Arbeitsgemeinschaft für Sicherheit der Wirtschaft e.V.

Anmerkungen zur Sicherheitslage

der deutschen Wirtschaft

2003/2004

ASW
Arbeitsgemeinschaft für Sicherheit der Wirtschaft e.V.
Haus der Deutschen Wirtschaft
Breite Str. 29

10178 Berlin

Tel.: 030-20308 1513
Fax: 030-20308 1581

eMail: asw@berlin.dihk.de
Internet: www.asw-online.de

Berlin, im Oktober 2004

Einleitung

Mit den nachfolgenden Anmerkungen zur Sicherheitslage der deutschen Wirtschaft will die ASW Unternehmer und ihre Sicherheitsverantwortlichen zusammenfassend über Bedrohungsphänomene unterrichten und diese veranlassen, über mögliche Schwachstellen im Sicherheitssystem des Unternehmens nachzudenken. Zugleich möchte die ASW damit die Öffentlichkeit darüber informieren, welchen kriminellen Angriffen die Wirtschaft ausgesetzt ist, welcher Schaden betriebswirtschaftlich und volkswirtschaftlich entsteht und was getan werden muss, um diese Risiken und Schäden einzudämmen. Auch Politikern muss immer wieder verdeutlicht werden, dass die Wirtschaft ein Teil der Gesellschaft ist, den zu schützen Aufgabe des Staates bleibt. Es ist ferner ein Anliegen der ASW mittels dieses Berichts, Entscheidungsträger in den Sicherheitsbehörden und den Nachrichtendiensten auf das hohe Informationsinteresse der Sicherheitsverantwortlichen in Unternehmen hinzuweisen, dass auf Veränderungen der Sicherheitslage, Veränderungen in der Täterstruktur und vor allem Veränderungen im Modus operandi konzentriert ist.

Die hohen Schäden, die Kriminalität den Unternehmen zufügt, gehen nicht nur zu Lasten der Unternehmen. Sie kosten Arbeitsplätze, schädigen den Fiskus, letztlich auch den Steuerzahler und Konsumenten, und sie stellen je nach Branche und Region auch eine ernsthafte Gefahr für den Wirtschaftsstandort Deutschland dar.

Grundlagen dieser Anmerkungen sind neben der Polizeilichen Kriminalstatistik:

- Berichte der Bundessicherheitsbehörden, also des Bundeskriminalamts (BKA), des Bundesamtes für Verfassungsschutz (BfV), des Bundesnachrichtendienstes (BND), des Bundesamtes für Sicherheit der Informationstechnik (BSI), des Zollkriminalamts (ZKA), punktuell auch Berichte von Polizei- und Verfassungsschutzbehörden der Länder

- Erhebungen und Analysen wissenschaftlicher Institute

- Fachpublikationen und Presseberichte.

Ein so mosaikartig zusammengesetztes Lagebild erhebt keinen Anspruch auf systematische Erfassung und Vollständigkeit. Sein Wert liegt eher in einer zielgerichteten Zusammenfassung vielseitiger Informationsquellen.

Gliederung

Einleitung

1 Zusammenfassung

1.1 Kriminalitätsbelastung wird nicht abnehmen

Die in diesem Lagebild dargestellte Entwicklung der die Wirtschaft belastenden Kriminalität zeigt, dass die Unternehmen auch in Zukunft mit beträchtlichen kriminellen Bedrohungen und Schäden rechnen müssen. Der Wertewandel hin zu Konsum- und Anspruchsdenken, Verlust an sozialen Bindungen, mehr Polarisierung der Gesellschaft, verbunden mit einer Abnahme gesellschaftlicher Solidarität, Offenheit der Grenzen, mangelnde Integration von Ausländern, Ghettobildungen am Rande und in Großstädten – um nur einige ungünstige Rahmenbedingungen zu nennen – legen den Schluss nahe, dass die Kriminalitätsbelastung wie seit dem Jahr 2000 auch in den folgenden Jahren trotz aller Anstrengungen der Kriminalitätsbekämpfung nicht insgesamt zurückgehen wird.

Ohne den Anspruch einer fundierten Prognose erheben zu können, lässt sich für einige Deliktsbereiche folgende weitere Entwicklung abschätzen, wenn man die in der PKS sichtbare Tendenz der letzten 10 Jahre in die Zukunft projiziert:
Quantitativ eher abnehmen werden der Bank- und Geschäftsraub, der schwere Diebstahl insgesamt, der Unternehmensdiebstahl, der Hotel- und Gaststättendiebstahl und der ermittelte Ladendiebstahl.
Zunehmen dürften dagegen die Vermögens- und Fälschungskriminalität insgesamt, insbesondere der Waren- und Warenkreditbetrug und der Betrug mittels rechtswidrig erlangter unbarer Zahlungsmittel, Veruntreuungen, Teilbereiche der Wirtschaftskriminalität und insbesondere die Computerkriminalität.

Die Entwicklung der Wirtschaftskriminalität prognostiziert das BKA im Bundeslagebild 2003 wie folgt:
Wegen der gegenwärtigen allgemeinen wirtschaftlichen Entwicklung, der gesamtwirtschaftlichen Lage, der EU-Osterweiterung und der Globalisierung ist damit zu rechnen, dass Straftaten im Deliktsfeld „Wirtschaftskriminalität“ weiter zunehmen werden. Gerade der durch die Globalisierung auch in Deutschland festzustellende Strukturwandel zieht starke Veränderungen der wirtschaftlichen und rechtlichen Rahmenbedingungen nach sich.
Wirtschaftsstraftäter machen sich diese Entwicklung zunutze und spüren u.a. sich ergebende Gesetzeslücken auf. Die sich immer schneller fortentwickelnde Technik bietet zusätzliche Möglichkeiten der Tatbegehung und Konspiration. Insbesondere die moderne Informationstechnik bietet eine Plattform, um ortsunabhängig und mit größtmöglicher Anonymität agieren zu können. Je mehr die Täter sich diese Technik zu Eigen machen, umso lukrativer werden die Straftaten, umso sicherer fühlen sie sich und umso mehr werden die Straftaten im Zusammenhang mit dem Wirtschaftsleben ansteigen.

Die konjunkturellen Aussichten in Deutschland und die teilweise für den Einzelnen mit massiven finanziellen Einschnitten verbundenen Reformen, unklare Perspektiven für die Zukunft, aber auch bezüglich der sich aufgrund der EU-Osterweiterung bietenden Chancen und Risiken führen zu Verunsicherungen in der Bevölkerung. Insbesondere am Beispiel der Insolvenzdelikte wird die Abhängigkeit zwischen der wirtschaftlichen Lage und der Wirtschaftskriminalität deutlich.

1.2 Empfehlungen an die Unternehmen

- Im Hinblick auf die zahlreichen kriminellen Bedrohungen, denen die Wirtschaft auch in Zukunft ausgesetzt sein wird, bittet die ASW die Unternehmensführungen, in ihren Anstrengungen zum Schutz der Unternehmen und ihrer Beschäftigten vor kriminellen Gefahren nicht nachzulassen und auch in wirtschaftlich schwierigen Zeiten die dafür erforderlichen Mittel bereitzustellen.

- Soweit Aufgaben des Unternehmensschutzes Dienstleistern übertragen werden, sollte darauf geachtet werden, dass die Auftragsvergabe auf der Grundlage der **DIN-Norm 77200** erfolgt und die in der Norm enthaltenen Qualitätsanforderungen eingehalten werden.

- Nach der bevorstehenden Umsetzung der neuen Eigenkapitalanforderungen des Baseler Ausschusses für Bankenaufsicht („Basel II“) ist eine Schwachstellenanalyse erforderlich, ob das in der Regelung geforderte Risk Management auch im Safety- und Security-Bereich ausreichend ist.

- Nachdem durch die Terrorismusgesetzgebung im Jahr 2002 die Möglichkeit geschaffen wurde, Beschäftigte in sicherheitsempfindlichen Funktionen lebens- oder verteidigungswichtiger Einrichtungen (Betriebsteile) einer Sicherheitsüberprüfung zu unterziehen, sollten Unternehmen diese auch als Chance begreifen und der gesetzlichen Pflicht nachkommen.

- Der Bankraub könnte noch erfolgreicher bekämpft werden, wenn alle Geldinstitute ihre Videoüberwachungsanlagen zur Polizei aufschalten, damit bei einem Überfall die dann übertragenen Bilder in Echtzeit ausgewertet und die Ergebnisse den anrückenden polizeilichen Einsatzkräften übermittelt werden. Die standardisierte technische Übermittlungsfähigkeit muss hierzu jedoch beidseitig vorliegen.

- Die Sicherheitsregeln für Geldtransportfahrzeuge sind ausnahmslos einzuhalten, Zuverlässigkeit und Integrität des mit Werttransporten betrauten Personals sind möglichst gründlich zu prüfen, damit Überfälle auf solche Transporte keine Chance haben.

- Kriminellen Angriffen sind Unternehmen nicht nur durch Außentäter ausgesetzt. Zur Abwehr von Betriebskriminalität sind alle angemessenen Kontrollmöglichkeiten zu nutzen. Stärkung der Loyalität der Mitarbeiter, ein gutes Betriebsklima und individuelle Betreuung der Beschäftigten sind die besten Präventionsmaßnahmen gegen Betriebskriminalität.

- Um Betriebsgeheimnisse, sensible Daten und wertvolles „Know-how“ zu schützen, müssen verschiedene Maßnahmen ergriffen werden und ineinander greifen. Dazu gehört die Entwicklung eines Frühwarnsystems, um Anzeichen für einen „Loslösungsprozess“ von „Know-how-Trägern“ rechtzeitig zu erkennen und gegenzusteuern, auch um etwaige Ursachen für die Unzufriedenheit solcher Mitarbeiter ausräumen zu können.

- Die ASW empfiehlt dem Einzelhandel, soweit er die Benutzung von Debitkarten ohne PIN akzeptiert, grundsätzlich den Personalausweis zu kontrollieren und die Notwendigkeit der Ausweiskontrolle anzukündigen. Die Umstellung auf Identifikation mittels PIN ist jedoch der bessere und sichere Weg.

- Je wichtiger Informations- und Kommunikationssysteme für die Wirtschaft sind, umso mehr Sorgfalt müssen die Unternehmen darauf verwenden, diese Systeme gegen Hacker, Viren und Würmer abzusichern und ihre permanente Verfügbarkeit zu gewährleisten. Auch von der elektronischen Signatur wird viel zu wenig Gebrauch gemacht.

1.3 Anliegen an Staat und Politik

Die ASW äußert im Zusammenhang mit den Inhalten dieses Sicherheitslageberichts gegenüber dem Staat, den politisch verantwortlichen Stellen und den Sicherheitsbehörden folgende Anliegen:

- Im Hinblick auf die anhaltende Bedrohung durch den internationalen Terrorismus und auf die nun schon im dritten Jahr in Folge wieder leicht steigende Kriminalität muss die Innere Sicherheit in der Innenpolitik von Bund und Ländern weiterhin einen Schwerpunkt bilden.

- Public Private Partnership muss auch im Sicherheitsbereich wesentlich verstärkt werden. Privatisierungen von Sicherheitsfunktionen ohne hoheitliche Befugnisse können zu erheblichen Kostenreduzierungen bei höheren Leistungsergebnissen infolge flexiblerer Arbeitszeitgestaltung und effektiverem Management führen.

- Die leichte Verbesserung der Konjunktur beruht im Wesentlichen auf Exporterfolgen der deutschen Wirtschaft. Um Niederlassungen deutscher Unternehmen in Krisenregionen vor terroristischen Angriffen und anderen kriminellen Bedrohungen möglichst zu schützen, sind die Sicherheitsverantwortlichen der Unternehmen auf die rechtzeitige Übermittlung von Lage- und Gefährdungsinformationen und auch auf die Unterstützung durch deutsche diplomatische Vertretungen in diesen Ländern angewiesen. Die ASW bittet die Bundesregierung, wie bisher diese Unterstützung zu gewährleisten und weiter zu intensivieren.

- Die deutsche Wirtschaft erleidet durch Marken- und Produktpiraterie hohe Schäden. Die ASW ersucht die Bundesregierung, in Verhandlungen mit Regierungen der Staaten, die bekanntermaßen die Produktpiraterie nicht ausreichend wirksam bekämpfen, ein stärkeres Engagement zu verlangen. Um das zu erreichen, müssen gegebenenfalls auch angemessene wirtschaftliche Druckmittel eingesetzt werden.

- Das BKA beklagte schon im Lagebericht Wirtschaftskriminalität 2002 eine zu geringe Intensität kriminalpolizeilicher Bekämpfung der Produktpiraterie. Die ASW fordert, diese Intensität zu verstärken, und mahnt eine stärkere Bündelung der Kompetenzen an.

- Die begrüßenswerte Erweiterung der EU durch mittel- und osteuropäische Staaten darf nicht zu verstärktem Kriminalitätsimport infolge des Wegfalls von Grenzkontrollen führen. Die Bundesregierung muss daher auch weiterhin sorgfältig prüfen, ob die neuen EU-Mitglieder die normierten Ausgleichsmaßnahmen für den Wegfall von Grenzkontrollen vollständig und nachhaltig durchführen und, soweit nötig, darauf drängen, dass ihre Sicherheitsbehörden mit den deutschen Sicherheitsbehörden bei der Kriminalitätsbekämpfung eng zusammen arbeiten.

- Kriminalität im Zusammenhang mit dem Arbeitsrecht schädigt den fairen Wettbewerb und fügt auch dem Staat großen Schaden zu. Die ASW bittet die Bundesregierung, das vom Bundestag beschlossene Gesetz zur Bekämpfung der Schwarzarbeit zügig und nachhaltig umzusetzen.

- Die Sicherheit der Informations- und Kommunikationssysteme gewinnt für die Wirtschaft von Jahr zu Jahr an Bedeutung. Die ASW bittet das BMI, in Kooperation mit dem BMWA diesem Aufgabenbereich weiterhin einen hohen Rang einzuräumen und das Verfahren zum Erlass des Gesetzes über Rahmenbedingungen für elektronische Signaturen möglichst zu beschleunigen, damit sich die elektronische Signatur mehr als bisher durchsetzt. Sie bittet das Bundesamt für Sicherheit der Informationstechnik, wie bisher die Interessen der Wirtschaft durch Gefährdungshinweise, Informationen und Beratung umfassend zu berücksichtigen.

- Die ASW kann ihrer Aufgabe, die Unternehmen rechtzeitig und umfassend mit Informationen der Sicherheitsbehörden über neue Kriminalitätsentwicklungen und Begehungsformen, mit Gefährdungshinweisen und Empfehlungen zur Kriminalitätsprävention nur gerecht werden, wenn ihr solche Informationen von den Bundesministerien, den Sicherheitsbehörden und Nachrichtendiensten eigeninitiativ laufend zur Verfügung gestellt werden, Die ASW bittet die zuständigen Stellen, die Arbeit der ASW derart so intensiv wie möglich zu unterstützen.

- Die ASW wiederholt ihren Vorschlag, auf der Basis der Erfahrungen mit Sicherheitsforen zwischen Staat und Wirtschaft in mehreren Bundesländern auch auf Bundesebene eine solche Sicherheitspartnerschaft einzurichten.

2 Gefährdung der Wirtschaft durch Terrorismus und gewalttätigen Extremismus

Die Gefährdung der Wirtschaft durch den Terrorismus, vornehmlich den islamistischen Terrorismus, ist tief greifend und komplex. Über Opfer an Menschenleben hinaus fügt er der Wirtschaft vielfältigen Schaden zu: durch Einschränkungen der Mobilität und des Geschäftsverkehrs, durch Bindung von personellen und finanziellen Ressourcen, die für Schutzmaßnahmen in Deutschland, aber vor allem bei Niederlassungen in Krisengebieten gebraucht werden, und durch das Schüren von Ängsten, die zur Zurückhaltung im Konsum und bei Investitionen führen.

Nach einem Bericht des State Department der USA wurden im Jahr 2003 weltweit 208 Terrorakte verübt, die 625 Tote und 3.646 Verletzte forderten. 2002 waren es 725 Tote und 1.593 Verletzte.

Weiterhin behalten die bereits in 2003 dargestellten potenziellen Angriffsziele und Angriffszenarien in Deutschland ihre Gültigkeit.

Bezüglich der Angriffsziele in Deutschland sind dies:

1. US-amerikanische Ziele (diplomatisch, militärisch);
2. Britische Ziele (diplomatisch, militärisch);
3. Israelische Ziele (diplomatisch, kulturell);
4. Bundesstaatliche Ziele in Berlin;
5. Wirtschaftsstandorte mit hohem Symbolcharakter, sehr hohem wirtschaftlichem Störfaktor, Zivilopferpotenzial oder Panikfaktor;
6. Transportinfrastruktur mit sehr hohem Störfaktor, Zivilopferpotenzial oder Panikfaktor;
7. Schlüsseleinrichtungen der Energie- und Versorgungswirtschaft mit sehr hohem Störfaktor, Zivilopferpotenzial oder Panikfaktor.

2.1 Die globale Wirtschaft als Feindziel von Al Qaeda

Schon der bisher folgenschwerste terroristische Anschlag der Terrororganisation Al Qaeda am 11. September 2001 auf das World Trade Center in New York hat gezeigt, dass eines der Hauptziele der islamistischen Terroristen die globale Wirtschaft ist, als deren architektonisches Symbol die beiden Türme gewertet werden konnten. Die Erkenntnis, dass die arabische und islamische Welt weitgehend zu den ‚Verlierern' der Modernisierung der Weltwirtschaft und der Weltgesellschaft gehört, schürt die Wut auf den globalisierten Kapital-, Personen- und Warenverkehr. In einem kürzlich aufgefundenen Strategiepapier, das Sicherheitsexperten Al Qaeda zurechnen (DIE WELT v. 05.04.04), werden Angriffe auf „wirtschaftliche Ziele" grundsätzlich als sinnvoll zur Vertreibung „fremder Kräfte" aus islamischen Ländern angesehen. Wörtlich heißt es: „Einige dieser Operationen haben Auswirkung auf die wirtschaftlichen Kräfte wie etwa jene, die jüngst in Madrid stattfand, die die gesamte europäische Wirtschaft traf. Solche Angriffe haben doppelte wirtschaftliche Effekte auf die Kreuzfahrer, die Juden und islamische Renegaten-Staaten." Die Wertung des Todes des saudi-arabischen Al Qaeda-Chefs Al Muqrin als Märtyrertod dürfte den Inhalt des Strategiepapiers zusätzlich aufwerten. Es ist zu befürchten, dass den Anschlägen und Geiselnahmen in Saudi-Arabien nach der Veröffentlichung des Strategiepapiers Signalwirkung zukommt. Gefährdet erscheinen insbesondere Vertreter international tätiger Unternehmen, internationale Wirtschaftsberater und Wissenschaftler und ebenso die Investitionen aus sog. „feindlichen Ländern".

Eine Verschärfung der Bedrohungslage ist vor allem seit dem Irak-Krieg für global agierende Firmen eingetreten. Die Control Risks Group hat auf der jährlich erstellten „Risiken-Weltkarte“ die Zahl der Staaten mit einem mittleren Risiko von 58 auf 71 heraufgestuft. Unter ihnen befinden sich so wichtige Handelspartner wie die Türkei, Russland, Israel, Saudi-Arabien und Thailand.

2.2 Angriffe auf sog. weiche Ziele und kritische Infrastrukturen

Nicht nur „harte“ Ziele wie Militärbasen und Regierungsgebäude, sondern „weiche“ Ziele kritischer Infrastrukturen, vor allem der Flug-, Bahn- und Schiffsverkehr, wo besonders viele Menschen getroffen werden können, gehören zu den bevorzugten Angriffspunkten islamistischer Terroristen.

Das haben die Anschläge
- in Riad (am 12. Mai und 8. November 2003 und erneut am 22. Mai 2004)
- in Casablanca (am 16. Mai 2003)
- in Jakarta (am 5. August 2003)
- in Istanbul (am 15. und 20. November 2003) und vor allem jener
- in Madrid (am 11. März 2004) gezeigt.

Solche weichen Ziele zu schützen ist besonders aufwendig und schwierig bis unmöglich.

Nachdem Al Qaeda-Anhänger Ende Mai 2004 in Saudi-Arabien das Erdölzentrum al-Chobar angegriffen und 22 Ausländer getötet haben, gilt die Erdölindustrie mit ihrer gesamten Ölinfrastruktur als nahe liegendes Angriffsziel. Dabei ist der Schutz der Pipelines in ihrer Länge von vielen tausenden Kilometern durch personelle Maßnahmen kaum sinnvoll. Zunehmend werden insbesondere in Europa Alarmsysteme einschließlich Videoüberwachung eingesetzt. Während Pipelines in relativ kurzer Zeit wieder repariert werden können, sind Terminals, Transportwege und Häfen besonders schutzbedürftig. Das US-Energieministerium hält sechs Wasserstraßen für mögliche Terrorziele, darunter den Bosporus, ein Nadelöhr für den Schiffsverkehr, und die Straße von Hormuz am Persischen Golf. „Einige Wasserstraßen sind so eng, dass ein einziger brennender Supertanker die Route für andere Schiffe unpassierbar machen könnte“, heißt es in einem Report des Institute for the Analysis of Global Security in Washington.

