Schriftenreihe
Forschungsforum Öffentliche Sicherheit

Cyberkriminalität Computerstrafrecht und die digitale Schattenwirtschaft

D. Brodowski, Felix C. Freiling

Forschungsforum Öffentliche Sicherheit

Freie Universität Berlin

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Freie Universität Berlin

Forschungsforum Öffentliche Sicherheit

Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft

Dominik Brodowski, Felix C. Freiling

Forschungsforum Öffentliche Sicherheit
Schriftenreihe Sicherheit Nr. 4
März 2011
ISBN: 978-3-929619-66-9

Anschrift:	Tel: +49 (0)30 838 57367
Freie Universität Berlin	Fax: +49 (0)30 838 57399
Fabeckstr. 15	www.schriftenreihe-sicherheit.de
14195 Berlin	kontakt@schriftenreihe-sicherheit.de

Über die Autoren

Prof. Dr. Felix Freiling ist seit Dezember 2010 Inhaber des Lehrstuhls für IT-Sicherheitsinfrastrukturen an der Friedrich-Alexander-Universität Erlangen-Nürnberg. Zuvor war er bereits als Professor für Informatik an der RWTH Aachen (2003-2005) und der Universität Mannheim (2005-2010) tätig. Schwerpunkte seiner Arbeitsgruppe in Forschung und Lehre sind offensive Methoden der IT-Sicherheit, technische Aspekte der Cyberkriminalität sowie digitale Forensik (IT-Beweismittelsicherung). In den Verfahren zur Online-Durchsuchung und zur Vorratsdatenspeicherung vor dem Bundesverfassungsgericht diente Felix Freiling als sachverständige Auskunftsperson.

Dominik Brodowski ist Wissenschaftlicher Angestellter am Lehrstuhl für Europäisches Straf- und Strafprozessrecht, Professor Dr. Joachim Vogel, an der Eberhard Karls Universität Tübingen und promoviert über verdeckte technische Ermittlungsmaßnahmen. Er entwickelt die Studieninhalte zu Computerstrafrecht und Computerstrafprozessrecht für einen Studiengang "Digitale Forensik" und forscht insbesondere über die Europäisierung des Strafrechts und der Strafrechtsdurchsetzung.

Kontak zu den Autoren

Prof. Dr. Felix Freiling	Dominik Brodowski
Friedrich-Alexander-Universität	Eberhard Karls Universität Tübingen
Department Informatik	Juristische Fakultät
Lehrstuhl für Informatik 1	Geschwister Scholl Platz
Am Wolfsmantel 46	72074 Tübingen
91058 Erlangen	Tel: +49 7071 29 72692
Tel. +49 9131 85 25300	E-Mail: dominik.brodowski@jura.uni-tuebingen.de

Inhaltsverzeichnis

1. Einleitung

Die Cyberkriminalität umgibt in der öffentlichen Diskussion eine Aura des Geheimnisvollen und Konspirativen. Dies zeigt sich bereits am Schlagwort – oder Mythos? – »rechtsfreier Räume im Internet« ebenso wie am Schlagwort – oder Mythos? – der »Hacker« als *den* Kriminellen des 21. Jahrhunderts. Wird die von Cyberkriminalität ausgehende Bedrohung eher unter- oder überschätzt? Werden die Möglichkeiten der Strafverfolger eher unter- oder überschätzt? Diese Fragen, die nur diffus wahrgenommene Bedrohungslage und die individuell, politisch und gesellschaftlich gefühlte Machtlosigkeit gegenüber Cyberkriminalität gilt es nun – wenigstens ein wenig – ins rechte Licht zu rücken.

Cyberkriminalität – was ist das?

Der Begriff »Cyberkriminalität« bezeichnet grob gesprochen diejenige Kriminalität, die im Cyberspace stattfindet. Die aus dem Kybernetikbegriff entstandene, englische Wendung »cyber« stellt einen Bezug her zum Einsatz von Informations- bzw. Computertechnologie. Dies schließt somit sowohl singuläre informationstechnische, Daten verarbeitende Systeme ein als auch die Vernetzung einer Vielzahl solcher Systeme, etwa im Internet.

Die Entwicklung der Cyberkriminalität ist eng verbunden mit der Entwicklung *vernetzter* Computersysteme. Böckenförde (2003, S. 4 ff.) beschreibt diese Entwicklung anschaulich im Zusammenhang mit der Entstehung des Internets. So herrschte »im Netz« zunächst ein Klima der Offenheit und Kreativität, in dem Informationen und Gedanken frei ausgetauscht werden konnten. Der dadurch entstandene soziale Raum wurde nach dem Roman »Neuromancer« von Gibson (1984) »Cyberspace« genannt. Mit dem Wachstum der Netzgemeinde, spätestens seit Mitte der 1990er Jahre, gewannen finanzielle und kommerzielle Interessen zunehmend an Bedeutung. Infolgedessen blieb auch der Cyberspace nicht verschont von Kriminalität. Während sich die Kriminalität anfangs nur vereinzelt und eher in Form ethisch-motivierter Hacker äußerte, dominiert heute eine finanziell-motivierte, professionelle Kriminalität den Cyberspace.

Forschung und Politik messen dem Thema Cyberkriminalität eine auch in Zukunft weiter wachsende Bedeutung zu. Hierbei ist Cyberkriminalität ein multidimensionales und damit sehr komplexes Phänomen. Der vorliegende Text versucht, sich diesem Phänomen aus unterschiedlichen Perspektiven anzunähern und damit die sachliche Diskussion im Rahmen des Forschungsforums Öffentliche Sicherheit zu unterstützen. Bedingt durch die Fachgebiete der beiden Autoren, eines Juristen und eines Informatikers, liegen die Schwerpunkte der folgenden Ausführungen naturgemäß auf juristischen und technischen Aspekten. In weiteren, zukünftigen Forschungsarbeiten auf diesem Gebiet müssen aber auch ökonomische, kriminologische, soziologische und psychologische Aspekte in die

Diskussion einbezogen werden, um diesem komplexen Thema vor dem Hintergrund gesellschaftlicher Auswirkungen und zukünftiger Anforderungen gerecht zu werden.

Fragestellungen

Ausgangspunkt für die Erstellung dieser Studie waren folgende Fragen:

- Auf welche Gefahren müssen sich Gesellschaft und Staat einrichten? Was sind die technischen Möglichkeiten? (Wie) Ist die Gefahrenlage überhaupt sinnvoll zu bewerten oder abzuschätzen?
- Wer sind die Akteure der Cyberkriminalität? Wie viel Schadwirkung halten Gesellschaft und Staat aus? Was bedeutet Internetkriminalität auf der Schadensseite (wirtschaftlich, human etc.)?
- Welche technischen, organisatorischen und rechtlichen Standardisierungen sind möglich und notwendig? Ist »weniger IT und weniger Vernetzung« eine Antwort? Wie kann eine politische Reaktion aussehen?

Fokus dieser Studie

Die Aura des Geheimnisvollen und Konspirativen der Cyberkriminalität manifestiert sich auch in der Art und Weise, wie das Thema in den Medien aufbereitet wird. Aber selbst für Wissenschaftler ist es manchmal schwierig, Mutmaßungen von Fakten zu unterscheiden. Den Autoren war es darum wichtig, die dargelegten Erkenntnisse entweder auf eigenes Wissen oder direktes Wissen aus der Forschungsliteratur zu stützen, statt auf indirektes Wissen aus der Presse.

Es gibt bereits zahlreiche andere Arbeiten, die das Themenfeld Cyberkriminalität aus unterschiedlichen Perspektiven beleuchten. Hilfreich bei der Entstehung dieses Textes waren vor allem die Bücher von Wall (2007), Kshetri (2010), Brenner (2010) und M. Gercke und Brunst (2009), die vor allem gesellschaftliche und ökonomische Aspekte sowie die Rechtslage in Deutschland betrachten.

Wie die Vorgänge um die Schadsoftware »stuxnet« zeigen, ist der Übergang zwischen Cyberkriminalität (*cybercrime*) und Cyberkrieg (*cyberwar*) fließend. Für letzteren Bereich ist das Buch von Gaycken (2011) umfänglich aussagekräftig, für die Bedrohungen durch die Aktivitäten terroristischer Organisationen im Internet die Darstellung von M. Gercke (2007a).

Gang der Darstellung

Um die Informationstechnologie und den Cyberspace zu entmystifizieren und um die grundlegenden Prinzipien zu erkennen, die der Cyberkriminalität und deren tatsächlichem Bedrohungspotential zugrunde liegen, vermitteln wir zunächst ein grundsätzliches Verständnis für die »Naturgesetze der Informatik« (Kapitel 2). Anschließend zeigen wir auf, was unter »Cyberkriminalität« überhaupt zu verstehen ist (Kapitel 3). Hierbei zeigt sich, dass nicht allein die bestehende Strafrechtsordnung diskutiert werden muss, sondern außerdem stets Wachsamkeit geboten ist, um auf neuartige technische Entwicklungen auch juristisch reagieren zu können. Die vielfältigen Möglichkeiten zur juristischen Bewältigung der Herausforderungen durch die Informationstechnologie stellen wir sodann nebst den verfassungsrechtlichen Rahmenbedingungen im Überblick vor (Kapitel 4).

Nach diesem – eher theoretischen – Teil der Studie widmen wir uns der Verlagerung der Kriminalität in den Cyberspace und die aus ihr resultierenden Herausforderungen (Kapitel 5). Auf dieser Grundlage stellen wir den Stand der Forschung zu den konkreten Erscheinungsformen der Cyberkriminalität, deren Akteure und den ökonomischen Prozessen und Folgen dar (Kapitel 6).

Was kann jeder Einzelne, was kann jedes Unternehmen und was kann Deutschland tun, um der Cyberkriminalität wirksam entgegen zu treten? In Kapitel 7 widmen wir uns diesen Fragestellungen zunächst aus technischer, dann aber schwerpunktmäßig aus juristischer Sicht. Hier zeigen wir auf, dass das deutsche Straf- und Strafprozessrecht rechtlich gesehen gut gerüstet ist zur Verfolgung von Cyberkriminalität. Da der Cyberkriminalität eine transnationale Komponente immanent ist, stellen wir schließlich auch die internationale Dimension der Cyberkriminalität und der informellen und formellen Möglichkeiten zur koordinierten Verfolgung von Cyberkriminalität vor (Kapitel 8).

Es verbleibt jedoch erheblicher weiterer Forschungsbedarf, insbesondere aus kriminologischer und soziologischer Sicht. Hinzu treten faktische Herausforderungen für eine effektive Verfolgung der Cyberkriminalität, wobei das Erfordernis einer verbesserten Ausbildung von Spezialisten zur Aufklärung und Abwehr von Cyberkriminalität hervorgehoben werden soll. Außerdem regen wir auch an, manche rechtlichen Schutzlücken zu schließen. Mit diesen offenen Fragen und Handlungsempfehlungen schließen wir unsere Darstellung (Kapitel 9).

Danksagungen

Die Autoren danken Marie-Luise Beck, Bruno Berger, Andreas Dewald, Hans-Georg Eßer, Ulrike Freiling, Lars Gerhold, Helmut Grohne, Hendrik Hoeth, Thorsten Holz, Helga Jäckel, Marion Liegl, Holger Morgenstern, Tilo Müller, Konstantin Sack, Kay H. Schumann, Sebastian Schinzel, Lena Schmidt, Sven Schmitt, Jörg Schwenk, Verena Seibold, Joachim Vogel, Victor Völzow und Stefan Vömel sowie unseren Familien für die hilfreiche Unterstützung bei der Erstellung dieser Studie.

2. Informationstechnische Systeme

2.1. Einleitung

Ohne Zweifel ist die moderne Informationstechnologie ein wesentlicher Antrieb für neue Formen der Kriminalität. Wenn es um neue, konkrete Kriminalitätsformen (wie beispielsweise »Phishing«) geht, dann muss man sich auch mit den konkreten Technologien (etwa »DNS-Spoofing«) auseinandersetzen, die diese Kriminalitätsformen ermöglichen. Die Informationstechnologie ist inzwischen ein sehr komplexes Feld geworden, auf dem es leider selbst Experten schwer fällt, den Überblick über aktuelle Entwicklungen zu wahren. Die schnelle Entwicklung erschwert auch die Erstellung von rechtlichen Normen, die auch noch mit der nächsten Computergeneration Schritt halten können. Dennoch zeichnen sich in dieser Entwicklung einige Prinzipien ab, die im Zusammenspiel mit krimineller Energie die heutigen und vermutlich auch die zukünftigen Trends im Bereich der Cyberkriminalität erklären können. Statt also auf konkrete Technologien einzugehen, möchten wir in diesem Kapitel die Prinzipien der Informationstechnik, sozusagen die »Naturgesetze der Informatik«, darstellen. Dieses Vorgehen soll verdeutlichen, dass der heutige Zustand des Cyberspace mit all seinen Unsicherheiten zu einem gewissen Grad unvermeidbar ist, dass also die historische Entwicklung notwendigerweise aus den technischen Rahmenbedingungen folgt. Die »menschlichen Rahmenbedingungen«, also etwa die Unkundigkeit vieler Benutzer, ja die unzureichende Erfahrung der gesamten Gesellschaft im Umgang mit vernetzten Computersystemen, bleibt bei dieser Betrachtung weitestgehend außen vor.

Grundlage für diese Sichtweise ist ein abstraktes und somit sehr weites Verständnis von Informationstechnologie, das sich in dem juristisch geprägten Begriff des *informationstechnischen Systems* manifestiert. Dieser Begriff findet etwa in Art. 91c Abs. 1 GG Verwendung und erfasst dabei sämtliche »technische Mittel zur Verarbeitung und Übertragung von Informationen« (BT-Drs. 16/12410, S. 8), um diese Norm auch für die zukünftige, noch unbekannte Weiterentwicklung der Informationstechnologie zu öffnen (vgl. Suerbaum, 2010, Art. 91c GG Rdn. 9 f.). Wir konkretisieren diesen Begriff in Form des *Zustandsautomaten* (2.2. und 2.3.) und verdeutlichen damit grundlegende Wirkungsprinzipien informationstechnischer Systeme, nämlich die Möglichkeit von Virtualisierung (2.4.), Vernetzung (2.5.) und die Problematik von Sicherheitslücken (2.6.).

Trotz aller Abstraktheit setzen dieses und die folgenden Kapitel ein gewisses Grundverständnis für konkrete Computersysteme und konkrete Rechnernetze voraus, wie man es etwa bei der alltäglichen Benutzung des Internets erlangt. Wir werden Begriffe wie Bit, Byte, Pixel, IP-Adresse oder Cookie nicht weiter erklären, sondern — wo es notwendig ist — auf Quellen verweisen.

2.2. Diskrete Zustände, Codierbarkeit und universelle Maschinen

Heute lernen bereits Kinder in der Schule, dass Computer nur »Nullen und Einsen« kennen. Meistens wird diese Feststellung lediglich benutzt, um die *binären Zahlen* und deren Arithmetik einzuführen, also das Rechnen mit Zahlen, die nur aus Nullen und Einsen bestehen (*Dualsystem*). Die Abstraktion von Stelle und Wertigkeit bei der Darstellung von Zahlen gehört zu den ersten grundlegenden Einsichten jedes Informatikers. Im Dualsystem zählt man nämlich nicht

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, \ldots$$

sondern

$$0, 1, 10, 11, 100, 101, 110, 111, 1000, 1001, \ldots$$

Entsprechend verstehen auch nur die Kenner von Binärzahlen den folgenden, unter Informatikern gebräuchlichen Witz:

> Es gibt genau 10 verschiedene Arten von Menschen auf der Welt: Solche, die Binärzahlen verstehen, und solche, die Binärzahlen nicht verstehen.

Der Blick auf die Binärzahlen lenkt aber häufig ab von einer anderen fundamentalen Einsicht, die für die folgenden Betrachtungen relevant sein wird. Da Computer alle Informationen schlussendlich im Binärformat abspeichern, kennen sie nur *eindeutig unterscheidbare* Zustände. In Anlehnung an die ursprüngliche Bedeutung des Wortes »diskret« als »abgesondert« verwendet man in der Informatik auch gerne den Begriff der *diskreten* Zustände. Diese Bezeichnung betont, dass es zwischen zwei binären Werten keine Zwischenwerte gibt. In der Folge befindet sich ein Computer zu jedem Zeitpunkt in einem klar definierten Zustand. Dies steht im Gegensatz zu einer grundlegenden Erfahrung, die man in der realen Welt macht: Materie ist (nahezu) beliebig zerteilbar.[1] Der Zustand der realen Welt ist also alles andere als »diskret« im Sinne der Informatik, während der Zustand eines Computers zu jedem Zeitpunkt immer bis ins letzte Bit exakt definiert ist.

Die Einsicht, dass Computer nur diskrete Zustände haben, erscheint anfangs als Einschränkung, als Unvollkommenheit. Wie soll eine Maschine, die nur diskrete Zustände kennt, Phänomene der realen Welt erkennen, verarbeiten und schließlich auf diese Phänomene zurückwirken können? Der Trick besteht darin, Phänomene nicht exakt nachzubilden, sondern nur *hinreichend* genau, also derart, dass die Maschine ihre Aufgabe erledigen kann. Diese Einsicht erscheint im Zeitalter digitaler Medien trivial: Es gehört heute zum Allgemeinwissen, dass beispielsweise digitale Bilder (der realen Welt) nur eine bestimmte

[1] Physiker mögen noch über die genaue Formulierung dieser Aussage streiten, vgl. etwa Heisenberg (1984).

maximale Auflösung haben und man bei hinreichender Vergrößerung schlussendlich auf die (nicht mehr unterteilbaren) Pixel stößt. Ähnlich verhält es sich mit den Codierungen von Geräuschen und Musik beispielsweise im MP3-Format, das sehr geschickt gerade so viel Information speichert, dass das menschliche Ohr das Geräusch als unverändert wahrnehmen kann.

In diesem Sinn sind alle Naturphänomene in einer vorher festgelegten Genauigkeit als binäre Zahl codierbar. Dies gilt umso mehr für schriftlich niedergelegte Informationen, Konzepte, Ideen. Diese sind oft schon bei ihrer Erzeugung bereits in »diskreter Form« vorhanden, wie etwa dieser Text, den der Autor gerade auf einer Tastatur als Folge einzelner, klar unterscheidbarer Tastendrücke in den Computer tippt. Die diskrete Form all dieser Artefakte macht es möglich, *perfekte Kopien* zu erzeugen, Kopien also, die nicht vom Original zu unterscheiden sind.

Die prinzipielle Codierbarkeit aller Arten von Informationen ist einerseits eine wesentliche Grundlage für den Siegeszug des Computers in allen Lebensbereichen. So kann man verschiedene relevante Phänomene in das Binärformat übersetzen (codieren) und dann alle diese Phänomene mit derselben Maschine (dem Computer) verarbeiten. Aber nicht nur diese »Gleichbehandlung« macht den Computer zu einer universellen Maschine. Alles, was hinreichend genau beschrieben werden kann, kann durch Computer berechnet werden.

Allerdings sind die prinzipielle Codierbarkeit von Information und die Universalität des Computers als Rechenmaschine auch ein Fluch der Informatik. Gemeint sind die von Gödel (1931) formulierten *Unvollständigkeitstheoreme* für digitale Computer, ein »Naturgesetz« der Informatik, das prinzipielle Grenzen der Leistungsfähigkeit von digitalen Maschinen aufzeigt. Grob gesprochen resultieren diese Grenzen aus der Möglichkeit, Programme auf sich selbst anzuwenden (vgl. zur Einführung Schöning, 1997). Dieses und andere Probleme zeigen, dass auch perfekt formalisierbare Rechenaufgaben nicht immer durch Computer gelöst werden können.

2.3. Zustandsautomaten

Computer befinden sich zu jedem Zeitpunkt also in einem fest definierten diskreten Zustand. Da ein Computer allerdings nur selten in ein- und demselben Zustand verharrt, ist die Frage berechtigt, wie sich der Übergang von einem zum anderen Zustand vollzieht. Wie dies konkret funktioniert, ist für die weiteren Betrachtungen (nahezu) unerheblich und wird andernorts erläutert (Hennessy & Patterson, 1990; Tanenbaum, 1990). Wesentlich ist vielmehr die Einsicht, dass eine Handlungsanweisung (ein Programm) vorliegen muss, die diesen Übergang regelt. In der Informatik wurde in Form des *Zustandsautomaten* ein einfaches Modell entwickelt, das eine Art Blaupause für jedes heutige digitale Rechensystem darstellt. Ein Zustandsautomat wird oft auch einfach nur als *Automat*

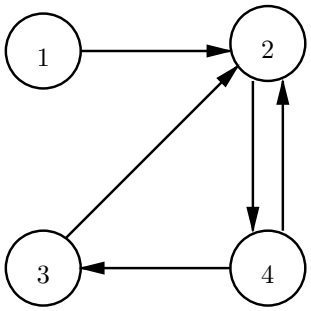

Abbildung 2.1: Beispiel für einen einfachen Zustandsautomaten.

bezeichnet. Seine Ideen gehen nicht zuletzt zurück auf die Arbeiten von Turing (1936, 1937) und seine berühmte »Turing-Maschine«.

2.3.1. Definition und Beispiel

Vereinfacht ausgedrückt besteht ein Automat aus zwei Bestandteilen:

1. einer Menge von diskreten Zuständen und
2. einer Beschreibung der Zustandsübergänge.[2]

Automaten haben den Vorteil, dass man sie recht intuitiv als Zeichnung darstellen kann. Abbildung 2.1 zeigt einen einfachen Zustandsautomaten mit vier Zuständen, die als Kreise dargestellt und mit den Ziffern 1 bis 4 bezeichnet sind. Die Zustandsübergänge sind als Pfeile zwischen den Zuständen eingetragen. Den Automat kann man sich als abstrakte Darstellung eines Parkscheinautomaten vorstellen. In Zustand 1 wurde er anschaltet. Anschließend geht er in Zustand 2 über, in dem er »Bitte Geld einwerfen« anzeigt. Wird Geld eingeworfen, welchselt der Automat in Zustand 4. Wenn die Geldmenge noch nicht ausreicht, dann wechselt der Automat wieder zurück in Zustand 2 (»Bitte Geld einwerfen«). Falls genug Geld eingeworfen wurde, wechselt der Automat in Zustand 3, in dem er das Parkticket ausgibt und wartet anschließend in Zustand 2 auf den nächsten Kunden.

Die Zustände des Automaten resultieren aus unterschiedlichen Belegungen des Speichers einer Rechenmaschine. Die Zustandsübergänge bilden im Wesentlichen die Aktivitäten des *Programms* ab, das die Rechenmaschine ausführt. Das Programm ist die Handlungsvorschrift des Computers (die *Software*) und wird auch im Speicher der Rechenmaschine gehalten. In der Praxis ist dieses Programm natürlich veränderbar (wenn man etwa neue Software installiert). Die Software des Rechners ist die Grundlage für die *Automatisierbarkeit* von Vorgängen. Wie oben bereits erwähnt, kann ein Computer alles,

[2] Letzteres wird mathematisch als Relation von Zuständen ausgedrückt, also als Menge von Paaren von Zuständen. Für eine formale Beschreibung und zur Vertiefung siehe Schöning (1997).

was hinreichend genau (also durch ein Programm) beschrieben werden kann, autonom berechnen.

2.3.2. Große Zustandsräume

Die Menge der möglichen Zustände eines Computers ist abhängig von der Größe seines Speichers. Ein hypothetischer Computer mit einem Speicher von einem Bit hätte zwei verschiedene Zustände (0 und 1). Bei zwei Bits kann man jeden Zustand des einen Bits mit jedem Zustand des anderen kombinieren, was in 4 verschiedenen Zuständen resultiert (00, 01, 10, 11). Je mehr Bits hinzukommen, desto mehr Kombinationen sind möglich.

Bei b Bits gibt es 2^b verschiedene Kombinationen und entsprechend viele Zustände, also beispielsweise bei 8 Bits, $2^8 = 256$ Zustände. Die Zahl der möglichen Zustände steigt also sehr schnell mit der Größe des Speichers. Ein moderner Computer mit einem Hauptspeicher von einem Gigabyte (2^{30} Bytes) kann $8 \cdot 2^{30} = 2^{33}$ Bits speichern. Folglich besitzt er

$$2^{2^{33}} = 2^{8589934592} \approx 10^{2576980378}$$

verschiedene diskrete Zustände. Das ist eine sehr große Zahl, wenn man bedenkt, dass die Anzahl aller Atome im (bisher bekannten) Universum zwischen 10^{78} und 10^{82} liegen soll. Die Anzahl der Zustände nimmt bei der Vernetzung mehrerer Computer ebenfalls explosionsartig zu. Das Internet schließlich ist in der Zahl seiner möglichen Zustände zahlenmäßig kaum mehr erfassbar. Nicht alle diese Zustände finden jeweils Verwendung in einem konkreten System. Typischerweise bewegt sich ein Computer in einem deutlich kleineren Zustandsraum. Diese Berechnungen sollen aber zeigen, dass informationstechnische Systeme sehr komplex sein können.

In der Praxis besteht also qualitativ kaum mehr ein Unterschied zwischen der Komplexität, die man von der realen Welt kennt, und der des Cyberspace. Mit der fortschreitenden Vernetzung wird diese Entwicklung noch weiter zunehmen. Damit halten aber auch Phänomene Einzug in den Cyberspace, die man dort lange nicht vermutete, wie beispielsweise die Schwierigkeit, keine Spuren zu hinterlassen. Mit diesen Phänomenen muss jeder zurecht kommen, der sich im Cyberspace bewegt, also sowohl rechtstreue Benutzer als auch Kriminelle. Dies manifestiert sich etwa darin, dass der Weg vieler ahnungsloser Benutzer beim Surfen im Internet durch Cookies nachvollzogen werden kann, oder dass Kriminelle Spuren ihrer Aktivitäten in Logdateien oder Caches übersehen. Dies führt zu der Erkenntnis, dass es bei einer hinreichenden Komplexität des zugrunde liegenden informationstechnischen Systems im Cyberspace genauso wenig die spurenlose Straftat gibt wie in der realen Welt.

2.3.3. Rechengeschwindigkeit und Flüchtigkeit von Zuständen

Ein Automat ist eine abstrakte Maschine, die ohne direkten Bezug zu einem konkreten Computer nur in der Theorie existiert. Damit ein Automat arbeiten kann, benötigt er

aber eine konkrete Maschine (Hardware), die ihn »zum Leben« erweckt. Diese konkrete Maschine wechselt dann über die Zeit gemäß ihrer Handlungsanweisung von Zustand zu Zustand. Dies kann sehr schnell geschehen. Moderne Computer vollziehen innerhalb von einer Sekunde mehrere Millionen Zustandsübergänge. Dabei geht jeweils der alte (vorherige) Zustand verloren. Das hat eine gewisse *Flüchtigkeit* der gespeicherten Daten zur Folge. Der neue Zustand ist aber in der Regel nicht vollständig neu. Viele Bits im Speicher bleiben unverändert. Insofern kann man aus dem aktuellen Zustand doch noch einige Rückschlüsse ziehen, in welchen Zuständen der Computer vorher einmal gewesen war.

Eine etwas andere Art von Flüchtigkeit besteht für Daten, die im Hauptspeicher eines Rechners abgelegt sind. Schaltet man den Rechner aus, sind diese Daten in der Regel nach kurzer Zeit (wenigen Sekunden) nicht mehr nachweisbar.

Trotz ihrer rasanten Rechengeschwindigkeit können in der Praxis viele Aufgaben nicht durch Computer berechnet werden. Das in unserem Kontext nächstliegende Beispiel ist das Brechen von Verschlüsselungsverfahren durch Ausprobieren aller Schlüssel. M. Gercke und Brunst (2009, Rdn. 49) verdeutlichen dies am Beispiel eines Computers, der eine Million Schlüssel innerhalb einer Sekunde prüfen kann. Die Entschlüsselung einer Datei, die mit einem Schlüssel der Länge 20 Bit verschlüsselt wurde, dauert dann im schlimmsten Fall, nämlich wenn man die tatsächlich verwendete Kombination zuletzt ausprobiert, etwa 1 Sekunde. Bei einem 40-Bit-Schlüssel dauert dieser Vorgang im ungünstigsten Fall bereits 2 Wochen, bei 56-Bit mehr als 2200 Jahre. Zwar sind in der Praxis viele kombinatorische Probleme lösbar, meist aber nur dadurch, dass man Einschränkungen in der Lösungsqualität hinnimmt. Viele Herausforderungen bei der Speicherung und Verarbeitung immer größer werdender Datenmengen sind noch ungelöst. Die Tatsache, dass die Speicher- und Netzwerkkapazität schneller wächst als die Berechnungskapazität, deutet möglicherweise auf ein weiteres grundsätzliches Problem hin, mit dem die Gesellschaft leben muss, nämlich auf eine fast unbeherrschbare Datenflut.

2.4. Virtualisierung

Ein konkreter Zustandsautomat, wie etwa der aus Abbildung 2.1, besitzt immer eine konkrete Menge von Zuständen und Zustandsübergängen. Wenn man mehrere Zustände gruppiert, entsteht ein neuer (abstrakterer) Zustandsautomat. Dies ist in Abbildung 2.2 an einem Beispiel dargestellt. Der Automat aus Abbildung 2.1 ist der Ausgangspunkt. Er hat vier Zustände, die mit den Ziffern 1 bis 4 bezeichnet sind. Der gestrichelte Automat »überlagert« den ursprünglichen Automaten dergestalt, dass die Zustände 1 und 2 zu einem neuen Zustand A zusammengefasst werden und die Zustände 3 und 4 zu einem neuen Zustand B. Immer wenn im ursprünglichen Automaten ein Zustandsübergang stattfindet, dann kann es sein, dass auch im gestrichelten Automaten ein Zustandsübergang stattfindet. Dies geschieht aber nur dann, wenn ein Zustandsübergang zwischen den

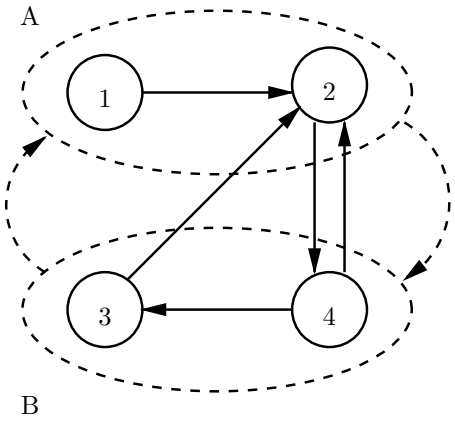

Abbildung 2.2: Ein Automat implementiert einen anderen Automaten (Virtualisierung).

ursprünglichen »Zustandsgruppen« (also 1 und 2 auf der einen Seite und 3 und 4 auf der anderen) stattfindet. Im Beispiel hat der gestrichelte Automat zwei Zustände und zwei Zustandsübergänge: den einen von A nach B und den anderen von B nach A. Wenn der ursprüngliche Automat arbeitet, dann arbeitet also der gestrichelte Automat auch (auch wenn dieser nicht notwendigerweise seinen Zustand dabei ändert).

Grob gesprochen bedeutet das eben vorgestellte Konzept, dass der urspüngliche Automat den gestrichelten Automaten *implementiert*: Der ursprüngliche Automat ist eine Maschine, die den gestrichelten Automaten realisiert. Der ursprüngliche Automat könnte beispielsweise eine konkrete Maschine (Hardware) sein und der gestrichelte Automat ein Programm, das auf der Hardware ausgeführt wird.

Prinzipiell kann so jeder Automat durch einen anderen Automaten implementiert werden. Dies bildet die Grundlage für das, was wir heute *Virtualisierung* nennen. Auf technischer Ebene wird dabei die Bindung einer Datenverarbeitung an eine physikalische Hardware aufgelöst. Das Konzept selbst ist so alt wie die Informatik, allerdings ist die Mächtigkeit des Konzepts erst dadurch in das Bewusstsein vieler Anwender gelangt, dass man *ganze Rechner* ausführen lässt. Lange Jahre war die Virtualisierung ganzer Rechner ein Wunsch der Informatiker, der sich aufgrund mangelnder Rechenleistung der Hardware nicht realisieren ließ.

Heute gibt es zahlreiche Programme, die herkömmliche PCs oder gar komplette Rechnernetze virtualisieren (VMWare Inc., 2009; Oracle Inc., 2010; Microsoft Inc., 2010). Man kann also ohne weiteres »auf« einem MacOS-Rechner einen Windows-Rechner starten. Gerade für Rechenzentren ist es von Vorteil, mehrere virtuelle Rechner auf einem einzigen, physischen Rechner laufen zu lassen. Wenn einer dieser virtuellen Rechner nicht mehr benötigt wird, kann man einfach das Programm, das diesen Rechner realisiert, abschalten, und die hierdurch freigesetzten Hardwareressourcen anderweitig nutzen. Man kann aber nicht nur virtuelle Rechner beenden und neu starten, man kann diese Rechner auch kopieren und »an anderer Stelle« wieder weiterlaufen lassen. Dies kann ein anderer

Bereich im Zustandsraum sein, also woanders im Speicher desselben physischen Rechners oder auf einem ganz anderen physischen Rechner. Die physikalischen Ressourcen – etwa Datenspeicher oder Rechenkapazität – verschiedener, auch räumlich verteilter informationstechnischer Systeme (»Computing Clouds«; s. hierzu Schneider, 2010) werden gebündelt und je nach Bedarf einzelnen »virtuellen« informationstechnischen Systemen zur Verfügung gestellt, die sich jeweils als isoliertes System präsentieren.

Gerade die Virtualisierung ganzer Rechner hat heute in auch für Laien verständlicher Form Rechenleistung von ihrem konkreten Ausführungsort entkoppelt. Dies führt zu ganz konkreten praktischen Schwierigkeiten überall dort, wo es notwendig ist, Berechnungen geografisch zu lokalisieren. So ist es etwa nicht überraschend, dass es im Bereich der Internetkriminalität so schwierig ist, den »Tatort« festzustellen. Als weiteres Beispiel nennen wir die Probleme, die im Bereich des Datenschutzes entstehen, wenn Berechnungen (zusammen mit ihren Daten) in geografische Regionen verlegt werden, in denen andere rechtliche Rahmenbedingungen gelten.

Virtualisierung ist auch ein Sinnbild für die Schwierigkeit festzustellen, ob eine Berechnung auf einem physischen Rechner oder auf einem virtuellen Rechner abläuft oder abgelaufen ist. Den Daten selbst sieht man es nicht an, und Programme, die etwa aus Gründen des Urheberrechtsschutzes nur auf einer speziellen Hardware ablaufen sollen, haben wenig Möglichkeiten, dies zu überprüfen. Dieses Dilemma wurde 1999 durch den Film »Matrix« von Andy und Larry Wachowski metaphorisch popularisiert. Aus »Matrix« wurden gleichermaßen mit »Red Pill« und »Blue Pill« Namen in die Informatik übernommen. Sie stehen dort für Programmierkniffe, die es erlauben, während der Laufzeit eines Programms die Virtualisierungsebene zu wechseln, also beispielsweise die Hardware, auf der ein Programm läuft, zu virtualisieren, ohne dass das Programm etwas davon merkt (Rutkowska, 2006, 2004).

Die einzige Möglichkeit, diese Beliebigkeit der Ausführungsumgebung zu vermeiden, liegt in der Veränderung der Hardware, also des physischen Rechners selbst. Das Ziel dabei ist, ein Programm wieder an seine physische Ausführungsumgebung zu binden. Ein gutes Beispiel dafür sind Chipkarten, wie man sie etwa zur Authentifikation beim Online Banking einsetzt. Eine Chipkarte enthält einen Kleinstcomputer mit einem eingebauten Geheimnis, der so mit seiner Umgebung (der Plastikkarte) verbunden ist, dass sein Zustandsraum und seine Zustandsübergänge nicht auslesbar sind (jedenfalls nicht ohne den Computer selbst zu zerstören). Man kann den darin realisierten Automaten also nicht kopieren oder ohne die Chipkarte selbst ausführen. Eine ähnliche Idee verfolgt der Ansatz des »Trusted Computing« (Sadeghi, Stüble & Pohlmann, 2004). Der Nachteil von derartigen Techniken ist, dass der Benutzer keine Freiheit mehr hat, die Ausführungsumgebung auszuwählen.[3]

[3] Eine etwas weichere Bindung von Ausführungsumgebung an Berechnung kann man erreichen, indem man Sensoren in die Berechnung mit einbezieht. Beispiele für derartige Sensoren sind eine eingebaute

Über den vielen Virtualisierungsebenen darf aber nicht vergessen werden, dass eine Berechnung schlussendlich *immer* eine konkrete Hardware (einen anfass- und lokalisierbaren Rechner) und dass ein abstraktes Datum *immer* einen konkreten Speicher (etwa eine Festplatte oder einen USB-Stick) benötigt, um zu existieren. Diese konkrete Hardware ist Teil der physischen, realen Welt. Der Cyberspace ist schlussendlich doch wieder Teil der realen Welt, und Handlungen, die im Cyberspace durchgeführt werden, können prinzipiell immer auch auf Handlungen in der realen Welt zurückgeführt werden. Diese Randbedingungen ermöglichen prinzipiell auch immer die rechtliche Erfassung und forensische Auswertung von Straftaten im Internet.

2.5. Vernetzung und Authentifikation

Die Vernetzung von Computern wird in der Informatik schon lange praktiziert. Die Möglichkeiten der Vernetzung wurden aber erst durch das Internet einer breiten Öffentlichkeit bekannt. Während Virtualisierung die (wenigstens lokale) Entkopplung von der Ausführungshardware mit sich bringt, führt Vernetzung zu einer (unbegrenzten) Entkopplung der Daten vom geographischen Aufenthaltsort. In der Literatur wird häufig der Begriff der *räumlichen Entgrenzung* verwendet.[4] Bildlich gesprochen bedeutet räumliche Entgrenzung, dass im Internet jeder eines jeden Nachbarn ist. Man kann also nicht wie in der realen Welt versuchen, in einer »besonders sicheren Gegend« zu wohnen.[5]

Vernetzung und Virtualisierung führen also zu einer vollkommenen Beliebigkeit des Ortes für eine Berechnung. Beliebigkeit bedeutet hier zweierlei: Einerseits bedeutet es, dass es einem Programm egal sein kann, wo auf der Welt der konkrete Rechner steht, der es ausführt. Andererseits hat das Programm auch gar keine Möglichkeit festzustellen, wo auf der Welt der Rechner steht, der es ausführt. Dies hat weit reichende Konsequenzen für die Praxis, wenn es etwa darum geht, die Identitätsüberprüfung (Authentifikation) eines Benutzers durchzuführen. Authentifikation ist die Grundlage für jede Form von Zugriffsschutz und ist insbesondere in vernetzten Systemen wichtig, da man im Gegensatz zu einem lokalen Rechner die Identitätsüberprüfung nicht so leicht an einem physischen Aufenthaltsort festmachen kann.

Um dieses Problem zu verdeutlichen, muss man sich eine Welt vorstellen, in der man

---

Uhr, die Zeitstempel vergibt, oder Ortssensoren (etwa via GPS), die prüfen, an welchem Ort sich das Computersystem befindet. Bei der Bewertung dieses Ansatzes spielt die Manipulierbarkeit dieser Sensoren eine entscheidende Rolle. Interessant erscheint auch der neue Ansatz der *physically unclonable functions*, bei dem ein Geheimnis auf atomare Strukturen zurückgeführt wird (Devadas, 2009). Die technische Entwicklung ist in diesem Bereich noch nicht abgeschlossen.

4 Konzeptionell ist Vernetzung aber kein neues Phänomen, sondern lässt sich über so genannte *Produktautomaten* auch in das Modell der Zustandsautomaten einbetten, siehe Schöning (1997). Auch das Internet ist also ein (wenn auch sehr großer) Zustandsautomat.

5 Natürlich können technische Vorkehrungen wie Firewalls einen gewissen Schutz bieten, aber allein die prinzipielle Zugreifbarkeit von Daten, etwa beim Surfen im Web, sorgt schon für eine Gefährdung.

beliebige Artefakte perfekt kopieren kann. Hier könnte sich Person A mühelos als Person B ausgeben, weil sich A nicht nur den Personalausweis von B kopieren sondern A auch das Aussehen von Person B annehmen könnte. Echte Authentifikation ist also nur möglich, wenn man etwas hat, was man nicht kopieren kann, oder wenn man zusätzliche Annahmen über die reale Welt machen kann. Hier kommt die Bindung der virtuellen Welt an die reale Welt wieder ins Spiel. Ein Passwort ist beispielsweise nur dann ein verlässliches Authentifikationsinstrument, wenn garantiert ist, dass keine andere Person oder kein anderes System jemals dieses Passwort lernt. Diese Annahme ist in der Praxis in der Regel nicht gegeben, sei es wegen der Unvorsichtigkeit vieler Benutzer bei der Wahl und im Umgang von Passwörtern oder der Möglichkeit, Passwörter durch Schadsoftware in einem Rechner oder Netzwerk auszuspähen.

Die Beliebigkeit des Ortes einer Berechnung verstärkt sich im Kontext der Authentifikation. In der Praxis reduziert man häufig die Frage, »wer« für einen Kommunikationsvorgang verantwortlich ist, auf die Frage, »woher« dieser Kommunikationsvorgang kommt. Wenn man den technischen Ausgangspunkt einer Kommunikationsverbindung identifiziert hat, heißt das aber nicht, dass die Kommunikation dort in der realen Welt initiiert wurde. Der Ausgangspunkt einer Kommunikationsverbindung kann zugleich Endpunkt einer anderen Kommunikationsverbindung sein. Durch ein dazwischen geschaltetes Programm werden diese Verbindungen wie durch einen Mittelsmann gekoppelt. Dieses Konzept wird in der Praxis in vielen Bereichen eingesetzt. Beispielsweise versuchen Kriminelle, beim Eindringen in Computersysteme ihre Spuren durch eine lange Kette von Internetverbindungen zu verschleiern (etwa mittels so genannter Proxy-Programme), die nach und nach zurückverfolgt werden müssen, um den eigentlichen Ausgangspunkt der Aktivitäten herauszufinden. Analog funktionieren auch Anonymisierungsdienste wie Tor (Dingledine, Mathewson & Syverson, 2004) oder Jap (Köpsell, Federrath & Hansen, 2003), die unter anderem durch lange Ketten von Zwischenrechnern die Rückverfolgbarkeit von Kommunikationsverbindungen erschweren sollen.[6] Eine einfache Rückverfolgbarkeit der Kommunikationsbeziehung ist dann nur noch möglich, wenn man die Kommunikationsinhalte betrachtet, etwa charakteristische Dateien, die ein Krimineller auf einem Server hinterlassen oder ein Benutzer über ein Anonymisierungsnetzwerk auf seinen eigenen Rechner heruntergeladen hat.

2.6. Sicherheitslücken in Systemen

Die Erstellung von Software ist eine sehr komplexe Angelegenheit, und es ist heute allgemein anerkannt, dass es unmöglich ist, Software zu schreiben, die keine Fehler enthält. Ein Fehler bewirkt, dass die Software sich in besonderen Situationen nicht wie

[6] Ein verwandtes Konzept sind die so genannten »man in the middle«-Angriffe. Dabei befindet sich der Angreifer zwischen den beiden Kommunikationspartnern und täuscht ihnen das jeweilige Gegenüber vor, ohne dass diese etwas davon bemerken.

gewünscht verhält. Dieses unerwünschte Verhalten hat Auswirkungen auf die Sicherheit eines Systems, wenn ein Angreifer beispielsweise die Kontrolle über das System gewinnen oder vertrauliche Daten ausspähen möchte. Wenn ein Fehler in dieser Form durch einen Angreifer ausgenutzt werden kann, spricht man von einer *Sicherheitslücke* oder *Schwachstelle* im System.

Um eine Sicherheitslücke auszunutzen, muss ein Angreifer Einfluss auf das System nehmen können. Am einfachsten kann dies geschehen durch eine physische Einflussnahme auf das System, etwa durch Einbau einer Überwachungshardware oder durch das Starten des Systems mit einem anderen Betriebssystem von CD. Aber auch ohne physischen Kontakt kann Einfluss auf ein System ausgeübt werden, zum Beispiel durch Manipulation der Eingabedaten, also etwa durch Versand von speziell gestalteten Nachrichtenpaketen über ein Netzwerk. Prinzipiell stellt aber *jede* Eingabe zum System eine potentielle Gefahr dar, denn jedes Programm enthält Schwachstellen. Diese Aussage gilt auch für jede Art von Anwendungsprogrammen, von Webbrowsern über Textverarbeitungsprogrammen bis hin zu Videoplayern. Durch gut ausgebildete Software-Entwickler und -Tester sowie durch extensive Untersuchungen und Erfahrungen mit Programmen kann die Menge an Schwachstellen deutlich reduziert werden. Allerdings bestehen die Gefahren in jeder neu geschriebenen Software von Neuem. Die Anfälligkeit von Software korrespondiert dabei nicht selten mit ihrer Funktionsvielfalt: Mehr Möglichkeiten, mehr »Features«, führen zu höherer Komplexität und damit zu mehr Schwachstellen. Dieses Phänomen lässt sich am Beispiel der heutigen Technologievielfalt im World Wide Web und den umfangreichen Anforderungen an heutige Webbrowser verdeutlichen. Blazakis (2010) bringt diese Entwicklung auf den Punkt, indem er schreibt:

> »It would be difficult to design a more exploit friendly environment than the classic web browser. Bursting at the seams with plug-ins, it requires a robust parser to salvage what could be any of 6+ versions of mark-up taking into account possible legacy work-arounds. With the advent of ›Web 2.0‹, a browser must also include a high performance scripting environment with the ability to rewrite those parsed pages dynamically.«

Aber auch Anwendungsformate wie PDF leiden an zunehmender Funktionsvielfalt und aus ihr resultierender Anfälligkeit ihrer Anwendungsprogramme.

Vernetzung verstärkt die Gefahr zusätzlich, dass ein System erfolgreich angegriffen wird. All dies trifft zu, auch ohne die »Schwachstelle Benutzer« zu betrachten. Technisch gesehen bringt der Angreifer das System in einen Zustand, der regulär nicht erreicht worden wäre. Von dort nimmt die Berechnung einen unerwünschten Verlauf.

Schwachstellen gibt es in unendlicher Vielfalt (Howard, LeBlanc & Viega, 2005). Bei den klassischen Pufferüberläufen (Aleph One, 1996) kann ein Angreifer in der Regel eigenen

Code in ein laufendes Programm einschleusen und zur Ausführung bringen. Aber nicht »böser Programmcode« ist notwendigerweise das Problem, sondern »böse Berechnungen«, wie die neuesten Entwicklungen im Bereich des Return-oriented Programming zeigen (Shacham, 2007; Hund, Holz & Freiling, 2009). Mit dieser Programmiertechnik steuert man ein System, indem man den Programmcode, der bereits auf diesem System existiert, gewissermaßen neu zusammensetzt. Böse Berechnungen sind viel schwieriger zu erkennen und zu vermeiden als nur böse Programme.

Insgesamt ist unser Wissen über die prinzipiellen Ursachen und die Natur von Systemschwachstellen heute noch sehr gering.

2.7. Zusammenfassung

Die Entwicklung informationstechnischer Systeme ist längst noch nicht abgeschlossen. Dennoch zeichnen sich in dieser Entwicklung einige Prinzipien ab, die im Zusammenspiel mit krimineller Energie die heutigen und vermutlich auch die zukünftigen Trends im Bereich der Cyberkriminalität erklären können. Wir fassen die wesentlichen Prinzipien hier kurz zusammen:

- Automatisierbarkeit: Im Cyberspace kann man Aktivitäten programmieren und durch Computer ausführen lassen. Ein begrenzter Aufwand kann durch massenhafte Ausführung ein Vielfaches an Wirkung erzielen.
- Flüchtigkeit: Im Gegensatz zu den archetypisch greifbaren und beständigen körperlichen Sachen sind Computerdaten regelmäßig flüchtig. Spuren verwischen so schneller als in der realen Welt.
- Räumliche Entgrenzung: Virtualisierung und Vernetzung führen dazu, dass programmierte Handlungen unabhängig vom realen Ort durchgeführt werden können. Prinzipiell sind nur der Ein- und Ausstiegspunkt einer Aktivität in den Cyberspace lokalisierbar, alles andere nicht.
- Kopierbarkeit: Beliebige Artefakte können im Cyberspace perfekt kopiert werden, also auch Authentifizierungsinformationen. Wird also eine Aktivität in den Cyberspace verlagert, kann man sie innerhalb des Cyberspace nicht mehr zweifelsfrei einer realen Identität zuordnen.
- Angreifbarkeit: IT-Systeme enthalten Schwachstellen, die von Angreifern ausgenutzt werden können, um schädliches Verhalten des IT-Systems zu erzeugen.

In Verbindung mit krimineller Energie führen diese Prinzipien zu großen Herausforderungen, die in den folgenden Kapiteln thematisiert werden.

3. Cyberkriminalität und Computerstrafrecht als ungeklärte Begriffe

3.1. Einleitung

Begriffe wie »Cyberkriminalität«, »Computerkriminalität«, »Computerstrafrecht« oder »Internetstrafrecht« sind in der deutschen Strafrechtsordnung gesetzlich nicht definiert. Zwar findet sich der Begriff »Computerkriminalität« etwa in der Bezeichnung des 41. Strafrechtsänderungsgesetzes aus dem Jahr 2007, doch weder dessen Gesetzgebungsmaterialien (vgl. BT-Drs. 16/3656) noch der Gesetzeswortlaut enthalten eine begriffliche Klarstellung. Doch auch außerhalb juristischer Fragestellungen werden die genannten Begriffe regelmäßig unpräzise verwendet. Als Ausgangspunkt für die weitere Betrachtung verschiedener rechtlicher und technischer Phänomene der Cyberkriminalität und des Computerstrafrechts ist es daher geboten, diese Begriffe näher zu erschließen.

3.2. Zum Kriminalitäts- und Strafrechtsbegriff

Doch bereits der Kriminalitätsbegriff ist in der juristischen Diskussion umstritten, in dessen Kern zudem der Begriff des Verbrechens steht. Eine *formelle* Betrachtungsweise bezeichnet mit Kriminalität die Erscheinungsformen, Konsequenzen und auch Ursachen aller Verhaltensweisen, die jeweils konkret unter Strafe stehen (Kaiser & Schöch, 2001, S. 195); dieser Begriff ist daher streng akzessorisch (abhängig) zur jeweils geltenden Strafrechtsordnung und kann daher Strafbarkeitslücken nur unzureichend beleuchten. Eine *kritische* Betrachtungsweise betrachtet hingegen die faktische Strafverfolgung durch staatliche Akteure (Albrecht, 2005, S. 84 ff.). Diese Sichtweise ist daher einerseits weiter als die formelle Theorie, da sie auch Strafverfolgungsmaßnahmen erfasst, die sich gegen strafloses Verhalten richten, andererseits aber auch enger, da sie strafbares Verhalten nicht erfasst, welches – aus welchen Gründen auch immer – nicht verfolgt wird. Eine *materielle* Sichtweise schließlich betrachtet neben den formell unter Strafe gestellten Verhaltensweisen auch diejenigen sozialschädlichen Verhaltensweisen, die der Gesetzgeber in legitimer Weise unter Strafe stellen könnte (Roxin, 2006, § 2 Rdn. 1).

Für die in dieser Studie zu behandelnde Thematik überzeugt die materielle Sichtweise. Die strafrechtliche Erfassung neuartiger, erheblich sozialschädlicher Verhaltensweisen hinkt nämlich notwendigerweise hinterher, da eine Strafdrohung vor der Begehung einer Tat gesetzlich angeordnet sein muss (*nulla poena sine lege*; Gesetzlichkeitsprinzip; Art. 103 Abs. 2 GG). Es erscheint uns für geboten, auch Strafbarkeitslücken zu analysieren; den Weg dafür bereitet am ehesten der materielle Verbrechens- und der darauf fußende Kriminalitätsbegriff.

Strafrecht wiederum ist die Summe aller Rechtsnormen, die für ein bestimmtes Verhalten eine bestimmte Strafe oder Maßnahme der Besserung oder Sicherung als Rechtsfolge

anordnen (Baumann, Weber & Mitsch, 2003, § 3 Rdn. 2; Roxin, 2006, § 2 Rdn. 1) und sich um dessen Durchsetzung bemühen. Das eigentliche Strafrecht umfasst dabei die Umschreibungen und Typisierungen von Unrecht (Tatbestände) vor allem im Besonderen Teil des StGB und grundsätzlichen Regeln über die Unrechts- und Schuldzurechnung im Allgemeinen Teil des StGB; der rechtliche Rahmen für die Durchsetzung des Strafrechts – das Prozessrecht – findet sich in der StPO.

3.3. Informationstechnische Systeme als Angriffsobjekt oder als Begehungsmittel

Es existieren viele verschiedene Versuche sowohl in der rechts- als auch in der ingenieurswissenschaftlichen Literatur, die Erscheinungsformen von Cyberkriminalität und deren rechtliche Erfassung zu klassifizieren (siehe etwa M. Gercke & Brunst, 2009, Rdn. 73 f.; Hilgendorf, Frank & Valerius, 2005, Rdn. 123; Kshetri, 2010, Kapitel 1.5; Marberth-Kubicki, 2010, Rdn. 50). Es ist zweifelhaft, ob diese Klassifikationen als solche einen Mehrwert bieten. Daher beschränken wir uns darauf, im Folgenden nur je eine grundsätzliche Klassifikationsmöglichkeit aus dem Bereich der Rechtswissenschaft – die Unterscheidung nach Angriffsobjekt und Begehungsmittel – und aus der Informatik – die Unterscheidung nach technik- und menschenorientierter Cyberkriminalität – vorzustellen.

Informationstechnische Systeme können einerseits verwendet werden, um eine Vielzahl herkömmlicher Straftaten vorzubereiten, etwa durch E-Mail-Kommunikation unter den Beteiligten, oder zu verwirklichen. Dies gilt jedenfalls für diejenigen Erfolgsdelikte, bei denen die konkrete Begehungsmodalität irrelevant ist. Die Beispiele hierfür sind mannigfaltig, und reichen etwa von einem Betrug (§ 263 Abs. 1 StGB), begangen durch den Versand einer das Opfer täuschende E-Mail, über eine Erpressung (§ 253 Abs. 1, Abs. 2 StGB), etwa zum Abtransport der Beute mittels eines ferngesteuerten Roboters (Fall »Dagobert«), bis hin zum Mord (§ 211 StGB), etwa durch vorsätzliche Manipulation der Steuerungsanlage eines Kraftfahrzeugs, so dass dessen Bremsanlagen versagen.

Andererseits aber werden zunehmend Delikte geschaffen, die als (unmittelbares) Angriffsobjekt informationstechnische Systeme vorsehen, wenn auch die Strafnormen mittelbar ganz anderen Zwecken dienen mögen, etwa dem Vermögens- oder dem Geheimnisschutz. Paradigmatisch hierfür genannt seien etwa das Ausspähen (§ 202a StGB) und Abfangen (§ 202b StGB) von Daten, Computersabotage (§ 303b StGB) sowie Computerbetrug (§ 263a StGB). Solche Delikte können daher als Computer- und Internetdelikte im engeren Sinne verstanden werden.

In der Informatik betrachtet man weniger die Begehungsmodalität sondern eher die Rolle der Technik, wenn es um die Klassifikation von Cyberkriminalität geht (S. Gordon & Ford, 2006). Es können dabei zwei Arten unterschieden werden, nämlich technikorientierte

und menschenorientierte Cyberkriminalität. Technikorientierte Cyberkriminalität besitzt drei typische Charakteristiken:

1. Aus Sicht des Opfers besteht der Schadensvorfall aus einem einzelnen Ereignis.
2. Typischerweise beruht dieses Ereignis auf der Anwendung von Schadsoftware.
3. Die Verwendung von Schadsoftware kann, muss aber nicht, auf Systemschwachstellen beruhen.

In diese Kategorie fallen alle Arten von Phishing, Computersabotage, Datenmanipulation sowie die später noch thematisierten Botnetze. Diese Kategorie korrespondiert daher weitgehend mit der oben genannten Begehungsmodalität des Computers als Angriffsobjekt. Allerdings fallen hierunter teilweise auch Fälle, bei denen ausschließlich die »Schwachstelle Mensch« ausgenutzt wird, etwa bei Angriffen durch *social engineering* (Mitnick & Simon, 2002).

Die zweite Kategorie der menschenorientierten Cyberkriminalität besitzt zwei typische Charakteristika:

1. Es gibt aus Sicht des Opfers in der Regel mehrere, zeitlich aufeinander folgende Ereignisse, wie etwa wiederholte Kontaktaufnahmen zwischen Täter und Opfer.
2. Die Tat beruht auf Software, die man normalerweise nicht als Schadsoftware einstuft, wie beispielsweise Webbrowser oder Instant Messenger.

In diese Kategorie fallen Delikte wie Cyberstalking, bei denen der Täter dem Opfer elektronisch nachstellt, oder etwa auch eBay-Betrug. Diese Kategorie korrespondiert also eher mit der Begehungsmodalität des Computers als Begehungsmittel.

S. Gordon und Ford (2006) geben weitere Beispiele, weisen aber darauf hin, dass es zwischen technik- und menschenorientierter Cyberkriminalität keine klare Trennlinie gibt. Dennoch erscheint die Unterscheidung aus Sicht der Strafverfolgung nützlich, denn die Ermittlungsansätze und daher auch die notwendige fachliche Qualifikation der Ermittlungsakteure sind unterschiedlich: Die Ausbildung vieler Strafverfolger vermittelt traditionell eher diejenige fachliche Qualifikation, die nützlich ist, um mit menschenorientierter Kriminalität umzugehen. In der Praxis spricht man hierbei häufig von »kriminalistischem Gespür«. Genau dies fehlt häufig den in der Informatik ausgebildeten IT-Sicherheitsexperten, die dazu neigen, der technischen Seite eines Delikts mehr oder sogar zu viel Bedeutung zuzumessen. Zur Verfolgung technikorientierter, aber auch menschenorientierter Cyberkriminalität ist es daher erforderlich, die Strafverfolgungsakteure – wenn auch mit unterschiedlicher Gewichtung – sowohl sozial-kriminalistisch als auch technisch-kriminalistisch adäquat auszubilden.

3.4. Zur europastrafrechtlichen Terminologie

Das wegweisende Budapester Übereinkommen über Computerkriminalität aus dem Jahr 2001 (s. noch unten 8.3.1., S. 157) enthält unter anderem Pönalisierungsverpflichtungen betreffend beider soeben aufgezeigter Modalitäten des Computerstrafrechts, aber auch umfangreiche Vorgaben betreffend der transnationalen Durchsetzung dieser und auch weiterer Strafandrohungen. Dies unterstreicht, dass mit den Begriff der Computer- oder Cyberkriminalität ein weites Feld von Konstellationen erfasst werden muss, in denen die Verwendung informationstechnischer Systeme das Strafrecht vor neue Herausforderungen stellt – mithin auch etwa, wenn bloß der verdeckte Zugriff auf ein E-Mail-Postfach erforderlich ist, von dem aus eine Person bedroht wird (krit. M. Gercke & Brunst, 2009, Rdn. 73).

Uneinheitlich ist allerdings die Verwendung der Begriffe im Recht der Europäischen Union: So soll einerseits Computerkriminalität (englisch: *computer crimes*) in Art. 83 Abs. 1 UAbs. 2 AEUV alle Straftaten erfassen, bei denen informationstechnische Systeme Angriffsobjekt oder -mittel sind (Vogel, in Druck, Art. 83 AEUV Rdn. 61); so ist andererseits Cyberkriminalität (englisch: *computer-related crime*) etwa in Art. 2 Abs. 2 des Rahmenbeschlusses über den Europäischen Haftbefehl (AblEG 2002 L 190 v. 17.7.2002, S. 1) historisch und systematisch dahingehend auszulegen, dass nur gegen informationstechnische Systeme gerichtete Straftaten erfasst werden (s. hierzu unten 8.5.3., S. 180).

3.5. Synthese

Im Folgenden sei daher Cyberkriminalität der Oberbegriff für alle Verhaltensweisen, die verfassungsrechtlich legitim unter Strafe gestellt sind oder werden könnten, und die entweder als Angriffsobjekt oder als Begehungsmittel informationstechnische Systeme einsetzen. Das Computerstrafrecht thematisiert dabei alle Aspekte des Straf- und Strafprozessrechts, welche eine Cyberkriminalität betreffende Strafdrohung anordnen und durchzusetzen versuchen.

3.6. Abgrenzung zur Rechtsinformatik, zum Informationsrecht und zum Internetstrafrecht

Abzugrenzen hiervon ist zunächst die Rechtsinformatik, ein Teilgebiet der Informatik, welche sich mit praktischen Anwendungsmöglichkeiten der Informationstechnologie in juristischen Konstellationen (etwa e-Justice) beschäftigt (Hilgendorf et al., 2005, Rdn. 2).

Das Informations-, IT- bzw. Informatikrecht wird teils als Oberbegriff angesehen für alle aus der Informationstechnologie resultierenden Aspekte des Öffentlichen Rechts, des

Zivilrechts und des Strafrechts (Informationsstrafrecht). Letzter Begriff hat sich allerdings in der juristischen Literatur nicht durchsetzen können, kann aber synonym verstanden werden zum hier verwendeten Begriff des Computerstrafrechts.

Für die hiesige Darstellung zu eng ist der Begriff des Internetstrafrechts, welcher sich auf die spezifischen strafrechtlichen Belange des Internets beschränkt und daher nicht oder nur lokal vernetzte informationstechnische Systeme ausklammert, die aber oftmals parallele rechtliche Schwierigkeiten mit sich bringen.

3.7. Zusammenfassung

Die Verbreitung der Informationstechnologie in vielen Lebensbereichen macht es erforderlich, das rechtliche, technische und auch soziale Phänomen der Cyberkriminalität zumindest in dieser Studie weit zu verstehen: Zu diskutieren ist daher nicht nur, was bereits konkret unter Strafe gestellt ist, und wie diese Straftaten ermittelt und verfolgt werden können. Vielmehr ist in einem zweiten Schritt zu fragen, was zusätzlich unter Strafe gestellt werden könnte, um erhebliche sozialschädliche Verhaltensweisen mit den Mitteln des Strafrechts zu verfolgen, und welche Ermittlungsmethoden hierfür bereitgestellt werden könnten. In einem dritten Schritt sind letztlich aber auch die Sinnhaftigkeit, der Nutzen und auch die Risiken bestehender Strafnormen und zukünftiger Veränderungen zu bewerten.

Cyberkriminalität sei daher im Folgenden verstanden als alle sozialethisch erheblich zu missbilligenden, sozialschädlichen Verhaltensweisen, die verfassungskonform unter Strafe gestellt sind oder unter Strafe gestellt werden könnten, und die entweder als Angriffsobjekt oder als Begehungsmittel informationstechnische Systeme einsetzen; Computerstrafrecht als Oberbegriff für alle Aspekte des Straf- und Strafprozessrechts, welche eine Cyberkriminalität betreffende Strafdrohung anordnen und durchzusetzen versuchen.

4. Cyberkriminalität: Verfassungsrecht, Regelungsmodelle und Alternativen

4.1. Einleitung

Der Begriff der Cyberkriminalität knüpft nach hier vertretener Auffassung nicht nur an den bestehenden Strafnormen des Computerstrafrechts an, sondern erfasst auch alle Verhaltensweisen, die in verfassungskonformer Weise legitim unter Strafe gestellt werden könnten. Eng damit verbunden ist sodann erstens die Frage, worin die verfassungsrechtlichen Grenzen des materiellen Computerstrafrechts, also für die Normierung von Straftatbeständen, liegen (4.2.). Zweitens ist zu erörtern, welche rechtlichen Regelungsmodelle zur Steuerung der Cyberkriminalität zur Verfügung stehen, seien es Modelle des Öffentlichen Rechts oder des Zivilrechts (4.3.) oder auch die verschiedenen Regelungsmodelle innerhalb des Strafrechts (4.4.). Drittens seien auch die verfassungsrechtlichen Grenzen für das prozessuale Computerstrafrecht, also für die computerspezifischen Aspekte des Strafprozessrechts, dargestellt (4.5.).

4.2. Verfassungsrechtliche Grenzen für das materielle Computerstrafrecht

Die Frage des materiellen Computerstrafrechts, welche Verhaltensweisen legitimerweise unter Strafe gestellt werden können, korreliert eng mit dem verfassungsrechtlichen und auch rechtstheoretischen und rechtsphilosophischen Verständnis des Strafrechts. Die in Deutschland wohl vorherrschende Strafrechtslehre fußt darauf, dass Strafrecht dem Rechtsgüterschutz und damit einem gänzlich eigenständigem Zweck diene. Europäisch und international überwiegt hingegen eine Sichtweise, dass Strafrecht so etwas besonderes nicht sei, und demnach wie die anderen Bereiche des Rechts unter anderem einer Verhaltensregulierung diene (4.2.1.). Diesen Streit gilt es hier nicht zu lösen. Dennoch ist es für den europäischen und internationalen Diskurs über die Regulierung von Cyberkriminalität wichtig, darauf hinzuweisen, dass selbst unter einem nicht rechtsgutsbezogenen Verständnis des Strafrechts Grenzen für den legitimen Einsatz des Strafrechts bestehen, die sich aus Gesichtspunkten der Verhältnismäßigkeit, des Schuldprinzips und aus speziellen Grundrechten ergeben (4.2.2.).

4.2.1. Dient Strafrecht nur dem Rechtsgüterschutz?

Strafrecht als Rechtsgüterschutz und als *ultima ratio*

Nach der in Deutschland vorherrschenden Strafrechtslehre ist der Einsatz von Strafrecht manchen strengen Beschränkungen unterworfen, die sich aus dem besonderen Wesen

des Strafrechts als dasjenige Mittel ergeben, mit dem der Staat auf härteste Weise in die (Freiheits-)Rechte seiner Bürger eingreift. Hervorzuheben ist insoweit zweierlei:

Erstens richtet sich die Abwägung, ob ein legitimes Ziel zum Einsatz des Strafrechts vorliege, nach einer Trias (vgl.Roxin, 2006, § 2 Rdn. 86 ff. m.w.N.):

1. Zum Schutz von Rechtsgütern mit Verfassungsrang – wie dem Bestand der Bundesrepublik Deutschland, dem Leben, der körperlichen Unversehrtheit, der Freiheit und dem Eigentum der Menschen – sei der Einsatz von Strafbestimmungen unbedenklich.

2. Bei Gütern, die hingegen als bloßer Verwaltungsungehorsam ohne Sozialschädlichkeit des Strafschutzes nicht würdig sind, sei die Rechtsdurchsetzung durch Strafrecht bedenklich.

3. Zwischen diesen Grenzfällen sei der Einsatz des Strafrechts grundsätzlich legitim, wenn ein demokratisch legitimierter Gesetzgeber dies für erforderlich erachtet.

Zweitens muss in besonderer Weise darauf geachtet werden, dass gleich effektive Mittel vorrangig genutzt werden müssen, wenn diese mit weniger einschneidenden Folgen verbunden sind. Daher sei stets nach außerstrafrechtlichen – etwa polizei- und ordnungsrechtlichen – Alternativen zu suchen. Strafrecht ist daher nach dieser Auffassung ausschließlich als subsidiäres Mittel, mithin nur als *ultima ratio* zulässig (Baumann et al., 2003, § 3 Rdn. 19).

Ein gewandeltes Bild vom Strafrecht?

Bereits die Vergangenheit zeigte jedoch, dass die Rechtsgutslehre und der Verweis auf das *ultima ratio*-Prinzip keine wirksame Begrenzung darstellte, welche der Expansion, Subjektivierung, Materialisierung, Ethisierung und sozialen Funktionalisierung des Strafrechts Einhalt hätte gebieten können (zu diesen – ungebrochenen – Entwicklungslinien des Strafrechts vgl. Vogel, 2004, S. 13 ff.). Europäisch und international haben sich diese Konzepte nicht oder nur unzureichend durchgesetzt. Daher ist es jedenfalls bei den europäischen und internationalen Diskussionen über die Regulierung von Cyberkriminalität durch die Mittel des Strafrechts (s. unten 8., S. 155) notwendig, sich über die Rechtsgutslehre hinausgehend Gedanken zu machen über die faktischen Einsatzzwecke des Strafrechts, und über die Begrenzungen, die sich auch abseits der Rechtsgutslehre formulieren lassen.

Daher sei zunächst auf zwei Tendenzen des heutigen Strafrechts hinzuweisen, erstens dem Einsatz des Strafrechts als Vehikel zur Verfolgung strafrechtsfremder Zwecke, und zweitens dem Einsatz des Strafrechts als Mittel zur Verhaltenssteuerung.

