die Treiber der Entwicklung waren und sind:

- Die Globalisierung und die mit ihr einhergehende massive Wohlstandsmehrung in großen Teilen der Dritten Welt. Spiegelbildlich dazu:
- Die zunehmende Konzentration der wachsenden Weltbevölkerung in Ballungszentren, die Entstehung von Armutsvierteln und in ihnen von rechtsfreien Räumen.
- Zunehmende Klimakatastrophen und die Bedrohung durch mögliche Pandemien.
- Die rasante Verbreitung des Internets und die Digitalisierung / Vernetzung von Produktions-/ Versorgungs- und Kommunikationsabläufen.
- Ausgeweitete Anstrengungen, öffentliche Einrichtungen präventiv vor Anschlägen zu schützen und die Transparenz von Transport-, Personen- und Kapitalbewegungen zu erhöhen.
- Ein stark gewandeltes Bedrohungspotenzial, das das Antlitz von organisierter Kriminalität, Industriespionage, Datenmanipulation und internationalem Terrorismus komplett verändert hat.

2. Der globale Sicherheitsmarkt

2.1 Marktabgrenzung

Eine allgemeingültige Definition des Sicherheitsmarktes ist nicht existent. Das liegt hauptsächlich an den immensen Abgrenzungsproblemen. Im Gegensatz etwa zur Automobil- oder Stahlindustrie mit klaren Produktprofilen und wohldefinierten Input- und Outputbeziehungen kommt es im Sicherheitsbereich, wie bereits angedeutet, zu mannigfaltigen Überschneidungen: Ist ein mobiler mit Infrarotkamera, biometrischen Erkennungs- und Schadstoffdetektionssystemen ausgerüsteter Roboter ein Produkt des Spezialmaschinenbaus, oder ist er ganz / teilweise der Sicherheitsindustrie zuzurechnen? Wie sind polizeiliche oder geheimdienstliche Tätigkeiten zu berücksichtigen? Als Folge dieser Problematik existierten zum Zeitpunkt der Erstellung dieser Studie kaum umfassende Untersuchungen zum Thema.

Relativ belastbares Datenmaterial gibt es für den bedeutenden Teilbereich der im Rahmen des Personen- und Objektschutzes erbrachten Dienste. Ähnliches gilt für Alarmanlagen und Werttransporte. Einige Prognosen liegen für den auf Sicht der kommenden zehn Jahre am schnellsten

Weltsicherheitsmarkt regionale Anteile, 1995–2005

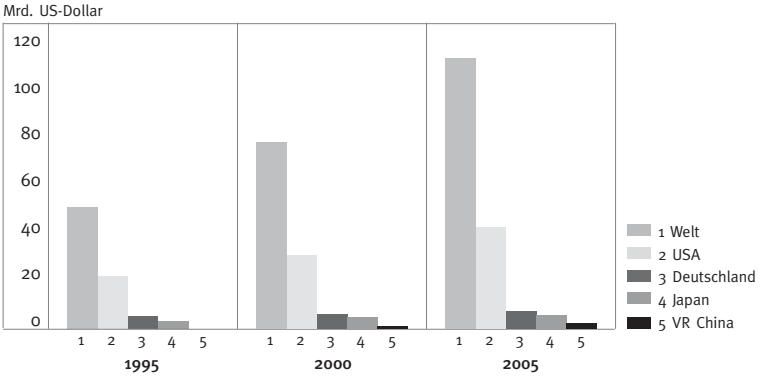

Abb. 14

Quelle: Berechnungen der Berenberg Bank aus aktuellen Marktdaten.

wachsenden Bereich, die Innere Sicherheit (Homeland Defense), vor. Wir werden uns an diese Grobeinteilung halten. Ausgaben und Umsätze für rein militärische Zwecke bleiben ausgeschlossen. Unter dem Begriff der Sicherheitsindustrie verstehen wir daher Produkte und Dienstleistungen zum Schutz vor

- terroristischen Bedrohungen der Kritischen Infrastruktur (öffentliche Gebäude, See- und Flughäfen, Transportwege, Versorgungs- und Kommunikationsnetze),
- organisierter Kriminalität / unerwünschter Migration,
- Internet-Kriminalität / Industriespionage,
- Personenschäden, unbefugtem Zugang zu Gebäuden / Zugriff auf Transportmedien und
- Naturkatastrophen und deren Folgen.

2.2 Marktgrößen und erwartetes Wachstum

Im Jahr 2005 lagen die weltweiten Ausgaben für Sicherheitsdienste bei 113 Mrd. US-Dollar. Das durchschnittliche jährliche Wachstum im vorangegangenen 5-Jahres-Zeitraum betrug 9,3 %, wobei eine deutliche regionale Differenzierung zu beobachten war. Legten Europäer und US-Amerikaner jeweils um durchschnittlich 7,4 % zu, so expandierten die Märkte im asiatisch-pazifischen Raum um 14 %. Die regionalen Anteile der wichtigsten Länder in 2005 sind in den folgenden Grafiken dargestellt.

Ausgaben für Sicherheit, 1995–2005

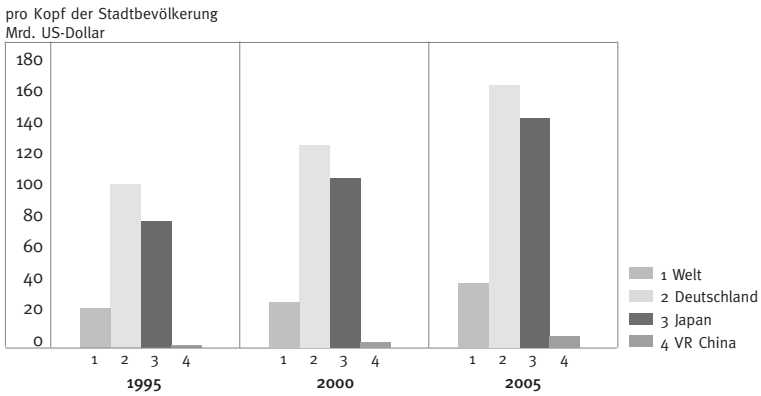

Abb. 15

Quelle: Berechnungen der Berenberg Bank aus aktuellen Marktdaten.

Weltmarkt für Sicherheitsdienste, 2005–2015

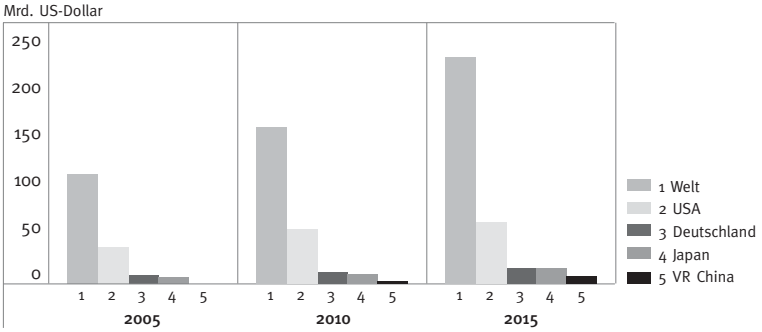

Abb. 16

Quelle: Berechnungen der Berenberg Bank aus aktuellen Marktdaten.

Zum Hintergrund: Wie bereits angesprochen, steigen die Aufwendungen für Schutzmaßnahmen in etwa proportional zur Wohlstandsmehrung. Insofern ist in den Pro-Kopf-Ausgaben der städtischen Bevölkerung ein guter Maßstab für den Grad der Entwicklung / Sättigung der Sicherheitsindustrie in den einzelnen Regionen zu sehen.

Daraus ergibt sich im Umkehrschluss ein überdurchschnittliches Wachstumspotenzial für die sogenannten BRIC-Staaten (Brasilien, Russland, Indien, China), Mittel- und Osteuropa einschließlich des Balkans sowie den Mittleren Osten, wobei hier in erster Linie Saudi-Arabien zu nennen ist (siehe unten). Als wesentliche Antriebskräfte für diese Ländergruppe dienen:

- das überdurchschnittliche Wirtschaftswachstum,
- die damit verbundene steigende Anzahl von Unternehmensgründungen, auch durch
- zunehmende Auslandsinvestitionen und
- eine Vielzahl von privatisierten Staatsbetrieben
- die Ausbildung einer einkommensstarken Mittelschicht und
- eine sich westlichen Standards annähernde, höhere Kriminalitätsrate.

Sowohl für die etablierten als auch für die zurückgebliebenen Zukunftsmärkte gilt:

- Das enorme Bedürfnis nach IT-Sicherheit führt in diesem Bereich zu nochmals schneller steigenden Ausgaben / Umsätzen als für die Gesamtindustrie. Die hierfür zur Verfügung stehenden Budgets werden mindestens im selben Umfang wie die generellen Hightech-Aufwendungen ausgeweitet, also in der Regel mit dem Faktor zwei, gemessen am Anstieg der gesamtwirtschaftlichen Leistung (BIP).
- Schließlich führen die zunehmenden staatlichen Anforderungen in Bezug auf die Homeland Defense wenigstens bis zum Jahr 2012/15 in den betreffenden Marktsegmenten zu überdurchschnittlichen Wachstumsraten, wenn auch mit degressiver Tendenz (siehe Kapitel 4).

Zusammenfassend lässt sich an dieser Stelle sagen:
Der globale Markt für Sicherheitsdienstleistungen hat das Potenzial, sich bis zum Jahr 2015 auf 231 Mrd. US-Dollar gut zu verdoppeln.[1] Das bedeutet: Für den 10-Jahres-Zeitraum von 2005–2015 liegt das Geschäftsvolumen für die beteiligten Unternehmen im vierstelligen Milliardenbereich. Die unterschiedlichen regionalen Tendenzen verzeichnet die nachstehende Grafik. Auf die relevanten Geschäftsfelder gehen wir im Folgenden näher ein.

1 Vgl. Fredonia Group (2006).

3. Die Bereiche der Sicherheitsindustrie – Innere Sicherheit (Homeland Defense)

Ausgaben für Sicherheit, 2005–2015

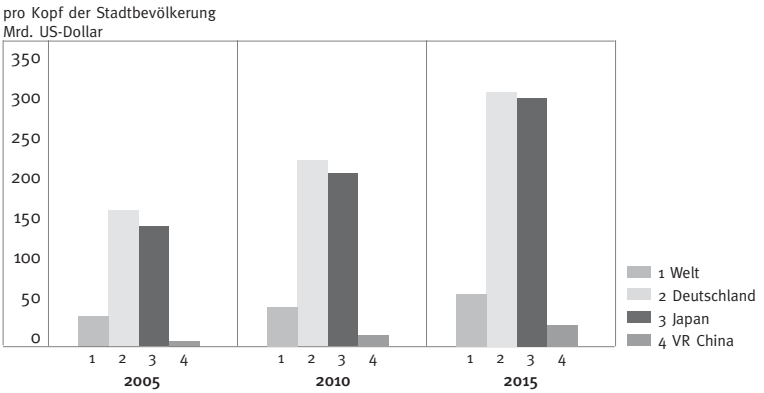

Abb. 17

Quelle: Berechnungen der Berenberg Bank aus aktuellen Marktdaten.

3.1 Entstehung

Der (eine) Markt für Innere Sicherheit oder Homeland Defense (HD) »verdankt« sein Entstehen mehr oder weniger den Ereignissen des 11. Septembers 2001 und der unmittelbar danach insbesondere in den USA einsetzenden Diskussion über verstärkte, konzentrierte Maßnahmen zur Abwehr terroristischer Bedrohungen.

Im Mittelpunkt stand zunächst eine lückenlose, transparente Nachvollziehbarkeit aller grenzüberschreitenden Personen- und Warenbewegungen mit dem Ziel, Gefährdungspotenziale frühzeitig zu erkennen und dann zu eliminieren. Dazu bedarf es unter anderem bestimmter elektronisch-digitaler Profile, dazu passender Identifikationsmechanismen und eines intensiven Datenaustausches zwischen unterschiedlichsten Behörden und Diensten nicht nur eines Landes, sondern auch auf internationaler Ebene. Hinzu kam die Sicherung von See- und Flughäfen. Aktuell werden Konzepte zum Schutz der »Kritischen Infrastruktur« (KI) eines Landes entwickelt. Dazu zählt auch die IT- und Kommunikationsnetzwerk-Sicherheit.

So hat sich aus anfänglich lediglich lose miteinander in Verbindung stehenden Nischenmärkten mittlerweile ein vibrierender neuer Sektor, geprägt von Hightech-Anwendungen und hohen Wachstumsraten, gebildet. Diese Entwicklung hat ab 2005 erheblich an Dynamik gewonnen. Vorausgegangen war eine Zeit konzeptioneller Arbeiten, in der von staatlicher Seite Rahmenbedingungen und Beschaffungsprogramme definiert wurden.

3.2 Marktgröße und erwartetes Wachstum

Gemäß einer Studie der Civitas Group[2] vom November 2006 belief sich der Weltmarkt für Produkte und Dienste zur Stärkung der Inneren Sicherheit im selben Jahr auf 55 Mrd. US-Dollar, was einem Zuwachs von 30 % zum Vorjahr entsprach. Davon entfielen auf die USA 56 % oder 31 Mrd. US-Dollar. Hier war die Marktdynamik mit um 36 % gesteigerten Erlösen immer noch am höchsten. Die USA gelten als die »Pioniere« der Homeland Defense. Ihre Anforderungen sind oftmals zum Weltstandard avanciert. Das verschafft vielen auf diesen Märkten mit einem Erfahrungsvorsprung versehenen US-Unternehmen internationale Wettbewerbsvorteile.

Weltweite Homeland-Defense-Ausgaben, 2003–2015

Mrd. US-Dollar

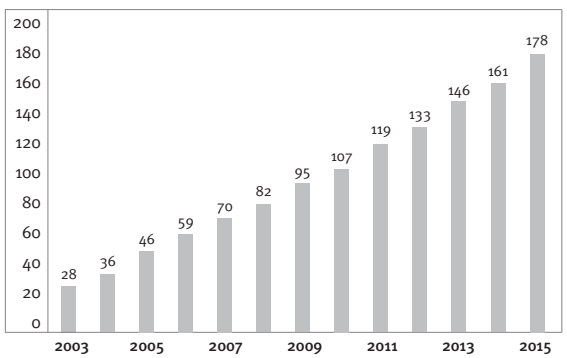

Abb. 18 Quelle: Homeland Security Research Corporation (2005).

Regionale Weltmarktanteile

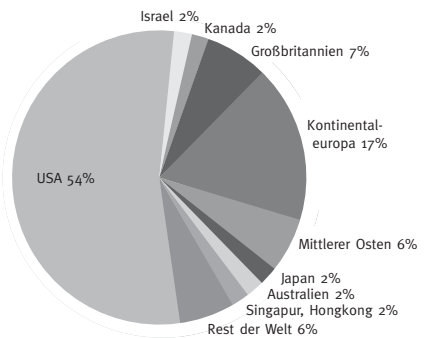

Abb. 19 Quelle: Civitas Group (2006).