Zu den vielfältigen Maßnahmen, die Betreiber von Flughäfen schon bisher durchführen mussten, um den besonders sensiblen Luftverkehr zu schützen, sind nach dem 11. September 2001 vor allem durch die Vorschrift 100prozentiger Gepäckkontrolle und durch die EU-VO 2320/2002 v. 16.12.2002 über das Erfordernis der Körper- und Gepäckkontrolle der Beschäftigten gekommen, bevor sie zu (national festzulegenden) sensiblen Teilen der Sicherheitsbereiche eines Flughafens Zutritt erhalten.

Zudem können die Betreiber internationaler Flughäfen zur Durchführung von Berechtigungskontrollen biometrische Verfahren einführen. Das wurde auch auf einer im April vom Deutschen Forum Kriminalprävention (DFK) veranstalteten Arbeitstagung betont. Eine zusammen mit dem ZVEI entwickelte Konzeption sieht über die biometrische Verifizierung der Berechtigung des Flughafenpersonals zum Betreten von Sicherheitszonen hinaus sogar den biometrisch gesicherten Flugpass vor. Die Wirtschaft wartet dringend auf die endgültige Entscheidung, welche biometrischen Daten Reisepässe enthalten sollen. Von dieser Entscheidung dürfte eine Anstoßwirkung auf die breitere Verwendung biometrischer Systeme in der Wirtschaft ausgehen.

Leistungsfähigkeit und Nutzen biometrisch gestützter Ausweise waren Gegenstand der öffentlichen Anhörung des Ausschusses für Bildung, Forschung und Technikfolgenabschätzung mit Fachpolitikern, externen Sachverständigen und weiteren Teilnehmern aus der Wirtschaft am 26. Mai 2004. Der Vertreter des Büros für Technikfolgenabschätzung beim Deutschen Bundestag bezeichnete bei der Präsentation des Arbeitsberichtes unter der Überschrift „Biometrie und Ausweisdokumente – Leistungsfähigkeit, politische Rahmenbedingungen, rechtliche Ausgestaltung“ die Biometrie als Sicherheitstechnologie, die vor ihrem weltweiten Durchbruch steht. Wesentlicher Treiber dieser Entwicklung seien die USA, aber auch auf EU-Ebene gebe es entsprechende politische und rechtliche Weichenstellungen für eine abgestimmte Strategie bei biometrischen Ausweisdokumenten. Neben die bisherigen Bemühungen um technische Praktikabilität sollten nach Ansicht des TAB nunmehr verstärkte Anstrengungen treten, die Frage der gesellschaftlichen Akzeptanz zu klären.

2.3 Szenario: Terrorangriff auf kerntechnische Anlagen

Immer wieder wird in der Öffentlichkeit das Terrorszenario eines terroristischen Flugzeugangriffs auf ein Atomkraftwerk gezeichnet. Wenn ein solcher Angriff auch nicht gänzlich ausgeschlossen werden kann, so ist die Wahrscheinlichkeit einer dadurch ausgelösten atomaren Katastrophe gleichwohl gering. Nach Medienberichten im Juni 2004 haben mehrere Kraftwerksbetreiber in Deutschland Vernebelungssysteme bestellt, mit deren Hilfe Atomkraftwerke gegen mögliche Terrorattacken aus der Luft gesichert werden sollen.

2.4 Auswirkungen des Terrorismus auf die wirtschaftliche Entwicklung

Die Schadensauswirkung des Terrorismus auf die Wirtschaft ist mehrschichtig. Er verursacht Ängste. Er führt zu höheren Aufwendungen für Schutzmaßnahmen. Und er beeinträchtigt die Investitions- und Konsumneigung. Auch nach Meinung des Bundeskanzlers Gerhard Schröder, geäußert bei der Eröffnung der diesjährigen CeBit-Messe, wird die positive Entwicklung der internationalen Konjunktur „nur dann zu halten sein, wenn es gelingt, externe Schocks zu vermeiden“. Der internationale Terrorismus müsse deshalb auch aus wirtschaftlichen Gründen bekämpft werden. Nur so könne es politische und ökonomische Stabilität geben. Ähnlich äußerte sich der Chef des Sachverständigenrats Wolfgang Wiegand (im Handelsblatt v. 17.03.04). Die erhöhten Sicherheitsvorkehrungen an den Grenzen verteuern den internationalen Handel. Nach Studien der OECD bremst ein Anstieg der Transportkosten um 1 % den Handel um 3 %. Nach Berechnungen von Volker Nitsch von der Freien Universität Berlin senkt eine Verdopplung der Zahl von Terroranschlägen den Handel mittelfristig (innerhalb eines Jahres) um 4 %. Steigende Ausgaben für Militär und Polizei lenken finanzielle Ressourcen vom privaten in den öffentlichen Sektor um und schaden damit der Produktivität.

2.5 Stimmungsbild der Wirtschaft

Die Terroranschläge v. 11. September 2001 haben das Sicherheitsdenken in vielen Unternehmen nachhaltig verändert. Sicherheitskonzeptionen wurden überprüft und Schwachstellen im System geschlossen oder wenigstens verringert.

Ob sich durch die Anschläge in Madrid das Stimmungsbild in der Wirtschaft erneut eingetrübt hat, wird unterschiedlich beantwortet. Die Financial Times Deutschland berichtete am 29.03.2004, dass sich bei den Geschäftsklimabefragungen in mehreren europäischen Län-

dern (einschließlich Deutschland) nach dem 11. März keine signifikanten Unterschiede gegenüber dem Stimmungsbild vor diesem Ereignis gezeigt hätten. Nach dem sog. Business-Monitor des Handelsblatts, bei dem nach den Anschlägen in Madrid 791 Führungskräfte telefonisch nach ihrer Einschätzung gefragt wurden, halten es 6 % für sehr und 45 % der Befragten für eher wahrscheinlich, dass sich auch in Deutschland ähnliche Anschläge ereignen werden. Fast jeder zweite Befragte (47 %) rechnet damit, dass in Deutschland Anschläge wie in Madrid starke (11 %) oder eher starke (36 %) negative Auswirkungen für die Konjunktur zur Folge hätten. Dagegen gehen 85 % der Manager davon aus, dass die Ereignisse in Madrid als solche eher oder sehr geringe oder gar keine negativen Folgen für die Wirtschaft in Deutschland und im Euro-Raum haben. Auch mit Auswirkungen auf das eigene Unternehmen rechnen 48 % überhaupt nicht, 46 % sehen nur eher geringe oder sehr geringe negative Konsequenzen.

2.6 Terrorversicherungen

Da nach dem 11. September 2001 fast alle Versicherer Terrorschäden aus ihren normalen Policen ausgeschlossen hatten, wurde von der Versicherungsbranche mit Unterstützung der Bundesregierung eine eigene Terrorversicherung – Extremus – gegründet. Bisher war die Nachfrage der deutschen Industrie gering. Statt der erwarteten 300 Mio € Prämieneinnahmen musste sich Extremus 2003 mit rund 105 Mio € begnügen. Ob sich die Zahl der Versicherungsabschlüsse nach den Anschlägen in Madrid im Jahr 2004 wesentlich erhöhen wird, bleibt abzuwarten.

2.7 Unternehmensschutz gegen den Terrorismus

Die Fülle der notwendigen Maßnahmen zum Schutz der Unternehmen vor terroristischen Angriffen hier zu beschreiben, erscheint wegen deren Abhängigkeit von Unternehmen, Größe und Auslandsbezug nicht sinnvoll. Wichtig ist, dass bei der Suche nach Schwachstellen im Sicherheitssystem eine gründliche Risikoanalyse durchgeführt wird, in der – auf der Grundlage aller erreichbaren Informationen über die Entwicklung der Bedrohungslage aus zuverlässigen Quellen – die spezifischen Gefährdungen für das Unternehmen und seine Beschäftigten sorgfältig analysiert wird. Wichtig ist ferner, dass das Sicherheitssystem ganzheitlich konzipiert wird, weil die einzelnen Elemente ineinander greifen. Als aktuelle Einzelmaßnahme sei die Möglichkeit der Sicherheitsüberprüfung einzelner Mitarbeiter zum vorbeugenden Sabotageschutz hervorgehoben, auf die an anderer Stelle des Berichts näher eingegangen wird. Besondere Bedeutung kommt dem Schutz von Niederlassungen, der in ihnen Beschäftigten und Geschäftsreisenden des Unternehmens in Krisenregionen zu.

2.8 Staatliche Maßnahmen der Terrorismusbekämpfung

Auf die Auflistung der Vielfalt der vom Staat nach dem 11. September 2001 ergriffenen Maßnahmen wurde hier verzichtet. Ziel des am 01. Januar 2002 in Kraft getretenen Terrorismusbekämpfungsgesetzes war es vor allem

- den erforderlichen Datenaustausch zwischen den Sicherheitsbehörden zu verbessern
- bereits die Einreise terroristischer Straftäter nach Deutschland möglichst zu verhindern
- identitätssichernde Maßnahmen im Visumverfahren zu verbessern

- den Einsatz bewaffneter Flugbegleiter des BGS in deutschen Flugzeugen zu ermöglichen
- Grenzkontrollmöglichkeiten zu verbessern
- bereits eingereiste Extremisten und Terroristen eher erkennen zu können
- und die uneingeschränkte Energieversorgung sicherzustellen.

Deshalb wurden in diesem Gesetzeswerk u.a.

- Sicherheitsüberprüfungen für Mitarbeiter in lebens- oder verteidigungswichtigen Einrichtungen ermöglicht,
- Rechtsgrundlagen für die Aufnahme biometrischer Merkmale in Pässe und Personalausweise geschaffen und
- bestimmte Sozialdaten in die Rasterfahndung einbezogen, um sie wirkungsvoller zu gestalten.

Wie schwierig es ist, alle notwendigen Maßnahmen zügig umzusetzen, zeigt sich allein darin, dass es Jahre gedauert hat, bis mit der gesetzlich angeordneten Sicherheitsüberprüfung von Beschäftigten in sicherheitsempfindlichen Bereichen begonnen worden ist, und dass bis heute noch nicht endgültig entschieden worden ist, welche biometrischen Merkmale in Reisepässe aufgenommen werden sollen.

Hervorgehoben seien die kontinuierlich verbesserten Sicherheitsmaßnahmen im Luftverkehr und auf Flughäfen durch

- den Einsatz bewaffneter Flugsicherheitsbegleiter in deutschen Flugzeugen
- den Einbau schuss- und einbruchsicherer Cockpittüren
- die verschärften Zuverlässigkeitsüberprüfungen, denen über 260.000 Personen, zumeist Beschäftigte, im Bereich der Luftfahrt unterzogen wurden
- die Einführung der vollständigen Kontrolle des aufgegebenen Gepäcks seit dem 1. Januar 2003
- die Einführung zusätzlicher Personal- und Gegenstandskontrollen beim Zutritt in sensible Bereiche des Flughafens und
- die Einrichtung einer umfassenden Qualitätskontrolle zur regelmäßigen Überprüfung der Luftsicherheitsmaßnahmen.

Auf EU-Ebene ist vor allem die VO(EG) Nr. 2320/2002 zur Festlegung gemeinsamer Vorschriften für die Sicherheit in der Zivilluftfahrt v. 16. Dezember 2002 zu erwähnen, die insbes. nationale Sicherheitsprogramme für die Zivilluftfahrt fordert, und in deren Anhang konkrete Vorschriften für die Flughafensicherheit, die Sicherheit von Luftfahrzeugen, die Behandlung von Fluggästen und Handgepäck, von aufgegebenem Gepäck, Fracht, Kurier- und Expresssendungen, Post und Material von Luftfahrtunternehmen, für Bordverpflegung und Bordvorräte, Reinigungsdienste, für die Einstellung und Schulung von Personals sowie Leitlinien für dessen Ausrüstung und für die Einstufung von verbotenen Gegenständen enthalten sind.

Der von den Staats- und Regierungschefs der EU nach den Anschlägen in Madrid verabschiedete Aktionsplan zur Bekämpfung des Terrorismus enthält keine bahnbrechenden Neuerungen. Dass die Teilnehmer beschlossen haben, „getroffene Beschlüsse umzusetzen“, ist ein Zeichen dafür, dass die nach dem 11. September 2001 verabschiedeten Maßnahmen nicht immer ernst genommen worden sind. Die Maßnahmen zur besseren Zusammenarbeit der staatlichen Nachrichtendienste – Einsetzung eines Koordinators, Beteiligung von EUROPOL, intensivere Kooperation mit Drittstaaten – ist auch aus der Sicht der Wirtschaft sicher zu begrüßen. Das gilt auch für die am 8. Juni 2004 vom Rat der Innenminister der EU-Staaten beschlossenen Einrichtung eines Lagezentrums im EU-Ratssekretariat, das rund um die Uhr fortdauernde oder potenzielle Krisen und Konflikte in aller Welt beobachten und regelmäßig Bedrohungsanalysen erstellen soll. Die Schaffung eines EU-Nachrichtendienstes

wurde aber ohne überzeugende Argumente abgelehnt. Zu wünschen ist, dass es bei dem Beschluss zur rascheren Einführung fälschungssicherer Ausweise in allen EU-Staaten und zur effizienteren Bekämpfung der Finanzierung terroristischer Aktivitäten nicht bei der Absichtserklärung bleibt.

Auf UN-Ebene ist von der International Maritime Organisation (IMO) die Initiative ergriffen worden, die Sicherheit der internationalen Seeschifffahrt und der von ihr angelaufenen Häfen zu verstärken, um sie vor Terrorangriffen möglichst zu schützen. Der International Ship and Port Facility Security (ISPS) Code, der am 01. Juli 2004 in Kraft getreten ist, enthält eine Fülle von Sicherheitsvorschriften. Die notwendigen Sicherungsmaßnahmen sind nach 3 Gefährdungsstufen gestaffelt. Für jede einzelne Hafenanlage, die Seeschiffe abfertigt, ist eine Gefährdungsanalyse zu erstellen und jedes Terminal muss einen Gefahrenabwehrplan erstellen, um zertifiziert zu werden. In Hamburg sind z.B. inzwischen die Gefahrenabwehrpläne von 64 Hafenbetrieben von der IMO zertifiziert worden.

Die EU-Kommission möchte das SOLAS-Übereinkommen und den ISPS-Code weiter ausdehnen und einen Inspektionsprozess der EU einführen. Insgesamt sollen die Sicherheitsmaßnahmen in internationalen Häfen und in der Seeschifffahrt dem Sicherheitsniveau im Luftverkehr angenähert werden.

Die US-Zollbehörde (Customs) hat schon 2002 die „Container Security Initiative“ (CSI) ergriffen. Danach muss Customs auf der Grundlage bestimmter Kriterien der Risikobewertung und von Überwachungsbestimmungen mindestens 24 Stunden vor Ankunft eines Containers im Zielhafen der USA der Inhalt der Ladung bekannt sein. Dadurch wird die internationale Logistikkette der maritimen Wirtschaft wesentlich erhöht. Es soll möglichst ausgeschlossen werden, dass unbemerkt in Containern unter Umständen gefährliche, insbes. biologische oder radioaktive Waffen befördert werden.

2.9 Gefahr gewalttätiger extremistischer Gruppen

In Deutschland wird die verfassungsmäßige Ordnung weiterhin durch rechtsextremistische und linksextremistische Bestrebungen angegriffen. Ende 2003 gab es 169 rechtsextremistische Organisationen mit insgesamt ca. 41.500 Mitgliedern und linksextremistische Gruppierungen mit zusammen etwa 31.300 Anhängern.

2.9.1 Politisch motivierte Kriminalität ‚Links’

Dazu gehören die gewaltbereiten so genannten Autonomen mit einem Mitgliederbestand von ca. 5.400 Mitgliedern. Die Hauptzielrichtung der linksextremistischen Gewalt liegt zwar im Kampf gegen rechtsextreme Kräfte; mit dieser Zielrichtung wurden im Jahre 2003 insgesamt 226 Gewalttaten verübt, im Rahmen der „Kampagnen gegen Kernenergie“ weitere 21.

Dass einzelne Gruppierungen bereit sind, theoretische Erwägungen auch in die Praxis umzusetzen, verdeutlichen die seitens der Autonomen in den letzten 12 Monaten verübten konspirativen Anschläge, Brandanschläge gegen Gebäude und Fahrzeuge, die zum Teil erheblichen Sachschaden verursachten. Besonders aktiv ist in jüngster Zeit die sog. „militante gruppe (mg)“ in Berlin. Durch die explizite Nennung von Personen in ihren Selbstbezichtigungen, sollen diese aus der „Anonymität“ geholt und ihre potenzielle „Angreifbarkeit“ reklamiert werden. So haben Täter aus dem Umkreis der mg im Oktober 2003 einen LKW der Abfallrecyclingfirma ALBA auf dem Firmengelände in Brand gesetzt und Flugblätter mit sozialrevolutionären Parolen am Tatort zurückgelassen. In der Nacht zum 1. Januar 2004 haben

Angehörige der mg einen Brandanschlag gegen das Bürogebäude des Deutschen Instituts für Wirtschaftsforschung (DIW) in Berlin-Steglitz verübt. Nach dem Brandanschlag auf ein Bezirks- und Arbeitsamt in Berlin im März 2004, wurde im von *mg* unterzeichneten Bekennerschreiben direkt Bezug genommen auf das in der Szenepublikation *Interim* debattierte Plattformprojekt für linke politische Gewalt. In den frühen Morgenstunden des 7. Mai 2004 wurde auf drei Fahrzeuge der Deutschen Telekom in Berlin-Wedding ein Brandanschlag verübt. In einer „Anschlagserklärung" bezichtigte sich die „militante gruppe" der Tat und bezeichnete sie als militante Aktion gegen die „sozialtechnokratische Offensive von Staat und Kapital".

Deutsche Linksextremisten haben ihre Debatte über die Zweckmäßigkeit und Legitimation politischer Gewalt (auch gegen Personen) weiter geführt.

Der so genannte Sozialabbau in Deutschland, der zweite Irakkrieg sowie die Weiterentwicklung der Europäischen Sicherheits- und Verteidigungspolitik (ESVP) durch die EU haben in weiten Teilen der Szene die Debatten bestimmt und anti-militaristische und kommunistische Grundauffassungen gestärkt.
Gewalttätige Aktionen richteten und richten sich vornehmlich gegen rechtsextreme Personen (Anti-Fa), die Bahn AG (Castortransport), die Bundeswehr (bzw. deren Zulieferer/ Dienstleister) und Arbeitsämter (sog. Sozialabbau). Bei den Protesten gegen Castor-Transporte setzte sich der Trend abnehmender Mobilisierung fort.

Die Anschläge blieben alle unter der Terrorismusschwelle.

2.9.2 Politisch motivierte Kriminalität ‚Rechts'

Gegen die im September 2003 wegen der Planung eines Anschlages auf das jüdische Gemeindezentrum in München festgenommenen Rechtsextremisten des so genannten „*Kameradschaft Süd-Aktionsbüro Süddeutschland*" bereitet derzeit die Staatsanwaltschaft die Anklage vor bzw. hat das zuständige Gericht bereits einen der drei mutmaßlichen Haupttäter zu einer Haftstrafe verurteilt. Die Tatvorbereitungen und Beteiligten gelten als größtenteils aufgeklärt.

Im vergangenen Jahr waren keine vergleichbar schwerwiegenden Tatplanungen bzw. Umsetzungen zu verzeichnen. Dagegen weiteten die deutschen Strafverfolgungsbehörden die Ermittlungen gegen andere rechtsextreme Gruppen aus:

In einer konzertierten Aktion wurden im Oktober 2003 in Schleswig-Holstein, Hamburg und Niedersachsen insgesamt 50 Objekte der Rechtsextremistengruppe *Combat 18* durchsucht. Die Ermittlungen richten sich allerdings auf den Straftatbestand der Gründung einer kriminellen Vereinigung und nicht auf einen terroristischen Hintergrund.

Das Bayerische Staatsministerium verhängte im Januar 2004 ein Vereinsverbot gegen die *Fränkische Aktionsfront* (FAF), einen rechtsextremistischen Zusammenschluss von ca. 15 Rechtsextremisten.