Strafrecht als Vehikel zur Verfolgung strafrechtsfremder Zwecke Je mehr man sich vom Kernstrafrecht im engsten Sinne – sprich: Delikten wie Mord und Totschlag – entfernt, desto eher finden sich Konstellationen, in denen das Strafrecht als ein Türöffner verwendet wird: Es dient dann dazu, eigentlich strafrechtsfremde Zwecke zu verfolgen. Das ist bereits in der Zweispurigkeit des strafrechtlichen Rechtsfolgensystems angelegt, das neben Strafen auch die Maßregeln der Besserung und Sicherung kennt, etwa die Verhängung von Berufs- und Fahrverboten sowie von Sicherungsverwahrung. Diese präventiv wirkenden Maßregeln haben in den letzten Jahren an Bedeutung gewonnen, wofür die Ausweitung der Sicherungsverwahrung paradigmatisch zu nennen ist.

Zweitens sei die Vorverlagerung der Strafbarkeit hinterfragt (Herzog, 1991; Završnik, 2010), wie sie typisch ist für ein modernes Risikostrafrecht, das jegliche Risiken von einer Gesellschaft fernzuhalten versucht. Solche Strafnormen wurden nicht nur im Bereich der Terrorismusbekämpfung eingeführt (§§ 89a, 89b StGB), sondern auch im Bereich des Computerstrafrechts (etwa § 202c StGB). Eine solche Vorverlagerung bringt es nun mit sich, dass frühe und leicht nachweisbare Anknüpfungspunkte existieren, auf deren Grundlage einschneidende strafprozessuale Ermittlungsmaßnahmen gestattet sind. Mit Hilfe dieser Ermittlungsmaßnahmen wiederum können sodann Verbrechensstrukturen ermittelt und tatsächliche Schädigungen rechtzeitig verhindert werden. Das Strafrecht dient in solchen Fällen auch als Vehikel zu einer originär polizeirechtlichen, konkreten Gefahrenabwehr.

Drittens aber wird das Strafrecht auch verwendet zur Effektivierung zivilrechtlicher Rechtsdurchsetzung. So ergab sich in der Vergangenheit regelmäßig die Konstellation, dass die Inhaber von Urheberrechten zwar Kenntnis von Urheberrechtsverletzungen hatten, aber den Täter nicht selbst ermitteln konnten. Hierfür war es erforderlich, zunächst Anzeige zu erstatten. Sodann konnten die Strafverfolgungsbehörden über strafprozessuale Eingriffsbefugnisse den Täter ermitteln und den Anzeigeerstatter hierüber informieren. Erst hierdurch konnte der Rechteinhaber auf zivilrechtlichem Wege gegen den Rechtsverletzer vorgehen.[1]

Strafrecht als Mittel zur Verhaltenssteuerung Herkömmlich verweist man als Legitimationsgrundlage für das Strafrecht unter anderem auf die Strafzwecke der Spezial- und Generalprävention, also unter anderem auf die positive Einwirkung auf den Täter und auf potentielle weitere Täter, nicht (erneut) straffällig zu werden. Erst in den letzten Jahren gewachsen ist ein Verständnis dafür, dass Strafrecht darüber hinausgehend verhaltenssteuernde Wirkung entfaltet.

[1] Inzwischen ist diese Prozedur aus drei Gründen von geringerer Bedeutung: Erstens existiert nunmehr ein eigener, problematischer, zivilrechtlicher Auskunftsanspruch in § 101a UrhG, zweitens beschränken restriktive Vorgaben mancher Generalstaatsanwaltschaften die Durchführung entsprechender Strafverfahren und drittens besteht derzeit die faktische Hürde, dass die entsprechenden Verbindungsdaten nur für kurze Zeit vorgehalten werden (zum Zusammenhang mit der Vorratsdatenspeicherung s. unten 7.5.3., S. 149 sowie BVerfGE 125, 260, 271 einerseits, Blankenburg, 2010 andererseits).

Vielbesungen ist daher die Bedeutung des Strafrechts zur Regulierung einer Selbstregulierung, insbesondere im Bereich des Wirtschaftsstrafrechts (*Compliance*, näher Rotsch, 2010; Sieber, 2008). Doch auch darüber hinausgehend dient das Strafrecht der Steuerung von Entscheidungsprozessen (Prozeduralisierung; Eicker, 2010; Eser, 2000; krit. W. Hassemer, 2007): Diese Effekte sind am stärksten, wenn es nicht um affekt- oder triebgesteuerte, sondern um rational oder ökonomisch gesteuerte oder steuerbare Verhaltensweisen der wirtschaftlich oder ökonomisch motivierten Kriminalität geht.

Doch auch in weiteren, sogar alltäglichen Bereichen sind verhaltenssteuernde Wirkungen festzustellen: Menschen versuchen zumeist, sich nicht einmal dem Risiko auszusetzen, dass strafrechtliche Ermittlungen gegen sie geführt werden könnten. Daher vermeiden sie auch legitime und legale Verhaltensweisen, die nur den falschen Eindruck erwecken könnten, es liege eine Straftat vor. Diese Konformität, diese Anpassung ist nur zu verständlich, denn sobald in das Umfeld oder sogar in die Öffentlichkeit dringt, dass ein Ermittlungsverfahren eingeleitet wurde, bedeutet dies nicht selten den sozialen Tod eines Beschuldigten – der Unschuldsvermutung zum Trotz.

Beurteilung Auf den ersten Blick erscheinen diese Ausweitungen des Strafrechts eine höchst bedenkliche Verwässerung und Expansion des Strafrechts. Darüber – und wie sich eine Rechtsgutslehre auch europäisch und international durchsetzen ließe – ist noch viel zu diskutieren. Jedoch sei an dieser Stelle darauf hingewiesen, dass diese modernen Entwicklungen differenzierter und nicht bloß negativ zu bewerten sind:

So ist die strafrechtliche wie keine zweite Rechtsordnung geprägt von Verfahrens- und Verteidigungsrechten, von einer Justizförmigkeit des Verfahrens und einer Sensibilität für die Eingriffe in die (Grund-)Rechte der Betroffenen. Verzichtet man auf ein strafrechtliches Verfahren und versucht dies etwa durch polizei- oder ordnungsrechtliche Mechanismen zu ersetzen, bleibt viel Raum für Kritik: Am evidentesten etwa bei der Inhaftierung von mutmaßlichen islamistischen Gefährdern durch die USA in Guantanamo Bay und anderswo, ebenso bedenklich bei der kompletten wirtschaftlichen Entrechtung durch die Listungsverfahren[2] der UN und der EU (vgl. hierzu Meyer, 2010; Brodowski, 2010c, S. 752), und schließlich auch bedenklich, soweit zur Kontrolle des Bundeskriminalamts, etwa beim Einsatz einer Online-Durchsuchung, das familiengerichtliche Verfahren der freiwilligen Gerichtsbarkeit heranzuziehen ist (§ 20v Abs. 2 S. 2 BKAG).

Auch das geschärfte Bewusstsein für die verhaltenssteuernde Wirkung des Strafrechts kann als eine Chance verstanden werden. Erstens schafft eine Regulierung durch Selbstregulierung Freiräume für eigenverantwortliche, freiheitliche Konzepte, die nur in ihren Grenzen strafrechtlich und damit hoheitlich flankiert werden. Sich selbst organisierende Strukturen eines *Internets der Bürger* und eines *Internets der Zivilgesellschaft* können

[2] Mit diesem Schlagwort beschreibt man, dass mutmaßliche Terroristen auf eine von exekutiven Gremien beschlossene und veröffentlichte Liste gesetzt werden. Sodann sind etwa die Banken verpflichtet, sämtliche Konten aller auf diesen Listen genannter Personen zu sperren.

hier an Stelle staatlicher Regulierung treten, und so staatliche Einflussnahme in weiten Teilen entbehrlich machen. Zweitens – und bedeutender – reicht heutzutage eine Bewertung, ob die Pönalisierung eines konkreten Verhaltens oder eine konkrete strafprozessuale Ermittlungsmaßnahme verhältnismäßig ist, nicht länger aus. Erforderlich ist vielmehr auch eine Bewertung, welche legitime Verhaltensweisen durch eine solche Strafdrohung, oder auch nur durch das Gefühl einer (vollständigen) Überwachung zurückgedrängt werden, und damit zu übertriebener Konformität führen (*Panoptismus*, Foucault, 1994).

Schließlich: Das grundlegende Prinzip der Verhältnismäßigkeit gebietet es bereits, grundsätzlich nach milderen Alternativen zum Strafrecht zu suchen. Strafrecht ist daher nach wie vor – aber eben nur grundsätzlich und nicht in jedem Falle – *ultima ratio*.[3] Das gesteigerte Bewusstsein für die Schärfe des staatlichen Eingriffs, für die Notwendigkeit verfahrensrechtlicher Garantien, und für die verhaltenssteuernden Auswirkungen in der jeweiligen Gesellschaft erfordert zudem einen erhöhten argumentativen Aufwand für den Einsatz des Strafrechts als Regulierungsmittel, anstatt wie bisher – und oftmals zu apodiktisch – dessen Unerlässlichkeit zur Verhinderung sozialschädlichen Verhaltens zu postulieren (s. auch Katz, 2002; Završnik, 2010).

4.2.2. Verhältnismäßigkeit und weitere prinzipielle Begrenzungen

Ausgangspunkt der Begrenzungen eines Straf- und Strafprozessrechts sind – neben der bereits genannten Rechtgutslehre – die Grund- und Menschenrechte, wie sie sich aus dem Grundgesetz, den europäischen Rechtsakten (wie der Charta der Grundrechte [GRC] der Europäischen Union) und der Konvention zum Schutze der Menschenrechte und Grundfreiheiten und auch aus internationalen Rechtsquellen ergeben.

Allerdings stammen diese Grundrechtskataloge aus einer anderen Zeit, in der die Informationstechnologie noch nicht Eingang in nahezu sämtliche Lebensbereiche gefunden hatte. Aufgrund dieser »Weiterentwicklung der Gesellschaft, des sozialen Fortschritts und der wissenschaftlichen und technologischen Entwicklung« (Erwägungsgrund 4 der Präambel der GRC) ist es daher unabdingbar und nach europäischem Verfassungsverständnis auch allgemein anerkannt, dass eine dynamische Weiterentwicklung des Grundrechtsschutzes erfolgen kann und auch muss. Dies kann einerseits interpretativ erfolgen, wozu technisch-funktionale, technikvergleichende und schutzfunktionale Ansätze zur Verfügung stehen (näher Brodowski, 2009, S. 403 f.), oder auch durch eine »Neuschöpfung« von Grundrechten. Daher ist es etwa grundsätzlich zu begrüßen, dass das Bundesverfassungsgericht in seinem wegweisenden Urteil zur »Online-Durchsuchung« informationstechnischer Systeme den durch das Allgemeine Persönlichkeitsrecht bereits gewährleisteten Schutz

[3] So auch explizit die Schlussfolgerungen des Rates der Europäischen Union über Musterbestimmungen als Orientierungspunkte für die Verhandlungen des Rates im Bereich des Strafrechts, Ratsdok. 16542/09.

um ein Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme anreicherte (BVerfGE 120, 274).

Verhältnismäßigkeit, Schuldprinzip, Gleichbehandlungsgrundsatz

Über den verschiedenen, speziellen Grundrechte dominiert im europäischen Rechtsraum das Prinzip der Verhältnismäßigkeit (Ellis, 1999; Klip, 2009, S. 163, 298 f.). Zwar kann man den Einsatz des Strafrechts – auch zur bloßen Verhaltensregulierung – für legitim erachten und im Vergleich zu anderen Regelungsmodellen auch weithin für erforderlich halten. Da jedoch der Einsatz des Strafrecht auch geeignet sein muss, einen (besseren) Schutz zu gewährleisten, bestehen erstens Bedenken gegen den bloß symbolischen Einsatz des Strafrechts (W. Hassemer, 2001), zweitens aber auch gegen eine auf den Strafrahmen fixierte Betrachtungsweise: Entscheidend für die verhaltenssteuernde und präventive Wirkung des Strafrechts ist nämlich mitnichten die abstrakte Strafdrohung (Robinson & Harley, 2003), sondern die von potentiellen Tätern wahrgenommene Wahrscheinlichkeit, zukünftig irgendeiner Strafverfolgung ausgesetzt zu sein (Kshetri, 2006).

Ebenfalls europäisch anerkannt ist das Schuldprinzip, demzufolge eine Strafe nur verhängt werden kann, wenn ein Verhalten dem Täter persönlich vorzuwerfen ist, da er sich nicht für eine (straffreie) Verhaltensalternative entschieden hat (vgl. Ratsdok. 16542/09). So wäre eine Strafnorm unzulässig, die allein darauf abstellte, ob eine Person eine Internetseite mit kinderpornographischem Inhalt betrachtet, selbst wenn diese Person eine solche Seite weder aufrufen wollte noch wusste (Vorsatz) oder damit rechnen musste (Fahrlässigkeit), dass er auf eine entsprechende Internetseite gelangt. Für eine solche so genannte *strict liability*, also allein objektiv begründete Strafdrohung, die auf Vorsatz- oder Fahrlässigkeitserfordernisse verzichtet, ist im deutschen und auch im europäischen Strafrecht kein Platz.

Noch wenig geklärt ist, ob dem Gleichbehandlungsgrundsatz eine beschränkende Wirkung für das materielle Strafrecht zukommt. Jedenfalls in krassen Fällen, in denen eine Strafdrohung nur höchst zufällig und damit ungleich durchgesetzt werden kann, ist dies zu diskutieren (vgl. BVerfGE 110, 94: nur normative Ineffektivität); ansonsten dürfte dies jedenfalls als ein die Eignung des Strafrechts reduzierender Abwägungsfaktor bei der Verhältnismäßigkeitsprüfung zu berücksichtigen sein.

Einzelne Grundrechte

Aus speziellen Grundrechten ergeben sich weitere Vorgaben für das materielle (Computer-)Strafrecht. Von zentraler Bedeutung sind insoweit die in Art. 5 GG gewährleisteten Kommunikationsgrundrechte, aber auch das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme.

Die Kommunikationsgrundrechte schützen nach deutschem Verständnis zunächst nur Meinungsäußerungen. Tatsachenbehauptungen sind nur als Annex hierzu, also weitaus

schwächer verfassungsrechtlich geschützt. Daher kann die Verbreitung von wahren und unwahren Tatsachen in größerem Maße reguliert werden als die Verbreitung von Meinungen. Hieraus ergeben sich international Spannungen, soweit sich Akteure im Internet auf das angloamerikanische, weitergehende und grundsätzlich auch Tatsachenbehauptungen erfassende Grundrecht des *freedom of speech* stützen (s. hierzu unten 8.4.2., S. 167).

Zweitens ist festzuhalten, dass sich die Medienfreiheit auch auf neuartige Medien wie Internetradios, Nachrichtenportale oder Videocasts erstreckt. Im Internet ist dabei der Übergang von einer privaten Meinungsäußerung hin zu einem an die Allgemeinheit gerichteten Angebot fließend: Was gestern noch ein privates Blog war, kann morgen ein umfänglich beachtetes und verlinktes Blog werden, um übermorgen wieder in der Bedeutungslosigkeit zu entschwinden. Dies ist eine der Chancen des Internets, welche eine Unterdrückung missliebiger Meinungsäußerungen erschwert – zugleich aber auch ein Risiko für diejenigen, die durch solche Äußerungen unbillig betroffen werden.

Auch das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme (Hoffmann-Riem, 2008) zeigt Grenzen für das Strafrecht auf: So ist dieses Grundrecht zu berücksichtigen in Diskussionen, die Verschlüsselung von Daten einzuschränken (»obligatorische Entschlüsselungstechnologien« diskutiert etwa Werthebach et al., 2010, S. 131), oder auch bei staatlichen Zugriffen auf Datenbanken, etwa im Rahmen automatisierter Auskunftsverfahren (§ 112 TKG sowie Zugriff auf Fluggastdatensätze), die durch flankierende Ordnungswidrigkeiten- oder Strafbestimmungen gewährleistet werden (vgl. § 149 Abs. 1 Nr. 31, Nr. 32 TKG).

Fazit

Da die genannten Grundrechte jedoch nicht schrankenlos gewährleistet werden, verbleibt ein erheblicher Spielraum für den demokratisch legitimierten Gesetzgeber, zur direkten oder indirekten Verfolgung sozialschädlicher Verhaltensweisen auf das Strafrecht zurückzugreifen. Dieser Beurteilungsspielraum überträgt dem Gesetzgeber allerdings zugleich eine Verantwortung, nicht sämtliche Grenzen des verfassungsrechtlich Möglichen auszuschöpfen und so auch bewusste Entscheidungen hin zur Freiheit zu treffen. Dies ist nicht nur geboten aus Effizienzgesichtspunkten, da der Einsatz des Strafrechts kostspielig ist. Vielmehr ist es die freiheitliche Grundordnung als solche, die nicht durch übermäßige Regulierung angegriffen werden darf, da die Grenze eines solchen schleichenden Prozesses nicht feststellbar ist. Daher ist stets zu erwägen, auf andere, mildere Regulierungsmittel zurückzugreifen, und jedenfalls bei nicht schwerwiegenden, marginalen Beeinträchtigungen zu erwägen, diese bisweilen auch schlicht hinzunehmen – zur Sicherung des hohen Gutes der Freiheit.

Andererseits ist inzwischen anerkannt, dass die Grundrechte nicht nur als Abwehrrechte gegenüber dem Staat wirken, sondern zugleich auch als Schutzpflichten des Staates gegenüber Beeinträchtigungen durch Dritte verstanden werden können. Hieraus können

in besonderen Fällen sogar Pflichten des Staates entstehen, bestimmte Verhaltensweisen unter Strafe zu stellen (so etwa Schwangerschaftsabbrüche, § 218a StGB, vgl. BVerfGE 88, 203). Daher erscheint es wenigstens diskutabel, eine Schutzpflicht des Staates auch gegenüber Angriffen auf den Datenschutz oder die Vertraulichkeit und Integrität informationstechnischer Systeme zu konstruieren. Da entsprechende Strafnormen jedoch existieren, erübrigt sich eine vertiefte Diskussion über diese Frage.

4.3. Ein Wettbewerb der Regelungsmodelle des Zivilrechts, des Polizei- und Ordnungsrechts sowie des Strafrechts

Nachdem soeben dargelegt wurde, wann der Einsatz des (Computer-)Strafrechts verfassungsrechtlich möglich ist und ebenfalls darauf hingewiesen wurde, dass zunächst die Frage zu stellen ist, ob eine Verhaltensweise überhaupt reguliert werden soll, gilt es nunmehr einen Überblick darüber zu geben, wann der Einsatz auch sinnvoll ist, und wann es sinnvoller ist, auf andere Regelungsmechanismen zurückzugreifen. Knapp vorgestellt werden hierzu erstens das Zivilrecht, also das Recht zwischen gleichrangigen natürlichen und juristischen Personen, wie es aus dem Vertragsrecht und dem Schadensersatzrecht auch allgemein bekannt ist, zweitens das Polizei- und Ordnungsrecht, das vom Gedanken der präventiven Gefahrenabwehr dominiert wird, und drittens das Ordnungswidrigkeiten- oder Bußgeldrecht als Zwischenstufe zwischen Ordnungsrecht und Strafrecht. Dabei werden exemplarische Vor- und Nachteile der jeweiligen Regelungsmodelle zur Regulierung von Cyberkriminalität aufgezeigt.

4.3.1. Zivilrechtliche Regelungsmodelle

Die zivilrechtlichen Regelungsmodelle lassen sich nach verschiedenen Typen von Ansprüchen – also von Rechten, von einem anderen ein Tun oder Unterlassen zu verlangen (§ 194 Abs. 1 BGB) – klassifizieren. Die im Zusammenhang mit Cyberkriminalität bedeutsamsten Anspruchsziele sind Leistung, Unterlassung sowie Schadensersatz, ggf. inkl. Schmerzensgeld.

Wesenstypisch für die zivilrechtlichen Regelungsmodelle ist es, dass die Betroffenen – seien es Verkäufer, die (noch) keine Kaufpreiszahlung erhalten haben, seien es Rechteinhaber, deren Urheberrechte verletzt wurden, oder seien es in ihrem allgemeinen Persönlichkeitsrecht Betroffene – einen finanziellen Ausgleich für erlittene Rechtsbeeinträchtigungen erhalten, insoweit also restituiert werden. Das Recht auf Schadensersatz umfasst nach deutschem Verständnis keinen Strafschadensersatz (*punitive damages*), also keine über die Wiedergutmachung hinausgehende, abschreckend wirkende Zahlung an das Opfer. Daher kommt dem Zivilrecht zunächst nur im sehr engen Bereich eines Schmerzensgeldes eine Genugtuungs- und Abschreckungsfunktion zu.

Zudem ist mit einer zivilrechtlichen Verurteilung kein sozialethisches oder moralisches Unwerturteil verbunden. Der Ausgleich erfolgt grundsätzlich auf monetärer Ebene und geht nicht über die Abschöpfung unbillig erlangter Vermögensvorteile, den Ersatz ersparter Aufwendungen und die Erstattung für die Durchsetzung der Rechte erforderlichen Aufwendungen hinaus.

Gerade dieser letzte Aspekt – die Erstattung von Anwalts- und Gerichtskosten des Geschädigten – bedeutet aber in der Praxis für Private eine vergleichbare Rechtsfolge zu einer Geldstrafe: Selbst mit einer Abmahnung ist oftmals eine Kostenforderung von über 1.000 € verbunden, und dies bei einem tatsächlich weit niedrigeren Bearbeitungsaufwand. Auch daher ist die Begrenzung des Erstattungsanspruchs durch § 97a Abs. 2 UrhG bei Urheberrechtsverletzungen außerhalb des geschäftlichen Verkehrs auf maximal 100 € zu begrüßen, wenn sich auch diese Bestimmung in der Praxis noch nicht im erforderlichen Maße durchsetzen konnte.

Nicht zu unterschätzen ist schließlich die weitestgehende Delegation des Rechtsausgleichs auf Private: Die weit überwiegende Zahl zivilrechtlicher Transaktionen gelingt ohne Einsatz staatlicher Zwangsmittel. Nur soweit Verhandlungen zwischen den Parteien scheitern, werden Gerichte mit dem Sachverhalt belastet, und nur soweit der Verurteilte nicht bereit ist, von sich aus die Geldsumme zu bezahlen, wird der Staat im Wege der Zwangsvollstreckung bemüht.

Dennoch ist das Zivilrecht nur ein geeignetes Modell, soweit ein individualisiertes »Opfer« existiert, das sich auf eigene Rechte gegenüber dem »Täter« berufen kann. Hingegen fehlt es etwa bei dem Delikt der Verbreitung (einfach-)pornographischer Schriften (§ 184 StGB) an einem »Opfer«, da konkret schädigende Einflüsse auf einen konkreten Minderjährigen gerade nicht Tatbestandsvoraussetzung dieses Delikts sind. Gleichermaßen ist es schlechterdings unangemessen, die Opfer sexuellen Missbrauchs von Kindern mit der Rechtsdurchsetzung gegenüber Verbreitern derjenigen Schriften zu betrauen, auf denen sie selbst abgebildet sind. Schließlich ist es den Opfern von Computerviren, Trojanischen Pferden etc. in der Regel nicht bekannt, wer diese erstellt und verbreitet hat. Abhilfe ist nur in Randbereichen durch die Einrichtung so genannter Verbandsklagen möglich, wie sie im Gesetz gegen unlauteren Wettbewerb und betreffend Verbraucherschutzvorschriften vorgesehen sind.

Die erheblichsten Schwierigkeiten der zivilrechtlichen Durchsetzung von Rechten im Zusammenhang mit Cyberkriminalität sind jedoch bei der Beibringung der erforderlichen Beweise zu sehen: So mag ein Rechteinhaber zwar erkennen, dass ein Musiktitel in einer Tauschbörse verfügbar ist. Den Anbieter und Abnehmer kann er allerdings in der Regel nicht selbst erkennen, sondern höchstens – und auch das teils nur mit technischen Kniffen – die von diesen verwendeten IP-Adressen. Einen Ausweg bieten hier einerseits zivilrechtliche Auskunftsansprüche, wie sie etwa in § 101a UrhG normiert sind, andererseits der

bereits diskutierte »Umweg« über eine Strafanzeige und spätere Einsichtnahme in die Ermittlungsakten, aus denen sich sodann der Schädiger ergibt.

Die dem Anspruchsinhaber überlassene zivilrechtliche Rechtsdurchsetzung ist auch mit erheblichen Kostenrisiken verbunden: Zunächst sind hier seine eigenen Aufwendungen zu nennen, auch für die Einschaltung von Sachverständigen und Rechtsbeiständen. Sodann hat jeder Kläger einen Vorschuss über die Prozesskosten zu zahlen, die er nur im Falle des Obsiegens und auch nur dann erstattet erhält, wenn der Beklagte zur Zahlung der Gerichtskosten in der Lage ist. Denn die finanzielle Leistungsfähigkeit der Schädiger ist in der Regel begrenzt: Ein 18jähriger Hacker mag zwar dazu in der Lage sein, einen Computervirus zu programmieren und auf diesem Wege Schaden in Millionenhöhe zu verursachen. Allein die Erstattung der Gerichts- und sonstigen Prozesskosten dürfte ihn regelmäßig aber finanziell überfordern, ganz zu schweigen von der Erstattung des eigentlichen Schadens.

4.3.2. Polizei- und ordnungsrechtliche Regelungsmodelle

Das Polizei- und Ordnungsrecht ist von dem Gedanken der Gefahrenabwehr geprägt. Potentiell schädigende Vorgänge sollen erst gar nicht in negativen Folgen münden.

Evidentester Vorteil polizei- und ordnungsrechtlicher Regelungsmodelle ist ihr Eingreifen bereits vor dem Eintritt schädigender Folgen. Werden bereits die Anreize zur Tatbegehung gesenkt – etwa durch eine ordnungsrechtliche Verpflichtung zur Absicherung informationstechnischer Systeme – so mögen damit auch die Angriffshäufigkeit bzw. deren Intensität sinken, und sich daher auch die Notwendigkeit des Einsatzes des Strafrechts reduzieren.

Auf ein konkretes Opfer kommt es im Gegensatz zum Zivilrecht nicht an. Zudem trifft die Opfer kein Risiko, die Kosten der Rechtsverfolgung tragen zu müssen: Der Staat erbringt mit der Gefahrenabwehr eine seiner Kernaufgaben, und dies i.d.R. unentgeltlich oder zu Lasten der Störer.

Am paradigmatischen Zugangserschwerungsgesetz (s. hierzu exemplarisch Sieber, 2009) zeigte sich, wie sehr auch das Ordnungsrecht mit Freiheitseinschränkungen korreliert – *in concreto* mit der Freiheit der Informationsdurchleitung, wie sie auch dem Modell des Telemediengesetzes entspricht (vgl. Sieber, 1999a). Zwar ist auch das Ordnungsrecht selbstverständlich an die freiheitliche Grundordnung und insbesondere an die Grundrechte gebunden. Aufgrund der geringeren Eingriffstiefe verglichen mit dem Einsatz des Strafrechts steht ihm jedoch ein weiteres Feld zur Regulation offen. Mitbetroffen können daher auch an sich legitime, nicht schädigende und nicht schädliche menschliche Verhaltensweisen sein, die zwar nicht unter Strafe gestellt, aber doch ordnungsrechtlich verboten oder verhindert werden. Im Bereich des Polizei- und Ordnungsrechts sind daher in noch stärkerem Maße als im Strafrecht bewusste Wertentscheidungen des Gesetzgebers

erforderlich, inwieweit es gesellschaftlich opportun ist, Freiheitsrechte der Bürger zu beschränken.

Schließlich ist darauf hinzuweisen, dass auch dem Polizei- und Ordnungsrecht kein Strafcharakter immanent ist.

4.3.3. Ordnungswidrigkeitenrechtliche Regelungsmodelle

Das Ordnungswidrigkeitenrecht fungiert als Brücke zwischen dem Ordnungs- und dem Strafrecht. Die formelle Abgrenzung zwischen Straf- und Ordnungswidrigkeitenrecht ist dabei klar: Spricht die Rechtsfolge eines Tatbestands von Freiheitsstrafe oder Geldstrafe, so liegt Strafrecht vor, spricht sie von einer Geldbuße, dann liegt Ordnungswidrigkeitenrecht vor. Materiell bzw. dem Regelungsmodell nach handelt es sich aber um einen im Ausgangspunkt quantitativen, in Teilen auch qualitativen Unterschied. Als Beispiel für Ordnungswidrigkeitenrecht seien die im Straßenverkehr drohenden Bußgelder zu nennen; nur bei den so genannten »Todsünden« im Straßenverkehr droht eine Kriminalstrafe (§§ 315c, 316 StGB).

Ordnungswidrigkeitenrecht ist demzufolge einzusetzen bei Verhaltensweisen, die einen quantitativ geringeren Schuld- und Unrechtsgehalt aufweisen – so bei bloß abstrakter Gefährdung, so bei bloßer Nachlässigkeit oder Unzuverlässigkeit. Strafrecht hingegen zeichnet sich durch eine besonders verwerfliche, grobe oder rücksichtslose Vorgehensweise des Täters aus; es handelt sich um sozial unangepasste, auffällige Verhaltensweisen (Mitsch, 2005, § 3 Rdn. 10). Qualitativ allerdings wird der Unterschied zwischen Strafen und Geldbußen, weil erstere nur gegenüber Menschen, letztere auch gegenüber juristischen Personen verhängt werden können (vgl. etwa § 30 OWiG als Umschaltnorm). Insofern drücken Ordnungswidrigkeiten auch keine Schuld, sondern lediglich Vorwerfbarkeit aus; ihre Blickrichtung ist zumindest im Ausgangspunkt, Verwaltungsunrecht zu erfassen, und nicht – wie das Strafrecht – sozialethisch zu missbilligende Verhaltensweisen.

Zur Verfolgung von Cyberkriminalität werden vor allem zur Absicherung ordnungsrechtlicher Vorschriften Ordnungswidrigkeiten eingesetzt: Zu nennen ist beispielhaft § 43 BDSG, der bestimmte Datenschutzverstöße mit einem Bußgeld belegt; nur wenn zudem der Täter gegen Entgelt oder in Bereicherungs- oder Schädigungsabsicht handelt, wird dies zu einer Straftat qualifiziert wird (§ 44 BDSG).

4.3.4. Fazit

Zivil-, polizei- und ordnungsrechtliche Regelungsmodelle sind stets als Alternativen zu einer strafrechtlichen Regulierung zu erwägen. Insbesondere das Zivilrecht ist aufgrund seiner Restitutionsfunktion – eingetretene Schäden sind finanziell zu kompensieren – und dem finanziellen Strafcharakter der Kostenforderungen bei Abmahnungen durchaus

geeignet, manches wirtschaftlich relevantes Fehlverhalten im Internet ausreichend zu regulieren.

Auch im Lichte der Strafzwecke ist aber in den Fällen, in denen es zu einer evidenten, erheblichen Beeinträchtigung rechtlich geschützter Interessen gekommen ist oder eine ausreichende Prävention durch Mittel des Polizei- und Ordnungsrechts gescheitert ist, eine strafende staatliche Reaktion erforderlich, der individuell und auch generell eine abschreckende Wirkung zukommt.

Jedenfalls bei einer besonders verwerflichen, groben oder rücksichtslosen Vorgehensweise des Täters und bei sozial unangepassten, auffälligen Verhaltensweisen erscheint dabei der Einsatz des Strafrechts als geboten. In vielen Fällen geringerer Rechtsverletzungen, die sich etwa in geringen finanziellen Schäden ausdrücken, ist als Alternative das Ordnungswidrigkeitenrecht im Blick zu behalten, welches in solchen Fällen eine ausreichende Sanktionierung bereithalten kann.

4.4. Strafrechtliche Regelungsmodelle zur Verfolgung der Cyberkriminalität

Welche Regelungsmodelle innerhalb des Strafrechts finden nun nach derzeit geltendem Recht (*de lege lata*) Anwendung; welche Regelungsmodelle werden bei möglichen Änderungen des Strafrechts (*de lege ferenda*) diskutiert? Zunächst zum geltenden Recht:

4.4.1. *de lege lata*

Die Delikte des deutschen Computer- und Internetstrafrechts im engeren Sinne sind im Wesentlichen vorsätzliche Erfolgsdelikte, d.h. sie knüpfen an eine vom Täter verursachte Veränderung in der Außenwelt an (Erfolgsdelikt), wobei der Täter diese Veränderung wollte, von ihr wusste oder diese Veränderung zumindest billigend in Kauf nahm (Vorsatz). Diese vorsätzlichen Erfolgsdelikte zeichnen sich durch eine Irrelevanz der Begehungsmodalität aus, d.h. sie können durch jedwedes Verhalten begangen werden, soweit es nur kausal und zurechenbar den »Erfolg« herbeigeführt hat, sprich das rechtlich geschützte Interesses beeinträchtigt hat. Dieses Modell hat den Vorteil, an einer evidenten Veränderung in der Außenwelt anzuknüpfen und daher den Tatbestand offen formulieren zu können, wie es etwa beim »Abfangen von Daten« geschehen ist (§ 202b StGB).

Ebenfalls handelt es sich *de lege lata* vorrangig um vorsätzliche Verletzungsdelikte, d.h. um Straftatbestände, die den Eintritt eines finanziellen oder sonstigen Schadens voraussetzen. Gleichwohl ist eine Kriminalisierung im Vorfeld möglich, wenn eine konkrete Gefahr geschaffen wird und es bloß noch vom Zufall abhängt, ob ein Schaden eintritt: Wenn ein sozialwidriges Verhalten typischerweise mit erheblichen Risiken verbunden ist und daher allgemein unterbunden werden muss, stehen dem Gesetzgeber daher die

Regelungsmodelle abstrakter und abstrakt-konkreter Gefährdungsdelikte zur Seite. Letzteres ist etwa genutzt bei dem Straftatbestand der Volksverhetzung (§ 130 Abs. 1 StGB), der nur die Eignung zur Störung des öffentlichen Friedens verlangt, nicht aber, dass eine Tat tatsächlich zu Gewalt- oder Willkürmaßnahmen führt: Der Aufforderung wird bereits so großes Gewicht beigemessen, dass schon dieses zu Recht als strafwürdiges Unrecht erfasst wird.

Schließlich nutzte der Gesetzgeber angesichts des Bedrohungspotentials von Schadsoftware auch Gefährdungsdelikte, so zur Pönalisierung von Vorbereitungshandlungen in § 202c StGB, auch i.V.m. §§ 303a Abs. 3, 303b Abs. 5 StGB.

Bei alledem dominieren Vorsatzdelikte das Bild. Dies ist im Lichte der genannten Erwägungen zu den Einsatzvoraussetzungen des Strafrechts zu begrüßen, denn eine Vorsatzverantwortlichkeit wiegt in aller Regel schwerer, und dem § 15 StGB ist durchaus ein Regel-Ausnahme-Verhältnis zu entnehmen, dass Fahrlässigkeit nur ausnahmsweise – und dann i.d.R. bei der Verletzung besonders wertvoller Rechtsgüter wie Leib (§ 229 StGB) oder Leben (§ 222 StGB) – strafbar ist.

4.4.2. *de lege ferenda*

Andererseits aber stehen die bei Cyberkriminalität gegenständlichen Schutzobjekte regelmäßig in besonderer Gefahr, vernachlässigt zu werden – man denke nur an das leichtfertige Unterlassen des Einspielens von Sicherheitsaktualisierungen – und können daher angesichts der damit verknüpften Risikoschaffung gerade in einer modernen »Risikogesellschaft« kritisch betrachtet werden. So verwundert es nicht, dass von mancher Seite bereits gefordert wird, Sicherheitsvorschriften oder eine »Zugangsberechtigung« für die Nutzung von Computertechnologie einzuführen (so genannter »Internet-Führerschein«) und die Durchsetzung durch Mittel des Strafrechts auch abzusichern (Brenner & Clarke, 2005; vgl. auch Kiviat, 2010).

Die Parallelen zu Straßenverkehrsdelikten sind offensichtlich: So ist das Führen eines KFZ ohne Fahrerlaubnis eine Straftat (§ 21 Abs. 1 StVG); so sind abstrakte Gefährdungen (*in concreto* Trunkenheit) im Straßenverkehr eine Straftat (§ 316 StGB); und so sind konkrete Gefährdungen, die durch »Todsünden« im Straßenverkehr entstehen, ebenfalls eine Straftat (§ 315c StGB). Dennoch ist unter Verhältnismäßigkeitsgesichtspunkten Vorsicht geboten: Dort sind abstrakte oder konkrete Gefährdungen von Menschenleben betroffen, hier sind es fast ausschließlich Vermögens- und immaterielle Werte. Infolgedessen wäre aus quantitativen, aber auch aus qualitativen Gesichtspunkten die Einführung mancher der ins Gespräch gebrachten Strafvorschriften im Lichte der freiheitlich-demokratischen Grundordnung höchst bedenklich.

4.5. Verfassungsrecht und das Computerstrafprozessrecht

4.5.1. Grundlagen

Auch die Durchsetzung des Strafrechts durch das rechtsförmige Verfahren des Strafprozesses ist an das Verfassungsrecht gebunden. Dabei begründet das Strafprozessrecht eine besondere Gefahrensituation: In Ermittlungsverfahren tritt der Staat einem Bürger gegenüber, dessen Schuld erst gerichtsfest erwiesen werden muss. Zumeist erfassen verdeckte Ermittlungsmaßnahmen auch unbeteiligte und unschuldige Dritte – wenn etwa ein Verdächtiger mit einer unbeteiligten Person ein Telefonat führt, das heimlich überwacht wird –; zudem werden gelegentlich auch Ermittlungsverfahren gegen Unschuldige geführt, erfreulicherweise aber – auch dies ist festzustellen – selten in missbräuchlicher Weise. Besonders problematisch ist allerdings das in den letzten Jahren vermittelte Gefühl genereller Überwachung, was zu einer Verhaltenseinschränkung auch bei legitimen, aber vielleicht inopportunen Verhaltensweisen führte. All dies erfordert es, auch an dieser Stelle eine dynamische Weiterentwicklung des Grundrechtsschutzes zu betreiben, wobei auch hierfür auf die technisch-funktionalen, technikvergleichenden und schutzfunktionalen Interpretationsansätze (Brodowski, 2009, S. 403 f.) sowie auf die vom Bundesverfassungsgericht gelegentlich vorgenommene »Neuschöpfung« von Grundrechten hinzuweisen ist. Vier Grundrechte – zwei davon entstammen der Feder des Bundesverfassungsgerichts in den letzten drei Jahrzehnten – seien nun knapp vorgestellt:

4.5.2. Einzelne Grundrechte

Brief-, Post- und Fernmeldegeheimnis (Art. 10 GG)

Leitgedanke des Art. 10 GG ist der Schutz von Kommunikation über räumliche Distanzen hinweg. In Zeiten der Globalisierung und der damit zusammenhängenden Tendenz zu (Fern-)Reisen, zu Freundschaften und auch zu Partnerschaften über räumliche Distanzen hinweg gewinnt deren Überbrückung durch vertrauliche und verlässliche Kommunikationswege an erheblicher Bedeutung und erfordert auch einen angemessenen grundrechtlichen Schutz, etwa zur Begrenzung einer Überwachung des Internet-Datenverkehrs einschließlich der Internet-Telefonie.

Der Schutzbereich des Art. 10 GG wird – trotz seines eingeschränkten Wortlauts – auf sämtliche Formen der Telekommunikation ausgedehnt. Zur genaueren Bestimmung des Schutzbereichs bedient sich die Rechtswissenschaft den Legaldefinitionen in § 88 Abs. 1 TKG, § 206 Abs. 5 StGB und erstreckt den Schutz auf den »Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war«.

Umstritten ist allerdings der Beginn und das Ende des Schutzes durch das Telekommunikationsgeheimnis: Die Rechtsprechung und Teile der Literatur stellen darauf ab, ob

der Kommunikationsvorgang den Herrschaftsbereich des Senders verlassen und den des Empfängers noch nicht erreicht habe (BVerfGE 120, 274, 307 f. auch unter Verweis auf BVerfGE 113, 166, 183 ff.; ferner VGH Kassel NJW 2009, 2470, 2471 sowie näher Brodowski, 2009, S. 404). Daher sollen etwa ein E-Mail-Entwurf oder eine auf einem Privatrechner abgespeicherte E-Mail nicht dem Schutzbereich des Art. 10 Abs. 1 GG unterfallen (BVerfGE 124, 43, 54 ff.; BVerfGE 115, 166, 183 ff.; s. ferner Graf, 2010, § 100a StPO Rdn. 27).

Dies zeigt eine Fragmentarisierung des Kommunikationsschutzes und eine unzureichende Berücksichtigung des Umstands, dass sich E-Mails weitaus leichter archivieren und später wieder sichten lassen als in Papierform vorliegende Briefe oder das via Telefon gesprochene Wort. Diesen Gefahren durch die Perpetuierung der Kommunikation begegnet die Rechtsprechung und Rechtswissenschaft nur unzureichend, indem sie sich zum Schutz der Privatsphäre mit einem Rückgriff auf das Allgemeine Persönlichkeitsrecht und dessen spezielle Ausprägungen wie den Grundrechten auf informationelle Selbstbestimmung und auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme bedient (Pagenkopf, 2009, Art. 10 GG Rdn. 10; Sachs & Krings, 2008).

Unverletzlichkeit der Wohnung (Art. 13 GG)

Mit der Unverletzlichkeit der Wohnung soll den Bürgern primär ein »elementarer Lebensraum« (BVerfGE 120, 274, 309) bzw. Rückzugsraum garantiert werden. Durch deren räumliche Abgrenzung wird eine Intim- und Privatsphäre geschaffen, die zur freien Entfaltung der Persönlichkeit unerlässlich ist. Hierzu ist die Wohnung in aller Regel frei von staatlicher Überwachung, aber auch von unzulässiger privater Kontrolle (§ 201a StGB) zu halten. Der Schutzbereich des Art. 13 Abs. 1 GG ist nach der Rechtsprechung des BVerfG die »räumliche Sphäre, in der sich das Privatleben entfaltet«, wobei auch Betriebs- und Geschäftsräume erfasst werden (BVerfGE 120, 274, 309 m.w.N.). Jegliches körperliches Eindringen in diese Sphäre sei vom Schutzbereich erfasst, aber auch die Verwendung von »besonderen Hilfsmitteln …, [um sich] …einen Einblick in Vorgänge innerhalb der Wohnung verschaffen, die der natürlichen Wahrnehmung von außerhalb« entzogen sind (BVerfGE 120, 274, 310). Nach Auffassung des Bundesverfassungsgerichts und von Teilen der Literatur ist aber die Lage eines mit dem Internet verbundenen Rechners innerhalb oder außerhalb einer Wohnung ein bloß zufälliges Merkmal: Zugriffe und Infiltrationen eines Computers könnten über das Internet »unabhängig vom Standort erfolgen, so dass ein raumbezogener Schutz nicht in der Lage ist, die spezifische Gefährdung des informationstechnischen Systems abzuwehren« (BVerfGE 120, 274, 310).

Dies ist aus drei Gründen abzulehnen: Erstens vermittelt die räumliche Abgrenzung einer Wohnung dem Benutzer eines Computers das Gefühl einer Anonymität und der Möglichkeit einer unbeobachteten, schützenswerten freien Entfaltung seiner Persönlichkeit – anders als etwa bei einer Benutzung des Laptops im öffentlichen Raum. Zweitens

ist die zufällige Lage im Raum auch sonst – nur scheinbar ungeeignetes – Kriterium für eine unterschiedliche Betrachtung der Grundrechte: Es mag »Zufall sein, ob der Mörder die Tatwaffe auf der Flucht in einem See versenkt oder später in seiner Wohnung versteckt – grundrechtlich macht es sehr wohl den Unterschied, daß im ersten Fall Polizeitaucher ohne jede richterliche Ermächtigung nach der Waffe suchen können, während im zweiten Fall der Richter das Eindringen in die Wohnung und die Suche nach der Waffe autorisieren muß« (Vogel & Brodowski, 2009, S. 633 Fn. 18)

Drittens: Da in der Öffentlichkeit weit weniger Privatheit und Abgeschiedenheit zu finden ist – Stichworte: Videoüberwachung, Veröffentlichung von Bildern und Videos auf sozialen Netzwerken – gewinnt die Suche nach dem Rückzugsraum einer unverletzlichen Wohnung an Bedeutung. Deren Infiltration durch neuartige Techniken – und wenn es auch »nur« der Festspeicher eines dort befindlichen Computers ist – greift diesen Rückzugsraum an. Wenn auch aus technischer Sicht die »räumliche Sphäre« bei einem vernetzten informationstechnischen System ohne Belang ist, so gilt es aus rechtlicher Sicht auch diese soziale Komponente adäquat zu würdigen.

Schließlich darf in Zeiten der Globalisierung, in Zeiten vermehrter Freundschaften und auch Beziehungen über räumliche Distanzen hinweg die Wohnung als Rückzugs-, Lebens- und Entfaltungsraum nicht isoliert betrachtet werden: Die Telekommunikation zwischen zwei Wohnungen – sei es durch Texte, sei es durch Videos, sei es in »virtuellen Welten« – dient in diesen Fällen auch als (teilweiser) Ersatz oder als Bereicherung für das, was früher allein innerhalb einer Wohnung möglich war. Daher ist zumindest zu diskutieren, ob der Schutz des Fernmeldegrundrechts (Art. 10 Abs. 1 GG) in gewissen Konstellationen durch den Schutz einer funktional zu verstehenden Unverletzlichkeit der Wohnung zu verstärken ist (Schutzbereichsverstärkung; vgl. hierzu Merten, 2009, Rdn. 114 ff.).

Informationelle Selbstbestimmung (Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG)

Das schon länger anerkannte, aber recht unspezifische Allgemeine Persönlichkeitsrecht sichert die Achtung der Persönlichkeit und die Möglichkeit zur freien Entfaltung der Persönlichkeit. Dabei garantiert es einen besonderen Schutz der Intim- und auch der Privatsphäre; geringerer grundrechtlicher Schutz wird der Sozialsphäre zuteil. Bedingt durch die Zunahme elektronischer Datenverarbeitung sah das Bundesverfassungsgericht im so genannten Volkszählungsurteil (BVerfGE 65, 1) die Notwendigkeit, eine spezielle Ausprägung dieses Grundrechts herauszuarbeiten, welches sich dem Datenschutz – genauer: dem Schutz personenbezogener Daten – widmet, das Grundrecht auf informationelle Selbstbestimmung.

Leitgedanke dieses Grundrechts ist es, dass jeder Bürger grundsätzlich selbst entscheiden können muss, wann er Daten über seine Person preisgibt und wie diese Daten verwendet werden dürfen. Andernfalls bestünde nämlich die Gefahr, dass die Bürger sich aus Vorsicht übermäßig konform und angepasst verhalten, mithin sich nur unzureichend frei

entfalten und sich auch nur unzureichend am freiheitlich-demokratischen Gemeinwesen beteiligen (vgl. BVerfGE 65, 1, 43). Relevanz gewinnt dieses Grundrecht bei jeglichen Datenerhebungen und -verwendungen durch Strafverfolgungsbehörden, wobei es aber zumeist von spezielleren Grundrechten – wie insbesondere dem Fernmeldegrundrecht – verdrängt wird.

Das Grundrecht auf informationelle Selbstbestimmung ist in heutiger Zeit unterschätzt: Zu freigiebig geben Bürger – gerade Kinder und Jugendliche – im Internet und gegenüber Unternehmen, etwa durch Kundenkarten, personenbezogene Daten preis, ohne sich der Bedrohungslage bewusst zu sein, der sie sich hierdurch aussetzen. Missbrauchsszenarien sind leider nicht nur theoretischer Natur. Dabei ist es müßig, darüber zu diskutieren, ob die derzeit gefährlichere Bedrohung durch Private (»Datenkraken«) oder aber durch staatliche Stellen vorliegt, die vermehrt untereinander Daten austauschen (»Prinzip der Verfügbarkeit« statt »Zweckbindung der Daten«). Da Grundrechte auch eine objektive Werteordnung vorgeben und Grundrechte als Leitfunktion für das private und wirtschaftliche Miteinander dienen, muss sich der Staat seiner gesellschaftsprägenden Verantwortung bewusst werden und mit dem guten Beispiel einer Zurückhaltung bei Datenerhebungen vorangehen.

Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG)

Während das Grundrecht auf informationelle Selbstbestimmung dem Schutz vor übermäßiger Nutzung von Informationstechnologie durch Dritte und insbesondere dem Staat dient (»externer Datenschutz«), so dient das neue Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme dem Schutz der eigenen Nutzung von Informationstechnologie (»interner Datenschutz«; s. auch Hoffmann-Riem, 2008). Aufgrund der vermehrten Nutzung von Informationstechnologie durch Private und durch Unternehmen, aber auch aufgrund eines erhöhten Bedrohungspotentials durch die Vernetzung der Informationstechnologie und daraus resultierender technischer Angriffsszenarien, hielt es das Bundesverfassungsgericht auch hier für geboten, eine weitere, spezielle Ausprägung des Allgemeinen Persönlichkeitsrechts herauszuarbeiten (BVerfGE 120, 274). Diesem Grundrecht kommt zwar rechtlich lediglich eine subsidiäre Bedeutung zu, soweit nicht der Schutzbereich eines spezielleren Grundrecht eröffnet ist, wie etwa das Fernmeldegrundrecht oder die Unverletzlichkeit der Wohnung. Ferner wird diesem Grundrecht (wie auch dem Grundrecht auf informationelle Selbstbestimmung) vorgeworfen, dass es von dem Bundesverfassungsgericht quasi aus dem Nichts kreiert wurde. Dennoch ist die durch dieses neue Grundrecht verkörperte Wertentscheidung positiv zu würdigen.

Der Schutzbereich ist nur eröffnet bei informationstechnischen Systemen oder Netzen, die »personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges

Bild der Persönlichkeit zu erhalten« (BVerfGE 120, 274, 314). Paradigmatisches Beispiel hierfür sind Arbeitsplatzrechner, aber auch Laptops und sogar Smartphones. Da mit einer Beeinträchtigung der Integrität eines solchen Systems »die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen« ist, genießt auch diese grundrechtlichen Schutz.

Bezüglich Eingriffe für präventive Zwecke sind der Rechtsprechung des Bundesverfassungsgerichts detaillierte Vorgaben für eine »Online-Durchsuchung« zu entnehmen, die etwa einen präventiven Richtervorbehalt oder auch eine Beschränkung auf Gefahren für überragend wichtige Rechtsgüter vorsehen. Das Urteil des Bundesverfassungsgerichts verhält sich allerdings nur am Rande zu den Eingriffsvoraussetzungen für eine strafprozessuale »Online-Durchsuchung«. Hier ist daher noch manches ungeklärt, was unten 7.5.4., S. 150 vertiefter Analyse bedarf.

4.5.3. Fazit

Die verfassungsrechtliche Adaption der Grundrechte an die Herausforderungen, die sich aus der Verbreitung und Verwendung der Informationstechnologie ergeben, bereitet erhebliche Schwierigkeiten: So gewinnen neuartige Bedrohungsszenarien – etwa eines *data mining*, also einer Verknüpfung verschiedenster Datenquellen, auch durch Private – an Bedeutung, und so sind neuartige Kommunikationsformen nicht ohne Weiteres mit klassischen Verhaltensmustern adäquat zu erfassen. Eine zu punktuelle Betrachtungsweise führt dazu, dass erhebliche Schutzlücken entstehen können, was etwa zu einem Gefühl der Überwachung, zu einer Anpassung des Verhaltens und zu einem Verzicht auf Teilhabe am demokratischen Meinungsaustausch führen kann. Statt dessen ist bei besonderer Schutzbedürftigkeit und -würdigkeit bestimmter Verhaltensformen (etwa: Kommunikation in der Familie oder mit engen Freunden, das Schreiben eines Tagebuchs, politische Meinungsäußerungen) darauf zu achten, dass ein umfassender und alle Facetten abdeckender grundrechtlicher Schutz gewährleistet wird.

Andererseits aber darf das Internet nicht idealisiert werden und dem Internet und der Informationstechnologie auch kein rechtsfreier Raum zugestanden werden, da dies mit der friedensstiftenden und ordnenden Funktion des Staates unvereinbar wäre. Bei dem Ausgleich dieser widerstreitenden Interessen darf schließlich nicht übersehen werden, dass weniger die betroffenen Grundrechte entscheidend sind als die zu gewährleistenden rechtlichen Schutzstandards, wie sie sich aus einer abstrakten Bewertung und Typisierung als Ausprägung des grundlegenden Prinzips der Verhältnismäßigkeit ergeben (vgl. zu alledem Brodowski, 2009, S. 402 ff. m.w.N.)

4.6. Zusammenfassung

Es ist zu beobachten, dass das Strafrecht auch im Bereich der Cyberkriminalität als Vehikel zur Durchsetzung strafrechtsfremder Zwecke und als Mittel zur Verhaltenssteuerung eingesetzt wird. Das ist Risiko und Chance zugleich: Es ist ein Risiko, dass durch die Kriminalisierung von nicht oder nur marginal sozialschädlichen Verhaltensweisen auch legitime Verhaltensweisen und damit die Freiheit der Bürger beschnitten wird. Es ist aber zugleich eine Chance, denn ein gesteigertes Bewusstsein für die Verhaltensbeeinflussung durch Strafrecht fordert zugleich eine vertiefte Prüfung, ob der Nutzen einer Strafdrohung oder einer Ermittlungsmaßnahme überwiegt, oder ob die möglichen Nebenfolgen – Konformität, verminderte Nutzung von anonymen Beratungsdiensten, verminderte politische Teilhabe usw. – zu unerwünschten, größeren Schäden für die Gesellschaft führt.

Bei dieser Beurteilung ist auch zu berücksichtigen, dass unterschiedliche Gesellschaften auch unterschiedliche Kriminaljustizsysteme und damit auch unterschiedliche Straftatbestände und Ermittlungsbefugnisse erfordern. So mag man einerseits eine (vermeintliche) deutsche Zurückhaltung beim Einsatz des Strafrechts kritisieren, so muss man aber andererseits berücksichtigen, dass neben der Frage des *law in the books* auch die Frage des *law in the street* tritt: Wie gründlich werden die Normen hierzulande und anderswo praktisch umgesetzt und angewendet? Wie viele Ressourcen stehen zur Strafverfolgung zur Verfügung? Welche konkreten Auswirkungen sind in einer bestimmten Gesellschaft durch das Phänomen überzogener Konformität zu befürchten? All diese Fragestellungen sind relative, und erfordern weit mehr interdisziplinäre Expertise, als ihnen derzeit zuteil wird.

Strafrecht ist aber nur eines von mehreren Regelungsmodellen, das zur Regulierung des Internets und zur Regulierung von Cyberkriminalität zur Verfügung steht. Für bestimmte Konstellationen – etwa Urheberrechtsverletzungen zum eigenen Gebrauch und in geringem Umfang – können zivil-, ordnungs- und bußgeldrechtliche Maßnahmen unter Umständen eine ausreichende, verhältnismäßige und effektive Alternative darstellen, die den auch kostspieligen Einsatz des Strafrechts verzichtbar machen.

Schließlich sind die verfassungsrechtlichen Grenzen an das Strafrecht und an das Strafprozessrecht zu berücksichtigen: Diese reichen vom überragenden Prinzip der Verhältnismäßigkeit über die einzelnen Grundrechte – etwa die Meinungsäußerungs- und Medienfreiheit in Art. 5 GG oder das Fernmeldegeheimnis des Art. 10 GG – hin zum Schuldprinzip, demzufolge nur persönlich vorwerfbares Verhalten zu einer strafrechtlichen Reaktion führen darf. Hingegen ist kritisch zu hinterfragen, ob die als weitere Einschränkung des Strafrechts verstandene, in Deutschland vorherrschende Rechtsgutslehre sich auch europäisch und international durchsetzen lässt und ob sie eine zukunftsweisende, wirksame Begrenzung für die Expansion des Strafrechts darstellt. Entscheidend sind aber ohnehin nicht die verfassungsrechtlichen und rechtstheoretischen Grundlagen, sondern die daraus

resultierenden Schutzstandards: Diese dürfen einerseits weder fragmentarisch noch unzureichend sein, andererseits aber muss sämtlicher verfassungsrechtlicher (Daten-)Schutz auch ausreichende Zugriffsmöglichkeiten für eine effektive Strafverfolgung belassen.

5. Von klassischer Kriminalität zur Cyberkriminalität

5.1. Einleitung

Die Geschichte der Kriminalität ist so alt wir die Geschichte der Menschheit. So gab es auch schon vor der Entstehung des Internets viele Kriminalitätsformen, die heute und in Zukunft andauern. Mit der Verlagerung vieler Aktivitäten in den Cyberspace verlagert man zwangsläufig alle mit diesen Aktivitäten einhergehenden Delikte auch dorthin. So ist es kein Wunder, dass es alles, was es ohne das Internet gab, etwa Betrug, Beleidigung oder Erpressung, nun auch im Internet gibt. Wie wir aber in Kapitel 2., S. 15 gesehen haben, existieren im Cyberspace jedoch andere Rahmenbedingungen als in der realen Welt. Diese werden durch die folgenden fünf Schlagworte charakterisiert (s. hierzu auch M. Gercke, 2008):

- Automatisierbarkeit: Im Cyberspace kann man Aktivitäten programmieren und durch Computer ausführen lassen. Ein konstanter Aufwand kann durch massenhafte Ausführung ein Vielfaches an Wirkung erzielen.
- Flüchtigkeit: Im Gegensatz zu den archetypisch greifbaren und beständigen körperlichen Sachen sind Computerdaten regelmäßig flüchtig. Spuren verwischen so schneller als in der realen Welt.
- Räumliche Entgrenzung: Virtualisierung und Vernetzung führen dazu, dass programmierte Handlungen unabhängig vom realen Ort durchgeführt werden können. Prinzipiell sind nur der Ein- und Ausstiegspunkt einer Aktivität in den Cyberspace lokalisierbar, alles andere nicht.
- Kopierbarkeit: Beliebige Artefakte können im Cyberspace perfekt kopiert werden, also auch Authentifizierungsinformationen. Wird also eine Aktivität in den Cyberspace verlagert, kann man sie innerhalb des Cyberspace nicht mehr zweifelsfrei einer realen Identität zuordnen.
- Angreifbarkeit: IT-Systeme enthalten Schwachstellen, die von Angreifern ausgenutzt werden können, um schädliches Verhalten des IT-Systems zu erzeugen.

Diese veränderten Rahmenbedingungen schaffen vor allem in Verbindung mit ökonomisch motivierter krimineller Energie neue Probleme, die wir in diesem Kapitel betrachten wollen. Unsere Ausführungen sollen zeigen, dass es in der Tat Bereiche der Cyberkriminalität gibt, die spezifisch »cyber« sind, in denen also ein Handlungsbedarf entsteht und die mit spezifischen technischen und juristischen Mitteln verfolgt werden müssen. Für alles andere sollten die Schutzmöglichkeiten in Betracht gezogen werden, die bereits ohne das Internet erfolgreich zur Anwendung kamen. Dieses Kapitel betrachtet darum zunächst

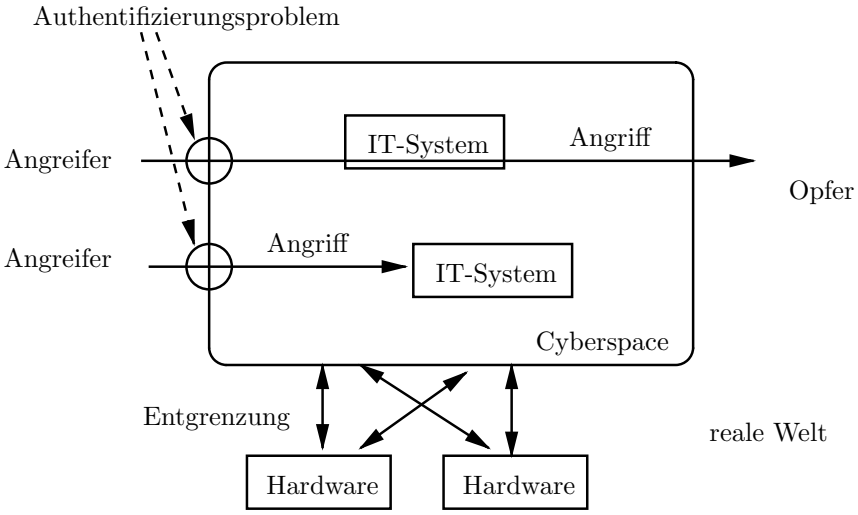

Abbildung 5.1: Auswirkungen der Informationstechnologie auf die Kriminalität im Cyberspace.

die Herausforderungen, die durch die veränderten Rahmenbedingungen entstehen (5.2.) und gibt anschließend einen Überblick über die drei wesentlichen Entwicklungslinien der Cyberkriminalität und ihrer strafrechtlicher Erfassung (5.3.). Kapitel 6., S. 63 wird dann im Anschluss die konkreten Begehungsformen moderner Cyberkriminalität illustrieren.

5.2. Herausforderungen

Der Cyberspace ist ein großer und komplexer digitaler Raum, der in unsere reale Welt eingebettet ist. Die im Cyberspace agierenden Personen stehen am Rand dieses Raums und interagieren durch diesen Raum hindurch miteinander. Die sozialschädigenden Effekte der Kriminalität entstehen notwendigerweise in der realen Welt, so dass der Beziehung zwischen den handelnden Personen (Tätern, Opfern, Ermittlern) eine zentrale Bedeutung zukommt. Abbildung 5.1 stellt die Zusammenhänge schematisch dar. Sie soll im Folgenden auch dazu dienen, die Herausforderungen aufzuzeigen, denen sich die IT-Sicherheit und das Computerstrafrecht gegenüber sieht.

5.2.1. Probleme bei der Identifizierung handelnder Personen

Egal ob ein IT-System als Ziel oder Werkzeug einer Straftat verwendet wird, ist es unter den gegebenen Rahmenbedingungen des Cyberspace deutlich schwieriger als in der realen Welt, die Ursache einer Systemaktivität zurück zu verfolgen. Dies beruht auf den vielen »Indirektionen«, die im Cyberspace auf einfache Art und Weise aufgebaut werden können, um Aktivitäten zu verschleiern.

Die erste Indirektion existiert an der Grenze zwischen Cyberspace und der realen Welt (siehe Abbildung 5.1) und wird vielfach als *Anonymität* wahrgenommen (zur juristischen

Diskussion siehe etwa Brunst, 2009b; M. Gercke & Brunst, 2009, Rdn. 22 f.; Hilgendorf et al., 2005, Rdn. 340). Die im Cyberspace verwendeten Identitäten, wie etwa E-Mail-Adressen oder Namen in Diskussionsforen, müssen in keinem Zusammenhang stehen mit der realen Identität eines Benutzers. Zwar besteht bei der Vergabe von Zugangskennungen in Organisationen wie Unternehmen, Behörden oder Hochschulen eine oft erkennbare Verbindung, wenn etwa die E-Mail-Adresse aus dem Vornamen und dem Nachnamen der Person zusammengesetzt wird. Im privaten Bereich, wenn man etwa eine E-Mail-Adresse bei einem Diensteanbieter registriert, ist dies regelmäßig ohne Nachweis der Legitimation möglich. Ähnlich gestaltet es sich bei der Verwendung von frei zugänglichen Netzzugangspunkten wie Internetcafes oder fremden, ungesicherten WLAN-Zugängen.

Problematisch wirken hier zusätzlich die Probleme, die durch die Kopierbarkeit im Cyberspace entstehen. Anders als eine handschriftliche Unterschrift, die per Definition nur die betreffende Person selbst leisten kann, ist die Zuordnung einer Aktivität zu einer konkreten Person in der Regel sehr schwierig, da die Authentifizierungsinformationen wie Passwort oder PIN leicht weitergegeben werden können. Im Cyberspace ist es folglich viel einfacher, die Identität einer anderen Person anzunehmen, als in der realen Welt, was sich im Phänomen des massenhaften Identitätsdiebstahls manifestiert. Begünstigt wird dies durch die Unachtsamkeit vieler Nutzer und die Möglichkeit, durch automatisierte Verfahren deren Zugangsdaten auszuspähen, etwa beim Phishing.

Zunehmend versucht man, das Phänomen des Identitätsdiebstahls durch die Bindung der Authentifikationsinformationen an Hardware wie eine Chipkarte einzudämmen. Dabei ist es allerdings wichtig, dass diese Informationen durch die Hardware »geschützt« gespeichert werden, also nicht ohne weiteres auslesbar sind. Diese Bindung ist etwa bislang bei Kredit- oder EC-Karten nicht gegeben, was sich im Phänomen des Skimming äußert.[1] Sind die Authentifikationsinformationen innerhalb der Hardware verborgen, so kann man eine Zugangskennung mit derjenigen Person in Verbindung bringen, die sich im Besitz der Hardware befindet. Dies ist ein erster wichtiger Schritt bei der Zuordenbarkeit einer digitalen Handlung zu einer realen Person. Beispiele für entsprechende Technologien sind viele Chipkarten im Bereich des Online-Banking (das so genannte Chip-TAN-Verfahren) und der neue elektronische Personalausweis.

Ähnlich zu bewerten ist die Identifizierung eines Anschlussinhabers, etwa bei der Auflösung einer IP-Adresse. Allerdings erschweren auch bei der Auflösung von IP-Adressen wieder andere Effekte die Identifizierung. Im Cyberspace können beliebige Systemaktivitäten programmiert werden. Statt einer Person kann also auch eine Maschine als Aktivitätsträger auftreten. Dies geschieht etwa bei der Verwendung von Re-Mailern, Web-Proxies oder Anonymisierungsdiensten wie AnON oder TOR (Dingledine et al.,

[1] Bei deutschen EC-Karten gibt es zwar ein Merkmal, was die Karteninformationen an die Karte selbst bindet (*moduliertes Merkmal*). Um auch im Ausland Geld abheben zu können, enthalten die Karten allerdings zudem einen leicht auslesbaren Magnetstreifen.

2004; Köpsell et al., 2003). Bei unzureichend gesicherten Kommunikationsverbindungen besteht dadurch auch die Gefahr von Angriffen durch zwischengeschaltete Mittelsmänner, so genannte »man in the middle«-Angriffe. Hierbei gibt eine dazwischen geschaltete Maschine beiden Kommunikationspartnern wechselseitig vor, dass sie sich mit dem jeweils anderen unterhalten. Tatsächlich sitzt die Maschine zwischen den Kommunikationspartnern und leitet die Nachrichten weiter. Dabei kann sie die Inhalte mitlesen und unter Umständen auch verändern. Dies passiert etwa bei Schadprogrammen, die Transaktionen beim Online-Banking auf dem Rechner des Benutzers manipulieren, bevor diese an die Bank weitergeleitet werden (Holz, Engelberth & Freiling, 2009). Ähnlich funktioniert auch die so genannte »Quellen-Telekommunikationsüberwachung«, bei der sich ein Überwachungsprogramm zwischen das Mikrophon und die Software schaltet, die die Sprachsignale verschlüsselt. Diese Angriffe sind besonders tückisch, da es für sie in der realen Welt kaum Analogien gibt.

Die Verwendung von biometrischen Technologien löst die Probleme nur bedingt. Einerseits müssen die Erkennungsalgorithmen hinreichend robust sein, um eine eindeutige Identifizierung von Personen zu gewährleisten. Andererseits muss sichergestellt werden, dass die verwendete Technologie es nicht erlaubt, über Mittelsmänner oder durch die digitale Einspielung von biometrischen Informationen angegriffen zu werden. So kursierte kürzlich im Internet der digitale Fingerabdruck des ehemaligen deutschen Innenministers (Chaos Computer Club, 2008).

5.2.2. Inhärente Transnationalität

Die Probleme an den Systemgrenzen setzen sich innerhalb des Systems fort. Dabei spielt die räumliche Entgrenzung des Cyberspace eine wesentliche Rolle, also die Abkopplung des Cyberspace vom geographischen Ausführungsort (siehe Abbildung 5.1). Die nationalen Grenzen spielen bei der Übertragung von Daten heute kaum eine Rolle. Wie oben erwähnt, ist jeder eines jeden Nachbarn. Die räumliche Entgrenzung der Computertechnologie stellt seit jeher ein handfestes Problem für die transnationale Strafdurchsetzung dar. Einerseits betrifft dies Diskrepanzen der jeweils geltenden Strafgesetze, Grundrechte und Grundwertungen am Handlungs- und Erfolgsort, am Ergreifungs- und Verfolgungsort. Andererseits aber sind auch die rechtlichen Schwierigkeiten der Beweissicherung, -erhebung und des Beweistransfers aus Sicht der Ermittlungsbehörden (M. Gercke & Brunst, 2009, Rdn. 31) und die Gefahren von Parallelermittlungen (*shadow proceedings*, *forum shopping*) zu diskutieren (M. Gercke & Brunst, 2009, Rdn. 40 ff.).