Die in Washington ansässige Homeland Security Research Corp. bezifferte den globalen Markt ebenfalls für 2006 auf 59 Mrd. US-Dollar. Die Marktforscher erwarten folgende Entwicklung.

Von 2007–2015 erscheint also ein globales Marktwachstum von 150 % realistisch zu sein. Die Gesamtausgaben für diesen 9-Jahres-Zeitraum dürften 1 100 Mrd. US-Dollar erreichen. Regional wird es zu einer differenzierten Entwicklung kommen.

Während beispielsweise für die Asien-Pazifik-Region ein eher moderater Anstieg um 110 % unterstellt wird – von 7,5 Mrd. auf 15,8 Mrd. US-Dollar –, so sollten auch hier Indien und die VR China ganz vorne liegen. Es kann mit einem Anstieg der Erlöse um 390 % von 3,3 Mrd. auf 16,3 Mrd. US-Dollar gerechnet werden. Daneben werden Sonderbewegungen in stärker bedrohten Ländern wie etwa Russland oder Saudi-Arabien (vgl. Abschnitt 4.3.1: Grenzsicherung) zu beobachten sein. Während Moskau seine Probleme auch weiterhin wohl ohne ausländische Beteiligung regeln dürfte, ist für die Etablierung des saudischen Sicherheitsmarktes ein hohes Geschäftsvolumen insbesondere für US-Unternehmen zu erwarten.

2 Vgl. Civitas Group (2006).

3.3 Die Subsektoren: Anforderungen, Entwicklungspfade und Interkonnektivität

Da die USA mit Abstand der bedeutendste Einzelmarkt bleiben, werden wir im Folgenden mit wenigen Ausnahmen die wesentlichen Subsektoren und ihre erwartete Marktentwicklung am Beispiel des Mutterlandes der Homeland Defense beleuchten.

3.3.1 Grenzsicherung / Flughafenkontrolle

Zu den wichtigsten Aufgabenbereichen der Homeland Defense gehört die Grenzkontrolle. Sei es entlang physischen Grenzen oder zur See beziehungsweise auf Flughäfen. Das bedingt allein schon das erwartete starke Wachstum des Welthandels / Warenverkehrs und die damit verbundene Zunahme des Schiffsverkehrs.[3] So sollen die Containertransporte bis zum Jahr 2030 um bis zu 620 % zunehmen. Das Flugpassagier-Aufkommen dürfte sich zwischen 2005 und 2025 von 4,2 Mrd. auf 8,9 Mrd. Reisende mehr als verdoppeln. Die durchschnittlichen jährlichen Wachstumsraten liegen bei 4,1 %.[4] Noch stärker expandiert demnach das Frachtaufkommen (+5,4 %). Die Anzahl der Flugbewegungen soll um 3,5 % jährlich zulegen, was offensichtlich wesentlich größere Flugzeugtypen impliziert. Neben den Folgen der Globalisierung leitet sich die überragende Bedeutung der Grenzsicherung aber auch aus einem erheblich gestiegenen Bedrohungspotenzial ab. Dies rührt her aus den Problemen

- der unerwünschten Migration,
- veränderter Formen der organisierten Kriminalität (OK) und des
- internationalen Terrorismus.

Die Herausforderung besteht im präventiven Abfangen von unerwünschten Personen und Gefahrstoffen möglichst schon vor Grenzübertritt. Dies hat in der jüngeren Vergangenheit zu einer Reihe von Maßnahmen geführt. Deren ausgeprägte Interkonnektivität lässt die Grenzsicherung im Rahmen dieser Studie besonders geeignet als zentrales Beispiel für das Ineinandergreifen fast aller relevanten Anforderungen / Beteiligten aus Innerer und Äußerer Sicherheit, dem Einsatz intelligenter Hardware-Lösungen, der Verwendung biometrischer Erkennungsmerkmale, Systemen integrierender Software und den Problemen des Zugriffs auf Datenbanken beziehungsweise des (auch internationalen) Datenaustausches erscheinen.

Biometrie und Funkchips (RFID)

Im Mittelpunkt der Erkennung von Personen und Handelswaren stehen elektronische Ausweisdokumente, die sogenannten E-Pässe, und RFID-gesicherte Frachtbehälter, die im Rahmen der Kontrolle von Häfen und Transportwegen zur Anwendung kommen.

In Deutschland begann die Entwicklung von elektronischen Reisedokumenten bereits in 1997, also lange vor den Anschlägen auf das World Trade Center. Allerdings kam es aufgrund erheblicher

3 Vgl. Berenberg Bank / HWWI (2006 a).
4 Vgl. Bundesdruckerei (2007).

technischer Probleme erst ab 2005 zu ersten Auslieferungen. Eine spürbare Verbreitungsdichte ist ab 2010 zu erwarten. Auf Druck der USA werden bis zu diesem Zeitpunkt etwa 40 Staaten mit ca. 50 % der Weltbevölkerung E-Pässe ausgegeben haben.

Zentraler Bestandteil sind auch hier spezielle aktive Funkchips, auf denen biometrische Merkmale der Passinhaber gespeichert werden. Zurzeit sind dies überwiegend die zehn Fingerabdrücke und Abbildungen der Iris. Zukünftig sollen 3D-Darstellungen des Kopfes und unveränderliche, persönliche Merkmale hinzukommen. Es mussten hierfür nicht nur Spezialkameras, Smart Cards, Wege der Übertragung beziehungsweise Speicherung auf den RFIDs und entsprechende »Lesegeräte« entwickelt werden.

Anwendungsprobleme

Viel größere Probleme bestanden oder bestehen noch

- in der Automatisierung der Identifizierung / Verifizierung der gespeicherten Daten. Es muss sichergestellt sein, dass der RFID nicht manipulierbar / austauschbar ist. Sonst bestünde wieder das alte Problem, dass Terroristen mit bis zu 50 verschiedenen Identitäten / Ausweisdokumenten unterwegs sind. Zudem müssen die E-Pässe überall auf der Welt lesbar sein. Dazu gehört ein möglichst identischer Aufbau der Lesezonen. Dazu müssen die verwendeten internetbasierten Software-Anwendungen international kompatibel sein. Dazu sollten die Interface-Lösungen dem Standardprotokoll genügen. Ähnliches gilt für die zum Einsatz kommenden IT-Systeme, gleich ob stationär oder mobil, für den Einsatz in Zügen, auf Schiffen oder im Landesinneren.
- Mit alldem wird ein enorm hohes Datenaufkommen verbunden sein. Große Herausforderungen bestehen in einem schnellen und sicheren Datentransfer. Dies betrifft nicht nur den gegenseitigen Zugriff auf Datenbanken von unterschiedlichen nationalen Behörden, Regierungsstellen und Nachrichtendiensten. Auch international muss ein koordiniertes Vorgehen / Ermitteln beispielsweise zwischen Inter- und Europol möglich sein. Eine wesentliche Rolle wird zudem im Vorfeld von Reisebewegungen den Auslandskonsulaten bei der Ausstellung von Visa-Dokumenten und der entsprechenden Erstellung von Persönlichkeitsprofilen zukommen. Ähnliches gilt für die Fluglinienbetreiber, die schon vor Reiseantritt beziehungsweise der Landung passagierbezogene Informationen an US-Dienststellen zu melden haben. Überdies sind hier aufgrund der geplanten langen Speicherfristen von zehn Jahren und länger Fragen der Persönlichkeitsrechte und des Datenschutzes von Belang.

Andererseits können wohl nur so unverhältnismäßig lange Wartezeiten vor den Sicherheitskontrollschaltern bei Ab- und Einreise an den Flughäfen vermieden werden. Denkbar sind auch automatisierte Identifikations-Gates für besonders vertrauenswürdige Fluggäste. Alles muss reibungslos funktionieren. Sonst besteht durchaus die Gefahr, dass überzogene Sicherheitsbestimmungen und unzulängliche Abwicklungsmodalitäten Fluglinien, Flughafenbetreiber und den internationalen Warenverkehr kostenmäßig durch zeitliche Verzögerungen massiv behindern.

Von einer befriedigenden Lösung kann noch keine Rede sein. Die USA wollten bereits mit einer Vielzahl von Partnerstaaten das geschilderte System eines internationalen Personen- und Waren-Monitoring bis Ende 2004 installiert haben. Der Start erfolgte aber erst in 2007. Der Prozess gilt als längst noch nicht abgeschlossen.

Physische Grenzkontrollen

Als Folge des Abkommens von Schengen sind die innereuropäischen Grenzen fast vollständig verschwunden. Die Außengrenzen haben sich verschoben. Sie konzentrieren sich auf wenige Staaten, die in ihren Aufwendungen zur Grenzsicherung der Gemeinschaft von der EU finanziell unterstützt werden. Insofern spielen mobile Personenkontrollen eine wesentlich größere Rolle. Die hierfür benötigte Technologie entspricht überwiegend den im vorangegangenen Abschnitt beschriebenen Anwendungen zur Flugpassagierkontrolle.

Anders in den USA. Angesichts von bis zu 12 Millionen illegalen Einwanderern gilt der Grenzsicherung im Süden zu Mexiko und mit Abstrichen im Norden zu Kanada das besondere Augenmerk der dortigen Regierungsstellen. Als zu aufwendig wurde inzwischen die flächendeckende Errichtung von Mauer- beziehungsweise Zaunanlagen verworfen. Absolute Priorität gilt nun dem Virtual Fence, das heißt einer möglichst umfassenden Kontrolle der Grenzterritorien mittels elektronischer Überwachungssysteme. Gegen Ende des Jahres 2008 soll eine unter der Bezeichnung »Project 28« bekannt gewordene Teststrecke von 45 km Länge in der Wüste von Arizona voll funktionsfähig sein. Die Installationsphase hätte dann fast drei Jahre in Anspruch genommen. Sie war von vielfältigen Problemen, insbesondere im Software-Bereich, begleitet. Die Projektleitung lag bei Boeing. Haupt-Subkontraktor war Unisys.

Generell geht es um eine Kombination aus stationären und mobilen Überwachungssystemen. Über die 45 km verteilt werden neun Türme errichtet. Sie sind unter anderem mit verschiedensten Sensoren, Spezialkameras, GPS-Einrichtungen, Radargeräten und Up-to-date-Kommunikationsanlagen ausgerüstet. Die beweglichen Einheiten bestehen hauptsächlich aus unbemannten Flugkörpern (Drohnen) und motorisierten Bodeneinheiten. Die von allen Subsystemen gesammelten Daten werden per Funk automatisch an Einsatzzentralen und mobile Grenzwächter weitergeleitet. Sie entscheiden dann über geeignete Gegenmaßnahmen. Bei geplanten Kosten von 2,5 Mio. US-Dollar pro km ergibt sich ein Gesamtvolumen in Höhe von 2,8 Mrd. US-Dollar für die zu sichernden mexikanischen Grenzabschnitte von 1 130 km Länge. Nicht eingerechnet sind die erforderlichen Personalaufstockungen von etwa 9 000 Grenzschützern in 2001 auf 18 000 in 2009.

Das privaten Anbietern von Sicherheitslösungen für die Bereiche Grenzsicherung / Flughafenkontrolle jährlich zur Verfügung stehende Marktvolumen wird für die USA bis zum Jahr 2010 auf 18–19 Mrd. US-Dollar geschätzt.[5]

5 Vgl. Civitas Group (2006).

Sondersituation Saudi-Arabien

Das saudische Königreich nimmt nicht nur aufgrund seiner traditionellen Nähe zu den USA im Mittleren Osten eine gewisse Sonderrolle ein. Es fühlt sich und seine Ölindustrie daher nachhaltig bedroht. Das Land gilt als hochgradig al-Qaida-infiltriert. Deren Anhänger haben bereits mehrfach versucht, die Ölanlagen zu attackieren. Sollte es gelingen, das Förderpotenzial dieses weltgrößten Rohöllieferanten nachhaltig vom Markt zu nehmen, würde dies mit großer Wahrscheinlichkeit zu einer Weltrezession führen. Die Saudis sind andererseits als Folge ihres Ölreichtums in einer finanziell sehr komfortablen Lage. Sie planen daher mit einem ungeheuren Kapitalaufwand, ihre Förderanlagen und Raffineriebetriebe sowie die Grenzen zum Jemen und Irak bis zum Jahr 2018 massiv zu schützen. Über den 10-Jahres-Zeitraum von 2008–2018 sind Ausgaben von 115 Mrd. US-Dollar geplant. Dabei wird die Sicherung der physischen Grenzen mit einem höheren Aufwand als in den USA betrieben. Saudi-Arabien könnte hinter den USA weltweit zum zweitwichtigsten Markt für Homeland-Defense-Anwendungen avancieren. Aufgrund der angesprochenen US-Affinität dürften nordamerikanische Branchenführer hier über besonders gute Geschäftsaussichten verfügen.

3.3.2 Strahlungs- und Explosivstoffdetektion / Schutz vor Pandemien

Einer der Schwerpunkte der US-Behörden liegt auf dem Schutz von Land, Einrichtungen und Bürgern vor den Auswirkungen eines Einsatzes von radioaktiven, biologischen oder chemischen Kampfstoffen. Erinnert sei an den Giftgasanschlag auf die U-Bahn in Tokio von 1995. Damals kamen zwar »nur« 12 Menschen ums Leben. Bei 5 000 Verletzten hätten es allerdings leicht sehr viel mehr Opfer sein können. Angeblich entging die Stadt New York im Jahr 2003 nur knapp einem ähnlichen Attentat durch Al-Qaida-Anhänger.

Geschützt werden soll ebenso vor den Folgen einer »Biologischen (Viren-)Kriegsführung«. Verhindert werden soll der Einsatz radiologischer Sprengsätze (Dirty Bomb). Bekanntermaßen stellt der zunehmende Schmuggel radioaktiven Materials ein globales Problem dar.

Zu diesem Zweck sollen bis Ende 2008 die Voraussetzungen zur Kontrolle jeden Containers, der aus dem Ausland in die USA gelangt, nach ABC-Stoffen geschaffen sein. Dies bedingt die Installation entsprechender Hard- und Software in allen Häfen, in einem weiteren Schritt aber auch an zentralen Zufahrtsstrecken in Großstädte (Straßen- und Bahnverbindungen).

Von der Öffentlichkeit eher missachtet werden die erheblichen Anstrengungen sowohl präventiver als auch die Nachsorge betreffender Maßnahmen gegen mögliche Pandemien. Die Ausbreitung des Vogelgrippe-Virus über Asien hinaus mag als Beispiel gelten. Zu den Profiteuren der geschilderten Anstrengungen gehören Unternehmen aus den Bereichen Biosensorik, Robotik, Software und Pharmazie. Geschätztes Marktvolumen in 2010: 20 Mrd. US-Dollar.