Grundsätzlich ist nicht auszuschließen, dass rechtsextreme Einzeltäter oder Gruppierungen sich erneut terroristischer Methoden bedienen und Anschläge planen. Rechtsextreme Gewalt äußert sich allerdings meist in Form von spontanen und unter Alkoholeinfluss verübten Körperverletzungen gegen die den rechtsextremen Feindbildern entsprechenden Personengruppen.

2.10 Extremistische Gruppierungen in Europa

2.10.1 Linksextremistische und anarchistische Gruppierungen in Griechenland

Die linksextremistische Terrorgruppe „*Revolutionäre Organisation 17. November*“ (N17) gilt nach der Verurteilung von 15 Mitgliedern als zerschlagen. Gegen die zweitgrößte Terrorgruppe *Revolutionary Peoples Struggle* (ELA) konnte dieses Jahr ebenfalls ein Fahndungserfolg verbucht werden. Im Februar 2004 wurde gegen fünf mutmaßliche Mitglieder Anklage erhoben.

Die lange ausgebliebenen Erfolge der griechischen Strafverfolgungsbehörden gegen die heimischen Terrororganisationen begründen sich zum großen Teil auf die Zusammenarbeit mit ausländischen Geheimdiensten und den Bemühungen, die Olympischen Sommerspiele 2004 in einem sicheren Umfeld auszurichten.

Allerdings sind ähnlich wie in Italien auch in Griechenland neue Gruppierungen im linksextremistischen Spektrum nachgewachsen, die für zahlreiche kleinere Bomben- und Brandbombenanschläge (z.B*. Popular Revolutionary Action*) verantwortlich sind. So auch für den versuchten Bombenanschlag auf eine Zweigstelle der Citybank im März 2004 oder Anschläge auf einen EU-Beamten und Büros griechischer Parteien.

Es gibt Hinweise auf eine internationale Zusammenarbeit zwischen diesen griechischen Gruppierungen und anderen europäischen linksextremistischen Terroristen. Dies ist insbesondere im Hinblick auf die Sicherheit der Olympischen Sommerspiele von Relevanz. Es wird damit zu rechnen sein, dass die politisch motivierte Kriminalität in Griechenland anhält und unter Umständen auch größere Anschläge verübt werden.

2.10.2 Real/ Continuity - IRA & UDA (Großbritannien)

Die politische Entwicklung in Nordirland bleibt weiterhin geprägt von gegenseitigen Anschuldigungen zwischen den politischen Lagern. Das von dem britischen Premierminister Tony Blair verkündete Ziel, bis zum Juni 2004 zu einer Einigung im Konflikt um die Machtverteilung zu kommen, wurde nicht erfüllt. Auch die Entwaffnung der *Provisional IRA (PRIA)* sorgt für anhaltende Verstimmungen der Konfliktparteien.

Vor diesem politischen Hintergrund kam es auch in den vergangenen Monaten zu politischen Gewalttaten wie z.B. Brandstiftungen, Briefbomben und Erpressungen. Trotz des erklärten „Waffenstillstandes“ wurden aber sowohl von republikanischer Seite (*real/ continuity IRA*) als auch von loyalistischer Seite (*Ulster Freedom Fighters, Ulster Young Militants Ulster Defence Association*) Versuche unternommen, die Gewalt mittels Bombenanschlägen erneut eskalieren zu lassen.

Im Fokus befinden sich Sicherheitskräfte, politische Einrichtungen sowie politisch engagierte Einzelpersonen in Nordirland. Britische Sicherheitskreise schließen auch die Möglichkeit eines gegen Zivilisten gerichteten Anschlages in Nordirland oder Irland nicht aus. Eine erneute Zuspitzung der Lage könnte sich in dem Zusammenhang mit den Neuverhandlungen des „Good Friday Agreements“ ergeben.

2.10.3 Neue Rote Brigaden und extremistische Anarchisten (Italien)

Die italienischen Strafverfolgungsbehörden konnten an den Festnahmen des vergangenen Jahres anknüpfen und verhafteten im Januar 2004 ranghohe Mitglieder der *Roten Brigaden* in Kairo, Ägypten. Es kann nun davon ausgegangen werden, dass die ursprüngliche Struktur dieser linksextremistischen Terrorgruppe zerschlagen ist.

Allerdings treten nach derzeitigem Kenntnisstand mit geografischem Schwerpunkt in der Toskana und in Sardinien, italienische Linksextremisten in die Fußstapfen der *Roten Brigaden* als *Neue Rote Brigaden* (N-BR). Unter anderem sehen sich folgende Gruppen als Nachfolger der *RB*: *Red Brigades Communist Combatant Party (BR-PCC), Red Brigades Union of Combatant Communists (BR-UCC), Red Brigades Urban Guerillas for the Construction of the Anti-Imperialist Fighting Front.*

Eine Reihe von vereitelten und durchgeführten kleineren Bombenanschlägen auf Polizeistationen in Rom und Genua bzw. auf einen lokalen Flughafen deutet auf eine zunehmende Aktivität dieser Gruppen hin.

Eine Verbindung zu der in Italien ausgeprägten anarchistischen Extremistenszene (z.B. *Territorial Anti-Imperialist Cells, 20th July Brigades, Proletarian Nuclei for Communism*) soll nicht ausgeschlossen werden können. Letztere steht im Mittelpunkt der Ermittlungen im Zusammenhang mit den im Dezember 2003 bei europäischen Institutionen eingegangenen Briefbomben. Die sich zu den Briefbomben bekennende *Federatione Anarchia Informale* (FAI) kündigte weitere Angriffe an.

Sollten tatsächlich weitere Angriffe erfolgen, werden sich diese aller Vorrausicht nach auf EU-Institutionen, auf italienische Polizeibehörden, Politiker und ggf. italienische Unternehmen beschränken.

2.10.4 Kadek/PKK/Kongra-Gel und Dhkp-c (Türkei)

Die im Jahr 2003 bekannt gegebene Kündigung des Waffenstillstandes durch die kurdische *KADEK* hat keine neue Welle an ethnisch-nationalistischer Gewalt in der Türkei ausgelöst. Auch die Demonstrationen anlässlich des fünften Jahrestages der Festnahme Abdullah Öcalans in Europa verliefen weitgehend friedlich.

Derweilen hat sich die Organisation zum zweiten Mal umbenannt. Die sich in *KADEK* umbenannte *PKK* gab sich den neuen Namen *Volkskongress Kurdistan* (Kongra-Gel), bleibt aber weiterhin auf der Liste der terroristischen Organisationen der EU.

Zu Verwechslungen mit dem islamistischen Terrorismus führten Pressemeldungen über am 01.04.04 europaweit zeitgleich durchgeführte Razzien gegen die Terrororganisation *Revolutionären Volksbereiungspartei-Front* (DHKP-C). Nach derzeitigem Kenntnisstand unterhält die *DHKP-C* keine Verbindungen zum islamistischen Terrorismus, stellte aber ihre in der Türkei verübten Bombenanschläge gegen eine McDonalds Filiale und ein staatliches Hotel in Istanbul als Teil des irakischen Widerstandes gegen die Besatzungsmächte dar. Die *DHKP-C* ging aus der stalinistischen *Dev Sol* hervor und ist eine sozialrevolutionär und marxistisch motivierte türkische Terrororganisation. Derzeit wird nicht von einer terroristischen Gefährdung durch die DHKP-C in Europa ausgegangen.

2.10.5 Korsische Separatisten (Frankreich)

Sowohl in Korsika als auch im Süden Frankreichs verübten korsische Terrorgruppen eine Reihe von kleineren Brand- und Bombenanschlägen gegen Einrichtungen der französischen Verwaltung. Verdächtigt werden u.a. die *Corsican National Liberation Front Combatants Union* (FLNC) sowie die *Corsican National Liberation Front* (CNLF).

Derzeit wird von anhaltenden terroristischen Aktivitäten der korsischen Extremisten in Frankreich ohne die gezielte Tötung von Zivilisten ausgegangen.

2.10.6 Eta (Spanien)

Sowohl spanische als auch französische Sicherheitsbehörden konnten beachtliche Erfolge im Kampf gegen die baskische Terrorgruppe *Euzkadi Ta Askatasuna* (ETA) verzeichnen. Es gelang in mehreren separaten Aktionen wichtige Mitglieder der Terrororganisation festzunehmen, Anschläge zu verhindern und Waffendepots auszuheben.

Nach den Madrider Anschlägen vom 11. März 2004 verdächtigten die spanischen Ermittlungsbehörden zunächst die *ETA*. Wie sich später herausstellte, waren diese Verdächtigungen und Falschaussagen über den in der Anschlagsserie verwendeten Sprengstoff teils politisch motiviert und durch die Regierung Aznar gezielt gestreut worden. Allerdings muss hierbei auch berücksichtigt werden, dass spanische Sicherheitsbehörden im Dezember 2003 beim Deponieren von Bomben an Bahnschienen und in einem Bahnhof verhaftet worden waren und somit ein Anfangsverdacht berechtigt war.

Inwiefern die islamistischen Anschläge in Madrid und die öffentliche Reaktion hierauf einen Einfluss auf das Anschlagsverhalten der *ETA* haben wird, bleibt abzuwarten. Als Reaktion auf die Verhaftungen der vergangenen Monate ist derweil eine Umstrukturierung der *ETA* in kleinere und autonome Kommandos zu beobachten. Angesichts der breiten Unterstützung in Teilen der baskischstämmigen Bevölkerung und weiterer mutmaßlicher Waffendepots, ist von einer anhaltenden terroristischen Aktivität der *ETA* in Spanien auszugehen.

3 Tendenz der Kriminalitätsentwicklung

3.1 PKS als Grundlage

Die Sicherheitslage wird zu einem wesentlichen Teil durch Deliktsarten gekennzeichnet, die in der jährlichen Polizeilichen Kriminalstatistik (PKS) aufgelistet werden. Auch wenn das Zahlenwerk dieser Statistik jeweils der Interpretation bedarf, vor allem weil es selbstverständlich nur die ermittelten Fälle enthalten kann – also das von Deliktsart zu Deliktsart unterschiedlich große „Dunkelfeld“ nicht entdeckter und nicht angezeigter Kriminalität unberücksichtigt lassen muss – und weil es auf einer „Momentaufnahme“ der Ermittlungen im Zeitpunkt der Abgabe an die Staatsanwaltschaft beruht – also nicht den anschließenden „Ausfilterungsprozess“ des justiziellen Strafverfahrens einbezieht, ergibt die PKS jedenfalls ein angemessenes Bild der Kriminalitätsentwicklung. Denn die Kriterien der Fallerfassung bleiben, soweit nicht Rechtsänderungen zu neuen oder veränderten Straftatbeständen führen, jedes Jahr gleich. Freilich muss bei der Analyse der PKS-Zahlen bedacht werden, dass die Belastung der Personen und der Unternehmen, zu deren Nachteil eine Straftat begangen wird, von Fall zu Fall unterschiedlich schwer ist.

3.2 Gesamtkriminalität

In der PKS für das Jahr 2003 sind fast 6,6 Millionen Verdachtsfälle registriert. Bezogen auf je 100.000 Einwohner ergibt dies eine Häufigkeitszahl (HZ) von 7.963. Sie ist im Verhältnis zu 1993 – dem Jahr mit der bisher höchsten Belastung – um 4,5 % gesunken, im Verhältnis zu 1998 (5 Jahres-Zeitraum) nahezu gleich geblieben (7.869) und im Verhältnis zu 2002 um 0,88 % gestiegen, innerhalb der letzten 3 Jahre sogar insgesamt um 4,4 %.

Die Aufklärungsquote (AQ) – von Deliktsart zu Deliktsart höchst unterschiedlich (zwischen 5,33 % beim Taschendiebstahl bis 100 % bei einer Reihe von Kontrolldelikten) – betrug 2003 insgesamt 53,1 %. Sie lag damit nur geringfügig unter dem seit langem höchsten Stand von 53,2 % im Jahre 2000.

3.3 Unterschiedliche Belastung nach sozialen Räumen und Bundesländern

Die Kriminalitätsbelastung ist in Großstädten selbstverständlich wesentlich höher als in kleineren Kommunen. Sie differiert aber auch erheblich von Bundesland zu Bundesland. Seit jeher besteht ein erhebliches Nord/Süd-Gefälle. Das Risiko, Opfer einer Straftat zu werden, ist in Norddeutschland insgesamt fast doppelt so hoch wie in Baden-Württemberg und Bayern und in Berlin ebenfalls fast doppelt so hoch wie in München. Eine so beachtliche Differenz kann – herabgebrochen auf bestimmte, die Wirtschaft besonders belastende, Deliktsarten – im Einzelfall durchaus Auswirkung auf eine Investitionsentscheidung haben.

Häufigkeitszahlen	2003
Berlin	16.622
Hamburg	15.698
Bremen	14.361
Mecklenburg-Vorpommern	10.762
Brandenburg	9.515
Schleswig-Holstein	9.348
Sachsen-Anhalt	8.992
Nordrhein-Westfalen	8.287
Sachsen	8.114
Hessen	7.462
Niedersachsen	7.438
Rheinland-Pfalz	7.091
Saarland	7.011
Thüringen	6.917
Bayern	5.709
Baden-Württemberg	5.456

3.4 Täterbezogene Entwicklung

Die Kriminalitätsbelastung ist in den einzelnen Altersgruppen unterschiedlich hoch. Von den 2003 ermittelten Tatverdächtigen (TVen) waren

- 5,4 % Kinder (Seit 1999 mit 6,7 % ist der Anteil rückläufig.)
- 12,5 % Jugendliche (Der Anteil liegt nur knapp unter dem Höchststand 1999 mit 13,1 %.)
- 10,5 % Heranwachsende (Der Höchststand lag 1984 bei 11,9 %, der niedrigste Anteil 1994 bei 9,6 %.)
- 11,9 % Jungerwachsene zwischen 21 und 25 Jahren (Der Höchststand betrug 1992 14,6 %, der niedrigste Stand 11 % im Jahr 1998.)
- 71,6 % Erwachsene (Der Höchststand wurde mit 75,9 % im Jahr 1992 erreicht.)

Die Veränderungen in der Altersstruktur beruhen in erster Linie auf demographischen Einflüssen, d.h. auf der Veränderung der Altersstruktur in der Bevölkerung und auf dem Umfang der Migration sowie der Alters- und Sozialstruktur der Einwanderer.

Der Anteil nichtdeutscher TVer lag mit 23,5 % zwar weit über ihrem Bevölkerungsanteil von 8–9 %. Allerdings darf aus diesem Vergleich nicht der falsche Schluss gezogen werden, die ausländische Bevölkerung sei insgesamt wesentlich stärker kriminalitätsbelastet. Die Kriminalitätsbelastung von Ausländern in Deutschland liegt umso höher, je weniger diese beruflich und sozial integriert sind.

Von den tatverdächtigen Nichtdeutschen waren	2003	1984
Arbeitnehmer	18,2 %	3,6 %
Illegal Aufhältliche	17,4 %	13,6 %
Asylbewerber	13,3 %	7,7 %
Studenten/Schüler	8,0 %	14,7 %
Touristen/Durchreisende	7,4 %	6,7 %
Gewerbetreibende	3,0 %	3,6 %
Stationierungskräfte u. Angehörige	0,6 %	4,5 %
Sonstige (insbes. Erwerbslose und nicht anerkannte Asylbewerber mit Duldung)	32,1 %	16,1 %

3.5 Entwicklung der Kriminalitätssektoren

Angaben in Tausend (i.T.)	2003	1998
Straßenkriminalität	1.754	1.800
Einfacher Diebstahl	1.541	1.526
Schwerer Diebstahl	1.488	1.800
Vermögens- u. Fälschungsdelikte	1.111	899
Rauschgiftkriminalität	256	220
Gewaltkriminalität	204	186
Wirtschaftskriminalität	86	86
Computerkriminalität	60	46
Umweltkriminalität nach StGB	25	41

Von der Tendenz, dass die mit physischen Handlungen und physischer Gewalt verbundene Kriminalität in den letzten 5 Jahren reduziert werden konnte, macht die Gewaltkriminalität selbst eine Ausnahme. Ursächlich ist dafür allerdings nicht die Raubkriminalität, sondern sind Körperverletzungen, Nötigungen und Bedrohungen. Ansonsten ist die Kriminalität in den letzten 5 Jahren „intelligenter“ geworden. Auf dem Vormarsch sind Vermögens- und Fälschungsdelikte sowie die Computerkriminalität.

Mit einem weiteren Anwachsen dieser Kriminalitätsbereiche ist auch in Zukunft zu rechnen. In der global ausgerichteten Wirtschaft, die immer mehr auf elektronische Informations- und Kommunikationssysteme angewiesen ist, und deren Geschäftsverkehre in ihrer Komplexität eine Fülle von Missbrauchs-, Fälschungs- und Betrugsmöglichkeiten bieten, wird viel kriminelle Energie darauf verwendet, diese Möglichkeiten zu nutzen. Unter Missbrauch moderner Informations- und Kommunikationstechnologien wird die Vermögens- und Fälschungskriminalität zu Lasten der Wirtschaft ihren quantitativen wie qualitativen Anteil am Kriminalitätsgeschehen steigern.

3.6 Materieller Schaden

Wie viel Schaden Kriminalität anrichtet, ist nicht exakt zu ermitteln. Schon die Schadensdefinition bereitet Schwierigkeiten. Ohnehin kann nur der materielle Schaden beziffert werden. Und seine Feststellung bleibt auf das „Hellfeld“ ermittelter Kriminalität beschränkt. Bei den einzelnen in diesem Bericht beschriebenen Deliktsarten und Bedrohungsphänomene werden Schadensschätzungen angegeben, die zumeist auf Opfer befragen und Expertenschätzungen beruhen.

Die PKS bietet Schätzungen der Polizei bei vollendeten Straftaten an.

Die Gesamtsumme betrug	2003	Veränderung gegenüber 1998
beim Diebstahl	2.700 Mio. €	+ 10 %
davon:		
beim schweren Diebstahl (im wesentlichen Einbruch)	2.000 Mio. €	+ 11 %
davon:		
Wohnungseinbruch	622 Mio. €	+ 94 %
Kfz-Aufbruch	224 Mio. €	+ 15 %
Veruntreuungen	1.500 Mio. €	+ 58 %

4 Diebstahlskriminalität

4.1 Geschäftsdiebstahl in der PKS

Nach der Anzahl der ermittelten Fälle ist der Diebstahl ebenso wie in der Gesamtgesellschaft auch in der Wirtschaft die häufigste Deliktsart. Aus der PKS lassen sich insbesondere folgende Deliktsarten zu Lasten der Wirtschaft entnehmen:

i.T.	2003	1998	1993
Diebstahl aus Verkaufsräumen	632	761	837
in/aus Büros, Fabriken, Lagern	186	199	228
in/aus Gaststätten, Hotels	69	75	96
von/aus Automaten	29	58	115
in/aus Kiosken	10	12	18
in/aus Schaufenstern, Vitrinen	4	7	13
in/aus Banken	3	3	6

Die Gegenüberstellung der Zahlen im 10 Jahres-Abstand zeigt den massiven Rückgang der Geschäftsdiebstähle. Insgesamt beträgt er fast 29 %. Ursächlich für diesen erheblichen Rückgang ist sicher vor allem ein verstärkter Werk- und Unternehmensschutz.

4.2 Einbrüche in Gewerbeobjekte

Dass auch eine verbesserte Ausstattung von Gewerbeobjekten mit Sicherheitstechnik zu diesem Rückgang beigetragen hat, lässt sich aus der Auflistung der dem BayLKA gemeldeten Einbruchsversuche schließen, die aufgrund mechanischer Sicherungsausrüstung und Einbruchmeldeanlagen im Versuchsstadium stecken geblieben sind. Für 2003 ergibt sich folgendes Bild:

	Anzahl der Erfolge aufgrund von
mechanischen Sicherungen insgesamt	563
bei Türen	439
Zusatzverriegelungen	124
widerstandsfähiger Türkonstruktion u. Anbauteile	315
bei Fenstern, Terrassen- u. Balkontüren	97
Fensterzusatzsicherungen	73
sonstiger Sicherungen (z.B. Gitter, Rollläden)	24
bei Schaufenstern	27
Einbruchmeldeanlagen insgesamt	235
Fernalarm	56 (24 %)
örtlichem Alarm	73 (31 %)
kombiniertem Alarm	106 (45 %)

Im gewerblichen Bereich waren in Bayern mit einem Anteil von 45 % die meisten Erfolge nach einer kombinierten Alarmierung aus örtlicher Alarmierung und Fernalarmierung zu verzeichnen, d.h. mittels Sirenen und Blitzleuchte am Objekt mit entsprechendem Abschreckungseffekt und gleichzeitiger „stiller“ Alarmierung über ein Telefonwählgerät.