Aufgrund dieser Besonderheiten, aber auch aufgrund der sozialen Struktur der Meinungsführer in der Informationstechnologie ist dem Computerstrafrecht sowie dem Informationsrecht generell ein Drang nach Selbständigkeit, Autonomie und größtmöglicher Freiheit anheim. Ein autonomes, internationales Recht *sui generis* hat sich aber bislang nicht

durchsetzen können; allein gibt es einen technischen (Minimal-)Konsens, der ohnehin notwendig ist, um überhaupt mittels des Internets kommunizieren zu können.

Zu diesem Drang nach der Freiheit eines neuen Mediums kann man eine historische Parallele zur Freiheit der Meere ziehen. Verfochten die ursprünglichen Seegroßmächte Spanien und Portugal zunächst, dass allein sie Herrschaftsgewalt über sämtliche Ozeane haben, hat sich – auf höchst differenzierte Begründungsansätze aufbauend (vgl. Vitzthum, 2007, 5. Abschn. I 4 b Rdn. 62) – der Grundsatz der internationalen, staatsfernen hohen See herausgebildet. Freilich: sämtliche Zugangspunkte hierzu (Häfen, Küsten) unterliegen staatlicher Kontrolle. Alle Staaten dürfen ihre jeweilige Strafgewalt ausdehnen auf Delikte, die ihre Staatsangehörige auf hoher See begehen oder gegen diese dort begangen wird; Piraterie betrifft die Staatengemeinschaft als Ganze und darf daher von jedem Staat, selbst ohne besonderen völkerrechtlichen Anknüpfungspunkt, auch strafrechtlich verfolgt werden.

5.2.3. Größe, Geschwindigkeit, Entwicklungsdynamik

Die dynamische, weltweite Entwicklung und Verbreitung der Computertechnologie erzeugt zusätzliche Herausforderungen. Zum einen sind dies technische Herausforderungen, die aus der Geschwindigkeit und Flüchtigkeit der Technologie herrühren. Zum anderen sind die Herausforderungen gesellschaftlicher Natur.

Im Gegensatz zu körperlichen Sachen sind Computerdaten regelmäßig flüchtig. So hinterlässt etwa ein Chat regelmäßig keine Daten auf Festspeichern und auch der Versand einer E-Mail hinterlässt nicht notwendigerweise Spuren auf einem Rechner. Verschlüsselt auf einem Festspeicher abgelegte Daten sind regelmäßig nur vorübergehend im Arbeitsspeicher eines informationstechnischen Systems entschlüsselt verfügbar, der nach Unterbrechung der Stromzufuhr oder jedenfalls nach dem Überschreiben nicht oder nur selten wiederhergestellt werden kann. Dies führt regelmäßig zu Problemen bei der Spurensicherung durch die Ermittlungsbehörden.

Als gegenläufige Strömung ist aus technischer Sicht auch ein umgekehrtes Phänomen zu beobachten, nämlich die massenhafte Ansammlung von Daten auf Datenspeichern. Im privaten Bereich ist es beispielsweise kaum mehr nötig, Dateien, Bilder oder E-Mails zu löschen, weil die Kapazität von Festplatten stetig zunimmt. Außerdem werden bei der individuellen Anpassung von Software, etwa bei der Wahl der persönlichen Benutzungspräferenzen, zahlreiche Einstellungen vorgenommen, die persistent gespeichert werden. Aus vielfältigen Gründen wird heute auch vielfach das Verhalten von Benutzern protokolliert, beispielsweise bei der Benutzung von Firmenrechnern, beim Surfen im Internet (durch das Verfolgen von Cookies; s. Steidle & Pordesch, 2008) oder im Rahmen der Beteiligung an sozialen Netzwerken. Schließlich benötigen Suchmaschinen wie Google oder Bing riesige Datenspeicher, um einen einfachen Zugang zu den Informationsressourcen

im Netz zu bieten. Die gespeicherten Datenmengen übersteigen mittlerweile mutmaßlich alles, was jemals in nicht-digitaler Form gespeichert wurde. Eine neue Qualität erreicht diese Datenmenge aber aus der Möglichkeit, die gespeicherten Daten automatisiert zu Verarbeiten. So können große Textmengen in Sekundenbruchteilen nach Schlüsselwörtern durchsucht werden, und es ist bekannt, dass Nachrichtendienste einen Großteil des Netzwerkverkehrs im Internet automatisiert hinsichtlich bestimmter IP-Adressen, Begriffe oder Zahlenkombinationen wie Telefonnummern analysieren (Bamford, 2002).

Die Verarbeitungsgeschwindigkeit der Computertechnologie birgt insbesondere in Verbindung mit der Kopierbarkeit digitaler Information auch noch andere Herausforderungen. Manipulationen von Finanztransaktionen können bereits binnen weniger Millisekunden zu erheblichen Schäden führen. Datenmengen sind innerhalb weniger Sekunden über Ländergrenzen hinweg zu schaffen und können so schnell dem Zugriff von Strafverfolgungsbehörden entzogen werden. Umgekehrt bieten diese Umstände auch den Nährboden für Plattformen wie WikiLeaks, die darauf basieren, dass man in einfacher Weise und in großen Mengen Daten dem Herrschaftsbereich seiner rechtmäßigen Besitzer entziehen kann. Rechtswidrige Inhalte und urheberrechtlich geschützte Werke können ebenfalls in kürzester Zeit an ein großes Publikum verbreitet werden (M. Gercke & Brunst, 2009, Rdn. 18). Hinzu treten auch die Schnelligkeit der Weiterentwicklung der Computertechnologie und die damit verbundenen technischen wie rechtlichen Schwierigkeiten für Ermittlungsbehörden, hiermit Schritt zu halten.

Die Automatisierbarkeit und die weltweite Vernetzung führt zu Massenphänomenen und Multiplikatoreffekten, die durch das Internet erst ermöglicht werden oder eine gänzlich neue Bedeutung gewinnen. Eines der bekanntesten Beispiele ist der massenhafte Versand von unerwünschten E-Mails (Spam). Aber auch der massenhafte parallele Zugriff auf eine Website ist problematisch. Dabei ist unerheblich, ob dies durch unabhängige Benutzer geschieht, wie etwa bei der Online-Vergabe der Eintrittskarten zur Fußballweltmeisterschaft 2006, oder durch eine koordinierte Aktivität eines einzigen Cyberkriminellen, etwa durch Nutzung von Tausenden von kompromittierten Rechnern in Form eines »Botnetzes«. Analog sind die Betrugsmaschen, die pro Transaktion einen unscheinbaren Geldbetrag bewegen (beispielsweise den Bruchteil eines Cents) und erst in der millionenfachen Ausführung einen bemerkbaren Schaden erzeugen.

Durch einen einzelnen Eintrag auf einem viel gelesenen Blog kann eine Person aus der Anonymität geholt und zum »Star«, aber auch zum Opfer der öffentlichen Aufmerksamkeit werden. Andererseits aber verschafft das Internet vielen die Möglichkeit, sich selbst zum Urheber, Multiplikator oder Meinungsmacher zu erheben und dabei selbständig gestaltend tätig zu werden.

5.2.4. Ubiquität und Expansion

Das Internet wird inzwischen von über eineinhalb Milliarden Menschen genutzt, weitere Formen der Computer- und Informationstechnologie dürften die Reichweite des Cyberspace und auch der Cyberkriminalität noch erhöhen. Ein Internetzugang genügt, um – z.T. auch ohne vertieftes technisches Wissen – eine Computerstraftat zu begehen, und um an weitere Tatwerkzeuge wie Spezialsoftware zu gelangen (M. Gercke & Brunst, 2009, Rdn. 16). Auch angesichts der Abhängigkeit der Informationsgesellschaft von der IT-Infrastruktur ist daher von einer ubiquitären Bedrohungslage auszugehen. Hinzu tritt eine Expansion der im Internet verfügbaren Daten und der über das Internet vorgenommenen Datenübertragungen, welche die effektive Verfolgung von Cyberkriminalität erschweren (M. Gercke & Brunst, 2009, Rdn. 38 f.). Die Automatisierung der Erkennung rechtswidriger Inhalte und auch die personelle Ausstattung der Strafverfolgungsbehörden und deren Ausbildung haben mit dieser Entwicklung bislang nicht Schritt halten können.

5.2.5. Fragile Technologien

Schließlich muss man immer wieder feststellen, dass moderne informationstechnische Systeme zum überwiegenden Teil noch recht fragil sind. Dies äußert sich nicht nur in der (Un)Zuverlässigkeit der Hardware sondern auch in ihrer mangelnden Benutzbarkeit. In der Informationstechnik entscheidet man sich im Zweifel eher für eine größere Systemkomplexität (mehr »Features«) als für kleine und einfache Systeme. In der IT-Branche wird dies häufig als eine »stürmische Entwicklung« bezeichnet. Der Computerpionier Roger Needham hat jedoch dazu treffend festgestellt: »People have said that computing is a fast moving subject and what they mean is that the wheel of re-incarnation goes faster« (Omitola, 2001).

Aus Systemkomplexität folgen neue Systemschwachstellen. Fragestellungen von Nachhaltigkeit, Benutzbarkeit und den gesellschaftlichen Auswirkungen der Informationstechnologie werden durch die Informatik als Disziplin noch nicht mit dem notwendigen Stellenwert behandelt. Durch Technologie verursachte gesellschaftliche Effekte sind meist erst nach Jahren beobachtbar. In diesem Sinne wird der Gewöhnungsprozess der Gesellschaft an die Informationstechnik noch Generationen andauern.

5.3. Entwicklungslinien

Die bisherigen Ausführungen lassen drei Entwicklungslinien der Cyberkriminalität und deren strafrechtlicher Erfassung erkennen, die historisch aufeinander aufbauen und dabei ineinander übergehen. Sie reichen von bisher gut verstandenen und erfassten Delikten aus dem Umfeld einer örtlich begrenzten Datenverarbeitung, über zur Zeit diskutierte Delikte wie Spam, die aus der massenhaften Vernetzung entstehen, bis hin zu noch wenig

verstandenen und strafrechtlich noch kaum thematisierten Deliktsformen, die aus der räumlichen Entgrenzung entstehen.

5.3.1. Verwendung elektronischer Datenverarbeitung

Zunächst ergab sich aus der isolierten *Verwendung* informationstechnischer Systeme und *elektronischer Datenverarbeitung* das Erfordernis, Schutzlücken zu schließen, die sich aus der Ersetzung menschlicher Entscheidungsprozesse durch automatisierte Verfahren ergab. Paradigmatisches Beispiel hierfür ist die Einfügung des Delikts des Computerbetrugs (§ 263a StGB) durch das 2. Gesetz zur Bekämpfung der Wirtschaftskriminalität im Jahre 1986. Im gleichen Zuge wurde die Geheimhaltung, der Bestand und die Verwendung von Daten strafrechtlich geschützt (§§ 202a, 303a, 303b StGB).

5.3.2. Internationale Vernetzung der Computertechnologie

Die zunehmende, *internationale Vernetzung der Computertechnologie*, insbesondere durch das Internet, führt zu einer zweiten Entwicklungsstufe und begleitet die Transformation von Industrie- zu Informationsgesellschaften. Rechtliche Schwierigkeiten ergeben sich hierbei etwa aus der neuen Nutzungsmöglichkeit als Kommunikationsmedium (E-Mail und Chat als Individualkommunikation, Webseiten als Massenkommunikation), aus räumlichen Diskrepanzen zwischen Dateneingabe, -speicher und -ausgabeort und den hieraus entstehenden Problemen einer Strafdurchsetzung, oder auch aus räumlich verteilten, koordinierten und nur in ihrer Summe erheblichen Angriffen (Distributed Denial of Service- Attacken), die erst durch die Neufassung des § 303b Abs. 1 Nr. 2 StGB durch das 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität im Jahre 2007 effektiv strafrechtlich erfasst werden können.

Die Gesellschaft wird zunehmend abhängig von Informationstechnologie; Ausfallerscheinungen sind mit erheblichen finanziellen Folgen verbunden – merklich etwa für Millionen ec-Karteninhaber, deren Bargeldversorgung zum Jahreswechsel 2010 aufgrund eines Softwaredefekts eingeschränkt war. Hinzu tritt die Sorge betreffend Gesundheits- und auch Lebensgefahren, etwa bei Angriffen gegen Flugkontrollsysteme oder – bislang glücklicherweise nur hypothetisch – gegen Datenübertragungen im Rahmen medizinischer Behandlungen (vgl. Brenner, 2009b).

5.3.3. Vollständige räumliche Entgrenzung

Erst in ihren Kinderschuhen steckt die rechtliche Erfassung der zunehmenden *Virtualisierung*, die zusammen mit der Vernetzung zur vollständigen Abkopplung von Berechnungsvorgängen vom Ort ihrer Ausführung führt. Konsequenz dessen ist etwa, dass der Speicherort der Daten eines virtualisierten E-Mail-Servers nicht ohne Weiteres feststellbar ist, auf mehrere Rechner auf mehreren Kontinenten verteilt sein könnte und auch eine

Verlagerung des Speicherorts in Sekundenschnelle – etwa von den USA nach Japan – möglich ist.

Auf sozialer Ebene entstehen derzeit virtuelle (Parallel-)Welten, etwa in Massen-Mehrspieler-Online-Rollenspielen, in denen Beteiligte (»Bewohner«, Spieler) die Steuerung virtueller Charaktere übernehmen und sich teilweise mit diesen eher identifizieren als mit ihrem eigenen Körper. Diese virtuellen Charaktere können auch Handel treiben mit rein virtuellen Gütern oder virtuellen Währungen, welche aber regelmäßig mit »echter«, »harter« Währung bezahlt (»getauscht«) werden können.

5.4. Zusammenfassung

Diese veränderten Rahmenbedingungen des Cyberspace schaffen vor allem in Verbindung mit ökonomisch motivierter krimineller Energie neue Probleme, die in diesem Kapitel betrachtet wurden. Vor allem die vollständige räumliche Entgrenzung und die dadurch verursachte inhärente Transnationalität sind aus Sicht der Strafverfolgung problematisch. Im folgenden Kapitel sollen diese Probleme anhand einer Reihe von Beispielen aus der Literatur illustriert werden.

6. Wertschöpfungsprozesse, Akteure, Schäden

6.1. Einleitung

Dieses Kapitel soll den aktuellen Zustand der Cyberkriminalität illustrieren. Hierzu stellen wir Erkenntnisse aus der wissenschaftlichen Literatur zur Strukturierung der Akteurslandschaft (6.2.), zum *modus operandi* der Cyberkriminalität (6.3.) und zum Umfang der Schäden (6.4.) vor.

6.2. Akteure

Wir geben nun einen Überblick über die Akteure im Bereich Cyberkriminalität. Dies sind zunächst die Täter, die Opfer und die Strafverfolgungsbehörden.

Auch wenn viele Aktivitäten der Cyberkriminalität ohne sie nicht denkbar wären, werden die *Anbieter anonymer Zahlungsmittel* im Internet meist nicht zu den Akteuren der Cyberkriminalität gerechnet. Es gibt eine Vielzahl solcher Anbieter, die weltweite Geldtransfers erlauben, ohne dass sich Sender und Empfänger ausweisen müssen. Oft können Gelder unter bloßer Nennung eines Zahlencodes ein- oder ausgezahlt werden. Derartige Dienstleistungen erleichtern in ganz erheblichem Maße die Geldwäsche und verwischen auch aussagekräftige Spuren zu den Hintermännern von Cyberkriminalität. Obwohl das Internet eine ausgezeichnete Plattform für die *Umsetzung* derartiger Dienstleistungen ist, gab es sie auch schon lange vor der Entstehung des Internet.

6.2.1. Cyberkriminelle

Über die Gruppe der Täter von Cyberkriminalität (die Cyberkriminellen) gibt es in der Breite bisher wenig gesicherte Erkenntnisse. Wenn informationstechnische Systeme als Begehungsmittel eingesetzt werden, kommen praktisch alle klassischen Täter auch als Cyberkriminelle in Frage; so sind Urheberrechtsverletzungen ein nahezu ubiquitäres Deliktsfeld. Aber auch der Zugriff auf kinderpornographische Inhalte im Internet erfolgt durch einen diesbezüglich auch in der Vergangenheit beobachteten Täterkreis, die Pädokriminellen.

Für die eher technischeren IT-Delikte (IT-Systeme als Angriffsobjekt) wird in der Literatur häufig eine Einteilung nach zwei Unterscheidungsmerkmalen getroffen: Motivation und Fähigkeiten (*skill*), siehe etwa Rogers (2005). Entsprechend findet man in der Literatur (etwa bei Kshetri, 2010, Kapitel 1.6 und 2.4) eine Unterscheidung folgender Gruppen von Personen, die als Täter in Frage kommen:

- Viele IT-Sicherheitsvorfälle in Unternehmen und Behörden werden durch so genannte *Innentäter* verursacht, also Beschäftigte des Unternehmens oder der Be-

hörde selbst, aber auch ausgeliehene Arbeitskräfte und auch Beschäftigte fremder Unternehmen, die ihren Arbeitsplatz innerhalb des Unternehmens haben.

- Im Bereich des »Hacking« sind in der Regel weltweit vernetzte kriminelle Gruppen aktiv. Die Profile der dort aktiven Personen sind hochspezialisiert und fallen nicht in das typische Raster der klassischen Kriminalität (Kshetri, 2010, Kapitel 2.4.3). In diesen Kreisen scheint eine sehr differenzierte Arbeitsteilung vorzuherrschen. Kriminelle koordinieren sich über elektronische Foren und gehen zum Teil nur sehr kurzfristige Kooperationen ein (Brenner, 2002). Dies unterscheidet ihre Organisationsform von den stark hierarchischen Schemata der klassischen organisierten Kriminalität. Wall (2010) spricht hierbei von einem »flat e-commerce business model«.

- Näher am Raster der klassischen Kriminalität sind die so genannten »Script-Kiddies«, die »Kleinkriminellen« der Cyberkriminalität. Dies sind in der Regel Personen mit mangelndem Grundlagenwissen, die versuchen, mit frei im Netz verfügbaren Angriffswerkzeugen Straftaten wie Phishing oder Kreditkartenmissbrauch zu begehen. Diese Gruppe von Straftätern nimmt in der Praxis zahlenmäßig zu. Schließlich wird es dem technisch ambitionierten Jugendlichen durch die starke Automatisierung und die Verbreitung von Malware-Frameworks immer leichter fällt, menschliche Schwächen sowie technische Schwachstellen auszunutzen.

Häufig genannt werden des Weiteren die »Cyberterroristen« und die staatlichen Akteure, insbesondere die Nachrichtendienste. Zwar resultieren aus ihren Aktivitäten auch Straftaten, die man als Cyberkriminalität bezeichnen und verfolgen kann. Wir wollen aber aus verschiedenen Gründen diese beiden Gruppen nicht weiter betrachten.

Cyberterroristen besitzen keine primär finanzielle Motivation. Allein deshalb sind deren Strukturen schwerer berechen- und nachvollziehbar als bei Kriminellen, die ein Geschäftsmodell verfolgen. Gebräuchlich ist die Verwendung des Internets zur Verbreitung von Propaganda und zur Anwerbung von Sympathisanten. Die Notwendigkeit, konspirativ in voneinander stark abgeschotteten Zellen zu agieren, erschwert allerdings den Aufbau technischer Expertise. Insgesamt erscheint das Problem der politisch motivierten Cyberkriminalität in der öffentlichen Diskussion überbewertet. Für eine weitergehende Diskussion sei auf M. Gercke (2007a) verwiesen.

Staatliche Akteure unterscheiden sich von »normalen« Cyberkriminellen im Wesentlichen durch die ihnen zur Verfügung stehenden Ressourcen, die praktisch als unbegrenzt angenommen werden können. Zu den staatlichen Akteuren zählen nicht nur die Nachrichtendienste, sondern auch Zweige des Militärs. Bei ihren Handlungen stehen andere Kosten/Nutzen-Abwägungen im Vordergrund als bei ökonomisch orientierter Cyberkriminalität. Wir möchten daher auch diese Gruppe aus der weiteren Betrachtung ausschließen und verweisen zu diesem Themenkomplex stattdessen auf Gaycken (2011).

6.2.2. Opfer von Cyberkriminalität

Die wesentlichen unmittelbaren Opfer von Cyberkriminalität sind Behörden, Regierungen, Unternehmen sowie Privatpersonen (Kshetri, 2010, Kapitel 1.6).

Behörden und Unternehmen stehen häufig im Fokus von finanziell motivierter Industriespionage (Többens, 2000); die Unterhaltungs»industrie« zudem im Fokus der spezifischen Urheberrechtskriminalität. Trotz eines gestiegenen Bewusstseins für die Gefahren sind vor allem kleinere Unternehmen in der Regel technisch und organisatorisch gegen die Gefahren von Cyberkriminalität noch unzureichend geschützt.

Auch wenn die Verwendung des Internets für viele Privatpersonen zum Alltag gehört, haben sich noch keine verlässlichen Handlungsvorschriften und sozialen Codes etabliert, die vor den wesentlichen Gefahren im Cyberspace schützen. Die zunehmende Professionalität der Angreifer, etwa beim Verfassen von Spam-E-Mails oder dem Aufsetzen von Phishing-Seiten, verstärkt die Orientierungsschwierigkeiten. Die scheinbare Freiheit, Anonymität und die riesige Auswahl an frei verfügbarer Software für fast jeden Zweck wirken zusätzlich irritierend.

6.2.3. Strafverfolgungsbehörden

Die Strafverfolgungsbehörden haben die Aufgabe, repressiv gegen Cyberkriminalität vorzugehen. Die in Kapitel 5., S. 53 genannten Herausforderungen erschweren die Arbeit dieser Behörden allerdings deutlich.

So ist es für die Verfolgung von Cyberkriminalität notwendig, eine ausreichende Anzahl technisch gut ausgebildeter Personen zur Verfügung zu haben. Dies erfordert allerdings einen Ressourcentransfer, den Behörden erfahrungsgemäß nur sehr langsam vollziehen können. In vielen Bereichen der Polizei wird der *Breite* der Ausbildung noch eine höhere Priorität eingeräumt als deren Tiefe. Dies ist vor allem im Bereich der Cyberkriminalität bisher kontraproduktiv gewesen. Auch können Strafverfolgungsbehörden gegenüber der Industrie keine kompetitiven Gehälter für hochspezialisierte technische Experten bieten (Kshetri, 2010, Kapitel 2.4.2). Dies resultiert in einer starken Fluktuation der Mitarbeiter in den Dienststellen, die sich mit Cyberkriminalität befassen.

6.3. Arbeitsteilung und Wertschöpfung

In der Literatur sind der hohe Grad an Organisation und eine ausdifferenzierte Arbeitsteilung der Schattenwirtschaft sehr gut dokumentiert. Die Arbeitsteilung manifestiert sich in einem raffinierten Organisationskreislauf, der in vergleichbarer Form mehrfach beschrieben wurde (Bolduan, 2008; Manske, 2007; Spoenle, 2010). Dieser Kreislauf ist in schematischer Form in Abbildung 6.1 dargestellt und soll im Folgenden näher erläutert werden.

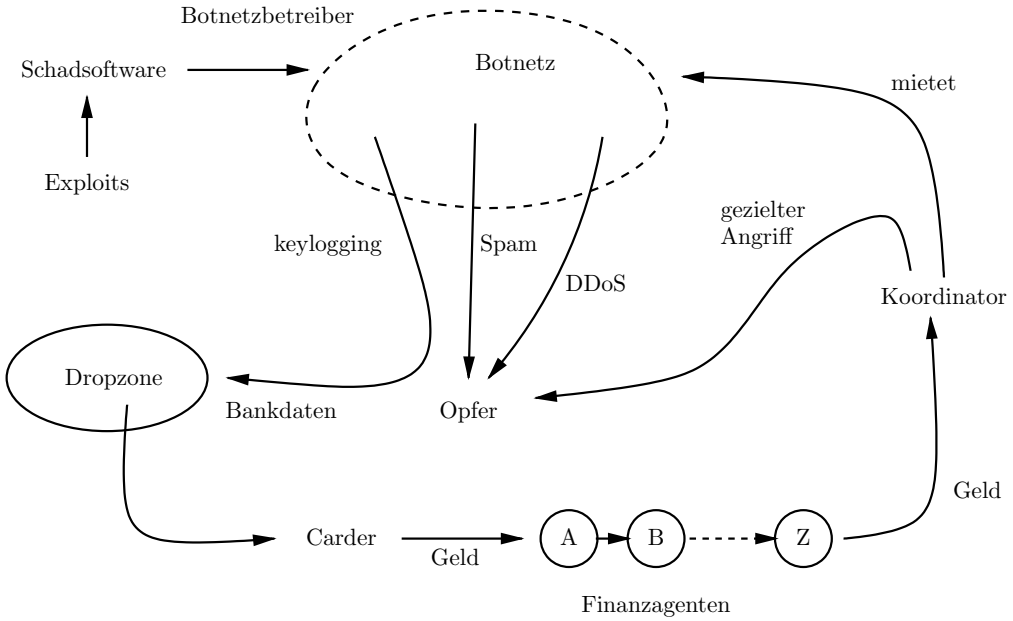

Abbildung 6.1: Der Kreislauf der digitalen Schattenwirtschaft (nach Bolduan (2008)).

6.3.1. Automatisierte Ausnutzung von Schwachstellen

Ausgangspunkt des Kreislaufes ist die Arbeit von technischen Experten (»Hacker«), die fremde Systeme erfolgreich angreifen können. Dazu gehören die Suche nach Schwachstellen in bestehenden Systemen sowie die Programmierung von Werkzeugen, die diese Schwachstellen möglichst automatisiert ausnutzen, um schlussendlich die Kontrolle über das System zu gewinnen. Man spricht dann auch von einer *Kompromittierung* oder einer *Infektion*. Die Vorgehensweise der Szene hat sich in den letzten beiden Jahrzehnten grundlegend verändert. Während noch bis zur Jahrtausendwende das Angreifen von Systemen häufig noch händisch erfolgte, sind die meisten Vorgänge heute mittels Software hochgradig automatisiert. Im Ergebnis können bei Vorliegen einer entsprechenden Schwachstelle deutlich mehr Systeme erfolgreich angegriffen werden als früher.

Aufgrund der Komplexität der Aufgabenstellung ist die Arbeitsteilung in diesem Bereich besonders weit fortgeschritten. So gibt es Spezialisten, die sich ausschließlich mit der Suche nach Schwachstellen in bestimmten Systemen (Betriebssystemen, Anwendungssoftware, Smartphones etc.) beschäftigen. Das Ergebnis ist dann meist ein so genannter *Exploit*, also eine Beschreibung der Schwachstelle mitsamt einem kleinen Programm, das den Angriff ausführt und damit dessen Erfolg dokumentiert. Exploits sind daher der eigentliche Rohstoff der digitalen Schattenwirtschaft.

Exploits werden anschließend zur eigentlichen *Schadsoftware* (*Malware*) weiterverarbeitet. Dies geschieht auf verschiedene Arten. In der Regel muss ein Exploit verfeinert werden, damit er mit höherer Wahrscheinlichkeit und auf einer größeren Menge von IT-Systemen funktioniert. Anschließend bauen andere Spezialisten den Exploit in Werk-

zeuge ein, die damit beispielsweise automatisiert und großflächig Systeme angreifen können. Andere Spezialisten wiederum setzen den Exploit ein, um zielgerichtet eine bestimmte, sehr kleine Anzahl von Systemen anzugreifen (*targeted attack*).

Weiter gibt es Akteure, die für den Vertrieb – im betriebswirtschaftlichen Sinne! – von Schadsoftware zuständig sind. Diese bieten die Schadsoftware selbst sowie dazugehörige Dienstleistungen auf entsprechenden Internetforen zum Kauf an. Zu den Diensten gehören etwa die Erstellung von Schadsoftware für bestimmte Zwecke (Spionage, Erpressung etc.) oder deren Härtung gegen bekannte Antivirenprodukte. Im Preis inbegriffen ist meist ein professioneller »Support« mit einer 24-stündigen Erreichbarkeit via Skype oder Internet Relay Chat (Fossi et al., 2008).

Die Identifizierung von Schwachstellen und deren Ausnutzung ist ein hochspezialisiertes Gewerbe, in dem man auch auf legale Weise Geld verdienen kann (Miller, 2007). So gibt es auch in Deutschland eine Vielzahl an Unternehmen, die so genannte *Penetrationstests* anbieten. Dies sind kontrollierte Angriffe auf IT-Systeme, die von den Eigentümern der Systeme selbst in Auftrag gegeben werden. Derartige Tests gehören mittlerweile zum Standardvorgehen bei der Absicherung von IT-Infrastrukturen und werden in der Regel mit höchster Diskretion durchgeführt. Auch das Bundesamt für Sicherheit in der Informationstechnik bietet derartige Dienstleistungen für Behörden an. Des Weiteren gibt es Unternehmen, die aktiv nach Schwachstellen in existierender Software suchen und entsprechende Exploits entwickeln oder auch aus unterschiedlichen Quellen ankaufen. Das Wissen über diese Exploits und entsprechende Schutzmöglichkeiten wird dann exklusiv an den eigenen Kundenkreis weitergegeben. Schließlich nutzen auch die Hersteller von Antivirenprodukten ihr Wissen über Schwachstellen und Schadsoftware, um auf legale Weise Geld zu verdienen.

6.3.2. Verbreitung von Schadsoftware

Schadsoftware gibt es in ungezählten Formen und Varianten. Man unterscheidet sie in der Regel anhand von drei Komponenten:

- Die *Verbreitungsmethode* bezieht sich auf die Art und Weise, wie Rechner infiziert werden. Infektionen können dabei nicht nur durch Exploits erfolgen, sondern auch dadurch, dass Benutzer zur »freiwilligen« Installation von Software verleitet werden. Während früher vollständig automatisierte Verbreitungsmethoden mit Exploits auf Betriebssystemebene die Regel waren, dominieren heute Angriffe auf Anwendungsebene, also beispielsweise der Versand von Schadsoftware per E-Mail oder die Ausnutzung von Schwachstellen in Browsern (so genannte *Drive-by-Downloads*).
- Ihre bösartige Wirkung entfaltet Schadsoftware erst durch die *Schadfunktion*. Hierbei ist alles möglich, was dem Angreifer nutzt. Die Palette der Möglichkeiten reicht

von Keylogging, also dem Mitschneiden von Keditkartennummern und anderen kritischen Benutzereingaben, über das heimliche Versenden von Spam bis hin zu Datenmanipulation beim Online-Banking.

- Schließlich bestimmt die *Kommunikationsmethode*, ob und wie die Schadsoftware nach der Infektion ferngesteuert werden kann. Fernsteuerung hat für die Angreifer viele Vorteile. Analog zur Aktualisierungsfunktionalität von legitimer Software kann man Schadsoftware so regelmäßig verändern, etwa um der Erkennung durch Antivirenprodukte zu entgehen, Fehler in der Schadsoftware zu beseitigen oder spezifische neue Funktionalitäten umzusetzen. Fernsteuerung ist zudem zur Koordination von Überlastungsangriffen (*Denial-of-Service*) notwendig. Abhängig von der Funktionalität benötigt die Schadsoftware auch eine Möglichkeit, ausgespähte Daten an den Angreifer zurückzusenden.

  Als Kommunikationsmethode kommen Netzwerkverbindungen über Standardprotokolle wie HTTP, IRC oder verschiedene Protokolle aus dem Filesharing-Umfeld in Betracht. Teilweise werden diese Protokolle aber auch adaptiert und verändert, was eine Analyse erschwert. Neuerdings wird die Kommunikation zunehmend verschlüsselt.

Bayer, Habibi, Balzarotti, Kirda und Kruegel (2009) geben einen statistischen Überblick über das Verhalten von etwa einer Million verschiedener Schadsoftware-Exemplare, die aus einer Vielzahl von Quellen in den Jahren 2007 und 2008 gesammelt wurden. Wondracek, Holz, Platzer, Kirda und Kruegel (2010) weisen nach, dass die so genannte »*adult industry*« im Internet auch als Multiplikator für Schadsoftware verwendet wird. Einen Einblick in die Mechanismen des Phishing geben schließlich Cova, Kruegel und Vigna (2008).

6.3.3. Botnetze

Die massive Verbreitung von Schadsoftware mit einer einheitlichen Möglichkeit der Fernsteuerung führt wiederum zu neuen Geschäftsformen. Die Infrastruktur liefern dabei die so genannten *Botnetze*. Ein Botnetz besteht aus einer Menge von aktiven Schadsoftware-Exemplaren (den *Bots*), die über das Internet überwacht und ferngesteuert werden können. Botnetze sind daher universelle Plattformen für nahezu jede Art bösartiger Aktivitäten im Internet. Mit ihnen kann man den Effekt der Schadfunktion von einem infizierten Rechner auf tausende Rechner ausdehnen. Dies führt zu einer neuen Qualität der durchgeführten Aktivitäten, etwa dem Spam-Versand oder dem massenhaften Keylogging. Erst durch Botnetze werden auch verteilte Überlastungsangriffe auf einzelne Rechner oder die Internet-Infrastruktur als Ganzes möglich.

Zum Aufbau eines Botnetzes muss man notwendigerweise eine große Anzahl von Rechnern angreifen und infizieren (Freiling, Holz & Wicherski, 2005). Die Verbreitungsfunk-

tion der Schadsoftware kann dabei allerdings auch auf eine bestimmte geographische Region oder bestimmte Adressbereiche des Internets eingeschränkt werden. Die massenhafte Infektion erhöht allerdings nicht nur die Schadenswirkung, sondern erhöht auch die Wahrscheinlichkeit, dass die bösartige Aktivität entdeckt wird. In bestimmten Fällen ist es für die Geschäftszwecke der digitalen Schattenwirtschaft sinnvoller, möglichst lange unerkannt zu bleiben und dafür auf eine großflächige Verbreitung zu verzichten, etwa im Fall von Industriespionage, so dass keineswegs alle modernen Angriffe auf Botnetze zurückgreifen.

Im Extremfall wird daher eine Schadsoftware speziell zur Infektion eines individuellen Rechners geschaffen. Die Verbreitung geschieht dann etwa durch den Versand der Schadsoftware mittels einer persönlichen E-Mail an das Opfer oder die Übergabe eines Speichermediums (CD oder USB-Stick), dessen Benutzung zur Infektion führt. Derartige *gezielte Angriffe* sind eine außerordentlich schwer wiegende Bedrohung, gegen die es letztendlich keinen technischen Schutz gibt. Auf diesem Wege erfolgen daher auch staatliche Eingriffe zur Quellen-Telekommunikationsüberwachung und zur Online-Durchsuchung.

6.3.4. Wertschöpfung

Wertschöpfung erfolgt immer dann, wenn illegale Aktivitäten im Cyberspace zu einem wirtschaftlichen Vorteil in der realen Welt führen. Da ein Großteil der heutigen Cyberkriminalität von finanziellen Interessen getrieben zu sein scheint, ist die Frage der Wertschöpfung von ganz entscheidender Bedeutung.

Bei den Wertschöpfungsprozessen kann man unterscheiden zwischen Aktivitäten, die eine direkte Analogie in der realen Welt haben, und neuartigen Geschäftsideen, die ohne vernetzte Informationstechnik nicht denkbar sind. Zur ersten Gruppe zählen etwa

- der Versand von »klassischem« Spam, also Werbebotschaften für online bestellbare Produkte,
- die Monetarisierung von Informationen aus gezielten Angriffen, also etwa der Verkauf von Geschäftsgeheimnissen im Rahmen von Spionageaktivitäten,
- elektronische Schutzgelderpressungen, also etwa Geldforderungen gegen Online-Wettanbieter bei gleichzeitiger Drohung, deren Webpräsenz durch einen Überlastungsangriff massiv zu stören, oder
- die Monetarisierung von anderweitigen Informationen, die einen Wert an sich darstellen, wie etwa digitale Wertgegenstände in Online-Rollenspielen wie World of Warcraft, von urheberrechtlich geschützten Werken und von kinderpornographischen Schriften (s. hierzu aber European Financial Coalition against Commercial

Sexual Exploitation of Children Online, 2010, S. 12: nur 22 % der beobachteten Angebote waren kommerziell).

Eine solche Monetarisierung kann entweder auf direktem Wege – d.h. Leistung gegen Bezahlung – erfolgen, aber auch indirekt: So können Werbeeinnahmen durch den Besuch einer Downloadseite erzielt werden, und so können die durch *Drive-by-Downloads* kompromittierten Rechner weiterverkauft werden (s. 6.5.1., S. 76).

Im Rahmen von Botnetzen sind jedoch auch andere und neuartige Wertschöpfungsprozesse möglich, die bis vor kurzem nur schwer vorstellbar waren. Sie zielen auf die Monetarisierung von Daten, die in großer Menge durch Keylogger gesammelt werden. Wertvoll sind beispielsweise Kreditkartendaten und Zugangsinformationen (Kennung und Passwort) zu diversen Onlinediensten oder – dies war ein beliebtes Deliktsfeld der vergangenen Monate – Zugangsdaten zu Online-Rollenspielen.

In Abbildung 6.1 ist dies am Beispiel von Kreditkartendaten deutlich gemacht. Sobald der Benutzer eines infizierten Rechners seine Kreditkartennummer auf einer Webseite eintippt, wird sie durch die Schadsoftware mitprotokolliert und in einer Datei lokal gespeichert. In regelmäßigen Abständen werden die so gesammelten Daten auf einen Rechner im Internet übertragen, von dem der Angreifer die Daten abholt. Man spricht bildlich von einer »Abwurfstelle« (*dropzone*). Diese *Dropzone* ist entweder selbst ein infizierter Rechner oder wird in einem Land betrieben, in dem die Strafverfolgungsbehörden gegen entsprechende Aktivitäten nicht vorgehen wollen oder können.

Die so gesammelten Daten werden anschließend verwendet, um beispielsweise an Geldautomaten Geld abzuheben. Dies ist »Handarbeit«, weshalb sich auch hierfür ein eigener Dienstleistungszweig der Schattenwirtschaft etabliert hat, die so genannten *Carder* (Spoenle, 2010). Mit den Kreditkartendaten kann man aber auch Waren bestellen, die bei Bedarf auf Auktionsplattformen im Internet zu Geld gemacht werden können. Hier braucht man allerdings eine *physische* Abwurfstelle, um die Waren entgegen zu nehmen. Aber auch hierauf hat sich ein Zweig der Schattenwirtschaft spezialisiert. Anschließend muss wie in der klassischen Kriminalität die Herkunft des Geldes verschleiert werden.

Etwas einfacher stellt sich die Situation dar, wenn direkt die Zugangsdaten zu Zahlungsdienstleistern wie PayPal oder Webmoney ausgespäht werden. Mit ihnen kann man direkt Geld vom Konto des Opfers auf ein anderes Konto überweisen. (Ähnlich gestaltet es sich bei vielen Online-Banking-Verfahren in den USA, die im Gegensatz zu Deutschland kein PIN/TAN-Verfahren benutzen.) Da derartige Zahlungen aber in der Regel durch die Banken und Strafverfolgungsbehörden leicht nachvollzogen werden können, werden so genannte *Finanzagenten* (*money mules*) zwischengeschaltet. Dies sind meist ahnungslose Arbeitslose, die von dubiosen Vermittlern oder in Spam-Nachrichten mit der Aussicht auf das »schnelle Geld« angeworben werden. Die Finanzagenten werden unter einem

Vorwand angewiesen, Geldeingänge auf ihrem eigenen Konto über einen anonymen Zahlungsdienst (wie Western Union) ins Ausland weiterzuleiten. Einen bestimmten Prozentsatz der Geldsumme dürfen sie als Provision behalten.

Die direkte Monetarisierung gestohlener Daten gehört zu den schwierigsten Abschnitten des Kreislaufs der digitalen Schattenwirtschaft. Die in Menge und Aggressivität zunehmende Werbung für den Job des Finanzagenten deutet auf die Schwierigkeit hin, hinreichend viele Personen für diesen Zweck zu rekrutieren (Florêncio & Herley, 2010). Auf diesem Gebiet ist deshalb in Zukunft mit neuen Entwicklungen zu rechnen. Es gibt beispielsweise Indizien, dass virtuelle Welten wie Second Life oder Online-Rollenspiele wie World of Warcraft mit ihren eigenen virtuellen Währungen zunehmend zur Geldwäsche eingesetzt werden (Spoenle, 2010).

6.3.5. Infrastruktur

Im Hintergrund steht eine Infrastruktur, die den Kreislauf der digitalen Schattenwirtschaft duldet oder sich mit ihm arrangiert hat. Entgegen einer häufig geäußerten Meinung gibt es keinerlei wissenschaftliche Belege dafür, dass es engere Verbindungen zwischen der traditionellen organisierten Kriminalität (etwa im Bereich Drogen- oder Menschenhandel) und den Infrastrukturanbietern für die digitale Schattenwirtschaft gibt (Wall, 2010).

Zur Infrastruktur gehören erstens Staaten, die Cyberkriminalität rechtlich oder faktisch nur unzureichend verfolgen und hieraus durchaus auch kurzfristige wirtschaftliche Vorteile ziehen können. Zweitens sind hierzu die bereits genannten anonymen Zahlungsdienste zu zählen, welche eine Nachverfolgung der wirtschaftlichen Ströme zumindest deutlich erschweren.

Schließlich und drittens benötigt man aber auch immer eine Reihe willfähriger Internet-Service-Provider, welche die Strafverfolgungsbehörden nicht unterstützen und denen das Benehmen ihrer Kunden egal ist, sofern diese nur pünktlich ihre Rechnungen bezahlen (Stone-Gross et al., 2009). Dieses so genannte *Bulletproof Hosting* ist ein Mehrwert, den sich die Provider gut bezahlen lassen. Sie sind somit direkte Nutznießer der digitalen Schattenwirtschaft.

Zu den Angeboten derartiger Provider zählen auch schnelle Änderungen bei der Namensauflösung durch den Namensdienst DNS. Diese werden für so genannte Fast-Flux-Netzwerke benötigt, eine besonders raffinierte Verschleierungstechnik von Botnetzen (Holz, Gorecki, Rieck & Freiling, 2008). Hierbei wird das Botnetz selbst als eine Art Anonymisierungsdienst genutzt, indem Kommunikationsverbindungen zwischen dem Angreifer und den Bots über mehrere Zwischenstationen innerhalb des Botnetzes weitergeleitet werden.

Bulletproof Hosting-Provider gibt es insbesondere in hoch entwickelten Staaten mit guter technischer Infrastruktur. Eine Untersuchung von Göbel und Holz (2008) im Universi-

tätsnetz der RWTH Aachen zeigte, dass die Kontrollrechner für die dort aktiven Botnetze mehrheitlich in den USA, China und Deutschland standen.

6.4. Schäden durch Cyberkriminalität

Wie groß ist der Einfluss von Cyberkriminalität auf die Gesellschaft, auf die Wirtschaft? Dieser zentrale Aspekt, der einer evidenzbasierten politischen Willensbildung zugrunde liegen muss, wird häufig zugespitzt auf die Frage nach der »Menge« an Cyberkriminalität, die derzeit existiert. Dabei ist es keineswegs überraschend, dass diese Frage schwer zu beantworten ist, gibt es doch – wie auch in anderen Bereichen der Kriminalität – immer das so genannte Dunkelfeld, das *per definitionem* nicht genau bezifferbar ist.

Veröffentlichte Schätzungen über die durch Cyberkriminalität verursachten Schäden sind erstaunlich inkonsistent. Kshetri (2010, S. 7) gibt einen Überblick über Zahlen aus verschiedenen öffentlichen und privatwirtschaftlichen Quellen, deren Beträge zwischen 100 und 300 Milliarden Dollar rangieren. Selbst bei relativ klar zu definierenden Kenngrößen, wie dem weltweiten Prozentsatz an infizierten Rechnern, die Teil eines Botnetzes sind, liegen die Schätzungen oft weit auseinander (zwischen 7% und 25%, Angaben nach Kshetri, 2010).

6.4.1. Einflussfaktoren auf die öffentliche Wahrnehmung

Neben der Dunkelfeldproblematik wirken im Bereich der Cyberkriminalität noch andere Faktoren negativ auf die realistische Wahrnehmung des Phänomens. Zum einen tragen die Medien eine große Verantwortung für die realistische Wahrnehmung der Gefahren, die durch Cyberkriminalität entstehen. Das Thema »Internet« ist jedoch gerade innerhalb medial-bevorzugter Zielgruppen derzeit so nachrichtentauglich, dass ein einzelner großer Sicherheitsvorfall schnell zu einer die Medienlandschaft beherrschenden Schlagzeile wird (Wall, 2007, S. 14). Derartige Schlagzeilen haben mit der Zeit das Potential, die öffentliche Wahrnehmung zu formen, und münden nicht selten in Forderungen nach »schnellen Lösungen« für extrem komplexe Probleme. Auch hat die Filmindustrie mit Filmen wie »GoldenEye« (1995), »Hackers« (1995), »Enemy of the State« (1998), oder »AntiTrust« (2001) das Bild des Hackers geprägt als eine Person, die mit wenigen Mausklicks große Zerstörungen hervorrufen kann und die sich kaum an ethische Richtlinien, geschweige denn an Gesetze hält (Wall, 2007, S. 16). All dies erzeugt bei den Zuschauern ein Gefühl der gesellschaftlichen und politischen Ohnmacht und verstärkt die verschiedentlich beobachteten Tendenzen einer »Kultur der Angst« (Furedi, 2002); zugleich aber werden die individuellen Möglichkeiten zur Verhinderung von Cyberkriminalität mit dem Verweis darauf, dass es bei einem selbst nichts Interessantes auszuspähen gebe, unterschätzt.

Zum anderen sind die IT-Sicherheitsindustrie und Teile der Sicherheitsbehörden selbst nicht ganz unschuldig an der unübersichtlichen Informationslage bezüglich Cyberkrimi-

nalität. Schließlich hilft die zunehmende Besorgnis über eine verstärkte Bedrohungslage beim Wettbewerb um Stellen und Ressourcen oder bei der Sicherung einer Monopolstellung am Markt (Kshetri, 2010, S. 9). Der bekannte IT-Sicherheitsexperte Bruce Schneier charakterisierte die IT-Sicherheitsindustrie einmal wenig schmeichelhaft und nur halb scherzhaft als »[a] self-dramatizing and fear-mongering world of security pundits« (Schneier, 2006).

6.4.2. Das Fehlen verlässlicher Zahlen

Zur politischen Einschätzung des Risikos von Cyberkriminalität ist es notwendig, zwischen *potentiellen* Schäden und *wirklichen* Schäden zu unterscheiden. Werden die potentiellen Schäden mit den wirklichen Schäden verwechselt, verschiebt sich die öffentliche Meinung schnell in Richtung der Bedürfnisse des Staates nach Kontrolle und Überwachung und gegen grundlegende Freiheitsrechte der Bürger. Helfen können hier nur verlässliche empirische Daten. Solche Daten fehlen aber leider weitestgehend. So stellt Kshetri (2010, S. 7) fest: »No reliable statistics exist.«

Ein erster Aspekt hiervon ist, dass bei Urheberrechtsverstößen keineswegs die Anzahl der Downloads mit dem Ladenverkaufspreis des Produkts multipliziert werden darf, um den Schaden zu beziffern: Es ist höchst ungewiss, ob diejenigen, die sich urheberrechtlich geschützte Musik oder Filme für den privaten Gebrauch heruntergeladen haben, diese Waren überhaupt zu diesem Preis auf dem legalen Markt erworben hätten.

Ferner erschweren geschlossene, kleinere Benutzergruppen eine analytische Bewertung, wie sie etwa im Bereich der Verbreitung und des Tauschs kinderpornographischer Schriften zu beobachten sind (European Financial Coalition against Commercial Sexual Exploitation of Children Online, 2010, S. 31).

Ein weiterer Grund für das Fehlen relevanter Statistiken ist die internationale Dimension von Cyberkriminalität (Wall, 2007, S. 17). Damit ähnelt sie stark der (internationalen) Wirtschaftskriminalität und der globalen organisierten Kriminalität, für die es auch keine zentrale internationale Registrierungsstelle gibt, wie sie etwa die Polizei auf nationaler Ebene bei normaler Straßenkriminalität darstellt. Auch werden viele Schadensfälle an den Strafverfolgungsbehörden vorbei geregelt, also ohne Strafanzeige und durch interne Ermittlungen innerhalb von Unternehmen. Insofern ist auch die vielzitierte Polizeiliche Kriminalstatistik (Bundeskriminalamt, 2010) im Bereich Cyberkriminalität nur bedingt aussagekräftig.

Ähnliches gilt für den zuletzt verstärkt zitierten jährlichen IT-Sicherheitsbericht von CSI und FBI in den USA (CSI/FBI, 2006) und andere Überblicksstatistiken von Unternehmen und Behörden, wie etwa Symantec (2009), G Data (Ester & Benzmüller, 2010), Panda Security (2010), PricewaterhouseCoopers (Bussmann et al., 2009), der Federal Trade Commission in den USA (Rantala, 2010) oder vom Department of Trade and Industry

in Großbritannien (DTI, 2004). Alle diese Erhebungen stimmen darin überein, dass die Anzahl der Sicherheitsvorfälle und die dadurch verursachten Schäden in den vergangenen Jahren stetig und deutlich zugenommen haben.

Die beste Art, verlässliche und statistisch repräsentative Zahlen über die Auswirkungen von Kriminalität zu erhalten, ist die *umfangreiche* Befragung von Personen und Unternehmen. Die bedeutendsten uns bekannten Umfragen im Bereich Cyberkriminalität stammen aus Großbritannien. Dort wurden erstmals 2003 (Allen, Forrest, Levi, Roy & Sutton, 2005) und letztmals 2004 (Wilson, Patterson, Powell & Hembury, 2006) im Rahmen der jährlich stattfindenden Kriminalitätserhebung (*Britisch Crime Survey*) Fragen zu Erfahrungen mit Cyberkriminalität gestellt. Befragt wurden etwa 40.000 Personen über 16 Jahren, die in einem Privathaushalt wohnen. Die Rücklaufquote betrug jeweils knapp 75%.

Die Zahlen der beiden Befragungen stimmen im Wesentlichen überein. Wir geben hier einen Überblick über die Ergebnisse der zweiten Befragung, die 2006 erschien (Wilson et al., 2006). Demnach gaben etwa ein Viertel der Befragten, die regelmäßig das Internet nutzten, an, innerhalb der letzten 12 Monate von einem Computervirus befallen worden zu sein. Allerdings hatten nur 2% den Eindruck, dass der heimische Rechner das Ziel eines erfolgreichen Hackerangriffs gewesen sei, bei dem Daten ausgespäht worden sein könnten.

25% der regelmäßigen Internetnutzer hatten innerhalb der vergangenen zwölf Monate anstößige Inhalte erhalten oder auf derartige Inhalte zugegriffen. Zum Vergleich hatten nur 12% eine anstößige oder belästigende E-Mail erhalten. 26% der Befragten unter 25 Jahren gaben an, mindestens ein Mal während des vergangenen Jahres urheberrechlich geschütztes Material illegal heruntergeladen zu haben. Die Befragungen enthalten auch interessante Aufschlüsse über die Profile von Tätern in der Cyberkriminalität.

In Deutschland wurden an der Universität Bonn in der Vergangenheit mehrere nichtrepräsentative Online-Umfragen zum Thema »Sicherheit und Delinquenz im Internet« durchgeführt, zuletzt 2006 mit mehr als 2000 Teilnehmern (Rüther, 2007, 2006). Dort wurde unter anderem die Betroffenheit der Befragten bezüglich spezifischer Delikte erhoben. Im Resultat hatten mehr als 40% der Befragten mindestens einen »Viren-Befall« innerhalb der letzten zwölf Monate erlebt, allerdings lag der Anteil an Opfern von Phishing, Auktionsbetrug oder Hacking bei weniger als 5%.

Weitere Erhebungen in Deutschland sind uns nicht bekannt. Auch die Autoren der kürzlich erschienenen Studie zum Thema Identitätsdiebstahl und Identitätsmissbrauch im Internet Borges, Schwenk, Stuckenberg und Wegener (2011) weisen mehrfach darauf hin, dass empirische Daten zu kritischen Fragestellungen fehlen. Einen ersten, im Detailreichtum freilich nur unzureichenden Ansatz hin zu einer empirischen Analyse liefert nunmehr eine

Statistik der Europäischen Kommission, welche die durch die anderen Studien genannten Größenordnungen bestätigen (eurostat, 2011).

Eine Möglichkeit für repräsentative Messungen technisch definierbarer Phänomene bieten verteilte Sensornetzwerke, etwa in Form von *Honeynets*. Honeynets sind Netzwerke von elektronischen Ködern für Schadsoftware (*Honeypots*) (Göbel, 2010; Provos & Holz, 2007; Spitzner, 2003), welche als Sensoren für Schadsoftware wirken. Mit ihnen kann man beispielsweise großflächig die Angriffsaktivität von sich autonom verbreitender Schadsoftware messen (Engelberth et al., 2010; Göbel & Trinius, 2010; Pouget, Dacier & Pham, 2005). Für repräsentative Aussagen, etwa bezüglich der Frage, wie viele Rechner im deutschen Internet mit einer speziellen Klasse von Schadsoftware infiziert sind, ist jedoch eine Art »Zufallsstichprobe« mit mindestens 100 Sensoren des untersuchten Netzwerkbereichs notwendig (Freiling, 2010). Uns ist nicht bekannt, dass derartige Hochrechnungen bereits durchgeführt wurden.

6.4.3. Mögliche Abhilfe

Zur Bezifferung der Schäden von Cyberkriminalität in Deutschland wäre es sinnvoll, eine breit angelegte, repräsentative, kriminologische Studie durchzuführen. Sinnvoll wäre zudem, eine solche Studie in regelmäßigen Abständen zu wiederholen, um auch einen Einblick in die zeitliche Entwicklung zu erhalten. Ein anderer möglicher Ansatz wäre es, die Verlässlichkeit der polizeilichen Kriminalstatistik zu erhöhen.

Allerdings stehen diesen Vorhaben die mangelnde Anzeigebereitschaft vor allem der Wirtschaft und die geringe Bereitschaft entgegen, an empirischen Studien mitzuwirken (Kiethe & Hohmann, 2006, S. 185, Többens, 2000, S. 511 f.). Dass vor allem Unternehmen eine Anzeige bei den Strafverfolgungsbehörden scheuen, liegt in der Angst um die eigene Reputation und das Vertrauen der Kunden in die eigenen Produkte begründet (Dornseif, 2005, Kapitel 2). Bei Mitarbeitern dieser Unternehmen wirkt zusätzlich die Angst, dass nach einer Anzeige und der öffentlichen Bekanntmachung des Angriffs andere Kriminelle das eigene Unternehmen als Angriffsziel auswählen könnten, was auch den eigenen Arbeitsplatz gefährden könnte (Wall, 2007, S. 20). Auch die Einführung einer Pflicht zur Anzeige IT-bezogener Straftaten würde daher nicht wirklich weiterhelfen.

Notwendig ist vielmehr eine gesamtgesellschaftliche Einsicht, dass eine geringe Anzeigebereitschaft schlussendlich zu einer Schieflage bei der internen Ressourcenzuteilung der Strafverfolgungsbehörden führt (Wall, 2007, S. 20). Dies wiederum führt zu weniger Wissen über Opfer und Täter – ein Teufelskreis.

6.5. Illustrierende Beispiele

Im Folgenden möchten wir die oben beschriebenen Sachverhalte mit Beispielen aus der wissenschaftlichen Literatur illustrieren.

6.5.1. Handel mit gestohlenen Daten

Die ersten wissenschaftlichen Erkenntnisse zum elektronischen Handel mit gestohlenen Daten stammen aus dem Honeynet Project (Spitzner, 2003). Mittels der dort entwickelten Honeypot-Technologie kann man kompromittierte Rechner exakt überwachen. Auf einigen solchen Rechnern stellte man verstärkte Netzwerkaktivitäten in einer Reihe von Chat-Kanälen (IRC) und Webseiten mit Namen wie www.ccpower.info oder www.ccpowerforms.org fest. Eine Analyse des Netzwerkverkehrs (Honeynet Project, 2003) ergab, dass dort in großem Umfang und teilweise in automatisierter Form mit gestohlenen Kreditkartendaten gehandelt wurde. Diese waren insbesondere auch durch Innentäter (in Hotels oder Gaststätten) ausgespäht worden. Der Artikel gibt keine konkreten Zahlen über den Umfang der beobachteten Tatbestände, erläutert aber den »Sprachcode«, den die Benutzer verwendeten.

Die bisher umfangreichste wissenschaftliche Studie zum Handel mit gestohlenen Daten stammt von Franklin, Perrig, Paxson und Savage (2007). Sie gehört zu den am meisten zitierten Quellen, wenn es darum geht, den Wandel vom »*hacking for fun*« zum »*hacking for profit*« zu belegen. Die Autoren beobachteten zwischen Januar und August 2006, also sieben Monate lang, den IRC-Verkehr in einschlägigen Chat-Foren. Daraus resultierten mehr als 13 Millionen Chat-Nachrichten, die qualitativ und quantitativ ausgewertet wurden. Eindrucksvoll ist die Bandbreite an »Waren«, die mittlerweile online gehandelt wird. Neben Kreditkartendaten gibt es kompromittierte Rechner (beispielsweise als Teil eines Botnetzes), Zugangsdaten zu Online-Zahlungsdiensten wie PayPal und Online-Banking, sowie Dienstleistungen im Kontext von Spam-Versand und Phishing zu erwerben. Aus den aufgezeichneten Daten konnten auch Preise für diverse Waren berechnet werden. Der Preis für den Zugriff auf einen kompromittierten Rechner betrug beispielsweise zwischen 2 und 25 US-Dollar. Bemerkenswert ist weiterhin, wie offen der Handel in den entsprechenden Foren betrieben wird. Schließlich wurden für die Studie ausschließlich allgemein zugängliche Nachrichten aufgezeichnet. Thomas und Martin (2006) sprechen von einem Handel »[in a] blatant manner [...] with no need to hide«.

Die Ergebnisse von Franklin et al. (2007) wurden durch weitere Studien (Thomas & Martin, 2006; Fossi et al., 2008; Symantec, 2009; Vömel, Holz & Freiling, 2010; Fallmann, Wondracek & Platzer, 2010; Zhuge et al., 2008) bestätigt. Im Ergebnis stellen alle Autoren fest, dass der Umfang der digitalen Schattenwirtschaft ein signifikantes Niveau erreicht hat. Allerdings wurden die genannten Studien auch kritisiert (Herley & Florêncio, 2009), weil nicht beachtet wurde, dass es sich bei den beobachteten Waren um »saure

Gurken« handeln könnte. Dies ist ein ökonomischer Fachterminus für Waren, bei denen die Preise schwer aus öffentlich verfügbaren Informationen abzulesen sind (*lemon markets*) (Akerlof, 1970). Es kann also durchaus sein, dass der eigentliche Handel doch im Verborgenen und über ganz andere Kanäle stattfindet. Die Schwierigkeit, die gestohlenen Daten schlussendlich zu Geld zu machen (also der Mangel an Finanzagenten), könnte ein weiterer Grund dafür sein, dass die beobachteten Preise nicht das Marktvolumen wiedergeben (Florêncio & Herley, 2010).

Einen etwas direkteren Ansatz, um die Menge und Qualität der gehandelten Waren zu beurteilen, verfolgten Holz et al. (2009). Sie analysierten mehrere Familien von Schadsoftware und konnten so die Abwurfstellen (*dropzones*) identifizieren, auf denen die mittels Keyloggern massenhaft gesammelten Daten regelmäßig abgelegt wurden. Diese Daten waren dort öffentlich zugänglich und wurden von den Autoren in systematischer Art und Weise gesammelt. Innerhalb von sieben Monaten, zwischen April und Oktober 2008, fielen so von mehr als 70 Dropzones insgesamt 33 Gigabyte an vertraulichen Daten an, die statistisch ausgewertet wurden. Durch diese Daten war es erstmals möglich, detaillierte Studien der eigentlichen Opfer von Cyberkriminalität durchzuführen, also etwa welche Betriebssysteme sie benutzten und welche Webseiten sie regelmäßig ansteuerten. Nimmt man die aus anderen Studien bestimmten Marktpreise für die gestohlenen Waren als Grundlage, so konnte ein *täglicher* Umsatz von Waren im Wert von mehreren Hundert US-Dollar berechnet werden.

6.5.2. Spam

Der Versand von Spam entwickelt sich heute zunehmend zu einem Vehikel, um Schadsoftware zu verbreiten. Spam ist deshalb nicht mehr nur lästig, sondern auch gefährlich. Dennoch hat Spam seinen Wert als Überbringer von Werbenachrichten nie verloren. Dies belegen Kanich et al. (2009) mit einer Untersuchung über die so genannte *Konversionsrate* von Spam. Die Konversionsrate ist die Wahrscheinlichkeit, dass eine Spam-E-Mail zu einem finanziellen Umsatz bei den beworbenen Produkten führt. Die Autoren infiltrierten ein Botnetz, das zum Spam-Versand verwendet wurde, und bezifferten die Konversionsrate für die drei betrachteten Spam-Kampagnen auf zwischen 0,0081 und 0,561 *Promille*.

Böhme und Holz (2006) betrachten das Phänomen des *Stock Spam*, einer Klasse von Spam-Nachrichten, die Werbung für so genannte *penny stocks* macht, also Aktien, die kaum gehandelt werden und in der Regel nur wenige Cents kosten. Im Ergebnis kommen die Autoren zum Schluss, dass Stock Spam eine messbare Auswirkung auf den Aktienkurs der beworbenen Titel hat und sich demnach als Geschäftsmodell durchaus eignet.

6.5.3. Ökonomie der IT-Sicherheit

IT-Sicherheit ist kein rein technisches Problem. Viele Autoren haben beobachtet, dass Anreize fehlen, um ausreichend in IT-Sicherheitstechnologien zu investieren. Dies geschieht selbst dann, wenn sich die Akteure innerhalb ihres lokalen Umfeldes vollkommen rational verhalten (L. Gordon & Loeb, 2006; Schneier, 2006). Johnson, Grossklags, Christin und Chuang (2010) zeigen etwa mittels eines mathematischen Modells, dass eine hohe technische Sicherheitsexpertise bei einem Großteil der Entscheidungsträger nicht notwendigerweise zu mehr Sicherheit führt; zu diesbezüglichen spieltheoretischen Ansätzen siehe ferner Böhme und Schwartz (2010). Sinnvoller ist vielmehr ein Verständnis für die gesamtgesellschaftlichen Effekte ihrer Entscheidungen. Hierfür gibt es viele Beispiele, etwa die mangelnde Bereitschaft vieler Menschen, in die Sicherheit ihrer privaten PCs zu investieren. Insbesondere dann, wenn sie darauf keine kritischen Daten speichern, nehmen es viele Menschen hin, dass ihr System zum Bestandteil eines Botnetzes wird und eine gesamtgesellschaftlich schädigende Wirkung entfaltet. Ein anderes Beispiel ist die mangelnde Kooperationsbereitschaft nationaler Sicherheitsbehörden, die bei der Zuteilung von Ressourcen in Konkurrenz stehen.

Die fehlenden ökonomischen Anreize manifestieren sich auch im Mangel an Versicherungsprodukten für die Risiken, die durch Cyberkriminalität entstehen. Versicherungen sind ein gebräuchlicher Mechanismus, um Risiken ökonomisch zu verwalten. Zu den ungünstigen Einflussfaktoren im Bereich Cyberkriminalität gehören eine hohe Risiko-Korrelation (Böhme, 2005; Böhme & Kataria, 2006) und Interdependenz von Schadensereignissen (Bolot & Lelarge, 2008; Kunreuther & Heal, 2003) sowie starke Informations-Asymmetrien (Bandyopadhyay, Mookerjee & Rao, 2009; Shetty, Schwartz, Felegyhazi & Walrund, 2009).

6.6. Zusammenfassung

Dieses Kapitel beleuchtete die handelnden Akteure im Bereich der Cyberkriminalität, den Grad an Organisation und die Dunkelfeldproblematik.

Die Dunkelfeldproblematik ist eines der drängendsten Probleme. So stellt Dornseif (2005, Kapitel 2) fest, dass »bisherige Aussagen zum Dunkelfeld [von IT-Delikten] scheinbar überwiegend auf anekdotischem Wissen« aufbauen. Trotzdem zeigen verschiedene wissenschaftliche Studien, dass die digitale Schattenwirtschaft ein Markt von erheblicher Bedeutung ist. Die Arbeitsteilung und die Verwendung gewerblicher oder geschäftsähnlicher Strukturen erlauben es, auch im juristischen Sinne von organisierter Kriminalität zu sprechen (vgl. RiStBV Anlage E Nr. 2.1).

Ohne verlässliche Zahlen besteht die Gefahr, dass das Ausmaß von Cyberkriminalität auf Dauer unterschätzt wird. Kshetri (2010, Kapitel 2.4) beschreibt dies in Form eines

Teufelskreises: Die mangelnde Investition des Staates in den Schutz vor Cyberkriminalität führt zu einem geringen Vertrauen in die Fähigkeiten der Strafverfolgungsbehörden und zu einem unzureichenden Wissen über technischen und organisatorischen Selbstschutz. Dies wiederum resultiert in einer geringen Anzeigebereitschaft und schwachen technischen Abwehrmechanismen, was die Risikokalkulation für die Cyberkriminellen in Richtung höheren Profits verschiebt. Dies schließlich führt zu mehr noch ausgefeilteren Geschäftsmodellen der Schattenwirtschaft, was den Investitionsbedarf des Staates wiederum erhöht.

Zugleich besteht aber auch eine weitere Gefahr: Aufgrund der Unkenntnis über Cyberkriminalität und einer wahrgenommen, vermeintlichen gesellschaftlichen und politischen Machtlosigkeit gegenüber Cyberkriminalität entsteht von ihr ein diffuses, übertriebenes und als bedrohlich empfundenes Bild.

7. Schutz »im Kleinen«: Selbstschutz und nationale Strafverfolgung

7.1. Einleitung

Wie kann man sich selbst, wie kann die Gesellschaft sich gegen diese aktuellen und zukünftigen Gefahren der Cyberkriminalität schützen? Diese Frage gilt es nun aus technisch-präventiver und aus juristisch-repressiver Sicht zu beleuchten. Dabei wollen wir ausdrücklich die Frage nach einer Verteidigung durch Gegenangriffe ausklammern; die dabei auftretenden rechtlichen Schwierigkeiten betrachtet (A. Koch, 2006).

Zunächst zeigen wir hierzu unter 7.2. auf, welche Schutzmechanismen für jeden Einzelnen, jedes Unternehmen und jede Behörde technisch möglich und sinnvoll sind, um sich oder sein Unternehmen vor Angriffsszenarien zu schützen. Zugleich ist auf organisatorische, aber auch auf regulatorische Aspekte hinzuweisen, um die technische Prävention gegen Cyberkriminalität zu fördern.

Die juristisch-repressive Reaktion auf Cyberkriminalität, also die strafrechtliche Ahndung entsprechender krimineller Verhaltensweisen, erfordert zweierlei:

Erstens müssen die kriminellen Erscheinungsformen von hinreichend bestimmten, normenklaren und verhältnismäßigen Straftatbeständen erfasst, diese also *typisiert* werden. Dies ist eine notwendige Bedingung für jegliche strafrechtliche Verfolgung, denn das Gesetzlichkeitsprinzip erlaubt nur die Bestrafung einer Tat, deren Strafbarkeit bereits vor der Tat gesetzlich bestimmt war (Art. 103 Abs. 2 GG). Daher werden unten 7.3. die für die Verfolgung von Cyberkriminalität bedeutendsten Straftatbestände des deutschen Rechts vorgestellt und dabei auch einer Überprüfung unterzogen, ob bestimmte, strafrechtlich sinnvollerweise zu verfolgende Verhaltensweisen durch deren fragmentarisches Raster fallen, wo also gesetzgeberischer Handlungsbedarf besteht.