»Handelswaffe« Container-Scanning?

Um einen Teil der Kosten und Verantwortung auf die Handelspartner abzuwälzen, werden die USA zukünftig nur noch Container aus weltweit 50 bis 60 Häfen in ihr Land lassen, die vor der Verladung dieselben Sicherheitschecks durchgeführt haben. Diese sollen zudem regelmäßig vor Ort von US-Beamten kontrolliert werden. Die US-Regierung will das Personal entsprechend von aktuell 50 auf 1 875 Beamte bis 2012 aufstocken. Nicht die Kosten des Durchleuchtens der Container – sie werden bei den hohen Durchsatzraten auf 6–10 US-Dollar je Box veranschlagt – sind das Problem. Vielmehr geht es um eine erzwungene Wettbewerbsverzerrung zwischen den Häfen weltweit. Die Konzentration der Exportströme auf die »Auserwählten« führt zudem zu einer zeit- und damit kostenintensiven Umlenkung der für die Ausfuhr bestimmten Güter innerhalb vieler Lieferländer.

Kasten 4

3.3.3 IT-Netzwerksicherheit

Hier geht es weniger um den reinen Datenschutz oder die Infiltration privat oder in Unternehmen genutzter PCs und Kommunikationsanlagen. Im Mittelpunkt steht vielmehr der Schutz staatlicher IT-Netzwerke, insbesondere im Bereich von Regierungsstellen, öffentlichen Verwaltungen und des Militärs. Spätestens seitdem im Mai 2007 große Teile der öffentlichen Regierungs- und Finanzinfrastruktur Estlands durch Internet-Attacken auf deren zentralen Webseiten für mehrere Tage lahmgelegt wurden, wird von den Gefahren des Cyber-Krieges gesprochen. Möglichkeiten des Schutzes standen auch im Mittelpunkt der NATO-Tagung vom April 2008.

Besonders alarmiert zeigte sich die US-Regierung. Bereits in 2007 wurden etwa 80 000 Angriffe auf Behörden und militärische Einrichtungen registriert. Als Sofortmaßnahme soll die Anzahl der Internetzugänge zu diesen Stellen von 1 300 auf nur noch 50 reduziert werden. Zudem bekannte die chinesische Regierung kürzlich in einem entsprechenden »Weißbuch«, bis 2050 die Fähigkeiten erlangen zu wollen, einen möglichen Internetkrieg gegen jeden gewinnen zu können.

Als Reaktion werden die USA unter Führung der Luftwaffe ein Cyber-Command mit bis zu 40 000 Mitarbeitern einrichten. Es soll bis Ende 2009 einsatzbereit sein und die langfristige Überlegenheit der Vereinigten Staaten im Cyberspace sicherstellen. Neben den Maßnahmen, die auch Unternehmen und Privaten zur Netzwerksicherung zur Verfügung stehen (siehe unten), wird es hier auch zu geheimdienstlichen Operationen kommen. So werden demnächst sämtliche Suchanfragen, E-Mails oder Dateiübertragungen an kritische Stellen überwacht. So könnten auch große Teile des Geschäftsverkehrs mit den USA »gläsern« werden.

Natürlich sollen diese Operationen auch vor terroristischen Gefahren und Auswirkungen der organisierten Kriminalität schützen. Die Regierung hat ihre Mittel für die Jahre 2008–2012 erheblich aufgestockt: Sie stellt 35 Mrd. US-Dollar zur Verfügung.

3.3.4 Schutz der »Kritischen Infrastruktur«

Zur »Kritischen Infrastruktur« (KI) eines Landes zählen neben der bereits angesprochenen Netzwerksicherheit auch der Schutz öffentlicher Gebäude, der Transportwege wie Straßen, Brücken, Tunnel oder Bahnstellwerke, aber auch die Wasser- und Stromversorgungsnetze. Gerade diese sind, wie auch eine Vielzahl anderer industrieller Produktionsprozesse, mittlerweile IT-basiert und -gesteuert. Hier tut sich ein Riesenmarkt für Sicherheitslösungen der Prozesssteuerung auf – genannt SCADA (Supervisory Control and Data Acquisition).

Diese Aussagen gelten in hohem Maße auch für den Finanzsektor (siehe unten). Schutzmaßnahmen konzentrieren sich sowohl von staatlicher Seite als auch durch die Unternehmen auf bauliche Verbesserungen und verlässliche Zugangskontrollen. Insofern ergeben sich durchaus Schnittstellen zu anderen Anwendungsbereichen, etwa in der klassischen Sicherheitsindustrie.

Die deutsche Regierung hat für die Sicherung von IT-Netzwerken und KI 6 Mrd. Euro innerhalb der kommenden fünf Jahre zugesagt. In Bezug auf den US-Markt soll bis 2010 ein geschätztes Marktvolumen von 11 Mrd. US-Dollar erreicht werden.

3.3.5 Waren-, Transport- und Hafensicherheit

Auf die Anstrengungen zur Sicherung der Hafenzonen sind wir erstmals bereits im Rahmen unserer Studie »Maritime Wirtschaft und Transportlogistik«[6] (Teil B, S. 21–24) aus dem Jahr 2006 ausführlich eingegangen. Die verschärften US-Anforderungen an das Container-Scanning wurden weiter oben beschrieben. Im Rahmen der einzurichtenden Sicherheitszonen innerhalb der Hafengelände und der damit verbundenen Zugangskontrollen werden zusätzlich in Kürze in den USA die 3,5 Mio. Fahrer von Gefahrguttransporten überwacht. Sie müssen den E-Pässen ähnliche Identifikationsdokumente mit sich führen.

Ein anderer Schwerpunkt liegt im öffentlichen Nahverkehr (Bahnen, Bahnhöfe, Busse). Neben Videoüberwachungssystemen bieten sich hier an zentralen Punkten installierte Detektionsmechanismen für Gefahrstoffe an. Gerade in diesem Bereich gibt es erhebliche Wachstumschancen. Das gilt auch für ein entlang einer globalen Logistikkette integriertes Überwachungskonzept. Geschätztes US-Marktvolumen bis 2010: 11–12 Mrd. US-Dollar.

3.3.6 Katastrophenschutz

Das schlimme Versagen von örtlichen Stellen bis hinauf zur Bundesebene im Fall des Wirbelsturmes »Katrina« im September 2005 machte schlagartig den erheblichen Nachholbedarf für Prävention und Reaktion auf Naturkatastrophen einerseits, aber auch als Folge industrieller Unfälle oder terro-

6 Vgl. Berenberg Bank/HWWI (2006 a).

ristischer Aktivitäten andererseits erkennbar. Zutage traten erhebliche Mängel an geeigneter Ausrüstung für Rettungskräfte, Bergungsmaschinen, Auffanglagern für Opfer und in der Koordination der Kommunikationswege im Rahmen vorgegebener Notstandspläne der beteiligten Katastrophenstäbe. Im Rahmen des viel diskutierten globalen Klimawandels ist mit einem zukünftig gehäuften Auftreten bedrohlicher Naturereignisse zu rechnen.

Eine effizientere Bewältigung der Folgen industrieller Störfälle muss auf neu entwickelte Hightech-Geräte und -Systeme zur Gefahrstoffidentifikation setzen. Beispielhaft sind Produkte wie das HazMat (Hazardous Material Identification) zum Stückpreis von ca. 80 000 Euro zu nennen. Es kann per Infrarotbestrahlung Gefahrstoffe analysieren. Oder das in Deutschland entwickelte »SIGIS 2« für etwa 100 000 Euro. Es ist auf die Erkennung von Gaswolken spezialisiert und kann deren Giftstoffkonzentration auf Entfernungen von bis zu 5 km messen. Mit etwas geringerem Leistungsumfang werden sich solche Applikationen in Kürze in Mobiltelefone integrieren lassen, die dann die analysierten Daten automatisch an die Leitstellen funken.

In eine ähnliche Richtung zielen die von der deutschen Robowatch vertriebenen Sicherheitsroboter Ofro und Morso. Sie sind mit Videokameras, Radar, Wärmebildkameras, Temperatur- und Biosensoren und Geigerzähler ausgerüstet. Sie werden auch im Rahmen der Überwachung von Großveranstaltungen eingesetzt. Das Unternehmen gehört technologisch zu den absoluten Weltmarktführern. Hilfreich dürfte auch die Übertragung von Gebäudegrundrissen auf in die Feuerwehrhelme integrierte Minibildschirme sein. In Verbindung mit einer GPS-Ortung wissen Rettungskräfte so auch bei starker Raucheinwirkung jederzeit, wo sie sich befinden. Das für den US-Markt geschätzte Marktvolumen in 2010 beläuft sich auf 13–16 Mrd. US-Dollar. Weltweit dürfte es doppelt so hoch liegen.

3.3.7 Geheimdienstliche Aufklärung

Unter diesen Punkt fällt eine Vielzahl von Aktivitäten. Die Kerntätigkeiten dieser Dienste bestehen unter dem Aspekt der Inneren Sicherheit im Sammeln, in der Auswertung und der Überwachung sensibler Daten insbesondere aus der Nutzung moderner Kommunikationsmittel. Dazu bedarf es des Ausbaus einer bislang nur rudimentär bestehenden Koordination von Auslands- und Inlandsdiensten mit Polizei- und Regierungsstellen in den betreffenden Staaten. Zusätzlich müssen Verbindungen zu den Kontrollpunkten in Häfen, an Grenzen und kritischen Infrastrukturobjekten hergestellt werden. Über gemeinsame Beschaffungsstellen sollten einheitliche Hard- und Softwarelösungen angestrebt werden. Letztendlich wird ein starker Personalaufbau unabdingbar sein.

Zwar gab auch hier die terroristische Bedrohungslage den Anstoß für den begonnenen enormen Ausbau geheimdienstlicher Vorgehensweisen. Die spektakulärsten Erfolge gelangen bislang jedoch eher im Kampf gegen Wirtschaftskriminalität und die organisierte Kriminalität. Erinnert sei an das mehrfache Aufdecken international operierender Kinderpornografie-Ringe oder an die führende Rolle von Banken in Liechtenstein bei versuchten Steuerhinterziehungen.

Homeland-Defense Sektoranteile

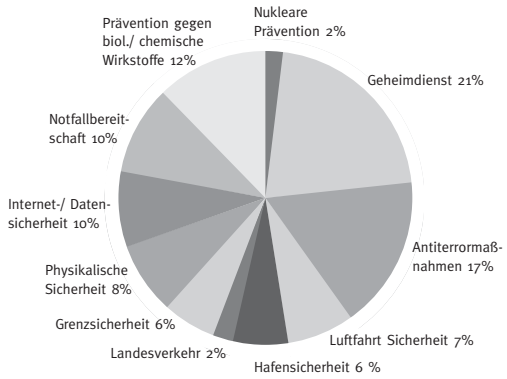

Abb. 20 Quelle: Civitas Group (2006).

Organisierte Kriminalität und die »Ökonomie des Krieges«

Unter diesem Motto stand die Fach-Tagung des Bundesnachrichtendienstes (BND) vom November 2007 in Berlin. Die dort vertretene These lautete: Gebiete mit mangelnder beziehungsweise zerfallender staatlicher Ordnung werden von der organisierten Kriminalität genutzt, um illegale Geschäfte (Drogen, Waffen, Geldwäsche, Menschenhandel etc.) abzuwickeln. Der BND machte 35 solcher »Failed States« aus. Dazu zählen unter anderem der Libanon, Kolumbien, Irak, Cebu (Philippinen), Albanien, Afghanistan und Teile Afrikas. Aber auch in den Slums der Mega-Citys wie Bombay, Jakarta, São Paulo etc. gedeihen diese Geschäfte. Durch ihr Entstehen werden ganze Regionen destabilisiert und Fluchtbewegungen ausgelöst. Sie sind der Nährboden für den internationalen Terrorismus, den man im Zweifel auch mit militärischen Mitteln bekämpfen müsse.

Die Dimension des Problems wird aus der BND-Schätzung der weltweiten Einnahmen der organisierten Kriminalität deutlich. Sie sollen sich auf 700–1000 Mrd. US-Dollar p. a. belaufen. Dies entspräche rund 3% des Welt-Bruttoinlandsproduktes.

Kasten 5

Während in Deutschland und anderen Ländern lange heftig über das Ausspähen privater Computer gestritten wurde, bestehen diese Möglichkeiten technisch natürlich seit Längerem. Sie werden ständig verfeinert. So ist es heute durchaus möglich, vom Notebook aus den Zugriff auf bestimmte Webseiten zu orten, zum Nutzer zurückzuverfolgen, unbemerkt einen Cookie auf dessen PC zu platzieren und anschließend sämtliche Dateien auszuspähen. Aus alledem wird klar, dass sich angesichts des erwarteten Marktvolumens enorme Chancen für Unternehmen bieten, die sich mit der Aufbereitung (Data mining), Analyse und Interpretation riesiger Datenmengen, der Entschlüsselung, der Vernetzung, aber auch der IT-Implementation und -integration sowie der Schulung befassen. Geschätztes globales Marktvolumen bis 2010: 38–44 Mrd. US-Dollar.

Geldwäsche

Gemäß Internationalem Währungsfonds (IWF) wird Geldwäsche wie folgt definiert: »Geldwäsche ist das Verbergen oder der verborgene Transfer von Vermögenswerten, die aus kriminellen Aktivitäten entstanden sind, um die Verbindung zwischen dem Verbrechen und den Vermögenswerten zu verschleiern.«[7]

In dem Maße, in dem die Bedeutung von Kriminalität und Terrorismus steigt, nimmt auch der Bedarf der daran Beteiligten zu, die kriminell erwirtschafteten oder für terroristische Zwecke vorgesehenen Mittel in den offiziellen Wirtschaftskreislauf einzuschleusen. Die Quantifizierung der Geldwäsche ist jedoch – ähnlich wie die Quantifizierung der Schattenwirtschaft – nur schwer möglich, denn es fehlen naturgemäß verlässliche Statistiken. Der IWF hat im Jahr 1999 geschätzt, dass zwischen 2 und 5 % des Welt-Bruttoinlandsproduktes aus illegalen Quellen stammen.