4.3 Blitzeinbrüche

In Deutschland haben sich seit Mitte 2001 Raubüberfälle und Blitzeinbrüche bei Juwelieren gehäuft. Der Schaden wurde bis 2003 auf mehr als 25 Millionen € geschätzt. Nach den bisherigen Ermittlungen befinden sich die Organisatoren der Tätergruppen meist im Ausland, besonders in Polen und im früheren Jugoslawien. Nachdem sich in Bayern ca. 40 Taten ereignet hatten, wurde beim Landeskriminalamt eine Sonderkommission gebildet. Auch hier leistet bei der Aufklärung die DNA-Analyse wertvolle Dienste. So konnte nach einem Überfall in Aschaffenburg durch einen DNA-Abgleich ein Mann auch als Täter einer Serie von Überfällen in Nordrhein-Westfalen überführt werden.

4.4 Kfz-Diebstahl

Nach der PKS 2003 kam es in diesem Jahr insgesamt zu 63.240 Diebstählen von KFZ. Das waren – nach den der Einführung der elektronischen Wegfahrsperre verdankten ständigen Rückgängen seit 1993 – nochmals 10,4 % weniger als 2002.
Nach einer im Oktober 2003 von AOL Deutschland veröffentlichten Analyse standen 2002 folgende Modelle am höchsten „im Kurs“ bei Autodieben:

		Diebstahlsrate (in Promille)	durchschn. Schaden/€
1.	BMW X5 4.4	38,9	49.382
2.	Mercedes CL 500	21,6	65.443
3.	Mercedes 300 D	15,9	8.567
4.	Audi 100/A 6 Diesel	15,7	7.028
5.	Toyota Landcruiser J 10 4.2 D	14,0	35.473
6.	Mercedes 250 D	11,7	8.985
7.	Mercedes 320 E	11,6	8.637
8.	Mercedes 500 SL	11,4	83.575
9.	Audi A 8 4.2	11,0	21.304
10.	Mercedes 300 TE-24	10,7	10.583

Pro 1.000 Fahrzeuge wurde 2003 bundesdurchschnittlich 1,1 KFZ entwendet. An der Spitze liegt Berlin mit 4,2, gefolgt von Hamburg mit 3,6 entwendeten Autos.

Inzwischen ist es professionellen Tätern, zumeist organisierten Banden, teilweise gelungen, die elektronische Wegfahrsperre zu überwinden. Nach Erkenntnissen der Frankfurter Kriminalpolizei brechen sie nicht mehr Autotüren auf und knacken Lenkradschlösser, sondern sie manipulieren die zur Sicherheit eingesetzte Elektronik, zapfen die Steuersoftware an oder wechseln das komplette Steuergerät aus. Auf illegalen Ersatzteilmärkten im Ausland lassen kriminelle Profis Steuergeräte für Motor- und Wegfahrsperren fertigen, die dann nur noch gegen die Originale ausgetauscht werden müssen. Oder sie stehlen bei Autohändlern und Werkstätten Diagnosegeräte. Aus dem elektronischen Speicher der eingebauten Motorsteuergeräte lassen sich Daten für den Steuercode herauslesen. 200 solcher KFZ-Diagnosegeräte sind derzeit als gestohlen gemeldet.

Insgesamt aber bleibt die elektronische Wegfahrsperre hochwirksam gegen KFZ-Diebstahl.

4.5 Fracht- und LKW-Diebstähle

LKW-Diebstähle und Frachtdiebstähle werden in der PKS nicht gesondert ausgewiesen.
2002 haben sich die Verluste bei den Mitgliedern der Technology Asset Protection Association Europe (TAPA), einer Vereinigung von Technik- und Logistikfirmen, mehr als verdoppelt. Laut Medienberichten hat eine Bande von Frachtdieben am Frankfurter Flughafen 2003 Waren im Wert von 4,6 Mio € gestohlen. Sie hatten es besonders auf Camcorder, Handys und Computerprozessoren abgesehen. Die Nordsee-Zeitung berichtete im Januar 2004 von einer Serie von LKW-Diebstählen, deren Aufdeckung mit der Ermittlung eines gestohlenen Sattelzuges im Fischereihafen in Bremerhaven begann. Am Ende wurden 100 LKW-Diebstähle mit einem Gesamtschaden von ca. 10 Mio € ermittelt. Die Täter sind der organisierten Kriminalität zuzurechnen.

Besonders betroffen von Diebstählen sind LKW-Ladungen mit hochwertigen IT-Produkten.
Im Mai 2003 haben SIEMENS und das Logistik-Unternehmen Kühne & Nagel das Logistic Ident Consortium (Licon) gegründet. Sein Ziel ist ein Konzept, das Sicherheit in allen Phasen des Transports garantiert. Entwickelt wird eine Ortung ohne Außenantennen, so dass es für LKW-Diebe keinen Hinweis auf die Existenz einer Ortungsvorrichtung gibt.

4.6 Ladendiebstahl

Gegenüber 1993 ist die Zahl der in der PKS ausgewiesenen Fälle von Diebstählen aus Verkaufsräumen um über 24 %, der Ladendiebstähle im engeren Sinne um über 20 % gesunken. Für diesen Rückgang kann beides ursächlich sein: eine Abnahme der Kontrolltätigkeit ebenso wie umgekehrt eine Zunahme der Überwachungstätigkeit, verbunden mit einem höheren Grad der Ausstattung mit Videoüberwachungskameras und Detektionsgeräten, beides mit dem Ergebnis verstärkter Abschreckung potenzieller Täter.

Eine gemeinsame Erhebung des Bundesverbandes des Deutschen Groß- und Außenhandels (BGA) und des Europäischen Handelsinstituts, die im Mai 2004 veröffentlicht wurde, kommt zu dem Ergebnis, dass durch Ladendiebstahl dem Einzelhandel in Deutschland 2003 ein Schaden von 2,1 Mrd. € entstanden ist. Dazu wurden 81 Unternehmen mit 9.400 Verkaufsstellen befragt. Eine Untersuchung des Berliner Einzelhandelsverbandes, die zwischen sog. einfachen Ladendiebstählen und besonders schweren Fällen mit Überwindung technischer Sicherungen unterscheidet, zeigt, dass bei den schwereren Fällen Schwerpunkte beim Diebstahl von Zigaretten in Supermärkten, Handys und Elektrowaren im Vordergrund stehen. Eine Chance, den Ladendiebstahl wesentlich zu reduzieren, besteht in der Einführung von RFID (Radio Frequency Identification Chips)-Technologie. Es handelt sich um elektronische Etiketten, deren Information drahtlos und ohne Sichtkontakt über ein Lesegerät automatisch ausgelesen werden können. Passiert ein Kunde mit gefülltem Einkaufskorb eine Zone mit RFID-Lesegeräten, dann werden alle Waren erfasst, und der fällige Endbetrug erscheint auf einem Monitor an der Kasse. Freilich dürfte noch geraume Zeit bis zur Einführung solcher RFID-Etiketten vergehen. Bisherige Praxistests sind noch nicht zufrieden stellend ausgefallen. Auch an internationalen Standards wird noch gearbeitet. Nach einer Umfrage von Booz Allen Hamilton und der Universität St. Gallen wollen nur 18 % der in Europa und den USA befragten Großunternehmen in diesem Jahr mehr als 500.000 € in die neuen Etiketten investieren. Dennoch nehmen Marktforscher an, dass der Gesamtumsatz bis 2008 Milliardenbeträge erreicht.

5 Betriebskriminalität

Ein Teil der zuvor beschriebenen Diebstahlsdelikte wird durch Innentäter begangen, teilweise in kriminellem Zusammenwirken mit Außentätern. Die sog. Betriebskriminalität umfasst darüber hinaus andere Deliktsarten: Unterschlagung, Untreuehandlungen, betrügerische Manipulationen, Korruption: sämtlich Straftaten zum Nachteil des Unternehmens und/oder einzelner Beschäftigter. Bei Tätern aus den Führungsetagen des Unternehmens spricht man auch von Managerkriminalität.

Beziffern lässt sich die Zahl der Fälle ebenso wenig wie der Schaden, der den Unternehmen durch diese Kriminalität entsteht. Nach einer Umfrage von PriceWaterhouseCoopers im Jahr 2001 bei 1492 international tätigen Unternehmen sollen ca. 60 % der Kriminalität zu Lasten von Unternehmen durch Innentäter begangen werden. Nach einer Umfrage der Association of Certified Fraud Examiners (ACFE) 1998 bei 250 europäischen Unternehmen werden die meisten Betrugsdelikte zum Nachteil des Unternehmens von Einzeltätern im Unternehmen begangen. Der durch die Tat angerichtete Schaden wurde im Durchschnitt mit 27.000 € beziffert. In Fällen, in denen der Täter Partner außerhalb des Unternehmens hatte, lag die mittlere Schadensquote dagegen bei 375.000 €.

Die der Betriebskriminalität zugrunde liegende Erosion des Unrechtsbewusstseins hängt zu einem Teil mit dem erkennbaren Wertewandel in unserer Gesellschaft zusammen. Sie kann aber auch unternehmensbedingt sein. Dabei können eine ganze Reihe negativer Umstände und Einstellungen eine Rolle spielen: vom mangelhaften Vorbild des Vorgesetzten und einem „Laissez faire“-Führungsstil bis hin zu Sozialneid und verwahrlosten Arbeitsplätzen.

Die Stärkung der Loyalität der Mitarbeiter, ein gutes Betriebsklima, angemessene und gerechte Entlohnung sowie intensive individuelle Betreuung sind die besten Präventionsmaßnahmen gegen Betriebskriminalität. Nach einer internationalen Studie des Marktforschungsunternehmens Gallup ist die emotionale Bindung der Arbeitnehmer zu seinem Unternehmen in Deutschland schwächer ausgeprägt als in vielen anderen Staaten:

Nach dieser Untersuchung ist die emotionale Bindung	hoch	gering	nicht vorhanden
USA	30 %	54 %	16 %
Kanada	24 %	60 %	16 %
Israel	10 %	65 %	15 %
Australien	18 %	63 %	19 %
Großbritannien	17 %	63 %	20 %
Deutschland	12 %	70 %	18 %
Japan	9 %	72 %	19 %
Frankreich	6 %	68 %	16 %
Singapur	4 %	84 %	12 %

6 Raubkriminalität

Die Raubkriminalität hat zwar in den letzten zwei Jahren leicht zugenommen (auf derzeit fast 59.800 Fälle). Aber sie lag damit um über 14 % unter dem Höchststand von 1997.

6.1 Bank- und Poststellenraub

918 Raubüberfälle auf Geldinstitute, Postfilialen und Postagenturen wurden 2003 begangen. Die Zahl dieser oft mit Schusswaffen durchgeführten Raubüberfälle – von den über 11.000 Fällen, in denen 2003 mit einer Schusswaffe gedroht wurde, waren die weitaus meisten (95,7 %) Raubüberfälle – ist seit den 80er Jahren konstant rückläufig gewesen, dank der Verwendung zeitverzögernder Geldautomaten und lückenloser Videoüberwachung der Schalterräume. Nur 2002 lag die Zahl um 5,3 % niedriger. Dass die Überfälle auf Postagenturen 2003 um 50 % (auf 45) gestiegen sind, ist vermutlich sowohl auf eine Zunahme der Postagenturen (zu Lasten von Postfilialen) zurückzuführen wie auf Mängel ihrer technischen Ausstattung.

Der Bankraub könnte noch erfolgreicher bekämpft werden, wenn alle Bankfilialen/Poststellen ihre Videoüberwachungsanlagen zur Polizei aufschalten würden. Die informierte Polizei könnte sich dann schon vor dem Eintreffen am Tatort „ein Bild“ von der Zahl und Gewaltbereitschaft der Täter und den am Tatort herrschenden Zuständen machen.

6.2 Raubüberfälle auf Geld- und Wertspezialtransporte

Dass 2003 nur 11 Überfälle auf Geld- und Wertspezialtransporte verübt wurden (2002: 12), darf nicht darüber hinwegtäuschen, mit welcher Brutalität solche Überfälle sehr oft begangen werden. So haben am 29. April 2004 fünf Täter bei Wetter-Volmarstein in Nordrhein-Westfalen einen Geldtransporter überfallen und mit zwei Maschinenpistolen zehnmal auf den Fahrer und den Beifahrer geschossen. Nur dank der Panzerung des Fahrzeugs wurde niemand ernsthaft verletzt. Die Täter drohten auch mit dem Einsatz einer Panzerfaust, dessen Attrappe sie mitführten.

Immer wieder ereignen sich brutale Überfälle auf Geld- und Werttransporter, deren Panzerung sich letztlich als lebensrettend für die Besatzung des Fahrzeugs erweist. Es kann nicht oft genug betont werden, dass Geldtransportfahrzeuge nur dann ausreichend gesichert sind, wenn sie den Bestimmungen der Unfallverhütungsvorschrift „Fahrzeuge“ (BGV D 29) und insbesondere der BG-Vorschrift „Sicherheitsregeln für Geldtransportfahrzeuge“ (BGR 135) entsprechen. Wie wichtig ferner die strikte Einhaltung der 2003 neu gefassten Sicherheitsvorschriften der BDGW ist, wird in den 2003 erstatteten Jahresberichten der Sicherheitsbeauftragten der BDGW hervorgehoben. Konkret wird u.a. empfohlen:

- Sicherstellung einer umfassenden Nachweisführung über Existenz und Verbleib sicherheitsrelevanter Schlüssel, Kombinationen, Patches und ID-Karten
- Veränderungen der Zahlenkombinationen an den Wertgelassen in unregelmäßigen Zeitabständen
- Keine Auftragsannahme in den Fällen, in denen der Auftraggeber fordert, dass ein GAA auch dann zu versorgen und zu entsorgen ist, wenn der direkte Zugriff auf die Werte nur durch eine Zahlenkombination geschützt ist

- Regelmäßige Überprüfungen der Bildaufnahme- und Bildwiedergabequalität sicherheitsrelevanter Abläufe
- Sorgfalt bei der Personalauswahl, insbes. bei der Überprüfung der Zuverlässigkeit und Integrität.

6.3 Überfälle auf Tankstellen und andere Geschäfte

Geschäfte sind im Vergleich zu Banken sicherheitstechnisch oft nicht optimal ausgerüstet. Deshalb ist die AQ hier mit 46,5 % wesentlich niedriger als bei Banküberfällen (AQ 67,5 %). Insgesamt 5.095 solcher Überfälle wurden 2003 begangen.

Leicht angestiegen gegenüber dem Vorjahr sind auch die Raubüberfälle auf Tankstellen (um 2,5 % auf 1.256 Fälle), im Vergleich zu 1998 um 43 %. Auch hier ist die sicherheitstechnische Ausstattung nicht überall optimal.

7 Naturkatastrophen, Brände, Arbeitsunfälle

Wie stark auch die Wirtschaft von Naturkatastrophen betroffen sein kann, hat die „Jahrhundertflut“ des Jahres 2002 deutlich werden lassen.

Eine Untersuchung des Schweizer Rückversicherers Swiss Re hat ergeben, dass die weltweiten Schäden durch Naturkatastrophen 2003 durchschnittlich hoch ausgefallen sind. Demnach entstanden volkswirtschaftliche Schäden von 70 Mrd. Dollar, wobei 18,5 Mrd. Dollar versichert waren. Dieser Wert lag seit 1987 durchschnittlich bei 20 Mrd. Dollar.
Der Studie zufolge gibt es immer mehr Hinweise für einen Anstieg von extremen Wettermustern. Außerdem seien deutliche Anzeichen zu erkennen, dass die Zahl der Großschäden zunimmt. So habe es zuletzt sechs Ereignisse gegeben, bei denen die fällige Versicherungssumme eine Milliarde Dollar überschritten habe. Faktoren für diesen Trend seien eine steigende Bevölkerungsdichte, höhere Konzentration von versicherten Sachschäden und die Erschließung exponierter Gebiete.

Die Zahl der vorsätzlich oder in strafbarer Weise fahrlässig verursachten Brände hat sich nach der PKS unterschiedlich entwickelt:

	2003	1998	1993
vorsätzliche Brandstiftung	15.450	14.111	15.018
fahrlässige Brandstiftung	14.858	10.227	8.918

Insgesamt stellt die Brandgefahr – je nach Art des Unternehmens – die größte physische Gefahr für seine Existenz dar. Umso wichtiger ist ein optimaler vorbeugender baulicher und technischer Brandschutz und die Einhaltung aller Vorschriften für die Lagerung und Bearbeitung brand- und explosionsgefährlicher Stoffe sowie für die Durchführung entsprechender gefährlicher Produktionsprozesse. Vorbeugender baulicher und technischer Brandschutz, eine hoch entwickelte Gas-, Rauch- und Brandmeldetechnik und je nach Örtlichkeit und Rahmenbedingungen optimale Löschanlagen- und Löschmitteltechnik stehen zur Verfügung.
Zum vorbeugenden baulichen Brandschutz gehört eine zuverlässige Planung und Sicherung von Fluchtwegen. Die Berechnung, wie lange es dauert, bis alle Beschäftigten ein Betriebs- oder Geschäftsgebäude verlassen haben und wo Staus auftreten, wird jetzt durch eine neu entwickelte Simulations-Software erleichtert. Mit dieser Software lässt sich auch gut feststellen, ob Hindernisse wie Säulen oder Schränke einen Stau verursachen können.

Die Zahl der Arbeitsunfälle in Deutschland ist 2003 auf ein Rekordtief gesunken. Verbesserte Vorsichtsmaßnahmen führten binnen Jahresfrist zu einem Rückgang um 10,5 % auf ca. 871.000 registrierte Unfälle. Die insgesamt positive Entwicklung wird auf die erhöhten Anstrengungen der Unternehmen zurückgeführt, Unfälle zu vermeiden. 2003 wurden 29,4 Arbeitsunfälle je 1.000 Vollzeitarbeitskräfte gemeldet. 2002 lag die Quote noch bei 32,4. Dies entspricht einem Rückgang um 9,5 %. Die Zahl der tödlichen Arbeitsunfälle verringerte sich um 5 %. Die erfreuliche Entwicklung setzt sich fort. Im ersten Halbjahr 2004 ist die Zahl der Arbeitsunfälle nochmals um 6 %, die der Wegeunfälle um annähernd 11 % gesunken, wie der Hauptverband der gewerblichen Berufsgenossenschaften am 27. August mitteilte. Da die Unfallversicherung allein von den Unternehmen über eine Umlage auf die Lohnsumme finanziert wird, wird sich der Rückgang auch positiv auf die Kosten der Unternehmen aus.

Trotz dieser erfreulichen Entwicklung müssen alle Anstrengungen fortgeführt werden, um den Arbeitsschutz ständig zu optimieren.

8 Sachbeschädigungen durch Vandalismus, Graffiti und Scratching

Durch Graffiti und andere mutwillige Beschädigungen verunstaltete gewerbliche Liegenschaften beeinträchtigen über den materiellen Schaden hinaus auch das Image des Unternehmens.

8.1 Graffiti

Immer mehr Bauwerke im öffentlichen Raum und öffentliche Transportmittel werden von Jugendlichen mit Graffiti verunstaltet. In einer Bundestagssitzung am 15. Januar 2004, in der Gesetzentwürfe der CDU/CSU, der FDP und des Bundesrates zur Schaffung eines neuen Straftatbestandes des Verunstaltens zur Debatte standen, wurde der jährliche Schaden von Gemeinden und Privateigentümern durch Graffiti mit 200 bis 250 Mio € geschätzt. Die Reinigungskosten liegen – je nach Untergrundbeschaffenheit und Eindringtiefe der Schmierschrift – zwischen 15 und 60 € pro qm. Keines der von ca. 30 Firmen in Deutschland hergestellten Produkte kann das Aufsprühen verhindern. Die Anstriche sorgen nur dafür, dass die Oberfläche schnell wieder von der Schmierschrift befreit werden kann. Die richtige Entscheidung zwischen Permanent- und Semipermanentanstrich sowie temporärem Schutzsystem wird vom Untergrund und dem möglichen Aufwand für die Reinigung bestimmt. Dauerhafte Schutzschichten überstehen zwar bis zu 20 Reinigungen, sind jedoch verhältnismäßig teuer, während Wachsbeschichtungen nur wenige Jahre halten.