Zweitens aber – und dies ist eine hinreichende Bedingung – erfordert eine strafrechtliche Verfolgung auch ein ausreichendes juristisches, forensisches und organisatorisches Instrumentarium, um Cyberkriminelle ihrer Taten zu überführen. Dabei standen und stehen die juristischen Eingriffsbefugnisse im Zentrum der öffentlichen Diskussion über Cyberkriminalität; schlagwortartig sei verwiesen auf die Vorratsdatenspeicherung von Verbindungsdaten und auf die Online-Durchsuchung informationstechnischer Systeme. Es ist allerdings unerlässlich, zunächst die technisch-forensischen und organisatorischen Rahmenbedingungen vertieft zu betrachten, um daraufhin die Erforderlichkeit und Nützlichkeit strafprozessualer Eingriffsbefugnisse fundiert analysieren zu können (7.4.). Trotz aller tagespolitischen Brisanz und der Gefahr, sich an diesem Thema die Finger zu verbrennen, soll schließlich auch bezüglich der strafprozessualen Eingriffsbefugnisse der gesetzgeberische Handlungsbedarf, jedenfalls aber der weitere Forschungs- und Diskussionsbedarf aufgezeigt werden (7.5.).

7.2. Technischer und organisatorischer Selbstschutz

Es gibt eine Vielzahl von Maßnahmen, mit denen man sich – als Privatperson oder als Unternehmen – vor Cyberkriminalität schützen kann. Wie in anderen Bereichen der Prävention reichen schon wenige Maßnahmen aus, um ein hohes Schutzniveau zu erzielen. Die meisten dieser Maßnahmen sind gut dokumentiert (siehe etwa das Portal »BSI für Bürger«, Bundesamt für Sicherheit in der Informationstechnik, o. J.) und werden durch die entsprechenden Interessengruppen und Behörden gebetsmühlenartig wiederholt. Trotz zum Teil groß angelegter Öffentlichkeitsarbeit, wie etwa dem »Safer Internet Day« oder Initiativen wie »Deutschland sicher im Netz« dringen diese Vorsichtsmaßnahmen nur langsam in das breite Bewusstsein der Öffentlichkeit ein. Wir geben im Folgenden nur kurz die wesentlichen Schutzmöglichkeiten wieder.

7.2.1. Schutz vor bösartiger Software

Bösartige Software wird für immer ein Problem bleiben, egal ob im privaten oder betrieblichen Umfeld. Man muss also die möglichen »Installationswege« kennen, um sich effektiv davor schützen zu können.

Der klassische Weg, den bösartige Software nimmt, um auf einen Rechner zu gelangen, führte in der Vergangenheit meist über technische Schwachstellen im Betriebssystem des Rechners. Durch technische Verbesserungen sind Betriebssysteme heute nicht mehr so einfach angreifbar wie noch vor wenigen Jahren. Deswegen versucht Schadsoftware heute verstärkt auch technische Schwachstellen in Anwendungsprogrammen wie Webbrowsern, Textverarbeitungsprogrammen und Videoplayern auszunutzen. Die übliche Empfehlung lautet dabei immer, die Software auf dem eigenen Rechner immer in einem aktuellen Zustand zu halten, um möglichst wenige Schwachstellen anzubieten. Dazu gibt es bei den meisten Programmen eine Aktualisierungsfunktion, die auch automatisch auf Sicherheitsupdates prüft. Besonders hinzuweisen ist auch darauf, dass es nicht ausreicht, bloß den Arbeitsplatzrechner auf aktuellem Stand zu halten: Auch Smartphones, WLAN-Router und sämtliche mit dem Internet verbundenen Geräte stellen lohnenswerte Angriffsziele für Cyberkriminelle dar.

Ein im Umfang zunehmender Vebreitungsweg für Schadsoftware ist die freiwillige Installation durch den Benutzer des Rechners selbst. Bei der Menge an im Internet kostenlos zum Download angebotenen Software ist es schwierig zu unterscheiden, welche davon gutartig ist und welche möglicherweise eine Schadfunktion enthält. Ein großer Anteil an Rechnern, die Teil des *Storm*-Botnetzes waren, wurden beispielsweise durch die Ausführung von Dateien infiziert, die an Spam-Nachrichten angehängt waren (Holz, Steiner, Dahl, Biersack & Freiling, 2008). Eine gute Hilfestellung bei der Unterscheidung zwischen guter und böser Software bieten die Produkte der Antiviren-Hersteller. Die zunehmende Vielfalt und Raffinesse von Schadsoftware hat jedoch dazu geführt, dass die

Antiviren-Produkte nur noch »die wichtigsten« Klassen von Schadsoftware erkennen. Vor allem gegen neue Varianten bieten Antiviren-Produkte nur bedingt Schutz. Eine Studie von Bächer, Kötter, Holz, Dornseif und Freiling (2006) zeigte, dass die Erkennungsraten von vier Antiviren-Produkten auf Schadsoftware, die jeweils innerhalb der letzten 24 Stunden in einem Honeynet gesammelt worden waren, zwischen 73% und 84% lagen – die normale Erkennungsrate sollte bei über 90% liegen.

Benutzer benötigen also auch eine gewisse Sensibilität, wenn es darum geht, Software aus dem Internet zu installieren. Um die damit verbundenen Probleme deutlich zu machen, wird häufig die folgende Analogie benutzt: Software auf dem eigenen Rechner zu installieren ist wie jemanden den Schlüssel zur eigenen Wohnung zu überlassen. Software kann beliebige Einstellungen auf dem Rechner vornehmen und beliebige Vorgänge starten. Wenn man jemanden auf der Straße trifft, der einem einen kostenlosen Zugang zu verlockenden Angeboten verspricht und gleichzeitig behauptet, er müsse dafür nur kurz in Ihre Wohnung, dann würde man dieser Person auch nicht ohne weiteres den Haustürschlüssel überlassen.

Eine etwas ferner liegende Analogie vergleicht das Beherbergen von Schadsoftware auf dem eigenen Rechner mit der Tätigkeit von Sympathisanten der Baader-Meinhof-Bande in den 1970er Jahren, die den Terroristen leichtfertig die eigene Wohnung als Unterschlupf überließen (vgl. Aust, 2008).

7.2.2. Authentifikationsproblematik

Viele Probleme entstehen auch wegen der bereits wiederholt angesprochenen Problematik der Authentifikation im Cyberspace. So ist weiterhin vielen Benutzern unbekannt, dass die Absenderinformationen in einer E-Mail sehr leicht manipuliert werden können. Ein Blick auf die Absenderadresse reicht deshalb nicht aus, um die Vertrauenswürdigkeit einer E-Mail einzuschätzen.

Authentifikationsmethoden wie Passwörter sind zudem leicht angreifbar. Dies ist umso mehr ein Problem, als sich Benutzer immer mehr Passwörter merken müssen und deshalb dazu tendieren, Passwörter wiederzuverwenden. Stärkere Authentifikationsmethoden, die auf kryptographischen Zertifikaten oder auf den Geheimnissen innerhalb einer Chipkarte basieren, sind oftmals durch »man in the middle«-Angriffe angreifbar.

Aufgrund der Rahmenbedingungen wird es auch in Zukunft schwierig sein, im Cyberspace das gleiche Authentifikationsniveau zu erreichen wie in der realen Welt. In der realen Welt gibt es sehr viele verschiedene Kanäle, über die man oft unbewusst Authentifikationsinformationen austauscht (Stimme, Körpersprache, Mimik). Ein ähnlich multidimensionales Authentifikationspanorama ist im Cyberspace nur schwer abzubilden.

7.2.3. Selbstdatenschutz

Gerade mit der Diskussion über die so genannten »sozialen Netzwerke« ist das Problem des Datenschutzes verstärkt in den Blickpunkt der Öffentlichkeit gerückt. Das Zusammentragen von Daten und das Erkennen von Beziehungen zwischen einzelnen Informationen im Netz ist eine automatisierbare Aufgabe, die durch Rechner gelöst werden kann. Im Cyberspace ist es also deutlich einfacher, Persönlichkeitsprofile zu erstellen, als in der realen Welt. Das Buch »Database Nation« von S. Garfinkel (2001) führt die realen Möglichkeiten deutlich vor Augen.

In der Praxis sollte man sich also nicht scheuen, nur so wenige Daten wie möglich über sich preiszugeben. In vielen Systemen können pseudonyme Benutzernamen verwendet werden. Da heute oft die E-Mail-Adresse als Benutzerkennung vorgegeben ist, kann es sinnvoll sein, »Wegwerf-E-Mail-Adressen« zu verwenden, die man zu gegebener Zeit wieder löscht. Wenn Postadressen angegeben werden müssen, dann kann es sich bei bestimmten Anbietern lohnen, einen kleinen Buchstabendreher in den Straßennamen oder ein zusätzliches »c/o«-Feld einzubauen. So kann man bei realer Post feststellen, über welche Kanäle der Absender an die eigene Adresse kam.

Es ist durchaus auch sinnvoll, in regelmäßigen Abständen die eigene Online-Präsenz selbst zu kontrollieren, also sich selbst in die Situation eines Detektivs zu begeben, der im Internet möglichst viel über die eigene Person herausfinden möchte.

7.2.4. Schutz in Unternehmen

In Unternehmen hat man in der Regel jemanden zur Hand, der für den technischen Schutz der dort verwendeten informationstechnischen Systeme sorgt. Im Unternehmensumfeld ist dieser Schutz heute zahlreichen Regulierungen unterworfen, so dass es sinnvoll ist, sich an etablierte Rahmenwerke zu halten, wie etwa an den *Grundschutz* des Bundesamtes für Sicherheit in der Informationstechnik.

In der Vergangenheit hat sich jedoch gezeigt, dass ähnlich wie im privaten Bereich auch im Unternehmen eine gewisse Sensibilität für die Andersartigkeit der Gefahren im Cyberspace notwendig ist. Dies wird neudeutsch als »Awareness« bezeichnet. Maßnahmen, die die Awareness erhöhen, sollten bei den Investitionsentscheidungen genauso stark gewichtet sein wie technische Sicherheitsmaßnahmen, wenn nicht sogar stärker. Nur durch eine entsprechende Sensibilität, auch und insbesondere im Management, können die zunehmenden gezielten Angriffe wirksam eingedämmt werden.

7.2.5. CERTs

Viele Institutionen betreiben Abteilungen, deren Aufgabe es ist, Angriffe auf die informationstechnische Systeme zu untersuchen. Diese werden nach dem ersten solchen Team an

der Carnegie Mellon University in den USA als *Computer Emergency Response Teams* (CERTs) bezeichnet. Die Fachleute eines CERT sind für die jeweilige Institution zentrale Ansprechpartner für die operative Sicherheit und werden bei allen relevanten Fragestellungen in den Entscheidungsprozess mit einbezogen. Teilweise obliegen den CERTs auch die Verteilung von Informationen über neue Sicherheitslücken und die Konzeption und Durchführung von Maßnahmen zur Verbesserung der Sensibilität für IT-Sicherheitsfragen im Unternehmen.

CERTs haben sich in der Vergangenheit als effektives und pragmatisches Mittel zur Eindämmung von IT-Sicherheitsgefahren erwiesen. Sie bilden über Organisations- und Ländergrenzen hinweg eine Vernetzungsmöglichkeit, um auf Gefahren kontrolliert und koordiniert zu reagieren. In Deutschland wird der Aufbau von CERTs durch den nationalen CERT-Verbund (DFN-CERT Services GmbH, o. J.) gefördert.

7.2.6. Die Rolle der Internet-Provider

Die Internet-Provider spielen vor allem im Bereich der privaten Nutzer eine Schlüsselrolle beim Umgang mit Cyberkriminalität. So können etwa IP-Adressen nur mit Hilfe der Provider auf den eigentlichen Anschlussinhaber aufgelöst werden. Auch haben die Provider in ihren Netzen die Möglichkeit, bösartige Aktivitäten zu erkennen und zu unterbinden. Im Universitätsnetz der RWTH Aachen werden beispielsweise Computer, die sich so verhalten, als seien sie durch Schadsoftware infiziert, in ein Quarantänenetz verlegt und müssen sich erst wieder physisch »gesund melden«, um am normalen Netzwerkverkehr teilnehmen zu können (Göbel, Holz & Willems, 2007; Hektor & Göbel, 2008). Ähnlich verfahren bereits einige kommerzielle Internet-Provider. Die Erkennung von bösartigem Verhalten führt dann zu einem Hinweis auf das Anti-Botnet-Beratungszentrum des Verbandes der deutschen Internetwirtschaft (eco – Verband der deutschen Internetwirtschaft e.V., o. J.), das Software bereitstellt, um den Rechner zu reinigen.

7.2.7. Kritische Infrastrukturen

Gerade im Unternehmensumfeld oder im Bereich der kritischen Infrastrukturen muss aber immer wieder genau hinterfragt werden, welche Systeme mit dem Internet verbunden sein müssen und welche nicht.

Im Bereich der Automatisierung etwa werden oft Anlagen betrieben, die eine Lebenszeit von 10 bis 20 Jahren haben. Die IT-Infrastruktur wird dabei anfangs installiert und anschließend kaum verändert. Oft werden auch Sicherheitsupdates nicht mehr eingespielt, um keine Funktionsstörungen mit veralteten Peripheriegeräten oder Ähnlichem zu riskieren. Derartige Systeme müssen besonders geschützt werden. Insbesondere müssen diejenigen Wege streng reglementiert werden, über die Software auf diese Systeme gelangen könnte. Ob derartige Systeme dann mit dem Internet verbunden sein sollten, ist mehr als fraglich.

7.3. Materiell-strafrechtlicher Schutz

Diese Studie kann und soll keine juristischen Kommentare und Lehrbücher ersetzen. Daher liegt der Schwerpunkt der folgenden Darstellung *nicht* in einer umfassenden Diskussion der jeweiligen Tatbestandsmerkmale der für die Verfolgung von Cyberkriminalität relevanten strafrechtlichen Tatbestände. Insoweit sei auf die vorhandene Literatur verwiesen (insbesondere M. Gercke & Brunst, 2009; Hilgendorf & Valerius, in Druck; Malek, 2005; Marberth-Kubicki, 2010). Statt dessen sollen bestehende, vermutete und zum Teil nur vermeintliche Schutzlücken, aber auch Überkriminalisierungen einer vertieften Beurteilung unterzogen werden.

Bei dieser Betrachtung seien für die folgende Darstellung sechs Schwerpunkte nach den jeweils zugrunde liegenden Schutzgütern oder -subjekten gebildet, die sich freilich nicht stets trennscharf voneinander abgrenzen lassen:

- Der Schutz der Kinder und Jugendlichen, insbesondere vor sexuellem Missbrauch und sexuellen Übergriffen, sei es das Phänomen des *Grooming* betreffend – der sexuell motivierten Kontaktaufnahme von Pädokriminellen zu Kindern –, sei es kinder- und jugendpornographische Darstellungen betreffend (7.3.1.),
- der Schutz des persönlichen Lebens- und Geheimnisbereiches, aber auch von Geheimnissen der Privatwirtschaft und öffentlicher Stellen, der angesichts aktueller Veröffentlichungen von Plattformen wie WikiLeaks an Aufmerksamkeit gewonnen hat (7.3.2.),
- Meinungs- und Äußerungsdelikte im Internet, die von Beleidigungen über Volksverhetzung hin zur Verbreitung terroristischer Schriften – etwa Anleitungen zum Bau von Sprengsätzen – reichen (7.3.3.),
- der Schutz des Vermögens im engeren Sinne, sei es durch betrügerische Verhaltensweisen, sei es gegen unerlaubtes Glücksspiel, oder sei es durch die unerlaubte Inanspruchnahme von Diensten (7.3.4.),
- der Schutz des geistigen Eigentums durch das Urheber- und Patentrecht und durch sonstige Schutzrechte (7.3.5.) sowie
- der Schutz der informationstechnischen Infrastruktur als solcher, die freilich nicht um ihrer selbst willen geschützt wird, sondern wegen ihrer technischen und wirtschaftlichen Bedeutung sowie wegen der sich im Lichte der genannten Schutzgüter und Schutzsubjekte bietenden Angriffsszenarien. Neben Denial-of-Service-Attacken steht insoweit die Verfügbarkeit von so genannten *Hacking Tools* im Vordergrund (7.3.6.).

7.3.1. Schutz der Kinder und Jugendlichen

Der Schutz von Kindern und Jugendlichen vor sexuellem Missbrauch durch eine strikte Verfolgung der Kinder- und Jugendpornographie ist seit je her *das* in der öffentlichen Wahrnehmung dominierende Thema der Cyberkriminalität; ein Teilaspekt – das so genannte *Grooming* – wird durch die reißerische mediale Inszenierung in den vergangenen Monaten in der Fernsehsendung »Tatort Internet« dabei noch besonders herausgehoben. Neben diesen beiden Deliktsfeldern soll im Folgenden auch kurz auf Aspekte des Kinder- und Jugendschutzes im engeren Sinne eingegangen werden, also auf Vorschriften, welche bestimmte mediale Angebote für Kindern und Jugendlichen verbieten.

Bei aller Dominanz dieses Deliktsfelds in der öffentlichen Wahrnehmung – man könnte auch vom *casus belli* der Diskussionen über »rechtsfreie Räume« im Internet und über neue Ermittlungsbefugnisse sprechen – ist zu berücksichtigen, dass der Kriminalstatistik zufolge diese Delikte nur etwa 3% der im Jahr 2009 begangenen internetbezogenen Straftaten ausmachten (Bundeskriminalamt, 2010, S. 243).

Kinder- und Jugendpornographie

Die Strafvorschriften betreffend kinder- und jugendpornographischer Schriften (§§ 184b, 184c StGB; zum letzten Änderungsgesetz und mit regelungstechnischer Kritik s. Hörnle, 2008; Reinbacher & Wincierz, 2007; Schroeder, 2009) dienen dem Schutz der missbrauchten Kinder und Jugendlichen, auch soweit die Weiterverbreitung bereits bestehenden pornographischen Materials gegenständlich ist: Einerseits führt auch diese Weiterverbreitung zu einer Fortwirkung und Perpetuierung der Rechtsverletzung, andererseits soll – im Sinne eines Marktdelikts – die Nachfrage nach neu erstellten Schriften und daher nach neuen Missbrauchsfällen ausgetrocknet werden (Fischer, 2011, § 184b Rdn. 2 m.w.N.; M. Heinrich, 2005, S. 362; grundsätzlich hierzu Hörnle, 2006). Die Betrachtung als *Marktdelikt* erklärt die Struktur der Tatbestände: Deren ersten drei Absätze belegen dabei die Verbreitung oder sonstige Weitergabe – also gewissermaßen die Aktivseite – mit einer höheren Strafdrohung als die nur indirekt über den Besitz erfasste Passivseite in Abs. 4. Tatobjekt muss dabei eine pornographische Schrift im Sinne des § 11 Abs. 3 StGB sein, die sexuelle Handlungen von, an oder vor Kindern (Alter: bis 14 Jahre, § 184b StGB) oder Jugendlichen (Alter: bis 18 Jahre, § 184c StGB) zum Gegenstand haben.

Pornographie und »Posing«-Fotos Nach in Rechtsprechung und Literatur einhelliger Auffassung sind nicht alle Nacktfotos von Kindern und Jugendlichen verboten, vielmehr nur pornographische Darstellungen – dies ergibt sich bereits aus dem klaren Wortlaut des Gesetzes. Nach der Rechtsprechung liegt Pornographie nur vor, wenn »unter Hintansetzung sonstiger menschlicher Bezüge sexuelle Vorgänge in grob aufdringlicher, anreißerischer Weise in den Vordergrund rücken und ausschließlich oder überwiegend auf die Erregung sexueller Reize abzielen« (BGHSt 37, 55, 60), wobei auch fiktive oder manipulierte Darstellungen genügen (BGHSt 47, 62; BGH NStZ 2000, 307). Nur bei den

besitzbezogenen Delikten (§ 184b Abs. 2, Abs. 4 StGB) ist zudem entweder ein tatsächliches oder ein wirklichkeitsnahes Geschehen erforderlich. Nur als solche erkennbare, ausschließlich virtuelle Darstellungen sind insoweit – nicht aber bei § 184b Abs. 1 StGB – straffrei (vgl. zur virtuellen Kinderpornographie Hopf & Braml, 2007).

Lobenswert ist, dass seit 2008 klargestellt ist, dass das erzwungene sexuell aufreizende Posieren von Kindern als sexueller Missbrauch (§ 176 Abs. 4 Nr. 2 StGB) bestraft werden kann und Bildaufnahmen hiervon als kinderpornographische Schrift gelten können (Hörnle, 2008, S. 3525; Röder, 2010). (Nachweis-)Schwierigkeiten können allerdings verbleiben bei isolierten Großaufnahmen und bei Bildern, die von schlafenden Kindern angefertigt werden. Die von Röder, 2010 vorgeschlagene Erweiterung des § 184b Abs. 1 StGB auf

> sexuell aufreizende Darstellungen der unbedeckten Genitalien [und] des unbedeckten Gesäßes

ist dabei grundsätzlich zu begrüßen. Allerdings erscheint die von ihm vorgeschlagen, entsprechende Änderung auch der §§ 184a, 184c StGB, als nicht in gleichem Maße erforderlich.

Das Erfordernis einer Schrift im Sinne des § 11 Abs. 3 StGB Die §§ 184b, 184c StGB verweisen in ihren Definitionen kinder- und jugendpornographischer Schriften auf § 11 Abs. 3 StGB, so dass neben Druckwerken usw. auch *Datenspeicher* erfasst werden. Eine gewichtige Auffassung in der Literatur möchte nun zwischen dem körperlichen Datenträger und den darauf abgespeicherten Daten – dem Inhalt – unterscheiden (M. Gercke & Brunst, 2009, Rdn. 283; M. Gercke, 2010a; Hörnle, 2010b, S. 706 m.w.N.; Kudlich, 2002, S. 311). Konsequenz davon wäre es, dass jegliches Herunterladen einer kinderpornographischen Bilddatei auf die Festplatte usw. nach § 184b Abs. 4 S. 1 StGB straflos wäre, da der Täter bereits vorher im Besitz dieser Festplatte war (M. Gercke & Brunst, 2009, Rdn. 327), gleichermaßen wäre die Weitergabe an einen anderen nicht von § 184b Abs. 2 erfasst (M. Gercke & Brunst, 2009, Rdn. 334).

Historisch und teleologisch – also dem Sinn und Zweck der Norm gemäß – lässt sich allerdings ohne Weiteres die Gegenauffassung der Rechtsprechung begründen, die neben stofflichen Datenspeichern wie Festplatten auch das technisch-virtuelle Konzept einer Datei erfasst (BGHSt 47, 55, 59; BGH StV 2007, 186; Brodowski, 2011, S. 105; Hilgendorf et al., 2005, Rdn. 267). Daher ist auch der Versuch, sich an einer kinderpornographischen Bilddatei Besitz zu verschaffen – etwa durch das gezielte Herunterladen dieser Datei auf einen USB-Stick – von § 184b Abs. 4 S. 1 StGB erfasst; einer Änderung des § 11 Abs. 3 StGB bedarf es – entgegen der genannten Literaturauffassung – nicht.

Die Austrocknung des Marktes Die Angebots- oder Aktivseite des Marktes an kinder- und jugendpornographischen Schriften ist nach diesem Verständnis des Schriftenbegriffes auch umfassend und adäquat kriminalisiert: Jegliche Verbreitung und jeglicher Tausch – auch in geschlossenen Benutzergruppen – von Bild- und Videodateien ist durch §§ 184b Abs. 1, Abs. 2, 184c Abs. 1, Abs. 2 StGB kriminalisiert, Echtzeitdarbietungen oder Streamingangebote, die nicht zu einem Besitz eines Kunden an einer Bild- oder Videodatei führen, werden über § 184d StGB erfasst. Die gewerbs- oder bandenmäßige Begehung wird dabei mit einer Freiheitsstrafe von bis zu zehn Jahren geahndet (§ 184b Abs. 3 StGB).

Auf die Nachfrage- oder Passivseite des Marktes adäquat und angemessen zu reagieren, bereitet noch erhebliche Schwierigkeiten. Dabei gilt es aus grundsätzlicher Sicht erstens, Verdachtsstrafen zu vermeiden (s. hierzu Schroeder, 1990) und zweitens, Ermittlungsverfahren ressourcenschonend nur dort einzusetzen, wo es wirkliche Kunden von Kinder- oder Jugendpornographie gibt (vgl. auch Müller, 2010, S. 345). Drittens sollte sich die strafrechtliche Ahndung auf die durch die Nachfrage verursachten spezifischen Gefahren konzentrieren, namentlich auf die Finanzierung der Kinderpornographie (Brodowski, 2011, S. 107 f.): Die im Gesetzgebungsverfahren geäußerte Befürchtung, der Konsum kinderpornographischer Schriften rege zum Kindesmissbrauch an (BT-Drucks. 12/3001, S. 6), ließ sich bislang nicht belegen (Endrass et al., 2009).[1]

Nach geltendem Recht erfasst ist auf der Nachfrageseite der *Besitz* einschlägiger Schriften sowie die *Besitzverschaffung*, einschließlich des Versuches. Die Rechtsprechung lässt es dabei genügen, wenn sich entsprechende Dateien im Zwischenspeicher (Cache) des Browsers befinden und der Täter zumindest rudimentäres Wissen über die Funktionsweise dieses Caches hat. Weder mit dem Wortlaut, der Systematik noch mit der Teleologie der §§ 184b Abs. 4, 184c Abs. 4 StGB vereinbar ist allerdings eine obergerichtliche Auffassung, dass bereits der bewusste und gewollte Aufruf von Internetseiten kinderpornographischen Inhalts eine versuchte Besitzverschaffung sei (OLG Hamburg NStZ 2010, 704 = StV 2011, 99 m. abl. Anm. Brodowski, 2011; Hörnle, 2010b; Müller, 2010). Zur zielgerichteten Erfassung des strafwürdigen ökonomischen Anreizes, der durch die Finanzierung von kinderpornographischen Schriften bewirkt wird, sei eine Erweiterung der §§ 184b Abs. 4, 184c Abs. 4 StGB auf den Ankauf und den entgeltlichen Erwerb einer Zugangsmöglichkeit angeregt (umfangreiche Begründung in Brodowski, 2011, S. 107 f.; insoweit zustimmend Hörnle, 2010b, S. 706):

[1] Nur bei bestimmten Hochrisikogruppen sei eine positive Korrelation zwischen (legalem) Pornographiekonsum und sexueller Gewalt gegeben, wobei zugleich vor vorschnellen Schlüssen, was Ursache, was Wirkung sei, gewarnt wurde (Hill, Briken & Berner, 2006; Malamuth, Addison & Koss, 2000, S. 26 ff., insb. S. 84 f.; Vega & Malamuth, 2007, S. 115).

Wer es unternimmt,

1. kinderpornographische Schriften anzukaufen, die ein tatsächliches oder wirklichkeitsnahes Geschehen wiedergeben,
2. Zugang zu solchen Schriften entgeltlich zu erwerben, oder
3. sich den Besitz von solchen Schriften zu verschaffen,

oder wer

4. solche Schriften besitzt,

wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

Noch disparater ist die Angebots- und Nachfrageseite bei der Erfassung von Echtzeit-Darbietungen und Streamingangeboten, bei denen es nicht notwendigerweise zu einer Speicherung von Bild- und Videodateien auf den informationstechnischen Systemen des Betrachters kommt. Entgegen der vorherrschenden Auffassung in der Literatur (vgl. etwa M. Gercke & Brunst, 2009, Rdn. 348 m.w.N.) enthält der Wortlaut und die Teleologie des § 184d StGB keine Einschränkung auf Echtzeitdarbietungen; auch die Systematik gebietet es, verzögerte Übertragungen jedenfalls dann zu erfassen, wenn – wie bei Streamingangeboten – aufgrund der technischen Vorgänge kein Verbreiten einer Schrift gegeben ist. Regelungsbedarf besteht dennoch: Erstens, weil diese Norm keine Darbietungen für einzelne oder wenige Personen erfassen dürfte (Fischer, 2011, § 184d Rdn. 4), und zweitens, weil die Nachfrage nach derzeitiger Rechtslage nicht nach § 184d StGB (ggf. aber über §§ 176 ff. StGB) strafbar ist (Fischer, 2011, § 184d Rdn. 6, 9). Auch hier ist schutzzweckbezogen auf den ökonomischen Anreiz abzustellen, so dass folgende Neufassung des § 184d StGB angeregt sei (Änderungen kursiv hervorgehoben):

(1) Nach den §§ 184 bis 184c wird auch bestraft, wer eine pornographische Darbietung durch Rundfunk oder *durch elektronische Informations- und Kommunikationsdienste* verbreitet. In den Fällen des § 184 Abs. 1 ist Satz 1 bei einer Verbreitung *durch elektronische Informations- und Kommunikationsdienste* nicht anzuwenden, wenn durch technische oder sonstige Vorkehrungen sichergestellt ist, dass die pornographische Darbietung Personen unter achtzehn Jahren nicht zugänglich ist.

(2) *Wer es unternimmt, gegen Entgelt auf eine pornographische Darbietung nach Absatz 1 in Verbindung mit § 184b zuzugreifen, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.*

Spezifische Aspekte der Erfassung jugendpornographischer Schriften Die 2008 erfolgte Ausweitung auf jugendpornographische Schriften wirft gleich mehrere – nicht spezifisch internettypische – Fragen auf. So dürfte es erstens schlicht unmöglich sein, das äußere Erscheinungsbild einer unbekannten 17½jährigen von einer 18jährigen Person zu unterscheiden. Hier hilft allerdings eine restriktive Auslegung, wie sie auch das Bundesverfassungsgericht (MMR 2009, 178) fordert: Ist das Alter der abgebildeten Personen nicht bekannt, so besteht ein Strafbarkeitsrisiko auch nach § 184c StGB nur, wenn sie »ganz offensichtlich noch nicht volljährig sind, etwa dann, wenn sie (fast) noch kindlich wirken« und somit die Darstellungen in die Nähe des § 184b StGB geraten (krit. Liesching, 2009). § 184c StGB wird damit in der Praxis vermehrt zu einem Auffangtatbestand, wenn der Nachweis, eine abgebildete Person sei noch ein Kind, nicht zu führen ist. Die hierdurch bewirkte, effektivere Verfolgung der Kinderpornographie geschieht freilich mit dem Risiko einer gewissen Überkriminalisierung von Jugendlichen, die etwa eine selbst von sich hergestellte Aufnahme ihrem Freund oder ihrer Freundin aushändigen (s. Hörnle, 2008, S. 3524; Reinbacher & Wincierz, 2007, S. 197, jew. auch zu weiteren Kritikpunkten an § 184c StGB).

Grooming

Mit Grooming bezeichnet man das Phänomen, dass Pädokriminelle über elektronische Kommunikationsformen – etwa Chatrooms – Kontakt mit Kindern aufbauen, diese zu Treffen überreden und sodann auch sexuell missbrauchen (M. Gercke, 2010a, S. 798). Ohne Weiteres erfasst das geltende Strafrecht den sexuellen Missbrauch; strittig ist allein, ob bereits die Vorbereitungshandlungen des Kontaktaufbaus und des Überredens zu Treffen unter Strafe gestellt sind. Dreh- und Angelpunkt hierbei ist die Auslegung des § 176 Abs. 4 Nr. 3 StGB, der die Einwirkung mit Schriften auf ein Kind unter Strafe stellt, wenn diese von einer sexuellen Absicht getragen ist, aber auch des § 176 Abs. 4 Nr. 4 StGB, soweit der Täter durch pornographische Abbildungen auf das Kind einwirkt.

Eine erste Strafbarkeitslücke – allerdings nicht betreffend der Internetkriminalität – ergibt sich daraus, dass § 176 Abs. 4 Nr. 3 StGB an der Einwirkung durch *Schriften* anknüpft, und daher eine mündliche Verabredung mit einem Kind zu einem sexuellen Treffen nicht erfasst wird (Perron & Eisele, 2010, § 176 Rdn. 14). Darüber hinaus ist hier der Schriftenbegriff auch problematisch, weil dieser eine gewisse Verkörperung des Gedankeninhalts – etwa in einer Datei – voraussetzt und daher die flüchtige Kommunikation in Chatrooms oder durch (Internet-)Telefonate nicht erfasst, wohl aber eine E-Mail-Kommunikation (noch weiter einschränkend M. Gercke, 2010a, S. 802; relativierend Duttge, Hörnle & Renzikowski, 2004, S. 1067 f.). Eine maßvolle Erweiterung auf weitere Kommunikationsformen erscheint daher geboten, etwa durch folgende Neufassung des § 176 Abs. 4 Nr. 3 und Nr. 4 (Änderungen kursiv hervorgehoben):

3. auf ein Kind durch Schriften (§ 11 Abs. 3) *oder durch die Übermittlung von Daten (§ 202a Abs. 2)* einwirkt, um es zu sexuellen Handlungen zu bringen, die es an oder vor dem Täter oder einem Dritten vornehmen oder von dem Täter oder einem Dritten an sich vornehmen lassen soll, oder
4. auf ein Kind durch Vorzeigen pornographischer Abbildungen, Darstellungen *oder Schriften (§ 11 Abs. 3)*, durch Abspielen von Tonträgern pornographischen Inhalts oder durch entsprechende Reden einwirkt.

Eine zweite, allerdings nur vermeintliche Strafbarkeitslücke resultiert aus dem Verzicht auf eine Versuchsstrafbarkeit. Da bereits die Einwirkung auf ein Kind vom Tatbestand erfasst ist, und es allein einer weitergehenden Absicht des Täters bedarf, liegt bereits eine erhebliche Vorverlagerung der Strafbarkeit vor. Mangels Versuchsstrafbarkeit straflos sind daher nur Konstellationen, in denen der Täter mit einem Jugendlichen oder Erwachsenen kommuniziert, der sich als Kind ausgibt, oder aber Fälle, in denen das Kind die Kommunikation nicht wahrnimmt – etwa, weil die E-Mail das Kind nicht erreicht. Auch wenn die öffentlichkeitswirksame Fernsehsendung »Tatort Internet« gegensätzliches behauptet, besteht daher kein Änderungsbedarf.

Kinder- und Jugendschutz im engeren Sinne; Cyberstalking und Cybermobbing

Pornographieverbote Dem – abstrakten – Jugendschutz dienen zunächst die Pornographieverbote der §§ 184, 184a StGB. Zwar ist wissenschaftlich hoch umstritten, ob die Kenntnisnahme oder Konfrontation mit »einfacher« oder »harter« Pornographie zu persönlichkeitsschädigenden Entwicklungen führt (vgl. BVerfGE 83, 130, 140 ff.; BVerfG MMR 2010, 48). Da aber bei entsprechender Prädeterminierung (genetische Disposition, soziales Umfeld) ein entsprechendes Risiko nicht auszuschließen ist, durfte der Gesetzgeber in gewissem Rahmen abstrakte Gefährdungsdelikte einführen. Dabei existieren durchaus Wertungswidersprüche, auf die der Bundesgerichtshof ausdrücklich hingewiesen hat (BGH NJW 1998, 1162); auch kann die Zweckmäßigkeit der Ausnahmeklauseln im Lichte der umfassenden Verfügbarkeit ausländischer pornographischer Angebote im Internet angezweifelt werden. Strafbarkeits*ausdehnender* Handlungsbedarf besteht insoweit aber jedenfalls nicht.

Entwicklungsstörende Angebote Die Strafvorschrift des Staatsvertrags über den Schutz der Menschenwürde und den Jugendschutz in Rundfunk und Telemedien (Jugendmedienschutz-Staatsvertrag – JMStV; s. hierzu Lober, 2005), die auch durch die gescheiterte Novelle unangetastet bleiben sollte, knüpft nicht an bestimmte Inhalte – wie Pornographie – an, sondern erfasst generell Telemedienangebote, die »offensichtlich geeignet sind, die Entwicklung von Kindern oder Jugendlichen oder ihre Erziehung zu einer eigenverantwortlichen und gemeinschaftsfähigen Persönlichkeit unter Berücksichtigung

der besonderen Wirkungsform des Verbreitungsmediums schwer zu gefährden« (§ 23 JMStV). Angesichts des offenen Wortlauts ist bei der Handhabung dieser Strafvorschrift Restriktion geboten, und primär auf die speziellen Straftatbestände – auch etwa bezüglich Gewaltdarstellungen (§ 131 StGB) – und auf die Bußgeldvorschriften in § 24 JMStV abzustellen. Ob letztere Norm und deren gescheiterte Novellierung, etwa die ahndbare Verpflichtung zur Benennung eines Jugendschutzbeauftragten für alle inländischen Internetangebote (§ 24 Abs. 1 Nr. 11 JMStV-E), über alle Zweifel erhaben sind, bedarf im Zuge der Neuauflage der Novellierung einer vertieften Analyse.

Cyberstalking und Cybermobbing Die Gefahren eines auf das Internet verlagerten Cyberstalking (Hilgendorf & Hong, 2003; Hoffmann, 2006) und Cybermobbing (Fawzi, 2009), insbesondere für Kinder und Jugendliche, dürfen nicht unterschätzt werden. Diese sind zwar nicht ein qualitativ neues, dafür aber ein quantitatives Problem geworden. Das mag zum einen an gesellschaftlichen Entwicklungen liegen, zum anderen aber auch an der von Tätern im Internet wahrgenommenen, vermeintlichen Anonymität und der physischen Distanz, welche auf die Täter enthemmend wirken kann.

Rechtlich ist die Reaktion auf Stalking und Mobbing (zu den Unterschieden zwischen diesen beiden Phänomenen vgl. Bieszk & Sadtler, 2007) deswegen schwierig, weil hier die Übergänge von sozial anerkanntem Verhalten über lästige Erscheinungen bis hin zu kriminellen Verhaltensweisen fließend und situationsbezogen zu beurteilen sind. Zunächst sind hier die bestehenden gesellschaftlichen und auch zivilrechtlichen Möglichkeiten – etwa das Gewaltschutzgesetz oder die Unterlassungsansprüche (s. hierzu OLG Köln MMR 2008, 672; Ernst, 2009, S. 1321; Peifer & Kamp, 2009) – zu nutzen. Wo aber die Schwelle zu einer Beleidigung (§ 185 StGB) oder zu einer üblen Nachrede (§ 186 StGB) überschritten ist, so stehen Straftatbestände zur Verfügung (s. unten 7.3.3., S. 102), ebenso bei Eingriffen in den persönlichen Lebens- und Geheimbereich nach den §§ 201 ff. StGB (s. sogleich 7.3.2.) und schließlich auch bei kriminellen Nachstellungen (§ 238 Abs. 1 StGB): Bei allen Schwächen dieses Tatbestands (Mitsch, 2007; Valerius, 2007b) und dessen Anwendung in der Praxis (Peters, 2009) erfasst er sämtliche Kontaktaufnahmen »unter Verwendung von Telekommunikationsmitteln« (Nr. 2), also auch und gerade Nachstellungen im Internet. Strafrechtlicher Korrekturbedarf ist daher derzeit nicht zu beobachten.

7.3.2. Daten- und Geheimnisschutz

Der Schutz von elektronisch gespeicherten Geheimnissen im speziellen und der Vertraulichkeit und Integrität informationstechnischer Systeme (vgl. BVerfGE 120, 274) im generellen ist von evidenter Bedeutung: Sei es in der Wirtschaft, etwa zur Abwehr von Industriespionage, sei es in der Exekutive und der Politik, etwa zur Vermeidung illegitimer und zu weit gehender Weitergabe interner Informationen, aber sei es auch zur

Gewährleistung vertraulicher, privater Rückzugs- und Kommunikationsräume (s. oben 4.5.2., S. 49; vgl. ferner Hoffmann-Riem, 2009).

Diesbezüglich war zwischenzeitlich eine Erosion des politischen und gesellschaftlichen Bewusstseins für den Datenschutz festzustellen. Für Privatpersonen galt es als schicklich, sich im Internet und insbesondere in sozialen Netzwerken zu inszenieren (vgl. Hoeren, 2010; Wagner, 2008); für den Staat galt es als alternativlos, sämtliche irgendwie verfügbaren Daten zu erheben, zu sichern und für präventive sowie repressive Zwecke nutzbar zu machen. Nunmehr ist aber ein gewisses, langsames Umdenken zu verzeichnen, hin zu einem umfassenden Bewusstsein für Datenschutz, für eine Begrenzung staatlicher Zugriffsrechte und auch für eine Evaluierung, ob eine umfassende Verfügbarkeit aller Daten für Gefahrenabwehr- und Strafverfolgungszwecke wirklich mit einem Sicherheitsgewinn verbunden ist.

Doch noch immer bestehen – bisweilen auch selbstverschuldete – Bedrohungslagen für Private, sei es durch zu unsichere Handhabung von informationstechnischen Systemen, sei es durch eine zu exzessive Nutzung von Bonusprogrammen, sei es durch exzessive Preisgabe von Informationen und mittelfristig nachteiliger Fotos in sozialen Netzwerken und durch ein unzureichendes Bewusstsein dafür, dass eine vollständige Löschung von einmal preisgegebenen Inhalten im Internet oft nicht mehr als ein Wunschtraum ist.

Für Unternehmen und die Exekutive wiederum ergeben sich aus zwei Richtungen erhebliche Herausforderungen: Erstens richten sich gegen sie gezielte, wirtschaftlich motivierte (Spionage-)Angriffe. Zweitens aber haben sie ein Geheimhaltungsinteresse an zum Teil misslichen, zum Teil sensiblen Informationen; dies steht im Konflikt zu dem legitimen, öffentlichen Interesse an politischen und gesellschaftlichen Vorgängen und Missständen. Die Möglichkeiten zur Teilhabe und zur Veröffentlichung von solchen Missständen haben durch die wahrgenommene Anonymität, die dezentrale Struktur des Internets und Plattformen wie WikiLeaks eine neuartige Dimension erlangt.

Den strafrechtlichen Schutz von elektronisch gespeicherten Geheimnissen und Daten bezweckt ein komplexes Puzzle an Tatbeständen, je nach Täterkreis, Art des Geheimnisses und Art der Kenntniserlangung. Diese können auch zusammentreffen mit den Straftatbeständen etwa des Urheber- und des Patentrechts (s. unten 7.3.5., S. 109), ferner mit manchen Vorbereitungsdelikten (s. unten 7.3.6., S. 117). Insgesamt ist der materiellstrafrechtliche Schutz in Zwei-Personen-Konstellationen als weit reichend und ausreichend, wenn nicht gar als zu weit gehend zu beurteilen; Schutzlücken sind hingegen in Drei-Personen-Konstellationen zu verzeichnen. Zu monieren ist allerdings ein Vollzugsdefizit, das im Wesentlichen aus einer fehlenden Anzeigebereitschaft der Wirtschaft resultieren dürfte (so auch Kiethe & Hohmann, 2006, S. 185; Többens, 2000, S. 511 f.).

Betriebs- und Geschäftsgeheimnisse, Wirtschaftsspionage und Konkurrenzausspähung

Die zentralen Normen zur Verfolgung von (staatlicher) Wirtschaftsspionage und (privater) Konkurrenzausspähung finden sich nicht im StGB, sondern in §§ 17 ff. UWG (Bär, 2007a, Rdn. 95 ff.; Möhrenschlager, 2007.) Diese Normen beziehen sich sachlich auf Geschäfts- und Betriebsgeheimnisse, also unternehmensbezogene Informationen, die nicht offenkundig, sondern nur einem begrenzten Personenkreis zugänglich sind und an deren Nichtverbreitung der Rechtsträger ein berechtigtes Interesse hat (BVerfG MMR 2006, 375, 376), also beileibe nicht auf sämtliche unternehmensbezogene oder in einem Unternehmen gespeicherten Daten.

Persönlich bezieht sich § 17 Abs. 1 UWG auf unternehmens*interne* Angriffe, wobei der Beschäftigte das Geheimnis zudem »zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Unternehmens Schaden zuzufügen« weitergeben muss. Nach Auffassung der Literatur soll »zugunsten eines Dritten« auch handeln, wer ideologische (BT-Drucks. 10/5058, S. 40) oder umweltpolitische Motive verfolge (so Janssen & Maluga, 2010, § 17 UWG Rdn. 63). Zwar erscheint eine solch weit gehende Auslegung bereits mit dem Wortlaut des § 17 UWG nicht vereinbar. Dennoch verbleibt ein zu hohes Strafbarkeitsrisiko für Personen, die eklatante Missstände innerhalb von Unternehmen aufdecken möchten, insbesondere wenn die Literatur hier einen strengen Maßstab – etwa den des § 138 StGB – anlegen möchte (in diese Richtung Janssen & Maluga, 2010, § 17 UWG Rdn. 67). Dies ist nicht mehr zeitgemäß, und so wäre es höchst wünschenswert gewesen, wenn es bereits vor Monaten zu einer Weitergabe derjenigen Testergebnisse gekommen wäre, die eine Belastung von Tierfuttermittel mit Dioxin ergeben hatten (s. hierzu noch sogleich S. 96).

§ 17 Abs. 2 UWG wiederum erfasst unternehmens*externe* Angriffe, wobei die Betriebsspionage (Nr. 2) umfassend strafrechtlicher Verfolgung unterliegt, auch wenn informationstechnische Systeme zur Angriffsbegehung eingesetzt werden (lit. a). Die so genannte Geheimnishehlerei (§ 17 Abs. 2 Nr. 2 UWG) hingegen setzt eine wirtschaftliche Verwertung – eine Verwertung für Strafverfolgungszwecke ist daher nicht erfasst – oder eine weitere Perpetuierung durch Weitergabe an eine dritte Person voraus.

Eine Zwischenstellung erfassen nun die §§ 203, 204 StGB: So erfahren etwa Rechtsanwälte, Wirtschaftsprüfer, Steuerberater und auch Amtsträger regelmäßig von Betriebs- und Geschäftsgeheimnissen. Diese Personen sind zugleich zu besonderer Verschwiegenheit verpflichtet und berechtigt (vgl. exemplarisch die Zeugnisverweigerungsrechte in § 53 Abs. 1 StPO). Die Offenbarung und (wirtschaftliche) Verwertung von Betriebs- und Geschäftsgeheimnissen durch diese Personengruppen ist allerdings mit deutlich niedrigerer Strafe bedroht als die zuvor genannten unternehmensinternen und -externen Angriffe. Ob dies der besonderen Vertrauensstellung von Amtsträgern und der weiteren genannten Berufsgruppen angemessen ist, muss dabei angezweifelt werden.

Auch ist grundsätzlich anzuregen, die §§ 17 ff. UWG in das StGB – etwa in den fünfzehnten Abschnitt – zu übernehmen (Scheffler & Dressel, 2000, S. 517; Többens, 2000, S. 512), um die Bedeutung des Geheimnisschutzes weiter hervorzuheben und ins Bewusstsein nicht nur der Unternehmen, sondern auch der Strafverfolgungsbehörden zu rücken. Dabei könnte zugleich eine Angleichung an die §§ 202a, 204 StGB und auch an § 159 StGB erfolgen. Wesentlicher materiell-rechtlicher Änderungsbedarf ist derzeit aber nicht gegeben (so auch Kiethe & Hohmann, 2006; Többens, 2000).

Staats- und Dienstgeheimnisse

Ebenfalls umfassend materiell-strafrechtlich gewährleistet ist der Schutz von Staatsgeheimnissen (§§ 93 ff. StGB), von Dienstgeheimnissen (§ 353b StGB) und von Privatgeheimnissen, die Amtsträgern bekannt geworden sind (§ 203 StGB). Der mit deutlich härterer Strafe bedrohte Verstoß gegen § 353b StGB setzt dabei zwar dem Wortlaut zufolge eine konkrete Gefahr eines Nachteils für gewichtige öffentliche Interessen voraus (BGHSt 11, 402); die Rechtsprechung will aber bereits eine mittelbare Gefährdung genügen lassen, etwa wenn »das Vertrauen der Allgemeinheit in die Unparteilichkeit, Unbestechlichkeit und Funktionsfähigkeit der öffentlichen Verwaltung erschüttert wird« (vgl. Fischer, 2011, § 353b Rdn. 13a m.w.N.). Dass dies im Lichte des bisweilen erforderlichen *Whistleblowing* – dem Aufdecken von Missständen außerhalb des innerbehördlichen Geschäftswegs – eine ausgesprochen harte Sichtweise ist, gilt es sogleich noch vertieft zu betrachten.

Schutz der Presse, Informationsfreiheit und Whistleblowing

Nach bisheriger Rechtsprechung ergibt sich ohne Weiteres die Möglichkeit, dass sich nicht nur die Beschäftigten von Unternehmen nach § 17 Abs. 1 UWG und Amtsträger nach § 353b StGB strafbar machen, wenn sie die Presse über (vermeintliche) Missstände informieren (vgl. auch Király, 2010), sondern auch Journalisten, die sodann die Geheimnisse veröffentlichen (vgl. Fischer, 2011, § 353b Rdn. 14a). Der verfassungsrechtlich – über Art. 5 GG – und strafprozessual – über die Zeugnisverweigerungsrechte des § 53 Abs. 1 Nr. 5 StPO und das Beschlagnahmeverbot des § 97 Abs. 5 StPO – gewährleistete Schutz erwies sich dabei in der Vergangenheit als mangelhaft; eine Rechtfertigung eines Geheimnisverrats – auch bei Missständen – wurde nur sehr zurückhaltend angenommen, und die juristisch nicht über alle Zweifel erhabene Konstruktion einer »sukzessiven Beihilfe« wurde bereitwillig genutzt, um über die Strafverfolgung der Journalisten auch die Täter des Geheimnisverrats zu ermitteln.

Daher ist es vollumfänglich zu begrüßen, dass die Bundesregierung (BR-Drs. 538/10) und auch die Opposition (BT-Drs. 17/3989) Gesetzentwürfe zur Stärkung der Pressefreiheit im Straf- und Strafprozessrecht eingebracht haben. Diese konzentrieren sich allerdings auf eine Straffreistellung der Beihilfe zu § 353b StGB und lassen daher einen zweiten, wesentlichen Bereich außen vor: die Stärkung der Pressefreiheit auch dann, wenn die

Presse Missstände in der Wirtschaft aufdeckt und es dabei auch zur Veröffentlichung von Geschäfts- und Betriebsgeheimnissen kommt (zur zivil- und arbeitsrechtlichen Seite s. Deiseroth & Derleder, 2008). Beispielhaft seien die aktuellen Vorfälle bezüglich Tierfuttermittel herangezogen, denn auch hier wäre es wünschenswert gewesen, wenn die Presse Informationen über solches strafwürdiges Verhalten ohne Furcht vor einer (Beihilfe-) Strafbarkeit hätte veröffentlichen können. Es sei daher angeregt, diese Gesetzentwürfe um Verweisungen in §§ 17, 19 UWG

> § 353b Absatz 3a des Strafgesetzbuches findet entsprechende Anwendung.

und auch in § 203 StGB zu ergänzen:

> § 353b Absatz 3a findet bezogen auf Betriebs- und Geschäftsgeheimnisse entsprechende Anwendung.

Darüber hinausgehend stellen sich aber auch grundsätzliche Fragen zur Sicherung der Presse-, Meinungs- und Informationsfreiheit, die sich selbst innerhalb der Europäischen Union Gefährdungen ausgesetzt sieht. Erstens ist es für eine mündige, informierte Öffentlichkeit als Grundlage eines demokratischen Gemeinwesens erforderlich, dass Missstände und Versäumnisse auch außerhalb des exekutiven und gubernativen Meldeweges veröffentlicht werden dürfen, wenn andere Abhilfe nicht oder nur unter Inkaufnahme persönlicher Nachteile möglich ist, etwa wenn eine Information von Vorgesetzten als »Anschwärzen« diffamiert wird und daher berufliche Nachteile drohen. Dies darf aber zugleich kein Freibrief sein, sämtliche, auch belanglose und harmlose Dokumente frei zu veröffentlichen; auch Plattformen wie WikiLeaks sollten dann und nur dann Schutz genießen, wenn sie sich auf die Veröffentlichung von Missständen und Versäumnissen konzentrieren.

Zweitens ist die demokratische Bedeutung des Informationsinteresses auch bei der praktischen Anwendung der Informationsfreiheitsgesetze zu berücksichtigen (erfreulich nun aber OVG Berlin-Brandenburg, Urt. v. 5.10.2010 – 12 B 5.08 –) und gewisse Beeinträchtigungen von Geheimhaltungsinteressen von Unternehmen und Privatpersonen hinzunehmen, insbesondere wenn andernfalls eine parlamentarische und öffentliche Kontrolle nicht möglich ist. Drittens aber ist in besonderer Weise auch auf die Gefahren hinzuweisen, die der Pressefreiheit von privater Seite drohen; ob sich der »fliegende Gerichtsstand« – dass sich vermeintliche Opfer den Gerichtsstand zur zivilrechtlichen Abwehr nahezu frei aussuchen dürfen – auch in Zeiten der Internet-Medienlandschaft bewährt, muss angezweifelt werden.

Schutz der privaten Lebensgestaltung

Zum engeren Bereich der Privatsphäre zählende Bild- und Tonaufnahmen sind nach §§ 201, 201a StGB strafbar, auch wenn diese etwa durch eine Manipulation eines in einer Wohnung befindlichen Computers bewirkt werden. Angriffsszenarien etwa, dass Pädokriminelle auf in Kinder- und Jugendzimmern befindliche Rechner zugreifen, um mittels »Webcam« Videoaufzeichnungen vorzunehmen, sind daher bereits umfassend und auch adäquat unter Strafe gestellt. Trotz mancher nicht unberechtigter Kritik an der konkreten Ausgestaltung des § 201a StGB (vgl. hierzu Fischer, 2011, § 201a Rdn. 2, 14 f., 29; s. ferner Eisele, 2005) ist derzeit zur Verfolgung von Cyberkriminalität kein Änderungsbedarf ersichtlich.

Das Strafrecht ist hingegen ein nur stumpfes Schwert zum allgemeinen Schutz personenbezogener Daten: Zwar stellt § 44 BDSG manche Verstöße gegen das Datenschutzrecht unter Strafe; praktische Bedeutung hat diese Norm aber bislang quasi nicht erlangt. Viel spricht aber dafür, dass hier das Ordnungswidrigkeiten- und Ordnungsrecht eine adäquatere Reaktion auf wirtschaftlich motivierte Verstöße gegen das Datenschutzrecht verspricht; in Teilbereichen – soweit Daten einem Dienstleister *anvertraut* werden – ist aber über personenbezogene Daten hinaus ein besserer Schutz als derzeit zu gewährleisten (s. hierzu sogleich S. 101).

(Auffang-)Schutz informationstechnischer Systeme

Neben diesen bereichsspezifischen Strafbestimmungen treten schließlich die weit reichenden §§ 202a Abs. 1, 202b, 206 StGB zum Schutz von einzelnen informationstechnischen Systemen, aber auch zum Schutz von Datenübertragungen zwischen informationstechnischen Systemen.

Einzelnes informationstechnisches System Angriffe auf einzelne informationstechnische Systeme werden nicht als solche vom Straftatbestand des § 202a Abs. 1 StGB erfasst, sondern erst, wenn sich der Täter auch tatsächlich eine unbefugte Zugangsmöglichkeit – besser: *Zugriffs*möglichkeit – zu Daten verschafft. Auf den Inhalt dieser Daten kommt es dabei nicht an; erfasst werden neben Geheimnissen daher auch offenkundige Daten, verschlüsselte Daten, dem Täter ebenfalls bekannte Daten und sogar belanglose, inhaltsleere Daten. Zwei sinnvolle Einschränkungen sind aber bezüglich der konkreten Tathandlung in § 202a Abs. 1 StGB enthalten: Der Täter muss sich Zugriff schaffen auf Daten, die nicht für ihn bestimmt sind, und dies muss unter Überwindung einer Zugangssicherung geschehen.

Ob Daten für jemanden bestimmt sind, richtet sich zunächst nach dem Willen dessen, der zur *Verfügung* über die Daten *berechtigt* ist (M. Gercke & Brunst, 2009, Rdn. 93; Hilgendorf, 2010b, § 202a Rdn. 20 ff.; jew. m.w.N.). Das ist im Ausgangspunkt der Skribent, also derjenige, der die entsprechenden Daten originär gespeichert hat oder

hat abspeichern lassen. Die zivilrechtliche Eigentumslage am Datenträger ist hingegen genauso unerheblich wie die Frage, auf wen sich die Daten beziehen. Die Verfügungsberechtigung über Daten kann jedoch – nach zivilrechtlichen Grundsätzen – übertragen werden; so können etwa Datenbestände verkauft werden. Von dieser Übertragung der Verfügungsberechtigung zu unterscheiden ist die – weitaus häufigere – Einräumung einer *Zugriffsberechtigung* (M. Gercke & Brunst, 2009, Rdn. 93; Graf, 2003, § 202a Rdn. 18). Dies erfolgt erneut nach zivilrechtlichen Grundsätzen. So erwirbt man mit dem Kauf einer Software die Berechtigung, diese zu nutzen, also Kopien der Programmdaten auf dem eigenen Rechner zu installieren und – bei Ausführen des Programms – durch das Betriebssystem diese Programmdaten in den Arbeitsspeicher laden zu lassen. Gleiches gilt für die Einräumung eines Zugriffs auf eine nichtöffentliche Datenbank, etwa über das Internet. Die Nutzung dieser Datenbank und der dort hinterlegen Daten ist daher für den Berechtigten (Vertragspartner) jedenfalls im Rahmen des ihm Eingeräumten straflos.

Umstritten und noch weitgehend ungeklärt sind allerdings die Konstellationen, in denen ein prinzipiell Berechtigter die Daten unter Verstoß gegen die zivilrechtliche Bestimmung nutzt. Einer Auffassung zufolge sind Bedingungen und Befristungen bei der Einräumung solcher Zugriffsberechtigungen vollständig wirksam, soweit sie sich auf den Zugang als solchen beziehen und nicht auf die bloße Zweckbestimmung des Zugangs (Graf, 2003, § 202a Rdn. 19 f.). Eine andere Ansicht unterscheidet zwischen der Einräumung einer Nutzungsberechtigung und dem Zugänglichmachen von Daten (Lenckner & Eisele, 2010, § 202a Rdn. 6). Dieser Auffassung nach ist etwa an Bankkarten die Nutzung der Daten – vermittelt über Bankautomaten oder Zahlungsterminals – gestattet, nicht jedoch der eigene Zugriff auf die dort abgespeicherten Daten. Diese Differenzierungen können jedoch nicht überzeugen: Auch bei fehlender unmittelbarer Wahrnehmung mancher Informationen bei bloßer »Nutzung« werden ebendiese Daten einem zur Hilfe genommenen informationstechnischen System zugänglich gemacht. Die bloße Auslagerung der Zugänglichmachung auf ein informationstechnisches System kann diese Zurechnung nicht durchbrechen. Vorzugswürdig erscheint es, Bedingungen und Befristungen bei Zugriffsberechtigungen nur zu akzeptieren, soweit sie sich auf die *Art* des Zugriffs beziehen. So kann man erneut das Auslesen von Daten von einer Bankkarte und könnte damit grundsätzlich das *Skimming* strafrechtlich über § 202a Abs. 1 StGB erfassen – wenn denn die Daten auf einem Magnetstreifen besonders gesichert wären (BGH NStZ 2010, 275; BGH JR 2010, 497) –, ebenso das *Hacking* von Computersystemen. Hierdurch vermeidet man allerdings auch eine zu weit gehende Kriminalisierung von wenig schwer wiegenden Überschreitungen einer zivilrechtlich eingeräumten Zugriffsmöglichkeit.

Taugliches Tatobjekt sind ferner nur Daten, die gegen unberechtigten Zugriff besonders geschützt sind. Diese Sicherung muss sich zwar spezifisch auf die Daten beziehen, kann aber durch verschiedenste physische oder technische Methoden verwirklicht werden. Einen besonderen Schutz können aber nur Sicherheitsmechanismen bieten, die von einem Durchschnittsbenutzer, der den Stand der Technik beherrscht, nicht in trivialer Weise

überwunden werden können, wie etwa der Zugriff auf die auf einem Magnetstreifen einer Bankkarte gespeicherten Daten (BGH NStZ 2010, 275; BGH JR 2010, 497; s. hierzu noch unten 7.3.4., S. 107). Zu hohe Anforderungen an die Datensicherung gingen fehl: Denn ist der technische Schutz bereits hoch genug, so laufen Angriffe ohnehin ins Leere. Rechtlichen Schutzes bedürfen daher gerade Sicherungsmechanismen, die sich nicht als technisch unüberwindbar gezeigt haben.

Für eine Strafbarkeit nach § 202a Abs. 1 StGB reicht es allerdings nicht aus, dass ein Täter im Besitz von Zugangsdaten ist, die ihm später den Zugriff auf besonders geschützte Daten ermöglichen würden. Daher ist das *Phishing* nach Zugangsdaten zu einem Online-Banking-System nicht nach § 202a Abs. 1 StGB strafrechtlich zu erfassen (so auch M. Gercke & Brunst, 2009, Rdn. 97; Graf, 2007); insoweit kann aber an dieser Stelle auf das Vorbereitungsdelikt des § 202c Abs. 1 Nr. 1 StGB verwiesen werden (s. näher unten 7.3.4., S. 106, auch zum gesetzgeberischen Handlungsbedarf).

Während Angriffe gemäß § 202a Abs. 1 durch einen direkten Zugriff auf ein informationstechnisches System oder auch durch Netzwerkzugriffe erfolgen, stellen die elektromagnetischen Abstrahlungen eines informationstechnischen Systems einen weiteren Angriffsvektor zur Erlangung fremder Daten dar. Technischer Schutz ist hiergegen nur schwer zu bewerkstelligen, so dass es umso mehr eines (straf-)rechtlichen Ansatzes bedarf. Hierauf hat der Gesetzgeber mit § 202b Alt. 2 StGB umfassend und unserer Einschätzung nach auch ausreichend reagiert.

Vernetzte informationstechnische Systeme Die Übertragung von Daten zwischen vernetzten informationstechnischen Systemen wird durch § 202b Alt. 1 StGB strafrechtlich geschützt. Dieser Tatbestand ist erfüllt, wenn ein Täter sich nicht für ihn bestimmte Daten aus einer nicht-öffentlichen Datenübertragung verschafft, d.h. tatsächlich Zugriff erlangt. Im Gegensatz zu § 202a Abs. 1 StGB reicht daher die bloße Zugriffs*möglichkeit* nicht aus. Die Art des Zugriffs kann dabei durch sämtliche technische – i.d.R. also durch andere informationstechnische Systeme – erfolgen. Ein Zugriff auf Zwischenspeicher (Buffer) mag bei § 202b StGB zwar noch unter den Wortlaut zu fassen sein und damit strafrechtlicher Ahndung unterliegen, nicht erfasst sind hingegen aus einer Datenübermittlung herrührende Daten, die etwa von einem Diensteanbieter auf einer »Internetfestplatte« gespeichert werden (s. hierzu sogleich S. 101).

Den Schutz der eigentlichen Telekommunikation mitsamt ihren näheren Umständen bezweckt § 206 StGB. Der persönliche Anwendungsbereich auf Inhaber und Beschäftigte von Unternehmen, die geschäftsmäßig Post- oder Telekommunikationsdienste erbringen, ist dabei weiter als auf den ersten Blick ersichtlich: Auch Universitäten, Behörden und Unternehmen sind erfasst, soweit sie für ihre Mitarbeiter nachhaltig E-Mail-Dienste zur Verfügung stellen. Der strafrechtliche Schutz ist zwar gegeben (a.A. Vetter, 2002, S. 131 ff.), allerdings nur unvollkommen: Nur die Mitteilung an Dritte und die Unterdrückung

einer E-Mail unterfallen den § 206 Abs. 1, Abs. 2 Nr. 2 StGB, nicht jedoch das bloße Mitlesen, die bloße Kenntnisnahme einer E-Mail.

Schließlich beschäftigt die Frage Juristen, ob die Löschung von virenverseuchten E-Mails und von SPAM-Mails im Hinblick auf das Unterdrücken einer E-Mail strafrechtlich relevant ist. Dies ist zu verneinen, jedenfalls solange eine automatische Löschung erfolgt: Erstens vermittelt § 88 Abs. 3 S. 1, 2 TKG eine rechtfertigende Wirkung, zweitens obliegt es jedem, selbst zu entscheiden, welche E-Mails er empfangen möchte, so dass auch seine Einwilligung in die Löschung ausreicht, und drittens ist regelmäßig von einer mutmaßlichen – oder auch hypothetischen – Einwilligung auszugehen.

Unzureichender Schutz von Dritten anvertrauten Daten Es hat sich bislang gezeigt, dass Daten umfassend geschützt sind gegenüber dem Angriff von Tätern, die nicht zum Zugriff befugt sind; innerhalb von Unternehmen greifen auch die Sonderregelungen der §§ 17 ff. UWG. Eine Schutzlücke verbleibt hingegen bei Daten, die einem Diensteanbieter anvertraut wurden, etwa bei Verwendung einer »Internetfestplatte« oder einer sonst ausgelagerten Speicherung von Daten. Die zunehmende Nutzung von Virtualisierung und »Cloud Services« birgt hier eine Gefahr, da Administratoren, aber auch weitere Mitarbeiter dieser Diensteanbieter regelmäßig umfassende Zugriffsmöglichkeiten auf sämtliche Datenbestände haben. Ein Missbrauch dieser Befugnis unterliegt aber weder § 202a Abs. 1 StGB – angesichts des leichten Zugriffs und fehlender Zugangssicherungen – noch § 202b Abs. 1 StGB oder § 206 Abs. 1 StGB, da kein Übertragungsvorgang betroffen ist und nicht notwendigerweise Kommunikationsdaten abgegriffen werden. Schließlich ist der Anwendungsbereich des mit § 206 korrelierenden Fernmeldegeheimnisses in Art. 10 GG auf archivierte E-Mails nach wie vor umstritten (s. hierzu oben 4.5.2., S. 47). Die Strafvorschriften des BDSG und des UWG helfen in solch einer Konstellation nur in Ausnahmefällen. Um daher mit der technischen Entwicklung der Virtualisierung und der Nutzung ausgelagerter Speichermedien nicht nur strafprozessual Schritt zu halten (vgl. § 110 Abs. 3 StPO), ist es erforderlich, diesbezüglich eine neue Strafnorm einzuführen:

> § 207 Verbreitung fremder Daten
>
> Wer unbefugt Daten (§ 202a Abs. 2), die ihm als Inhaber oder Beschäftigtem eines Unternehmens anvertraut wurden, das geschäftsmäßig Telekommunikations- oder Telemediendienste erbringt,
>
> 1. verbreitet,
> 2. einem anderen übermittelt oder
> 3. einem anderen zugänglich macht,
>
> wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

7.3.3. Schutz der Ehre; Meinungs- und Äußerungsdelikte

Schutz der persönlichen Ehre

Der Schutz der persönlichen Ehre durch die Beleidigungsdelikte in den §§ 185 ff. StGB ist unabhängig von der Begehungsform gewährleistet, so dass sich ohne Weiteres auch ein Täter wegen einer Beleidigung strafbar machen kann, die er über E-Mail, über eine Pinnwand in einem sozialen Netzwerk oder über eine Internetseite tätigt. Eine erhöhte Strafdrohung ist vorgesehen, wenn eine üble Nachrede (§ 186 StGB) oder eine Verleumdung (§ 187 StGB) öffentlich (d.h. durch eine größere Anzahl von Personen wahrnehmbar, etwa auf einer öffentlichen Internetseite) oder durch das Verbreiten von Schriften und damit auch das Verbreiten von Dateien als Datenspeichern (s. hierzu erneut die Diskussion über den Schriftenbegriff oben 7.3.1., S. 88) begangen wurde.

Inhaltlich muss bei alledem darauf hingewiesen werden, dass der Ehrbegriff der §§ 185 ff. relativ und situationsbezogen ist: So stellte es keine Beleidigung dar, dass Udo Bölts bei der Tour de France 1997 seinen Teamkollegen Jan Ullrich mit den Worten »Quäl dich, du Sau!« zu Höchstleistungen anspornte. Genausowenig ist es aber eine Beleidigung, wenn sich auf einer bestimmten Internetplattform raue Umgangsformen entwickelt haben und dort nun zwischen den Beteiligten dieser Plattform diesen Umgangsformen entsprechende Äußerungen getätigt werden, die man in anderen Situationen durchaus als Ausdruck der Missachtung oder Nichtachtung verstehen könnte. Diesen situativen Kontext gilt es in Internetkonstellationen besonders genau zu hinterfragen, denn durch die wahrgenommene Anonymität und die physische Distanz kann es leicht zu einer Erosion der sonst vorzufindenden Umgangsformen kommen. Soweit dies die situative Umgebung prägt, in der eine Äußerung getätigt und vom Adressaten der Äußerung wahrgenommen wurde, ist es nicht Aufgabe des Strafrechts, bevormundend und erzieherisch die Einhaltung eines bestimmten absoluten Kanons an Umgangsformen sicherzustellen. Ist aber der situativ-relative Rahmen verlassen, so kann durchaus strafwürdiges Verhalten vorliegen, das eine Reaktion des Strafrechts erfordert, wofür die Mittel der §§ 185 ff. StGB genügen (s. zu alledem auch Beck, 2009; Hilgendorf, 2010a, die aber eine Qualifikation für öffentliche Beleidigungen bei § 185 StGB fordern).