Die polizeiliche Ermittlungsarbeit stößt bei der Bekämpfung der organisierten Kriminalität an Grenzen. Deshalb müssen auch indirekte Wege gefunden werden, die illegalen Tätigkeiten einzudämmen. Ein wichtiger Baustein beim Kampf gegen die organisierte Kriminalität ist die Verhinderung von Geldwäsche. Wenn es gelingt, die Verschleierungsmethoden aufzudecken und damit die Verbindung von Verbrechen und Vermögenswerten transparent zu machen, wird der organisierten Kriminalität zumindest ein Teil der finanziellen Basis entzogen. Der Staat ist jedoch auf die Hilfe derjenigen Unternehmen und Personen angewiesen, ohne die die organisierte Kriminalität nicht zur Geldwäsche in der Lage wäre. Dazu gehören Spielbanken und unter bestimmten Umständen auch Steuerberater, Anwälte und Immobilienmakler, vor allem sind es aber Unternehmen der Finanzindustrie, die dem Staat bei der Erkennung und Vermeidung von Geldwäsche zu Hilfe verpflichtet sind.[8]

Kreditinstitute und Versicherungsunternehmen unterliegen umfangreichen Pflichten bei der Bekämpfung der Geldwäsche und einer laufenden Überwachung durch die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin). Dabei werden die Kreditinstitute in nennenswertem Umfang in staatliche Aufgaben mit einbezogen.[9] Unter anderem gehört dazu die Auskunftspflicht von Mitarbeitern gegenüber Strafverfolgungs- und Finanzbehörden, die Auskunftspflicht gegenüber der BaFin, die Pflicht zur Identifizierung bei der Annahme von Bargeld, Wertpapieren und Edelmetallen ab einem Wert von 15 000 Euro sowie die Anzeige von Geldwäscheverdachtsfällen. Jedes Kreditinstitut hat einen Geldwäschebeauftragten zu benennen. Die gesetzlichen Grundlagen der Geldwäscheprävention sind das Strafgesetzbuch – Geldwäsche ist gemäß § 261 Strafgesetzbuch strafbar – und das Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (»Geldwäschegesetz«). Die dritte EU-Geldwäscherichtlinie aus dem Jahr 2005 wird im dritten Quartal 2008 in nationales Recht umgesetzt.[10]

7 Internationaler Währungsfonds (2003).
8 Vgl. dazu im Detail: Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (2007), §§ 2 ff.
9 Einen Überblick gibt Höche (2002).
10 Vgl. Europäische Union (2005).

Bürokratiekosten in der Kreditwirtschaft

Angaben in Mio. Euro

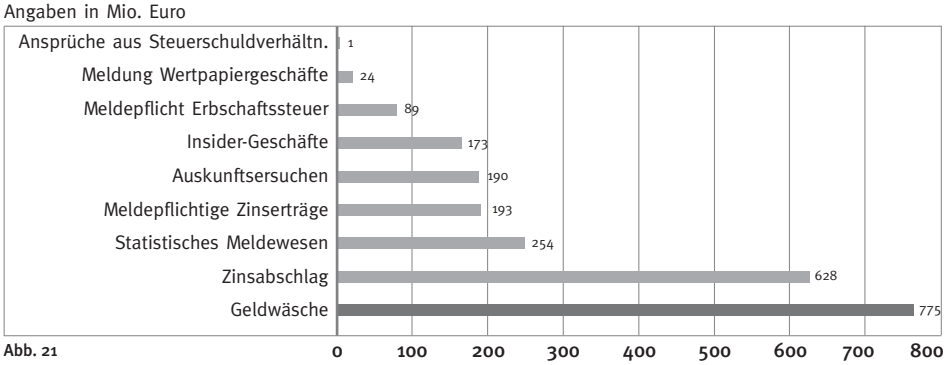

Abb. 21

Quelle: IW-Consult (2006).

Die Geldwäscheprävention hat sich für die Kreditinstitute zu einer erheblichen finanziellen Belastung entwickelt. An den Bürokratiekosten, mit denen die Kreditwirtschaft insgesamt konfrontiert wird, macht der Anteil der Geldwäscheprävention den mit Abstand größten Teil aus.[11] Insgesamt betragen die branchenspezifischen Bürokratiekosten rund 3,1 Mrd. Euro pro Jahr, davon resultieren 775 Mio. Euro aus der Geldwäscheverhinderung und -bekämpfung. Geldwäscheprävention schlägt sich vor allem bei den Personalkosten nieder. Neben den Spezialisten für Geldwäscheprävention müssen aber auch die übrigen Mitarbeiter geschult werden, um Auffälligkeiten zu erkennen und in Verdachtsfällen die richtigen Maßnahmen ergreifen zu können. Zusätzliche Kosten entstehen durch den Einsatz von Computerprogrammen, mit deren Hilfe die Institute in der Lage sind, frühzeitig auffällige Transaktionen zu erkennen.

Doch die Geldwäsche verursacht nicht nur Kosten bei den Unternehmen, die an der Geldwäscheprävention beteiligt sind. Wenn für die organisierte Kriminalität Geldwäsche zum Thema wird, sind die kriminellen Handlungen bereits geschehen, und die Geschädigten haben die entsprechenden finanziellen Belastungen zu tragen. Weitere Kosten der Kriminalität kommen durch den eigentlichen Vorgang der Geldwäsche hinzu, denn das Einschleusen des Geldes in die offizielle Wirtschaft führt oft zu Wettbewerbsverzerrungen. Werden Unternehmen nur »zum Schein«, also nur mit dem Zweck der Geldwäsche, betrieben, können sie ihre Produkte und Dienstleistungen günstiger anbieten als die Anbieter der offiziellen Wirtschaft. Mit der Geldwäsche werden die Preise des »zum Schein« betriebenen Geschäfts quasi subventioniert. Diese Wettbewerbsverzerrungen können als volkswirtschaftliche Kosten der Geldwäsche bezeichnet werden.

Volks- und betriebswirtschaftlich sind die Kosten der Geldwäsche unerwünscht. Dennoch führen sie für Unternehmen aus der Sicherheitsbranche zu einer Erweiterung der Geschäftsfelder. Software für die Erkennung ungewöhnlicher Kontobewegungen gehört ebenso dazu wie die Vernetzung mit Informationen aus anderen Sicherheitsbereichen. Geldwäscheprävention ist somit ein weiterer Baustein des Produktportfolios von Sicherheitsunternehmen.

Kasten 6

11 Vgl. Utzig (2007).

4. Sicherheitsdienste und -technik: Eine weit verzweigte Branche

Neben der Sicherung vor Terrorismus oder Sabotage gerät die private Sicherung von Hab und Gut, und nicht zuletzt des Lebens, immer stärker in das Bewusstsein von privaten Haushalten und Unternehmen. Die Gründe sind, wie bereits thematisiert, vielfältig,[12] die Folgen zukunftsweisend: Die Sicherheitsrisiken haben sich gewandelt, und die Sicherheitsbedürfnisse sowohl bei Unternehmen als auch Privatpersonen haben zugenommen. Hiervon profitieren in zunehmendem Maße private Sicherheitsdienste, da der Staat dem wachsenden Grundbedürfnis an Personen- und Objektschutz allein nicht länger nachkommen kann, sowie innovative Lösungen zur Verbesserung von technischen Überwachungs-, Gefahrenerkennungs- und Frühwarnsystemen. Im Folgenden werden wir uns vorrangig dem Personen- und Objektschutz sowie der Zukunftsbranche der Sicherheitstechnologien widmen. Den Schwerpunkt bildet dabei das Thema Sicherheit von Großveranstaltungen, das angesichts des Sport-Mega-Events in diesem Jahr – der Olympischen Spiele in Peking – von besonderer Aktualität ist.

Sicherheitsdienstleistungen weltweit

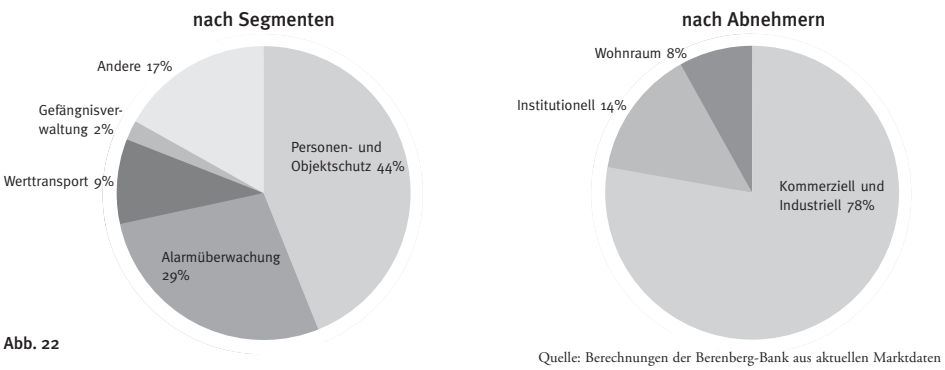

Abb. 22

Quelle: Berechnungen der Berenberg-Bank aus aktuellen Marktdaten

Wie eingangs beschrieben, ist das Marktvolumen für den Bereich Sicherheit nur schwer greifbar. Dies gilt auch für die weit verzweigte Branche der Sicherheitsdienstleistungen und -technik. Weltweit wird das Umsatzvolumen mit etwa 130 Mrd. US-Dollar angegeben (2007). Unterteilt man den Markt für private Sicherheitsdienstleistungen nach Segmenten, entfällt der Löwenanteil mit 44 % auf den Personen- und Objektschutz, gefolgt von 28 % auf Alarmanlagen und 9 % auf Sicherheitstransporte. Unterteilt nach Endabnehmern, entfallen drei Viertel auf Industrie und gewerbliche Unternehmen, 13 % auf institutionelle Endabnehmer (unter anderem Museen, Kirchen, Bibliotheken, Schulen usw.) und 12 % auf Wohngebäude (Daten jeweils aus dem Jahr 2005). Der Markt für die Sicherheit von Sportveranstaltungen wird mit 6 Mrd. US-Dollar beziffert.[13] Größter Abnehmer sind die USA mit einem Anteil von knapp 40 %. Dort liegen die Sicherheitsausgaben der urbanen Bevölkerung mit 220 US-Dollar pro Kopf (2005) weltweit am höchsten. Ähnlich hohe Ausgaben verzeichnen in Europa Länder wie Großbritannien, die Niederlande und Schweden. In Deutschland liegen die durchschnittlichen Pro-Kopf-Ausgaben bei 170 US-Dollar. Der westeuropäische Sicherheitsmarkt hat einen Marktanteil von einem Drittel. Auf den asiatisch-pazifischen Raum entfallen 16 %. Starkes Entwicklungspotenzial dürfte China haben. Der Marktanteil liegt lediglich bei 1 %.

12 Vgl. Teil A, Punkt 2 beziehungsweise Teil B, Punkt 2.
13 Vgl. Security Park (o. J.).

Weltsicherheitsmarkt Personen- und Objektschutz, 1995–2015

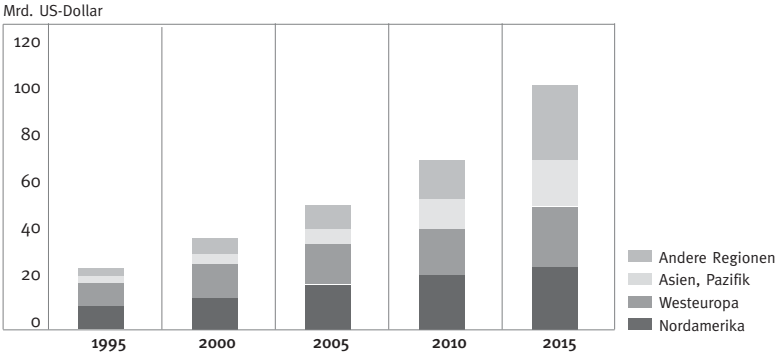

Abb. 23

Quelle: Berechnungen der Berenberg Bank aus aktuellen Marktdaten.

Milliarden-Dollar-Markt: Private Gefängnisse in den USA

Überbelegte Gefängnisse und Kapitalnot bei Kommunen und Ländern: Dies führte dazu, dass während der 90er-Jahre in den angelsächsischen Ländern, allen voran den USA, der Betrieb und der Neubau zahlreicher Verwahranstalten in private Hände übergeben wurden. In jenem Zeitraum war dies der am schnellsten wachsende Teilbereich der Sicherheitsindustrie. Die größte Verbreitung fand in den USA statt. Die Vereinigten Staaten haben den weltweit höchsten Pro-Kopf-Anteil von Gefangenen an der Bevölkerung.

2,3 Mio. oder 0,8 % aller US-Bürger sind inhaftiert. Das sind 800 000 Menschen mehr als in dem fünfmal so bevölkerungsreichen China. Dabei sitzt jeder neunte Farbige im Alter zwischen 20 und 34 Jahren hinter Gittern. In Deutschland sind es etwa 77 000 oder 0,15 % aller Einwohner. Zwar wurden nicht alle Erwartungen hinsichtlich möglicher Kostenersparnisse von 10–20 % der staatlichen Ausgaben erfüllt. Teilweise zu hohe Fluchtquoten, Gewalttätigkeiten unter den Insassen und zunehmende Suizidfälle wirkten ab 2000 dann als »Wachstumsbremse«.

Für die aktuell in diesem Geschäftsfeld tätigen Unternehmen bietet sich jedoch ein unverändert attraktives Umfeld. In den USA liegen die Einnahmen zwischen 60 und 100 US-Dollar pro Tag und Inhaftierten. Sie sind gut kalkulierbar und bieten bei strenger Kontrolle der eigenen Kosten eine stabile Ertragsgrundlage. Mit einer Prise Humor kann man daher sagen: Betreiber privater Gefängnisse sind wie Immobilienfirmen mit Problemmietern, aber ohne Vermietungsprobleme. Marktführer in den USA mit einem 50 %-Anteil ist die »Corections Corp.« mit 65 Objekten, 74 500 Betten (zu 98 % ausgelastet) und einem Jahresumsatz von 1,47 Mrd. US-Dollar (in 2007). Die daraus erzielte operative Marge lag bei 29,5 %, die Börsenkapitalisierung bei 3,5 Mrd. US-Dollar.

Privatgefängnisse gibt es auch in Kanada, Australien, Großbritannien und Südafrika. Die in ihnen festgesetzten Personen entsprechen 1,5 % aller weltweit Gefangenen (ca. 10 Mio.). Aufgrund der aufgetretenen Probleme haben sich jedoch erhebliche politische Widerstände gegen weitere Privatisierungen gebildet. Die zukünftigen Wachstumsraten dürften daher trotz des enormen theoretischen Potenzials auf durchschnittlich 5 % p. a. begrenzt bleiben.

Kasten 7

Sicherheitsdienstleistungen in Deutschland, 2005

nach Segmenten

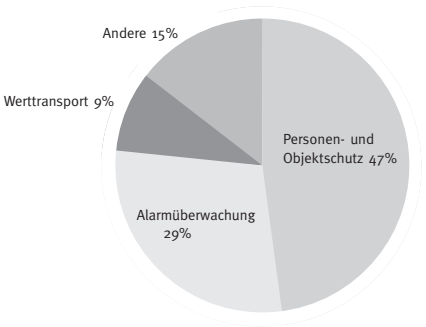

Abb. 24

Quelle: Berechnungen der Berenberg Bank aus aktuellen Marktdaten.