Videoüberwachungsmaßnahmen sind nur punktuell sinnvoll. Bewährt hat sich hingegen die Mobilisierung der Öffentlichkeit, Schmierereien unverzüglich anzuzeigen und so die Fahndungsmöglichkeiten zu verbessern. Da die Rechtsprechung den Straftatbestand der Sachbeschädigung nur als erfüllt ansieht, wenn die beschmierte Fläche offensichtlich in ihrer Substanz beschädigt wird und es umstritten ist, ob diese Voraussetzung erst vorliegt, wenn die Farbe in das Mauerwerk eindringt, bemühen sich einige Bundesländer seit Jahren über den Bundesrat einen Straftatbestand in das Strafgesetzbuch aufnehmen zu lassen, nach dem schon die erhebliche Veränderung des Erscheinungsbildes eines Gebäudes oder eines Fahrzeugs gegen den Willen des Eigentümers strafbar ist. Der seit ca. zwei Jahren im Bundestag liegende Gesetzentwurf wird jedoch mit dem Argument blockiert, es handle sich um ein Vollzugsproblem, weil nur 30 % aller Sprayer ermittelt würden und in den allermeisten Fällen, in denen es zu einem Strafverfahren kommt, eine Sachbeschädigung zweifelsfrei belegt werden könne. Der Freistaat Sachsen hat inzwischen eine Verordnung erlassen, nach der das Sprühen von Graffiti als Ordnungswidrigkeit mit einer Geldbuße bis zu 1.000 € geahndet wird.

8.2 Scratching

Unter den vandalistischen Praktiken hat das „Scratching“ – das Zerkratzen von Scheiben – in den letzten Jahren deutlich zugenommen. Zerkratzt werden alle möglichen Glasflächen, insbesondere Fenster in Straßen- und Regionalbahnen, Glasflächen an Haltestellen und Schaufenstern. Allein der Stadt Köln entstehen dadurch jährlich Schäden von mehr als 1,5 Mio €. Zunehmend werden in Bussen und Bahnen des ÖPNV Videokameras installiert, um sowohl Gewalttätigkeiten wie vandalistischen Sachbeschädigungen durch Abschreckung und Täterermittlung vorzubeugen.

9 Vermögens-, Fälschungs- und Wirtschafts- und Organisierte Kriminalität

9.1 Vermögens- und Fälschungskriminalität

Die Vermögens- und Fälschungskriminalität wird in der PKS mehrfach abgestuft aufgegliedert. Sie wird hier nur insoweit behandelt, als sie nicht den im nachfolgenden Abschnitt (9. Wirtschaftskriminalität) zuzuordnen ist.

i.T.	2003	1998
Vermögens- und Fälschungskriminalität	1.111	899
Davon:		
Betrug	876	706
Unterschlagung	103	78
Urkundenfälschung	69	75
Veruntreuungen	51	32
Insolvenzstraftaten	7	4
Geld-, Wertzeichen- u. Kartenfälschung	6	4

Anders als bei den meisten Deliktsgruppen der Raub- und der Diebstahlskriminalität nimmt die Vermögens- und Fälschungskriminalität tendenziell zu. Ursächlich für diese massive Strukturverschiebung in der Kriminalität ist vor allem die immer komplexere Entwicklung der Wirtschaftsbeziehungen und Geschäftsverkehre, die Kriminellen vielfältige Ansatzpunkte für leichtere Bereicherungsmöglichkeiten bietet als der physische Angriff auf das Eigentum.

9.2 Wirtschaftskriminalität

Der Wirtschaftskriminalität werden Straftaten zugerechnet, die im Rahmen wirtschaftlicher Tätigkeit begangen werden und über eine Schädigung von Einzelnen hinaus das Wirtschaftsleben beeinträchtigen und die Allgemeinheit schädigen können, und/oder deren Aufklärung besondere kaufmännische Kenntnisse erfordert. Diese unscharfe Definition führt im Einzelfall zu Abgrenzungsschwierigkeiten.

	2003	1998
Wirtschaftskriminalität	86.149	86.232
und zwar:		
bei Betrug	42.764	52.604
bei Insolvenzstraftaten	13.902	18.536
bei Wettbewerbsdelikten	5.071	6.833
iZm Arbeitsverhältnissen	14.896	6.722
iZm Beteiligungen und Kapitalanlagen	11.105	15.068

Die Anzahl der erfassten Fälle von Wirtschaftskriminalität ist in den letzten Jahren stark geschwankt:

1999: + 26,3 %
2000: - 16,7 %
2001: + 23,1 %
2002: - 22,9 %
2003. + 0,1 %

Solche Schwankungen werden im Wesentlichen durch größere Ermittlungskomplexe mit vielen Einzelfällen beeinflusst.

Wie schadensintensiv sich Fälle von Wirtschaftskriminalität auswirken, wird im Jahresbericht Wirtschaftskriminalität des BKA dargestellt: Die Fälle hatten rein quantitativ nur einen Anteil von 1,32 % an der Gesamtkriminalität des Jahres 2002, verursachten aber ca. 50 % des materiellen Schadens der Gesamtkriminalität.

Dabei sind die immateriellen Schäden noch gravierender:
- Folgewirkungen von kriminell verursachten Wettbewerbsverzerrungen
- Verlust des Vertrauens in die Redlichkeit einzelner Berufe und Branchen
- gesundheitliche Gefährdungen als Folge von Verstößen gegen Umweltrecht, gegen das Arbeitsschutzrecht, das Lebensmittel- und Arzneimittelrecht
- Verlust von Arbeitsplätzen.

In einer Ende 2002 durchgeführten Studie der Wirtschaftsprüfungsgesellschaft ERNST & YOUNG wurden 203 Unternehmen repräsentativ ausgewählt und befragt. Sie gingen von einem Anstieg der Wirtschaftskriminalität in den nächsten 5 Jahren aus und nehmen an, dass nur jede zweite Tat entdeckt wird. Nur 60 % der befragten Unternehmen verfügten über spezielle interne Kontrollverfahren oder Prüfungsmethoden durch die Innere Revision, um sich vor Verletzungen ihres geistigen Eigentums zu schützen. Die Wirksamkeit interner Sonderprüfungen sowie spezieller Maßnahmen durch die Innere Revision wird von der Hälfte der Unternehmen als hoch eingeschätzt. Als effiziente Maßnahme zum Schutz vor wirtschaftskriminellen Handlungen wird in der Studie die kontinuierliche Überprüfung der im Computersystem des Unternehmens gespeicherten Daten genannt.

Das BKA führt im Jahresbericht Wirtschaftskriminalität 2002 als mögliche Ansätze zur präventiven Bekämpfung von Wirtschaftskriminalität durch die Wirtschaft selbst an:

- Warnfunktion zum frühest möglichen Zeitpunkt durch intensive Marktbeobachtung der „seriösen“ Wirtschaftsteilnehmer und Mitteilung (neuer) fragwürdiger Praktiken und Unternehmen an die Strafverfolgungsbehörden
- Institutionalisierter (anlass- bzw. themenbezogener) Info-Austausch (Wirtschaft/Polizei/Staatsanwaltschaft)
- Einwirkung auf „schwarze Schafe“ über Interessenverbände der Wirtschaft
- Prävention durch Verringerung der Tatgelegenheitsstrukturen (z.B. technische Sicherheitsvorkehrungen gegen Softwarepiraterie).

9.3 Organisierte Kriminalität

9.3.1 Deutschland

Die OK hat in den letzten Jahren nichts von ihrer Bedrohlichkeit verloren – weder in Deutschland noch in Europa. Zwar ist die Zahl der Verfahren, in denen Straftaten der OK ermittelt wurden, auf 637 gesunken. Das ist ein Rückgang von über 25 % gegenüber dem Höchststand von 854 Verfahren im Jahr 2000. Aus dem Rückgang kann aber – wie das BKA im Bundeslagebild Organisierte Kriminalität 2003 feststellt – kein Rückgang der OK gefolgert werden. Die Lageerkenntnisse sind vielmehr vom Ressourceneinsatz und dem Ausmaß und der Intensität der Strafverfolgung abhängig.

Von den in der (unglücklichen) Definition genannten alternativen Voraussetzungen für OK
- unter Verwendung gewerblicher oder geschäftsähnlicher Strukturen
- unter Anwendung von Gewalt
- unter Einflussnahme auf Politik, Medien, öffentliche Verwaltung, Justiz oder Wirtschaft
erfüllten 599 Erfahren 2003 die erste Alternative.
In 32 Verfahren wurden strafrechtlich relevante Korruptionshandlungen festgestellt.

Die für den Berichtszeitraum 2003 gemeldet Schadenssumme betrug rund 522 Mio Euro. Sie lag deutlich unter den Werten der Vorjahre (2002: 3,1 Mrd. Euro), was nach Feststellungen des BKA maßgeblich auf den Rückgang bei Steuer- und Zolldelikten zurückzuführen ist. Dennoch wurden die nächsten Schäden bei den Steuer- und Zolldelikten (ca. 126 Mio €) und insbesondere bei der Kriminalität iZm dem Wirtschaftsleben (ca. 280 Mio €) verursacht. Bei der zuletzt genannten Begehungsform wurden auch die höchsten kriminellen Gewinne (ca. 164 Mio €) erzielt. In 161 Ermittlungsverfahren wurden Maßnahmen zur Sicherung der Vermögensabschöpfung getroffen. Dabei wurden Vermögenswerte im Gesamtwert von rund 69 Mio € (mehr als doppelt so viel wie 2002) vorläufig gesichert.

Mit einem Anteil von fast 14 % aller OK-Verfahren stellt Kriminalität iZm dem Wirtschaftsleben 2003 den drittgrößten Kriminalitätsbereich dar. Die Aktivitätsschwerpunkte der OK-Gruppierungen in diesem Bereich waren sehr breit gestreut. Am häufigsten begingen die Gruppierungen Finanzierungsdelikte (insb. Kredit- und Warenkreditbetrug), Anlagebetrug sowie Wettbewerbsdelikte (insbes. Ausschreibungsbetrug).

Der Anteil deutscher Gruppierungen ist bei der OK iZm mit dem Wirtschaftsleben erneut gestiegen und liegt bei über 60 %. Dies steht im Kontrast zum Anteil deutscher Staatsangehöriger in allen OK-Verfahren, der nach 48 % im Jahr 2001 und 44,4 % 2002 im Jahr 2003 nur noch 38,8 % betrug.

9.3.2 Europa

Im März 2004 hat EUROPOL über die Entwicklung der OK in Europa im Jahr 2003 berichtet. Laut EUROPOL haben die OK-Aktivitäten im EU-Raum in den vergangenen 15 Jahren kontinuierlich zugenommen. Eine Trendumkehr scheint in naher Zukunft kaum wahrscheinlich. Die mit der Osterweiterung verbundene Grenzöffnung wirke wie eine Einladung für die OK. 2001 seien 3.000 OK-Gruppen im EU-Raum mit ca. 30.000 Mitgliedern registriert gewesen. Im Jahr 2003 seien es 4.000 Organisationen mit etwa 40.000 Mitgliedern – Tendenz steigend.
Die Internationalität der OK-Netze nimmt laut EUROPOL ständig zu, sowohl was die Beteiligten, als auch die Operations- und Rückzugsgebiete betrifft. Die Mannschaftsstärke wächst mit den Einzugsgebieten. In Europa immer stärker vernetzt tauschen sich die OK-Gruppen auch mit ihresgleichen in Kanada, den USA, China, Kolumbien, dem Iran, Marokko, Nigeria, Pakistan, Surinam, der Türkei und Vietnam aus. Die OK habe sich zusammen mit der Weltwirtschaft globalisiert.

Warenschmuggel, Betrügereien aller Art, vor allem mit der Mehrwertsteuer, haben sprunghaft zugenommen. Die OK nutzt auch Erleichterungen bei der Firmenniederlassung und der Flexibilität von Arbeitskräften. Auch das erschwere die Überwachung laut EUROPOL. Die Bewegungsfreiheit im EU-Raum habe enorm zugenommen. Die legale Wirtschaft werde dadurch seitens der OK empfindlich geschädigt.

EUROPOL betont, dass die Urbanisierung mit ihrer Anonymität dunkle Geschäfte begünstigt. Die leichten Reisemöglichkeiten kämen den multinationalen und multikulturellen OK-Netzen gerade recht. Diaspora von Flüchtlingen und Einwanderern böten sich der OK als Reservoir

für Manpower und lokales Know how an. EUROPOL nennt hier speziell Türken, Albaner, Nigerianer, Iraner und Iraker. EUROPOL sieht wachsende Gefahren für die offene Gesellschaft und befürchtet ein Abnehmen des Vertrauens der Bevölkerung in Justiz und Politik.

Eine weitere Gefahr sieht EUROPOL in der rasanten technischen Entwicklung. Davon profitiert natürlich auch die OK. Telekommunikation, Logistik, Cyberspace, alles sei der OK willkommen, ganz besonders das E-Business wegen seiner Anonymität. Prepaid Handys seien ein Knüller bei Kriminellen. Gerne benutzt würden auch Krypto-Handys. Beliebt seien gestohlene Sim-Cards, die ständig gewechselt werden.

Laut EUROPOL ist die OK zu einer komplexen Industrie herangewachsen. Bei OK-Aktivitäten laufe ein Prozessmanagement mit vielen Einzelaktivitäten ab:

- Verträge mit Zulieferern und Subunternehmen
- Geldbeschaffung
- Transport, Lagerung und Verteilung von Waren
- Dokumentenfälschung und
- Sicherheitsüberwachung aller Vorgänge.

EUROPOL gibt in seinem Jahresbericht auch detaillierten Einblick in die verschiedenen OK-Gruppen, die in der EU aktiv sind und wie sie zusammenarbeiten. Besonders viele Kontakte bestehen zur Mafia in den Niederlanden. Betrachtet man die weiter westlich gelegenen EU-Staaten, so kommt der spanischen OK eine ähnlich herausragende Stellung zu, vor allem beim Handel und Schmuggel mit Haschisch und Kokain. Die italienische Mafia arbeite dagegen bevorzugt mit Albanern zusammen. Es geht um Drogen und Menschenhandel. Belgische OK-Gruppen haben Kontakt nach England, in die Niederlande, nach Deutschland, Frankreich und Albanien.

Die albanische OK gilt derzeit als besonders aggressiv. Ihr Geschäft liege im Bereich Drogen und Menschenhandel. Sie neigten zu exzessiver Gewalt.

Die russische OK ist laut EUROPOL eine der mächtigsten. Zu ihren Geschäftsfeldern gehören illegale Finanzgeschäfte, vor allem Geldwäsche, Schutzgelderpressung und illegale Einwanderung. Die russische OK sei bekannt für streng hierarchische Ordnung und effektive Arbeitsteilung.

Die türkische OK tummele sich im Drogen- und Waffengeschäft, sei aber auch bei Geldwäsche und Schutzgelderpressung aktiv.

Nach den Türken sei die Polen-Mafia die Nummer zwei in Deutschland. Fahrzeugdiebstähle und Zollbetrügereien aller Art, ebenso Warenschmuggel, gehen auf das Konto der Polen-OK, die mit der polnischen Gemeinde in Deutschland zusammenarbeite.

Die baltischen Länder seien eine Drehscheibe für den Warenschmuggel im nordeuropäischen Raum. Die dortige OK engagiere sich außerdem bei Frachtdiebstählen und Fälschereien.

Als höchst dynamisch bezeichnet EUROPOL die Rumänen- und Bulgaren-OKs, ebenso breit seien deren Betätigungsfelder.

9.3.3 Geldwäsche

Geldwäsche ist ein typisches Handlungsmuster der OK. Die Schätzungen über den jährlichen Gesamtbetrag des gewaschenen Geldes sind rein spekulativ. Die Zahl der Hinweise auf Geldwäschehandlungen in OK-Verfahren nimmt zwar zu, 2003 wurden in 197 OK-Verfahren Hinweise auf Geldwäscheaktivitäten festgestellt. Der Bekämpfungsansatz über die Finanzspur bleibt aber ein überaus schwieriger Weg. Im Jahr 2003 wurden insgesamt 745 Verdachtsfälle in der PKS registriert. Das sind 30 % weniger als im Jahr zuvor. Angesichts des vermutlich riesigen Dunkelfeldes geben diese Zahlen nicht im Entferntesten die Realität wieder.

Ein Ende Juni 2004 veröffentlichter Entwurf für eine neue EU-Richtlinie sieht vor, künftig auch Treuhand- und Unternehmensdienstleister sowie Versicherungsvermittler zur Feststellung der Identität und Überprüfung ihrer Kunden und bei Geldwäscheverdacht zum Kontakt mit den Sicherheitsbehörden zu verpflichten. Bislang gibt es entsprechende Vorschriften für Kredit- und Finanzinstitute, Abschlussprüfer, Immobilienmakler, Spielkasinos und Angehörige der Rechtsberufe. Nach dem Entwurf sollen die Geldwäschevorschriften künftig zudem für alle Personen gelten, die Geschäfte gegen Barzahlung in Höhe von mindestens 15.000 € tätigen.

10 Einzelne Deliktsbereiche der Vermögens-, Fälschungs- und Wirtschaftskriminalität

10.1 Betrug

Allein die Betrugskriminalität wird in der PKS in 19 Deliktsgruppen (teilweise mit Untergruppen) differenziert, von denen hier nur die wichtigsten genannt werden können:

	2003	1998
Waren- u. Warenkreditbetrug	225.909	123.908
Erschleichen von Leistungen	176.019	159.463
Leistungskreditbetrug	32.459	20.743
Leistungsbetrug	27.486	29.542
Sozialversicherungsbetrug	22.207	21.539
Computerbetrug	11.388	6.465
Beteiligungs- u. Kapitalanlagebetrug	10.287	15.144
Versicherungsbetrug	8.605	1.135
Geldkreditbetrug	7.508	11.165
Grundstücks- u. Baubetrug	719	915

Besonders hervorzuheben ist der Betrug zu Lasten der EU. Nach dem Jahresbericht der EU-Kommission zur Betrugsbekämpfung gingen schon 2002 durch betrügerische Machenschaften 1,18 Mrd. € an Haushaltsmitteln verloren, wobei offenbar Meldungen und Untersuchungen durch einzelne Mitgliedsstaaten unterblieben, damit die Staaten nicht für den entstandenen Schaden haftbar gemacht werden konnten. Besonders viele Betrugsfälle ereignen sich im Zusammenhang mit Subventionen für die Landwirtschaft sowie mit Unterstützungsprogrammen für Osteuropa. 2003 war erstmals seit drei Jahren wieder ein Anstieg der ermittelten Subventionsbetrugsfälle zu verzeichnen. Die dennoch geringe Zahl von 625 ermittelten Fällen lässt eine hohe Dunkelziffer vermuten. Der Schaden ging auf 67,7 Mio Euro zurück. Inwieweit dies auf eine verstärkte Kontrolle der Vergabestellen oder auf restriktivere Bewilligungen aufgrund der angespannten Lage öffentlicher Haushalte zurückzuführen ist, muss

offen bleiben. Bei den gemeldeten Fällen im Rahmen von Strukturfondmitteln lag Deutschland 2002 mit ca. 2.000 Fällen weit an der Spitze vor den Niederlanden (932) und Frankreich (463). Bei den Beanstandungen im Bereich der Agrarfondsmittel liegt Spanien mit 997 Fällen vor Deutschland (712) und Frankreich (451)

Das Europäische Amt für Betrugsbekämpfung (OLAF) hat sich nach dem Jahresbericht 2002/2003 auf 1.200 Fälle konzentriert. Nach eigenen Schätzungen beläuft sich das Finanzvolumen der von Juli 2002 bis Juni 2003 abgeschlossenen Fälle auf über 850 Mio €.
In dem Zeitraum wurden 375 neue Untersuchungen eingeleitet und 805 abgeschlossen. Dabei hat sich OLAF vor allem auf Fälle des Betrugs und der Korruption konzentriert.
Die Hälfte der Vorwürfe wegen Korruption innerhalb der EU-Einrichtungen betrafen Unregelmäßigkeiten bei Ausschreibungs- und Zuschussverfahren sowie bei der Auftragsvergabe. Die meisten Hinweise kamen aus Italien, Belgien und Deutschland.

Der Jahresbericht enthält eine Fülle von Fallbeispielen, die die Betrugsanfälligkeit des Gemeinschaftshaushalts aufzeigen. Die meisten Betrügereien finden in EU-Mitgliedstaaten und im Rahmen des Handels mit Drittstaaten statt. Am 30. Juni 2003 waren im Case Management System von OLAF insgesamt 3.440 Fälle registriert. Die meisten Anstöße zu Untersuchungen (ca. 26 %) kamen von der Kommission, 5 % von anderen EU-Einrichtungen, 18 % von den Mitgliedstaaten, 47 % aus sonstigen Quellen, insbesondere Medien. Von den EU-Staaten kamen die meisten Meldungen aus Italien (89), Belgien (83), Deutschland (79) und Spanien (70).

Im Modus operandi bei Betrugs- und Untreuehandlungen im Zusammenhang mit Beteiligungen und Kapitalanlagen hat das BKA im Jahr 2002 u.a. folgende Veränderungen beobachtet: Anleger werden nicht nur mit hohen Renditeversprechen geködert. Inzwischen spielt auch das Sicherheitsdenken, z.B. bezüglich der Altersvorsorge, bei vielen Anlageprojekten eine wesentliche Rolle. Anlagegelder werden u.a. nach dem Schneeballsystem vereinnahmt bzw. veruntreut.