In der Praxis ist allerdings die Verfolgung von Beleidigungsdelikten auch deshalb selten, weil es sich um Privatklagedelikte handelt (§ 374 Abs. 1 Nr. 2 StPO) und das Zivilrecht dem Geschädigten oftmals eine bessere Plattform zur Durchsetzung seiner Rechte – ggf. einschließlich einer monetären Entschädigung – bietet.

Volksverhetzung

Die Verbreitung volksverhetzender Äußerungen im Internet ist nicht nur ein theoretisches Problem, doch das Strafrecht zeigt sich zur Ahndung dieser Kriminalitätsform nach derzeitigem Stand aus technischer und rechtlicher Sicht adäquat gerüstet. § 130 Abs. 2 StGB,

auch in Verbindung mit dessen Abs. 4, erfasst die Verbreitung entsprechender Texte im Internet, durch E-Mails und durch sonstige elektronische Kommunikationsformen, da der Schriftenbegriff nach der Rechtsprechung und auch nach der hier vertretenen Auffassung auch Dateien als Datenspeicher im Sinne des § 11 Abs. 3 StGB betrachtet (s. zu diesem Meinungsstreit oben 7.3.1., S. 88). Eine Erweiterung auf flüchtige Kommunikationsformen, in denen es nicht notwendigerweise zu einer Verkörperung in einer Datei kommt, enthält § 130 Abs. 2 Nr. 2 StGB.

Aus inhaltlicher Sicht gilt es angesichts der erst am 16. Dezember 2010 beschlossenen Änderung des § 130 StGB (vgl. BT-Prot. 17/81, S. 9092A; zum unveränderten § 130 Abs. 4 StGB s. aber BVerfG JZ 2010, 298 m. Bespr. Degenhart, 2010; Hörnle, 2010a), erste Erfahrungen mit der Anwendung dieser neu gefassten Norm in der Praxis abzuwarten; eine Stellungnahme zum jetzigen Zeitpunkt wäre verfrüht.

Gewaltdarstellungen; Anleitung zu Straftaten; Terrorismusdelikte

Eine legitime Inhaltsregulierung des Internets und weiterer informationstechnisch relevanter Sachverhalte bewirken schließlich auch die §§ 91, 130a, 131 StGB. Der Anwendungsbereich dieser Vorschriften erfasst nach von der Rechtsprechung vertretener Auffassung zum Schriftenbegriff (s. oben 7.3.1., S. 88) auch und gerade Internetsachverhalte, soweit entsprechende Dateien als Datenträger verbreitet (§§ 130a, 131 Nr. 1 StGB) oder zugänglich gemacht werden (§§ 91, 130a, 131 Nr. 2 StGB).

Dabei hat der Tatbestand der Gewaltdarstellung (§ 131 StGB) eher wissenschaftliche denn praktische Relevanz erlangt in der Diskussion über die strafrechtliche Ahndung von so genannten »Killerspielen«, aber auch betreffend der Ahndung von Gewaltdarstellungen im Internet. Dabei bereitet zwar die Auslegung des Begriffs menschenähnlicher Wesen im Lichte des Bestimmtheitsgebots gewisse Schwierigkeiten (Köhne, 2004), insgesamt handelt es sich jedoch um ausreichende Strafbestimmungen, mit denen man diesem Phänomen auch in der Praxis begegnen könnte (Höynck, 2008; Höynck & Pfeiffer, 2007). Auch die Schwierigkeiten bezüglich der verfassungsrechtlich garantierten Kunstfreiheit (Art. 5 Abs. 3 GG) lassen sich lösen, denn Gegenstand der Gewaltdarstellung muss gerade die Hintansetzung sonstiger menschlicher Bezüge sein. Sind aber menschliche Bezüge vorhanden, wenn etwa in der Überhöhung der Gewalt ein Aufschrei gerade gegen die Gewalt zu lesen ist, so tritt die Kunstfreiheit mit rechtfertigender Wirkung einer Bestrafung des Künstlers entgegen.

Die Anleitung zu den schweren Straftaten des § 126 Abs. 1 StGB (§ 130a StGB) und zu den schweren staatsgefährdenden Gewalttaten des § 89a Abs. 1 StGB (§ 91 StGB) setzt grundsätzlich eine Verkörperung in einer Schrift (§ 11 Abs. 3 StGB) voraus; eine bloß flüchtige Erläuterung in einem Telefongespräch oder einem Chatroom wird daher nicht erfasst. Wirkliche Strafbarkeitslücken entstehen dabei freilich nicht, denn in aller Regel

dürfte hierin bereits die Beihilfe zu einer wenigstens in ihren Umrissen konkretisierten Haupttat bestehen.

Schließlich sei in diesem Zusammenhang noch auf § 89b StGB verwiesen, die Aufnahme von Beziehungen zur Begehung einer schweren staatsgefährdenden Gewalttat. Die Aufnahme von oder das Unterhalten von Beziehungen ist dabei offen formuliert, so dass auch und gerade die Kontaktaufnahme via Internet erfasst ist. Diese rechtspolitisch nicht unumstrittene Strafnorm hat allerdings bislang in der Praxis keine wesentliche Bedeutung erlangt. Für eine vertiefte Beurteilung dieser Terrorismusdelikte und auch des Cyberterrorismus, die nicht Gegenstand dieser Studie sind, sei verwiesen auf Gazeas, Grosse-Wilde & Kießling, 2009; M. Gercke, 2007a; Radtke & Steinsiek, 2010 und Zöller, 2010.

7.3.4. Schutz des Vermögens

Ausweislich der polizeilichen Kriminalstatistik ist Internetkriminalität im Wesentlichen Vermögenskriminalität: Die verschiedenen Erscheinungsformen des Betruges machen allein 82% der erfassten Straftaten mit dem Tatmittel Internet aus (Bundeskriminalamt, 2010, S. 243). Cyberkriminalität ist aber auch bei nicht oder nicht über das Internet vernetzten informationstechnischen Systemen festzustellen. Besondere Schwierigkeiten bereitet dabei das Phänomen des *Skimming*, des Auslesens von Bankkarten und späteren Missbrauchs derselben. Schließlich ist noch auf weitere vermögensrelevante Tatbestände hinzuweisen, namentlich die Erpressung – begangen etwa durch sogenannte *Scareware* –, unerlaubtes Glücksspiel und das Erschleichen von Leistungen.

Betrug und Computerbetrug

Betrug (§ 263 Abs. 1 StGB) Betrug im Sinne des Strafrechts (§ 263 Abs. 1 StGB) ist die vorsätzliche Täuschung über eine Tatsache, die dazu führt, dass sich ein Opfer irrt und daher über Vermögen verfügt. Dies muss zu einem Vermögensschaden auf Seiten des Opfers führen, und der Täter muss hierdurch seine eigene Bereicherung beabsichtigen. Aus Sicht der Cyberkriminalität ist hierfür entscheidend, dass nur ein *unmittelbar menschlicher Irrtum* erfasst wird, nicht hingegen etwa eine fehlerhafte Entscheidung eines Computerprogramms. In solchen Fällen kann nur ein Computerbetrug, § 263a Abs. 1 StGB vorliegen.

Seitdem das Internet wohl zu dem zentralen Medium für das wirtschaftliche Handeltreiben geworden ist, haben sich die altbekannten Betrugskonstellationen auch dorthin verlagert. Da bei Verträgen, die über das Internet abgeschlossen werden, in aller Regel Leistung und Gegenleistung nicht zeitgleich erfolgen, ist diesen ein Insolvenz-, Leistungs- und Zahlungsrisiko inhärent. Dieser wirtschaftliche Nachteil wird allerdings erstens durch den weitaus größeren Markt aufgewogen. Zweitens ist die Diebstahlskriminalität – im Handel vor allem im Rahmen des Ladendiebstahls ein erhebliches Problem – bei

der Internetkriminalität nahezu ausgeschlossen, da sämtlicher Warenversand durch den Verkäufer oder dessen Computersysteme erfolgt.

Juristisch bereitet es keine größeren Schwierigkeiten, die klassischen Formen des Warenkreditbetruges oder Leistungskreditbetruges – also Täuschungen über die Zahlungsfähigkeit oder den Zahlungswillen – und des Waren- oder Leistungsbetruges – also Täuschungen über die Fähigkeit und den Willen, eine Ware zu liefern oder eine Leistung zu erbringen – auch bei Internetsachverhalten unter § 263 StGB zu subsumieren (s. etwa M. Gercke & Brunst, 2009, Rdn. 200 ff.; vgl. ferner Hilgendorf, 2006). Dies gilt auch für Dreieckskonstellationen, wenn ein Täter etwa fremde Kreditkartendaten zur Bezahlung einer Ware oder Dienstleistung verwendet. Lediglich die gesteigerten Anforderungen der Rechtsprechung an die Spezifikation eines Gefährdungsschadens (BGHSt 53, 199) bedürfen kritischer Beobachtung auch durch die Legislative.

Zurückhaltung ist aber geboten, wenn ein Täter eine Ware bestellt und diese plangemäß später unter Berufung auf sein zivilrechtliches Widerrufsrecht zurücksendet, dadurch für eine gewisse Zeit – i.d.R. bis zu zwei Wochen – diese Ware nutzen kann und regelmäßig hierfür keine Kosten tragen muss. Hier ist ein Betrug wohl nur bei »hinreichenden Anhaltspunkte[n] für einen eindeutigen Missbrauch« (Rettenmaier & Kopf, 2007, S. 231) anzunehmen.

Computerbetrug (§ 263a Abs. 1 StGB) Soweit es durch die zunehmende Verwendung von informationstechnischen Systemen zu einer Automatisierung von Entscheidungsprozessen kommt, entfällt mit dem *menschlichen Irrtum* auch ein Tatbestandsmerkmal des Betruges. Diese Strafbarkeitslücke wurde bereits frühzeitig und umfassend durch den Tatbestand des Computerbetruges (§ 263a Abs. 1 StGB) geschlossen (Lenckner & Winkelbauer, 1986; Möhrenschlager, 1986; Tiedemann, 1986), dessen Bedeutung zur Verfolgung von Cyberkriminalität nicht unterschätzt werden kann.

Die Merkmale der Täuschungshandlung und des durch diese Täuschungshandlung hervorgerufenen Irrtums sind beim Computerbetrug ersetzt durch die Einleitung oder Beeinflussung eines Datenverarbeitungsvorgangs, diese wiederum begangen durch eine von vier Tathandlungen:

- Die praktisch wichtigste Variante davon ist die unbefugte Verwendung von Daten. Nach in Rechtsprechung und Literatur vorherrschender Auffassung ist die Verwendung unbefugt, wenn ein Mensch – an die Stelle der Datenverarbeitungsanlage gedacht – unter Zugrundelegung der durch die Daten vermittelten Informationen getäuscht würde (betrugsspezifische Auslegung).
- Ebenfalls erfasst ist aber auch die unrichtige Gestaltung eines Programms, wobei es umstritten ist, ob es auf den Willen des Verfügungsberechtigten oder aber auf den objektiven Zweck eines Programms ankomme,

- die Verwendung unrichtiger – d.h. nicht mit der Wirklichkeit übereinstimmender – oder unvollständiger Daten, sowie schließlich
- die unbefugte Einwirkung auf den Ablauf, etwa durch Hardware-Manipulationen.

Zum ebenfalls in § 263a StGB geregelten Vorbereitungsdelikt (Abs. 3) siehe sogleich und auch noch unten 7.3.6., S. 117.

Phishing, Skimming und Abofallen als aktuelle Kriminalitätsphänomene Mit Phishing bezeichnet man es, wenn Bankkunden durch Täuschungen, etwa durch gefälschte E-Mails oder gefälschte Internetseiten, zur Preisgabe von Zugangs- oder Kreditkartendaten verleitet werden und Täter sodann diese Informationen nutzen, um Überweisungen oder Kreditkartenzahlungen zu Lasten des Kunden vorzunehmen. Bei der strafrechtlichen Erfassung dieser Kriminalitätsform sind verschiedenen Stadien zu unterscheiden (zutr. Seidl & Fuchs, 2010):

1. Der Versand von täuschenden E-Mails oder die Veröffentlichung einer täuschenden Internetseite unterfallen allenfalls den urheber- und markenrechtlichen Strafbestimmungen und, nach nicht unumstrittener Auffassung und je nach konkreter Tatsituation, auch der Fälschung beweiserheblicher Daten gemäß § 269 Abs. 1 StGB (Graf, 2007; Heghmanns, 2007; Seidl & Fuchs, 2010, S. 85 ff.).
2. Die Eingabe von Zugangs-, nicht jedoch von Kreditkartendaten durch die Opfer auf der gefälschten Internetseite oder als Antwort auf die gefälschte E-Mail und deren Verarbeitung oder Kenntnisnahme durch den Täter begründet sodann eine Strafbarkeit gemäß § 202c Abs. 1 Nr. 1 StGB, unter Umständen auch nach datenschutzrechtlichen Bestimmungen (Seidl & Fuchs, 2010). Eine Gefährdung des Opfervermögens ist nicht hinreichend konkretisiert, um bereits in diesem Stadium einen Betrug bejahen zu können (Popp, 2004; Stuckenberg, 2006).
3. Die missbräuchliche Nutzung der Kreditkarten- oder Bankdaten erfüllt ohne Weiteres den Straftatbestand des Computerbetruges gem. § 263a Abs. 1 StGB (Heghmanns, 2007; Popp, 2004; Seidl & Fuchs, 2010). Soweit durch die Eingabe dieser Zugangsdaten der Täter zudem Möglichkeiten zur Kenntnisnahme weiterer geschützter Daten hat – etwa den aktuellen Kontostand – ist zugleich § 202a Abs. 1 StGB verwirklicht (Heghmanns, 2007; Seidl & Fuchs, 2010).
4. Sodann erfolgt typischerweise eine Weiterleitung der so erlangten Gelder durch – zum Teil gutgläubige – »Finanzagenten« unter Zuhilfenahme von Sofortüberweisungen und anonymen Zahlungsdiensten. Hierdurch machen sich diese Finanzagenten regelmäßig wegen leichtfertiger Geldwäsche (§ 261 Abs. 1 Var. 4, Abs. 2 Nr. 2, Abs. 5 StGB), ggf. auch wegen kreditwirtschaftlicher Verstöße, strafbar (Neuheuser, 2008; Seidl & Fuchs, 2010, S. 90 f.).

Die Strafbarkeitslücken sind daher – entgegen Graf, 2007 – zwar nur als gering zu bewerten (Goeckenjan, 2008). Dennoch befriedigt der Rückgriff auf das Urheber- und Markenrecht und die unvollständige Erfassung aller Phishing-Mails und -Internetseiten nicht. Auch aus Klarstellungsgründen ist daher eine Erweiterung des § 263a Abs. 3 StGB zu erwägen, der sinnvollerweise (zutr. Heger, 2008) in einen eigenständigen Paragraphen verschoben und dabei an § 202c Abs. 1 StGB angepasst werden sollte (Änderung in kursiv):

> § 263b Vorbereiten des Computerbetrugs
>
> (1) Wer eine Straftat nach § 263a Absatz 1 vorbereitet, indem er
>
> 1. *Passwörter oder sonstige Sicherungscodes für Zahlungskarten oder Zahlungsdienste, oder*
> 2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist,
>
> herstellt, *verkauft*, sich oder einem anderen verschafft, *verbreitet oder sonst zugänglich macht*, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.
>
> (2) § 149 Abs. 2 und 3 gilt entsprechend. *Absatz 1 ist nicht anzuwenden, wenn die Handlung der Wissenschaft, der Forschung oder der Lehre oder der Erfüllung rechtmäßiger beruflicher oder dienstlicher Pflichten dient.*

Durch diese Erweiterung des § 263a Abs. 3 StGB könnte auch auf die neuere Rechtsprechung reagiert werden, welche das Auslesen von Bankkarten durch Manipulation von Bankautomaten oder Türöffnern (Skimming) als nicht gemäß § 202a Abs. 1 StGB strafbar erachtet: Im Gegensatz zu chip-basierten Lösungen lassen sich die Magnetstreifen solcher Bank- und Kreditkarten ohne Überwindung einer Zugangssicherung auslesen (BGH NStZ 2010, 275; BGH NStZ 2010, 509; BGH JR 2010, 497; Gräfin Tyszkiewicz, 2010, Schiemann, 2010; anders noch BGH NStZ 2005, 566). Das spätere Aufspielen dieser ausgelesenen Daten auf Blanko-Magnetkarten kann allerdings ohne Weiteres als Fälschung von Zahlungskarten (§ 152b StGB; s. hierzu BGH, Beschl. v. 14.9.2010 – 5 StR 336/10 –), deren Verwendung sodann als Computerbetrug (§ 263a StGB) strafrechtlich geahndet werden. Wegen der Möglichkeit, mithilfe dieser Magnetkarten sich etwa auch den Kontostand anzeigen zu lassen, kann man mit gewissen Bedenken bereits im Auslesen der Bankkarten eine Vorbereitungsstraftat nach § 202c Abs. 1 Nr. 1 StGB sehen. Erneut sprechen aber die besseren Gründe für eine entsprechende Erweiterung des § 263a Abs. 3 StGB.

Als Abofallen oder Kostenfallen werden Internetangebote bezeichnet, bei denen Kunden über die Kostenpflichtigkeit des Angebots getäuscht werden. Zumeist handelt es sich dabei

um anderswo im Internet kostenlos verfügbare Leistungen; die Preisangaben finden sich zumeist an nur versteckter Stelle. Wie Eisele (2010) überzeugend darlegt, verwirklichen die Akteure – übrigens auch Rechtsanwälte, die sich in Kenntnis der Umstände an diesen Machenschaften beteiligen – regelmäßig einen (versuchten) Betrug i.S.d. § 263 Abs. 1 StGB. Daher ist zu begrüßen, dass in einem solchen Fall nunmehr das OLG Frankfurt am Main die Anklage zugelassen hat (Beschl. v. 17.12.2010 – 1 Ws 29/09 –); dies zeigt auch, dass insoweit den Strafverfolgungsakteuren ein ausreichendes Instrumentarium zur Verfügung steht.

Nur noch geringe praktische Relevanz haben schließlich so genannte Dialer, also Schadprogramme, die kostenpflichtige, teure Wählverbindungen herstellen und so zu erheblichen Vermögensverschiebungen zwischen Opfer und Täter führen. Daher kann diesbezüglich auf die Aufarbeitung in der juristischen Literatur verwiesen werden (M. Gercke & Brunst, 2009, Rdn. 209 ff. m.w.N.).

Erpressung; Unerlaubtes Glücksspiel; Erschleichen von Leistungen

Auch Erpressungen (§ 253 Abs. 1, Abs. 2 StGB) machen vor dem Internet nicht halt: So existiert beispielsweise Schadsoftware, die den Benutzer zur Zahlung eines Geldbetrages auffordert. Andernfalls werden Daten des Benutzers unwiderruflich gelöscht. Die Verbreitung solcher *Scareware* lässt sich ohne Weiteres strafrechtlich als Erpressung ahnden, da insoweit mit einem empfindlichen Übel – dem Löschen wichtiger Daten – gedroht und hierdurch der Betroffene zu einem Vermögensopfer genötigt wird.

Ein schwieriges Feld ist hingegen die strafrechtliche Erfassung des unerlaubten Glücksspiels. Dies liegt weniger an den Straftatbeständen der §§ 284 ff. StGB denn an der europarechtlichen Überformung des Glücksspielrechts, welche zu einer unklaren Gesetzeslage über die Legalität und Illegalität von Glücksspielangeboten, auch im Internet, geführt hat (vgl. u.a. EuGH NJW 2009, 3221; EuGH MMR 2010, 838; EuGH MMR 2010, 840; EuGH MMR 2010, 844; EuGH MMR 2010, 854; EuGH EuZW 2010, 668; EuGH EuZW 2010, 947; Dederer, 2010; Lober & Neumüller, 2010; Spindler, 2010). Dies ist eine im Wesentlichen ordnungsrechtliche Vorfrage, die hier nicht vertieft behandelt werden kann.

Zuletzt sei noch auf den Straftatbestand des Erschleichens von Leistungen (§ 265a Abs. 1 StGB) hingewiesen, der eine weitere Lücke der Betrugsstrafbarkeit auch bei Cyberkriminalität schließt. Tatobjekte sind – neben dem archetypischen Schwarzfahren – auch öffentlichen Zwecken dienende Telekommunikationsnetze, was weit ausgelegt wird und daher auch DSL-Anschlüsse, WLAN-Router usw. erfasst (M. Gercke & Brunst, 2009, Rdn. 218). Zusätzliches Erfordernis ist die Entgeltlichkeit der konkret erschlichenen Leistung. Hieran fehlt es bei Zugriffen auf unzureichend gesicherte private WLAN-Netzwerke, so dass insoweit eine Strafbarkeit ausscheidet. Schließlich aber ist noch ungewiss, ob es für die Tathandlung des Erschleichens auch hier ausreicht, ob sich

der Täter mit dem Anschein der Ordnungsgemäßheit seines Verhaltens umgibt (vgl. BGH NJW 2009, 1091, 1092 zum Schwarzfahren). Festzuhalten ist aber, dass die – zivilrechtlich unzulässige – Nutzung eines fremden, ungesicherten und nicht gegen Entgelt angebotenen WLAN-Netzwerks (»Schwarz-Surfen«) unter keinem rechtlichen Gesichtspunkt strafbar (und im Übrigen auch nicht strafwürdig) ist (LG Wuppertal K&R 2010, 838; Ernst & Spoenle, 2008; Gramespacher & Wichering, 2010; a.A. noch AG Wuppertal NStZ 2008, 161).

7.3.5. Schutz des geistigen Eigentums

Die Krise des Urheber(straf)rechts

Die – entgegen der Polizeilichen Kriminalstatistik – häufigste Deliktsform der Cyberkriminalität dürfte in den Urheberrechtsdelikten zu finden sein: Hier gibt es ein großes Dunkelfeld gerade im Bereich der Bagatell- und kleineren Kriminalität (vgl. M. Gercke & Brunst, 2009, Rdn. 405 ff.). Nachdem über mehrere Jahre die rechtswidrige Verwendung von Software im Vordergrund stand, hat sich dies nun phänomenologisch hin zur Unterhaltungs»industrie« und der rechtswidrigen Verbreitung von Musik- und Filmdateien verlagert.

Im allgemeinen Sprachgebrauch hat sich für diese Verhaltensweisen der Begriff *Raubkopie* bzw. im englischen Sprachraum *piracy* eingebürgert. Diese Begriffe sind allerdings irreführend, da unter Raub die Wegnahme einer Sache unter (Personen-)Gewalt oder Drohung mit Gefahren für Leib oder Leben zu verstehen ist (§ 249 StGB), und daher Raub zu mittelschwerer und schwerster Kriminalität gehört, und Piraterie ebenfalls für schwerste Gewaltkriminalität auf Hoher See steht. Hingegen thematisieren die Urheberrechtsverletzungen im Ausgangspunkt eine Auflehnung gegen einen Exklusivitätsanspruch des Urheberrechtsinhabers. Der Angriff richtet sich demnach gegen die (formale) Ordnung geistigen Eigentums.

Hiermit korreliert auch das gängige kriminalpolitische Postulat, das Urheberrecht solle demnach die auf geistigem Eigentum fußende moderne Wirtschaftsordnung auch mit Mitteln des Strafrechts schützen. Wenn auch eine Notwendigkeit flankierenden strafrechtlichen Schutzes der Urheberrechtsordnung nicht verneint werden kann, so ist diesem Ansatz nicht in seinem vollen Umfang zu folgen: Erstens ist für die wirtschaftliche Nutzung geistigen Eigentums dessen Geheimhaltung – etwa gegenüber Konkurrenten – weitaus bedeutsamer, die durch andere Strafnormen zielgerichtet geschützt wird (s. oben 7.3.2., S. 93). Zweitens ist das Urheberrecht hauptsächlich nur für zwei Wirtschaftssparten werthaltig: einerseits für die Medien-, Unterhaltungs- und Kulturunternehmen, andererseits für die Softwareindustrie, wobei sich diese zunehmend auf den patentrechtlichen Schutz zu berufen versucht. Drittens ist auf die außerordentlich langen Schutzfristen zu verweisen, die regelmäßig erst 70 Jahre nach dem Tod des Schöpfers enden (§ 64 UrhG),

was den Unternehmen – die i.d.R. die wirtschaftlichen Verwertungsrechte innehaben, und nicht etwa die Künstler und deren Erben – ein erhebliches wirtschaftliches Interesse an langfristigen Exklusivitätsrechten begründet.

Mehr noch als die unüberhörbaren Klagen der betroffenen Industrien spricht das hohe Dunkelfeld dafür, von einer Krise der Durchsetzung des Urheberrechts zu sprechen, der eine expansive Tendenz des zivilrechtlichen und strafrechtlichen Urheberrechtsschutzes entgegenzuwirken versucht. Das unzureichende Unrechtsbewusstsein weiter Teile der Bevölkerung – nicht nur in Deutschland, sondern weltweit –, die wohlfahrtssteigernde Wirkung eines zeitlich nur begrenzten Urheberrechtsschutzes (Yuan, 2006) bei Beibehaltung eines Urheberpersönlichkeitsschutzes, eine Fokussierung auf die Urheber und Künstler und schließlich auch die Langsamkeit der Rechteinhaber, sich auf neue Vermarktungsmodelle im Internet einzustellen, sollten durchaus als Anregung dienen, auch über Alternativen zum bestehenden Urheberrechtssystem – etwa eine »Kultur-Flatrate« nachzudenken (vgl. EMR/provet, 2009 sowie die Stellungnahmen zur Anhörung »Entwicklung des Urheberrechts in der digitalen Gesellschaft« der Enquete-Kommission »Internet und digitale Gesellschaft« des Bundestags).

Prozessual entwickelt sich der strafrechtliche Schutz des Urheberrechts zu einem Äquivalent des Ladendiebstahlsrechts im 21. Jahrhundert. Hier wie dort handelt es sich um massenhaft auftretende Bagatellfälle mit individuellen Schäden von selten über 50 €, die jedoch in der Summe gesehen zu erheblichen finanziellen Schädigungen der – wenigen – Opfer durch die – vielen – Täter führen. Hier wie dort existieren zivilrechtliche Unterlassungs- und Schadensersatzansprüche, die aber bisweilen an ihrer ungenügenden Durchsetzbarkeit und an ihrem fehlenden Strafcharakter leiden. Hier wie dort ist das Gesamtbild eines der »›kriminalitätsverwaltenden‹ Praxis« (vgl. Vogel, 2010, Vor § 242 Rdn. 11), da im unteren Bereich der Urheberrechtskriminalität zumeist mit Verfahrenseinstellungen nach §§ 153, 153a StPO reagiert wird (vgl. M. Gercke & Brunst, 2009, Rdn. 553 unter Verweis auf die Richtlinien der Generalstaatsanwaltschaften; krit. Esser, 2010).

Im Gegensatz zum Ladendiebstahlsrecht ist derzeit allerdings – jedenfalls gegenüber Rechteverletzungen durch Private – ein Primat der zivilrechtliche Rechtsdurchsetzung zu verzeichnen: Seit der Einführung eines zivilrechtlichen Auskunftsanspruch in § 101a UrhG ist es für die zivilrechtlichen Rechteinhaber nämlich nicht länger erforderlich, zunächst ein Strafverfahren einzuleiten, um die Person des mutmaßlichen Täters zu ermitteln. Hierdurch wurde die zivilrechtliche Durchsetzung von Schadensersatz- und Unterlassungsansprüchen weiter vereinfacht. Im Gegensatz zum Strafrecht ermöglicht es eine solch zivilrechtliche Rechtsdurchsetzung den Rechteinhabern, sich eine durchaus einträgliche finanzielle Ertragsquelle zu erschließen. Die Abmahnung von Rechtsverletzungen ist zudem mit einer hohen Kostenforderung verbunden, der ein gewisser Strafcharakter zuteil wird und die in keinem Verhältnis zu den tatsächlich entstehenden Kosten steht.

Diese Fehlentwicklung erklärt auch die nunmehrige Begrenzung der Kostenforderung auf 100 € in § 97a Abs. 2 UrhG bei »einfach gelagerten Fällen mit einer nur unerheblichen Rechtsverletzung außerhalb des geschäftlichen Verkehrs«. Bedauerlicherweise werden allerdings noch immer zu vorschnell erhebliche oder geschäftsmäßige Rechtsverletzungen angenommen (so etwa LG Hamburg ZUM 2010, 611; vgl. ferner grundsätzlich zu § 97a Abs. 2 UrhG Malkus, 2010; Möller, 2010 sowie BVerfG NJW 2010, 1347), welche die Wirksamkeit des § 97a Abs. 2 UrhG in der Praxis noch reduzieren. Dies gilt es auch in Zukunft kritisch zu begleiten.

Das Urheberstrafrecht

Akzessorietät zum Urheberrecht Das Urheberstrafrecht gemäß §§ 106 ff. UrhG (umfassend Weber, 1976) steht und fällt mit der zivilrechtlichen Ausgestaltung des Urheberrechts: Eine strafrechtlich relevante Urheberrechtsverletzung gemäß § 106 UrhG liegt nur dann vor, wenn das verletzte Werk urheberrechtlich geschützt ist und die Verletzungshandlung durch keine der Schranken des Urheberrechts gestattet wird. Der Schutz erstreckt sich dabei auf menschliche, persönliche und individuelle – d.h. sich von anderen Werken unterscheidende – geistige Schöpfungen, die eine gewisse Gestaltungshöhe aufweisen. Erfasst werden neben Texten und Sprachwerken, Werken der Musik und des Films auch Quelltexte einer Software oder einer Website sowie Sammel- und Datenbankwerke. Die Schutzdauer beträgt – auch für Computerprogramme respektive deren Quelltexte – siebzig Jahre nach dem Tod des letzten (Mit-)Urhebers (§§ 64 ff. UrhG).

Neben der Erlaubnis des Urhebers gestatten vor allem folgende Schranken eine Nutzung eines urheberrechtlich geschützten Werkes:

- Die freie Benutzung eines Werkes, etwa als Anregung für ein eigenes Werk (§ 24 UrhG),
- Zitate (§ 51 UrhG),
- flüchtige technische Begleitvervielfältigungen (§ 44a UrhG),
- bestimmte öffentliche oder gemeinnützige Zwecke (§§ 45–47, 52–52b UrhG),
- die Vervielfältigung von bis zu sechs oder sieben Exemplaren zum privaten oder sonstigen eigenen Gebrauch (§ 53 UrhG), sofern für die Vervielfältigung nicht eine offensichtlich rechtswidrige Quelle verwendet wird, sowie schließlich
- bei Computerprogrammen die Erstellung von Sicherungskopien (§ 69d Abs. 2 UrhG), die Untersuchung sowie die Dekompilierung des Programms, um dessen Interoperabilität herzustellen (§§ 69d Abs. 3, 69e UrhG).

Strafnormen der § 106 ff. UrhG Die zentrale Strafnorm des Urheberrechts, § 106 UrhG, stellt das Vervielfältigen – also die körperliche Reproduktion –, das Verbreiten und die öffentliche Wiedergabe eines urheberrechtlich geschützten Werkes unter Strafe. Da auch der Versuch strafbar ist (§ 106 Abs. 2 UrhG), haben manche dogmatische Streitigkeiten – etwa, ob das Vervielfältigen erst mit der Vollendung der Reproduktion gegeben ist – nur wenig praktische Bedeutung. § 108 UrhG enthält eine vergleichbare Strafnorm für die dem Urheberrecht verwandten Schutzrechte, etwa Tonträger, Lichtbilder und Datenbanken betreffend.

Aktuelle Schwierigkeiten bereitet hierbei weniger die Nutzung von Tauschbörsen (s. hierzu etwa M. Gercke, 2009c; Heghmanns, 2004; Röhl & Bosch, 2008) als vielmehr die Frage, ob neben den Anbietern auch die Nutzer so genannter Streamingangebote einer Strafbarkeit gemäß § 106 Abs. 2 UrhG unterliegen. Bei diesen kommt es nicht zu einer Duplizierung von Film- oder Musikdateien auf dem Rechner des Nutzers, vielmehr wird der Datenstrom – ggf. mit kurzer Zwischenspeicherung – direkt in Ton und Bilder umgesetzt. Manche Stimmen in der Literatur verneinen hier die urheberrechtliche Zulässigkeit und postulieren so auch die Strafbarkeit des Nutzers (Hullen, 2008; Radmann, 2010), die Gegenauffassung verneint eine Vervielfältigungshandlung des Nutzers oder sehen diese durch § 44a UrhG als gerechtfertigt an (F. A. Koch, 2010; Fangerow & Schulz, 2010). Eine obergerichtliche Klärung dieses Aspekts steht noch aus; bis dahin erscheint legislative Zurückhaltung geboten. Jedenfalls aber spricht vieles dafür, die Nutzung von offensichtlich rechtswidrigen Streaming-Angeboten zwar zivilrechtlich (in den Schranken des § 97a Abs. 2 UrhG; vgl. Hullen, 2008) zu ahnden, nicht jedoch strafrechtlich.

Die in § 108b UrhG normierten Vorbereitungs- und Begleitstraftaten sollen schließlich den technischen und rechtlichen Schutz des Urheberrechts weiter absichern:

Die Strafvorschrift des § 108 Abs. 1 Nr. 1 UrhG knüpft an wirksame technische Maßnahmen zur Absicherung des Urheberrechts an, also nach der Legaldefinition in § 95 Abs. 2 UrhG »Technologien, Vorrichtungen und Bestandteile, die im normalen Betrieb dazu bestimmt sind, geschützte Werke oder andere nach diesem Gesetz geschützte Schutzgegenstände betreffende Handlungen, die vom Rechteinhaber nicht genehmigt sind, zu verhindern oder einzuschränken.« Ist ein Programm etwa erst nach Eingabe eines Passworts oder nach Anschluss eines USB-Dongles nutzbar, handelt es sich bei dem Passwortschutz bzw. bei der Kombination USB-Dongle und Programmcode um eine technische Maßnahme. Ähnlich wie bei § 202a Abs. 1 StGB ist bei der Wirksamkeit des technischen Schutzes – § 95a Abs. 2 UrhG ist kaum zur Präzisierung dieses Begriffes tauglich – wiederum auf die Fähigkeiten eines Durchschnittsbenutzers abzustellen, der sich freilich am Stand der Technik orientiert. Ob etwa die bezüglich DVDs Verwendung findende Absicherung eine wirksame ist, wird derzeit höchstgerichtlich geklärt (Vorinstanz: OLG München MMR 2009, 118). Die Umgehung ausschließlich zum privaten Gebrauch bleibt bei alledem straffrei.

§ 108 Abs. 1 Nr. 2a UrhG enthält eine Strafvorschrift zum Schutz von »zur Rechtewahrnehmung erforderliche[n] Informationen« im Sinne des § 95c Abs. 2 UrhG: Dies sind daher nur *elektronisch* vorliegende Informationen über »den Urheber oder . . . anderen Rechteinhaber« und die eingeräumten Nutzungsrechte, wie etwa Lizenztexte, Lizenzbezeichnungen oder Copyright-Vermerke. Die Entfernung und Veränderung dieser Informationen – sofern diese nicht zum persönlichen Gebrauch erfolgt – wird bestraft, wenn hierdurch eine Rechtsverletzung veranlasst, ermöglicht, erleichtert oder verschleiert wird.

Hinzuweisen ist schließlich noch auf die Marktdelikte der § 108b Abs. 1 Nr. 2b, Abs. 2 UrhG, welche die Weiterverbreitung manipulierter Werke und die Herstellung, Einfuhr, das Verbreiten, Verkaufen oder Vermieten von Vorrichtungen oder Erzeugnissen unter Strafe stellt, die der Umgehung von Schutzvorrichtungen dienen. Auf die diesbezüglichen Schwierigkeiten sei bei dem Parallelproblem der Vorbereitungsdelikte hingewiesen (7.3.6., S. 117).

Eine § 108b Abs. 1 Nr. 2, Abs. 2 UrhG vergleichbare Strafvorschrift enthält auch § 4 ZKDSG. Werden Telemedien oder Rundfunkdarbietungen nur gegen Entgelt und unter Verwendung eines Zugangskontrollmechanismus angeboten (§ 2 ZKDSG), so ist »die Herstellung, die Einfuhr und die Verbreitung von Umgehungsvorrichtungen zu gewerbsmäßigen Zwecken« (§ 3 Nr. 1 ZKDSG) strafbewehrt.

Es zeigt sich daher, dass das Urheberstrafrecht bereits auf modernen Stand gebracht wurde und neben der effektiven zivilrechtlichen Rechtsdurchsetzung – dank des Auskunftsanspruchs in § 101a UrhG – auch ein adäquates strafrechtliches Instrumentarium zur Verfolgung krimineller Urheberrechtsverletzungen zur Verfügung steht. Ob das Strafrecht auch für alle Fälle geringer Urheberrechtsverletzungen ein adäquates und auch erforderliches Mittel ist, ist allerdings anzuzweifeln. Soweit das Zivilrecht einen hinreichend effektiven Mechanismus zur Wahrung der finanziellen Interessen der Urheber bietet, ist daher eine Entkriminalisierung geringer, durch Privatpersonen begangener Urheberrechtsverstöße in Erwägung zu ziehen.

Schutz weiterer Formen des geistigen Eigentums

Auch andere Formen des geistigen Eigentums werden flankierend strafrechtlich geschützt, seien es Marken, seien es Rechte am eigenen Bild und seien es auch Patente. Wirtschafts- und auch kriminalpolitische Bedeutung erlangt in Sachen Cyberkriminalität dabei die Frage, ob auch Computerprogramme patentrechtlichen Schutz genießen können.

Zum derzeitigen Stand sind jedoch Computerprogramme »als solche« (§ 1 Abs. 4 PatG, Art. 52 EPÜ) in Deutschland nicht patentrechtlich geschützt, anders hingegen »computerimplementierte Erfindungen«, die ein konkretes technisches (nicht betriebswirtschaftliches, rechtliches oder allein die Informatik betreffendes) Problem zu lösen vermögen. Bestrebungen auf europäischer und internationaler Ebene richten sich *de lege ferenda*

auf eine eine Zulassung reiner »Softwarepatente«; bedenklich erscheint auch die Rechtsprechung, welche diese Abgrenzung immer weiter verwischt (zuletzt BGH MMR 2010, 552; s. hierzu Hössle, 2010; Rempe, 2010). So ist dem BGH entgegenzuhalten, dass die Softwareentwicklung stets die technischen Grenzen der Hardware im Auge behalten muss. Von daher wären der in BGH MMR 2010, 552 angedeuteten Auffassung zufolge zumindest viele Betriebssystem- und Compilerprogrammierungen patentierbar – was im offenen Widerspruch zu § 1 Abs. 4 PatG steht.

Doch der dahinter stehende Meinungsstreit um Softwarepatente als solche kann und soll an dieser Stelle nicht vertieft werden (s. hierzu S. L. Garfinkel, Stallman & Kapor, 1991; Keller, 2009; Lejeune & Sieckmann, 2010; Wimmer-Leonhardt, 2007). Es ist aber erstens zu berücksichtigen, dass der Quelltext als Grundlage eines jeden Computerprogramms bereits den hohen Schutz des Urheberrechts genießt, zweitens die Schwierigkeit, mathematische oder informatische Strukturen – und nichts anderes ist Software – als technische Erfindung zu formulieren, drittens, dass Patente aufgrund der kostspieligen Rechtsdurchsetzung zumeist nur für große Unternehmen einen nützlichen Mechanismus darstellen können, während kleine und mittlere Unternehmen durch die notwendigen, aufwendigen Recherchen und das Risiko kostspieliger Gerichtsverfahren in ihrer Innovationsfreude gehemmt werden können und viertens, dass ökonomische Analysen des Patentrechts eher nachteilige Folgen für die Innovationsfreude nahelegen, soweit Softwarepatente zugelassen werden (Arai, 2009; Bessen & Hunt, 2004; Bessen & Hunt, 2007).

Ist die Schutzdauer für Software noch zeitgemäß?

Bei der Diskussion über den urheberrechtlichen und patentrechtlichen Schutz von Software – und dessen strafrechtlicher Absicherung – sollte ein weiterer Aspekt Berücksichtigung finden: die gewährte Schutzdauer. Die Schnelllebigkeit der modernen Informationstechnologie, deren rasante Weiterentwicklung und die relativ geringen Entwicklungskosten von Software sprechen dagegen, einer neuartigen Entwicklung denselben Exklusivitätsschutz zu gewähren wie etwa einem neuartigen Medikament. Daher ist für computerimplementierte Erfindungen eine Verkürzung des patentrechtlichen Schutzes von derzeit bis zu 20 Jahren auf höchstens 10 Jahre zu erwägen. Aber auch die urheberrechtliche Schutzdauer von Software – derzeit 70 Jahren nach dem Tod des letzten Urhebers – ist rechtspolitisch nicht zu rechtfertigen (zutr. Grützmacher, 2009, § 69a UrhG Rdn. 76). Eine deutliche Verkürzung dieser Schutzfristen – nicht aber des Urheberpersönlichkeitsrechtes – würde den Innovationsdruck auf die Unternehmen erhöhen und so zu einer weiteren Beschleunigung der Innovationsleistungen führen; zudem aber würde auch das gesellschaftliche Verständnis für die Notwendigkeit eines Exklusivitätsschutzes wachsen.

7.3.6. Schutz der informationstechnischen Infrastruktur

Zuletzt seien die Tatbestände vorgestellt, die dem Schutz der informationstechnischen Infrastruktur dienen: sei es ihrer Sachsubstanz, sei es ihrer technischen Funktionsfähigkeit (einschließlich des Datenbestandes), und sei es schließlich durch das Verbot von Vorbereitungshandlungen. Auf dieser Grundlage lassen sich sodann typische und aktuelle Erscheinungsformen der Cyberkriminalität – etwa Denial-of-Service-Attacken und Spamming – näher betrachten.

Schutz der Substanz

Die informationstechnische Infrastruktur besteht aus Sachen, deren Substanz und physische Integrität durch den Straftatbestand des § 303 Abs. 1 StGB geschützt wird. Auch dabei kommt es auf die Art und Weise der Tatbegehung nicht an: Wenn ein Täter einen Computervirus dergestalt programmiert und verbreitet, dass dieser zu einer Überhitzung des Rechners und so zu irreparablen Schäden führt, so macht er sich ohne Weiteres gemäß § 303 Abs. 1 StGB strafbar – wie es übrigens auch dem Tatbestand des § 303 Abs. 1 StGB unterfällt, Zentrifugen zur Uran-Anreicherung durch eine Manipulation der Ansteuerung zu beschädigen. Ebenfalls dem Tatbestand unterfällt die Demontage eines aus mehreren Komponenten bestehenden Rechners (vgl. RGSt 13, 27; RGSt 20, 353).

Noch nicht abschließend geklärt ist allerdings die Frage, ob auch die Eingabe von Daten dann dem Tatbestand des § 303 Abs. 1 StGB unterfällt, wenn dies die technische Brauchbarkeit der Sache nachhaltig beeinträchtigt. Ein Beispiel hierfür wäre es, wenn aufgrund eines Computervirus ein Rechner auf Eingaben des Benutzers nicht länger reagiert und nur durch eine umfangreiche, fachkundige Reparatur wieder in Gang gesetzt werden kann. Die Rechtsprechung vertritt bei § 303 Abs. 1 StGB eine funktionale Betrachtungsweise, die auch außerhalb der Cyberkriminalität zu bedenklichen Ausweitungen der Strafbarkeit führt (vgl. Fischer, 2011, § 303 Rdn. 6 m.w.N.). Bislang hält sie aber noch am Erfordernis einer körperlichen Einwirkung und einer körperlichen Veränderung fest (so u.a. BGHSt 44, 34), die bei der bloßen Eingabe von Daten zu verneinen ist. In diesen Fällen ist auf den durch §§ 303a, 303b StGB gewährleisteten und auch ausreichenden Schutz zu verweisen.

Ein weiteres, freilich eher dogmatisches denn praktisches Problem betrifft die Frage, ob die auf einem Datenträger körperlich festgehaltenen – gespeicherten – Daten Sachen sind, das Löschen oder Überschreiben von Daten daher auch dem Tatbestand der Sachbeschädigung unterliegt. Zutreffender Ansicht nach liegt weder bezüglich des Informationsgehalts der Daten noch bezüglich der Speicherung der konkreten Daten – durch Veränderung des physikalischen Zustands kleinster Partikel – eine Sache vor (Fischer, 2011, § 303a Rdn. 18, Haft, 1987, S. 10; Rombach, 1990, S. 104 f.). Konsequenz dieser Auffassung war die Einführung der §§ 303a, 303b StGB, um auch die »Datenbeschädigung« erfassen zu können. Anderer Ansicht nach ist das Überspielen eines Tonbandes oder eines sonstigen Datenträgers mit einer Veränderung dessen physikalischer Sachsubstanz und damit mit

einem Eingriff verbunden, so dass § 303 Abs. 1 StGB bezüglich des Datenträgers neben § 303a Abs. 1 StGB bezüglich der auf dem Datenträger gespeicherten Daten treten würde (Stree & Hecker, 2010, § 303a Rdn. 25 m.w.N.) Beschädigt wäre ein Datenträger freilich nur bei Veränderung darauf gespeicherter Daten; das bloße Hinzufügen von Daten – und in weiterer Konsequenz wohl auch die hierfür notwendige, unerhebliche Veränderung von Metadaten – ist nicht tatbestandsmäßig.

Schutz der Funktionsfähigkeit

Datenveränderung Die informationstechnische Funktionsfähigkeit eines informationstechnischen System steht und fällt mit der Integrität der Daten. Aus der soeben aufgezeigten Unsicherheit betreffend des strafrechtlichen Schutzes der Daten erklärt sich die Einführung des Straftatbestandes der Datenveränderung, § 303a Abs. 1 StGB. Dessen Tatobjekt sind Daten in ihrer konkreten Form, über die der Täter keine Verfügungsberechtigung hat. Diese sind gelöscht, wenn sie unwiederbringlich und vollständig unkenntlich gemacht wurden. Die typischen Löschfunktionen des Betriebssystems bewirken hingegen nur ein – ebenso tatbestandsmäßiges – Unterdrücken von Daten. Sie sind unbrauchbar gemacht, wenn sie in ihrer Gebrauchsfähigkeit beeinträchtigt sind, und schließlich verändert, wenn deren Informations- oder Aussagegehalt nunmehr ein anderer ist.

Zwei Einschränkungen der Strafbarkeit sind jedoch bedeutsam: Erstens sind auch hier, äquivalent zur Sachbeschädigung, ganz unerhebliche Verletzungshandlungen aus dem Tatbestand auszuschließen, wenn etwa der Originalzustand ohne nennenswerten Aufwand aus einer Sicherungskopie rekonstruiert werden kann (Hilgendorf, 2009, § 303a Rdn. 8).

Zweitens ist das bloße Kopieren von Daten und nachfolgende Veränderungen der Kopie nicht tatbestandsmäßig: Als Skribent der Kopie ist der Kopierende insoweit verfügungsberechtigt (Fischer, 2011, § 303a Rdn. 12; Malek, 2005, Rdn. 177) Ebenso nicht erfasst ist das Hinzufügen von Daten, soweit hierdurch keine anderen Daten unbrauchbar, verändert, unterdrückt oder gar gelöscht werden (Fischer, 2011, § 303a Rdn. 12; Hilgendorf, 2009, § 303a Rdn. 11; Hilgendorf et al., 2005, Rdn. 201 f.; a.A. wohl M. Gercke & Brunst, 2009, Rdn. 130). Das schlichte Hinzufügen eines Programms oder einer Datei auf einen Datenträger ist daher nicht tatbestandsmäßig, auch nicht im Hinblick auf die notwendige Veränderung der Metadaten auf Dateisystemebene, da es insoweit an jeglicher Erheblichkeit mangelt.

Computersabotage Als Tat- bzw. Angriffsobjekt setzt der Straftatbestand der Computersabotage (§ 303b Abs. 1 StGB) eine Datenverarbeitung voraus, die für einen anderen objektiv von wesentlicher Bedeutung ist. Datenverarbeitung sind alle Vorgänge, bei denen Daten unter Zuhilfenahme informationstechnischer Systeme erfasst, aufbereitet, umgewandelt oder bearbeitet werden. Für eine Strafbarkeit nach § 303b Abs. 1 StGB ist ferner erforderlich, dass der Täter die Datenverarbeitung nicht nur unerheblich beeinträchtigt, also gestört hat. An die Erheblichkeit können vergleichbare Anforderungen wie bei

§§ 303, 303a Abs. 1 StGB gestellt werden, so dass etwa bei ohne weiteren Aufwand verfügbaren Sicherheitskopien oder bei einer nur kurzzeitigen Nichterreichbarkeit einer Internetpräsenz der Taterfolg zu verneinen ist. Diese Störung wiederum muss durch eine der folgenden drei Varianten herbeigeführt worden sein:

- Der Täter hat eine Datenveränderung i.S.d. § 303a Abs. 1 StGB begangen,
- er hat Daten am informationstechnischen System eingegeben oder an dieses übermittelt, und hatte dabei die Absicht, jemanden einen Nachteil zuzufügen, oder
- er hat eine Manipulation an der Hardware vorgenommen, etwa durch eine Sachbeschädigung, aber auch durch bloße Unterbrechung der Stromzufuhr.

Vorbereitungsdelikte

Die Kriminalisierung verschiedener Vorbereitungsdelikte der Cyberkriminalität in den §§ 263a Abs. 3, 202c StGB, letzteres auch i.V.m. §§ 303a Abs. 3, 303b Abs. 5 StGB, stößt im Wesentlichen aus zwei Gründen auf rechtspolitische Kritik: Einerseits wird die – auch generell – zunehmende Tendenz des Gesetzgebers in Frage gestellt, bereits im Vorfeld signifikanter Rechtsverletzungen mit den Mitteln des Strafrechts einzugreifen (Herzog, 1991; Završnik, 2010). Besonders pikant sei dieser Auffassung zufolge etwa, dass bestimmte Vorbereitungshandlungen zu einem Ausspähen oder Abfangen von Daten gemäß § 202c StGB unter Strafe stünden, nicht jedoch der – in zeitlich näherer Folge zur Rechtsverletzung liegende – Versuch dieser Delikte (Gröseling & Höfinger, 2007, S. 628 ff.; Schumann, 2007, S. 679).

Andererseits aber ist problematisch, dass viele Programme, die zu strafrechtswidrigen Zwecken eingesetzt werden und daher vom Anwendungsbereich dieser Strafnormen erfasst sein können, auch höchst nützliche Dienste bereitstellen, um Sicherheitslücken in IT-Systemen aufzudecken. Doch selbst vermeintlich »eindeutige« Fälle schädlicher Programme finden unter IT-Sicherheitsexperten und nunmehr auch von staatlicher Seite – Stichwort: Online-Durchsuchung informationstechnischer Systeme – Verwendung. Die Vorbereitungsdelikte werden daher als einengende Kriminalisierung legitimer Verhaltensweisen verstanden (vgl. Borges, Stuckenberg & Wegener, 2007; Böhlke & Yilmaz, 2008; Cornelius, 2007; I. M. Hassemer & Ingeberg, 2008).

Diese Vorbereitungsdelikte knüpfen in einer Variante an Computerprogramme an, »deren Zweck die Begehung« einer folgender, bereits oben beschriebener Straftaten ist:

- Aussphähen von Daten (§ 202a Abs. 1 StGB),
- Abfangen von Daten (§ 202b StGB),

- Computerbetrug (§ 263a Abs. 1 StGB),
- Datenveränderung (§ 303a Abs. 1 StGB), und
- Computersabotage (§ 303b Abs. 1 StGB).

Die Tathandlungen betreffend Computerprogramme unterscheiden sich zwischen der Vorbereitung eines Computerbetrugs und den anderen Vorbereitungstatbeständen nur marginal und ohne große praktische Relevanz; eine Anpassung des § 263a Abs. 3 StGB an den Wortlaut des § 202c Abs. 1 Nr. 2 StGB sei aber angeregt (so schon oben 7.3.4., S. 107). Strafbar macht sich jedenfalls, wer solche Programme herstellt oder sich oder einem anderen verschafft, d.h. wenn der Täter, oder ein Dritter, die Verfügungsmacht – also die uneingeschränkte Nutzungsmöglichkeit – über ein Tatobjekt erlangt.

Schwierigkeiten bereitet nun aber der subjektive Tatbestand: Wie weitgehend muss der Täter bei der Herstellung oder bei dem Download eines solchen Programms bereits eine spätere Straftat konkretisiert haben? Einigkeit besteht dahingehend, dass diese wenigstens in ihren wesentlichen Umrissen feststehen muss (BVerfG ZUM 2009, 745, 750; Fischer, 2011, § 202c Rdn. 8 i.V.m. § 194 Rdn. 5; § 149 Rdn. 5; Hilgendorf, 2010b, § 202c Rdn. 28; Gröseling & Höfinger, 2007, S. 629). Ob darüber hinaus auch Wissentlichkeit oder Absicht vorliegen muss, ist umstritten und wird bisweilen auch trotz identischem Wortlaut bei § 202c Abs. 1 Nr. 2 StGB und § 263a Abs. 3 StGB unterschiedlich gesehen (so M. Gercke & Brunst, 2009, Rdn. 124 ff. entgegen Rdn. 196); das Bundesverfassungsgericht hat diese Frage noch offen gelassen (BVerfG ZUM 2009, 745). Sie hat aber bereits deswegen geringe praktische Bedeutung, weil nach dieser Rechtsprechung des Bundesverfassungsgerichts die Hürden an die Annahme eines tauglichen Tatobjekts hoch zu setzen sind: Ein Programm verfolge nur dann einen illegitimen Zweck im Sinne der Vorschriften, wenn es »mit der Absicht entwickelt oder modifiziert« wurde, es zur Begehung solcher Straften einzusetzen; diese Absicht müsse »sich ferner objektiv manifestiert haben« (BVerfG ZUM 2009, 745, 749 f.; krit. hierzu Höfinger, 2009; s. ferner Hornung, 2009; Popp, 2008; Stuckenberg, 2010). Wünschenswert wäre jedoch gleichwohl eine normative Klarstellung in §§ 202c, 263a StGB und auch in §§ 108b UrhG, 4 ZKDSG, wie sie auch an anderer Stelle im StGB zu finden ist (so auch Holzner, 2009):

> (2) § 149 Abs. 2 und 3 gilt entsprechend. *Absatz 1 ist nicht anzuwenden, wenn die Handlung der Wissenschaft, der Forschung oder der Lehre oder der Erfüllung rechtmäßiger beruflicher oder dienstlicher Pflichten dient.*

§ 202c Abs. 1 Nr. 1 StGB stellt auch das Verschaffen von Passwörtern und Sicherungscodes zur Vorbereitung einer Straftat nach §§ 202a, 202b StGB – und auch §§ 303a, 303b StGB – unter Strafe. Auf das fehlende Äquivalent bei § 263a Abs. 3 StGB und auf die praktischen Konsequenzen wurde bereits oben 7.3.4., S. 107 hingewiesen.

Angriffsmethoden

Viren, Trojaner und Würmer Die Herstellung, der Download, der Besitz und auch die Verwendung von Schadsoftware als solcher unterfällt daher nicht einem bestimmten Straftatbestand. Statt dessen ist zu differenzieren; hierbei zeigt sich, dass Strafbarkeitslücken nicht bestehen (s. auch Eichelberger, 2004; Ernst, 2003):

- Wird eine auf einem fremden Rechner installierte Schadsoftware *verwendet*, etwa
  - um heimlich Bild- oder Tonaufnahmen,
  - um auf einen anderen Rechner und dort gespeicherte, gesicherte Daten zuzugreifen – hier reicht die bloße Möglichkeit zur Verwendung aus –,
  - um Daten zu löschen oder zu unterdrücken, oder
  - um hierdurch auf dritte Computersysteme schädigend und in Nachteilszufügungsabsicht zuzugreifen,

  so begeht der Täter hierdurch jeweils ohne Weiteres eine der bereits aufgezeigten Straftaten – § 201, 201a, 202a, 303a oder 303b StGB.

- Wird eine Schadsoftware auf einen fremden Rechner *aufgespielt*, so kommt es auf die konkrete technische Vorgehensweise an. In aller Regel erfolgt wenigstens zwischenzeitlich eine Veränderung von anderer Software, etwa durch das Ausnutzen einer Sicherheitslücke und dem Einschleusen veränderter Programmanweisungen. In all diesen Fällen liegt bei diesem Zwischenschritt eine strafbare Datenveränderung gemäß § 303a Abs 1 StGB vor (vgl. auch Hilgendorf et al., 2005, Rdn. 202). Ob in den übrigen, wenigen und eher theoretischen Fällen eine Straftat gemäß § 303b Abs. 1 Nr. 2 StGB vorliegt (in diese Richtung Weidemann, 2010, § 303b Rdn. 10), oder ob dieser Zwischenschritt im Einzelfall straflos sein könnte, bedarf noch weiterer rechtswissenschaftlicher Klärung.

- Wird eine entsprechende Schadsoftware – mit den aufgezeigten objektiven und subjektiven Anforderungen – *hergestellt* oder *verschafft*, so macht sich der Täter bereits hierdurch gemäß § 202c Abs. 1 StGB, ggf. i.V.m. §§ 303a Abs. 3, 303b Abs. 5 StGB strafbar.

Spam Der Versand von unerwünschten E-Mails (Spam), der zumeist kommerziell motiviert ist, unterliegt als solcher keinem strafrechtlichen Verbot. Anderes gilt freilich, soweit der Inhalt einer E-Mails einem strafrechtlichen Verbot unterliegt, so etwa, wenn hierdurch unerwünschte Bilder pornographischen Inhalts (§ 184 Abs. 1 Nr. 6 StGB) oder kinderpornographische Bilddateien (§ 184b Abs. 2 StGB) versandt oder Schadsoftware verbreitet wird. Je nach Tatkonstellation kann allerdings eine Fälschung beweiserheblicher Daten gemäß § 269 Abs. 1 StGB oder auch eine Verletzung urheber- und markenrechtlicher Strafbestimmungen vorliegen (vgl. grundlegend Frank, 2004).

Im Kern handelt es sich aber bei Spam um eine bloß lästige Angelegenheit, der durch zivil- und auch ordnungsrechtliche (vgl. etwa § 6 Abs. 2 TMG) Maßnahmen begegnet werden kann. Soweit keine weiteren Schädigungen erfolgen ist ein Einsatz des Strafrechts nicht erforderlich; legislativer Änderungsbedarf ist daher derzeit nicht gegeben.

Denial-of-Service-Attacken Bei einer Denial-of-Service-Attacke wird ein – zumeist netzwerkbasiertes – informationstechnisches System durch eine geschickte oder massenhafte Dateneingabe derart überlastet, dass es auf weitere (legitime) Anfragen nicht mehr reagiert.

Einer Literaturauffassung zufolge liege hierdurch eine Datenunterdrückung vor, die bereits von § 303a Abs. 1 StGB erfasst werde (so M. Gercke & Brunst, 2009, Rdn. 130 m.w.N.). Dies überzeugt jedoch nicht: Nicht die Daten als solche werden unterdrückt, sondern es wird nur einer von mehreren Zugangswegen blockiert. Richtigerweise stellt daher die vorherrschende Auffassung in der Literatur auf § 303b Abs. 1 Nr. 2 StGB ab (Hilgendorf, 2009, § 303b Rdn. 10), der neben der Eingabe oder Übermittlung von Daten auch erfordert, dass es sich um eine Datenverarbeitung handelt, die für einen anderen von wesentlicher Bedeutung ist – was bei typischen Angriffszielen, etwa Internetauftritten von Unternehmen, aber in aller Regel gegeben ist. Ferner ist die Absicht des Täters erforderlich, dem Opfer einen Nachteil hinzuzufügen. Nach nicht unumstrittener Auffassung fehlt es hieran auch, wenn es sich um eine – nach Art. 5 Abs. 1 GG schützenswerte – konzertierte Meinungsäußerung (»Online-Demonstration«) handelt. Dem ist jedenfalls dann zuzustimmen, wenn es sich – vergleichbar »Offline-Demonstrationen« – nur um eine temporäre (etwa bloß wenige Stunden andauernde) Aktion handelt, andernfalls das Recht der Meinungsäußerung in rechtsmissbräuchlicher Weise ausgeübt würde (s. zu alledem auch BT-Drucks. 16/5449; OLG Frankfurt a.M. StV 2007, 244; sowie Kelker, 2009; Wolff, 2008, § 303b Rdn. 29).

7.3.7. Privilegierungen des Telemedienrechts

Das Internet ist durch das Zusammenwirken verschiedenster Akteure geprägt: so ist es alles als unüblich, dass ein Benutzer A in einem Forum, das auf einem Internetserver eines Hosting-Providers B, der von C betrieben und administriert wird, eine Nachricht hinterlässt, die sodann über einen »Access-Provider« D an einen anderen Benutzer E übertragen wird. Seit März 2007 besteht eine einheitliche und umfassende Regelung in §§ 7 ff. TMG, um die Verantwortlichkeit der verschiedenen Akteure klar voneinander abzuschichten. Nur durch einen solchen Rechtsrahmen wird den Akteuren hinreichende Rechtssicherheit geboten, um das Internet zu einem der Informations- und Kommunikationsfreiheit dienendem Medium zu entwickeln.

Die §§ 7 ff. TMG haben eine Querschnittswirkung dahingehend, dass sie eine Privilegierung im Öffentlichen Recht, im Zivilrecht und auch im Strafrecht entfalten. Daher

werden diese Fragen auch in allen drei Rechtsgebieten vertieft behandelt (Bleisteiner, 1999; Sieber, 1999c) und sollen hier nur knapp umrissen werden:

- Übermittler und Zugangsvermittler (*Access Provider*) zu fremden Inhalten sind nicht verantwortlich, wenn sie die übermittelten Informationen weder ausgewählt haben, noch (inhaltlich) verändert haben, noch mit einem Nutzer zusammengewirkt haben, um eine rechtswidrige Handlung zu begehen (§ 8 TMG).
- Wer für jemand anderen Informationen speichert und zum Abruf auch durch Dritte bereithält (*Hosting Provider*), ist für fremde Inhalte nicht verantwortlich, es sei denn, er hat positive Kenntnis des konkreten Inhalts und wurde sodann nicht unverzüglich tätig, um die Informationen zu entfernen oder den Zugang zu sperren (§ 10 TMG)

Höchst umstritten ist – auch aus rechtspolitischer Sicht – die Behandlung von Sprungmarken im Internet (*Hyperlinks*). Die Rechtsprechung erkennt bei Hyperlinks keine Haftungsprivilegierung per se an (s. nur BGH JZ 2008, 738). Dies ist *de lege lata* auch stimmig: Je nach Kontext des Hyperlinks kann sich der Autor die fremde Internetseite (»erste Ebene«) zu Eigen machen (etwa: »wie unter http://internetadresse/ fälschlicherweise behauptet wird«) oder auch die dort angegebenen Hyperlinks (»zweite Ebene«, etwa: »wie auf den von http://internetadresse/ verlinkten Seiten ersichtlich«), oder aber auch bloß auf fremde Inhalte verweisen. Zudem liegt weder eine Speicherung noch eine Übermittlung von Informationen vor. Schließlich entspricht dies dem ausdrücklichen Wunsch des historischen Gesetzgebers (vgl. M. Gercke & Brunst, 2009, Rdn. 630).

Bemerkenswert ist lediglich die Alternative der Zugangsvermittlung (§ 8 Abs. 1 Alt. 2 TMG), die allerdings historisch auf »Access Provider« gemünzt ist und gerade nicht die – zudem ausgewählte, § 8 Abs. 1 Nr. 3 TMG – Angabe von elektronisch auswertbaren Referenzen meint, sondern den technischen Zugang zu einem Internetdienst. Nur eine Minderheitsauffassung in der Literatur wendet daher auf die »zweite Ebene« von Verlinkungen § 8 Abs. 1 Alt. 2 TMG an (Hilgendorf et al., 2005, Rdn. 334). Richtigerweise ist in solchen Hyperlink-Konstellationen kritisch zu hinterfragen, ob derjenige, der einen solchen Hyperlink setzte, überhaupt vorsätzlich betreffend des dort vorgehaltenen Inhalts handelte. Zweitens ist auf die Meinungsfreiheit und auf die Notwendigkeit eines freien Diskurses hinzuweisen, auch um etwa auf Missstände wie demjenigen aufmerksam machen zu können, dass auf ausländischen Internet-Sperrlisten mitnichten nur Internetseiten kinderpornographischen Inhalts erwähnt waren, sondern zum Großteil harmlose Inhalte – weswegen in solchen Fällen, wenn überhaupt, die Schuld eines Täters, der eine solche Sperrliste verbreitet, als gering einzustufen ist.

7.3.8. Fazit

Der materiell-strafrechtliche Schutz gegen Cyberkriminalität ist insgesamt als adäquat, angemessen und ausreichend anzusehen. Nahezu sämtliche Verhaltensweisen, die erheblich sozialschädlich sind, unterfallen mindestens einer Strafnorm und können daher zu einer strafrechtlichen Reaktion und Sanktion führen. Dabei knüpfen die Strafnormen – insbesondere betreffend der »Internetdelikte« in §§ 202a, 202b, 202c, 303a, 303b StGB – bereits an frühe Stadien einer Rechtsgutsverletzung an bzw. kriminalisieren Vorbereitungshandlungen. Daher ist eine weitere Vorverlagerung der Strafbarkeit durch Einführung einer Versuchsstrafbarkeit nicht geboten und auch nicht erforderlich, um die in der Praxis bedeutsamen Kriminalitätsphänomene auch wirksam verfolgen zu können.

Betreffend mancher Strafnormen sind jedoch gewisse Modifikationen in Erwägung zu ziehen, so etwa zur Verfolgung des entgeltlichen Erwerbs von Kinderpornographie (s. oben 7.3.1., S. 90), zur zielgerichteten Verfolgung des *Phishing* und des *Skimming* (s. oben 7.3.4., S. 107) und zum Schutz von Daten, die einem Diensteanbieter anvertraut wurden (s. oben 7.3.2., S. 101). Ferner kann eine Verlagerung der §§ 17 ff. UWG in das StGB dazu dienen, die wirtschaftlichen Gefahren der Industriespionage zu verdeutlichen und so die strafrechtliche Reaktion effektiver zu gestalten (s. oben 7.3.2., S. 97).

Für eine demokratische Gesellschaftsordnung ist es unabdingbar, die Presse und insbesondere auch den investigativen Journalismus zu schützen. Die Aufdeckung auch von Missständen in der Wirtschaft ist selbst dann zu begrüßen, wenn es dabei zu einer Veröffentlichung von Geschäfts- und Betriebsgeheimnissen kommt – aber so die Öffentlichkeit etwa früher über die Beimischung von dioxinhaltigen Fetten in Futtermitteln informiert wird. Daher ist eine Ausweitung des ohnehin geplanten § 353b Abs. 3a StGB-E auch auf §§ 17, 19 UWG anzuregen (s. oben 7.3.2., S. 97).

In der IT-Sicherheitsforschung und in der digitalen Forensik besteht durch die Strafdrohung für die Vorbereitungsdelikte der §§ 263a Abs. 3, 202c StGB eine erhebliche Verunsicherung, auch wenn das tatsächliche Strafbarkeitsrisiko eher als gering einzuschätzen ist. Eine Klarstellung kann hier eine Straffreistellungsklausel für Handlungen bewirken, die der Wissenschaft, der Forschung oder der Lehre oder der Erfüllung rechtmäßiger beruflicher oder dienstlicher Pflichten dienen (s. oben 7.3.6., S. 118).

7.4. Zum Potential forensischer Analysen

Die Nachweisbarkeit einer Tat ist Grundlage für deren strafrechtliche Ahndung. Im Bereich der Cyberkriminalität hat man es in der Regel mit Nachweisen zu tun, die in Form *digitaler* Beweismittel vorliegen. Dies können Rechner, Festplatten oder Mobiltelefone sein, aber auch Mitschnitte von Netzwerkverkehr oder Abzüge von Webseiten. Die Sicherung und Analyse digitaler Beweismittel ist der Inhalt der digitalen Forensik. Bevor wir

uns der Frage widmen, ob die aktuellen strafprozessualen Eingriffsbefugnisse ausreichen, müssen wir uns Klarheit über das Potential der digitalen Forensik verschaffen.