In Deutschland hat der Markt für sicherheitstechnische Produkte und Dienstleistungen ein geschätztes Umsatzvolumen von 10 Mrd. Euro (2005), davon werden Branchenangaben zufolge 3,6 Mrd. Euro für die IT-Sicherheit ausgegeben. In den Segmenten Personen- und Objektschutz sowie Großveranstaltungen engagieren sich aktuell 3 300 Unternehmen mit 170 000 Beschäftigten. Der Umsatz lag im vergangenen Jahr bei 4,3 Mrd. Euro, verglichen mit 2,5 Mrd. Euro vor zehn Jahren. Die Wachstumsraten sind mit 6–8 % p. a.[14] beachtlich und dürften auf absehbare Zeit mit Blick auf die weiter hohe Kriminalitätsrate, die alternde Bevölkerung sowie die wachsende Angst vor terroristischen Anschlägen zumindest ähnliche Größenordnungen erreichen können. Gleich bleibende Zuwächse unterstellt, würde sich das Umsatzvolumen bis 2030 auf etwa 12 Mrd. Euro belaufen.

Weltweit dürfte der Markt für Sicherheitsdienstleistungen auf Sicht der kommenden zehn Jahre ebenfalls um die 7–8 % p. a. wachsen. Für die Entwicklungs- und Schwellenländer sind dabei zweistellige Wachstumsraten zu erwarten. Dies gilt insbesondere für China, wo die Pro-Kopf-Ausgaben für Sicherheit gerade in den wachsenden Millionenstädten und angesichts einer zunehmend kaufkräftigen Mittel- und Oberschicht noch enormen Nachholbedarf haben. Auch die zunehmende Industrialisierung und nicht zuletzt Privatisierung sollte hierzu beitragen.

Während der Personenschutz auch künftig weiter auf den Menschen zugeschnitten sein wird, dürfte der Gebäudeschutz verstärkt über den (zusätzlichen) Einsatz von Robotern geleistet werden. So gehen die Fähigkeiten eines Bewachungsroboters – abgesehen von den menschlichen Schwächen und dem daraus resultierenden »menschlichen Versagen« – zum Teil weit über das hinaus, was Wachdienste leisten können. Hierzu zählt das frühzeitige Erkennen von Rauch und Gasen, die Personenerkennung in dunklen Räumen mithilfe von Infrarot- und Wärmebildkameras sowie die Wahrnehmung kleinster Geräusche mit hochempfindlichen Mikrofonen.[15]

Unterstützung kommt beim Personen- und Gebäudeschutz über Alarmanlagen sowie Videoüberwachungssysteme. Eine Stabilisierung beziehungsweise Erholung der Bautätigkeit unterstellt, könnte sich der weltweite Bedarf an technisch fortgeschrittenen privat beziehungsweise gewerblich genutzten Alarmanlagen von derzeit 2,4 Mrd. US-Dollar allein in den nächsten zehn Jahren mehr als verdoppeln. Bei der Videoüberwachung gehen Branchenkenner davon aus, dass die Zukunft der

14 Vgl. innovations-report (o. J.).

15 So hat beispielsweise das Fraunhofer-Institut gemeinsam mit der Firma Neobotix, einem der europaweit führenden Hersteller von mobilen Robotern, einen innovativen Bewachungsroboter entwickelt, der über einen hochgenauen Laserscanner zur exakten Navigation verfügt, eigenständig Gefahren erkennen, Personen detektieren und gegebenenfalls automatisch Alarm schlagen kann. Die mobile Einheit kann zudem ein Netz aus Sensorsonden auslegen, die per W-LAN mit dem Roboter in Verbindung stehen. Die Sonden erweitern so den Bereich, den der Überwachungsroboter sensorisch erfassen kann. Vgl. Fraunhofer-Institut Produktionstechnik und Automatisierung (o. J.).

netzwerkbasierten Videoüberwachung gehört. Schon heute hat die Verwendung von Netzwerkkameras eine Wachstumsrate von 45–50 % p. a. gegenüber einem Branchenwachstum von 8 % (Video insgesamt). Das Wachstum der dazugehörigen Netze und Übertragungstechniken wird mit 30 % prognostiziert. Gute Wachstumschancen werden neben dem Objekt- und Personenschutz auch dem Sicherheitsconsulting und der Vernetzung von Sicherheitssystemen vorhergesagt.

5. Zukunftsbranche Sicherheitstechnologien

Wie bereits in Teil I beschrieben, wird die Abhängigkeit der Gesellschaft von reibungslos funktionierenden Versorgungs- und Sicherheitssystemen mit dem zunehmenden Technisierungsgrad, der zunehmenden Komplexität und Vernetzung der Informationsgesellschaft sowie der wachsenden Konzentration der Bevölkerung in Ballungszentren immer größer.

So sieht das Bundesministerium für Bildung und Forschung (BMBF) »Deutschland mit seinem freien Informations-, Personen- und Warenverkehr als exportorientierte Wirtschaftsnation und als Land hoher Bevölkerungsdichte einerseits und einer stark ausgebauten, auf Hochtechnologie aufbauenden Infrastruktur andererseits in besonderem Maße neuen Bedrohungen ausgesetzt«.[16]

Auf diese Herausforderungen hat die Bundesregierung im vergangenen Jahr mit dem ersten »Programm zur zivilen Sicherheitsforschung«[17] reagiert. Danach werden bis zum Jahr 2010 über 120 Millionen Euro Fördergelder an Hochschulen, Unternehmen und Forschungseinrichtungen fließen. Im Rahmen der »High-Tech-Strategie« wurden zudem 17 Zukunftsfelder festgelegt, die als arbeitsplatz- und wohlstandsrelevant gelten. Hierzu zählt auch der Bereich Sicherheitstechnologien, der unter dem Motto »Keine Chance für Kriminalität und Terrorismus« steht.

Bis zum Jahr 2013 wird die EU zudem eine Milliarde Euro für die Sicherheitsforschung bereitstellen. Auch wenn dies kein reines Technologieprogramm ist, so zielt es doch sehr stark auf die gesamte Branche ab[18] und lässt zusätzliche Impulse für den Einsatz und die Entwicklung entsprechender Sicherheitstechnologien erwarten. Zu den Sicherheitstechnologien zählt die Fraunhofer-Gesellschaft[19] unter anderem

- Biometrie zur Identifikation von Personen und Werkstoffen,
- Analytik, Sensorik und Detektion von sicherheitsrelevanten Stoffen wie Drogen und Explosivstoffen,
- Schutzkonzepte inkl. Gefährdungs- und Risikoanalyse sowie
- Daten- und Kommunikationssicherheit.[20]

16 Vgl. Bundesministerium für Bildung und Forschung (2007 a).
17 Das Programm ist in einen europäischen Rahmen eingepasst und besteht aus zwei Programmlinien. Programmlinie 1 umfasst die »Szenarienorientierte Sicherheitsforschung«. Auf der Basis der Szenarien wird gewährleistet, dass alle für die Erarbeitung umsetzungsfähiger Sicherheitslösungen notwendigen Disziplinen aus den Technik-, Natur-, Geistes- und Sozialwissenschaften eingebunden und auf gemeinsame Anwendungsziele ausgerichtet werden. Kernelemente der Förderung sind: Schutz von Verkehrsinfrastrukturen, Schutz und Rettung von Menschen, Schutz vor Ausfall von Versorgungsstrukturen, Sicherung der Warenketten. Programmlinie 2 zielt auf die Erforschung von Querschnittstechnologien in »Technologieverbünden« ab. Dazu zählen die Technologien zur raschen und mobilen Erkennung von Gefahrstoffen, zur Einsatzertüchtigung von Sicherheits- und Rettungskräften, zur Mustererkennung und zur schnellen und sicheren Personenidentifikation.
18 Vgl. innovations-report (o. J.).
19 Vgl. Fraunhofer-Gesellschaft (2005).
20 Vgl. Teil A, Kapitel 3.3, IT-Sicherheit.

Science-Fiction und Orwell in einem: Ein Stadionbesuch 2030

Wir wollen – der Aktualität der sportlichen Großveranstaltungen in diesem Jahr angemessen – unsere Leser an dieser Stelle auf einen Besuch in die Sportarena 2030 einladen. Wir erwarten, dass der Besucher dort auf Schritt und Tritt von neuen Sicherheitstechnologien überwacht und begleitet werden wird. Denn gerade Stadien sind aufgrund ihrer dicht mit Menschen besetzten Plätze neuralgische Punkte, wo Terroranschläge, aber auch jede Art von Unfällen größeren Ausmaßes, katastrophale Konsequenzen haben können. Dies gilt in ganz besonderem Maße für hochsensible und gleichzeitig medienwirksame Großveranstaltungen wie Olympische Spiele. In diesem Zusammenhang sei an die Anschläge auf die israelischen Sportler im Olympischen Dorf 1972 in München erinnert. Auch heute und in Zukunft umso mehr wird die Angst bei Sportveranstaltungen mitspielen. Der Schutz und gegebenenfalls die Rettung von Menschen werden somit zu einer immer größeren Herausforderung für Staat und Privatwirtschaft. Neue Technologien sollen dieser Herausforderung begegnen.

Ein aus heutiger Sicht zum Teil noch recht utopisch anmutender Stadionbesuch im Jahr 2030 könnte wie folgt aussehen:

- Bereits der Einlass ins Stadion 2030 dürfte künftig weit über das hinausgehen, was unser Besucher vom Passieren gängiger Kontrollen kennt, und sich dem Prozedere an Flughäfen vermutlich immer stärker annähern. Um Gefährdungsquellen frühzeitig zu erkennen und zu analysieren, werden Identifikation, Kontrolle und Durchsuchung weiter zunehmen. Vor diesem Hintergrund wird es auch künftig nicht ohne den Einsatz von Sicherheitspersonal gehen, dieser wird aber verstärkt technisch unterstützt werden.
- Überproportional zunehmen dürfte der Einsatz neuer Überwachungs- und Identifikationstechnologien bei der Personenkontrolle. Diese werden weit über die reine Ausweiskontrolle, deren obligatorisches Herzstück optimierte RFID-Systeme zur kontaktlosen Datenübertragung sein werden, hinausgehen. So wird sich der Stadionbesucher 2030 zuerst einmal einem biometrischen Verfahren zur Identifizierung und Verifizierung seiner Person unterziehen müssen. Dabei wird die herkömmliche Fingerabdruck-Identifikation künftig nicht mehr reichen. Zum einen wird die Überprüfung, ob seine Fingerabdrücke tatsächlich von echten Fingern stammen, zunehmend an Bedeutung gewinnen. Bereits heute wird an Verfahren für eine optionale Lebenderkennung gearbeitet, sodass das Lesegerät die Verwendung von gefälschten Fingerabdrücken, wie zum Beispiel durch Plastikfinger oder künstliche Fingerkuppen, erkennen kann.

  Zum anderen werden zusätzliche unveränderliche Merkmale unseres Besuchers zum »Türöffner« der Zukunft. Erst wenn neben dem Fingerabdruck die Stimme, die Augen (Netzhautmuster), das Gesicht oder im Bedarfsfall noch zusätzlich bestimmte verhaltensabhängige Attribute (beispielsweise der Schreibrhythmus bei Unterschriften oder auf der Tastatur) erkannt sind, wird

i h m

der Einlass gewährt werden. Dabei geht der Trend zu Kontrollsystemen, die all diese Parameter gleichzeitig überprüfen und abgleichen, in vielen Fällen in Verbindung mit elektronischen und optischen Smart Cards beziehungsweise Sicherheitslabeln.[21] Auch die körperliche Untersuchung wird natürlich weiter eine Rolle spielen. Jedoch werden auch hier im Jahr 2030 vielfältige technische Innovationen zum Einsatz kommen, zum Beispiel um Plastiksprengstoffe oder Materialien, aus denen Handfeuerwaffen bestehen / entstehen könnten, selbst an vollständig bekleideten Menschen erkennen zu können.[22]

- Ist die erste Hürde automatischer Zugangskontrollen mit integrierten biometrischen Systemen genommen, werden Kameras jeden Schritt unseres Zuschauers im Jahr 2030 beobachten und analysieren. Intelligente, automatisierte Mustererkennungsverfahren, die sich heute noch in den Kinderschuhen bewegen, werden die Sicherheitssysteme der Zukunft optimiert haben. Diese Systeme werden zunehmend mit Referenzbildern und Mustervergleichen arbeiten. Dabei kommen Bildauswertungssysteme zum Einsatz, die sicherheitskritisches Verhalten erkennen und über automatisierte Entscheidungsverfahren beziehungsweise simulationsgestützte Risikoanalysen entsprechende Gegenreaktionen auslösen können.
- Ist unser Stadionbesucher als »unauffällig« eingestuft, werden weitere Gefahrenherde – nicht nur für die Innere, sondern auch für die äußere Sicherheit der Stadien – abgeklopft. Dabei werden Sensoren eine dominierende Rolle spielen. Sie werden zunehmend zur Detektion von toxischen Substanzen, von Sprengstoffen sowie von atomaren, biologischen oder chemischen Kampfstoffen als Spürnasen verwandt. So wird beispielsweise ein berührungsloses Verfahren mithilfe von hoch spezialisierten Infrarotlasern zuverlässig Sprengstoffpartikel in der Luft nachweisen können.[23]
- Während dies für unseren Stadionbesucher 2030 völlig im Verborgenen geschieht, wird ihm dagegen ein sensorischer Spürhund, der ähnlich präzise wie eine richtige Hundeschnauze Explosivstoffe anhand des Geruchs identifizieren kann, des Öfteren auf den Tribünen oder im Labyrinth des Stadioninneren begegnen. Wer weiß, vielleicht wird dieser Roboter-Hund sogar mit dem Schwanz wedeln. Begegnen werden unserem Stadionbesucher auch immer wieder Überwachungs-Roboter, die an nahezu allen Punkten für die Stadionsicherheit im Einsatz sein werden.[24]
- Heute noch nicht vorstellbar, aber im Stadion 2030 werden über den Köpfen der Zuschauer unbemannte Luftfahrzeuge – einzeln oder in Schwärmen – schweben und für die Sicherheit von Sportlern und Besuchern sorgen. Branchenkenner gehen davon aus, dass Flugroboter in Zukunft zu unserem Alltag gehören und in den verschiedensten Bereichen zur Aufklärung und Überwachung eingesetzt werden.[25] So werden diese sogenannten Drohnen computergesteuert Überwachungsflüge unternehmen, über Satelliten-Navigationssysteme ihre Positionsdaten liefern und über Bildauswertungssysteme Verdächtiges zeitnah an ihre Computer-Auswertungszentralen liefern. Sicherheits- und Rettungsdienste werden sich mithilfe von Drohnen ein genaues Bild über

21 Vgl. Fraunhofer-Gesellschaft (2005).
22 Vgl. Rheinmetall (o. J.).
23 Um Sprengstoff im Freien, wie in einem Stadion, erkennen zu können, sind zum Beispiel spektroskopische Methoden sinnvoll. So forscht das Fraunhofer-Institut für Chemische Technologien gemeinsam mit der Fachhochschule Düsseldorf an einem Verfahren, das den typischen Attentatssprengstoff TATP aus der Luft über den Köpfen der Fußballfans identifizieren könnte. Oder fachmännisch ausgedrückt: TATP, das bereits unter Zimmertemperatur zu verdampfen beginnt, kann mit einer bestimmten Infrarot-Spektroskopie auf mehrere Hundert Meter gemessen und erkannt werden.
24 So hat die deutsche Robowatch Technologies GmbH zu den Olympischen Spielen 16 Sicherheitsroboter nach Peking geliefert.
25 Vgl. Gawrych (2008).

die Lage aus der Luft machen können.