Zur erfolgreichen Vermarktung ihrer Produkte nutzen Anbieter des Grauen Kapitalmarktes darüber hinaus die anhaltende Schwäche des geregelten Kapitalmarktes sowie die Diskussionen über Änderungen des Steuerrechts.
Laut der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) ist eine verstärkte Nutzung des Internet zu beobachten, indem erlaubnispflichtige Dienstleistungen angeboten werden. Der Umfang dieser ohne physische Präsenz in Deutschland betriebenen grenzüberschreitenden Dienstleistungen mit deutschen Kunden hat aufgrund der technischen Entwicklung in den letzten Jahren stark zugenommen. Im Berichtsjahr setzte das Aufsichts- und Verfolgungsinstrumentarium, das auf diese Vertriebsform noch nicht hinreichend eingestellt ist, der Überprüfung durch deutsche Aufsichtsbehörden Grenzen.

Eine weitere Variante stellen Unternehmen dar, die die Sicherheit ihrer Anlageprodukte mit ihrer Mitgliedschaft in der Entschädigungseinrichtung der Wertpapierhandelsunternehmen (EdW) begründen. Die EdW entschädigt Anleger nur unter bestimmten Voraussetzungen und kommt z.B. für fehlerhafte oder unseriöse Anlageberatung nicht auf.

Ferner bestanden laut BaFin bei einzelnen konzessionierten Instituten Anhaltspunkte für ein unseriöses Geschäftsgebaren, eine undurchsichtige Vertriebsorganisation oder das Angebot dubioser Anlageprodukte. Das unseriöse Geschäftsgebaren bestand z.B. in Gebührenschinderei („Churning“) oder zielgerichteter „Kurspflege“ eigener Aktien zur Vertriebs- bzw. Kurssteigerung, die der tatsächlichen Werthaltigkeit nicht entsprach.

Durch Bilanzmanipulationen einzelner börsennotierter Unternehmen wurde das Vertrauen Tausender Anleger schwer geschädigt. Wie der Vorsitzende der Deutschen Prüfstelle für Rechnungslegung (DPR) kürzlich mitteilte, wird in einem von der Bundesregierung vorberei-

teten Bilanzkontrollgesetz die DPR mit der Bilanzüberwachung der 980 an der Börse notierten deutschen Firmen betraut werden. Damit hat in Zukunft erstmals eine privatrechtlich organisierte Institution neben Abschlussprüfer und Aufsichtsrat das Recht auf Einsicht in die Unternehmensbilanzen. Wenn betroffene Unternehmen nicht mit den DPR-Prüfern kooperieren, kann die BaFin eingeschaltet werden. Sie setzt eine Bilanzprüfung dann mit hoheitlichen Mitteln durch. Die Behörde kann das Unternehmen zur Veröffentlichung von Rechnungslegungsfehlern verpflichten und bei der Feststellung von Ordnungswidrigkeiten bis zu 50 000 Euro Geldbuße verhängen.

10.2 Betrug mittels rechtswidrig erlangter unbarer Zahlungsmittel

Betrug mittels rechtswidrig erlangter unbarer Zahlungsmittel	2003	2002
	130.467	116.344
davon:		
mittels Debitkarten ohne PIN	64.507	40.348
mittels Debitkarten mit PIN	35.954	36.969
mittels Kreditkarten	21.469	29.326
mittels Scheck	2.880	4.135
mittels Daten von Zahlungskarten	2.434	3.354

Auch gegenüber dem Vorjahr ist der Betrug mittels rechtswidrig erlangter unbarer Zahlungsmittel um über 12 % angestiegen, im Wesentlichen wegen der Zunahme des Betrugs mittels Debitkarten ohne PIN (Steigerung um fast 60 % mit einer Schadenssumme von fast 39 Mio. €). Obwohl Debitkarten der Banken sicherer sind, wenn die Zahlung erst nach Eingabe des PIN-Codes erfolgt, begnügt sich der Einzelhandel mit dem unsicheren elektronischen Lastschriftverfahren, bei dem nur die Unterschrift auf dem Kassenbeleg verlangt und zu ungenau geprüft wird. Auch auf eine Ausweiskontrolle wird bei geringeren Beträgen verzichtet. Die Folge: Wenn der Kunde die EC-Karte sperren lässt, bleibt der Verkäufer auf den Kosten des betrügerischen Einkaufs sitzen. Ein Ausweg läge in der Übermittlung der Daten gesperrter EC-Karten von der Polizei an den lokalen Einzelhandel, der die Karte dann für einige Tage sperrt. Aber der Aufwand für ein solches flächendeckendes System erscheint den meisten Bundesländern zu hoch. Die Innenminister von Bund und Ländern möchten den Einzelhandel dazu bewegen, auf PIN-Nummer-Systeme umzusteigen. Der Einwand des Handels: Bei Systemen mit PIN-Eingabe seien die Bankgebühren zu hoch (etwa0,3 % des Umsatzes).

Seit Anfang des Jahres 2004 werden – wie das BKA mitgeteilt hat - zunehmend EC-Karten von deutschen Urlaubern in der Südtürkei unbemerkt kopiert und die dazu gehörige PIN ausgespäht. Die Handlungen finden in Geldwechselstuben, Schmuck- und Juweliergeschäften statt. Die so erlangten Kartendaten werden zur Fertigung von Kartenfälschungen verwendet.
Mit den gefälschten Karten werden in den meisten Fällen innerhalb von 3 Wochen unberechtigte Verfügungen an Geldautomaten in der Türkei, Großbritannien, Belgien und den Niederlanden vollzogen. Da die Geschädigten weiter im Besitz ihrer Originalkarten verbleiben, schöpfen sie zunächst keinen Verdacht. Erst wenn die Karteninhaber oder ihre Hausbank die Fremdverfügungen auf den Konten bemerken, wird eine Sperrung der Zahlungskarten veranlasst.

Das BKA rät dazu, die PIN-Eingabe verdeckt durchzuführen und die EC-Karte nicht aus den Augen zu verlieren. Erscheint der Bezahlvorgang aufgrund irgendwelcher Merkwürdigkeiten verdächtig, sollte unverzüglich die EC-Karte gesperrt werden.

10.3 Steuerkriminalität, insbes. systematischer Umsatzsteuerbetrug

Durch Steuerkriminalität entgehen dem Staat jährlich Einnahmen in zweistelliger Milliardenhöhe. Zu diesem Ergebnis kommt der Bundesrechnungshof in einem neuen Sonderbericht über systematischen Umsatzsteuerbetrug. Organisierter Umsatzsteuerbetrug basiert stets darauf, dass ein Teilnehmer der Betrugskette Vorsteuer vom Fiskus erstattet bekommt und sie selbst oder ein anderer Teilnehmer die fällige Umsatzsteuer nicht entrichtet. Bemerkt das Finanzamt den Betrug, kann es die fällige Steuer nicht mehr eintreiben, weil der Betrüger sich ins Ausland abgesetzt hat oder insolvent ist.

Der Bundesrechnungshof unterscheidet mehrere Fallgruppen von organisiertem Steuerbetrug:

Karussellgeschäfte:
Bei einem Umsatzsteuerkarussell liefert ein inländischer Unternehmer hochpreisige Güter und erhält diese ohne nennenswerte Preisaufschläge über eine Kette von innergemeinschaftlichen Zwischenhändlern und Scheinfirmen zurück. Dabei wird ausgenutzt, dass innergemeinschaftliche Lieferungen umsatzsteuerfrei sind, Lieferungen innerhalb eines EU-Staates hingegen steuerpflichtig. Die Zwischenhändler kommen ihrer Steuerpflicht jedoch nicht nach, sondern verschwinden, nachdem sie die Vorsteuer kassiert haben. Laut Rechnungshof entstehen EU-weit auf diese Weise Schäden von rund 12 Mrd. €. Seit der Osterweiterung der EU hat der Mehrwertsteuerbetrug mittels gefälschter Zollstempel drastisch zugenommen. Mit gefälschten Stempeln können Betrüger einen Export fingieren und sich so die Mehrwertsteuer vom Lieferanten „zurückerstatten“ lassen, der sie wiederum vom Finanzamt zurückfordert. Um die Betrügereien einzudämmen, wird seit 2001 eine Technik eingesetzt, mit deren Hilfe gefälschte Stempel auf den Ausfuhrbelegen zu erkennen sind. Die vom Fraunhofer-Institut entwickelten Lesegeräte vergleichen den jeweils vorgelegten Stempel mit einem Originalabdruck, der auf einem PC gespeichert ist.

Kettenbetrug im Baugewerbe:
Firmengeflechte mit tatsächlichem oder vorgegebenem Sitz im Ausland verursachen laut Bundesfinanzministerium jährliche Steuerausfälle von rund 64 Mrd. € – fast 15 % des aktuellen Steueraufkommens. Dabei schalten Bauunternehmen gezielt mehrstufige Sub- und Scheinunternehmerketten ein. So verschleiern sie, dass die mit der tatsächlichen Bauausführung beauftragten „Kolonnenschieber“ und die Subunternehmer der unteren Ebenen weder Steuern noch Sozialabgaben zahlen. Hinzu kommt, dass die Subunternehmer dem Generalunternehmer Rechnungen mit Umsatzsteuerausweis erstellen, so dass diese Vorsteuer geltend machen können.

Insolvenz des Leasingnehmers:
Durch geplante Insolvenzen von Leasingnehmern entstehen Umsatzsteuerausfälle „weit im dreistelligen Milliardenbereich“. Der Trick: Bei Leasingverträgen ist sofort der Gesamtwert des Wirtschaftsgutes umsatzsteuerpflichtig. So entstehen beim Leasingnehmer Vorsteueransprüche. Geht der Leasingnehmer pleite, holt sich der Leasinggeber das Gut zurück, und die gezahlte Umsatzsteuer wird ihm erstattet. Die Vorsteuer des Leasingnehmers ist wegen dessen Insolvenz aber nicht mehr eintreibbar.

10.4 Zollkriminalität

Im Vordergrund des Zollbetrugs steht der Schmuggel mit Zigaretten. 400 Millionen hat allein der Zoll im Jahr 2003 sichergestellt. Die organisierten Banden schmuggeln verstärkt kleinere Mengen. Zudem stellt die „Nikotin-Mafia“ immer mehr Zigaretten samt ihrer Verpackung

selbst her. So wurde bei einer Razzia im Juli 2003 in Oberhausen eine aus Russland stammende Maschine entdeckt, die stündlich 1.500 fertig verpackte Stangen mit einem Steuerausfall von 45.000 € produzierte. Im Juli 2004 gelang Fahndern von Zoll und Polizei die Entdeckung einer internationalen Bande, die 44 Millionen unverzollter Zigaretten geschmuggelt hatte. Sie hatten dabei einen Steuerausfall von mehreren Millionen Euro verursacht. Der „Verband der Deutschen Cigarettenindustrie“ befürchtet, dass nach dem Wegfall der Zollkontrollen im Rahmen der Osterweiterung der EU der Schmuggel mit Zigaretten noch weiter steigt. Neben dem „Ameisenverkehr“ ist dies ein Operationsbereich Organisierter Kriminalität, bei dem ein „Unternehmer“ von Mittelsmännern jenseits der Grenze eine Containerladung Zigaretten aufkauft, um sie diesseits der Grenze durch eine gesonderte Verteilorganisation möglichst schnell an Konsumenten verkaufen zu lassen.

10.5 Schwarzarbeitskriminalität

10.5.1 Umfang der Schwarzarbeit

Die Schätzungen des Umfangs der Schwarzarbeit in Deutschland reichen von 300–370 Mrd. € jährlich. Der gesamtwirtschaftliche Schaden durch entgangene Steuereinnahmen und Sozialversicherungsbeträge wird auf einen mindestens zweistelligen Milliardenbetrag geschätzt. Allein in den vom Zoll ermittelten Fällen ergab sich 2003 ein Gesamtbetrag von 348 Mio € hinterzogener Steuern und Abgaben. Das waren 82 % mehr als im Jahr 2002. Mehr als 9 Millionen Menschen arbeiten zumindest teilweise schwarz. Die IG Bergbau schätzt die Zahl der illegalen Arbeitsverhältnisse im Baugewerbe auf ca. 300.000.

Dass die Schwarzarbeit in die Organisierte Kriminalität hineinreicht, zeigt folgender in der Süddeutschen Zeitung am 23. März geschilderter Fall: Die Hamburger Polizei hatte einen internationalen Schwarzarbeitsring zerschlagen. Fünf Hauptverdächtige wurden verhaftet. Die Bande soll mehr als 4,6 Mio € Schaden verursacht haben. Nach zwei Anzeigen wegen Verdachts der Geldwäsche ermittelte das Hamburger LKA gegen Bandenmitglieder. Es war aufgefallen, dass von zwei Konten Hamburger Baufirmen größere Mengen Bargeld abgeholt wurden, angeblich zur Bezahlung von Arbeitern. Mehreren Beschuldigten wird vorgeworfen, seit 2000 in großem Stil Ausländer illegal beschäftigt zu haben. Sie wurden nur dann nachträglich und kurz zur Sozialversicherung angemeldet, wenn es Überprüfungen gab. Nach den Ermittlungen haben die Beschuldigten 4,8 Mio € in bar von Geschäftskonten für Schwarzlöhne entnommen. Der harte Kern der Bande besteht aus drei Niederländern und zwei Männern aus dem früheren Jugoslawien. Die Beschuldigten betrieben Baufirmen, die als Werkvertragspartner meist mittelständischer Bauunternehmen Aufträge mit illegal Beschäftigten durchführten.

Innerhalb der (alten) EU werden nach Beurteilung der Europäischen Kammer für Handwerk und Klein- und Mittelbetriebe (UEAPME), einer Vereinigung der Europäischen Wirtschaftskammer Eurochambres und der Europäischen Handelskammer Eurocommerce schätzungsweise 10–16 % des Bruttosozialprodukts von der Schattenwirtschaft erzeugt. Nach der von der UEAPME angegebenen Zahl der schwarz Beschäftigten innerhalb der EU von rund 21 Millionen Menschen liegt Deutschland weit über dem Durchschnitt.

Ähnlich beurteilt das der Präsident des Bundesverbandes deutscher Unternehmensberater BDU e.V., Remi Redley. Er sieht kein Anzeichen dafür, dass mit dem derzeitigen Anteil von ca. 16 % des Bruttoinlandsprodukts ein Höchststand der Schattenwirtschaft erreicht sei. Trotz der von ihm als „wertvollen Beitrag gegen die Fluchttendenzen in Schwarzarbeit und Steuerhinterziehung begrüßten 1. Steuerreform sieht er die Steuer- und Abgabenhöhe als

weiterhin zu hoch und unberechenbar an, um einen durchschlagenden ökonomischen Anreiz zu schaffen, erzielte Einnahmen und erbrachte Dienstleistungen immer ordnungsgemäß anzugeben.

Misst man den Anteil der Schattenwirtschaft nicht nach der sog. Bargeldmethode (Vergleich der tatsächlich umlaufenden Bargeldmenge mit der Geldmenge, die zur Erwirtschaftung des offiziellen BIP erforderlich wäre), sondern aufgrund von Befragungen, so fällt dieser Anteil wesentlich niedriger aus. So kommt eine kürzlich von der EU-Kommission vorgestellte Studie für Deutschland auf lediglich 6 %. Die Studie weist übrigens große Unterschiede zwischen Nord- und Südeuropa auf. Nach ihren Ergebnissen lag der Anteil im Jahr 2000 im Vereinigten Königreich bei 2 %, in Ungarn und Polen im gleichen Jahr zwischen 14 und 19 %. Der höchste Prozentsatz wird 2002 für Bulgarien angegeben: zwischen 22 und 30 %.

10.5.2 Bekämpfung

Es ist zu begrüßen, dass der Bundesfinanzminister die Anstrengungen zur Bekämpfung der Schwarzarbeit verstärken wird. Dazu soll die Zahl der Fahnder von 5.000 um 2.000 erhöht werden. Durch die Zusammenführung der bisher ca. 2.500 Fahnder der Arbeitsämter und der ebenso hohen Zahl zuständiger Zollbeamter unter dem Dach der FKS ist ein systematischeres Vorgehen zu erwarten. Das Gesetz zur besseren Bekämpfung der Schwarzarbeit ist vom Bundesrat am 9. Juli 2004 endgültig beschlossen worden.

Wichtiger als die Zahl der Personenüberprüfungen, die im Jahr 2003 bereits rund 80.000 erreicht, ist die von Bundesminister Eichel betonte Konzentration auf die organisierte Wirtschaftskriminalität, auf Kriminelle, die mit Schwarzarbeit ihre Konten füllen und ehrliche Unternehmer in den Ruin treiben.
Die optimistische Annahme des Bundesfinanzministers, dass die EU-Osterweiterung der Schwarzarbeit keinen weiteren Auftrieb gibt, kann nicht geteilt werden. Vielmehr besteht die Gefahr, dass zunehmend Angebote von Unternehmern aus Billiglohnländern, die sich durch den EU-Beitritt noch mehr als bisher auf die Hochlohnländer ausrichten, den von Dumpingpreisen ausgehenden Druck auf einheimische Unternehmer erhöhen, durch Beschäftigung von Schwarzarbeitern Preise senken zu können.

Im Einzelnen wurden 2003	ermittelt	als materieller Schaden festgestellt
Beitragsbetrug z.N.v. Sozialversicherungen	765 Fälle	14,0 Mio €
Vorenthalten u. Veruntreuen von Arbeitsentgelten	13.921 Fälle	142,4 Mio €
Illegale Ausländerbeschäftigung	191 Fälle	0,948 Mio €
Illegale Arbeitnehmerüberlassung	3.400 Fälle	

Wie der Leiter der „Finanzkontrolle Schwarzarbeit“ (FKS) kürzlich mitteilte, ist die Flut der eingehenden Hinweise auf Schwarzarbeit in den letzten Monaten „drastisch“ angeschwollen. Er führt dies einerseits auf die abschreckende Wirkung der bisher durchgeführten Razzien, andererseits auch auf einen allmählichen Bewusstseinswandel der Bürger zurück. Für die 5.100 Mitarbeiter des Zolls, die derzeit im Kampf gegen die Schwarzarbeit eingesetzt sind, gelte die Vorgabe, pro Kopf durchschnittlich 165.000 € zu „erwirtschaften“. Deshalb gehe die FKS auch ähnlich zielorientiert wie die Steuerfahndung vor und konzentriere sich auf die großen Fälle. Im Durchschnitt seien die Fahnder bei fast jeder 4. Kontrolle auf einen Schwarzarbeiter gestoßen: so bei Großbaustellen in 14 % aller Fälle, im Taxi- und Mietwagengewerbe 15 %, im Reinigungsgewerbe 16 %, in Spielhallen 20 % und im Hotel- und Gaststättengewerbe sogar 25 %. Da sich die Fälle, bei denen Ausländer den Fahndern ins Netz gingen, schon bisher auf Ost- und Südosteuropa konzentriert hätten, seien nach der Osterweiterung der EU bisher noch keine auffälligen Veränderungen aufgetreten.

10.6 Produktpiraterie

10.6.1 Ausmaß und Schadensdimension

Produktpiraterie stellt für viele auf Markenprodukte spezialisierte Unternehmen eine erhebliche Belastung dar. Der volkswirtschaftliche Schaden wird weltweit nach Angaben der Zentralstelle für Marken- und Namensrecht der Robert Bosch GmbH auf 220 Mrd. € geschätzt. Allein für Deutschland wird ein volkswirtschaftlicher Schaden in Höhe von ca. 35 Mrd. € angenommen.

Die EU und die Internationale Handelskammer schätzen, dass rund 10 % des Welthandels plagiierte Produkte sind. Zehntausende Arbeitsplätze gehen Jahr für Jahr durch die Produktpiraterie verloren. Eine Studie von PriceWaterhouse Coopers kam schon 1998 zu dem Ergebnis, dass eine Verringerung allein der Softwarepiraterie um 10 % in Europa etwa 250.000 Arbeitsplätze schaffen würde. Die Business Software Association (BSA) gibt den jährlichen Schaden für Software-Unternehmen mit 13,1 Billionen $ an. Fast 20 % aller Unternehmen weltweit haben nach einer Umfrage von PriceWaterhouse Coopers in den Jahren 2001/2002 festgestellt, dass ihre Produkte gefälscht wurden.

10.6.2 Bevorzugte Produkte

Die EU hat ermittelt, dass Plagiate bei einzelnen Produkten folgende Prozentsätze erreichen:

- bei Schuhen und Bekleidung ca. 22 %
- bei Filmen ca. 16 %
- bei CDs ca. 10 %
- bei Kfz-Teilen 5–10 %

Nach dem Bundeslagebild Wirtschaftskriminalität 2003 bilden in Deutschland
- Sport- und Freizeitbekleidung mit insgesamt 40 % (Vorjahr: 59 %)
- Accessoires mit 20 % (Vorjahr: 9 %)
- Uhren und Schmuck mit 15 % (Vorjahr: 7 %)

Schwerpunkte.