Generell steckt die forensische Informatik, also die Anwendung wissenschaftlicher Methoden der Informatik auf die IT-Beweismittelsicherung und -analyse, noch in den Kinderschuhen. Die bisherige Entwicklung des Faches war sehr stark geprägt von Erwägungen aus der Praxis. Auch fehlt bisher eine substantielle Auseinandersetzung der forensischen Informatik mit anderen, lange etablierten forensischen Wissenschaften und deren Theorien (Inman & Rudin, 2000). Das Gebiet hat aber durch den Eingang von stärker offensiv ausgerichteten Techniken der IT-Sicherheit in den akzeptierten Themenkanon großer wissenschaftlicher Informatikkonferenzen in den letzten Jahren stark an Dynamik gewonnen, so dass man bereits grobe Entwicklungslinien erkennen kann, die wir im Folgenden Skizzieren wollen.

7.4.1. Technisch unvermeidbare Spuren

Die Grundvoraussetzung jeder Ermittlungsarbeit besteht in der Annahme, dass es das perfekte Verbrechen, also eine Tat ohne Spuren, in der Realität nicht gibt. In der Konsequenz bedeutet dies: Täter machen Fehler. In der Diskussion um Cyberkriminalität wird dieser Aspekt oft vernachlässigt, wenn etwa darauf abgehoben wird, wie leicht es ist, die eigenen Spuren im Cyberspace zu verwischen. Der einzige Unterschied zur realen Welt liegt darin, dass die Spuren im Cyberspace *digital* vorliegen.

Generell unterscheidet man zwei Arten digitaler Spuren:

- *Technisch vermeidbare Spuren* sind Spuren, die um ihrer selbst Willen erzeugt wurden. Beispiele hierfür sind Log-Dateien, Backups oder Zeitstempel in Dateisystemen. Aber auch jede Datei oder abgespeicherte E-Mail ist eine solche Spur.
- *Technisch unvermeidbare Spuren* hingegen sind Spuren, die unweigerlich anfallen und daher nicht durch einfache Änderungen an der Konfiguration eines Systems vermieden werden können. Beispiele hierfür sind gelöschte Dateien im Dateisystem, alte Stackframes im Hauptspeicher oder Inhalte des DNS-Caches.

Technisch vermeidbare Spuren sind leicht manipulierbar. So kann man beispielsweise eine E-Mail, die man auf der eigenen Festplatte abgespeichert hat, sehr leicht nachträglich verändern oder löschen. Technisch vermeidbare Spuren fallen in der Regel in großen Mengen an. In der digitalen Forensik hat sich hier ein eigener Zweig entwickelt, der sich mit der Analyse und Korrelation großer Datenmengen befasst und häufig als »*e-discovery*« bezeichnet wird. Derartige Problemstellungen sind aber auch aus anderen Bereichen bekannt. Zur Bewältigung der großen Aktenmengen in Wirtschaftsstrafsachen

werden beispielsweise häufig die Akten durch Dienstleister zunächst digitalisiert und anschließend elektronisch durchsuchbar gemacht.

Technisch unvermeidbare Spuren können zwar prinzipiell manipuliert werden. Eine Manipulation erfordert jedoch hohen Aufwand (hohe Expertise und spezielle Werkzeuge) oder birgt die Gefahr, dass das IT-System unbenutzbar wird.

Es gibt eine gewisse Analogie zwischen technisch unvermeidbaren digitalen Spuren und den mikroskopischen physischen Spuren (Haare, Fasern etc.), die von Kriminaltechnikern an Tatorten gesichert werden. Mikroskopische Spuren, insbesondere solche, die die eigene DNA enthalten, sind sehr schwer zu vermeiden. Entsprechend wird ihnen bei der Beweisaufnahme ein höherer Beweiswert zugemessen. Ähnliches gilt für technisch unvermeidbare Spuren.

7.4.2. Analyse von Speichermedien

Der Standardfall einer forensischen Analyse ist eine beschlagnahmte Festplatte oder ein vergleichbares Speichermedium. Bei der Untersuchung müssen die klassischen forensischen Prinzipien eingehalten werden: So muss jeder Schritt der Untersuchung im Nachhinein nachvollziehbar sein. Veränderungen am Beweismittel sind entweder ganz zu vermeiden oder nur in gut begründeten und genau zu dokumentierenden Ausnahmefällen erlaubt.

Abhängig von der verwendeten konkreten Technologie kann man aus einem Speichermedium sehr viele Informationen gewinnen. Ein wesentliches Untersuchungsfeld ist die Wiederherstellung gelöschter Dateien. Die Technik des »*file carving*« ermöglicht es sogar, Fragmente von größeren Dateien wie Bildern zu rekonstruieren. Moderne Dateisysteme erlauben zudem die Rekonstruktion von zurückliegenden Dateiversionen, anhand derer man die Modifikationen an einer Datei über die Zeit nachvollziehen kann. Eine Analyse von gebrauchten Festplatten im Rahmen einer universitären Lehrveranstaltung ergab, dass fast jeder Datenträger seinem ursprünglichen Besitzer zugeordnet werden konnte, auch wenn die Datenträger vollständig leer erschienen (Freiling, Holz & Mink, 2008).

Ein sich ebenfalls sehr schnell entwickelndes Gebiet ist die Analyse von Speichermedien aus Mobiltelefonen. Hier können in der Regel auch die mobilfunkspezifischen Daten wiederhergestellt werden, also Ruflisten, Kontaktlisten und Kurzmitteilungen.

Die prinzipielle Verfügbarkeit vieler Informationen auf einem Datenträger ist praktisch nur eingeschränkt durch die Vielzahl an Formaten und Versionen, die es heute im Bereich der Anwendungssoftware und der Betriebssysteme gibt. Man benötigt oft für jede spezifische Kombination ein spezielles Werkzeug. Die in der Praxis verfügbaren Werkzeuge decken nur einen kleinen Bereich an Kombinationen ab, der jedoch einen großen Prozentsatz der in der Praxis auftretenden Fälle ausmacht. Es gibt also noch eine Menge

an Dateisystemen und Anwendungsdateiformaten, die nicht effektiv analysiert werden können. Es hängt von der weiteren Entwicklungsdynamik des Feldes ab, ob und wie schnell auch diese Formate analysierbar sein werden.

Trotz der genannten Fortschritte der digitalen Forensik bleibt es weiterhin möglich, Daten unwiderruflich von Speichermedien zu löschen. Eine Möglichkeit besteht im Überschreiben der Daten mit anderen Daten. Aufgrund der hohen Integration moderner Festplatten ist es heute kaum mehr möglich, derart überschriebene Daten wiederherzustellen, auch wenn man dazu die Festplatte öffnet und im Labor untersucht. Im Gegensatz zu früher reicht heute in der Regel das einmalige Überschreiben aus (Wright, Kleiman & Sundhar R.S., 2008; Berghel & Hoelzer, 2006). Da dies kaum mit Bordmitteln des Betriebssystems durchführbar ist, benötigt man hierfür spezielle Werkzeuge, die jeweils für sich ihre Stärken und Schwächen haben.

Einen gewissen Sonderfall bilden Speichermedien auf Basis von Flash-Speichertechnologie. Hierzu gehören viele USB-Sticks, Speicherkarten und die so genannten *Solid State Disks*, also nicht-rotierende Festplatten, die meist in kleinen Notebooks verbaut sind. Dort ist technologiebedingt die Lebenszeit einzelner Speicherzellen abhängig von der Anzahl der Schreibzugriffe. Deswegen versuchen diese Speichermedien durch interne Algorithmen, die auf sie geschriebenen Daten möglichst gleichmäßig über alle Speicherzellen zu »verschmieren« (*wear levelling*). Es entstehen also innerhalb des Speichermediums deutlich mehr forensisch verwertbare Spuren als bei rotierenden Festplatten. Dieser Schatz wurde durch die forensische Informatik aber bisher noch nicht gehoben.

Die andere Möglichkeit, Daten unwiderruflich zu löschen, besteht in der *physischen Vernichtung* des Datenträgers. Hierzu gibt es, ähnlich Aktenvernichtern, bereits sehr eindrucksvolle Geräte am Markt, die keine Wünsche offen lassen. Im Zweifel sollte man ausgediente Datenträger immer physisch vernichten.

7.4.3. Umgang mit Verschlüsselung

Ein zunehmendes Problem für Strafverfolgungsbehörden ist der Einsatz von Verschlüsselungstechnologien. Zu unterscheiden sind dabei verschlüsselte Datenträger (z.B. Festplattenverschlüsselung oder verschlüsselte Dateicontainer) und verschlüsselte Kommunikationsinhalte.

Für die Analyse von verschlüsselten Datenträgern besteht immer die Möglichkeit, den Schlüssel zu erraten. Datenträgerverschlüsselung basiert in der Regel auf einen Schlüssel, der von einem Passwort abgeleitet ist. Hat man dieses Passwort, so hat man auch Zugang zum Datenträger. Abhängig von der konkreten Ermittlungssituation kann man also lange Listen von in Frage kommenden Passwörtern, die etwa aus dem Umfeld des Beschuldigten stammen, automatisiert ausprobieren.

Trifft man ein System mit aktiver Festplattenverschlüsselung im laufenden Zustand an, so kann man in der Regel leicht, nämlich auf dieselbe Art wie der Besitzer des Datenträgers, auf die Inhalte zugreifen. Entsprechende Techniken erfordern allerdings zur Beweismittelsicherung die Benutzung des zu untersuchenden Systems selbst. Wegen der Gefahr der Veränderung des Beweismittels muss man hierbei sehr vorsichtig vorgehen.

Trifft man das System im Standby-Modus oder im Ruhezustand an, gibt es eine vielversprechende Alternative zum Ausprobieren möglicher Passwörter. Im laufenden Betrieb wird der für die Verschlüsselung verwendete geheime Schlüssel notwendigerweise im Hauptspeicher des Rechners gehalten. Im Standby-Modus oder im Ruhezustand besteht die Möglichkeit, eine Kopie des Hauptspeichers anzufertigen und darin strukturiert nach möglichen Schlüsselkandidaten zu suchen. Dies funktioniert erstaunlicherweise in Form der so genannten *Cold Boot*-Angriffe auch bei kürzlich ausgeschalteten Computern (Halderman et al., 2009).

Prinzipiell möglich ist natürlich das Ausspähen des Passwortes durch einen im Vorgriff einer Beschlagnahme auf das System eingebrachte Spionagesoftware (*Remote Forensic Software*). Dies ist aus forensischer Sicht problematisch, da das Beweismittel notwendigerweise manipuliert wird. Durch die verdeckte Natur des Eingriffs und die Komplexität moderner IT-Systeme ist es zudem sehr schwer, die Aktivitäten der eingebrachten Software exakt und nachvollziehbar zu dokumentieren. Schließlich muss auch die Software selbst verdeckt operieren. Sie ist also nur vermeintlich einfacher durchzuführen als die oben genannte Speicheranalyse. Zur endgültigen Abschätzung wird es zunächst notwendig sein, die Speicheranalysetechniken zur Marktreife weiterzuentwickeln, um sie in der Praxis der Strafverfolgung zu erproben. Schließlich werden zugleich Techniken erforscht, die eine Speicheranalyse ins Leere laufen lassen (Müller, Dewald & Freiling, 2010).

Der Umgang mit verschlüsselter Kommunikation ist deutlich schwieriger als der Umgang mit verschlüsselten Datenträgern. In Kommunikationssystemen werden zur Verschlüsselung meist temporäre Schlüssel mit großer Länge verwendet. Das Ausprobieren vieler oder gar aller Kombinationen ist hierbei aussichtslos. Abhängig von der verwendeten Technologie besteht die Möglichkeit, den Service-Provider einzuschalten, falls dieser eine Möglichkeit für die Entschlüsselung besitzt. Möglich ist hingegen immer ein *Man in the Middle*-Angriff auf die Verbindung selbst. Dieser funktioniert auch durch das Abfangen der Daten vor oder nach der Verschlüsselung. Hierzu muss eine Spionagesoftware auf eines der beteiligten Endgeräte eingebracht werden, die verdeckt operiert. Ein solches Vorgehen wird als »Quellen-Telekommunikationsüberwachung« bezeichnet.

Bei der Quellen-Telekommunikationsüberwachung besteht demnach dieselbe forensische Problematik, die weiter oben bereits beschrieben wurde. Man gefährdet prinzipiell den Beweiswert der auf dem jeweiligen IT-System vorhandenen Daten. Angesichts der höheren praktischen Notwendigkeit erscheint uns eine hinreichend technisch und auch

rechtlich abgesicherte Quellen-Telekommunikationsüberwachung weitaus sinnvoller zu sein als ein genereller Einsatz von Spionagesoftware zu Strafverfolgungszwecken.

7.4.4. Rückverfolgbarkeit von Kommunikation

Die Rückverfolgbarkeit von Kommunikation ist im Cyberspace wegen der technischen Gegebenheiten ein großes Problem. Beispielsweise ist die De-Anonymisierung einer IP-Adresse durch den Service-Provider ein grundsätzliches Bedürfnis der Strafverfolgungsbehörden. Besonders relevant ist dies bei *dynamisch vergebenen* IP-Adressen. Ohne jegliche Möglichkeit, dynamische IP-Adressen aufzulösen, werden Ermittlungen im Bereich der Cyberkriminalität jedenfalls deutlich erschwert.

Aus Sicht der digitalen Forensik möchte man idealerweise den *Endpunkt* einer Kommunikation identifizieren, also den Ort, an dem die Kommunikation in den Cyberspace hinein- bzw. hinausgelangte. Dies ist nicht notwendigerweise immer durch die Ermittlung einer IP-Adresse erreicht. Schließlich kann diese IP-Adresse nur der Zwischenpunkt einer längeren Kette von separaten Kommunikationsverbindungen sein, wie sie etwa bei Anonymisierungsdiensten verwendet werden. Eine Rückverfolgung durch Abarbeiten der Kette ist praktisch unmöglich, insbesondere, wenn die Kommunikationsverbindungen häufig nationale Grenzen überwinden.

Ein Ansatzpunkt für die Rückverfolgung ist die Verwendung der Kommunikationsverbindung selbst. Wenn die Möglichkeit besteht, in den Kommunikationsvorgang selbst eigene Inhalte einzubringen, dann kann man unter Umständen später die direkte Kommunikation zwischen zwei Systemen nachweisen. Dies funktioniert analog zu Banknoten, die man mit unsichtbarer Farbe präpariert, um beispielsweise später einen Erpresser zu überführen. Hat ein Angreifer Zugang zu einem System erlangt, dann kann man versuchen, ihm spezifische Dateien zum Download anzubieten. Findet man diese Dateien später bei der Untersuchung eines beschlagnahmten Rechners auf dessen Festplatte, dann kann man nachweisen, dass dieser Rechner in den Kommunikationsvorgang involviert war. Diese Technik funktioniert meist nur dann, wenn man bereits einen kleine Personenmenge im Verdacht hat.

Das gleiche funktioniert auch in der Gegenrichtung. Grundlage hierfür ist das Einbringen eines Spionageprogramms auf den Rechner des Angreifers. Dieses Programm kann nun einerseits in regelmäßigen Abständen »Lebenszeichen« über das Netz an die Strafverfolgungsbehörden senden, was die Identifizierung des Aufenthaltsortes des Rechners erleichtert. Andererseits kann ein solches Programm auch verwendet werden, um den Rechner des Angreifers nach identifizierenden Merkmalen zu durchsuchen (Namen, E-Mail-Adressen, Telefonnummern). Da es sich hierbei wieder um eine verdeckte Maßnahme handelt, bestehen dieselben weiter oben bereits beschriebenen forensischen Probleme fort.

7.5. Strafprozessuale Eingriffsbefugnisse

Strafprozessuale Ermittlungen im Bereich der Cyberkriminalität verlaufen nicht fundamental anders als Ermittlungen in anderen Kriminalitätsbereichen. Hier wie dort sind – von gewissen Spezialzuständigkeiten abgesehen – die gleichen Behörden, die gleichen Akteure und auch die gleichen Gesetze anzuwenden. Hier wie dort ist es ein unerlässlicher Schwerpunkt der Ermittlungsarbeit, Opfer, Zeugen, Verdächtige und Beschuldigte zu befragen. Hier wie dort reicht das Kriminalitätsspektrum von massenhaft begangener, mit jeweils nur geringen Schäden verbundenen Delikten (hier Ladendiebstahl, dort Urheberrechtsverstöße) bis hin zu schwereren Kriminalitätsformen. Hier wie dort ist es grundsätzlich unproblematisch, wenn Polizeibeamte auf »Streife« gehen. Hier wie dort ist eine Öffentlichkeitsfahndung nach Verdächtigen und auch nach Zeugen zulässig, soweit die gesetzlichen Grundlagen erfüllt sind (vgl. hierzu etwa LG Saarbrücken wistra 2004, 279). Und hier wie dort ist es notwendig, die verfassungsrechtlichen Grundlagen des Strafprozessrechts zu achten (vgl. hierzu oben 4.5., S. 46).

Dennoch gibt es, von den transnationalen Aspekten (s. hierzu unten 8., S. 155) ganz abgesehen, Unterschiede, vor allem im praktischen Bereich: Da sämtliche Delikte der Cyberkriminalität nach der hier zugrunde gelegten Definition entweder über informationstechnische Systeme begangen werden oder diese unmittelbar angreifen, gelangt die forensische Auswertung dieser Systeme zu wesentlicher Bedeutung. Durch die vermehrte Speicherung und Archivierung erhalten umfangreiche Datenbestände, die von dritter Seite vorgehalten werden oder vorgehalten werden müssen, eine ungeahnte Bedeutung. Auch werden Forderungen nach dem verstärkten Einsatz verdeckter, technischer Ermittlungsmaßnahmen und verdeckter Datenbankabfragen laut, da sich die Cyberkriminalität nicht auf offener Straße abspiele und daher nur mit heimlichen Mitteln verfolgt werden könne.

In der folgenden Darstellung strafprozessualer Eingriffsbefugnisse zur Verfolgung von Cyberkriminalität soll daher ein Schwerpunkt gelegt werden auf diese Abweichungen von normalen Ermittlungsverfahren. Hierzu sollen zunächst die Besonderheiten vorgestellt werden, die sich betreffend Durchsuchungen, Beschlagnahmen und Herausgabeanordnungen (7.5.1.) insbesondere in Dreieckskonstellationen ergeben, also wenn sich beweisrelevante Daten nicht bei einem Beschuldigten, sondern bei einem Dritten befinden. Sodann folgt ein Überblick über die Telekommunikationsüberwachung, einschließlich der Überwachung der E-Mail-Kommunikation und der Quellen-Telekommunikationsüberwachung (7.5.2.), bevor auf die auch politisch heiklen Themen der Vorratsdatenspeicherung von Verbindungsdaten (7.5.3.) und der so genannten Online-Durchsuchung eingegangen wird (7.5.4.).

7.5.1. Durchsuchung, Beschlagnahme und Herausgabeanordnungen

Beschlagnahme und Sicherstellung

Unter einer Beschlagnahme versteht man die förmliche Sicherstellung eines Gegenstands, der nicht freiwillig herausgegeben wird, und der sodann in aller Regel amtlich zu verwahren ist (§ 94 StPO). Auch wenn sich die dogmatische Herleitung unterscheidet, so ist doch unstrittig, dass die gleichen Grundsätze auch für die Anfertigung und Sicherung einer digitalen Kopie eines Datenträgers gelten (vgl. nur BVerfGE 113, 29, 50). Gegenstand einer solchen Sicherstellung und Beschlagnahme können daher alle Gegenstände und Daten sein, »die als Beweismittel für die Untersuchung« – sprich: für das gesamte Strafverfahren – »von Bedeutung sein können« (§ 94 Abs. 1 StPO). Differenzierte Beschlagnahmeverbote enthält allerdings § 97 StPO bei Konfliktsituationen, die auch zu Zeugnisverweigerungsrechten führen – diese setzen sich nämlich auch in den schriftlichen Aufzeichnungen fort.

Ob jemand einen Gegenstand oder Daten freiwillig herausgeben darf oder ob es einer förmlichen Beschlagnahme bedarf, kann nicht der StPO entnommen werden, sondern nur den jeweiligen datenschutzrechtlichen Bestimmungen, so etwa den § 28 Abs. 2 BDSG (Brodowski, 2010a, S. 548 f.), §§ 14 Abs. 2, 15 Abs. 5 S. 4 TMG (M. Gercke & Brunst, 2009, Rdn. 641, 711), § 39 PostG oder auch den strafrechtlichen Geheimhaltungsvorschriften, etwa § 206 Abs. 2 StGB (Meyer-Goßner, 2010, § 99 Rdn. 2). Die Mitwirkungspflichten in Strafverfahren werden unten 7.5.1., S. 132 noch näher thematisiert.

Charakteristisch für eine Beschlagnahme nach den §§ 94 ff. StPO ist dabei erstens der einmalige, punktuelle Zugriff auf zu diesem Zeitpunkt vorliegende Gegenstände oder Daten. Es ist daher nicht möglich, über eine Beschlagnahme auch zukünftige Daten, wie sie etwa bei einer laufenden Überwachung der Telekommunikation anfallen, sicherzustellen. Hierfür sind andere Eingriffsgrundlagen erforderlich. Zweitens ist die Sicherstellung oder Beschlagnahme im Ausgangspunkt ein offener, kein verdeckter Zugriff. Der Betroffene ist daher über eine erfolgte Beschlagnahme zu informieren (§§ 35, 98 Abs. 2 S. 6 StPO), auch um ihm die Möglichkeit zu geben, gerichtlichen Rechtsschutz gegen eine Beschlagnahme in Anspruch zu nehmen. Ist allerdings der Gewahrsamsinhaber (ausschließlich) ein unverdächtiger Dritter – so etwa ein Kreditinstitut, das über verdächtige Kontenbewegungen informieren soll – so erfährt freilich unmittelbar nur dieses Kreditinstitut von der Beschlagnahme. Das Kreditinstitut selbst wird in aller Regel den Kunden nicht informieren, um sich nicht der Gefahr eigener Strafverfolgung wegen Strafverfolgungsvereitelung auszusetzen (§ 258 Abs. 1 StGB); die Benachrichtigungspflichten des § 101 StPO enthalten keinen Verweis auf §§ 94 ff. StPO. Dies führt aus grundrechtlicher Sicht zu erheblichen Defiziten bei solch kollusiven Zugriffen, insbesondere soweit eine Unterrichtung des Betroffenen entgegen §§ 33 Abs. 1, 35 Abs. 2 StPO unterbleibt (vgl. BGH NJW 2010, 1297, 1298).

Anordnung, Durchsuchung und Durchsicht der Papiere

Beschlagnahme: Anordnung und deren Voraussetzungen Die Anordnung einer Beschlagnahme richtet sich nach § 98 Abs. 1 StPO und unterliegt daher einem präventiven Richtervorbehalt. Bei Gefahr im Verzug können allerdings auch die Staatsanwaltschaft und deren Ermittlungspersonen eine Beschlagnahme anordnen, woraufhin allerdings eine gerichtliche Entscheidung folgen kann (§ 98 Abs. 2 StPO). Dabei ist die Verhältnismäßigkeit der konkreten Beschlagnahme kritisch zu würdigen: Die Schwere der Tat und die Stärke des Tatverdachts (nicht bloß Vermutungen) müssen also in einem angemessenen Verhältnis zur Beschlagnahme und Sicherstellung stehen und diese für die Ermittlungen notwendig erscheinen. Als Abwägungsfaktoren zu berücksichtigen sind dabei insbesondere, ob (auch) zugegriffen werden soll auf für das Verfahren irrelevante Daten, insbesondere nicht am Strafverfahren beteiligter Personen, auf höchstpersönliche Daten, etwa auf Patientenkarteien, auf umfangreiche Datenbestände oder auf solche Datenbestände, aus denen sich ein Persönlichkeitsprofil erstellen ließe. Bei alledem ist zusätzlich zu erwägen, ob der Umfang der Beschlagnahmeanordnung – etwa auf bestimmte Daten statt auf ganze Datenträger – reduziert werden kann (s. auch BGH NJW 2010, 1297).

Die Beschlagnahme selbst kann – je nach konkreter Situation – erstens durch Sicherstellung der Datenträger erfolgen, zweitens durch Anfertigung einer exakten, bitweisen Kopie. Drittens kann durch entsprechende technische Sicherungen ein »nur-Lese-Zugriff« auf den Datenträger erfolgen, und sodann nur die relevanten Dateien oder Daten gesichert werden. Viertens aber ist auch eine Analyse am laufenden System grundsätzlich gestattet (vgl. hierzu umfassend Bär, 2007c), was aber durch die damit zwangsläufig einhergehende Veränderung des zu untersuchenden Objekts den Beweiswert der so gewonnenen Beweismittel reduzieren kann.

Durchsuchung: Anordnung und deren Voraussetzungen Um aber überhaupt körperlichen Zugriff auf sicherzustellende Gegenstände zu erlangen, ist es in aller Regel erforderlich, Wohn- oder Geschäftsräume zu betreten und dort nach diesen Gegenständen zu suchen. Sofern sich der Betroffene hiermit nicht einverstanden erklärt, ist für einen solchen staatlichen Eingriff – auch und gerade in die Unverletzlichkeit der Wohnung, Art. 13 GG – eine entsprechende Ermächtigungsgrundlage mit prozeduralen und materiellen Hürden erforderlich. Diese finden sich in §§ 102 ff. StPO. Eine Durchsuchung unterliegt prozedural einem präventiven Richtervorbehalt; materiell reichen bei einem Verdächtigen »zureichende tatsächliche Anhaltspunkte« aus (BVerfG NJW 1991, 690), dass er eine Straftat bereits begangen hat. Bei Dritten ist hingegen eine Durchsuchung nur zulässig, wenn sich aufgrund bestimmter Tatsachen der Schluss ziehen lässt, dass sich dort bestimmte, konkret und präzise zu benennende verfahrensrelevante Gegenstände oder Spuren auffinden lassen (vgl. LG Frankfurt a.M. MMR 2004, 339; Bär, 2007d, Rdn. 353; M. Gercke & Brunst, 2009, Rdn. 961).

Hierzu ein Beispiel: Zureichende tatsächliche Anhaltspunkte liegen nicht vor, wenn über eine Internetverbindung einmalig binnen 45 Sekunden 46 Vorschau-Bilddateien kinderpornographischen Inhalts (*Thumbnails*) heruntergeladen werden: Dann sei es unwahrscheinlich, dass der Beschuldigte den Server mit kinderpornographischen Bildern gezielt aufgesucht und die Dateien heruntergeladen habe, sondern vielmehr wahrscheinlich, dass es zum Übersenden der Bilder nur durch Verlinkung mit anderen pornographischen Webseiten oder durch entsprechende Pop-Ups gekommen sei (LG Aachen MMR 2008, 764; s. hierzu M. Gercke, 2009a, S. 534). Daher war in diesem Fall eine Durchsuchung rechtswidrig.

Durchsicht vor Beschlagnahme Die bei der Durchsuchung aufgefundenen Papiere sind zunächst durchzusehen und nicht etwa pauschal zu beschlagnahmen (§ 110 Abs. 1 StPO). Das bereitet bei aufgefundenen Datenspeichern, Datenträgern und informationstechnischen Systemen durchaus Schwierigkeiten, insbesondere wenn umfangreiche forensische Analysen notwendig sind, um die wirklich beweiserheblichen Daten herauszufiltern. Bis dahin ist aber der gesamte Datenträger als beweisrelevant anzusehen und daher auch dessen Beschlagnahme und Sicherstellung zulässig; gleichwohl ist stets zu fragen, ob eine Anfertigung einer bitweisen Kopie und Rückgabe des Original-Datenträgers als milderes und verhältnismäßiges Mittel in Betracht kommt.

Durchsicht räumlich getrennter Speichermedien (§ 110 Abs. 3 StPO) Ist auch ein informationstechnisches System Objekt der Durchsuchung, so ermöglicht es § 110 Abs. 3 StPO, auch auf getrennte Datenspeicher im Inland zuzugreifen, diese durchzusehen und ggf. dort aufgefundene Daten zu sichern und der Beschlagnahme zuzuführen. Ist der Betroffene hiermit nicht einverstanden, so ist auf folgende Voraussetzungen zu achten:

- Erstens muss eine rechtmäßige, offene Durchsuchung vorliegen.
- Zweitens muss dabei ein informationstechnisches System (»Speichermedium«) aufgefunden worden sein.
- Drittens muss ein weiteres Speichermedium im Inland existieren, auf das zuvor vom Betroffenen zugegriffen wurde und das dieser – nicht etwa ein Dritter! – zur Speicherung von Daten nutzt.
- Viertens muss ein Zugriff auf dieses weitere Speichermedium von dem aufgefundenen informationstechnischen System aus möglich sein. Ob hierfür auch vorgefundene Passwörter eingegeben werden dürfen, ist umstritten, dürfte aber zu bejahen sein (so auch Meyer-Goßner, 2010, § 110 Rdn. 6; Schlegel, 2008, S. 28).
- Fünftens muss der Ausführende zur Durchsicht befugt sein. Das sind im Ausgangspunkt nur Beamte der Staatsanwaltschaft (§ 110 Abs. 1 StPO). Die Staatsanwaltschaft kann dies durch eine konkrete, vorherige Anordnung allerdings auch auf Ermittlungspersonen delegieren.

Aufgrund dieser kumulativen Anforderungen ist mit § 110 Abs. 3 StPO ein weitaus geringeres Missbrauchspotential verbunden als von Kritikern zunächst befürchtet. Bedenklich ist allerdings, dass sich in der Praxis nicht alle diese formalen Anforderungen auch durchgesetzt haben, sondern auch ein weitergehender Zugriff erfolgt: etwa auf bei einem E-Mail-Provider zum Abruf lagernde, ungelesene E-Mails, oder etwa auf passwortgeschützte Daten, zu denen kein Passwort aufgefunden wurde, aber ein Diensteanbieter einen Zugang bereitstellen kann. Hier ist auf eine Wahrung der Rechtsförmigkeit des Verfahrens zu achten, und die Staatsanwaltschaften und deren Ermittlungspersonen entsprechend zu instruieren und zu schulen.

Herausgabe- und Auskunftsverlangen

Anstatt selbst nach einem Gegenstand zu suchen, können die Strafverfolgungsbehörden auch die Herausgabe des Gegenstands verlangen (§ 95 Abs. 1 StPO). Dies kommt insbesondere bei unverdächtigen und unbeteiligten Dritten als milderes Mittel zu einer Durchsuchung in Betracht.

Vergleichbar einem Herausgabeverlangen, aber erneut milder ist ein Auskunftsverlangen: Dieses bezieht sich auf Daten oder sonstige Informationen, die dem Betroffenen zur Verfügung stehen, die dieser aber erst aufbereiten muss, um Auskunft zu erteilen: So etwa ein Kreditinstitut, das über Kontobewegungen Auskunft gibt. Ein solches Auskunftsverlangen ersetzt die (vorübergehende) Herausgabe sämtlicher Datensätze bzw. einer kompletten Datenbank und die anschließende Auswertung der Datenbank durch die Strafverfolgungsbehörden (Brodowski, 2010a, S. 549 m.w.N.).

Da es sich dennoch um Zwangsmittel handelt, gelten dieselben Anordnungsvoraussetzungen und damit auch ein präventiver Richtervorbehalt wie bei einer Beschlagnahme (vgl. Schäfer, 2004, § 95 Rdn. 20 m.w.N.). Ein Teil der Rechtsprechung und der Literatur verneint dies (vgl. Meyer-Goßner, 2010, § 95 Rdn. 2 m.w.N.), was aber erstens den psychischen Druck einer solchen Anordnung, zweitens die Regelungssystematik und drittens die regelmäßig zu schützenden Drittbelange außer acht lässt.

Noch milder ist es schließlich, wenn Strafverfolgungsbehörden gestützt auf die Ermittlungsgeneralklausel (§§ 161 Abs. 1, 163 Abs. 1 StPO) Privatpersonen oder Unternehmen um freiwillige Herausgabe oder um freiwillige Auskunft bitten.

Mitwirkungspflichten

Sind nun Privatpersonen und Unternehmen dazu verpflichtet, auf eine Bitte um freiwillige Herausgabe zu reagieren? Sind sie dazu verpflichtet, eine Datei zu entschlüsseln, wenn die Strafverfolgungsbehörden vermuten, dass sich in dieser Datei beweiserhebliche Daten befinden?

Eine solche Mitwirkung in Strafverfahren ist nicht nur für den Beschuldigten selbst eine Last: So mag es nahen Freunden oder Angehörigen höchst unangenehm sein, den Beschuldigten durch eigene Aussagen oder durch eigene Mitwirkung zu belasten. So mag es Unternehmen höchst unangenehm sein, sich selbst in das Licht der Öffentlichkeit zu ziehen, dass sie etwa Opfer einer Computerstraftat geworden sind. Dennoch: Es besteht eine grundsätzliche, nicht nur staatsbürgerliche sondern auch durchsetzbare Pflicht, an einem bereits eingeleiteten Strafverfahren mitzuwirken. Gewisse Konfliktlagen berücksichtigt allerdings die Rechtsordnung; damit erkennt sie auch an, dass es keine »Wahrheitsfindung um jeden Preis« geben darf.

Beschuldigte Aufgrund des auch verfassungsrechtlich und menschenrechtlich verbürgten Grundsatzes der Selbstbelastungsfreiheit (*nemo tenetur*) darf ein Beschuldigter nicht verpflichtet werden, aktiv zur Sachaufklärung beizutragen. Er darf auch nicht dazu gezwungen werden, Schriftproben abzuliefern, an einer Tatrekonstruktion mitzuwirken oder sonstwie aktiv tätig zu werden. Manche Ermittlungsmaßnahmen – die dann aber eine explizite Ermächtigungsgrundlage voraussetzen – muss er aber ebenso dulden wie das Strafverfahren als solches.

Aufgrund dieses Grundsatzes ist ein Beschuldigter auch nicht verpflichtet, einen kryptographischen Schlüssel (Passwort) preiszugeben. Dies bereitet erhebliche praktische Schwierigkeiten für die Strafverfolgungsbehörden, so dass verschiedene Lösungsansätze diskutiert werden (vgl. auch Gerhards, 2010):

- Erstens ermöglicht es ein verdeckter Zugriff auf einen Rechner – sei es durch eine optische Überwachung der Tastatur, sei es durch Einsatz einer *Remote Forensic Software* (Online-Überwachung) –, das verwendete Passwort zu ermitteln. Solche Maßnahmen sind aber derzeit strafprozessual nicht gestattet (s. näher unten 7.5.4., S. 150).

- Zweitens gibt es Bestrebungen, den Einsatz von Verschlüsselungstechnologie zurückzudrängen oder wenigstens »Zweitschlüssel« für staatliche Zwecke vorzuhalten (Werthebach et al., 2010, S. 131). Neben den Missbrauchsgefahren – es entsteht so ein Angriffspotential für Dritte, etwa für Wirtschaftsspionage – und den verfassungsrechtlichen Implikationen droht eine solche Vorgabe aber auch praktisch zu versanden, da sichere kryptographische Verfahren weltweit ohne Weiteres verfügbar sind.

- Einen dritter Ansatz liefert die britische Rechtsordnung, welche sich dem *nemo tenetur*-Grundsatz nicht verpflichtet sieht: Diese stellt die Weigerung, ein Passwort preiszugeben, unter Strafe (*Regulation of Investigatory Powers Act 2000, Part III, Art. 53*). Dies oder eine Beweislastumkehr, dass im Falle eines verschlüsselten Datenträgers der Beschuldigte seine Unschuld zu beweisen hätte, sind aber mit deutschen und wohl auch europäischen Vorgaben unvereinbar.

- Viertens – und dies scheint der erfolgversprechendste Ansatz zu sein – ist auf technische Möglichkeiten zur Umgehung oder zur Entsperrung von Verschlüsselungsmechanismen zu rekurrieren: Eine Überlistung des Täters war und ist den Ermittlungsbehörden stets gestattet. So ist es ohne Weiteres rechtlich zulässig, mit Hilfe von Wörterbuch-, Brute-Force- oder kryptographischen Angriffen die Verschlüsselung zu überwinden. So können durch kreative Möglichkeiten – etwa durch einen Zugriff auf ein laufendes oder auf ein soeben erst ausgeschaltetes informationstechnisches System – Informationen gewonnen werden, aus denen sich der kryptographische Schlüssel rekonstruieren lässt (s. oben 7.4.3., S. 126). Eine vertiefte Forschung in diesem Bereich und die Übertragung dieser Forschungsergebnisse in die kriminalistische Praxis erscheint der verfassungsrechtlich und auch rechtspolitisch beste Weg; eine Anpassung der strafprozessualen Rechtslage ist hierfür auch nicht erforderlich.

Dritte Unbeteiligte und unverdächtige Dritte sind grundsätzlich zur Mitwirkung in Strafverfahren verpflichtet. Sie müssen daher auf Herausgabe- und Auskunftsverlangen reagieren sowie spezialgesetzliche Auskunftspflichten wahren, um sich nicht der Gefahr auszusetzen, dass Zwangsmittel (insbesondere Ordnungsgeld bis zu 1.000 €, ersatzweise bis zu 42 Tage Ordnungshaft; Beugehaft von bis zu 6 Monaten) gegen sie verhängt werden. Ferner riskieren sie, dass die Strafverfolgungsbehörden statt milder Auskunfts- oder Herausgabeverlangen zukünftig Durchsuchungen durchführen werden. Sie sind jedoch grundsätzlich nicht verpflichtet, auf eine bloß freiwillige Bitte um Mitwirkung zu reagieren, also etwa auf eine Bitte um Auskunft. In der Praxis zeigen sich jedoch vor allem Unternehmen in weitem Maße dazu bereit, freiwillig auf ersten Zuruf der Polizei Auskunft zu erteilen, auch wenn hierdurch Drittbelange betroffen sind. Insbesondere bei besonderen Vertrauensverhältnissen und bei sensiblen Daten – und dies sind auch Finanztransaktionen – ist allerdings eine frühe Einbindung eines Richters geboten, um diese Drittbelange zu wahren (Brodowski, 2010a).

Ausnahmen von der Pflicht zur Mitwirkung gelten allerdings erstens bei beschlagnahmefreien Gegenständen (§ 97 StPO): Solche braucht niemand herauszugeben, und über deren Inhalt muss niemand Auskunft erteilen. Zweitens existieren gelegentlich spezielle Verwertungs- oder Verwendungsverbote, so etwa in § 20v Abs. 5 BKAG für manche im Rahmen eines verdeckten Zugriffs auf ein informationstechnisches System gewonnene Erkenntnisse, oder etwa für Zugriffe auf (manche) dem Fernmeldegeheimnis unterliegende Informationen. Drittens darf aufgrund des *nemo tenetur*-Grundsatzes auch die Vorlage solcher Gegenstände verweigert werden, durch die man sich selbst einer Straftat bezichtigen würde.

Auch bei Dritten stellt sich die Frage, wie mit nur verschlüsselt zur Verfügung stehenden, möglicherweise beweiserheblichen Daten umzugehen ist: Ein Dritter kann hier durch Anwendung der genannten Ordnungs- und Zwangsmittel zur Herausgabe der entschlüsselten

Daten oder auch zur Auskunft über das verwendete Passwort verpflichtet werden. Einzige Einschränkung hierfür ist das Verhältnismäßigkeitsprinzip, was aber nur bei Straftaten von geringem Gewicht dazu führen könnte, dass eine Verpflichtung zur Entschlüsselung entfällt. Das oben geschilderte Problem der Verschlüsselung durch den Beschuldigten stellt sich daher bei unverdächtigen Dritten nicht.

Fazit

Auf körperliche Gegenstände und auf verkörpert vorliegende Daten haben die Strafverfolgungsbehörden weitestgehende Zugriffsmöglichkeiten: So können sie bei einem Beschuldigten, wenn es nur zureichende tatsächliche Anhaltspunkte gibt, er könne eine Straftat begangen haben, durchsuchen und im Rahmen eines solchen Zugriffs auch räumlich getrennte Speichermedien durchsuchen.

Gegenüber Dritten sind zwar Durchsuchungen nur in engerem Rahmen zulässig, doch dies wird durch die Mitwirkungspflichten – und die noch darüber hinausgehende Mitwirkungsbereitschaft durch Unternehmen – mehr als nur ausgewogen. So sind Dritte grundsätzlich auch zur Entschlüsselung von verschlüsselten Datenbeständen oder auch zur Herausgabe eines Passworts verpflichtet.

Bedenken bereiten daher weniger die – das notwendige und gebotene Maß treffenden – strafprozessualen Eingriffsbefugnisse, sondern die zu häufige gesetzwidrige Anwendung: So etwa, wenn eine zeitnahe Benachrichtigung aller Betroffenen unterbleibt (mahnend BGH NJW 2010, 1297; s. aber BVerfG JR 2010, 543 zu einem eklatanten Fall unterbliebener Benachrichtigung) oder wenn ein präventiver Richtervorbehalt nicht gewahrt wird und Staatsanwaltschaft oder Polizei selbst Herausgabeverlangen anordnen, ggf. auch unter dem Deckmantel einer Zeugenvernehmung (s. hierzu Brodowski, 2010a, S. 548; Schnabel, 2009, S. 384): Zeugen können nur über *persönliche* Wahrnehmungen berichten und müssen sich nicht durch eigene Recherchen auf eine Vernehmung vorbereiten. Wann immer also Strafverfolgungsbehörden eine Auskunft aus einem elektronischen Datenbestand begehren – etwa Kontobewegungen bei einem Kreditinstitut –, so müssen sie ein entsprechendes auf § 95 StPO gestütztes Auskunftsverlangen stellen, das dem präventiven Richtervorbehalt unterliegt.

7.5.2. Telekommunikationsüberwachung

Mit Telekommunikationsüberwachung bezeichnet man alle staatlichen Eingriffe in die verfassungsrechtlich garantierte Fernmeldefreiheit (Art. 10 GG); sie zielt daher auf den »Inhalt der Telekommunikation und ihre näheren Umstände«, also auch auf die an ihr beteiligten Personen, ab.

Es wäre aber ein erster Trugschluss, dass nur die unmittelbare Kommunikation zwischen Menschen geschützt wäre: Auch die Kommunikation zwischen einem Mensch und

einer Maschine – einem informationstechnischen System – unterliegt diesem Schutz. Informationstechnische Systeme dienen nämlich auch einem mittelbaren kommunikativen Austausch zwischen Menschen, so etwa, wenn eine passwortgeschützte, verschlüsselte Internetseite aufgerufen wird, die Informationen enthält, die eine Person für eine andere Person dort bereitgestellt hat.

Ein zweiter, leider weitaus häufiger zu beobachtender Trugschluss ist es, allein daraus, dass § 100a StPO von »Telekommunikationsüberwachung« spricht, den Schluss zu ziehen, dass diese Norm alle nur denkbaren Eingriffe in die Fernmeldefreiheit aus strafprozessualer und auch aus verfassungsrechtlicher Sicht abdecken würde (Becker & Meinicke, 2011, S. 50). Dies ergibt sich bereits daraus, dass etwa §§ 99, 100g StPO ebenfalls Eingriffe in die Telekommunikationsfreiheit gestatten (Meyer-Goßner, 2010, § 99 Rdn. 1, § 100g Rdn. 3). Daher ist für jede strafprozessuale Eingriffsgrundlage zu fragen, auf welche Eingriffstypen sie jeweils zugeschnitten ist – und dies ist primär eine Frage des Strafprozessrechts. Sodann sind allerdings jeweils auch die verfassungsrechtlichen Anforderungen zu berücksichtigen, insbesondere die Prinzipien der Normenklarheit, der Normenbestimmtheit und der Verhältnismäßigkeit.

In diesem Abschnitt soll nun die Inhaltsüberwachung der Telekommunikation näherer Betrachtung unterzogen werden, wobei auch diese nicht nur in § 100a StPO, sondern etwa auch in § 99 StPO Niederschlag im Gesetz gefunden hat. Die Inhaltsüberwachung ist in der Strafverfolgungspraxis eine ausgesprochen beliebte Ermittlungsmaßnahme: 2009 wurde in 5.301 Strafverfahren eine Inhaltsüberwachung nach § 100a StPO angeordnet. Der Schwerpunkt liegt dabei allerdings auf der Überwachung von Festnetz- und Mobilfunkanschlüssen und darüber geführter Telefonate (3.470 bzw. 16.376 einzelne Anschlüsse), während die Überwachung des Internet-Datenstroms in vergleichsweise wenigen Fällen – 759 Anschlüsse – angeordnet wurde (Bundesamt für Justiz, 2010).

Telekommunikationsüberwachung im engeren Sinne

Anwendungsbereich Die typischste Maßnahme zur Inhaltsüberwachung von Telekommunikation ist aber die Telekommunikationsüberwachung im engeren Sinne, wie sie in §§ 100a, 100b StPO normiert ist. Auf dieser Grundlage können – soweit ist man sich einig – Eingriffe gestützt werden, mittels derer Telefonate an den Schaltzentralen der Telefonunternehmen ausgeleitet und zum Abhören und Aufzeichnen an die Strafverfolgungsbehörden weitergeleitet werden. Ebenfalls auf diesem technischen Wege können auch die Daten einer Datenfernübertragung, die zwischen einem (DSL-, Kabel-, Modem-)Teilnehmeranschluss und einem Internetanbieter transferiert werden, in Kopie an die Strafverfolgungsbehörden geleitet werden.

Die technische Mitwirkung der Telekommunikationsbetreiber ist dabei in der TKÜV näher spezifiziert; eine generelle Mitwirkungspflicht ordnet § 100b Abs. 3 StPO an.

Ferner gestattet §§ 100a, 100b StPO – auch das ist unstreitig – ein Abhören oder Abgreifen von Telekommunikation durch manipulative Veränderungen an den Telefon- und Datenleitungen; auch wenn eine Mitwirkung der Telekommunikationsbetreiber daher typisch für eine Maßnahme nach §§ 100a, 100b StPO ist, so ist sie dennoch nicht eine Voraussetzung hierfür.

Ob diese Eingriffsgrundlage allerdings auch einen Zugriff auf temporär ruhende Telekommunikationsdaten gestattet, etwa auf in einem Zwischenspeicher oder in einem E-Mail-Postfach lagernde Daten, oder ob hierfür andere Normen Anwendung finden, sei unten S. 141 näher diskutiert.

Verfahrensrechtliche Sicherungen Zur Wahrung der Verhältnismäßigkeit des signifikant grundrechtssensiblen Eingriffs in die Fernmeldefreiheit sehen die §§ 100a f. StPO sowohl verfahrensrechtliche als auch materiell-rechtliche Sicherungsmechanismen vor. Verfahrensrechtlich ist dabei zunächst auf den präventiven Richtervorbehalt hinzuweisen: Ein Richter hat die Rechtmäßigkeit vor Beginn einer Telekommunikationsüberwachung und sodann mindestens alle drei Monate neu zu überprüfen, und in einer zu begründenden Entscheidung genau zu spezifizieren, gegen wen und zur Überwachung welchen Anschlusses sich die Anordnung richtet (§ 100b Abs. 1, Abs. 2 StPO). Bis zu drei Tage lang kann allerdings bei Gefahr im Verzug auch die Staatsanwaltschaft eine Telekommunikationsüberwachung anordnen (§ 100b Abs. 1 StPO).

Eine zweite verfahrensrechtliche Garantie ist in der öffentlichen, anonymisierten Berichtspflicht über die im Laufe eines Jahres erfolgten Überwachungsmaßnahmen nebst Anlasstat zu sehen (§ 100b Abs. 5, Abs. 6 StPO), mehr noch aber in der nachträglichen Pflicht zur Benachrichtigung *aller* an überwachten Telekommunikationsvorgängen beteiligten Personen (§ 101 Abs. 4 S. 1 Nr. 3 StPO), die nur unterbleiben darf, wenn eine Person von dieser »Maßnahme nur unerheblich betroffen wurde und anzunehmen ist, dass sie kein Interesse an einer Benachrichtigung hat« (§ 101 Abs. 4 S. 4 StPO). Zugleich mit der Benachrichtigung ist über die Möglichkeit zu belehren, dass eine nachträgliche, erneute gerichtliche Überprüfung der Maßnahme erfolgen kann (vgl. BGHSt 53, 1; BGHSt 54, 30 zum Rechtsweg; BGH StV 2010, 169 zur Akteneinsicht).

Eine dritte verfahrensrechtliche Garantie liegt schließlich im Schutz des Kernbereichs privater Lebensgestaltung begründet (§ 100a Abs. 4 StPO). Diesen höchst unscharfen Begriff hat die Rechtsprechung bislang nur dahingehend konkretisiert, dass höchstpersönliche Gesprächsinhalte, etwa im engsten Familien- und Freundeskreis, mit Ärzten und Seelsorgern erfasst werden, nicht jedoch Gespräche – auch mit diesen Personen – die einen konkreten Bezug zu Straftaten aufweisen (BVerfGE 107, 279; s. auch Baldus, 2008). Kaum praktische Bedeutung wird allerdings § 100a Abs. 4 Satz 1 StPO zuteil, demzufolge eine Telekommunikationsüberwachung nicht angeordnet werden darf, wenn zu befürchten ist, dass *allein* kernbereichsrelevante Inhalte aufgezeichnet würden. Dies dürfte praktisch nur bei einer Telefonüberwachung einer Telefonseelsorge gegeben sein.

Dieser Norm lässt sich jedoch noch ein anderer Inhalt geben: Es ist stets nach Wegen zu suchen, die Überwachung eines Teilnehmeranschlusses noch weiter einzuschränken, indem etwa Telefonate zu bekanntermaßen unverdächtigen Dritten, zu denen der Überwachte ein höchstpersönliches Verhältnis pflegt, gar nicht erst aufgezeichnet werden. Größere Bedeutung haben hingegen die § 100a Abs. 4 Satz 2 bis 4 StPO: Den Kernbereich privater Lebensgestaltung betreffende Inhalte sind unverzüglich zu löschen – bis zu einer ersten Überprüfung dürfen sie allerdings gespeichert werden – und dürfen in keiner Weise für Strafverfahren verwendet werden.

Materiell-rechtliche Sicherungen Neben diesen verfahrensrechtlichen Sicherungen ist auch der materielle Anwendungsbereich der Telekommunikationsüberwachung begrenzt. Das bedeutet, dass diese Ermittlungsmaßnahme nur in manchen Ermittlungsverfahren und dabei nur in bestimmten Konstellationen eingesetzt werden kann. Diese materiellen Voraussetzungen hat in der Regel der Richter eigenständig, nur hilfsweise und vorübergehenderweise die Staatsanwaltschaft zu prüfen (s. hierzu Kinzig, 2004).

Erstens darf die Überwachung nur solche Anschlüsse betreffen, die dem Beschuldigten eines Strafverfahrens zuzuordnen sind. Anschlüsse von Dritten dürfen nur überwacht werden, wenn Dritte für den Beschuldigten als Nachrichtenmittler fungieren, oder aber wenn der Beschuldigte diesen Anschluss nutzt (§ 100a Abs. 3 StPO). Dass bei diesen Maßnahmen aber unter Umständen auch Unbeteiligte Telefonate oder Internetverbindungen nutzen, ist kein Ausschlussgrund für eine Telekommunikationsüberwachung, muss aber im Rahmen der Verhältnismäßigkeitsprüfung berücksichtigt werden.

Zweitens genügt nicht ein bloßer Anfangsverdacht, dass der Beschuldigte eine Straftat begangen hat. Erforderlich sind vielmehr »bestimmte Tatsachen«, wobei diesem Begriff kein zu großes Gewicht zuteil wird: Er soll nach der Rechtsprechung nur Vermutungen oder vage Anhaltspunkte ausschließen (BVerfG NJW 2005, 2603, 2610; BVerfG NJW 2007, 2749, 2751). Angesichts des präventiven Richtervorbehalts ist allerdings zu fordern, dass sich aus den bei den Akten befindlichen oder mündlich mitgeteilten Informationen ein wenigstens schemenhaftes Bild einer Tat zeichnen lässt, anhand derer der Richter oder – hilfsweise – der Staatsanwalt das Vorliegen auch der weiteren materiellen Voraussetzungen prüfen kann.

Drittens muss die Tat, auf die sich der durch »bestimmte Tatsachen« untermauerte Verdacht bezieht, dem Katalog der schweren Straftaten des § 100a Abs. 2 StPO unterfallen. Dabei handelt es sich größtenteils um Staats-, Gewalt- und Drogenkriminalität. Aus Sicht der Computerkriminalität sind nur wenige Deliktsgruppen hervorzuheben: Erstens die Verbreitung und die Besitzvermittlung kinderpornographischer Schriften (§ 184b Abs. 1 bis 3 StGB), aber nicht der Besitz oder die Besitzverschaffung an solchen Schriften, zweitens die gewerbs- oder bandenmäßige Verbreitung jugendpornographischer Schriften (§ 184c Abs. 3 StGB), und drittens bestimmte besonders schwere Fälle des Betruges und des Computerbetruges (§ 263 Abs. 3 S. 2, Abs. 5 StGB, auch i.V.m. § 263a Abs. 2 StGB).

Viertens darf keine milderere Ermittlungsmaßnahme zur Verfügung stehen, mit der – auch mit gewissem Mehraufwand – der gleiche Ermittlungserfolg herbeigeführt werden kann (§ 100a Abs. 1 Nr. 3 StGB).

Fünftens muss die Tat auch im Einzelfall schwer wiegen. Dies leitet bereits über zu einer allgemeinen Verhältnismäßigkeitsprüfung, in der die Schwere der konkreten Tat, die zu erwartende Strafe, die Schwere des konkreten Eingriffs, die Mitbetroffenheit Dritter und weitere Aspekte einer Gesamtabwägung zu unterziehen sind.

Anlasstaten in der Praxis Eine Auswertung der nach § 100b Abs. 5 und 6 StPO vorliegenden Statistik über die Praxis der Überwachung von Internet-Datenübertragungen im Jahr 2009 (Bundesamt für Justiz, 2010) wird dadurch erschwert, dass die Katalogtaten nicht nach den verschiedenen Kommunikationsformen aufgeschlüsselt werden. Insgesamt betrachtet überwiegt mit ca. 50% aller Anordnungen die Verfolgung der Betäubungsmittelkriminalität. Weitere 15% entfallen auf schwere Raub- und Bandendiebstahlsdelikte, 6% auf Mord und Totschlag. Betrugsdelikte – einschließlich Computerbetrug – dienen knapp 4% aller Anordnungen. Die für Cyberkriminalität geradezu archetypisch wirkende Deliktsgruppe der Kinder- und Jugendpornographie betraf nur 0.1% aller Anordnungen (19 Fälle) auf gleichbleibend niedrigem Niveau (Vorjahr: 14 Fälle, Bundesamt für Justiz, 2009).

Ausweitung des Deliktskatalogs? Diese Verteilung der Anlasstaten in der Praxis legt den Schluss nahe, dass die Telekommunikationsüberwachung nur eine äußerst geringe Bedeutung hat für die Verfolgung typischer Erscheinungsformen der Cyberkriminalität. Einzige erwähnenswerte Ausnahme ist dabei die Verfolgung schwerer Betrugsdelikte. Wenn aber diese Ermittlungsmaßnahme bereits jetzt nur marginal herangezogen wird zur Verfolgung verschiedener Erscheinungsformen der Cyberkriminalität, so erscheint es allein deshalb sehr zweifelhaft, ob eine Ausweitung auf weitere Erscheinungsformen zweckdienlich ist oder eine bloß symbolische Änderung darstellte.

Eine Ausweitung des Deliktskatalogs in § 100a Abs. 2 StPO auf weitere Straftaten der Cyberkriminalität wäre in weiten Teilen zudem weder angemessen noch zielführend: Sie wäre erstens nicht angemessen, da sich die Schwere einer Straftat stets auch an der Strafdrohung und der Bedeutung der betroffenen Rechtsgüter zu orientieren hätte. Aus den oben näher analysierten Deliktsbereichen der Computerkriminalität erfüllen dieses Merkmal allenfalls die in § 303b Abs. 4 StGB genannten besonders schweren Fälle der Computersabotage. Dabei ist allerdings auch zu berücksichtigen, dass zugleich eine auch politische Diskussion vonnöten ist, in welchem Rahmen und Umfang und in welcher Struktur eine »Online-Demonstration« – wie sie etwa 2001 gegen das Buchungssystem der Lufthansa und 2010 gegen Webseiten von Finanz- und Kreditkartenunternehmen im Zuge von Veröffentlichungen von WikiLeaks erfolgten – rechtlich zulässig sein sollen, und wann das rechtlich zulässige Maß überschritten und eine Strafbarkeit nach § 303b Abs. 4 StGB gegeben ist. Nach den oben bereits aufgezeigten Grundsätzen könnte eine

begrenzte, temporäre, sich nur in einer »Online-Demonstration« erschöpfende Aktion im Lichte der Meinungsäußerungsfreiheit hinzunehmen sein; bei einer nicht nur wenige Stunden andauernden Aktion dürfte jedoch eine grundrechtlich und auch strafrechtlich relevante Grenze erreicht sein (s. näher oben 7.3.6., S. 120).

Zweitens ist zu bezweifeln, dass eine Ausdehnung zielführend wäre: Ein wesentlicher Teil der Kommunikation hochgradig Krimineller im Internet erfolgt verschlüsselt, so dass deren Überwachung mit keinem oder nur kaum einem Informationsgewinn verbunden ist. Statt dessen verspricht eine Ausdehnung der Analyse der Zahlungsströme – nicht nur bei der Verfolgung des Marktes an kinderpornographischen Schriften (BVerfG JR 2010, 543) – weitaus spezifischere Erkenntnisse über strafrechtlich relevante Aspekte.

Überwachung von E-Mail-Kommunikation

Einen rechtlich schwierig zu beurteilenden Sonderfall stellen elektronische Kommunikationsformen dar, bei denen eine Nachricht nicht unmittelbar einen Empfänger erreicht, sondern es zu einer oder mehreren Zwischenspeicherungen kommt. Paradigmatisches Beispiel hierfür sind E-Mails, die unter Umständen über längere Zeit bei einem E-Mail-Provider darauf warten, bis der Empfänger diese liest, herunterlädt und löscht; dieselbe rechtliche Problematik stellt sich aber auch bei weiteren Kommunikationsformen wie etwa Nachrichten in sozialen Netzwerken.

Der technische Kommunikationsvorgang lässt sich dabei in bis zu sieben Phasen aufteilen (Brodowski, 2009, S. 402 m.w.N.):

1. Das Entwerfen einer E-Mail kann entweder »clientbasiert«, d.h. auf dem Rechner des Absenders erfolgen, oder aber die Rohdaten – einzelne Zeichen – werden in Echtzeit auf einen Mailserver eines E-Mail-Providers (»serverbasiert«) übertragen und dort gespeichert.

2. Sobald eine E-Mail abgesendet wird, wird die Nachricht an eine spezielle Software, einen Mail Transport Agent, übergeben, der die Nachricht auch um Meta-Informationen wie Datum, Uhrzeit und Absender vervollständigt.

3. Der Mail Transport Agent überprüft dabei, ob er überhaupt zur Annahme und Weiterleitung einer solchen Nachricht befugt ist, d.h. ob sich der Absender hinreichend legitimiert hat. Gelegentlich findet auch eine Inhaltskontrolle statt, bei der unerwünschte Nachrichten (etwa SPAM oder mit Schadsoftware versehene Nachrichten) ausgefiltert werden. Sodann ermittelt diese Software einen für die weitere Zustellung zuständigen Mail Transport Agent und versucht die Nachricht diesem zu übermitteln.

4. Gelangt nach – unter Umständen mehreren – Weiterleitungen die Nachricht auf den Zielserver, so leitet der dortige Mail Transport Agent an eine andere Software –

einen Mail Delivery Agent – aus, welche die Nachricht schließlich im Postfach des Empfängers abspeichert.

5. Der Empfänger kann nun die eingegangenen Nachrichten nach Belieben abrufen – sei es ein- oder mehrmalig, sei es vollständig oder teilweise – und sich auf einer Webseite anzeigen lassen (*Webmail*) oder auf einen lokalen Rechner abspeichern.

6. Bis zu einer Löschung der Nachricht aus dem serverseitigen Postfach wird diese dort noch vorgehalten, unter Umständen sogar noch darüber hinaus.

7. Nach Abruf einer Nachricht kann der Empfänger diese lokal speichern oder auch auf weiteren internetbasierten Diensten, etwa einer »Internetfestplatte« abspeichern.

Bezüglich mancher dieser Phasen besteht nun Einigkeit, auf welcher rechtlicher Grundlage ein strafprozessualer Zugriff erfolgen kann: Die Phasen 2, 3 und 5 betreffen die laufende Übertragung von Kommunikationsinhalten; daher ist insoweit allein ein Zugriff nach §§ 100a, 100b StPO gestattet. Eine benutzereigene Lagerung – von Entwürfen in der Phase 1, von empfangenen Nachrichten in Phase 7, oder auch generell von gespeicherten Kopien von versandten E-Mails – kann nach Maßgabe des Rechts der (offenen) Durchsuchung, Beschlagnahme und Sicherstellung (§§ 94 ff., 102 ff. StPO) abgegriffen werden.

Schwierigkeiten bereiten aber die Phasen einer benutzerfremden Lagerung, insbesondere in den Phasen 4 und 6: Bei einem einmaligen, offenen Zugriff im Kontext einer Durchsuchung reichen nach der Rechtsprechung des Bundesverfassungsgericht die §§ 94 ff. StPO, auch i.V.m. § 110 Abs. 3 StPO als Eingriffsgrundlage aus (BVerfGE 124, 43 m. Anm. u. Bespr. Brodowski, 2009; Brunst, 2009a; B. Gercke, 2009a; Härting, 2009; Klein, 2009; s. auch BGH NJW 2010, 1297). Allerdings sei die Verhältnismäßigkeit des Zugriffs im Einzelfall kritisch zu prüfen, der Betroffene von diesem Zugriff unverzüglich zu benachrichtigen und darauf zu achten, dass – ggf. durch Verwendung geeigneter Suchkriterien – nur verfahrensrelevante Daten abgegriffen werden (BGH NJW 2010, 1297). Die Literatur widerspricht dem unter Hinweis auf die Qualität des Grundrechtseingriffs und fordert eine Anwendung des strengeren Schutzes der §§ 100a, 100b StPO. Auch bei einer laufenden, (verdeckten) Überwachung auch zukünftiger Nachrichten während der Phasen 4 und 6 besteht Streit: Die Rechtsprechung wendet hierauf die Vorschriften über eine Postbeschlagnahme (§§ 99, 100 StPO) analog an (BGH JR 2009, 428), was dazu führt, dass die sichergestellten Nachrichten nur von einem Richter, im Einzelfall auch durch einen Staatsanwalt, nicht jedoch durch Polizisten durchgesehen werden dürfen (§ 100 Abs. 3 StPO). Die Literatur fordert wiederum eine Anwendung der §§ 100a, 100b StPO.

Aus diesem wirren Feld verschiedener Eingriffsbefugnisse und der je nach einmaliger Durchsicht oder laufender Überwachung unterschiedlichen Eingriffsbefugnisse kann

letztlich nur der Gesetzgeber heraushelfen. Auch wenn insbesondere bei verdeckten Zugriffen viel für die Anwendung der §§ 100a, 100b StPO spricht, so dürfte der Unterschied bei einer Anwendung der §§ 99, 100 StPO nur gering sein: Auch dieser ist angesichts des Verhältnismäßigkeitsprinzips nur zulässig bei schweren Straftaten, die wenigstens in den Bereich der Katalogtaten des § 100a Abs. 2 StPO hineinragen (Brodowski, 2009, S. 408; vgl. aber auch Graf, 2010, § 99 Rdn. 5; Meyer-Goßner, 2010, § 99 Rdn. 12; Nack, 2008, § 99 Rdn. 10). Im Lichte der neueren Rechtsprechung des Bundesverfassungsgerichts und des Bundesgerichtshofs wäre daher entweder zu erwägen, die Regelungen der §§ 99 und 100a StPO zu vereinheitlichen (Valerius, 2008), oder aber – und dies erscheint vorzugswürdig – § 99 StPO dahingehend zu ändern, dass auch »Sendungen der elektronischen Post« vom Anwendungsbereich dieser Norm erfasst werden. Sodann ergeben sich die von der Rechtsprechung zu recht geforderten Benachrichtigungspflichten, die Möglichkeiten zum (Dritt-)Rechtsschutz und die spezifische Verhältnismäßigkeit bereits aus dem Text dieser Norm und nicht aus einer einschränkenden Auslegung der doch recht weit gehenden Beschlagnahmevorschriften. § 99 Abs. 1 S. 1 StPO sei daher wie folgt neu gefasst:

> Zulässig ist die Beschlagnahme der an den Beschuldigten gerichteten Postsendungen, Telegramme *und Sendungen der elektronischen Post*, die sich im Gewahrsam von Personen oder Unternehmen befinden, die geschäftsmäßig Post- oder Telekommunikationsdienste erbringen oder daran mitwirken.

Hierdurch wäre klargestellt, dass ein Zugriff in den Phasen 4 und 6 stets nach §§ 99, 100 StPO zu erfolgen hat. Im gleichen Zuge müsste ein vergleichbarer Schutz des Kernbereichs privater Lebensgestaltung und eine vergleichbare Dokumentationspflicht auch für die Postbeschlagnahme im Gesetzestext verankert werden, etwa durch eine Verweisungsnorm in einem § 100 Abs. 7 StPO:

> (7) § 100a Abs. 4 und § 100b Abs. 5 und Abs. 6 finden entsprechende Anwendung.

Zusätzlich ist in § 110 Abs. 3 StPO klarzustellen, dass auch bei einem Zugriff bei einer offenen Durchsuchung die höheren Hürden der §§ 99, 100 StPO zu wahren sind. Dies könnte durch einen neuen § 110 Abs. 3 S. 2 StPO erfolgen:

> § 99 bleibt unberührt.

Quellen-Telekommunikationsüberwachung

Ein zweites, derzeit hoch umstrittenes Gebiet ist das der Quellen-Telekommunikationsüberwachung. Damit bezeichnet man ein Abgreifen von Inhalten einer Telekommunikation bereits am Rechner eines Beschuldigten oder Nachrichtenmittlers, die sodann an die Strafverfolgungsbehörden übermittelt werden. Hierdurch lassen sich manche Verschlüsselungsmethoden bei Echtzeitkommunikation umgehen, da ein Abgreifen der Inhalte *vor* der Verschlüsselung erfolgt. Praktische Relevanz erlangte dies vor allem bei Verwendung von Internettelefonie über Skype, die verschlüsselt erfolgt und auf die – jedenfalls in früheren Jahren – die Ermittlungsbehörden keine Zugriffsmöglichkeiten hatten.

Wie kann eine solche Quellen-Telekommunikationsüberwachung technisch erfolgen? Theoretisch denkbar sind zwei Modelle, wobei nur ein Modell rechtliche Schwierigkeiten aufwirft:

- Ein Softwareanbieter kann es durch geeignete technische Maßnahmen ermöglichen, dass im Falle einer Telekommunikationsüberwachung die Verschlüsselung mit einem den Ermittlungsbehörden bekannten Schlüssel erfolgt, oder aber, dass eine unverschlüsselte Kopie der Telekommunikationsinhalte auch an die Strafverfolgungsbehörden übermittelt wird. Eine solche Maßnahme greift nicht zusätzlich in die Vertraulichkeit und Integrität informationstechnischer Systeme ein und ist daher ohne Weiteres gemäß §§ 100a, 100b StPO zulässig.
- Ermittlungsbehörden können verdeckt auf den Rechner des Betroffenen zugreifen und auf diesem eine sogenannte *Remote Forensic Software*, also eine Spionagesoftware installieren und sodann mittels der erschlichenen Administratorenrechte eine Ausleitung der noch unverschlüsselten Telekommunikationsdaten bewirken. Diese Konstellation ist rechtlich umstritten.

Eine solche Maßnahme ist nämlich – gleich einer Online-Durchsuchung informationstechnischer Systeme – mit schwerwiegenden Begleiteingriffen verbunden, namentlich in die Integrität und Vertraulichkeit eines informationstechnischen Systems. Die Übernahme von Administratorenrechten ist stets eine vollständige, die etwa auch zur verdeckten Durchsicht von auf dem informationstechnischen System gespeicherten Daten, zur Ansicht von bloß eingegebenen Daten, die noch nicht Gegenstand einer Telekommunikation sind (etwa durch *Screenshots*, siehe hierzu LG Landshut, Beschl. v. 20.1.2011 – 4 Qs 346/10 –), zur verdeckten Überwachung von Gesprächen im Raum und auch zur optischen Überwachung missbraucht werden könnte (vgl. BVerfGE 120, 274, 310). Daher hatte auch das Bundesverfassungsgericht in seiner Entscheidung über die präventive Online-Durchsuchung informationstechnischer Systeme festgehalten, dass eine solche Quellen-Telekommunikationsüberwachung nur dann allein am Maßstab des Art. 10 Abs. 1

GG zu messen sei, wenn »durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt« sei, dass ausschließlich auf den laufenden Telekommunikationsvorgang zugegriffen werde (BVerfGE 120, 274, 309).