- Die bisher bekannten Drohnen sind schon klein, dürften in Zukunft aber noch kleiner werden. Vorreiter auf dem Miniatur-Weg künftiger Flugroboter ist derzeit wohl das Micromechanical Flying Insect der Universität Berkeley, ein Kunstinsekt von der Größe einer Stubenfliege. Die Vorteile liegen auf der Hand. So können die kleinen Insekten beispielsweise feststellen, ob an unzugänglichen Stellen Gift austritt, oder auch unter zusammengestürzten Stadiondächern an für Menschen schwer zugänglichen Orten nach Verletzten suchen. Gearbeitet wird darüber hinaus an der Technischen Hochschule Lausanne an der Idee, viele kleine Flugroboter zu schlagkräftigen Schwärmen zu verbinden. Sollte im Falle einer Katastrophe die Handy- oder W-LAN-Infrastruktur ausfallen, könnte ein solcher Schwarm ein mobiles Funknetz aufbauen.
- Je kleiner diese Flugroboter werden, desto mehr Probleme sind allerdings noch bis zu unserem futuristischen Stadionbesuch 2030 zu lösen. So müssen für die kleinen insektenähnlichen Roboter leichte, aber leistungsfähige Batterien und Mini-Sensoren zur Erkennung von Hindernissen entwickelt werden. Als Lösung scheint sich hier vor allem die Bilderkennung der Insekten anzubieten. So liefert das Facettenauge der Stubenfliege zwar kein deutliches Bild der Umgebung, kann aber Bewegungen präzise erfassen. Sollte es gelingen, diese Mini-Flugroboter darüber hinaus in intelligenten, kommunikationsfähigen Schwärmen agieren zu lassen, dürfte die Luft der Stadien 2030 tatsächlich zunehmend von surrenden künstlichen Insekten gefüllt sein.
- Wovon unser Stadionbesucher 2030 – vermutlich – nie etwas bemerken wird: Ein potenzieller Sprengstoff-Attentäter wird künftig auch im Gewühl von Massenveranstaltungen rechtzeitig erkannt werden können. So ermöglicht beispielsweise die Terahertz-Strahlung den Blick ins bisher Unsichtbare. Diese für den Menschen unschädliche Strahlung, die den Bereich zwischen Mikrowellen und Infrarotstrahlung abbildet, kann Papier, Kleidung, Mauern und Kunststoff durchdringen und dadurch Waffen und Sprengstoff auch unter der Kleidung erspüren.[26] Um schneller auf Gefahren reagieren zu können, werden die Sicherheitskräfte mit einem Handyfrühwarnsystem ausgestattet sein, das mittels winziger Detektoren frühzeitig nukleare, biologische und chemische Gefahrstoffe identifizieren kann. Für die Erkennung möglicher Scharfschützen kommen weiter entwickelte optische Geräte und Sensoren zum Einsatz. Hochsensible akustische Sensoren werden darüber hinaus auffällige Fahrzeuge, die sich dem Stadion unbefugt nähern, rechtzeitig entdecken. Beim passiven Schutz wird das Ausschalten gegnerischer Elektronik, wie zum Beispiel mithilfe der Mikrowellentechnik, eine größere Rolle spielen. So werden sich funkgesteuerte und elektrotechnische Anlagen, die zum Beispiel über Handys zum Zünden von Sprengladungen eingesetzt werden könnten, durch Störeinrichtungen ganz gezielt lahmlegen lassen.[27]
- Trotz aller Vorbeugungs- und Sicherheitsmaßnahmen sind Anschläge auch im Jahr 2030 nicht auszuschließen. Sollte es zu einem Terrorakt – oder schwerwiegenden Unfall – kommen, werden die technologischen Sprünge in der Sicherheitsbranche aber helfen, verheerende Ausmaße wie nach den Anschlägen vom 11. September auf das World Trade Center zu verhindern bezie-

26 Quelle: Fraunhofer-Gesellschaft (2007).
27 Vgl. Rheinmetall (o. J.).

hungsweise zu minimieren. Mit Hochdruck wird an technischen Innovationen zur Verbesserung der Einsatzmöglichkeiten und Schutzsysteme für die Rettungs- und Sicherheitskräfte gearbeitet.

- Die Feuerwehr der Zukunft könnte so aussehen: In die (verbesserten) Schutzanzüge ist eine ausgeklügelte Sensor- und Kommunikationstechnik integriert, die Kommunikation hält die Hände frei, die Verständigung ist auch bei aufgesetzter Atemschutzmaske möglich, über ein Display im Helm werden Informationen über das Stadion weitergegeben, am Helm montierte Wärmebildkameras lassen Gefahren schneller und besser erkennen, intelligente Mikrosysteme in der Kleidung vermitteln Daten über die eigene körperliche Verfassung, helfen bei der Ortung und Orientierung in Gebäuden.[28] Unterstützt wird der Einsatz von Rettungskräften durch entsprechende Ortungs- und Navigationssysteme, die für schnellstmögliche Hilfe und Evakuierung sorgen werden. Zudem können Sendeeinheiten und Peilsender so verstreut werden, dass eine problemlose Kommunikation untereinander und mit den zentralen Lenkungseinheiten möglich ist. Zusätzlich zum Einsatz kommen Roboter, die für Hilfe in besonders gefährlichen Situationen ausgestattet sein werden.
- Verlässt unser Besucher 2030 nach einer ereignisreichen Sportveranstaltung schlussendlich das Stadion, werden ihm die Erfahrungen neuer Evakuierungstechniken zugutekommen. So werden beispielsweise unter Zuhilfenahme von Computersimulationen Gesetzmäßigkeiten über das Verhalten großer Menschenmengen nutzbringend angewandt, sodass Staus vor den Ausgängen der Stadien weitestgehend umgangen und die Massen unter Umständen über die Notausgänge ge-

28 Vgl. Bundesministerium für Bildung und Forschung (2007 b).
29 Vgl. Bundesministerium für Bildung und Forschung (2007 c).

Business Continuity Management – BCM

In den bisherigen Abschnitten hat sich gezeigt, dass Unternehmen einer Vielzahl von Gefahren ausgesetzt sind. Ob Naturkatastrophen, kriminelle beziehungsweise terroristische Attacken oder der Ausfall wichtiger Lieferanten – die Leistungsfähigkeit eines Unternehmens kann durch diese Gefahrenquellen erheblich beeinträchtigt werden. Der Schutz vor den Gefahren erfordert ein hohes Maß an Weitsicht und erhebliche organisatorische Vorkehrungen. Unternehmen müssen alle denkbaren Eventualfälle gedanklich durchspielen, um auf den Worst Case vorbereitet zu sein.

Viele Eventualfälle würden im Schadenfall nicht nur hohe Kosten verursachen, sie würden im ungünstigsten Fall sogar den Bestand des Unternehmens gefährden.[30] Zum Worst-Case-Szenario gehört die Unterbrechung beziehungsweise der Ausfall des Geschäftsbetriebes. Um diesen Fall auszuschließen oder die Wahrscheinlichkeit zu minimieren, unterhalten viele größere Unternehmen Abteilungen für Kontinuitätsmanagement beziehungsweise Business Continuity Management (BCM). Aufgabe der Abteilungen ist es, dass zumindest die kritischen Geschäftsprozesse auch bei Störungen oder Notfällen weiterhin funktionieren. Analog zum öffentlichen Katastrophenschutz könnte man das Kontinuitätsmanagement auch als »betrieblichen Katastrophenschutz« bezeichnen, der Notfallpläne erarbeitet und deren Umsetzung organisiert. Am Anfang der Aufgabenkette stehen jedoch die Identifikation der wichtigsten Geschäftsprozesse und eine Priorisierung der zu schützenden Geschäftsbereiche. Die Liste der denkbaren Schadenfälle ist lang.[31] Noch länger ist die Liste der Maßnahmen, die präventiv und gegebenenfalls kurativ zur Aufrechterhaltung des Geschäftsbetriebes eingeleitet werden müssen. Exemplarisch sollen drei Gefahrenbereiche skizziert werden:

Höhere Gewalt / Naturkatastrophen:

Naturkatastrophen sind in weiten Teilen der Welt ernsthafte Bedrohungen. Ein Beispiel mit meist noch vergleichsweise geringen Schäden sind die Hurrikans im Golf von Mexiko. Infolge der Schließung von Öl-Plattformen kommt es oft zu Lieferengpässen und zum Anstieg des Ölpreises. Da Art und Umfang der Schäden erfahrungsgemäß einem gewissen Muster folgen und das Auftreten der Hurrikans saisonal begrenzt ist, sind präventive Maßnahmen verhältnismäßig gut zu organisieren. Es gibt aber auch Ereignisse, deren Eintreten weniger vorhersehbar ist. So stellen zum Beispiel Erdbeben, Überschwemmungen oder Waldbrände in vielen Ländern die Bevölkerung, aber auch die Unternehmen, vor erhebliche Probleme. Neben den unmittelbaren Sachschäden und den – temporären – Produktionsausfällen sind auch Folgeschäden zu bedenken. Nach Erdbeben und Überschwemmungen drohen oft Epidemien, die zusätzliches Leid bewirken und Arbeitskräfte vorübergehend arbeitsunfähig machen. Die betrieblichen Abläufe werden dadurch zum Teil gravierend gestört.

30 Vgl. etwa Deloitte (2007), S. 10 ff.
31 Für eine Einteilung der Gefahren vgl. Müller (2007), S. 82.

Für Deutschland und weite Teile Mitteleuropas sind die Gefahren, die von Naturkatastrophen ausgehen, vergleichsweise gering. Sorglos dürfen die Unternehmen deshalb dennoch nicht sein. So hatte die Furcht vor einer Vogelgrippe-Pandemie im Jahr 2006 die BCM-Abteilungen vieler Unternehmen fest im Griff. Neben der präventiven Beschaffung von Medikamenten ging es vor allem darum, die Arbeitsabläufe für den Fall zu organisieren, dass die Vogelgrippe auf den Menschen übertragen wird. Da Ungewissheit darüber besteht, ob und in welcher Form die Vogelgrippe von Mensch zu Mensch übertragbar ist, musste in die Planungen mit einbezogen werden, dass im Krisenfall der Kontakt zwischen den Menschen, soweit es geht, eingeschränkt wird. In vielen Berufen ist die Einrichtung von Home Offices das geeignete Mittel, die Tätigkeiten wichtiger Mitarbeiter aufrechtzuerhalten, ohne dass sich diese durch unnötigen Kontakt zur Außenwelt einem Ansteckungsrisiko aussetzen müssen. Mit derartigen Home-Office-Lösungen sind Kosten verbunden, die dem IT-Bereich im weiteren Sinne zuzuordnen sind. Es profitieren Programmierer, Software-Entwickler, Systemadministratoren sowie Anbieter von Computer-Hardware und -Software.

Kriminalität / Terrorismus:

Neben den Naturkatastrophen sind Unternehmen zahlreichen von Menschen gemachten Risiken ausgeliefert. Zu den ältesten Herausforderungen zählt der Schutz vor kriminellen Handlungen. Dabei sind sowohl externe als auch interne Risiken zu berücksichtigen. Zu den externen Risiken zählen Raubdelikte jeglicher Art. So sind das Firmengelände beziehungsweise die Büroräume vor unbefugtem Zutritt zu schützen. Produktionsanlagen und Büroeinrichtungen müssen geschützt, aber auch der Industriespionage muss ein Riegel vorgeschoben werden. Im Sinne des Kontinuitätsmanagements geht es um die Sicherung essenzieller Produktionsfaktoren. Interne Sicherheitsrisiken spielen ebenfalls eine wichtige Rolle. So sind 49 % aller deutschen Unternehmen in den letzten zwei Jahren Opfer von Wirtschaftskriminalität geworden.[32] Die damit verbundenen Probleme sind jedoch im Regelfall nicht so gravierend, dass sie ein Fall für das Kontinuitätsmanagement werden.

Wichtiger als Kriminalität ist in diesem Zusammenhang der Terrorismus. Zwar ist die Wahrscheinlichkeit für ein Unternehmen, Ziel einer terroristischen Attacke zu werden, gering, jedoch wären die Folgen erheblich. Zudem dürfte die Wahrscheinlichkeit auch davon abhängen, wie groß ein Unternehmen und in welcher Branche es tätig ist. Denn Terroranschläge haben das Ziel, größtmögliche Aufmerksamkeit zu erlangen. Aus diesem Grunde sind Großveranstaltungen wie Fußball-Welt- und -Europameisterschaften sowie Olympische Spiele besonders gefährdet.

Die legendären Worte des damaligen IOC-Präsidenten Avery Brundage anlässlich der Geiselnahme während der Olympischen Spiele 1972 in München – »Die Spiele müssen weitergehen« – eignen sich als Leitsatz für jede BCM-Abteilung. Die Gefährdung solcher Groß-

32 Vgl. PriceWaterhouseCoopers (2007), S. 10.

Wirtschaftliche Bedeutung der Fußball-WM 2006 nach Sektoren

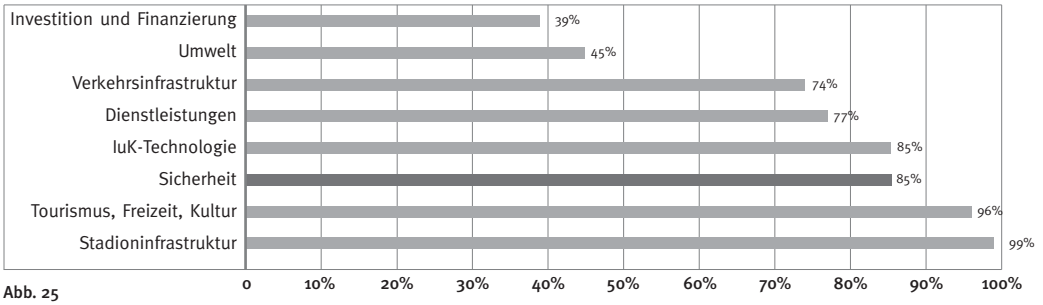

Abb. 25

Quelle: Wegweiser GmbH (2004).

veranstaltungen hat zur Folge, dass die Sicherheitsbranche zu den wirtschaftlichen Haupt-Profiteuren derartiger Events zählt. Zu diesem Ergebnis kam auch die Marktforschung im Vorfeld der Fußball-Weltmeisterschaft 2006 in Deutschland. Hinter den Bereichen »Stadioninfrastruktur« und »Tourismus, Freizeit, Kultur« wurde dem Bereich »Sicherheit« das drittgrößte wirtschaftliche Potenzial attestiert.