10.6.3 Gefälschte Arzneimittel

Der Internationale Verband der Arzneimittelhersteller geht davon aus, dass 7 % aller auf der Welt gehandelten Medikamente Fälschungen sind. Tausende Menschen sterben an Medikamenten, die nicht enthalten, was auf dem Beipackzettel steht. Statt hoch dosierter Wirkstoffe mischen Panscher Back- und Milchpulver bei. Mit Wasser versetzte Impfstoffe kosteten 1995 etwa 2.500 Menschen in Niger das Leben. Mit Lösungsmitteln angereicherter Hustensaft brachte in Haiti 89 Kindern den Tod. Nach einer Meldung des Pharmakonzerns Novartis sind 2001 in China über 100.000 Menschen an gefälschten Arzneimitteln gestorben. 50 % der in China verkauften Arzneien sind gefälscht, so die Federation of Pharmaceutical Manufacturers in Genf.

Aber die international operierenden Banden sind auch in Indien, Russland, der Ukraine und anderen Staaten tätig. Nach Angaben der Weltgesundheitsorganisation (WHO) sind in einigen Ländern Südostasiens, Lateinamerikas und Westafrikas mehr als 70 % aller angeblichen Arzneimittel gefälscht. Bei 19 % der Plagiate ist viel zu wenig Wirkstoff enthalten. 60 % der sog. Medikamente sind überhaupt keine, sondern sog. Placebos, noch dazu verunreinigt. Laut Mitteilung der Association of International Pharmaceutical Manufacturers (AIPM) betrug der Schaden im Jahr 2003 rund 32 Mrd. $ weltweit. Inzwischen hat der Marktanteil für die Nachahmungen rund 10 % erreicht.

10.6.4 Stammland der Produktpiraterie: China

China ist, wie Financial Times Deutschland am 6. April berichtete, auch nach seinem Beitritt zur Welthandelsorganisation (WTO) im Jahr 2002 ein Paradies für Raubkopien und Markenpiraterie geblieben. Die Umsetzung vieler WTO-Regeln erweist sich als schwierig – auch der Schutz von Marken- und Patentrechten. Ein Markenprodukt wie die „Barbie“-Puppe des US-Spielwarenherstellers Mattel wird in China unter Namen wie „Babie“ oder „Berbie“ kopiert und vermarktet.

Auch die Automobilwirtschaft leidet unter den Fälschungen. So tauchten in China Fahrzeuge mit der Frontpartie der Mercedes C-Klasse auf, deren Heck allerdings anders gestaltet war. Auch die Friedrichshafener ZF AG, die in China Achsen, Lenkungen und Getriebe herstellt, will verstärkt gegen Produktpiraterie vorgehen. Chinesische Firmen bauen vermehrt Kupplungen, Hydraulikpumpen oder mechanische Lenkungsteile nach und verkaufen sie an Kfz-Werkstätten. Nach Berechnung des Automobil-Newsdienstes Marsh-Watch beträgt der Umsatz von VW Schanghai mit Autoteilen jährlich 140 Mio. €. Doch das sei nur ein Drittel des Marktes. Den Rest machen willkürlich kopierte Teile aus. Topmanager führender japanischer Hersteller in China werden mit der Einschätzung zitiert, der Marktanteil der Plagiate erreiche 80 %.

Chinas Regierung startete im Sommer 2003 eine groß angelegte Kampagne gegen das Markenpiraterie-Unwesen. Viel hat dies jedoch bisher nicht bewirkt, denn das Gewerbe ist organisiert. Die Banden haben China zu einem Drehkreuz im internationalen Geschäft mit kopierten Autoteilen gemacht. Rund 12 Mrd. $ verliert die Autoindustrie weltweit jährlich wegen illegaler Kopien, so hat die International Anti Counterfeiting Coalition berechnet. Dadurch gingen 200.000 Arbeitsplätze in der Autoindustrie verloren. Hatten die Fälscher früher nur technisch einfache Ware nachgebaut, so kopieren sie heute aufgrund wachsender Erfahrung und Größe der Lieferanten komplizierte Teile wie Ölpumpen, Getriebe und sogar ganze Motorblöcke. Nach Angaben der Japan Automobile Manufacturers Association waren 1999 von 11 Millionen in China verkauften Motorrädern 7 Millionen Kopien japanischer Originale. In 123 chinesischen Automobilfabriken werden Original-Autoteile nachgeahmt.

Immerhin 57 % aller deutschen Firmen fühlen sich von Produktfälschungen der Chinesen betroffen, ergab die jüngste Umfrage der Deutschen Handelskammer in China.

10.6.5 Prognose

Im Lagebericht Wirtschaftskriminalität 2002 hat das BKA ausgeführt:
Der größte Teil der beschlagnahmten Plagiate stammt aus Ländern außerhalb der EU. Mit der EU-Osterweiterung und dem damit verbundenen Wegfall der Grenzkontrollen ist aller Wahrscheinlichkeit nach ein erhöhtes Aufkommen von Fälschungen zu erwarten. Gleichzei-

tig wird es für Produktfälscher einfacher, an moderne Technologien zu gelangen und diese für ihre Zwecke zu verwenden. Damit können Fälschungen in einer Qualität produziert werden, die kaum noch von den Originalen zu unterscheiden sind. Dem sollte bereits im Vorfeld durch die Intensivierung der internationalen Zusammenarbeit entgegengewirkt werden.

Es gibt keine Anhaltspunkte dafür, dass sich die Erscheinungsformen der Produktpiraterie gravierend verändern werden. Die Schwerpunkte bleiben weiterhin die klassischen Bereiche wie Fälschung von Textilien, Uhren/Schmuck und Datenträgern im Allgemeinen.

Einem hohen Dunkelfeld steht häufig eine geringe kriminalpolizeiliche Bekämpfungsintensität gegenüber, obwohl hohe volkswirtschaftliche Schäden evident sind.
In Zeiten wirtschaftlich rezessiver Entwicklungen ist davon auszugehen, dass Steigerungsraten in diesem Deliktsbereich wahrscheinlich sind.

10.6.6 Schutzmöglichkeiten

Die deutsche Wirtschaft ist den Produktpiraten nicht wehrlos ausgeliefert. Die Palette möglicher Schutzmaßnahmen reicht von rechtlichen Schritten bis hin zu sicherheitstechnischen Abwehrmöglichkeiten. Die sind insbesondere gegeben, wenn das gefährdete Produkt verpackt in den Handel kommt. Um Patienten und Pharmafirmen vor Fälschungen zu schützen, haben Spezialfirmen unterschiedliche Methoden entwickelt, mit denen Medikamentenpackungen eindeutig gekennzeichnet werden können.

So bietet 3M Security Market Center Labels an, die ja nach Blickwinkel die Farbe wechseln und sehr schwer zu fälschen sind. Das Unternehmen hat ein Baukastensystem entwickelt, mit dem verschiedene Sicherheitsmerkmale kombiniert werden können. Zu den Modulen gehören Kennzeichen, die nur unter UV-Licht erkennbar sind, Barcodes und Seriennummern, die mit spezieller Prägetechnik aufgebracht werden, reflektierende Folien und 2 D-Hologramme, in die ein individualisierbarer Mikrotext eingegeben werden kann.
Eine ähnliche Technik hat die Heidelberger Tesa Scribos GmbH im Programm. Dabei handelt es sich um ein winziges Pünktchen Tesafilm, mit dem Verpackungen eindeutig gekennzeichnet werden. Ein Laser schreibt in den sog. Holospot die Produktkenndaten, die via Computer in ein Hologramm umgewandet werden. Die Produktinformation wird also nicht auf das Etikett aufgebracht, sondern in das Etikett eingebracht. Selbst wenn das Etikett entfernt wird, hinterlässt das Spuren, die erkennbar werden lassen, dass an dieser Stelle etwas entfernt wurde.

MediaSec Technologies hat sog. Kopie-Erkennungsmuster entwickelt, die auf die Verpackungen aufgedruckt werden. Dabei handelt es sich um individuell für jeden Kunden erzeugte Muster, die aus einer dichten Ansammlung von Punkten verschiedener Helligkeit bestehen und in die verborgene Informationen eingebracht werden können. Jede Bearbeitung der Verpackung, jeder Kopiervorgang oder eine Bildverarbeitung hinterlässt Spuren auf dem Muster und kann später erkannt werden. Die Zukunft des Markenschutzes liegt in der Produktindividualisierung durch sichtbare und unsichtbare Elemente, so dass das Unternehmen auf Bedrohungen durch Markenpiraten flexibel reagieren kann.

Um in der Kfz-Industrie im Streitfall nach Verkehrsunfällen die Herkunft und sachgerechte Montage der konzerneigenen Bauteile bzw. ein Plagiat nachweisen zu können, wurde im ZF-Achswerk in Shenyang (Südmandschurei) ein aufwändiges Datensicherungsverfahren eingeführt. Alle Werkzeuge sind mit Kleincomputern verbunden, die jede Schraubenumdrehung registrieren und speichern. Jeder Arbeiter hat eine eigene Codenummer, die zugeordnet wird.

An rechtlichen Möglichkeiten sei auf die gewerblichen Schutzrechte (Patent, Gebrauchsmuster, Geschmacksmuster, Marken, Halbleiter- bzw. Topographienschutz) und auf die Möglichkeit der Beantragung eines Grenzbeschlagnahmeverfahrens hingewiesen.
Bei der Registrierung einer Marke in einem anderen Land ist darauf zu achten, die Marke auch in der Landessprache registrieren zu lassen, wenn die Registrierung nicht ins Leere laufen soll. Das gilt insbesondere für das Verfahren in der Volksrepublik China.

10.6.7 Bekämpfung der Produktpiraterie durch den Staat

Wirtschaftsverwaltung, Polizei und Zoll bekämpfen Produktpiraterie auf vielfältige Weise.
Im Rahmen der Öffentlichkeitsarbeit muss das Unrechtsbewusstsein der Verbraucher stärker entwickelt werden.
Um effektiv gegen Plagiatoren und Piraterie vorgehen zu können, benötigt die Polizei u.a. fundierte Informationen aus den Unternehmen. Häufig versprechen sich die Unternehmen von einer strafrechtlichen Verfolgung wenig und versuchen lediglich, entstandene Schadenersatzansprüche geltend zu machen.
Ein effektives Mittel zur Bekämpfung der Produktpiraterie stellt die Einziehung der Produkte und Tatmittel dar, auch wenn diese das Problem nicht an der Wurzel greift. Der Zoll hat 2003 in 3.461 Fällen Beschlagnahmungen durchgeführt und dabei einen Schaden von 178 Mio € ermittelt.

10.6.8 Rechtsprechung

Zur Problematik der Produktpiraterie gibt es eine Reihe aktueller höchstrichterlicher Entscheidungen. Der BGH hat mit Urteil v. 15.05.03 entschieden, dass die wettbewerbsrechtliche Haftung für den Vertrieb der Waren bereits mit der Auslieferung an den Zwischenhändler beginnt. Ansprüche des Unternehmens, dessen Produkte unerlaubt nachgeahmt werden, entstehen schon zu diesem Zeitpunkt, nicht erst, wenn die Ware zum Endabnehmer gelangt oder im Bestellkatalog zu finden ist.

Der EuGH zwingt zu einer schärferen Gangart gegen den Transithandel mit gefälschten Markenartikeln. Selbst wenn der Transit nach nationalem Recht nicht strafbar sei, müssen die Mitgliedstaaten aufgrund des EU-Rechts gegen den Transit „abschreckende Strafen“ verhängen (so eine Entscheidung v. 08.01.04).

In einem restriktiven Urteil hat der EuGH am 23.10.03 entschieden, dass der Markenschutz nicht berührt ist, wenn die Verbraucher eine Kennzeichnung von Bekleidung (vertikale Streifen auf der Trainingsjackennaht) nur als Verzierung auffassen.

10.7 Korruption

Die ermittelte Korruptionskriminalität hat in den letzten Jahren abgenommen:

	2001	2003	Veränderung
Vorteilsannahme	1.107	899	./. 19 %
Bestechlichkeit	745	278	./. 63 %
Vorteilsgewährung	413	333	./. 46 %

insgesamt	3.188	2.006	./. 37 %

Bei einer Bewertung dieser Zahlen ist zu berücksichtigen, dass es sich um ein typisches Kontrolldelikt handelt, so dass das Dunkelfeld der nicht ermittelten Bestechungsfälle unbestimmt groß ist.
Grund für den Rückgang der ermittelten Korruptionsfälle dürfte vor allem die Verschärfung der Rechtslage in den letzten Jahren sein. Seit 1999 sind Schmiergelder nicht mehr als Betriebsausgaben abzugsfähig. Die Bestechung ausländischer Amtsträger, Richter und Abgeordneter wurde unter Strafe gestellt. Und 2002 kam dann noch die Bestechung von Privatleuten, also Firmenangehörigen, hinzu.

Die Bundesregierung hat in diesem Jahr die Richtlinie zur Korruptionsprävention in der Bundesverwaltung von 1998 neu gefasst. Zu den wesentlichen Neuerungen gehören:
- Verschärfung der Regelung zur Rotation von Personal (in der Regel maximal 5 Jahre auf demselben Arbeitsplatz in einem Risikobereich, schriftliche Begründung von Ausnahmen, Ausgleichsmaßnahmen)
- Festschreibung der Weisungsunabhängigkeit der Ansprechperson für Korruptionsprävention und ihres direkten Vortragsrechts gegenüber der Hausleitung
- Konkretisierung der Regelung zur Sensibilisierung und Belehrung der Bediensteten
- weitere Verstärkung der Aus- und Fortbildung und
- Stärkere Betonung der Verantwortung der Führungskräfte.

Zugleich wurde vom BMI eine Empfehlung zur Umsetzung der Richtlinie vorgelegt, die sich mit der Feststellung und Analyse besonders korruptionsgefährdeter Arbeitsgebiete, mit der Prognose zur Korruptionsgefährdung neuen Personals und Leitsätzen für die Vergabe öffentlicher Aufträge befasst. Hinzu kommt ein Leitfaden für Vorgesetzte und Behördenleitungen und ein Verhaltskodex gegen Korruption. Die Dokumente finden sich auf der Website des BMI (www.bmi.bund.de).

10.8 Wettbewerbskriminalität

Unter Wettbewerbsdelikten werden alle Deliktsformen in Zusammenhang mit Verstößen gegen das Gesetz gegen den unlauteren Wettbewerb, das Markengesetz sowie gegen das Wettbewerbsrecht nach dem StGB verstanden. Neben sämtlichen Arten der Lizenzpiraterie gehören zu diesem Kriminalitätsbereich z.B. Scheinausverkäufe, Schleudergeschäfte, Sammlungen für angeblich wohltätige Zwecke sowie Rabattbetrügereien, Formen der progressiven Kundenwerbung im sog. Schneeballsystem, Ausschreibungs- und Subventionsbetrug und nicht zuletzt alle Fälle der Wirtschafts- und Konkurrenzspionage.

Die Häufigkeit der strafbaren Verstöße gegen das UWG – ohne Spionagedelikte gem. § 17 – schwankt stark. So wurden
- im Jahr 1999 11.657
- im Jahr 2002 2.385 und
- im Jahr 2003 741 Fälle festgestellt.

Progressive Kundenwerbung war im Jahr 2002 vorrangig von Fällen der
- Vermittlung von Nebenverdiensten und
- Übergabe von Gewinnen

geprägt.

Ausschreibungsbetrug führt zu einer erheblichen Schädigung des Wettbewerbs. Häufig wird Korruption in Zusammenhang mit dem Ausschreibungsbetrug festgestellt.

Der Deliktsbereich des Subventionsbetrugs ist ein äußerst schadensintensiver Bereich. Die 535 im Jahr 2002 ermittelten Fälle verursachten einen Schaden von ca. 175 Mio €. Die geringe Zahl ermittelter Fälle (625 im Jahr 2003) steht ein vermutlich breites Dunkelfeld gegenüber.

10.9 Konkurrenzspionage

Konkurrenzspionage droht den Unternehmen nicht nur durch Außentäter, sondern zunehmend durch unzufriedene Beschäftigte, die „Know-how"-Träger sind und sich selbständig machen oder zu einem Konkurrenzunternehmen wechseln möchten. Da dem Wechsel zumeist ein längerer „Loslösungsprozess" vorausgeht, sollten die Unternehmen auf entsprechende Warnzeichen achten, möglichst frühzeitig das Risiko identifizieren und reagieren. Selbst wenn das Ausscheiden feststeht und etwa eine Abfindungsvereinbarung getroffen worden ist, kann das Arbeitsverhältnis mit der Abfindungsvereinbarung aufgrund eines Geheimnisverrats noch fristlos gekündigt werden. Dass der vorsätzliche Verrat von Firmen-Interna an ein Konkurrenzunternehmen eine fristlose Kündigung rechtfertigt, hat das Berliner Landesarbeitsgericht in einer Entscheidung im April 2004 noch einmal bestätigt. Nach der PKS sind 2003 insgesamt 275 Fälle des Verrats von Betriebs- und Geschäftsgeheimnissen nach § 17 UWG bekannt geworden (2002: 269). Viel mehr Fälle dürften unerkannt geblieben sein. Die Zahl der Verdachtsfälle des Verrats solcher Geheimnisse durch eigene Beschäftigte ist gegenüber dem Vorjahr erneut angestiegen: auf 152.

10.10 Insolvenzkriminalität

Die Insolvenzkriminalität als Teil der Wirtschaftskriminalität hat auch 2003 wieder zugenommen (um 8,5 % auf fast 14.000 Fälle). Ursache dieser Steigerung ist die gegenwärtige Insolvenzwelle, die auch 2004 nicht abebbt. Von 19.300 Insolvenzen im ersten Halbjahr 2004 waren 322.000 Arbeitnehmer und rund 20.000 Ausbildungsplätze betroffen. Im gesamten Jahr werden etwa 40.000 Insolvenzen erwartet. Durch Insolvenzstraftaten wurde 2003 ein materieller Schaden von ca. 3,21 Mrd. Euro verursacht. Gegenüber 2002 bedeutet dies einen Anstieg von 32,6 %. Der Anteil des Insolvenzkriminalitätschadens am Gesamtkriminalitätsschaden beträgt fast 27 %.

Im Einzelnen wurden 2003	ermittelt	als Schaden festgestellt:
Bankrott	4.200 Fälle	926,0 Mio €
Insolvenzverschleppung nach HGB	225 Fälle	104,6 Mio €
Leistungskreditbetrug	2.000 Fälle	32,7 Mio €
Besonders schwerer Fall des Bankrotts	19 Fälle	6,4 Mio €
Insolvenzverschleppung nach GmbHG	7.500 Fälle	2,2 Mio €
Schuldnerbegünstigung	49 Fälle	1,3 Mio €

Auf die zunehmenden Bilanzskandale der vergangenen Jahre in zahlreichen Unternehmen der EU-Staaten reagiert die EU-Kommission mit einer Reform der EU-Richtlinien über Wirtschaftsprüfer. Sie enthält Mindestvorschriften für eine öffentliche Aufsicht der Prüfer. Unabhängige Überwachungsgremien sollen die Einhaltung der geplanten EU-Standards für die Durchführung der Abschlussprüfung, Qualitätssicherung und Unabhängigkeit der Prüfer von ihren Mandanten überprüfen. Beratungstätigkeiten der Prüfer für ihre Mandanten sollen verboten werden. Hinzu kommt eine Rotationspflicht: Entweder muss sich die Prüfgesellschaft nach mehreren Jahren der Prüftätigkeit von ihrem Mandanten trennen oder das Prüfpersonal rotieren lassen.

Zur Insolvenzkriminalität wird im Jahresbericht Wirtschaftskriminalität 2002 des BKA folgender Modus operandi betrügerischer Firmenaufkäufer dargelegt:

Durch Inserate in verschiedenen Printmedien bieten die Täter Unternehmenskonzept, Existenzsicherung und kostenloser Rechtsberatung geködert werden. Werden die angebotenen „Dienste“ von dem insolvenzbedrohten Unternehmen in Anspruch genommen, führen die Täter mehrfache Geschäftsführer-, Gesellschafter- und Firmensitzwechsel durch, damit kein Verantwortlicher mehr auszumachen ist. Die Geschäftsunterlagen sind später unauffindbar. Die tatsächliche „Dienstleistung“ der Täter beschränkt sich darauf, der Firma zum Nachteil der Gläubiger die Vermögenswerte zu entziehen und zu vereinnahmen. Darüber hinaus werden die übernommenen Firmenmäntel häufig missbräuchlich zur Begehung von Warenkreditbetrügereien (Stoßbetrug) genutzt. Nach Feststellungen des BKA im Bundeslagebild Wirtschaftskriminalität 2003 ist bei sog. „Firmenbestattungen“ immer häufiger das Phänomen des Verkaufs der insolventen Firmen mit einer Sitzverlegung ins Ausland zu beobachten. Die Probleme können sich verschärfen, wenn es im Rahmen der EU möglich sein wird, internationale bzw. Europagesellschaften zu gründen.