Dies nimmt eine höchst bedenkliche Auffassung in der Literatur (Meyer-Goßner, 2010, § 100a Rdn. 7a m.w.N.) und Rechtsprechung (AG Bayreuth MMR 2010, 266; LG Landshut, Beschl. v. 20.1.2011 – 4 Qs 346/10 –) zum Anlass, eine Quellen-Telekommunikationsüberwachung auf §§ 100a, 100b StPO zu stützen, obwohl diese Normen keine entsprechenden rechtlichen Vorgaben enthalten, obwohl diese Normen nicht einen solch atypischen Begleiteingriff gestatten und obwohl die technischen Vorgaben alles andere als leicht umzusetzen sind und ebenfalls eine rechtliche Kontrolle erfordern (s. zu alledem Becker & Meinicke, 2011; Vogel & Brodowski, 2009). Auch aus systematischen Erwägungen – schließlich ist in § 20l Abs. 2 BKAG eine spezielle Eingriffsgrundlage für eine präventive Quellen-Telekommunikationsüberwachung vorgesehen – ist ein solcher Eingriff unzulässig und rechtswidrig.

Wie eine rechtmäßige strafprozessuale Eingriffsbefugnis aussehen könnte, wurde bereits an anderer Stelle (Vogel & Brodowski, 2009, S. 634) ausführlich diskutiert, so dass es hier bei einer knappen Darstellung verbleiben kann: Angesichts der Eingriffstiefe ist an eine Katalogtat des § 100c Abs. 2 StPO und nicht des § 100a Abs. 2 StPO anzuknüpfen. Der Zugriff ist auf solche informationstechnische Systeme zu beschränken, über die der Beschuldigte ganz oder zum Teil selbständig verfügen kann. Schließlich ist durch rechtliche und technische Begleitbestimmungen – zu denken wäre etwa an eine Zertifizierung durch das BSI – abzusichern, dass nicht über die abzugreifende Telekommunikation hinausgehende Daten abgegriffen werden:

> § 100j [Quellen-Telekommunikationsüberwachung]
>
> (1) Auch ohne Wissen der Betroffenen darf die Telekommunikation in der Weise überwacht und aufgezeichnet werden, dass mit technischen Mitteln in vom Betroffenen ausschließlich oder überwiegend genutzte informationstechnische Systeme eingegriffen wird, wenn
>
> 1. bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in § 100c Absatz 2 bezeichnete besonders schwere Straftat begangen oder in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat,
> 2. die Tat auch im Einzelfall besonders schwer wiegt,
> 3. auf Grund tatsächlicher Anhaltspunkte anzunehmen ist, dass durch die Überwachung Äußerungen des Beschuldigten erfasst werden, die für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Mitbeschuldigten von Bedeutung sind,

4. die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Mitbeschuldigten auf andere Weise unverhältnismäßig erschwert oder aussichtslos wäre, und
5. durch technische Maßnahmen sichergestellt ist, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird.

(2) Die Anordnung darf sich nur gegen den Beschuldigten oder gegen Personen richten, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Beschuldigte überwiegend ihren Anschluss benutzt.

(3) §§ 100c Absatz 4 bis 7, 100d und 100e finden entsprechende Anwendung.

(4) Für Maßnahmen nach Absatz 1 dürfen nur vom Bundesamt für Sicherheit in der Informationstechnik im Hinblick auf Absatz 1 Nr. 5 zertifizierte technische Mittel eingesetzt werden.

Ob eine solche Änderung der StPO auch rechtspolitisch geboten ist, zeigt sich dabei bislang nicht in der gebotenen Deutlichkeit: schließlich gibt es effektive, mildere Alternativen zu einer solchen Quellen-Telekommunikationsüberwachung – sei es die Inpflichtnahme der Softwareanbieter, sei es die Überwindung von Verschlüsselungsmechanismen (s. hierzu Becker & Meinicke, 2011, S. 52), sei es eine akustische Wohnraumüberwachung, bei der auch das in Telefongesprächen gesprochene Wort mitgehört werden kann.

7.5.3. Bestandsdatenabfragen, Vorratsdatenspeicherung und die Verknüpfung von Datenbeständen

Bestands-, Verkehrs- und Inhaltsdaten

Über kaum ein anderes internetbezogenes strafrechtliches Thema wurde in den letzten Jahren so heftig diskutiert wie über die Vorratsdatenspeicherung von Verbindungsdaten. Zu einem besseren Verständnis der rechtlichen Problematik sei aber zunächst auf folgende Unterscheidung hingewiesen:

- *Bestandsdaten* sind solche Informationen, welche sich auf die »Begründung, inhaltliche Ausgestaltung oder Änderung« von Vertragsbeziehungen zwischen Diensteanbietern und Nutzern beziehen, also etwa Name und Anschrift des Nutzers (vgl. § 3 Nr. 3 TKG).
- *Verkehrsdaten* oder Verbindungsdaten sind diejenigen Informationen, welche sich auf die bloßen Umstände einer Telekommunikation beziehen, namentlich ob und

wann eine solche stattgefunden hat und wer an ihr beteiligt war, etwa durch Angabe der Empfänger- und Absenderadressen, einschließlich der IP-Adressen (vgl. hierzu der für nichtig erklärte § 113a Abs. 2 ff. TKG).

- *Inhaltsdaten* schließlich sind die durch die Telekommunikation übermittelten Daten; diesbezüglich ist auf die soeben diskutierte Inhaltsüberwachung zu verweisen.

Auskunftserteilung durch Telemedienanbieter

Tele*medien*anbieter – also etwa Betreiber einer Webseite – dürfen auf ersten Zuruf von Strafverfolgungsbehörden Auskunft über bei ihnen vorliegende Bestands- und manche Nutzungsdaten erteilen (§§ 14 Abs. 2, 15 Abs. 5 S. 4 TMG); also etwa Auskunft darüber geben, wann von einer bestimmten IP-Adresse auf eine Webseite zugegriffen oder unter welchen Angaben ein Konto bei einer Auktionswebseite eröffnet wurde. Allerdings sind diese Anbieter nicht zu einer derart weit reichenden Mitwirkung verpflichtet – gezwungen können sie nur werden durch ein entsprechendes Herausgabe- oder Auskunftsverlangen nach den §§ 94 ff. StPO. Die Gegenauffassung in der Literatur verlangt hingegen stets eine Anordnung gemäß §§ 94 ff. StPO, bisweilen sogar nach §§ 100a, 100b, 100g StPO (M. Gercke & Brunst, 2009, Rdn. 642, 712 f. m.w.N.). Dies kann aber nicht überzeugen, da es bei Zugriffen nach all diesen Regelungen einer datenschutzrechtlichen Spezialregelung im TMG nicht bedurft hätte. Daher reicht eine auf die Ermittlungsgeneralklausel (§§ 161 Abs. 1, 163 Abs. 1 StPO) gestützte Anfrage aus. Da bei Telemedienanbietern nur punktuelle Daten anfallen und §§ 14 Abs. 2, 15 Abs. 5 TMG den Zugriff auf bestimmte Datenkategorien beschränkt, ist dies auch aus verfassungsrechtlicher Sicht eine ausreichende Eingriffsgrundlage.

Auskunftserteilung durch Telekommunikationsanbieter

Gänzlich anders ist aber die Situation bei den Tele*kommunikations*anbietern, also den Nachrichtenmittlern: Aufgrund der weitaus umfassenderen Zugriffsmöglichkeiten und der daraus resultierenden Gefährdungslage unterliegt der Zugriff und die Nutzung von Verbindungsdaten einer weitaus kritischeren Überprüfung. Eine isolierte Anfrage von Bestandsdaten – also etwa: Ist Person X Kunde bei Ihnen, und falls ja, mit welcher Adresse ist er bei Ihnen registriert? – hingegen ist gleichermaßen unproblematisch.

Verwendungsmöglichkeiten für Verbindungsdaten Verbindungsdaten gelangen in zwei voneinander zu trennenden Weisen an Bedeutung:

- Erstens zur Zuordnung, welcher Kunde an einem bestimmten Telekommunikationsvorgang beteiligt war, also die Zuordnung einer IP-Adresse zu einem Kunden, dessen Namen und dessen Anschrift. Zur Beantwortung dieser Frage muss der Telekommunikationsanbieter zwar auf Verbindungsdaten zurückgreifen, die Antwort

an die Strafverfolgungsbehörden beschränkt sich sodann aber in der Preisgabe von Bestandsdaten.

- Zweitens zur Auswertung von Kommunikationsstrukturen – mit wem hatte ein Verdächtiger Kontakt? Hierfür benötigen die Strafverfolgungsbehörden einen detaillierteren Zugriff auf die Verbindungsdaten.

Hoch umstritten war bei der ersten Konstellation die Frage, ob die Anfrage, welchem Kunden eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war, sich auf Bestands- oder auf Verkehrsdaten bezieht (vgl. die Nachweise bei M. Gercke & Brunst, 2009, Rdn. 663). Nur bei ersterem wäre ein Zugriff gemäß § 113 TKG »auf Zuruf« möglich, letzteres erforderte einen Rückgriff auf die weitaus striktere Ermächtigungsgrundlage des § 100g StPO (vgl. M. Gercke & Brunst, 2009, Rdn. 666 ff.). Zwischenzeitlich war dieser Streit durch eine gesetzliche Fiktion in § 113b S. 1 Hs. 2 TKG dahingehend gelöst, dass bloß eine Bestandsdatenabfrage gemäß § 113 TKG vorliege (vgl. BVerfGE 125, 260, 340 ff.). Das Bundesverfassungsgericht hat dieses Vorgehen grundsätzlich gestattet: Eine solche mittelbare Nutzung von Verkehrsdaten sei grundsätzlich zulässig. Aufgrund von Mängeln in Randbereichen erklärte es § 113b S. 1 Hs. 2 TKG dennoch für nichtig. Bis auf weiteres fehlt daher derzeit eine hinreichende Eingriffsgrundlage auch für eine mittelbare Nutzung von Verkehrsdaten. Bis zu einer Neuregelung ist aber ein Zugriffs auf solche Daten jedenfalls unter den (engeren) Voraussetzungen des § 100g StPO zu dulden; die Praxis scheint aber auch auf die Ermittlungsgeneralklausel zurückzugreifen (vgl. nur HansOLG Hamburg K&R 2011, 54, 55 in einer zivilrechtlichen Entscheidung).

Speicherung von Verbindungsdaten auf Vorrat Auch eine nur mittelbare Nutzung von Verbindungsdaten erfordert es aber, dass diese noch vorliegen und daher ausgewertet werden können. Dies ist aber nicht selbstverständlich: Nach dem Ende einer Verbindung muss die IP-Adresse und die Zuordnung zu einem Kunden nur dann weiterhin gespeichert werden, wenn dies zur Störungsbeseitigung und zu Abrechnungszwecken erforderlich ist. Aus diesem Grunde wurde mit Wirkung zum 1.1.2008 eine sechsmonatige Mindestspeicherfrist angeordnet; diese Verbindungsdaten sollten also verdachtsunabhängig und anlasslos für sechs Monate auf Vorrat gespeichert werden (Vorratsdatenspeicherung von Verbindungsdaten; vgl. den für nichtig erklärten § 113a Abs. 4 TKG).

Diese Vorratsdatenspeicherung sah zusätzlich die Verpflichtung vor, auch noch weitere Daten vorzuhalten, die für die oben geschilderte Zuordnung von bekannten IP-Adressen zu einem konkreten Kunden völlig ohne Belang sind: So war auch zu speichern, wer wann wem eine E-Mail verschickt und wer wann von welcher IP-Adresse aus auf sein E-Mail-Postfach zugreift, und so waren entsprechende Daten auch für sämtliche Telefongespräche – einschließlich Internet-Telefonie – vorzuhalten (§ 113a Abs. 2 und 3 TKG, ebenfalls nichtig).

Vordergründiger Anlass für diese Speicherregelungen im TKG war eine 2006 beschlossene Richtlinie der Europäischen Union (AblEU 2006 L 105 vom 13.4.2006, S. 54), die auf höchst zweifelhafter – aber vom Europäischen Gerichtshof akzeptierter – Rechtsgrundlage erlassen wurde (EuGH NJW 2009, 1801 m. Anm. u. Bespr. Ambos, 2009; Braum, 2009; Petri, 2009; Simitis, 2009). Mehrere Mitgliedstaaten weigern sich bis heute, diese Richtlinie in nationales Recht umzusetzen; zudem ist in den nächsten Monaten mit einer umfassenden Änderung und Entschärfung dieser Richtlinie zu rechnen.

Das Bundesverfassungsgericht erklärte allerdings die Speicherverpflichtung und die Zugriffsbefugnisse in einem vielbeachteten Urteil vom 2.3.2010 für nichtig (BVerfGE 125, 260 m. Anm. u. Bespr. Hornung & Schnabel, 2010; Ohler, 2010; Schramm & Wegener, 2011), verbot aber eine sechsmonatige Mindestspeicherfrist nicht grundsätzlich. Zu einem neuen Versuch des Gesetzgebers, eine Vorratsdatenspeicherung nunmehr verfassungskonform einzuführen, kam es bislang nicht; allerdings wurden bereits verschiedene Entwürfe und Eckpunkte vorgestellt. Für die Praxis bedeutet dies, dass derzeit höchstens binnen weniger Tage – maximal sieben Tage – eine Zuordnung von IP-Adressen und Kunden vorgenommen werden kann: Telekommunikationsdienstleister halten die Daten längstens für diesen Zeitraum zur Störungsanalyse vor, manche Anbieter sogar für noch kürzere Zeiträume oder überhaupt nicht. Zwar scheint Deutschland gegen die europäische Rechtslage zu verstoßen, da es die Richtlinie nicht (mehr) umgesetzt hat. Diesem Verstoß kommt allerdings nur geringes Gewicht zuteil, da erstens die Grundrechtskonformität der Richtlinie noch nicht festgestellt ist und zweitens ohnehin eine Änderung der Richtlinie angekündigt ist. Wenn sich aber die europäischen Vorgaben ohnehin in Kürze ändern werden, so ist auch ein sofortiges Handeln des deutschen Gesetzgebers europarechtlich nicht erforderlich.

Bestandsdatenabfrage

Es fällt nicht schwer vorherzusagen, dass es schon bald zu einer Neuregelung einer Bestandsdatenabfrage kommen wird, also einer Abfrage, welchem Kunden eine bekannte IP-Adresse zu einem bestimmten Zeitpunkt zugeordnet war. Eine solche Zuordnung entspricht auch einem gewissen, gelegentlich aber auch überschätzten Bedürfnis bei der Verfolgung von Cyberkriminalität: So ist die Bestandsdatenabfrage oftmals nur ein Ermittlungsansatz neben anderen. Bei sämtlichen vermögensrelevanten Vorgängen – vom Verkauf von kinderpornographischen Schriften bis hin zum Phishing – kommt als Alternative etwa die Nachverfolgung von Finanztransaktionen in Betracht. Aufgrund dieser alternativen Ermittlungsansätze und der von einigen Telekommunikationsanbietern vorgenommenen Speicherung von Verbindungsdaten für sieben Tage konnte Internetkriminalität auch nach dem Urteil des Bundesverfassungsgerichts noch immer recht effektiv verfolgt werden.

Verfassungsrechtlich ist für eine solche Bestandsdatenabfrage lediglich zu beachten, dass eine »Auskunft nicht ins Blaue hinein eingeholt« werden kann und der Betroffene von

dieser Auskunftserteilung zu informieren ist (BVerfGE 125, 260, 343). Eine Speicherung der Zuordnung von IP-Adressen und Kunden wurde vom Bundesverfassungsgericht zwar für bis zu sechs Monate als verfassungskonform erachtet. Es ist aber nicht zwingend und auch nicht geboten, sämtliche verfassungsrechtlich zulässigen Eingriffe in die Freiheitsgrundrechte auch tatsächlich vorzunehmen. Von daher dürfte sich die rechtspolitische Diskussion diesbezüglich darauf konzentrieren, wie lange diese Daten auf Vorrat vorzuhalten sind. Auch diesbezüglich lässt sich leicht vorhersagen, dass sich die Maximalpositionen – 7 Tage bzw. 6 Monate – wohl nur schwer durchsetzen werden und ein Kompromiss innerhalb dieses Bereiches zu finden sein wird. Ob diese Vorratsdaten auch für den zivilrechtlichen Auskunftsanspruch nach § 101a UrhG geöffnet werden, erscheint angesichts politischer Forderungen nicht ausgeschlossen, im Lichte der Rechtsprechung des BVerfG aber bedenklich (vgl. BVerfGE 125, 260, 271).

Bei alledem ist auch zu berücksichtigen, dass das praktische Bedürfnis nach einer solchen Bestandsdatenabfrage in Zukunft sinken könnte: Das schon bald größere Verwendung findende Internetprotokoll IPv6 ist zumindest bislang von den Telekommunikationsanbietern, Hardware- und Softwareherstellern teilweise in einer Art und Weise implementiert, die eine eindeutige und konstante Zuordnung eines Gerätes zu einer IP-Adresse ermöglichen. Die Gefahren, die mit einer solchen Deanonymisierung einhergehen werden – und damit seien vor allem Gefahren von privater Seite angesprochen – können nur schwer abgeschätzt werden.

Vorratsdatenabfrage

Weitaus schwieriger zu beurteilen ist die Frage, ob Verbindungsdaten auch zu einer umfassenden Auswertung der Kommunikationsstrukturen vorzuhalten sind – der eigentliche Kernbereich der Vorratsdatenabfrage. Dabei handelt es sich nicht um ein spezifisches Problem der Verfolgung von Cyberkriminalität, sondern – über die Erfassung sämtlicher Telefongespräche – auch aller sonstigen Kriminalitätsformen.

Eine solche Vorratsdatenspeicherung und Vorratsdatenabfrage ist mit einem weitaus höheren Grundrechtseingriff verbunden und unterliegt daher weitaus strengeren verfassungsrechtlichen Anforderungen (s. BVerfGE 125, 260, 325 ff.) Diesbezüglich spricht daher viel für eine weitaus größere Zurückhaltung, als sie § 113a Abs. 1 bis Abs. 3 TKG wahrte. Als Alternative wird diesbezüglich ein »Quick Freeze« diskutiert:

Jedenfalls kurzfristig halten einige Telekommunikationsdienstleister manche dieser Verbindungsdaten ohnehin zur Störungsanalyse und ggf. zu Abrechnungszwecken vor. Diese könnten auf ersten Zuruf der Polizei oder der Staatsanwaltschaft vorläufig gesichert werden; ein Zugriff würde sodann dem Richtervorbehalt des § 100g StPO unterliegen.

Wie auch bei der Bestandsdatenabfrage erscheint es unwahrscheinlich, dass sich eine solche Maximalforderung, die nur an ohnehin bei Telekommunikationsdienstleistern vorhandene Daten anknüpft, auch europäisch durchsetzen lässt. Eine Speicherverpflichtung

könnte aber bei einem »Quick Freeze«-Verfahren deutlich kürzer als 6 Monate ausfallen und daher etwa in gleicher Größenordnung vorgesehen werden wie bei dem Vorschlag für eine Bestandsdatenabfrage (7 Tage). Schließlich sei angeregt, die unterschiedlichen Verbindungsdaten auch unterschiedlich zu handhaben, und etwa auf manche Datentypen betreffend der elektronischen Post zu verzichten.

Rasterfahndung oder die täterbezogene Verknüpfung von Datenbeständen

Die Verknüpfung verschiedener Ermittlungsergebnisse ist das tägliche Brot der Ermittlungsbehörden. Soweit hierzu *tatbezogene* Merkmale herangezogen werden – etwa: wer fährt ein Kraftfahrzeug eines bestimmten am Tatort beobachteten Typs? – ist dies auch datenschutzrechtlich weitaus weniger kritisch zu beäugen als eine Analyse oder ein *data mining täterbezogener* Merkmale – etwa: wer hat ein Maschinenbaustudium begonnen und wer ist in seinem Leben bereits nach Afghanistan gereist –, wie sie bei einer Rasterfahndung (§ 98a StPO) vorgenommen wird: Dabei sind falsch-positive Resultate häufig anzutreffen und es wird gerade die Erstellung eines umfassenden Persönlichkeitsprofils bezweckt (s. hierzu Brodowski, 2010a, S. 548). Allerdings kann – entgegen dem Bundesverfassungsgericht (BVerfG JR 2010, 543) – nicht entscheidend sein, dass bei einer Rasterfahndung Daten mehrerer Speicherstellen zusammengeführt werden müssen. Vielmehr kommt es auf das konkrete Gefahrenpotential einer Datenabfrage und darauf an, ob ein solches ermittlungsrelevantes Persönlichkeitsprofil erstellt werden soll oder ob lediglich eine tatbezogene Abfrage von Daten erfolgt: So liegen bereits bei einem einzelnen Internet-Großunternehmen unter Umständen derart umfangreiche und diverse Datenbestände über eine Person, so dass sich aus diesen Daten einer Speicherstelle ein umfangreiches Persönlichkeitsprofil erstellen ließe (Brodowski, 2010a, S. 548).

Eine Rasterfahndung darf sodann nur nach Wahrung eines präventiven Richtervorbehalts – eine Notkompetenz verbleibt bei der Staatsanwaltschaft – und bei bestimmten, in § 98 Abs. 1 StPO näher umrissenen Straftaten von erheblicher Bedeutung angeordnet werden.

7.5.4. Online-Durchsuchung und Online-Streife

Mit einer »Online-Durchsuchung« eines informationstechnischen Systems (vgl. hierzu BVerfGE 120, 274 m. Anm. u. Bespr. Böckenförde, 2008; Hornick, 2008; Hornung, 2008; Kutscha, 2008; Michalke, 2008; Roßnagel & Schnabel, 2008; Sachs & Krings, 2008; s. ferner Bär, 2007b; Beukelmann, 2008; Beulke & Meininghaus, 2007; Buermeyer, 2007b; Buermeyer, 2007a; M. Gercke, 2007b; Hansen & Pfitzmann, 2007; Hornung, 2007; Jahn & Kudlich, 2007; Kutscha, 2007; Rux, 2007; Valerius, 2007a Warntjen, 2007; Weichert, 2007) bezeichnet man im Gegensatz zu einer herkömmlichen Durchsuchung (s. hierzu oben 7.5.1., S. 130) ein verdecktes Vorgehen, bei dem Strafverfolgungsbehörden über eine *Remote Forensic Sofware*, also eine Spionagesoftware vollen Administrationszugang informationstechnisches System erlangen. Dieser kann erstens genutzt werden zu einer

Ausleitung von Telekommunikationsinhaltsdaten im Rahmen der so genannten Quellen-Telekommunikationsüberwachung (s. oben 7.5.2., S. 143). Zweitens aber ist es auch möglich, auf diesem Wege die in einem informationstechnischen System gespeicherten Daten einmalig abzugreifen (Online-Durchsicht) oder laufend zu überwachen (Online-Überwachung).

Die mit einem solchen Eingriff verbundenen Risiken und Gefahren sind mannigfaltig und reichen von der Beeinträchtigung der Vertraulichkeit und Integrität informationstechnischer Systemen, hiermit verbundenen Angriffsmöglichkeiten für Dritte – etwa auch für Wirtschaftsspionage – bis hin zur Unverletzlichkeit der Wohnung, wenn auch das Bundesverfassungsgericht letzterem Aspekt keine Bedeutung zukommen lässt (s. bereits die kritische Stellungnahme oben 4.5.2., S. 48).

Die präventive Online-Durchsuchung zur Gefahrenabwehr

Im Zuge einer Grundsatzentscheidung über das nordrhein-westfälischen Verfassungsschutzgesetzes entwickelte das Bundesverfassungsgericht in BVerfGE 120, 274 eine Blaupause für eine präventivpolizeiliche Regelung für eine Online-Durchsuchung informationstechnischer Systeme, insbesondere zur Verfolgung des internationalen Terrorismus. An dieser Blaupause und an deren Umsetzung im BKAG, aber auch im bayerischen und nun auch im rheinland-pfälzischen Polizeirecht gibt es viel zu kritisieren, etwa die zum Teil weichen Abwägungskriterien unter Verzicht auf die harten Vorgaben, wie sie etwa Art. 13 GG vorgeben würde. Aus der in dieser Studie vertieft zu behandelnden strafrechtlichen Verfolgung von Cyberkriminalität sei diesbezüglich allein auf die spätere Datenverwendung für Strafverfolgungszwecke hingewiesen:

§ 20v Abs. 5 BKAG gestattet polizei- und datenschutzrechtlich eine Übermittlung von Erkenntnissen, wenn sie erstens zur Verfolgung von Straftaten erforderlich ist. Zweitens darf dies nur Straftaten betreffen, die im Höchstmaß mit mindestens fünf Jahren Freiheitsstrafe bedroht sind. Dies ist aber bei Lichte besehen keine ernsthafte Einschränkung, denn im Terrorismusbereich bestehen ohnehin höhere Strafdrohungen, und selbst die einfache Körperverletzung, der einfache Diebstahl oder die einfache Urkundenfälschung ist im Höchstmaß mit einer Freiheitsstrafe von fünf Jahren bedroht. Drittens aber muss ein Auskunftsverlangen von Strafverfolgungsbehörden möglich sein, was mit der strafprozessualen Zulässigkeit der Datenverwendung zusammenhängt: § 161 Abs. 2 StPO verbietet aber stets eine unmittelbare Verwertung dieser Erkenntnisse, da eine vergleichbare strafprozessuale Befugnis auf Katalogtaten einzuschränken wäre, eine solche strafprozessuale Eingriffsbefugnis aber nicht besteht (Meyer-Goßner, 2010, § 161 Rdn. 18e m.w.N.).

Eine repressive Online-Durchsuchung zu Strafverfolgungszwecken?

Die Forderungen nach einer strafprozessrechtlichen Eingriffsgrundlage für eine verdeckte Online-Durchsicht oder Online-Überwachung informationstechnischer Systeme sind in

letzter Zeit etwas verstummt. Solche Maßnahmen erscheinen angesichts bestehender Alternativen auch nicht erforderlich zur Verfolgung der Cyberkriminalität: So ist etwa ein offener Zugriff auf ein laufendes oder auf ein soeben erst ausgeschaltetes informationstechnisches System möglich, oder auch eine akustische Wohnraumüberwachung oder eine Telekommunikationsüberwachung. Auch wäre der Beweiswert im Wege der Online-Durchsuchung erlangter Beweismittel deutlich reduziert (vgl. BVerfGE 120, 274, 320 f.; s. auch Hansen & Pfitzmann, 2007, S. 228).

Trotz der derzeit ruhenden rechtspolitischen Diskussion und trotz der fehlenden praktischen Notwendigkeit seien manche Eckpunkte genannt, an denen sich eine repressive Online-Durchsuchung zu Strafverfolgungszwecken im Lichte der verfassungsrechtlichen Vorgaben zu orientieren hätte. Erstens müsste sich die Regelung angesichts der Eingriffstiefe am Maßstab der akustischen Wohnraumüberwachung orientieren (§§ 100c, 100d StPO), sowohl was die materiellen Anordnungsvoraussetzungen, als auch was die prozeduralen Sicherungen betrifft. Zweitens aber wären aus dem Deliktskatalog diejenigen Delikte zu streichen, die nicht dem Schutz von Leib, Leben und Freiheit von Menschen dienen, also etwa manche der in § 100c Abs. 2 Nr. 1 lit. c, lit. h, lit. k, Nr. 2 bis Nr. 4 StPO genannten Delikte.

Online-Streife

So wie die Strafverfolgungsbehörden (in der realen Welt) von öffentliche Wegen aus Ausschau halten dürfen nach kriminellem Verhalten, so dürfen sie auch (in der virtuellen Welt) auf allgemein-verfügliche Websites, allgemein-verfügliche soziale Netzwerke usw. zugreifen (so auch BVerfGE 120, 274, 344 ff.; vgl. grundlegend Valerius, 2004). Dies erschließt sich von selbst, da es insoweit an schutzwürdigen entgegenstehenden Interessen fehlt und jedenfalls die Eingriffstiefe ausgesprochen niedrig ist. Zwei Grenzen sind dennoch zu diskutieren: Die Nutzung einer Legende (Identitätstäuschung) und die weitere Verwendung der durch eine »Online-Streife« ermittelten Erkenntnisse.

Nach der Rechtsprechung des Bundesverfassungsgerichts müssen sich Strafverfolger im Internet nicht als solche zu erkennen geben. Im Internet stünden nämlich keine Mechanismen zur Identitätsprüfung bereit. Daher sei das Vertrauen, nicht mit einer staatlichen Stelle zu kommunizieren, nicht schutzwürdig (BVerfGE 120, 274, 345). Hieraus resultiert aber auch: Soweit Identitätsprüfungsmechanismen bestehen – etwa durch den neuen Personalausweis –, so dürfen staatliche Stellen auch nicht ohne spezielle Ermächtigungsgrundlage diese Mechanismen umgehen. Ist die Anmeldung zu einem sozialen Netzwerk daher hypothetischerweise an eine wirksame Identitätsprüfung gebunden, so sind auch Ermittler grundsätzlich verpflichtet, ihre wahre Identität preiszugeben. Nur verdeckte Ermittler dürfen unter den Voraussetzungen der §§ 110a ff. auch täuschende Urkunden verwenden.

Zweitens besteht eine Gefahrenlage, wenn durch legitime und legale »Online-Streifen«

Erkenntnisse über Personen »gezielt zusammengetragen, gespeichert und gegebenenfalls unter Hinzuziehung weiterer Daten ausgewertet werden.« Hierfür wäre eine besondere Eingriffsgrundlage erforderlich, wie auch sonst eine gesetzliche Grundlage für Datenbanken und Datensammlungen zu Strafverfolgungszwecken erforderlich ist. Eine praktische Notwendigkeit dafür hat sich aber bislang nicht ergeben; die »Online-Streife« als Mittel zur Aufdeckung von konkreten Straftaten ist im bestehenden Rechtsrahmen effektiv genug. Lediglich diskutabel wäre eine Erweiterung des § 184b Abs. 4 StGB dahingehend, dass in einschlägigen Szenen operierende Ermittlungsbeamte auch *schein*kinderpornographische Schriften im Einzelfall verbreiten dürfen, wenn ihnen nur so der Zugang zu einschlägigen Netzwerken ermöglicht wird und daher nur auf diesem Wege eine effektive Strafverfolgung möglich ist.

7.5.5. Fazit

Das bestehende Instrumentarium zur Verfolgung von Cyberkriminalität ist weitgehend ausreichend und auch angemessen. Dies wird durch die polizeiliche Kriminalstatistik nur unterstrichen, derzufolge die Straftatenbegehung im Internet sogar überdurchschnittlich gut aufgeklärt werden kann – in 75,7% der Fälle im Vergleich zu einer Gesamtaufklärungsquote von 55,6% (Zahlen für 2009, vgl. Bundeskriminalamt, 2010, S. 70, S. 243).

Aus praktischer, verfassungs- und europarechtlicher Sicht geboten ist es allerdings, drei Eingriffsgrundlagen besser handhabbar zu gestalten: Erstens der Zugriff auf bei E-Mail-Provider lagernde Nachrichten – insoweit bietet sich eine Vereinheitlichung auf Basis der Postbeschlagnahme, §§ 99 f. StPO, an (s. oben 7.5.2., S. 142) –, zweitens eine juristisch tragfähige Grundlage für eine Quellen-Telekommunikationsüberwachung – wobei der Deliktskatalog im Vergleich zu § 100a Abs. 2 StPO einzuschränken ist und wirksame technische und rechtliche Schranken vorzusehen sind (s. oben 7.5.2., S. 144) – und drittens eine Neuregelung der Abfrage von Bestandsdaten anhand einer bekannten IP-Adresse. Bei alledem ist darauf zu achten, dass ein hinreichender materieller und verfahrensrechtlicher Schutz gewahrt bleibt und sich dieser nicht in einer bloßen Einzelfallabwägung erschöpft. Diese zeigte sich nämlich in der Vergangenheit als weniger treffsicher als eine durch den Gesetzgeber vorgenommene Typisierung des Schutzes, wie sie etwa die Deliktskataloge der §§ 100a Abs. 2, 100c Abs. 2 StPO vorsehen.

Schließlich aber – und dies erscheint uns der wichtigste Punkt zur effektiven Verfolgung der Cyberkriminalität – ist auf eine ausreichende Ausbildung der Strafverfolger und auf eine ausreichende personelle Stärke entsprechend ausgebildeter Strafverfolger hinzuwirken. Mit diesen Faktoren steht und fällt eine effektive Strafverfolgung: Mit der Schnelligkeit der Informationstechnologie kann nur Schritt halten, wer schnell auf Vorkommnisse reagieren kann und nicht erst nach Monaten auf einen Verdacht reagieren kann; mit den technischen Herausforderungen der Cyberkriminalität kann nur Schritt halten, wer sich vertieft mit den technischen Gegebenheiten, aber auch technischen Mög-

lichkeiten der digitalen Forensik beschäftigt hat. Solche Zusatzqualifikationen gilt es auch im Polizeidienst – etwa durch spezielle Laufbahngestaltungen – entsprechend zu würdigen.

7.6. Zusammenfassung

In diesem Kapitel haben wir uns mit dem Schutz »im Kleinen« befasst, also der Frage, was man selbst (als Privatperson oder Unternehmen) tun kann, um sich vor Cyberkriminalität zu schützen. Dabei sind wir zunächst auf konkrete technische und organisatorische Schutzmechanismen eingegangen. Anschließend haben wir betrachtet, welche Tatbestandsmerkmale des deutschen Strafrechts im Bereich Cyberkriminalität zur Anwendung kommen können. Wir sahen, dass das deutsche Strafrecht besser zur Verfolgung von Cyberkriminalität geeignet ist als gemeinhin vermutet: Nahezu sämtliche Verhaltensweisen der Cyberkriminalität, die einer strafrechtlichen Sanktion erfordern, werden bereits durch mindestens einen Straftatbestand erfasst. Eine weitere Vorverlagerung oder Expansion des materiellen Strafrechts ist daher grundsätzlich nicht erforderlich. Auch das strafprozessuale Instrumentarium ist – insbesondere bei Berücksichtigung der forensischen Möglichkeiten – ebenfalls als weitgehend ausreichend zu erachten. Eine gewisse Bedeutung kommt allerdings der derzeit nicht ausreichend geregelten Abfrage nach der Zuordnung einer IP-Adresse zu einem Kunden (Bestandsdatenabfrage) zu, doch auch die Bedeutung dieser Ermittlungsmethode wird teilweise überschätzt.

Nur in Randbereichen zeigte sich – bisweilen sogar erheblicher – Korrekturbedarf: Sei es zur Verfolgung der Finanzierung der Kinderpornographie, zur zielgerichteten Verfolgung des *Phishing* und des *Skimming* und zum Schutz von Daten, die einem Diensteanbieter anvertraut wurden. Der derzeit diskutierte Schutz der Presse sollte auch auf §§ 17, 19 UWG erstreckt werden; zudem ist durch eine Straffreistellungsklausel (*safe harbour*) bei den Vorbereitungsdelikten der §§ 202c StGB, 108b UrhG, 4 ZKDSG klarzustellen, dass Handlungen, die der Wissenschaft, der Forschung oder der Lehre oder der Erfüllung rechtmäßiger beruflicher oder dienstlicher Pflichten dienen, kein strafbares Unrecht darstellen. Aus strafprozessrechtlicher Sicht ist eine Vereinheitlichung der Rechtsgrundlage zum Zugriff auf E-Mails anzustreben sowie eine juristisch tragfähige Grundlage für eine Quellen-Telekommunikationsüberwachung und für eine Bestandsdatenabfrage in Erwägung zu ziehen.

Erheblicher Handlungsbedarf ist daher weniger in *rechtlicher* denn in *faktischer* Sicht geboten: Erstens ist der technische Schutz informationstechnischer Systeme zu verbessern, um so weniger Angriffsfläche für Cyberkriminalität zu bieten. Zweitens aber sind die Strafverfolgungsbehörden personell besser aufzustellen zur Verfolgung von Cyberkriminalität. Dies erfordert eine bessere Ausbildung in der Breite, aber auch ausreichende Anreize für Spezialisten auf dem Gebiet der digitalen Forensik, für die Strafverfolgungsbehörden tätig zu werden.

8. Schutz »im Großen«: Strafverfolgung und Transnationalität

8.1. Einleitung

In diesem Kapitel möchten wir uns schließlich der Frage zuwenden, was man jenseits des Selbstschutzes und der nationalen Strafverfolgung gegen Cyberkriminalität tun kann. Dies betrifft aufgrund der inhärenten Transnationalität vor allem Fragen nach der internationalen Zusammenarbeit.

Wir gehen zunächst auf wissenschaftliche und organisatorische Kooperationen ein, die jenseits einer formal-juristischen Zusammenarbeit liegen (8.2.). Hier gibt es vor allem im Bereich der Internet-Beschwerdestellen und bei der Bekämpfung von Botnetzen zahlreiche positive Beispiele.

Unabhängig von der Art der Kooperation ist manchmal problematisch, dass unterschiedliche Delikte in unterschiedlichen Ländern anders oder überhaupt nicht geahndet werden. Dem entgegenzuwirken dienen Harmonisierungsbestrebungen des Strafrechts (8.3.). Sodann thematisieren wir eine oft geäußerte Option für die Strafverfolgungsbehörden, nämlich die extraterritoriale Strafverfolgung (8.4.). Abschließend gehen wir auf die klassischen und modernen Möglichkeiten der justiziellen Zusammenarbeit in Strafsachen ein, insbesondere innerhalb der Europäischen Union (8.5.).

8.2. Informelle internationale Kooperation

Abseits der formalen internationalen Kooperation von Strafverfolgungsbehörden gibt es in vielen Bereichen bereits etablierte Kooperationen von Universitäten, Verbänden oder der Privatwirtschaft, die bei der internationalen Verfolgung von Cyberkriminalität helfen. Hier seien nun exemplarisch ein paar erfolgversprechende Kooperationen vorgestellt.

8.2.1. CERTs

CERTs (siehe 7.2.5., S. 84) bilden nicht nur im Rahmen des nationalen CERT-Verbundes (DFN-CERT Services GmbH, o. J.) sondern auch international eine hervorragende Plattform für informelle Kooperation. Das internationale Pendant zum nationalen CERT-Verbund ist das *Forum of Incident Response Teams* (FIRST). Die Effektivität der Kooperation ist jedoch immer auch abhängig von gegenseitigem Vertrauen, so dass sich kulturell, geografisch oder politisch homogenere Gruppen für eine intensive Zusammenarbeit in der Praxis eher eignen, wie beispielsweise die Gruppe der *European Government CERTs*.

8.2.2. Beschwerdestellen für illegale Inhalte

Seit mehreren Jahren betreiben der Verband der Internetwirtschaft und die Freiwillige Selbstkontrolle Multimedia-Diensteanbieter eine gemeinsame Internet-Beschwerdestelle für illegale Inhalte (eco – Verband der deutschen Internetwirtschaft e.V. & Freiwillige Selbstkontrolle Multimedia-Diensteanbieter, o. J.). Da nationale Beschwerdestellen in der Regel nur national aktiv werden können, hat sich 1999 mit dem Verband INHOPE (INHOPE, o. J.) ein globaler Dachverband gebildet, in dem mittlerweile mehr als 30 Staaten zusammenarbeiten. Die informelle Zusammenarbeit, etwa bei der Entfernung kinderpornographischer Schriften aus dem Netz, erscheint weitaus effektiver und schneller zu sein als zwischenstaatliche Bemühungen auf diesem Gebiet.

8.2.3. Bekämpfung von Botnetzen

Botnetze sind die mit Abstand am weitesten entwickelten technischen Artefakte der Cyberkriminalität. Insofern haben Botnetze von Anfang an das Interesse von Wissenschaftlern geweckt. Die heute auch bei Strafverfolgungsbehörden gängige Technik des *Botnet Tracking*, also der Infiltration eines Botnetzes mittels Honeypots, entstammt ursprünglich akademischen Arbeiten (Freiling et al., 2005).

Heute gibt es weltweit etwa ein Dutzend universitäre Arbeitsgruppen, die aktiv Forschung im Bereich Botnetze betreiben. Von Interesse sind dabei Fragen der Struktur, der Größe und der Arbeitsweise derartiger Netze. Es gibt in der Literatur viele Beispiele auch für erfolgreiche internationale Kooperationen. So brachten Forscher aus den USA im Jahr 2009 das Torpig-Botnetz mit geschätzt mehr als einer Million Bots für mehrere Wochen unter ihre Kontrolle (Stone-Gross et al., 2009). Weitere Beispiele sind die erfolgreichen Analysen des Storm- (Holz, Steiner et al., 2008) und des Waledac-Botnetzes (Stock, Göbel, Engelberth, Freiling & Holz, 2009). Diese Analysetechniken wurden im Frühjahr 2010 verwendet, um in einer internationalen Kooperation, die durch Microsoft angeführt wurde, das Waledac-Botnetz abzuschalten.

8.3. Harmonisierung des materiellen Strafrechts

Ein erster Ansatz, um international die Strafverfolgung von Cyberkriminalität zu verbessern, liegt darin, die Straftatbestände zu vereinheitlichen. Dies geschieht regelungstechnisch dadurch, dass sich Staaten wechselseitig verpflichten, bestimmte Verhaltensweisen unter Strafe zu stellen. Solche Pönalisierungsverpflichtungen richten sich demnach nur an die Staaten und enthalten daher keine Strafnormen als solche, sondern nur Arbeitsanweisungen an die jeweilige Legislative.

Eine solche Harmonisierung von Strafbestimmungen dient verschiedenen Zwecken: Erstens werden Rückzugsräume für Kriminelle geschlossen. Es wird zweitens gewährleistet,

dass bestimmte Verhaltensweisen in zwei oder mehr Staaten strafbar sind, und demnach Rechtshilfe zulässig ist, welche zumeist eine beiderseitige Strafbarkeit voraussetzt (M. Gercke, 2010b, S. 75). Drittens erleichtern solche internationale Vorgaben auch die Beurteilung, wie auf neuartige Bedrohungsszenarien zu reagieren ist (M. Gercke, 2009b, S. 410).

8.3.1. Übereinkommen gegen Computerkriminalität

Paradigmatisch für solche Harmonisierungen im Bereich der Verfolgung von Cyberkriminalität ist das Kapitel II, Abschnitt 1 des wegweisenden Budapester Übereinkommens über Computerkriminalität (*Cybercrime Convention*). Dieses Übereinkommen wurde als völkerrechtlicher Vertrag im Rahmen des Europarats entworfen und steht nach Maßgabe dessen Art. 37 weltweit zur Zeichnung offen; so ratifizierten es nicht nur etliche Mitgliedstaaten der Europäischen Union, sondern auch die USA.

Das Übereinkommen enthält umfangreiche Bestimmungen, denen zufolge der rechtswidrige Zugang (Art. 2), das rechtswidrige Abfangen von Daten (Art. 3), der Eingriff in Daten (Art. 4) und in ein informationstechnisches System (Art. 5) und der Missbrauch von Vorrichtungen (Art. 6) unter Strafe zu stellen sind. Ferner werden Pönalisierungsverpflichtungen bezüglich computerbezogenen Fälschungen (Art. 7) und Computerbetrug (Art. 8) sowie bezüglich kinderpornographischer Schriften (Art. 9) und im Zusammenhang mit Verletzungen des Urheberrechts und verwandter Schutzrechte (Art. 10) angeordnet.

Aufgrund von Meinungsverschiedenheiten über den Ausgleich zwischen Meinungsfreiheit und rassistischer und fremdenfeindlicher Propaganda wurden Bestimmungen »betreffend die Kriminalisierung mittels Computersystemen begangener Handlungen rassistischer und fremdenfeindlicher Art« in ein Zusatzprotokoll zum Übereinkommen ausgelagert (Art. 3 bis Art. 7 ZP).

Allerdings: Diese Übereinkommen sind völkerrechtlicher Natur und leiden daher an einem gewissen Effektivitäts- und Vollzugsdefizit. Im Ausgangspunkt steht es den Staaten frei, ob und inwieweit sie sich überhaupt einer solchen völkerrechtlichen Verpflichtung unterwerfen. Auch die Umsetzung des Übereinkommens in nationales Recht lässt sich nicht durchsetzen. Durch diplomatischen und politischen Druck entstehen allerdings faktische Zwänge, welche Staaten zur Ratifikation und auch zur Umsetzung solcher Übereinkommen drängen. Zudem ist es bei innerstaatlich unliebsamen politischen Maßnahmen durchaus dienlich, eine externe Vorgabe präsentieren zu können, die nunmehr eine innerstaatliche Reaktion alternativlos mache (so genanntes *policy laundering*).

In Deutschland war der Umsetzungsbedarf des Übereinkommens überschaubar, aber dennoch höchst umstritten: Durch das 41. Strafrechtsänderungsgesetz, das sich explizit auf die Umsetzung des Übereinkommens über Computerkriminalität bezog, wurden u.a. die Vorbereitungsstraftaten bezüglich der so genannten *hacking tools* eingeführt

(§ 202c StGB). In weiten Teilen entsprach aber die deutsche Rechtslage ohnehin den Vorgaben dieses Übereinkommens, da bereits zuvor die Notwendigkeit einer entsprechenden strafrechtlichen Absicherung informationstechnischer Systeme erkannt worden war. Die Ratifikation des Übereinkommens erfolgte im Anschluss an diese Umsetzung in Deutschland am 9.3.2009. Das Zusatzabkommen hingegen wird erst durch ein bereits verabschiedetes, aber noch nicht verkündetes Gesetz (Gesetzentwurf in BT-Drs. 17/3124) umgesetzt; gleiches gilt für das Ratifikationsgesetz (Gesetzentwurf in BT-Drs. 17/3123).

8.3.2. Maßnahmen der Europäischen Union

Auch die Europäisierung des Strafrechts in der Europäischen Union setzte über weite Jahre einen Schwerpunkt auf die Harmonisierung des materiellen Strafrechts, insbesondere auch des Computerstrafrechts (Schwarzenegger & Summers, in Druck). Dabei ist erstens zu bedenken, dass es der Europäischen Union bis heute an einer Rechtsgrundlage fehlt, eigene Straftatbestände im Bereich der Cyberkriminalität zu schaffen, sie sich bei der Regelung materiellen Strafrechts also auf dessen Harmonisierung beschränken muss. Zweitens aber ist zu beachten, dass sich durch das Inkrafttreten des Vertrags von Lissabon am 1.12.2009 Grundlegendes verändert hat: Waren bis dahin die Rechtsakte zur Harmonisierung dem Einstimmigkeitsprinzip unterworfen, so genügt nunmehr eine qualifizierte Mehrheit, um neue Pönalisierungsverpflichtungen zu erlassen. Waren bis dahin nur die Vertreter der Regierungen an Gesetzgebungsprozessen in diesem Bereich beteiligt, so ist nunmehr das Europäische Parlament gleichberechtigter Partner. Schließlich erstarkte auch die Charta der Grundrechte der Europäischen Union zu gleichwertigem Primärrecht.

Die Europäische Union erließ eine Fülle von Harmonisierungsbestimmungen, die sich auch auf die Deliktsbegehung durch informationstechnische Systeme beziehen können. Aus diesem weiten Fundus sei hier nur am Rande verwiesen auf den Rahmenbeschluss des Rates vom 28. Mai 2001 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln (AblEG 2001 L 149 v. 1.6.2001, S. 1; s. hierzu M. Gercke, 2010b, S. 77). Besonderes Augenmerk sei hingegen gerichtet auf die Rechtsakte über Angriffe auf Informationssysteme und betreffend der Verfolgung der sexuellen Ausbeutung von Kindern und der Kinderpornographie.

Rahmenbeschluss des Rates über Angriffe auf Informationssysteme

Der Rahmenbeschluss 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme (AblEU 2005 L 69 v. 15.3.2005, S. 67; s. hierzu Bier, 2005, S. 475; Brodowski, 2010b, S. 151 f.; M. Gercke, 2005) liest sich mehr oder weniger wie eine Kopie der Pönalisierungsverpflichtungen in den ersten Artikeln des Übereinkommens über Computerkriminalität. Insofern überrascht es nicht, dass innerstaatlich dieser Rahmenbeschluss zugleich mit dem Übereinkommen umgesetzt wurde. Wie das Übereinkommen auch leidet der Rahmenbeschluss an seiner mangelnden Durchsetzbarkeit: Vertragsverletzungsverfahren kann die Kommission bezogen auf solche Rahmenbeschlüsse erst ab

Dezember 2014 einleiten (Brodowski, 2010d, S. 377). Daher verwundert es auch nicht, dass die Umsetzung dieses Rahmenbeschlusses durch die Kommission in vielen Mitgliedstaaten als unzureichend erachtet wurde (KOM [2008] 448 endgültig). Die Umsetzung in Deutschland (vgl. Gröseling & Höfinger, 2007, Popp, 2007; Schumann, 2007) wurde im Wesentlichen nur bezüglich der Einschränkung des § 303b StGB (Computersabotage) auf informationstechnische Systeme, »die für einen anderen von wesentlicher Bedeutung« sind, kritisiert (KOM [2008] 448 endgültig, S. 5 f.). Allerdings können Angriffe gegen nicht wesentliche Datenverarbeitungsanlagen durchaus als »leichte Fälle« angesehen werden: Diese sind explizit von der Verpflichtung ausgenommen, unter Strafe gestellt zu werden.

Vorschlag für eine Richtlinie über Angriffe auf Informationssysteme

In den Organen der Europäischen Union wird derzeit ein Vorschlag diskutiert für eine Richtlinie des Europäischen Parlaments und des Rates über Angriffe auf Informationssysteme und zur Aufhebung des Rahmenbeschlusses 2005/222/JI des Rates (KOM [2010] 517 endgültig; s. hierzu Brodowski, 2010c, S. 753 f.). Mit diesem bezweckt die Kommission, Mindeststandards der strafrechtlichen Verfolgung betreffend Botnetzen und anderer moderner Formen von Cyberkriminalität einzuführen. In der Sache aber beschränken sich die Änderungen im Vergleich zum Rahmenbeschluss im Wesentlichen auf eine größere Differenzierung und Verschärfung der Strafrahmen. Diesbezüglich ist aber darauf hinzuweisen, dass die Wirksamkeit von unterschiedlichen Strafdrohungen in Zweifel zu ziehen ist (s. oben 4.2.2., S. 38). Entscheidender dürfte sein, dass die Umsetzung einer Richtlinie weitaus strenger und früher von den Organen der Europäischen Union überwacht werden kann.

Die bereits an anderer Stelle (Brodowski, 2010c, S. 753 f.) herausgearbeiteten materiellrechtlichen Veränderungen und der Umsetzungsbedarf in Deutschland sei hier kurz rezitiert: Erstens soll die Richtlinie auch Vorgaben enthalten betreffend dem Abfangen von Daten (Art. 6) und der Herstellung, dem Besitz und der Verbreitung von so genannten *Hacking Tools* (Art. 7); beides ist in Deutschland aufgrund der Vorgaben des Übereinkommens über Computerkriminalität bereits adäquat strafrechtlich erfasst. Zweitens sieht der Entwurf in zu kritisierender Weise nicht mehr vor, dass ein rechtswidriger Zugang zu einem Informationssystem nur bei einer »Verletzung von Sicherheitsmaßnahmen« gegeben ist (so aber noch Art. 2 Abs. 2 des Rahmenbeschlusses). Auch wenn eine entsprechende legislative Klarstellung wünschenswert wäre, so lässt sich ein Ausspähen von Daten ohne jegliche Überwindung einer Zugangssicherung durchaus als ein »leichter Fall« angesehen werden, der nach wie vor von der Pönalisierungsverpflichtung ausgenommen ist. Umsetzungsbedarf bestünde allein betreffend der Strafrahmen; da entsprechende kriminelle Vereinigungen bereits über § 129 StGB adäquat erfasst werden reduziert sich der – rechtspolitisch zweifelhafte – Änderungsbedarf daher nach aktuellem Stand auf:

§ 202d Besonders schweres Abfangen oder Ausspähen von Daten

In besonders schweren Fällen der §§ 202a Absatz 1 und 202b ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

1. ein technisches Mittel einsetzt, das dazu bestimmt ist, eine große Anzahl von informationstechnischen Systemen zu schädigen oder einen Vermögensverlust großen Ausmaßes herbeizuführen, oder
2. durch Täuschung über eine Tatsache einen Irrtum über seine Identität erregt, um den wahren Identitätsinhaber zu schädigen.

§ 303b Computersabotage

(3a) § 202d findet entsprechende Anwendung.

EU-Rechtsakte über die sexuelle Ausbeutung von Kindern und Kinderpornographie

Der Rahmenbeschluss 2004/68/JI vom 22. Dezember 2003 des Rates zur Bekämpfung der sexuellen Ausbeutung von Kindern und der Kinderpornografie (AblEU 2004 L 13 v. 19.1.2004, S. 44; krit. Böse, 2006) enthält eine Pönalisierungsvorgabe u.a. bezüglich der Verbreitung, des Anbietens, des Erwerbs und des Besitzes von kinderpornographischen Schriften, »unabhängig davon, ob sie unter Verwendung eines EDV-Systems begangen wurden« (Art. 3 Abs. 1), wobei der Rahmenbeschluss als Kind jede Person unter 18 Jahren definierte (Art. 1 lit. a). Dies führte dazu, dass in Deutschland auch die Verbreitung, der Erwerb und der Besitz jugendpornographischer Schriften in § 184c StGB unter Strafe gestellt werden musste (Umsetzungsgesetz in BGBl 2008 I, S. 2149).

Die Organe der Europäischen Union diskutieren derzeit eine Aufhebung dieses Rahmenbeschlusses und seine Ersetzung durch eine entsprechende Richtlinie (s. KOM [2010] 94 endgültig; vertiefend Brodowski, 2010d, S. 381; Brodowski, 2010c, S. 752). Neben der ordnungsrechtlichen Diskussion über Netzsperren (Art. 21) und strafprozessrechtlicher Vorgaben (s. hierzu unten 8.5.3., S. 177) enthält dieser Vorschlag auch neue Pönalisierungsverpflichtungen:

So soll erstens das bewusste Aufrufen von Kinderpornographie zwingend unter Strafe zu stellen sein (Art. 5 Abs. 3), wobei als Indizien hierfür die Zahlung für kinderpornographische Schriften oder der wiederholte Aufruf heranzuziehen seien. Rechtspolitisch ist dieser Vorschlag nur bezüglich der Inkriminierung der Zahlung für kinderpornographische Schriften über alle Zweifel erhaben. Nach hier vertretener Auffassung (s. oben 7.3.1., S. 89) ist zur Umsetzung einer solchen Vorgabe eine Anpassung der §§ 184b, 184c StGB erforderlich.

Zweitens soll eine Erscheinungsform des so genannten »Grooming« (s. hierzu bereits oben 7.3.1., S. 91) erfasst werden: Es sei unter Strafe zu stellen, wenn ein Erwachsener einer Person unter 18 Jahren mittels Informations- und Kommunikationstechnologie ein Treffen in der Absicht vorschlägt, bei diesem Treffen sexuellen Missbrauch zu begehen oder kinderpornographische Schriften herzustellen, und es sodann zu einem physischen Treffen gekommen sei (Art. 6). Der Versuch dieses Delikts ist nicht zwingend unter Strafe zu stellen (vgl. Art. 7 Abs. 2). Hieraus ergibt sich erstens die oben schon vorgeschlagene Änderung des § 176 Abs. 4 Nr. 3 StGB, der zukünftig über den Schriftenbegriff hinausgehende Kommunikationsformen erfassen müsste; andererseits müsste sich die Strafnorm auch auf Jugendliche, und nicht – wie bisher – nur auf Kinder erstrecken.

8.3.3. UN-Konvention über Cyberkriminalität

2010 diskutierten UN-Gremien, eine eigenständige UN-Konvention über Cyberkriminalität zu entwerfen und zur Unterzeichnung und Ratifikation aufzulegen (United Nations, 2010a). Hierbei sollte erstens auf neuartige Schwierigkeiten eingegangen werden, die durch das Übereinkommen über Computerkriminalität nicht adäquat gelöst werden, so etwa bezüglich extraterritorialer Ermittlungen (s. unten 8.4.3., S. 169). Zweitens war nicht zu überhören, dass es anderen Weltregionen missfiel, ein Europarats-Übereinkommen zu unterstützen bzw. Vertragspartei einer solchen Konvention zu werden (United Nations, 2010a, Nr. 44). Angesichts unüberbrückbarer politischer Differenzen wurde dieses Vorhaben allerdings bis auf Weiteres zurückgestellt (United Nations, 2010b, Nr. 202ff.).

8.3.4. Fazit

Erstens sorgen bereits die bestehenden internationalen und europäischen Rechtsakte für eine weit reichende Harmonisierung des materiellen Strafrechts betreffend Angriffe gegen Informationssysteme. Zudem sind auch etliche Delikte, bei denen informationstechnische Systeme als Werkzeug eingesetzt werden – so archetypisch Computerbetrug und die Verbreitung und der Besitz kinderpornographischer Schriften – harmonisiert.

Zweitens liegt es in der Regel bereits im Eigeninteresse der Staaten, bestehende Schutzlücken im Bereich der Cyberkriminalität zu schließen, so dass es internationaler Vorgaben nicht bedarf. Nur in wenigen Teilbereichen – etwa durch die Duldung mancher Formen der Wirtschaftskriminalität, etwa der Wirtschaftsspionage – mag es im Interesse einzelner Staaten liegen, auf eine Pönalisierung zu verzichten. Insoweit ist auf eine wechselseitige, idealerweise weltweite Verpflichtung zur Inkriminierung der Wirtschaftsspionage hinzuwirken.

Drittens verspricht eine weitergehende Harmonisierung und Verschärfung der Strafrahmen wenig Erfolg, da der abstrakten Strafhöhe keine oder nur geringe general- und spezialpräventive Wirkung zukommt.

Schließlich und viertens ist zu berücksichtigen, dass innerhalb der Europäischen Union das Rechtshilfeerfordernis beiderseitiger Strafbarkeit zurückgedrängt wird. Dies ermöglicht eine effektive transnationale Strafverfolgung also selbst dann, wenn in einem anderen Staat eine bestimmte Verhaltensweise nicht unter Strafe stehen sollte.

Eine Notwendigkeit für eine weitergehende Harmonisierung des materiellen Computerstrafrechts besteht daher derzeit nicht. Mehr Augenmerk sollte allerdings gerichtet werden auf die effektive Umsetzung der bestehenden Vorgaben, insbesondere im Bereich der Europäischen Union (s. insoweit KOM [2008] 448 endgültig).

8.4. Extraterritoriale Strafverfolgung

Kriminalität überwindet seit je her räumliche Grenzen: Sei es, dass Waren über Staatsgrenzen hinweg geschmuggelt werden; sei es, dass Täter über Staatsgrenzen fliehen. Die zunehmende Vernetzung und räumliche Entgrenzung der Informationstechnologie führt daher im Ausgangspunkt nur zu einer Intensivierung bekannter Phänomene, namentlich der Frage, wie eine Strafnorm auch über Staatsgrenzen hinaus durchgesetzt werden kann. Die Möglichkeiten und Risiken einer solchen transnationalen Strafverfolgung gilt es nun aus zwei Blickwinkeln zu beleuchten.

Die erste, in diesem Abschnitt betrachtete Sichtweise ist eine *nationale*: Auf welche Sachverhalte, die sich (auch) im Ausland zutragen, kann deutsches Strafrecht Anwendung finden? Inwieweit dürfen deutsche Strafverfolgungsbehörden auf Beschuldigte und Beweismittel im Ausland zugreifen? Drohen hier Konflikte mit anderen Staaten?

Aufgrund von faktischen und rechtlichen Begrenzungen einer solchen extraterritorialen Strafverfolgung, aber auch aus Effektivitätsgründen ist die zweite und im nächsten Abschnitt (8.5., S. 173) diskutierte Sichtweise die einer *justiziellen Zusammenarbeit verschiedener Kriminaljustizsysteme*: Deren Fragen reichen von den klassischen Instrumenten der Auslieferung und der so genannten »sonstigen Rechtshilfe« hin zu den modernen Maßnahmen der Europäischen Union.

Nun ist aber zu unterscheiden, woraus sich der transnationale Aspekt der Strafverfolgung ergibt: Wurde eine Straftat im Ausland begangen, so ist es eine Frage der extraterritorialen Anwendung des Strafrechts (des sogenannten internationalen Strafrechts), ob diese auch im Inland bestraft werden kann (8.4.1.). Wenn sich das Recht zweier Staaten auf einen Sachverhalt erstreckt, kann dies zu dreierlei Arten von Kompetenzkonflikten führen (8.4.2.). Ist hingegen die Frage, wie auf Beweismittel, Beschuldigte oder Zeugen im Ausland zugegriffen werden kann, so ist dies nach den engen Grundsätzen extraterritorialer Ermittlungen zu lösen (8.4.3.).

8.4.1. Extraterritoriale Anwendung des Strafrechts

Anknüpfungspunkte des deutschen internationalen Strafrechts

Die Frage, auf welche Sachverhalte eine Strafnorm räumlich Anwendung finden soll, ist im Ausgangspunkt vom nationalen Gesetzgeber zu klären. Gänzlich unproblematisch ist dies, soweit er sich dabei auf das eigene Staatsgebiet beschränkt, da seine ursprüngliche Staatsgewalt sich ohnehin auf dieses erstreckt (*Territorialitätsprinzip*, in Deutschland – § 3 StGB – Ausgangspunkt des internationalen Strafrechts). Dabei ist zu beachten, dass aufgrund des *Ubiquitiätsprinzips* sowohl die Sachverhalte erfasst werden, bei denen der Täter im Inland handelt oder aber eine strafrechtlich relevante Konsequenz im Inland eintritt.

Soll aber die Reichweite der Strafnorm über das eigene Staatsgebiet hinausreichen, also weder Handlungs- noch Erfolgsort im Inland liegen, so ist nach bisheriger Auffassung einzige völkerrechtliche Schranke, dass die Anwendung des Strafrechts an einem sinnvollen Aspekt anknüpfen müsse, der eine legitime Verbindung zwischen Tat und Staat herstelle (*genuine link*, s. hierzu ICJ, Reports 1955, 3, 4, 23 (*Nottebohm*); BGHSt 45, 68; s. ferner Satzger, 2010, § 4). Eine Fülle solcher Anknüpfungskriterien ist völkerrechtlich anerkannt: Beispielhaft herausgegriffen sei die Erfassung sämtlichen Verhaltens der eigenen Staatsangehörigen und gegen die eigenen Staatsangehörigen (aktives und passives Personalitätsprinzip), Verhaltens gegen Gemeininteressen (Schutzprinzip) und schließlich Straftaten, welche die Menschheit als Ganzes betreffen und daher von allen Staaten verfolgt werden dürfen (Weltrechtsprinzip).

Deutschland macht von sämtlichen diesen Prinzipien in den §§ 3 ff. StGB Gebrauch. Auf zwei Anwendungsregeln sei dabei besonders hingewiesen: Betriebs- und Geschäftsgeheimnisse inländischer Unternehmen werden gegen weltweite Angriffe, also auch gegen ausländische Niederlassungen, durch das deutsche Strafrecht geschützt (§ 5 Nr. 7 StGB). Dies erklärt sich aus dem Bedrohungspotential, dem die deutsche Wirtschaft durch Wirtschaftsspionage ausgesetzt ist, so dass sich etwa auch wegen Ausspähens von Daten (§ 202a Abs. 1 StGB) strafbar machen kann, wer im Ausland auf einen ausländischen Server zugreift, auf dem Geschäftsgeheimnisse eines deutschen Unternehmens abgespeichert sind. Die Verfolgung der Verbreitung harter Pornographie sowie der Verbreitung kinder- und jugendpornographischer Schriften (§ 6 Nr. 6 StGB) ist ein weltweites Anliegen, das dem Wortlaut des § 6 StGB zufolge weltweit dem deutschen Strafrecht unterliegt. Hiervon macht die Rechtsprechung allerdings eine gewisse Einschränkung, die aus Effektivitätsgründen zu begrüßen ist: Diese verlangt gleichwohl einen Anknüpfungspunkt an das Inland, der allerdings bereits durch den späteren Wohnsitz des Täters im Inland vorliegen kann (BGHSt 45, 68).

Übertragbarkeit auf Sachverhalte der Cyberkriminalität

Das Internet oder der *Cyberspace* ist kein gesonderter Raum, in dem man Straftaten begehen kann: Straftäter verhalten sich nach wie vor in der realen, physischen Welt, wenn sie etwa einen bestimmten Befehl auf einer Computertastatur eingeben, einen Computer anweisen, eine kinderpornographische Darstellung abzuspeichern, oder einen beleidigenden Text versenden. Der Handlungsort auch bei allen Delikten der Cyberkriminalität richtet sich danach, an welchem Ort sich der Täter befindet, so irrelevant dieser Aspekt auch aus technischer Sicht sein mag.

Weitaus schwieriger zu beantworten ist hingegen die Frage nach dem Erfolgsort: Bei Erfolgsdelikten wie Körperverletzung und Totschlag, aber auch dem Ausspähen von Daten lässt sich zwar noch ohne Weiteres feststellen, an welchem Ort und damit in welchem Land ein zum Tatbestand gehörender Erfolg eingetreten ist. Auch bei einem konkreten Gefährdungsdelikt lässt sich die konkrete Gefahr räumlich zuordnen. Große Schwierigkeiten bereiten jedoch abstrakt-konkrete Gefährdungsdelikte – auch Eignungsdelikte genannt – wie etwa die Volksverhetzung (§ 130 StGB). Die Rechtsprechung sieht hier einen Erfolgsort überall dort gegeben, wo die konkrete Tat ihre Gefährlichkeit im Hinblick auf den jeweiligen Schutzzweck der Norm entfalten könne (BGHSt 46, 212). Diese Rechtsprechung wurde eingeleitet durch ein Strafverfahren wegen Volksverhetzung gegen einen Australier, der allein in Australien gehandelt und die rechtswidrigen Schriften auf einem australischen Server zum Zugriff via Internet bereitgestellt hatte. Allerdings wiesen die Schriften die eindeutig zu erkennende Zielrichtung auf, Deutsche zum Lesen der Schriften zu bewegen. Daher – und weil ein völkerrechtlich legitimierender Anknüpfungspunkt im Sinne eines besonderen objektiven Bezugs zu Deutschlands vorliege – bejahte der Bundesgerichtshof das Vorliegen eines Erfolgsorts in Deutschland und so auch die Anwendbarkeit deutschen Strafrechts (BGHSt 46, 212 m. Anm. u. Bespr. Bremer, 2002; Hörnle, 2001; Jeßberger, 2001; Kudlich, 2001; Lagodny, 2001; Roggan, 2001; Sieber, 2001; Vec, 2002; s. ferner KG NStZ 2000, 533 m. Anm. B. Heinrich, 2000 sowie Hilgendorf, 2001; Sieber, 1999b). Die Gegenauffassung der Literatur verweist unter anderem darauf, dass abstrakt-konkrete Gefährdungsdelikte gerade keinen »Erfolgseintritt« erfordern, mithin der Wortlaut und auch der Sinn und Zweck des »Erfolgsorts« überdehnt wird. Daher werden verschiedene, restriktive Ansätze diskutiert (vgl. die exzellenten Darstellungen bei Fischer, 2011, § 9 Rdn. 5 ff. m.w.N.; Satzger, 2009, § 9 Rdn. 14 ff. m.w.N.), die sich auch verallgemeinern lassen:

Einer Auffassung zufolge sei entscheidend die subjektive Zielrichtung des Täters: Sollen volksverhetzende Inhalte von deutschen Nutzern bzw. von Nutzern in Deutschland in Anspruch genommen werden? Befindet sich der Adressat einer E-Mail im restriktiveren Deutschland, oder in den meinungsäußerungsfreundlicheren USA? Dem ist entgegenzuhalten, dass es für die Anwendbarkeit des deutschen Strafrechts auch sonst allein auf objektive Kriterien ankommt, ein Irrtum über die Anwendbarkeit deutschen Strafrechts

führt daher nicht zur Straflosigkeit (§ 16 StGB). Wenig tauglich ist es auch, auf die deutsche Sprache abzustellen – diese findet auch in Österreich Verwendung – oder zwischen gezieltem Übermitteln (*Push*) ins Inland oder bloßem Abruf durch inländische Nutzer von im Ausland verfügbaren Informationen (*Pull*) zu unterscheiden (vgl. Satzger, 2009, § 9 Rdn. 18 m.w.N.): Angesichts der technischen Beliebigkeit der zugrunde liegenden Technologien kann dies nicht zu sachgerechten Ergebnissen führen.