Die wichtigste Strategie beim Umgang mit den Folgen von Terroranschlägen ist für Unternehmen die Risikodiversifizierung. Idealerweise werden die kritischen Geschäftsbereiche dezentral organisiert. Wenn dies aus betrieblichen Gründen nicht möglich ist, sollte sichergestellt werden, dass für den Ernstfall Ersatzräumlichkeiten an anderen Standorten bereitgehalten werden.

Ausfall von Daten- und Energienetzen:

Die Aufrechterhaltung des Geschäftsbetriebes stellt die IT-Abteilungen vor zunehmende Herausforderungen. Die Sicherung von Daten vor dem Zugriff unbefugter Personen und der Schutz vor Datenverlust oder -manipulation gehören zum Kerngeschäft der IT-Abteilungen.[34] Ohne die Möglichkeit, permanent auf alle relevanten Daten zurückgreifen zu können, ist der Geschäftsbetrieb schnell gestört. Firewalls, Virenscanner, Ersatzserver und vieles mehr gehören zum Standard-Rüstzeug gegen IT-Sicherheitsrisiken. Die zunehmenden Erfordernisse im Bereich der Datensicherheit beleben nicht nur den Arbeitsmarkt für IT-Fachleute, auch Unternehmen, die entsprechende Softwarelösungen anbieten, profitieren.

Ein weiteres kritisches Thema ist die Energiesicherheit. Die südafrikanische Wirtschaft muss zum Beispiel derzeit die Erfahrung machen, welche Auswirkungen eine unzureichende Energiesicherheit hat. Strom wird rationiert, zahlreiche Unternehmen waren und sind gezwungen, ihre Produktion einzuschränken. Für die betroffenen Unternehmen führt das zu Umsatz- und Gewinneinbußen. Doch die Folgen sind auch für den Weltmarkt spürbar, denn wegen der Energiekrise sank die Förderung verschiedener Rohstoffe, und die Preise stiegen:

33 Vgl. ausführlich zum Thema Datensicherheit den Abschnitt 3.3, Teil A.

So kletterte der Platin-Preis in den ersten beiden Monaten des Jahres 2008 von 1 500 auf über 2 200 US-Dollar. Der Preisanstieg war zu einem guten Teil auf die Energiekrise und die Produktionsrückgänge in Südafrika zurückzuführen. Das Business Continuity Management hat in den letzten Jahren an Bedeutung gewonnen. In den USA und in Großbritannien ist es bereits fest etabliert. In Großbritannien wurde 1994 das Business Continuity Institute (BCI) gegründet, das heute über mehr als 4 000 Mitglieder in 85 Ländern verfügt – darunter zahlreiche Großunternehmen auch aus Deutschland. Das BCI hat den Leitfaden »Good Practice-Richtlinien« für das Business Continuity Management veröffentlicht.[34] Demgemäß sollte das BCM-Konzept eines Unternehmens fünf Phasen umfassen:

Business Continuity Management

Phase 1: Das eigene Geschäft verstehen
- Organisationsstrategie – Welche Bereiche sind wichtig?
- Business Impact Analyse – Quantifizierung möglicher Störfälle
- Risikobeurteilung und –kontrolle – Wahrscheinlichkeit von Störfällen

Phase 2: BCM-Strategien
- Strategie für Organisationen/Unternehmen – Wer ist verantwortlich?
- Prozessebenenstrategie – Wechselwirkungen der Geschäftsprozesse
- Ressourcen-Wiederherstellungsstrategie

Phase 3: Entwicklung einer BCM-Reaktion
- Krisenmanagement, Öffentlichkeitsarbeit und die Medien
- Business Continuity-Pläne – Reaktionsmuster vordefinieren
- Wiederaufnahmepläne für die Unternehmensbereiche

Phase 4: Entwicklung einer BCM-Kultur
- Beurteilung der BCM-Awareness
- Entwicklung und Umsetzung einer BCM-Kultur
- Ergebnismessung und Überwachung des kulturellen Wandels

Phase 5: Übungen, Pflege und Audit
- Übung von BCM-Plänen
- BCM-Pflege – Anpassungen an sich ändernde Rahmenbedingungen
- BCM-Audit – Unabhängige Überprüfung

Die am Beginn dieses Abschnitts skizzierten Beispiele signalisieren, dass ein Kontinuitätsmanagement im Eigeninteresse der Unternehmen liegt, denn es hilft, die wirtschaftlichen Risiken des Unternehmens im Ernstfall zu reduzieren. Ein wirksames Kontinuitätsmanagement kann aber auch ein Wettbewerbsvorteil sein, weil gegenüber Geschäftspartnern die Leistungsfähigkeit auch in Krisensituationen demonstriert werden kann. Das Business Continuity Institute bietet Zertifizierungen an, mit denen Unternehmen ihre BCM-Aktivitäten

34 Vgl. BCI – The Business Continuity Institute (2005).

dokumentieren können.[35] Schließlich scheint sich ein funktionierendes Kontinuitätsmanagement auch auf den Börsenwert eines Unternehmens auszuwirken. Studien haben ergeben, dass ein erfolgreiches Krisenmanagement und die Aktienkursentwicklung der Unternehmen positiv korreliert sind.[36]

Neben dem Eigeninteresse des Unternehmens, die Produktionsprozesse und den Geschäftsbetrieb gegen Störfälle abzusichern, gibt es Verordnungen und gesetzliche Vorgaben, die von bestimmten Unternehmen erfüllt beziehungsweise beachtet werden müssen. Für Kreditinstitute sind die Mindestanforderungen an das Risikomanagement (MaRisk) maßgeblich. Die MaRisk ist die verbindliche Vorgabe der Bundesanstalt für Finanzdienstleistungsaufsicht für die Ausgestaltung des Risikomanagements in deutschen Kredit- und Finanzdienstleistungsinstituten.[37] Das Notfallkonzept wird dort im Abschnitt AT 7.3 geregelt.

Notfallkonzept gemäß MaRisk

1) Für Notfälle in zeitkritischen Aktivitäten und Prozessen ist Vorsorge zu treffen (Notfallkonzept). Die im Notfallkonzept festgelegten Maßnahmen müssen dazu geeignet sein, das Ausmaß möglicher Schäden zu reduzieren. Die Wirksamkeit und Angemessenheit des Notfallkonzeptes ist regelmäßig durch Notfalltests zu überprüfen. Die Ergebnisse der Notfalltests sind den jeweiligen Verantwortlichen mitzuteilen. Im Fall der Auslagerung von zeitkritischen Aktivitäten und Prozessen haben das auslagernde Institut und das Auslagerungsunternehmen über aufeinander abgestimmte Notfallkonzepte zu verfügen.
2) Das Notfallkonzept muss Geschäftsfortführungs- sowie Wiederanlaufpläne umfassen. Die Geschäftsfortführungspläne müssen gewährleisten, dass im Notfall zeitnah Ersatzlösungen zur Verfügung stehen. Die Wiederanlaufpläne müssen innerhalb eines angemessenen Zeitraums die Rückkehr zum Normalbetrieb ermöglichen. Die im Notfall zu verwendenden Kommunikationswege sind festzulegen. Das Notfallkonzept muss den beteiligten Mitarbeitern zur Verfügung stehen.

Quelle: Bundesanstalt für Finanzdienstleistungsaufsicht (2007).

Ein effektives Business Continuity Management liegt im Eigeninteresse der Unternehmen, denn es trägt dazu bei, dass bei Störungen des Geschäftsbetriebes die Schäden in Grenzen gehalten werden. Die damit verbundenen Kosten sind mit Versicherungsprämien vergleichbar. Gleichwohl sind nicht alle Unternehmen in der Lage, ein angemessenes Business Continuity Management zu praktizieren. Kleine Unternehmen können im Prinzip nur einen Basisschutz für die Risiken mit der höchsten Wahrscheinlichkeit herstellen. Dazu gehört etwa die Absicherung gegen IT-Risiken. Es lässt sich aber für die kleineren Unternehmen vielfach nicht vermeiden, weitgehend ungeschützt mit bestimmten Risiken zu leben.

Kasten 8

35 Das Bundesamt für Sicherheit in der Informationstechnik (BSI) vergibt ein IT-Grundschutz-Zertifikat, mit dem Unternehmen und Behörden ihre Bemühungen auf dem Gebiet der IT-Sicherheit international dokumentieren und transparent machen können. Vgl. dazu die Webseite des BSI: http://www.bsi.bund.de/index.htm
36 Vgl. BCI – The Business Continuity Institute (2005), S. 6 und S. 51.
37 Vgl. Bundesanstalt für Finanzdienstleistungsaufsicht (2007).

6. Die Sicherheitsindustrie aus Anlegersicht

Wir hatten die Sicherheitsindustrie eingangs als einen Markt im Entstehen beschrieben. Tatsächlich trägt er typische Charakteristika eines Emerging Market. Das betrifft vor allem die Marktreife. Vieles befindet sich noch im Stadium einer frühen Entwicklung, insbesondere was einige Segmente der Homeland Defense anbelangt. Folglich gibt es eine Vielzahl von eher kleineren Nischenspielern, die ihren Ursprung oftmals in Abspaltungen von Großunternehmen der Hard- und Softwarebranche oder von Telekommunikations-Gesellschaften hatten beziehungsweise sich aus Mitarbeiterkreisen von Geheimdiensten gebildet haben. Hier besteht nur in wenigen Fällen eine Börsennotierung, sodass sie aktuell am ehesten für Private Equity-Gesellschaften interessant sein könnten.

Daneben hat sich jedoch eine Reihe hochkarätiger Markttreiber mit einer entsprechend langen Kapitalmarkthistorie etabliert. Im Vordergrund stehen naturgemäß die USA als Mutter der Homeland Defense. Hier gibt es einige, unterschiedlich abgegrenzte Branchenindizes, die mit entsprechenden Fonds- und Indexzertifikaten unterlegt sind. Wir nennen stellvertretend den global aufgestellten Mallon Global Security Index. Er umfasste im Sommer 2008 mehr als 170 Unternehmen.

Einen stärkeren Fokus auf die jeweiligen Marktführer legt der ISE-CCM Homeland Security Index. Er hat in den vergangenen Jahren eine außerordentlich positive Entwicklung aufzuweisen. Im Vergleich zum S&P 500 gelang ab dem Jahr 2000 eine doppelt so hohe Wertsteigerung. Im Sommer 2008 setzte sich der Index aus folgenden 20 Unternehmen zusammen (Reihung nach Indexgewichtung):

1. Symantec Corp.
2. Thermo Fisher Scientific
3. L-3 Communication
4. Flir Systems
5. SAIC Inc.
6. Zebra Tech.
7. STERIS Corp.
8. McAfee
9. Mantech Intern.
10. Harris Corp.
11. Unisys
12. SRA Intern.
13. Mine Safety Appl.
14. Tetra Tech
15. Websense Inc.
16. L-I Identity Solutions
17. Taser Intern.
18. OSI Systems
19. Secure ComputingCorp.
20. SI Intern.

Einen anderen Ansatz verfolgt wiederum der Mitte 2007 kompilierte SGI Global Security Index. Er bezieht auch Unternehmen der klassischen Sicherheitsindustrie, also aus Gebäude- und Personenschutz, mit ein. In ihm sind stets 30 Unternehmen enthalten. Auch seine Wertentwicklung verläuft zumindest aus der Sicht eines Euro-Anlegers und im Vergleich zum DJ EuroSTOXX 50 positiv.

ISE-CCM Homeland Security Index vs. S&P (rebasiert auf 100)

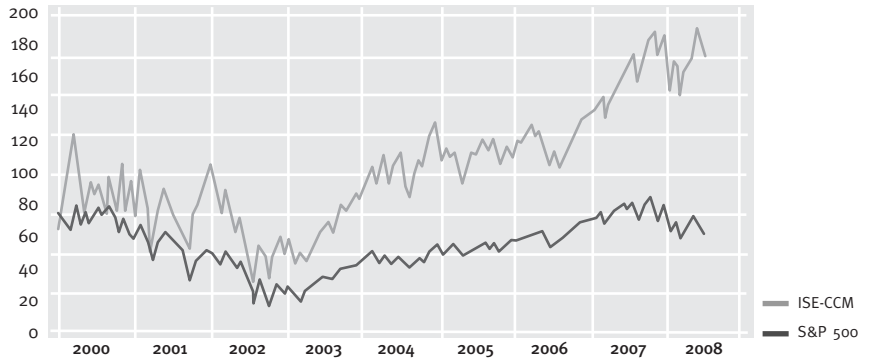

Abb. 26 Quelle: Bloomberg

SGI Global Homeland Security Index vs. DJ EuroStoxx 50 (rebasiert auf 100)

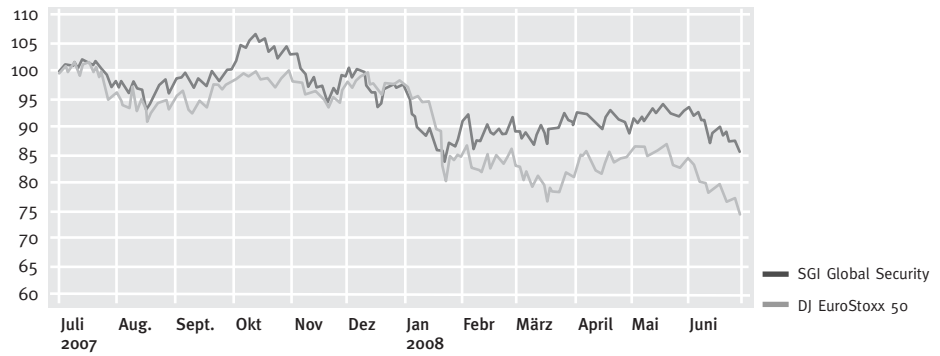

Abb. 27 Quelle: Bloomberg

Die Überschaubarkeit der verfügbaren Kapitalmarktinstrumente werten wir als starken Hinweis darauf, dass das Investmentthema Sicherheitsindustrie bei breiten Anlegerschichten noch nicht angekommen ist. Dabei sprechen die hervorragenden langfristigen Wachstumsperspektiven für dauerhaft stabile Wertsteigerungen.