11 IuK-Kriminalität

11.1 Verbreitungsgrad der Internetnutzung in der Wirtschaft

71 % der Unternehmen befragter Wirtschaftszweige setzten – wie das BKA im Bundeslagebild IuK-Kriminalität für das Jahr 2002 berichtet – in diesem Jahr Computer im Geschäftsablauf ein. Fast alle großen Unternehmen mit 250 und mehr Beschäftigten verfügten auch über einen Zugang zum Internet und waren mit E-Mail erreichbar. Bei den kleinen Unternehmen mit weniger als 20 Beschäftigten waren es knapp 60 %.

Bei den kleinen Unternehmen war einer der Hauptgründe für einen Internetzugang die Möglichkeit zum Online-Banking: Mehr als 2/3 der kleinen Unternehmen mit Internetzugang wickelten ihre Bank- und Finanzgeschäfte über das Internet ab. Bei den größeren Unternehmen ist dieser Anteil ähnlich hoch. Sie verwendeten das Internet allerdings primär zur Informationsbeschaffung und Marktbeobachtung. Ein Intranet findet sich hauptsächlich in großen Unternehmen. 84 % der Unternehmen mit mehr als 250 Beschäftigten verfügen über ein Intranet.

11.2 Computerkriminalität (entsprechend der PKS)

Je unentbehrlicher die Computertechnologie für das Wirtschaftsleben wird, umso anfälliger ist sie für kriminelle Angriffe und sonstige Störungen ihrer Verfügbarkeit. Aus der PKS lässt sich die Entwicklung dieser Störanfälligkeit nur bedingt ablesen. Zudem ist durch die Ausklammerung des Betrugs mittels rechtswidrig erlangter Debitkarten ohne PIN seit 2002 ein Bruch in der Zeitreise entstanden. Ohne diese Ausklammerung wäre die Zahl der in der PKS erfassten Fälle von Computerkriminalität seit Beginn der statistischen Erfassung ungebrochen angestiegen.

Computerkriminalität	1990: 5.004
	1995: 27.902
	2000: 56.684
	2001: 79.283

2002: 57.488
2003: 59.691

	2003	1998
Betrug mittels Debitkarten mit PIN	35.954	35.909
Computerbetrug	11.388	6.465
Betrug mit Zugangsberechtigung zu Kommunikationsdiensten	7.003	2.109
Fälschung beweiserheblicher Daten	6.068	349
Softwarepiraterie	2.053	362
Datenveränderung, Computersabotage	1.705	326
Ausspähen von Daten	781	267
Gewerbsmäßige Softwarepiraterie	570	289

Der durch Computerkriminalität verursachte Schaden belief sich – soweit er erfasst werden konnte – schon 2002 rund 85 Mio. €.

11.3 Bundeslagebild IuK-Kriminalität 2002

In seinem Lagebericht für 2002 weist das BKA darauf hin, dass auf den „Betrug mittels rechtswidrig erlangter Debitkarten mit PIN“ ca. 64 % der Gesamtzahl entfallen. Die IuK-Kriminalität umfasst neben der eigentlichen Computerkriminalität insbesondere Betrugsdelikte im Zusammenhang mit Onlineauktionshäusern, Propaganda- und Beleidigungsdelikte sowie Urheberrechtsverletzungen. Das Dunkelfeld ist erheblich. Die AQ lag 2002 wegen der Schwierigkeit insbesondere der Aufklärung von Hacking-Fällen insges. nur bei 50 %.

11.4 Missbrauch von TK-Anlagen

2002 wurden im Rahmen des IuK-Meldedienstes 50 Fälle registriert. Meist nutzen die Täter bereits eingerichtete Anwendungen und manipulieren diese für ihre Zwecke. Häufig wird in das Voice Mail-System eingedrungen und die Voice-Mail-Box einer Nebenstelle für die kriminellen Zwecke neu konfiguriert. Häufig sind die Standardeinstellungen der PIN von der Firma nicht verändert worden.

Aufgrund der zahlreichen Verschleierungsmöglichkeiten wird nicht mit einem Rückgang der Fallzahlen gerechnet. In diesem Deliktsbereich stehen einem geringen Entdeckungsrisiko relativ große Gewinnmöglichkeiten gegenüber. Viele Angriffe könnten schon durch das Verändern von Standardpasswörtern, die Sperrung von ungenutzten Anwendungen oder die Deaktivierung des Fernwartungsmodems bei Nichtgebrauch verhindert werden.

Aus der Verknüpfung des TK-Bereichs mit dem IT-Bereich ergibt sich grundsätzlich die Möglichkeit, über die Telefonanlage in das Computernetzwerk der angegriffenen Firma einzudringen. Innerhalb eines Computernetzwerkes stellt die TK-Anlage in der Regel das schwächste Glied dar. Nach Überzeugung des BKA wird es in Zukunft vermehrt Angriffe auf TK-Anlagen geben, um auf diesem Weg in die Netzstruktur einzudringen.

11.5 Viren und Würmer

Die wohl größte Bedrohung für die IT-Systeme in der Wirtschaft geht von Viren und Würmern aus. Auch 2003 haben Computerviren und andere Schädlinge im Internet weltweit Schäden in enormer Höhe verursacht. Der Email-Dienstleister Clearswift beziffert die entstandenen Kosten auf insgesamt 20 Mrd. $. Trend Micro spricht gar von 55 Mrd. $, die Angriffe durch Viren die Unternehmen weltweit gekostet haben. Dabei handelt es sich neben den Direktschäden um Gewinnausfälle durch Kommunikationsbehinderung. In einer Studie des britischen Instituts Datamonitor gaben Unternehmen eine Spanne von 7.000 bis 95.000 € zur jährlichen Behebung von Sicherheitslücken durch Virenbefall an. Der durchschnittliche Schaden betrug in den letzten Jahren bei großen Unternehmen 37.000 €. Aber mittelständische Unternehmen sind nach einer Umfrage von Network Associates besonders gefährdet. 42 % waren 2003 in Europa von Virenangriffen betroffen. Die deutschen Mittelständler kamen dabei mit 21 % noch glimpflich davon. Aber das Gefühl der Bedrohung wächst. Dabei setzen 11 % der Befragten überhaupt keine Antiviren-Software ein.

Viren werden immer aggressiver. Sie spähen Passwörter aus oder suchen gezielt nach Kreditkartennummern. Auch im IuK-Bericht des BKA wird darauf hingewiesen, dass Würmer der neueren Generation neben der reinen Verbreitungsroutine oftmals zusätzlich „Trojanerfunktionen“ beinhalten. So werden gezielt sensible Daten wie Passwörter, Kennungen für das Online-Banking oder für andere Webangebote wie z.B. für Online-Auktionen ausgespäht.

Aus der Vielzahl der Viren und Würmer ragen auch 2003 und 2004 einige mit einem besonders hohen Schadenspotenzial heraus. So hatte sich z.B. der Internetwurm Mydoom schon eine Woche nach seinem ersten Auftauchen zur bislang größten Wurmattacke entwickelt und 20-30 % des weltweiten Email-Verkehrs infiziert. Er suchte auf infizierten Rechnern nach Email-Adressen und sandte sich automatisch weiter, ohne dass der Anwender etwas davon bemerkte. Schon nach kurzer Zeit wurde der von Mydoom angerichtete Schaden auf 38,5 Mrd. € geschätzt. Er überragt damit den bisherigen Spitzenreiter Sobig. Die neueste Variante dieses Virus hat im Juli dieses Jahres auch die Internet-Suchmaschinen Google, Yahoo, Lycos und Altavista zeitweise lahmgelegt.

Schaden durch Computerviren	in Mrd. Dollar
Sobig	34,0
Klez	16,4
Love Bug	9,6
Yaha	8,1
BugBear	3,0
Code Red	2,9
SirCam	2,5
Mafia Boy	1,3
Melissa	1,2
Slammer	1,2

Stundenlange Verspätungen bei British Airways, eine lahm gelegte Küstenwache und Handbetrieb an den Postschaltern: Das waren die Folgen des Computerwurms Sasser, der im Mai 2004 vermutlich mehr als eine Million Computer in aller Welt befallen hat. Er verbreitet sich nicht wie andere Würmer als Anhang einer Email, sondern automatisch bei einer bestehenden Internet-Verbindung. Unternehmen mit elektronischen Firewalls mussten eigentlich keine Angst vor Sasser haben. Wenn jedoch Mitarbeiter infizierte Notebooks an das Firmennetz anschlossen, war der Schutz der Firewall nicht mehr gegeben.

Im Juni 2004 ist der erste Handy-Wurm aufgetaucht. Er funktioniert allerdings nur auf Mobiltelefonen mit eingeschalteter Bluetooth-Funktion und wird nur auf den multimediafähigen Smartphones aktiv. Gleichwohl gibt es nach Ansicht der Virenexperten keinen Grund zur Entwarnung. Der Schaden, den solche Angriffe auf Mobiltelefonen anrichten könnten, ist immens, Er reicht von dem automatischen Senden von Kurzmitteilungen an teure Premiumnummern bis zum Löschen von Daten oder dem permanenten Einschalten des Displays mit der Folge einer schnellen Entladung der Batterie.

DIE WELT berichtete am 13. Juli 2004, dass inzwischen 83 % der größten Banken und Finanzdienstleister weltweit Attacken auf ihr Computer-System abwehren müssen. Dies ergibt sich aus einer „Sicherheitsstudie 2004“ der Prüfungs- und Beratungsgesellschaft Deloitte, die auf einer Befragung der 100 größten Finanzdienstleister beruht. Viren und Würmer sind nach dieser Studie die größte Bedrohung der sensiblen Finanzsysteme. Dennoch sank der Anteil derjenigen Unternehmen, die für einen vollständigen Schutz durch Antivirensysteme sorgen, von 96 % im Vorjahr auf 87 %. Auch die Studie „IT-Budget“ des Fachmagazins „Informationweek“ kam kürzlich zu einem alarmierenden Ergebnis. Danach wiegt sich jede dritte Firma in Deutschland in Sicherheit, obwohl sie die Wirksamkeit ihrer Abwehrsysteme nicht kontrolliert. Jedes vierte Unternehmen hält nach dieser Studie seine Sicherheitssoftware nicht regelmäßig auf dem neuesten Stand.

Im Schnitt investieren- so das Beratungsunternehmen Mummert Consulting – deutsche Firmen nur 12 % ihrer IT-Budgets in Sicherheit.

11.6 Schutz vor Virenattacken und Hackerangriffen

Der IT-Branchenverband und die Bundesregierung erwägen den Aufbau eines Internet-Frühwarnsystems – ähnlich den Unwetterwarnungen des Wetterdienstes. Als Ergänzung zu bestehenden Computer-Notfallteams, den sog. CERTs (Computer Emergency Response Teams) in Behörden und Unternehmen, soll dieses Frühwarnsystem heraufziehende Viren- und Hackerangriffe erkennen, neue Bedrohungen erahnen und die Fachleute in den CERTs vorwarnen.

Um einen vernünftigen Schutz vor Angreifern zu bieten, ist es nötig, die verschiedenen Sicherheitsmechanismen – insbes. Firewalls und Intrusion Detection-Systeme – weitgehend zu zentralisieren. Mit dem Trend zur integrierten Daten- und Prozessverarbeitung sind partielle Sicherheitstechniken immer weniger gefragt. Ein zentraler Sicherheitsschirm sollte den kompletten Aktionsradius eines Unternehmens abdecken: Intranet, Extranet und Internet. Ein umfassender Schutzschirm auf der Basis aktueller Teilnehmeridentitäten versetzt das Unternehmen in die Lage, sein aktuelles Sicherheitskonzept schneller, flexibler und lückenloser als bisher in Technik umzusetzen.

Noch immer wird von der elektronischen Signatur zu wenig Gebrauch gemacht. Um die für einen sicheren elektronischen Rechts- und Geschäftsverkehr erforderliche Zahl an Anwendungen und Nutzern zu schaffen, will die Bundesregierung das Signaturgesetz ändern. Die Novelle der Bundesregierung zum Gesetz über Rahmenbedingungen für elektronische Signaturen (Drucks.15/3417) soll Rechtsprobleme lösen, die bei der Anwendung des Gesetzes aufgetreten sind. Und sie soll die Voraussetzungen dafür schaffen, dass Signaturkarten mit qualifizierten elektronischen Signaturen elektronisch beantragt und ausgegeben werden können. Damit könnten die bereits eingeführten Verfahren, etwa bei der Registrierung und Ausgabe von EC- oder Versichertenkarten auch für die Ausgabe von Signaturkarten mit qualifizierten elektronischen Zertifikaten genutzt werden.

11.7 Phishing

Eine neue Form betrügerischer Massen-Emails hat sich über das Internet sprunghaft verbreitet: sog. Phishing-Mails, von denen es nach einer Untersuchung von „Bright-mail“ im August 2003 weltweit schon 300 Millionen und im April 2004 bereits über 3 Mrd. gab. Sie tarnen sich meist als seriöse Nachricht eines Kreditinstituts und fordern den Empfänger auf, z.B. seine persönlichen Daten, Passwörter oder PIN-Codes zuaktualisieren. Mit diesen Daten können die Betrüger dann ungehindert Konten plündern. Betroffen sind vor allem Banken oder Online-Dienste, Bezahlsysteme und Fluggesellschaften.

Etwa 2/3 der Phishing-Mails stammen aus Osteuropa und Asien und bedrohten bislang eher den englischsprachigen Raum, mehr und mehr aber auch Kontinentaleuropa.
Angesichts dieser Bedrohung werden Behörden weltweit aktiv. Wirksamen Schutz bieten Antiphishing-Programme von Microsoft, Yahoo und Ebay. Polizeiliche Ermittlungen werden durch eine Antiphishing-Arbeitsgruppe mit der Erstellung schwarzer Listen unterstützt.

11.8 Spam-Flut

Unerwünschte Werbe-Emails werden für private Internetnutzer wie für Unternehmen zu einem wachsenden Problem Das britische Sicherheitsunternehmen Brightmail schätzt den Anteil solcher Mails inzwischen auf 60-70 %. Die Schäden, die Spam verursachen, schätzt die EU-Kommission für 2004 auf rund 8 Mrd. €, je Mitarbeiter ca. 300 €, nach einer Umfrage des britischen Unternehmens Sybari. Sie entstehen sowohl durch steigende Verwaltungskosten wie durch sinkende Produktivität der Beschäftigten. Obwohl viele Unternehmen inzwischen Filtertechniken oder schwarze Listen als Schutzmechanismen einsetzen, gelangen noch viele unerwünschte Emails in die Postfächer der Mitarbeiter. Nach einer Umfrage der Sicherheitsspezialisten von Clearswift zeigen die Unternehmen bisher wenig Engagement, die Spam-Flut einzudämmen. Nur 14 % gaben an, sich an Antispam-Initiativen zu beteiligen, obwohl 55 % glauben, dass ihre eigene Spam-Abwehr nicht ausreicht. Insbesondere wird die eingesetzte Software zu selten aktualisiert.

Der Gesetzgeber wird die Spam-Flut kaum aufhalten können. Die EU hat zwar eine entsprechende Richtlinie zum Schutz vor Spam erlassen. Ihre Wirksamkeit wird aber als eher gering eingestuft. Anders in den USA: Dort drohen Tätern bei Verstößen gegen das Antispam-Gesetz sogar Haftstrafen.

11.9 Raubkopien / Softwarepiraterie

Einen Schwerpunkt der Produktpiraterie bildet das illegale Kopieren von Filmen und Brennen von CDs.

11.9.1 Krise der Unterhaltungsindustrie

Das illegale Kopieren von Filmen hat in den vergangenen Jahren massiv zugenommen. Allein in den ersten 8 Monaten des Jahres 2003 wurden in Deutschland von über 5 Millionen Bürgern ca. 30 Millionen Mal illegal Filme auf CD oder DVD kopiert. Das ergab eine im

Herbst 2003 vorgestellte zweite „Brenner-Studie“ der Filmförderungsanstalt. Für 2003 rechnen die Unternehmen mit einem Schaden weit über 1 Mrd. €, nach 800 Mio. € 2002. Möglich wird dies durch die flächendeckende Verbreitung von CD- und DVD-Brennern sowie Tauschbörsen im Internet. Mehr als 20 Millionen Deutschen steht ein CD-Brenner zur Verfügung. Illegales Kopieren und Brennen von Filmen ist zu einem Massenphänomen geworden. Das Unrechtsbewusstsein ist verloren gegangen. Laut einer Infratest-Umfrage halten nur noch 47 % der Bundessbürger das kostenlose Herunterladen für Diebstahl. 60 % der Deutschen sind bereit, eine Software-Raubkopie auf ihrem PC zu installieren.

11.9.2 Softwarepiraterie

Der Branchenverband „Business Software Alliance“ (BSA) beziffert die Raubkopierrate bei Standardsoftware in Deutschland für 2001 mit 34 %. Der Softwareindustrie entstand dabei ein Schaden in Höhe von 762 Mio. €. Weltweit berechnet BSA den Schaden auf 13 Mrd. $. Der Umsatzausfall setzt sich bei den Zulieferern der Softwareindustrie ebenso wie im Fachhandel und bei den Serviceanbietern fort.

Die Schadensdimension lässt sich an einem praktischen Fall konkretisieren. Am 10. November 2003 wurden bei einer Razzia in mehreren Bundesländern 30 Gebäude durchsucht und 6 Personen verhaftet. Die Beschuldigten stehen nach Angaben des BKA in Verdacht, seit mehreren Jahren gewerbsmäßig gefälschte oder verfälschte Computersoftware betrügerisch in den Handel gebracht zu haben. Der mit den Raubkopien von Softwarepaketen verschiedener Hersteller entstandene Schaden lag nach ersten Berechnungen bei 16 Mio. €.

11.9.3 Kaum Schutzmöglichkeiten

Die Schutzmöglichkeiten gegen das illegale Kopieren sind gering. Softwarepakete wie „Windows“ oder „Outlook“ können auf fast jedem Rechner leicht kopiert werden. Der eingebaute Kopierschutz wird von den Softwarepiraten unterlaufen.

Auffällig ist, dass beim gewerbsmäßigen Handel mit raubkopierter Software das Internet eine bedeutsame Rolle spielt. Zur Erhöhung des Verfolgungsdruckes durch die Polizei und zur Aufhellung des Dunkelfeldes können – so der Jahresbericht Wirtschaftskriminalität 2002 des BKA – verdachtsunabhängige Recherchen im Internet ein geeignetes Mittel sein. Als sinnvollste Präventionsmöglichkeit wird die Einführung eines wirksamen Kopierschutzes angesehen. Hier sind die Entwicklungsfirmen und die Industrie gefragt.

Inzwischen ist das Urheberrechtsgesetz geändert worden. Eine unerlaubte gewerbliche Verwertung von Raubkopien kann mit bis zu 5 Jahren Gefängnis geahndet werden. Auch das Herunterladen von Kinofilmen über das Internet ist nunmehr illegal. Zu Recht unzufrieden mit der Änderung des Gesetzes sind Produzenten, Verleger und Verwerter urheberrechtlicher Werke allerdings mit der Regelung, dass Privatkopien weiterhin auch von illegalen Quellen zulässig sind, solange die Rechtswidrigkeit nicht offensichtlich ist. Diese Voraussetzung ist schwer festzustellen.

Um das nach wie vor kaum vorhandene Unrechtsbewusstsein zu wahren, hängt die Filmindustrie inzwischen in Videotheken und Kinos Poster auf, die an RAF-Fahndungsplakate erinnern. „Raubkopierer sind Verbrecher“ lautet das Motto der bundesweiten Kampagne zum Urheberrechtsschutz.

12 Umweltkriminalität

Die Zahl der in der PKS registrierten Umweltdelikte nach dem StGB ist bis zum 1998 aufgrund zunehmender Kontrolltätigkeit ständig gestiegen (bis auf 41.381), seither aber rückläufig (insgesamt um 68 % bis 24.573 im Jahr 2003). Zählt man allerdings die Straftaten gegen Nebengesetze auf dem Umweltsektor hinzu, dann sind 2003 insgesamt 31.879 Verdachtsfälle erfasst worden. Der Schwerpunkt lag wie in den Vorjahren auf unerlaubtem Umgang mit gefährlichen Abfällen (ca. 17.000 Fälle = 69 % aller Umweltstraftaten nach dem StGB).