Aus Anleger- und Investorensicht bietet nicht zuletzt die deutsche Sicherheitsbranche interessante Perspektiven. Bereits heute ist Deutschland bei einer Vielzahl von Basistechnologien gut positioniert. Laut BMBF sind dies unter anderem die Bereiche Mikrosystemtechnik, Informations- und Kommunikationstechnologien, optische Technologien, Anlagen- und Reaktorsicherheit, Bautechnik, Biotechnologie und Sensorik. Angesichts der beschriebenen Förderung von Sicherheitstechnologien dürfte die Branche zu den Gewinnern der kommenden Dekaden zählen. So ist zu erwarten, dass die bereits vorhandenen Kernkompetenzen in vielen innovativen, hochtechnologischen Bereichen gezielt ausgebaut werden. Damit sollten die Chancen gerade für deutsche Unternehmen gut stehen, die Technologieführerschaft in spezifischen Sicherheitstechnologien übernehmen zu können.[38]

38 Vgl. Bundesministerium für Bildung und Forschung (2007 a).

Dies eröffnet vielversprechende Perspektiven für ein breites Spektrum an deutschen beziehungsweise international tätigen Unternehmen, wie beispielsweise Bosch Sicherheitssysteme, Dräger, Panasonic (Netzhaut-Untersuchung), Rheinmetall, Siemens oder Tyco, ebenso wie für eine Reihe von kleineren Spezialanbietern wie zum Beispiel Funkwerk (mobile Kommunikationssysteme), Gemplus (Chipkarten / Zugangskontrollen) oder Smartrac (RFID-Technologie).

Für das Segment Sicherheitsdienste sind unter anderem Unternehmen wie Securitas als weltweit größter Anbieter sowie Brink's, Chubb, Group 4 Securicor, Générale de Protection Europe, Protection One zu nennen.[39]

Fazit:

Die Sicherheitsbranche kann ganz eindeutig als Zukunftsbranche identifiziert werden. Die Anlagechancen konzentrieren sich auch diesmal wieder auf die Thematik Technologie und ergänzen damit die bereits in früheren Untersuchungen dieser Studienreihe gewonnenen Erkenntnisse.[40]

Neben den etablierten Marktsegmenten Sicherheitsdienstleistungen, elektronische Sicherheitssysteme und Sicherheit von Information und Kommunikation werden unter anderem die Bereiche biometrische Sensorsysteme und Sensoren, unbemannte Fahrzeuge sowie die Authentifizierung von Personen eine zunehmende Rolle spielen.

Dies wird Anlegern viele Chancen eröffnen, sei es über Einzelwerte oder, wie beschrieben, über Indexzertifikate oder Themenfonds.

39 Bei den genannten Unternehmen handelt es sich um keine Empfehlungen, lediglich um einige Beispiele für Unternehmen, die neben vielen anderen in diesem Bereich tätig sind.
40 Vgl. hierzu insbesondere Berenberg Bank/HWWI (2006 b); Berenberg Bank/HWWI (2006 c).

Literatur- und Quellenverzeichnis

Teil A

Abadie, A. (2006): Poverty, political freedom and the roots of terrorism, in: American Economic Review 96 (2), S. 50–56.

Abadie, A. & Gardezabal, J. (2007): Terrorism and the world economy, working paper August 2007.

Abadie, A. & Gardezabal, J. (2003): The Economic Costs of Conflict: A Case Study of the Basque Country, in: American Economic Review 93 (1), S. 113–132.

Anderson, R. (2001): Why Information Security is Hard – An Economic Perspective, University of Cambridge.

Anderson, R. & Moore, T. (2006): The Economics of Information Security, University of Cambridge.

Becker, G. (1968): Crime and Punishment: An Economic Approach, in: The Journal of Political Economy 76, S. 169–217.

BERR Department for Business Enterprise & Regulatory Reform (2008): Information Security Breaches Survey.

Bram, J. & Orr, J. & Rapaport, C. (2002): Measuring the effects of the September 11 attack on New York City, in: Groshen, E. L. (ed.): The Economic Effects of September 11, Vol. 8 of Economic Policy Review, Federal Reserve Bank of New York.

Brannan, D. & Chalk, P. & Cragin, K., &. Daly, S. (2003): The MIPT terrorism annual 2002, National Memorial Institute for the Prevention of Terrorism.

Bundesamt für Sicherheit in der Informationstechnik (2007): Die Lage der IT-Sicherheit in Deutschland 2007, Bonn.

Bundesamt für Sicherheit in der Informationstechnik (2006): Jahresbericht 2005, Bonn.

Bundeskriminalamt, Kriminalistisches Institut (2007): Polizeiliche Kriminalstatistik Bundesrepublik Deutschland, Berichtsjahr 2006, Wiesbaden.

Bundesministerium des Innern, Bundesministerium der Justiz (2006): Zweiter Periodischer Sicherheitsbericht, Berlin.

Bundesministerium des Innern, Bundesministerium der Justiz (2007): Zweiter Periodischer Sicherheitsbericht, Berlin.

Computer Crime Research Center (2005): www.crime-research.org/news/06.07.2005/1344/.

Crenshaw, M. (2007): The organization of terrorism, in: MIPT (Hrsg.): Terrorism – What's coming – The mutating threat, Oklahoma.

Croissant, A. & Schwank, N. (2006): Violence, Extremism and Transformation, Bertelsmann Transformation Index 2006 Findings, in: Bertelsmann Stiftung (Hrsg.): Violence, Extremism and Transformation, Gütersloh.

Deloitte, D. (2006): Protecting the digital assets, in: The 2006 Technology, Media & Telecommunications Security Survey, London.

Deutscher Wetterdienst (2005): Klimastatusbericht 2005.

Dittmann, J. (2005): Entwicklung der Kriminalitätseinstellung in Deutschland – Eine Zeitreihenanalyse anhand allgemeiner Bevölkerungsumfragen, Deutsches Institut für Wirtschaftsforschung (DIW), Discussion Paper Nr. 468, Berlin.

Edelmann, B. (2006): Adverse selection in online 'trust' certificates, in: Fifth Workshop on the Economics of Information Security.

Entorf, H. & Spengler, H. (2000): Socio-economic and demographic factors of crime in Germany: Evidence from panel data of the German states, in: International Review of Law and Economics 20, S. 75–106.

Entorf, H. & Spengler, H. (1998): Die Ökonomik der Kriminalität: Theoretische Hintergründe und empirische Evidenz, in: Wirtschaftswissenschaftliches Studium (WiSt), Vol. 27, Nr. 7, S. 348–353.

Eurostat (2008): www.epp.eurostat.ec.europa.eu.

Heinz, W. (2007): Wie sicher lebt man in Deutschland? Fakten zur Kriminalitätslage und Folgerungen für eine wissensbasierte Kriminalpolitik: http://www.uni-konstanz.de/rtf/kis/Heinz_Wie_sicher_lebt_man_in_Deutschland_he310.pdf.

Heinz, W. (2004): Kriminalität von Deutschen nach Alter und Geschlecht im Spiegel von Polizeilicher Kriminalstatistik und Strafverfolgungsstatistik: http://www.uni-konstanz.de/rtf/kik, Stand 6/2004.

Hobijn, B. & Sager, E. (2007): What has homeland security cost? An assessment: 2001-2005, in: Current Issues, Vol. 13, No. 2, Federal Reserve Bank of New York.

Internationaler Währungsfonds (IMF) (2001): World Economic Outlook December 2001: The Global Economy After September 11, World Economic and Financial Surveys, Washington D.C.

KES – Die Zeitschrift für Informations-Sicherheit (2006): Lagebericht zur Informationssicherheit, KES-Microsoft-Sicherheitsstudie, Gau-Algesheim.

Krueger, A. B. & Maleckova, J. (2002): Education, poverty, political violence and terrorism: Is there a causal connection?, NBER Working Paper No. 9074.

Lal, R. & Jackson, B. A. & Chalk, P. & Ali, F. & Rosenau, W. (2006): The MIPT terrorism annual 2006, National Memorial Institute for the Prevention of Terrorism.

McAfee (2005): Bericht von McAfee zur virtuellen Kriminalität.

MIPT (2006): The MIPT terrorism annual 2006, National Memorial Institute for the Prevention of Terrorism.

Nanto, D. N. (2004): 9/11 terrorism: Global economic costs, CRS Report for Congress.

OECD Broadband Portal http://www.oecd.org/sti/ict/broadband.

Oertel, B. & Wölk, M. (2006): Anwendungspotenziale »intelligenter« Funketiketten, in: Aus Politik und Zeitgeschichte (APuZ) 5–6, S. 16–23.

PC-WELT (2007): Phisher erleichtern US-Verbraucher um Milliarden, 18.12.2007, http://www.pcwelt.de/start/sicherheit/sonstiges/news/1850964/phisher_erleichtern_us_verbraucher_um_milliarden/.

Statistisches Bundesamt (2007): Rechtspflege – Ausgewählte Zahlen für die Rechtspflege, Fachserie 10, Reihe 1, Wiesbaden.

Statistisches Bundesamt (2005): Finanzen und Steuern, Fachserie 14, Reihe 3.1, Wiesbaden.

Symantec Corporation (2008): Symantec Global Internet Security Threat Report, Trends for July–December, Cupertino (Kalifornien, USA).

United Nations Development Programme (2007): Human Development Report 2007/2008, Palgrave Macmillan, New York.

United Nations Development Programme (2003): Human Development Report 2003/2004: http://hdr.undp.org/en/media/hdr04_complete.pdf.

United Nations Office of Drugs and Crime 2003/2004: http://hdrstats.undp.org/indicators/147.html.

U.S.-Canada Power System Outage Task Force (2004): Final Report on the August 14, 2003 blackout in the US and Canada.

Varian, H. (2000): Managing online security risks, in: The New York Times vom 1.6.2000.

Weltbank (2002): Fifteen Months – Intifada, Closures and Palestinian Economic Crisis, An Assessment, Washington D.C.

World Urbanization Prospects (2007): Economic and Social Affairs, UN.

X-Force (2007): IBM Internet Security Systems 2006, Trend Statistics.

Zentrum für Umfragen, Methoden und Analysen (ZUMA) e.V. (2005): Informationsdienst Soziale Indikatoren, Ausgabe 34, Mannheim.

Zentrum für Umfragen, Methoden und Analysen (ZUMA) e.V. (2001): Die Wohlfahrtssurveys 1978–1998, Zeitreihendaten zur Wohlfahrtsentwicklung in der Bundesrepublik Deutschland, Mannheim.

Teil B

BCI – The Business Continuity Institute (2005): Business Continuity Management – Good Practice-Richtlinien.

Berenberg Bank & HWWI (2006 a): Maritime Wirtschaft und Transportlogistik, Band A, S. 62–63.

Berenberg Bank & HWWI (2006 b): Maritime Wirtschaft und Transportlogistik, Band B, S. 21–24.

Berenberg Bank & HWWI (2006 c): Klimawandel, S. 81–85.

Bundesanstalt für Finanzdienstleistungsaufsicht (2007): Rundschreiben 5/2007 (BA) – Mindestanforderungen an das Risikomanagement – MaRisk.

Bundesdruckerei (2007): A Bundesdruckerei Pocket Guide to Border Control, Bundesdruckerei, Berlin.

Bundesministerium für Bildung und Forschung (2007 a): Sicherheitstechnologien: Keine Chance für Kriminalität und Terrorismus.

Bundesministerium für Bildung und Forschung (2007 b): Forschung für die zivile Sicherheit – Eine Bestandsaufnahme, Berlin.

Bundesministerium für Bildung und Forschung (2007 c): Forschung für die zivile Sicherheit – Programm der Bundesregierung, Berlin.

Civitas Group (2006): The Homeland Security Market Essential Dynamics and Trends.

Deloitte (2007): Global Security Survey – The shifting security paradigm.

Europäische Union (2005): Richtlinie 2005/60/EG des europäischen Parlaments und des Rates vom 26.10.2005, in: Amtsblatt der Europäischen Union, L 309/15.

Fraunhofer-Gesellschaft (2007): Hightech-Strategie für Deutschland: Sicherheitstechnologien, München.

Fraunhofer-Gesellschaft (2005): Perspektiven für Zukunftsmärkte – Erfolg mit Innovationen auf internationalen Märkten, München.

Fredonia Group (2006): World Security Services to 2010.

Gawrych, P. (2008): Flugroboter, FH Dortmund, Fachbereich Informatik.

Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (2007): Geldwäschegesetz – GwG vom 25.10.1993 (BGBl. I S. 1770), zuletzt geändert durch Artikel 5 des Gesetzes vom 21.12.2007 (BGBl. I S. 3089).

Höche, T. (2002): Neue gesetzliche Regelungen zur Bekämpfung des Terrorismus und der Geldwäsche, in: Die Bank, 3/2002, S. 196–202.

Homeland Security Research Corporation (2005): Homeland Security / Homeland Defense – Global Market Outlook – 2006–2015.

Internationaler Währungsfonds (2003): Jahresbericht 2003, S. 32.

IW-Consult (2006): Bürokratiekosten in der Kreditwirtschaft.

Müller, K.-R. (2008): IT-Sicherheit mit System, 3. Auflage, Vieweg.

PriceWaterhouseCoopers (2007): Wirtschaftskriminalität 2007 – Sicherheitslage der deutschen Wirtschaft.

Utzig, S. (2007): Die Last wird sichtbar, in: Die Bank, 2/2007, S. 36–38.

Wegweiser GmbH (2004): Investitionen und Innovationen – Deutschland 2006.

Webseiten:

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2008): IT-Grundschutz-Zertifikat, [http://www.bsi.bund.de/literat/faltbl/F11Grundschutzzertifikat.htm].

Fraunhofer-Institut Produktionstechnik und Automatisierung (o. J.), [www.ipa.fraunhofer.de].

innovations-report (o. J.): Forum für Wissenschaft, Industrie und Wirtschaft, [www.innovations-report.de].

Rheinmetall (o. J.), [www.rheinmetall-ag.com].

Security Park (o. J.): The leading News portal for Security professionals, [www.securitypark.co.uk].

In der Reihe
»Strategie 2030 – Vermögen und Leben in der nächsten Generation«
sind bislang folgende Studien erschienen:

1 **Energierohstoffe**

2 **Ernährung und Wasser**

3 **Immobilien**

4 **Maritime Wirtschaft und Transportlogistik** (Band A und B)

5 **Klimawandel**

6 **Wissen**

Diese Studien stehen Ihnen auf der Homepage www.berenberg.de
unter dem Punkt »Publikationen« als Download zur Verfügung.