Auch ein anderer kultureller oder sozialer Hintergrund als derjenige, der einer Strafnorm zugrunde liegt, bietet keine Rechtfertigung für eine Verletzung des Strafgesetzes. So kann auch einem in den Vereinigten Staaten aufgewachsenen Täter kein Rechtfertigungsgrund zugute kommen, dass er in einem Land aufgewachsen sei, in dem die Meinungsäußerungsfreiheit einen ganz anderen Stellenwert aufweist als in Deutschland; allenfalls mag seine Schuld gemildert sein (§ 17 StGB; weitergehend Valerius, 2003).

Doch all diese nationalen Restriktionsansätze leiden an ihrer räumlichen Begrenzung, da sie nur die Anwendbarkeit deutschen Strafrechts reduzieren, nicht aber eine internationale Lösung des zugrunde liegenden Problems (zu) extensiver Anwendung des Strafrechts auf transnationale Sachverhalte bewirken. Richtigerweise ist daher zu überlegen, wie Konstellationen vermieden werden können, in denen mehr als eine Strafrechtsordnung Anwendung findet (Kompetenzkonflikte).[1]

8.4.2. Kompetenzkonflikte

Besteht zu mehreren Staaten ein *genuine link*, so führt dies nahezu zwangsläufig zu Kompetenzkonflikten: Welche Rechtsordnung ist zur Entscheidung darüber berufen, ob strafbares Verhalten vorliegt? Welche Rechtsordnung ist zur Strafverfolgung berufen oder gar verpflichtet? Drei verschiedene Arten von Kompetenzkonflikten lassen sich dabei differenzieren:

- Das Strafrecht von mindestens zwei Staaten ist anwendbar, daher schicken sich zwei oder mehr Staaten an, einen Beschuldigten strafrechtlich zu verfolgen (*positiver Kompetenzkonflikt*).
- Das Strafrecht von mindestens zwei Staaten ist anwendbar, keiner dieser Staaten möchte jedoch die Strafverfolgung übernehmen (*negativer Kompetenzkonflikt*).
- Das Recht zweier oder mehrerer Staaten ist anwendbar. Während ein Staat einen Sachverhalt einer Strafnorm unterwirft und den Verstoß auch verfolgen möchte, ist derselbe Sachverhalt im anderen Staat straflos, verfassungsrechtlich geschützt oder sogar rechtlich geboten (hier als *Divergenzkonflikt* bezeichnet).

[1] Als Ausnahme sei zugestanden, wenn sich ein *primär* zuständiges Kriminaljustizsystem als unfähig oder unwillig erwiesen hat, eine Strafverfolgung durchzuführen, vgl. Art. 17 Abs. 1 lit. a Römisches Statut des Internationalen Strafgerichtshofs.

Positive Kompetenzkonflikte

Führt ein positiver Kompetenzkonflikt zu einer gleichzeitigen oder nacheinander erfolgenden Doppelverfolgungen durch zwei oder mehr Staaten, so ist dies eine für den Beschuldigten überaus belastende Situation: Erstens muss er sich mehrfach gegen denselben Vorwurf zur Wehr setzen; nationale Verbote der Doppelbestrafung (*ne bis in idem*, Art. 103 Abs. 3 GG) stehen dem nicht entgegen. Zweitens stehen den Ermittlungsbehörden die verfahrensrechtlichen Möglichkeiten mehrerer Kriminaljustizsysteme offen, die sich auch zu Lasten des Beschuldigten und auch zu Lasten Drittbetroffener miteinander kombinieren lassen (*forum shopping*): Die Strafverfolger wählen für die jeweilige Ermittlungsmaßnahme die Rechtsordnung, welche diese im weitesten Umfang zulässt, und wählen sodann für die Anklageerhebung diejenige Rechtsordnung, welche die Beweisverwertung im weitesten Umfang zulässt. So lässt sich ein austariertes System an Beschuldigten- und Verteidigungsrechten ohne Weiteres umgehen. Drittens setzt sich die härtere der ausgeurteilten Strafen durch: Es wird auf die in Deutschland ausgeurteilte Strafe die bereits vorher verbüßte ausländische Strafe angerechnet (§ 51 Abs. 3 StGB), wenn aber die deutsche Strafe härter ist als die ausländische Strafe, so hat der Verurteilte die Strafdifferenz noch zu verbüßen.

Positive Kompetenzkonflikte sind allerdings auch für die beteiligten Staaten wenig zweckdienlich: Zur Schonung der begrenzten Ressourcen der Kriminaljustizsysteme ist allein aus Effizienzgesichtspunkten grundsätzlich darauf hinzuwirken, dass nur ein Staat die Strafverfolgung durchführt.

Zur Lösung positiver Kompetenzkonflikte werden innerhalb der Europäischen Union – und weniger weiterer Staaten – zwei Ansätze verfolgt: Erstens wurde durch Art. 54 Schengener Durchführungsübereinkommen ein europäisch-transnationaler Strafklageverbrauch eingeführt, der inzwischen auch justizgrundrechtlich in Art. 50 Charta der Grundrechte der Europäischen Union abgesichert ist (Burchard & Brodowski, 2010). Eine Verurteilung innerhalb der Europäischen Union und der weiteren Staaten des Schengenraums sperrt daher eine weitere parallele oder sequenzielle Strafverfolgung wegen derselben Tat. Bis zu einer ersten Verurteilung sind parallele Ermittlungs- und Strafverfahren jedoch nicht gesperrt, so dass das Problem des *forum shopping* verbleibt.

Zweitens wurde institutionell durch Eurojust und regulatorisch durch einen Rahmenbeschluss zur Vermeidung und Beilegung von Kompetenzkonflikten in Strafverfahren (AblEU 2009 L 328 vom 15.12.2009, S. 42) ein Mechanismus geschaffen, Parallelverfahren in mehreren Mitgliedstaaten der Europäischen Union zu vermeiden. Die jeweils betroffenen Mitgliedstaaten sollen hierzu untereinander klären, welcher Staat die Strafverfolgung durchführen solle. Die Rechtswissenschaft kritisiert daran zu recht, dass es sich weder um eine gerichtlich überprüfbare, justiziable Lösung noch um eine wirkliche Vermeidung von Doppelverfolgungen und des *forum shopping* handele.

Negative Kompetenzkonflikte

Laut informellen Angaben der Strafverfolgungsbehörden soll das praxisrelevantere Problem allerdings darin liegen, dass sich zwei an sich zur Strafverfolgung berufene Staaten jeweils mit einem eigenen Ermittlungs- bzw. Strafverfahren zurückhalten unter dem Hinweis darauf, dass der andere Staat diese Strafverfolgung vornehmen könne und auch solle. Die Gründe hiervon sind mannigfaltig und reichen von der individuellen Arbeitsersparnis bis hin zu auch politisch sensiblen Fällen, mit denen keiner der beiden betroffenen Staaten befasst sein möchte.

Erneut ist auf die Lösungsansätze in der Europäischen Union zu verweisen, die über Eurojust und die Konsultationspflichten des Rahmenbeschlusses zur Vermeidung und Beilegung von Kompetenzkonflikten explizit auch der Vermeidung negativer Kompetenzkonflikte dienen. Rein national ist auf das Legalitätsprinzip und die Verpflichtung der Staatsanwaltschaft zur Aufnahme von Ermittlungen betreffend aller verfolgbaren in- und ausländischen Straftaten hinzuweisen.

Divergenzkonflikte

Auf den wohl bekanntesten Fall eines Divergenzkonflikts wurde bereits zuvor hingewiesen: Ein Australier wurde in Deutschland wegen Volksverhetzung bestraft, obschon er allein in Australien unter Zuhilfenahme australischer Internet-Dienstleister gehandelt hatte, und obwohl seine Äußerungshandlung zum damaligen Zeitpunkt in Australien nicht nur straflos war, sondern deren Straflosigkeit auch durch australisches Verfassungsrecht garantiert wurde.

Mag man dieses Ergebnis bei einer Volksverhetzung – auch angesichts der besonderen historischen Verantwortung Deutschlands – auch billigen, doch stellen sich eine Vielzahl von Folgeproblemen, die freilich bislang noch keine praktische Relevanz erlangten: Ein Lehrbuchbeispiel handelt etwa davon, dass die Werbung für alkoholische Getränke in einem islamisch geprägten Land strafbar sei – und nun ein deutscher Bierbrauer, der für seine Produkte im Internet wirbt, sich auf Urlaubsreise in dieses Land begebe. Fischer (2011, § 9 Rdn. 8a) weist zutreffenderweise darauf hin, »dass Pornographie keinen, Hetze gegen australische Juden … einen ‚besonderen' Bezug zu Deutschland hat …, mag hier mit guten Gründen so gesehen werden, könnte dem australischen Neonazi in Australien aber ebenso einerlei sein wie zB dem deutschen Erotikfreund die Ansichten arabischer Fachleute für Sittlichkeit«.

Manches deutet darauf hin, dass drei erhebliche, auch wirtschaftlich und politisch bedeutsame Divergenzkonflikte bereits bald Kopfschmerzen bereiten werden:

- Erstens bezüglich der Legalisierung und strafrechtlichen Ahndung von Glücksspiel im Internet (s. bereits Spindler, 2004),

- zweitens zwischen einerseits Wirtschaftsregulierung und den damit verbundenen Offenlegungspflichten, insbesondere im angloamerikanischen Raum, und andererseits dem deutschen und kontinentaleuropäischen Verständnis des Datenschutzes, sowie
- drittens zwischen staatlichem und betrieblichem Geheimnisschutz und Presse-, Meinungs- und Informationsvermittlungsfreiheit (etwa bei WikiLeaks).

Aus völkerrechtlicher Sicht ist diesbezüglich festzuhalten, dass eine extra-territoriale Anwendung von Strafrecht bislang geduldet wird, wenn erstens ein legitimer völkerrechtlicher Anknüpfungspunkt besteht und zweitens die Exterritorialität von bestimmten Hoheitsträgern wie Botschaftern gewahrt bleibt (vgl. §§ 18–20 GVG in Deutschland). Allerdings stellt sich bei einem Divergenzkonflikt regelmäßig das faktische Problem, dass sich der mutmaßliche Täter in dem Land aufhält, in dem das relevante Verhalten straflos ist. Das klassische Rechtshilferecht beschränkt die Auslieferung jedoch durch das Erfordernis, dass die Tat in beiden Staaten strafbar sein muss – dies führt zu einer gewissen Vorhersehbarkeit einer strafrechtlichen Ahndung. Moderne Rechtshilfeinstrumente, insbesondere innerhalb der Europäischen Union, verzichten aber weitgehend auf dieses Kriterium. Hieraus erklärt sich eine Literaturauffassung, die bei Internetsachverhalten grundsätzlich eine beiderseitige Strafbarkeit am Handlungs- und Erfolgsort verlangt, damit eine Straftat verfolgt werden kann.

In gewissem Maße zur Lösung von Divergenzkonflikten nützlich sind erstens die bereits angesprochenen nationalen Reduktionsansätze des Strafanwendungsrechts. Allerdings ist eine Eindämmung der extraterritorialen Anwendung des Strafrechts politisch wenig erfolgversprechend. Zweitens liefert ein »strafrechtliches Herkunftslandprinzip« einen interessanten Ansatz (s. hierzu Kudlich, 2004; Dannecker, 2005, S. 714 ff.): Die Rechtmäßigkeit von Daten, von Internet-Auftritten usw. solle sich danach beurteilen, in welchem Staat sie eingegeben wurden. Sodann wäre das in Australien verfügbar gemachte volksverhetzende Material – angesichts der damaligen Rechtslage in Australien – weltweit geschützt und eine Strafverfolgung in Deutschland unzulässig gewesen.

Ein solches Herkunftslandprinzip setzt allerdings ein weit reichendes Vertrauen in eine ausländische Rechtsordnung voraus, dass diese erheblich sozialschädliche Verhaltensweisen auch dann unter Strafe stellt, wenn die schädlichen Wirkungen im Ausland eintreten. Ein solches Vertrauen – unter Umständen untermauert durch eine Harmonisierung des materiellen Strafrechts – ist aber zugleich Grundlage europäischer Instrumente betreffend die justizielle Zusammenarbeit in Strafsachen. In diesem europäischen Rahmen erscheint daher ein Herkunftslandprinzip auch für Daten und Internet-Angebote ein diskutabler Ansatz.

Über die Stärkung gegenseitigen Vertrauens kann eine Harmonisierung des materiellen Strafrechts sich als nützlich erweisen, um einen gemeinsamen Mindeststandard zu defi-

nieren, bei dessen Verletzung man überall mit Strafverfolgung zu rechnen hat (vgl. hierzu bereits oben 8.3., S. 156).

Darüber hinausgehend ist es aber auch dringend geboten, einen gemeinsamen Mindeststandard zu definieren, innerhalb dessen Rahmen man sich überall auf die Straflosigkeit seines Verhaltens verlassen kann (*safe harbours*). Ob es ausreicht, diesen Mindeststandard straflosen Verhaltens allein aus den internationalen Grundrechtskatalogen zu erschließen, erscheint dabei zweifelhaft: Diese eröffnen einen weiten Wertungs- und Beurteilungsspielraum und weite Schrankenbestimmungen, sind nur unzureichend an die Herausforderungen einer modernen Kommunikationsgesellschaft angepasst, und taugen eher für eine *ex post*-Beurteilung, ob eine strafrechtliche Verurteilung menschenrechtswidrig war. Dies zeigt, dass explizite, international Gültigkeit erlangende *safe harbour*-Bestimmungen sich nicht länger auf so exotische Rechtsgebiete wie das Wertpapierhandelsrecht beschränken sollten (vgl. dort § 14 Abs. 2 WpHG), sondern etwa auch für den Journalismus, für die IT-Sicherheitsforschung und für die Informationsfreiheit formuliert werden müssen.

8.4.3. Extraterritoriale Ermittlungen

Die Möglichkeiten der deutschen Strafverfolgungsbehörden sind räumlich begrenzt: Die Hoheitsgewalt des deutschen Staates und damit auch seiner Exekutive ist im Ausgangspunkt auf das deutsche Territorium begrenzt. Andernfalls besteht die Gefahr, dass für Deutschland tätige Akteure die Hoheitsrechte eines fremden Staates verletzen. Daher erfordert die Ergreifung eines in das Ausland flüchtenden Straftäters regelmäßig die Mithilfe oder zumindest das Einverständnis eines anderen Staates, ebenso der Zugriff auf sich im Ausland befindende Beweismittel. Diese internationale Rechtshilfe in Strafsachen und deren Grundprinzipien werden im nächsten Abschnitt näher vorgestellt (8.5.1), zunächst ist aber der Frage nachzugehen, ob es auch ohne Einverständnis eines ausländischen Staates Ausnahmen von dem Grundsatz gibt, dass deutsche Strafverfolgungsbehörden nur im Inland tätig sein dürfen.

Grundrechtsbindung

Als erster, wesentlicher Grundsatz ist diesbezüglich festzustellen, dass – entgegen einer in den USA teilweise vertretenen Auffassung (vgl. die Nachweise in US Supreme Court, Boumediene v. Bush, 553 U.S. 723 (2008)) – jegliches extraterritoriales Handeln Deutschlands an die verfassungsrechtlich garantierten Grundrechte und damit auch an das Recht auf ein faires, rechtsstaatliches Verfahren gebunden ist; dies ergibt sich bereits aus dem unzweifelhaften Wortlaut der Art. 1 Abs. 3, Art. 20 Abs. 3 GG.

Inkurs: male captus, bene detentus

Zweitens ist auf die nicht unproblematischen Fälle hinzuweisen, in denen ein Beschuldigter – sei es durch Geheimdienste, sei es durch Polizeibeamte, sei es durch Private – im

Ausland entführt und ins Inland verbracht wird, um ihn dort strafrechtlich zur Verantwortung ziehen zu können. Dass dies nicht nur ein theoretisches Konstrukt ist, zeigt etwa der Fall »Eichmann«, der von Agenten des Mossad in Argentinien festgenommen und sodann nach Israel überführt wurde, wo er wegen seiner Verbrechen während der nationalsozialistischen Unrechts- und Gewaltherrschaft verurteilt wurde; aber auch deutsche Polizeibeamte haben bereits extraterritorial Verdächtige festgenommen, so etwa einen Betäubungsmittelkriminellen in den Niederlanden. Deutsche, aber auch ausländische Gerichte verneinen in solchen Konstellationen – trotz aller völkerrechtlichen Brisanz – ein Verfahrenshindernis, wenn jedenfalls eine Straftat von erheblichem Gewicht vorliege (*male captus, bene detentus*; s. etwa BVerfG StV 1987, 137; US Supreme Court, US v. Alvarez-Machain, 504 U.S. 655 (1992)). Es erscheint allerdings zweifelhaft, ob ein rechtsförmiges, faires Strafverfahren noch gegeben ist, wenn die Ermittlungsbehörden ihre (völker)rechtlichen Befugnisse in einer solch deutlichen Weise bewusst überschreiten (vgl. Schubarth, 1987).

Extraterritorialer Zugriff auf Beweismittel

Dies ist nun auf einen extraterritorialen Zugriff auf Beweismittel zu übertragen: Inwieweit dürfen deutsche Strafverfolgungsbehörden auf Internetseiten, auf E-Mail-Postfächer oder passwortgeschützte Server im Ausland zugreifen? Auch hier ist zwischen der völkerrechtlichen Zulässigkeit und der Verwertbarkeit in einem nachfolgenden Strafverfahren zu unterscheiden:

Völkerrechtliche Zulässigkeit Allgemein anerkannt und zulässig ist es, auf »öffentlich zugängliche gespeicherte Computerdaten (offene Quellen)« zuzugreifen, und dies unabhängig davon, wo sich diese Daten befinden. So wie auch jede Privatperson keinen Eingriff in fremde Hoheitsrechte begeht, wenn sie eine im Ausland angebotene Internetseite aufsucht, so ist es mangels jeglicher Zwangswirkung auch kein völkerrechtlicher Verstoß, wenn der Zugriff durch staatliche Akteure erfolgt. Die entsprechende Klarstellung in Art. 32 lit. a des Übereinkommens über Computerkriminalität ist daher auch nur rein deklaratorischer Natur.

Ebenfalls anerkannt und unproblematisch gestattet ist der Zugriff auf passwortgeschützte oder sonstwie zugangsbeschränkte Daten, wenn eine rechtmäßige und freiwillige Erlaubnis einer Person vorliegt, die über diese Daten verfügen darf. Wenn also ein Beschuldigter einwilligt, auf seine im Ausland archivierten E-Mails zuzugreifen, so fehlt es an staatlichen Zwangswirkungen und damit an einem völkerrechtlich relevanten Vorgang. Auch dies ist in Art. 32 lit. b des Übereinkommens über Computerkriminalität nur klargestellt; ein solcher Zugriff ist daher über den Geltungsbereich des Übereinkommens hinaus gestattet.

Dabei ist allerdings kritisch zu hinterfragen, wer befugt ist, über Daten in dieser Weise zu verfügen: Ist dies neben dem Kunden auch der Anbieter eines E-Mail-Dienstes

bezüglich der im Postfach des Kunden abgespeicherten E-Mails? Ist dies auch der Anbieter einer Internet-Festplatte bezüglich der dort von Kunden abgelegten Daten? Die Praxis der bedeutenden Internet-Service-Dienstleister scheint hier eine großzügige zu sein; diese geben Daten recht freigiebig an die Strafverfolgungsbehörden heraus, wenn sie auch im Inland kommerziell tätig sind: Denn es ist für Außenstehende ohnehin nicht erkennbar, ob sich die relevanten Daten im In- oder Ausland befanden; Konflikte mit den Strafverfolgungsbehörden zu provozieren ist zudem für jedes Unternehmen unangenehm.

Bei Lichte besehen ist dies jedoch höchst problematisch, soweit es vorrangig einen Kunden betreffende, von diesem stammende oder an diesen gerichtete Daten betrifft: Aus dessen Sicht handelt es sich um einen verdeckten Zugriff der Ermittlungsbehörden, die mit den Internet-Service-Dienstleistern kollusiv zusammenwirken, und daher sehr wohl um einen Eingriff mit erheblicher Zwangswirkung und damit auch um einen völkerrechtlich relevanten Vorgang. Zur Wahrung dessen Interessen und auch zum Schutz vor Missbrauch – etwa zur Wirtschaftsspionage – erscheint es daher dringend geboten, das Einverständnis eines Internet-Service-Dienstleisters nicht genügen zu lassen, gleichzeitig aber nach einer praxistauglichen Alternative für eine schnelle, effektive Zugriffsmöglichkeit nach beweiserheblichen Daten zu suchen.

Ein verdeckter oder erzwungener Zugriff – also eine transnationale Durchsicht von Speichermedien, ein transnationaler Zugriff auf ein E-Mail-Postfach oder gar ein transnationaler, verdeckter Zugriff auf ein informationstechnisches System – ist völkerrechtlich ohne Einverständnis des betroffenen Staates unzulässig (s. LG Hamburg StV 2009, 70, 71; B. Gercke, 2009b, S. 272 f.; Klip, 2009, S. 371). Auch nach deutschem Recht sind daher solche transnationalen Zugriffe nicht von der Eingriffsgrundlage des § 110 Abs. 3 S. 1 StPO erfasst.

Entgegen einer Literaturauffassung (s. Meyer-Goßner, 2010, § 110 Rdn. 7a mit unzutreffendem Verweis auf Bär, 2007d, Rdn. 372 ff.) entfällt der völkerrechtliche Verstoß auch nicht, wenn die Daten zunächst nur gesichert werden (*quick freeze*) und bloß die spätere Auswertung und Verwendung von einem Einverständnis des anderen Staates abhängig gemacht wird – das Kind ist bereits in den Brunnen gefallen, da der zwangsweise Zugriff bereits erfolgt ist; nur die Intensität des völkerrechtlichen Verstoßes mag durch eine solche Vorgehensweise sinken.

Da all dies bereits seit längerem als misslich erachtet wird, werden – auch auf internationaler Ebene – verschiedene Lösungsansätze diskutiert (vgl. umfassend Bär, 2007d, Rdn. 372 ff.) Eine effektive und praxistaugliche, gleichwohl aber auch die Verhältnismäßigkeit wahrende und Missbrauchsmöglichkeiten – etwa zur Wirtschaftsspionage oder zur Verfolgung missliebiger Journalisten – vermeidende Lösung wird mehrere Schutzmechanismen kombinieren müssen: Ein kollusiver oder verdeckter Zugriff auf im Ausland befindliche Daten oder Speichermedien ohne vorheriges Einverständnis der anderen betroffenen Staaten ist daher erstens durch eine völkerrechtliche Vereinbarung zu regeln, die nur mit

vertrauenswürdigen Staaten abzuschließen ist. Diese muss zweitens den Zugriff nur bei dem Vorliegen von erheblichen Katalogtaten gestatten und drittens einen präventiven Richtervorbehalt vorsehen. Viertens ist der betroffene Staat zu informieren und ihm – etwa binnen einer Woche – die Möglichkeit zu geben, der Verwertung der sichergestellten Beweismittel zu widersprechen. Fünftens ist eine vorläufige Sicherung durch einen Internet-Service-Dienstleister einem sofortigen Zugriff vorzuziehen, wann immer dies technisch möglich ist und den Ermittlungserfolg nicht gefährdet, damit Daten nicht schon – ggf. zu missbräuchlichen Zwecken – transferiert werden, bevor der betroffene Staat dem Zugriff und der Verwertung widersprechen kann. Einfacher und genauso praxistauglich kann es aber alternativ auch sein, die bestehenden Kooperationsmechanismen und insbesondere das Kontaktstellennetzwerks (s. unten 8.5.2., S. 174) zu nutzen.

Verwertungsverbote im Strafverfahren? Bei aller Diskussion über die völkerrechtliche Zulässigkeit eines *quick freeze* oder auch eines kollusiven Zugriffs auf Daten ist zu berücksichtigen, dass die Rechtsprechung in Deutschland sehr zurückhaltend ist bei der Annahme eines Beweisverwertungsverbots, das sich auf einen völkerrechtlichen Verstoß stützt. Jedenfalls aber bei einer bewussten Umgehung des justizförmigen Verfahrens – sei es eines Richtervorbehalts, sei es aber auch der internationalen Rechtshilfe in Strafsachen – ist ein Beweisverwertungsverbot anzunehmen, auch wenn der Verstoß primär den Rechtskreis des anderen Staates und nicht den des Beschuldigten betrifft (B. Gercke, 2009b, S. 274).

8.4.4. Fazit

Der Cyberspace oder das Internet sind kein besonderer Raum. Das Internet bietet nur eine Kommunikationsstruktur zwischen in den verschiedenen Ländern befindlichen Personen und informationstechnischen Systemen. Daher gibt es stets auch einen räumlichen Anknüpfungspunkt, an dem eine Person gehandelt hat. Aufgrund dieses räumliche Bezugs der informationstechnischen Systeme – im Übrigen auch bei Virtualisierungsdiensten und bei *Cloud Computing* (s. hierzu M. Gercke, 2010c) – lässt sich ohne Weiteres mindestens ein Staat finden, dessen Strafrechtsordnung auf jede nur denkbare Internet-relevante Verhaltensweise Anwendung findet.

Das deutsche Strafrecht findet zudem auf eine Fülle von transnationalen Internet-Sachverhalten Anwendung. Da ausländische Rechtsordnungen gleichermaßen eine expansive Tendenz aufweisen, sind Kompetenzkonflikte vorprogrammiert. Hier gilt es neben einer Angleichung der Strafbestimmungen auch darüber zu diskutieren, welche Verhaltensweisen – etwa im Rahmen der Informations- und Medienfreiheit oder der IT-Sicherheitsforschung – gestattet sind und daher international einer Straffreistellung unterliegen müssen (*safe harbours*).

Ein direkter Zugriff auf im Ausland befindliche Beweismittel – ohne Einverständnis des ausländischen Staates – ist völkerrechtlich unzulässig. Eine zu weit gehende, freiwillige

Herausgabe von Daten durch Internet-Service-Dienstleister und die zu freigiebige Verwertbarkeit derart erlangter Daten in Strafverfahren führt zu einer Erosion nicht nur der Beschuldigtenrechte, sondern auch der Rechte von Drittbetroffenen oder von zu Unrecht Verdächtigten. Missbrauchsszenarien für Wirtschaftsspionage sind daher Tür und Tor geöffnet. Statt eigenständig auf im Ausland befindliche Beweismittel zuzugreifen, sollten daher die Möglichkeiten einer justiziellen Zusammenarbeit in Strafsachen (s. sogleich) verstärkt genutzt werden.

8.5. Justizielle Zusammenarbeit in Strafsachen

8.5.1. Die Entwicklung des Rechtshilferechts im Überblick

Aufgrund der eingeschränkten Möglichkeiten für einen extraterritorialen Zugriff auf Beweismittel – und auch auf Beschuldigte – verbleibt eine umfangreiche Notwendigkeit für eine internationale justizielle Zusammenarbeit in Strafsachen. Dabei sind drei verschiedene Entwicklungsstufen zu differenzieren:

Der vertragslose Auslieferungs- und Rechtshilfeverkehr ist ein politisch dominiertes und überformtes Gebiet, in dem es den beteiligten Staaten freisteht, ob sie eine Auslieferung oder eine sonstigen Rechtshilfe bewilligen. Das Rechtshilfeverfahren erfolgt dabei auf formalisierten diplomatischen Kanälen. Die rechtliche Absicherung – in Deutschland durch das Gesetz über die internationale Rechtshilfe in Strafsachen (IRG) – ist dabei recht umfassend, wenn auch in Teilen verbesserungsfähig. Die Schutzmechanismen reichen dabei von der Nichtauslieferung eigener Staatsangehöriger über das Erfordernis beiderseitiger Straf- oder Ahndbarkeit bis hin zu gewissen Überprüfungsmöglichkeiten des Schuld- bzw. Tatverdachts – auch bei Durchsuchungen (§§ 66 Abs. 2 Nr. 1, 67 IRG) und auch bei verdeckten Ermittlungsmaßnahmen wie einer Telekommunikationsüberwachung (§§ 59 Abs. 3, 77 Abs. 1 IRG, §§ 100a, 100b StPO; vgl. hierzu Nr. 77a Abs. 1 S. 2 RiVASt; Brodowski, 2009, S. 410; Schuster, 2006, S. 659).

Durch bi- und multilaterale völkerrechtliche Vereinbarungen verpflichteten sich Staaten in einem zweiten Entwicklungsschritt zur Bewilligung von Rechtshilfe in weit reichendem Umfang; zugleich wurden manche Rechtshilfehindernisse beseitigt und Spezialregelungen für bestimmte Maßnahmen im Ermittlungsverfahren eingeführt, etwa betreffend die Zustellung von Dokumenten oder die Vernehmung von Zeugen.

Ob die Europäisierung des Rechts der justiziellen Zusammenarbeit in Strafsachen, gegründet auf dem Prinzip der gegenseitigen Anerkennung, in der Tat einen Quantensprung darstellt, muss an dieser Stelle dahingestellt bleiben – jedenfalls ist auf Grundlage etlicher Maßnahmen der Europäischen Union ein eigenes, engmaschiges Kooperations- und auch Koordinationsrecht entstanden, welches auch und gerade in Bezug auf die Verfolgung von Cyberkriminalität nähere Betrachtung erfordert (unten 8.5.3., S. 176).

Schließlich: Durch eine Vielzahl völkerrechtlicher Verträge und Übereinkommen, aber auch durch eine Vielzahl informeller Entwicklungen ist ein Konglomerat von sich teilweise überschneidenden, teilweise ergänzenden Regelungen des Rechts der internationalen Rechtshilfe in Strafsachen gekommen, das selbst Experten auf diesem Gebiet nicht zu Unrecht als »Rechtshilfechaos« bezeichnen (Schomburg, 2006, Hauptteil II, Vorbem., Rdn. 4). Daher sollen an dieser Stelle lediglich die drei zur Verfolgung von Computerkriminalität wesentlichen Instrumentarien auf internationaler Ebene vertieft diskutiert werden, namentlich die grundlegenden Europarats-Übereinkommen betreffend Auslieferung und (sonstiger) Rechtshilfe, das G8 24/7-Netzwerk, und die rechtshilferechtlichen Bestandteile des Europarats-Übereinkommen über Computerkriminalität.

8.5.2. Bedeutende internationale Maßnahmen

Europäisches Auslieferungs- und Europäisches Rechtshilfeübereinkommen

Die Selbstverpflichtung der Vertragsstaaten, in größtmöglichem Umfang zulässige Auslieferungen und sonstige Rechtshilfe auch politisch zu bewilligen, ist die wohl wichtigste Errungenschaft des Europäischen Auslieferungsabkommens vom 15. Dezember 1957 (EuAlÜbk) und des Europäische Übereinkommens vom 20. April 1959 über die Rechtshilfe in Strafsachen (EuRhÜbk). Dennoch bestehen eine Vielzahl von Ablehnungsgründen fort, von dem Erfordernis beiderseitigen Strafbarkeit auch bei Durchsuchungen (Art. 5 EuRhÜbk) – jedenfalls, wenn Staaten, wie Deutschland, von einem entsprechenden Vorbehalt Gebrauch machen – bis hin zu einem umfassenden Vorbehalt, wenn die Leistung von Rechtshilfe wesentlichen Grundsätzen der deutschen Rechtsordnung widersprechen würde (nationaler *ordre public*-Vorbehalt).

G8 24/7-Network

Das langatmige tradierte Rechtshilferecht ist mit der Geschwindigkeit der Computertechnologie überfordert: Bis ein Ersuchen um sonstige Rechtshilfe auf diplomatischem Wege Entscheidungsträger im ersuchten Staat erreicht, können digitale Spuren ohne Weiteres verwischt werden. Daher beschlossen die G8 auf Initiative ihrer *Subgroup on High-Tech Crime*, ein informelles *G8 24/7 Network of Law Enforcement Points of Contact* einzurichten, dem sich auch weitere Staaten anschließen können. Derzeit bestehen Kontaktstellen in 49 Staaten. Durch die Verfügbarkeit von kompetenten Ansprechpartnern rund um die Uhr werden rasche, vorläufige Sicherungsmaßnahmen (*quick freeze*) erleichtert; die rechtliche Handhabe hierfür ist in Deutschland in § 67 IRG zu finden.

Beweismittel – etwa die vorläufig gesicherten Daten – können sodann im Ausgangspunkt nur nach herkömmlichem Rechtshilferecht übermittelt werden. Zwar haben sich die teilnehmende Staaten dazu bekannt, diese Rechtshilfe schnellstmöglich zu leisten. Die Praxis behilft sich aber oftmals mit Parallelermittlungen in beiden Staaten und einem

regen, zügigen und informellen Informationsaustausch zwischen den beteiligten Ermittlungsbehörden. Deren rechtliche Zulässigkeit ergibt sich in Deutschland nach den §§ 61a, 74 Abs. 4 IRG.

Der wesentlichste Gewinn durch dieses 24/7-Netzwerk liegt in der schnellen vorläufigen Sicherung von Beweismitteln (*quick freeze*), mittels derer eine Verwischung digitaler Spuren verhindert oder zumindest erschwert werden kann. Auch die Sicherungsmechanismen des Rechtshilferechts bleiben – zumindest theoretisch – erhalten, wenn sie nicht durch vorschnelle Parallelermittlungen, *forum shopping* und durch umfangreichen Informationsaustausch umgangen werden.

Übereinkommen über Computerkriminalität

Das im Rahmen des Europarats geschaffene Übereinkommen über Computerkriminalität (s. bereits oben 8.3.1., S. 157) widmet sich in ungewöhnlicher Ausführlichkeit den innerstaatlich bereitzustellenden Ermittlungsmaßnahmen bezüglich einer Herausgabe von Daten, bezüglich einer Durchsuchung und Beschlagnahme von Datenträgern und auch bezüglich eines *quick freeze* von Daten (Art. 16), um der durch die Flüchtigkeit von Computerdaten bestehenden Verdunkelungsgefahr zu begegnen. Dieser soll dadurch erfolgen, dass ein – besonders zur Vertraulichkeit verpflichteter – Diensteanbieter etwa einen (virtuellen) Datenspeicher derart sichert, dass eine Veränderung oder ein Verlust ausgeschlossen wird. Diese Daten sind sodann längstens 90 Tage vom Diensteanbieter vorzuhalten, so dass anschließend mittels üblicher Ermittlungs- und Rechtshilfemaßnahmen auf diese Daten zugegriffen werden kann. Ferner haben die Vertragsstaaten innerstaatliche Möglichkeiten zu einer Echtzeitüberwachung sowohl der Verkehrsdaten (Verbindungsdaten) als auch der Inhaltsdaten zu schaffen. Bei letzteren ist die Begrenzung auf bestimmte schwere Straftaten (Listendelikte), wie sie auch in Deutschland in § 100a Abs. 2 StPO vorgesehen ist, ausdrücklich anerkannt.

Bedeutsamer als diese rein nationalen Vorgaben sind die Neuerungen des zwischenstaatlichen Kooperationsrechts. Zwar ist der bereits diskutierte Art. 32 betreffend extraterritorialem, einvernehmlichen Zugriffs auf Daten nur deklaratorischer Natur, und zwar sind die Regelungen zur Weitergabe von Computerdaten (Art. 31) und Verkehrsdaten (Art. 30) – auch bei Echtzeitüberwachung (Art. 33, 34) – aus deutscher Sicht ohne näheren Belang, da die Herausgabe von (unkörperlichen) Gegenständen ohnehin in recht weit gehendem Umfang gestattet ist (s. hierzu BR-Drs. 666/07, S. 55). Auch das Kontaktstellennetz gemäß Art. 35 ist nur eine gewisse Formalisierung der vom G8-Kontaktstellennetz bekannten Herangehensweise, um mit der Schnelligkeit und Flüchtigkeit der Informationstechnik zumindest annähernd Schritt halten zu können.

Weit reichend ist allerdings die Verpflichtung, einen *quicke freeze* quasi auf ersten Zuruf eines anderen Staates durchzuführen, ohne dass eine intensive Prüfung der Rechtshilfevoraussetzungen vorgeschaltet ist. So entfällt die Prüfung einer beiderseitigen Strafbarkeit

jedenfalls bei den durch das Übereinkommen harmonisierten Straftatbeständen (Art. 29 Abs. 3, Abs. 4), und so gestattet Art. 29 Abs. 5 die Ablehnung nur bei politischen Taten und bei einem Verstoß gegen die nationalen Verfassungsgrundsätze (*ordre public*).

Fazit

Der informelle Mechanismus des G8-Kontaktstellennetzes, insbesondere aber auch die Regelung zu einem *quick freeze* von beweiserheblichen Daten auf ersten Zuruf im Übereinkommen über Computerkriminalität bieten den Strafverfolgungsbehörden weit reichende Möglichkeiten, auch in transnationalen Konstellationen mit der Schnelligkeit der Informationstechnologie Schritt zu halten. Problematisch ist allerdings die unzureichende Umsetzung dieser theoretischen Vorgaben in die Praxis: Noch immer haben nicht einmal sämtliche Mitgliedstaaten der Europäischen Union dieses Übereinkommen ratifiziert.

Auch ist zu begrüßen, dass die Sicherungsmechanismen des klassischen Rechtshilferechts – so unzureichend sie in manchen Konstellationen auch sein mögen – gewahrt bleiben, wie etwa eine Prüfung der beiderseitigen Strafbarkeit und der Wahrung des nationalen *ordre public*, bevor es zu einem Transfer beweiserheblicher Daten kommt. Schließlich verbleibt es auch bei einer Missbrauchsprüfung im politisch-administrativen Bewilligungsverfahren, wenn auch eine völkervertragliche Verpflichtung zur Leistung von Rechtshilfe im größtmöglichen Umfang gegeben sein mag.

Kritisch zu betrachten ist jedoch der umfassende und nicht ausreichend justiziell kontrollierte informelle, spontane Datenaustausch bei Parallelermittlungen, der zu *forum shopping* missbraucht werden kann, und der das austarierte innerstaatliche Gefüge zwischen Beschuldigtenrechten und Strafverfolgungsinteressen aus dem Gleichgewicht bringen kann. Ferner drohen Missbrauchsgefahren, soweit Verbindungsdaten weitergegeben werden müssen, auch ohne dass es einer beiderseitigen Strafbarkeit bedarf (Art. 30 des Übereinkommen über Computerkriminalität): Auf diesem Wege lassen sich etwa Netzwerke und Quellen missliebiger Journalisten rasch auch international aufdecken; dass der ersuchte Staat bei der erforderlichen »umgehenden« Erledigung erkennt, dass hierdurch der *ordre public* verletzt wird und dies die Ablehnung des Ersuchens gestattet (Art. 30 Abs. 2 lit. b), ist hoffentlich mehr als nur ein Wunschtraum.

8.5.3. Bedeutende Maßnahmen der Europäischen Union

Maßnahmen der Europäischen Union im Bereich des Strafrechts lassen sich theoretisch in fünf Kategorien einordnen, von denen inzwischen alle bedeutsam sind, um Strategien der Europäischen Union zur Verfolgung von Cyberkriminalität zu erkennen und zu bewerten.

- *Harmonisierung* ist nicht nur eine Frage des materiellen Rechts (s. hierzu oben 8.3.2., S. 158), sondern kann sich auch auf eine Rechtsangleichung bezüglich

Verfahrensrechten und auch bezüglich strafprozessualer Ermittlungsmaßnahmen beziehen.

- *Konvergenz* oder die offene Methode der Koordinierung (*Open Method of Coordination*) beschreibt einen Prozess, bei dem zunächst nicht-bindende Resolutionen, Entschließungen, Benchmarks usw. als politische Zielvorgaben auf internationaler Ebene definiert werden, auf die sodann in der weiteren rechtspolitischen Diskussion rekurriert wird. Solche nicht-bindenden Rechtsakte (*soft law*) lassen sich weitaus schneller – und oftmals ohne Beteiligung der Legislative – erreichen, sind aber oftmals mittel- bis langfristig Wegbereiter für einschneidende Veränderungen.
- *Kooperation* und damit eine Effektivierung der Rechtshilfe ist das zentrale Thema der Europäischen Union, und wird ergänzt durch eine
- *Koordination* der verschiedenen nationalen Kriminaljustizsysteme, etwa durch Europol und Eurojust.
- *Hochzonung* schließlich beschreibt eine Strafverfolgung auf genuin europäischer Ebene, etwa durch die Schaffung einer Europäischen Staatsanwaltschaft.

Harmonisierung des Verfahrensrechts

Die Harmonisierung des Verfahrensrechts wird in der Europäischen Union derzeit hauptsächlich im Hinblick auf einen Mindeststandard an Verfahrensrechten diskutiert (s. hierzu grundlegend AblEU 2009 C 295 v. 4.12.2009, S. 1). Für die Verfolgung von Cyberkriminalität bedeutender sind aber neuartige Harmonisierungsbestrebungen betreffend strafprozessualer Ermittlungsmaßnahmen. Hier ist zum einen die – auf durchaus zweifelhafter Rechtsgrundlage erlassene – Richtlinie über die Vorratsdatenspeicherung von Verbindungsdaten zu nennen (s. hierzu bereits oben 7.5.3., S. 145), zum anderen aber zwei noch im Gesetzgebungsprozess befindliche Richtlinienentwürfe:

Die Vorschläge für eine Richtlinie zur Bekämpfung der sexuellen Ausbeutung von Kindern und der Kinderpornographie und für eine Richtlinie zur Bekämpfung des Menschenhandels sahen ursprünglich weit gehende Verpflichtungen an die Mitgliedstaaten vor, so dass etwa »verdeckte Operation zumindest in den Fällen erlaubt sein sollten, in denen ein Informationssystem verwendet wird« (Art. 14 Abs. 3). Nach derzeitigem Stand der Diskussion ist allerdings im operativen Teil der Richtlinien-Entwürfe nur mehr die Verpflichtung zur Bereithaltung effektiver Ermittlungsmaßnahmen enthalten, die an diejenigen, die bei organisierter oder sonstiger schwerer Kriminalität zur Verfügung stehen, angeglichen werden sollen. Nur in den Erwägungsgründen wird weiterhin darauf hingewiesen, dass hierfür etwa ein verdeckter Zugriff auf informationstechnische Systeme, die Verwendung einer Legende zur Identitätstäuschung, Finanzermittlungen oder eine

elektronische Überwachung in Betracht kommen. Diese Entschärfung der Richtlinien-Vorschläge ist zu begrüßen, um auch weiterhin dem nationalen Gesetzgeber einen weiten Beurteilungsspielraum zu belassen, welche strafprozessualen Ermittlungsmaßnahmen er im Lichte verfassungsrechtlicher Vorgaben zur Verfolgung welcher Delikte einführen möchte.

Konvergenz

Bezüglich *soft-law*-Mechanismen zur Verfolgung von Cyberkriminalität ist auf mehrere Instrumente der Europäischen Union hinzuweisen, welche vorrangig die Bedeutung von Public-Private-Partnerships in diesem Bereich hervorheben und eine bessere Ausbildung fordern, aber auch Anregungen enthalten, wie die Rechtshilfe in diesen Fällen zukünftig vereinfacht werden könnte:

- Eine Empfehlung des Rates über Kontaktstellen mit einem rund um die Uhr erreichbaren Dauerdienst zur Bekämpfung der Hightech-Kriminalität (2001) legte den Mitgliedstaaten nahe, sich dem G8-Kontaktstellennetz anzuschließen.
- Eine Strategie für eine sichere Informationsgesellschaft (2006) arbeitet unter anderem die Bedeutung eines schnellen, länderübergreifenden Warnsystems bei akuten Bedrohungen und einer Inpflichtnahme der Wirtschaft zur Schaffung sicherer Informationstechnologie heraus.
- Eine allgemeine Politik zur Bekämpfung der Internetkriminalität (2007) unterstützt die Maßnahmen der G8 und des Europarats, betont die Notwendigkeit von Forschung über und Analyse der Bedrohungslage sowie eine bessere Schulung der Strafverfolgungsbehörden.
- Schlussfolgerungen über eine konzertierte Arbeitsstrategie und konkrete Maßnahmen zur Bekämpfung der Cyberkriminalität (2009) fordern unter anderem eine verstärkte Zusammenarbeit zwischen Strafverfolgungsbehörden und privaten Dienstleistern sowie die »Erleichterung von Ferndurchsuchungen, sofern diese nach nationalem Recht vorgesehen sind, so dass die Ermittlungsteams mit Zustimmung des Gastlandes raschen Zugang zu den Informationen erhalten können«, sprich die oben angesprochene Thematik des extraterritorialen Zugriffs auf Speichermedien.[2]

[2] Diese Schlussfolgerungen sahen als mittelfristig zu ergreifende Maßnahme vor, dass Diensteanbieter bestärkt werden sollten, Vorkehrungen zur Sperrung und/oder Schließung von kinderpornographischen Webseiten zu ergreifen. (Nr. 3 lit. b erster Spiegelstrich). Dass im Jahr darauf in Deutschland das Zugangserschwerungsgesetz und auf europäischer Ebene Initiativen hin zu einer europaweiten Regelung folgten, demonstriert auf eindrückliche Weise die politische Relevanz von solchen, rechtlich nicht bindenden Instrumenten der Konvergenz.

- Die EU-Strategie der inneren Sicherheit: Fünf Handlungsschwerpunkte für mehr Sicherheit in Europa (2010) kündigt die Schaffung eines EU-Zentrums für Cyberkriminalität für »operationelle und analytische Kapazitäten für einschlägige Ermittlungen« an, die als »Zentralstelle für die Bekämpfung der Cyberkriminalität in der EU« fungieren soll. Ob eine solche Zentralisierung im Lichte der Subsidiarität rechtmäßig und auch zweckmäßig ist, muss an dieser Stelle offen gelassen bleiben. Ferner sieht die Strategie vor, die »Robustheit des Netzes und der Informationsinfrastruktur« zu verbessern und die nationalen CERTs (s. oben 7.2.5., S. 84) zu stärken.

Kooperation

Phasen der Festnahme von Beschuldigten und der Vollstreckung von Rechtsfolgen Die wohl bedeutendsten Erfolge der Europäisierung des Strafverfahrens sind bislang im Bereich des Kooperationsrechts, sprich bei der Verbesserung des Rechts der internationalen Rechtshilfe in Strafsachen, zu verzeichnen. Dabei lag der Fokus in den vergangenen Jahren auf denjenigen Phasen eines Strafverfahrens, während der ein bestimmter Beschuldigter festgenommen, europaweit vor Gericht gebracht und die verhängten Rechtsfolgen sodann europaweit vollstreckt werden. Zu nennen sind hierbei folgende Rahmenbeschlüsse:

- Europäischer Haftbefehl (AblEG 2002 L 190 v. 17.7.2002, S. 1; s. hierzu BVerfGE 113, 273)
- Europäische Geldbuße oder Geldstrafe (AblEU 2005 L 76 v. 21.3.2005, S. 16)
- Europäische Einziehungsentscheidung (AblEU 2006 L 328 v. 23.11.2006, S. 59)
- Europäische Vollstreckungsanordnung (AblEU 2008 L 327 v. 4.12.2008, S. 27)
- Europäische Überwachungsanordnung im Ermittlungsverfahren (AblEU 2009 L 294 v. 11.11.2009, S. 20)

Diese Rechtsakte bezeichnen sich dabei dem Prinzip der gegenseitigen Anerkennung verpflichtet, das allerdings nur unvollkommen verwirklicht ist, denn eine ausländische justizielle Entscheidung wird mitnichten auf demselben Wege und nach demselben Maßstab ausgeführt wie eine inländische. Dennoch stellen diese Rechtsakte einen Meilenstein dar, denn sie verzichten bezüglich eines Katalogs von Delikten auf das Erfordernis beiderseitiger Strafbarkeit und fordern auch die Auslieferung von oder Vollstreckung gegenüber eigenen Staatsangehörigen.

In diesen Deliktskatalogen, bei denen auf die beiderseitige Strafbarkeit verzichtet wird, sind unter anderem enthalten »Kinderpornografie«, »Betrugsdelikte« und »Cyberkriminalität«. Grundsätzlich ist es eine Frage des jeweiligen nationalen Rechts, ob ein Straftatbestand unter eine dieser Kategorien subsumiert wird (EuGH, Urt. v. 3.6.2007, Rs. C-303/06 [Advocaten voor de Wereld VZW], Rdn. 53). So ist es nach der Systematik des deutschen Strafrechts ohne weiteres möglich, ja geradezu zwingend, Computerbetrug (§ 263a Abs. 1 StGB) als ein »Betrugsdelikt« im Sinne der Rahmenbeschlüsse aufzufassen, die Verbreitung und der Besitz kinder- und jugendpornographischer Schriften (§§ 184b, 184c StGB) als »Kinderpornografie« und schließlich Ausspähen und Abfangen von Daten, Datenveränderung sowie Computersabotage einschließlich der Vorbereitungstatbestände (§§ 202a, 202b, 202c, 303a, 303b StGB) als »Cyberkriminalität«. Dies lässt sich aber auch auf europäischer Ebene Übertragen: Da dieser Deliktskatalog Deliktsformen der Cyberkriminalität wie »Kinderpornografie« und »Betrug« in anderen Spiegelstrichen explizit erwähnt, ist aus systematischen Gründen hier »Cyberkriminalität« nur als Umschreibung des Angriffsobjekts, nicht jedoch des Tatmittels zu verstehen.

Dennoch: Diese verschiedenen Listendelikte verdeutlichen, dass bei den in der Praxis bedeutsamen Straftatbestände der Cyberkriminalität die Auslieferung innerhalb der Europäischen Union nicht länger von einem Erfordernis beiderseitiger Strafbarkeit abhängig ist und auch sonst einer rechtshilfefreundlichen Regelung unterworfen ist. All dies ist eine exzellente normative Grundlage für eine effektive europaweite Durchsetzung des Strafrechts bei Cyberkriminalität, wenn auch die Umsetzung in der Praxis und die bestehenden Schwächen, etwa die unverhältnismäßige Verwendung Europäischer Haftbefehle, auch in Zukunft kritisch begleitet werden müssen.

Phase der Beweisermittlung Nunmehr aber gewinnt die Phase der Beweisermittlung an politischer Relevanz, ja sogar an Brisanz. So wurde die weit reichende, von einer Gruppe von Mitgliedstaaten vorgelegte Initiative für eine Europäische Ermittlungsanordnung (s. hierzu sogleich S. 183) vom Bundesrat als auch vom Bundestag, dieser dabei sogar einstimmig, abgelehnt. Dabei darf allerdings keineswegs der bereits bestehende Rechtsrahmen unterschätzt werden, dessen Umsetzung und Wahrnehmung in der Praxis allerdings noch unzureichend ist. Besondere Bedeutung haben hier das EU-Rechtshilfeübereinkommen aus dem Jahr 2000, die Europäische Sicherstellungsanordnung – beide sind in Deutschland bereits umgesetzt – sowie die Europäische Beweisanordnung. Diese drei Instrumente sollen nun knapp vorgestellt werden:

Rechtshilfeübereinkommen von 2000 Das sogenannte Rechtshilfeübereinkommen von 2000 (*2000 MLA Convention*, eigentlich Übereinkommen vom 29.5.2000 über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union) erleichtert die Rechtshilfe zwischen den Mitgliedstaaten der EU über die Vorgaben des entsprechenden Europarats-Übereinkommens (s. oben 8.5.2., S. 174) hinaus. Zur Verfolgung von Cyberkriminalität besonders bedeutsam sind dabei die umfangreichen Bestimmungen

zur transnationalen Telekommunikationsüberwachung in Art. 17 bis 22 des Übereinkommens. Diese erfasst nämlich nicht nur Telefongespräche, sondern auch eine Überwachung des Datennetzwerkverkehrs, etwa des Internets. Wie auch im nationalen Recht ist dabei allerdings zu berücksichtigen, dass Gegenstand einer solchen Überwachung nur eine gerade andauernde Telekommunikation sein kann, nicht jedoch dauerhaft an einem Ort gespeicherte Daten, selbst wenn sie aus einer Telekommunikation herrühren oder für eine Telekommunikation verwendet werden können.

Das Übereinkommen sieht dabei gleich vier verschiedene Möglichkeiten vor, wie auf Telekommunikation im transnationalen Kontext zugegriffen werden kann. Neben der »klassischen« Echtzeitüberwachung, d.h. dem Abgreifen von Telekommunikation und die sofortige Weiterleitung der abgegriffenen Daten an den anderen Staat, ist auch eine verzögerte Weitergabe (Überwachung und Aufzeichnung) möglich (Art. 18). Gateways – d.h. Diensteanbieter in einem Land, die Telekommunikationsdienste für in einem anderen Land befindliche Personen anbieten – haben beiden Staaten die Möglichkeit einzuräumen, Telekommunikationsüberwachung durchzuführen (Art. 19). Diese Regelung betraf zwar zunächst Satelliten-Bodenstationen, dürfte wohl aber auch auf Betreiber virtueller privater Netzwerke (VPN) übertragbar sein. Zuletzt sind Regelungen für diejenigen Fälle vorgesehen, in denen ein Staat ohne technische Hilfe eines anderen Staates auf dort stattfindende Telekommunikation zugreifen kann (Art. 20). Dies ist etwa möglich durch eine entsprechende Steuerung der Datenströme des Internets.

Mit Ausnahme der Gateway-Konstellation kann allerdings der Staat, in dem sich der Betroffene befindet, die Telekommunikationsüberwachung davon abhängig machen, ob diese auch »in einem vergleichbaren Fall« im Inland durchgeführt würde (Art. 18 Abs. 5 lit. b, Art. 20 Abs. 4 lit. a i). Dies stellt erstens eine materielle Voraussetzung dar, d.h. in Deutschland müssen die entsprechenden Voraussetzungen des § 100a StPO (u.a. Katalogtat) gegeben sein. Zweitens aber ist dies auch eine formelle Voraussetzung, d.h. auch ein deutscher Richter hat nach Maßgabe des § 100b StPO über die Durchführung oder Duldung der Telekommunikationsüberwachung zu befinden (Schuster, 2006, S. 659).

Unter Berücksichtigung des europäischen *orde public* ist zudem festzuhalten, dass sowohl ersuchender als auch ersuchter Staat an die einschlägige Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte gebunden sind, derzufolge eine Telekommunikationsüberwachung nur zulässig ist, wenn diese zeitlich begrenzt erfolgt, hinreichende Verdachtsmomente betreffend einer schwerwiegenden Straftat vorliegen, eine zügige Löschung nicht benötigter Daten erfolgt und eine unabhängige Kontrollinstanz über die Telekommunikationsüberwachung wacht (EGMR, Urt. v. 18.2.2003 (*Prado Bugallo*), Nr. 58496/00; Grabenwarter, 2008, § 22 Rdn. 34).

Europäische Sicherstellungsanordnung Die sogenannte Europäische Sicherstellungsanordnung (Rahmenbeschluss über die Vollstreckung von Entscheidungen über die Sicherstellung von Vermögensgegenständen oder Beweismitteln in der Europäischen

Union, AblEU 2003 L 196 v. 1.11.2003, S. 45) wird aufgrund der unzureichenden und langsamen Umsetzung in den Mitgliedstaaten von Kritikern wie der Kommission als bloß »virtuell[e]« Regelung bezeichnet. Dies verkennt, welch umfassende Möglichkeiten dieser Rahmenbeschluss, insbesondere in Kombination mit der Europäischen Beweisanordnung (s. sogleich, S. 182) bietet.

Sachen, Schriftstücke oder Daten, die »als beweiserhebliche Gegenstände in einem Strafverfahren« in Betracht kommen, sind auf Aufforderung eines anderen Mitgliedstaats sicherzustellen; hierzu sind auch offene Durchsuchungen – auch bei unverdächtigen Dritten – und Beschlagnahmen vorzunehmen. Höchstpersönliche Bereiche oder vertrauenswürdige Konstellationen sind dabei durch die Europäische Sicherstellungsanordnung nicht gesondert geschützt; der Vollstreckung einer solchen Anordnung können aber Vorrechte des nationalen Rechts – wie sie etwa in Deutschland in § 97 StPO enthalten sind – entgegengehalten werden. Die grundsätzliche Prüfung durch einen Richter entfällt nicht (§ 94 Abs. 1 i.V.m. § 67 IRG), wohl aber die Prüfung der beiderseitigen Strafbarkeit, wenn es sich um ein Listendelikt, wie etwa »Kinderpornografie«, »Betrugsdelikte« oder »Cyberkriminalität« (s. hierzu oben S. 180), handelt.

Die Sicherstellung ist dabei nur eine vorläufige, so dass sich die spätere Übergabe der Beweismittel zunächst nach herkömmlichem Rechtshilferecht richtet. Dabei gilt allerdings, dass die Prüfung der beiderseitigen Strafbarkeit entfällt – allerdings nur, wenn es sich um ein solches Listendelikt handelt sowie die dem Täter zur Last gelegte Tat eine Höchststrafe von mindestens drei Jahren vorsieht. Dies ist nach deutschem Recht etwa bei der Verbreitung von Kinderpornographie gegeben, aber auch bei Betrug und bei schweren Fällen der Computersabotage. Auf Beweismittel, die zur Verfolgung schwerer Cyberkriminalität erforderlich sind, kann durch die Europäische Sicherstellungsanordnung hinreichend schnell und effektiv zugegriffen werden, wenn auch die Akzeptanz dieser Sicherstellungsanordnung in der Praxis noch verbesserungsfähig ist.

Europäische Beweisanordnung Einen noch weitergehenden Zugriff auf in einem anderen Staat befindliche Beweismittel soll nunmehr die – in Deutschland bislang nicht umgesetzte – Europäische Beweisanordnung ermöglichen. Im Gegensatz zur Sicherstellungsanordnung, die einen zu starken Bezug zu Vermögensgegenständen aufwies, soll ein einstufiges, schnelles Verfahren geschaffen werden, um extraterritorial auf Beweismittel zugreifen zu können. Explizit erlaubt sollen hierfür auch Eingriffsmaßnahmen wie Durchsuchungen und Beschlagnahmen sein, ausgenommen sind allerdings verdeckte Überwachungsmaßnahmen einschließlich Telekommunikationsüberwachung und Überwachung von Kontenbewegungen.

Die Europäische Beweisanordnung verzichtet bei den Listendelikten auf eine Prüfung der beiderseitigen Strafbarkeit, wobei Deutschland allerdings eine Ausnahmeregelung zuteil wird. Neuartig ist, dass die Europäische Beweisanordnung erstmals explizite Vorgaben betreffend die Verhältnismäßigkeit (Art. 7) und auch einen Versagungsgrund enthält,

sofern die verfahrensgegenständliche Tat »zum großen oder zu einem wesentlichen Teil« im Hoheitsgebiet des Vollstreckungsstaates begangen wurde. Hierdurch soll ein *Primat des Territorialitätsprinzips* gewahrt werden, dass also an erster Stelle derjenige Staat zur Verfolgung einer Straftat berufen ist, auf dessen Staatsgebiet gehandelt oder die Veränderung in der Außenwelt eingetreten ist.

Europäische Ermittlungsanordnung Es kann allerdings durchaus angezweifelt werden, ob die Europäische Beweisanordnung überhaupt praktische Relevanz erlangen wird: Bereits seit kurz nach deren Inkrafttreten wird deren Ersetzung durch eine umfassende Europäische Ermittlungsanordnung diskutiert, die so weit wie möglich alle Arten von Beweismitteln erfassen und die Verweigerungsgründe so weit wie möglich begrenzen soll.

Vieles bezüglich einer Initiative einer Gruppe von Mitgliedstaaten für eine solche Europäische Ermittlungsanordnung ist noch im Fluss; auch aus diesem Grund kann an dieser Stelle nur auf zwei grundsätzliche Aspekte hingewiesen werden:

Erstens ist eine derartige Europäische Ermittlungsanordnung verfrüht. Die Notwendigkeit einer solchen Maßnahme der Europäischen Union konnte bislang nicht hinreichend dargelegt werden, zumal die Umsetzungsfrist der Europäischen Beweisanordnung erst soeben abgelaufen ist und es angesichts der Rechtsunsicherheit nur zu verständlich ist, dass diese auch in Deutschland noch nicht umgesetzt wurde.

Zweitens soll sich die Europäische Ermittlungsanordnung auf einen bunten Strauß von Ermittlungsmaßnahmen erstrecken und so auch verdeckte Ermittlungen sowie – unter Umständen – auch eine verdeckte Telekommunikationsüberwachung erlauben. Bei solch grundrechtssensiblen Maßnahmen ist höchste Vorsicht geboten, um die Verhältnismäßigkeit zu wahren und grundrechtssensible Bereiche sowie Drittinteressen adäquat zu schützen. Bislang sehen die Entwürfe hier nur ein unzureichend austariertes System an Anordnungsvoraussetzungen und Ablehnungsgründen vor. Daher ist es durchaus zu begrüßen, dass die Ablehnungsgründe nunmehr nach der Schwere der Grundrechtseingriffe differenziert werden sollen; bei verdeckten Ermittlungsmaßnahmen erscheint allerdings zusätzlich eine Reziprozität geboten, also eine Prüfung, ob dieselbe Ermittlungsmaßnahme auch in einem vergleichbaren nationalen Strafverfahren angeordnet würde.

Datenaustausch, Gemeinsame Ermittlungsgruppen und Kontaktstellen Ebenfalls nicht zu unterschätzen sind Maßnahmen der Europäischen Union, die durch die Schaffung von gemeinsamen Ermittlungsgruppen und durch Förderung von Spontanermittlungen dazu beitragen, parallele Ermittlungen in verschiedenen Mitgliedstaaten zu fördern. Dabei ist aber auf die grundsätzlichen Bedenken an solchen Parallelermittlungen hinzuweisen, die von unzureichender justizieller Kontrolle bis hin zur Gefahr eines *forum shopping* und einer Umgehung der Sicherungsmechanismen des Rechtshilferechts reichen. Allerdings

kann durch die Beteiligung innerstaatlicher Akteure bei solchen Parallelermittlungen und gemeinsamen Ermittlungsgruppen das Missbrauchspotential reduziert werden, dass etwa eine transnationale Beweiserhebung nur zum Schein eine Strafverfolgung, in Wirklichkeit aber Wirtschaftsspionage bezweckt.

Vorbehaltlos zu unterstützen ist hingegen ein Aspekt des Vorschlags für eine Richtlinie über Angriffe auf Informationssysteme (s. zu diesem Vorschlag bereits oben 8.3.2., S. 159), demzufolge das bestehende 24/7-Netzwerk von Kontaktstellen gestärkt werden soll und für die Erledigung dringender Ersuchen eine Frist von acht Stunden vorgesehen ist. Je schneller auf diesem Wege eine vorläufige Sicherung von Beweismitteln bewerkstelligt werden kann, desto eher kann auf missbrauchsanfälligere Lösungen – sei es die Gestattung eines extraterritorialen Zugriffs auf Beweismittel, sei es eine Europäische Ermittlungsanordnung – verzichtet werden.

Koordinierung

Europol Die polizeiliche Koordinierung – insbesondere in Fällen von Parallelermittlungen – übernimmt das Europäische Polizeiamt (Europol). Hierzu stehen Europol umfangreiche Möglichkeiten zum Informationsaustausch zur Verfügung, ohne dass aber Europol eigene Ermittlungs- oder Exekutivbefugnisse übertragen wären. Allerdings ist Europol befugt, Mitgliedstaaten dazu aufzufordern, Ermittlungen aufzunehmen, und kann sich an gemeinsamen Ermittlungsgruppen beteiligen.

Eurojust; Europäische Staatsanwaltschaft Eurojust stellt die justizielle Ergänzung zu Europol dar, und unterstützt bei transnationalen Sachverhalten die justizielle Zusammenarbeit der beteiligten nationalen Akteure. Zudem wird Eurojust im Rahmen der Vermeidung von Kompetenzkonflikten tätig.

Primärrechtlich zwar vorgesehen, aber noch nicht sekundärrechtlich umgesetzt sind Befugnisse von Eurojust, strafrechtliche Ermittlungs- bzw. Verfolgungsmaßnahmen zu initiieren und auch – mit Bindungswirkung für die Mitgliedstaaten – zu koordinieren, oder auch Kompetenzkonflikte bindend zu entscheiden (vgl. zu alledem Art. 85 Abs. 1 UAbs. 2 AEUV).

Ferner kann in Zukunft Eurojust durch ein besonderes Verfahren zu einer Europäischen Staatsanwaltschaft aufgewertet werden. Zunächst ist deren Aufgabengebiet begrenzt auf die Verfolgung von Delikten zum Nachteil der finanziellen Interessen der EU – insbesondere Subventionsbetrug. Erste Anzeichen sprechen aber bereits jetzt dafür, dass zumindest manche Mitgliedstaaten es unterstützen würden, die Europäische Staatsanwaltschaft – oder auch ein aufgewertetes Eurojust – mit der Verfolgung und auch Anklage anderer Delikte zu betrauen, etwa der intrinsisch transnationalen Cyberkriminalität. Ein solches Projekt wirft jedoch eine Fülle von verfassungs-, europa- und strafrechtlichen Folgeproblemen auf, die an dieser Stelle nicht vertieft behandelt werden können.

Europäisches Justizielles Netz Zuletzt sei auf das an Eurojust angegliederte Europäische Justizielle Netz (EJN) hingewiesen, welches den Informationsaustausch und die Kooperation zwischen den Mitgliedstaaten dadurch fördern soll, dass den Justizbehörden Ansprechpartner in anderen Mitgliedstaaten zur Seite gestellt werden. Im Gegensatz zur vertikalen Koordinierung durch Eurojust liegt dem EJN ein (horizontaler) Netzwerkgedanke zugrunde; mit eigenen Befugnissen ist das EJN nicht ausgestattet.

Fazit

Die Europäisierung des Strafverfahrensrechts ist aus Sicht der Strafverfolgungspraxis eine Erfolgsgeschichte: Durch vielfältige Regelungen ist nicht nur der Zugriff auf Beschuldigte erleichtert, die sich im europäischen Ausland befinden, sondern auch der Zugriff auf Beweismittel, die zur Verfolgung von Cyberkriminalität erforderlich sind. Das Rechtshilfeübereinkommen aus 2000 enthält flexible, weit reichende Regelungen zu einer raschen Anordnung einer Telekommunikationsüberwachung, mittels einer Europäischen Sicherstellungsanordnung können Daten rasch in anderen Mitgliedstaaten gesichert werden, um sie sodann – sei es nach klassischem Rechtshilferecht, sei es zukünftig mit einer Europäischen Beweisanordnung – zu transferieren und so für ein Strafverfahren zu nutzen.

Der Datenaustausch zwischen den Kriminaljustizsystemen bei Parallelermittlungen, in Gemeinsamen Ermittlungsgruppen und über die verschiedenen Kontaktstellennetze und über die Koordinierungsstellen Europol und Eurojust bietet der Praxis eine weitere Möglichkeit, die intrinsisch transnationale Cyberkriminalität in mehreren Ländern effektiv zu verfolgen.

Gleichwohl sind Schwachstellen zu benennen: Erstens ist dies die fortdauernde Skepsis, bisweilen auch Unsicherheit in der Praxis, die neuartigen Instrumentarien auch zu gebrauchen; Parallelermittlungen sind dabei aus Sicht der Strafverfolgungsbehörden deutlich einfacher und effektiver als das immer noch mühsame Rechtshilferecht. Zweitens ist eine Fragmentierung des Rechtshilferechts entstanden, da etliche Regelungsinstrumente nur in manchen Mitgliedstaaten und bisweilen auch nur unzureichend umgesetzt sind. Daher besteht eine gewisse Notwendigkeit, auf eine Vereinheitlichung und Effektivierung des bestehenden Rechtsrahmens hinzuwirken. Ein weitergehender Aktionismus, wie er etwa der Europäischen Ermittlungsanordnung zugrunde liegt, ist hingegen verfrüht.

Schließlich ist es auch auf europäischer Ebene notwendig, die Verhältnismäßigkeit auch im Strafprozessrecht und im Rechtshilferecht zu wahren, und dabei auch nach der unterschiedlichen Grundrechtssensibilität der einzelnen Ermittlungsmaßnahmen zu differenzieren.

8.6. Zusammenfassung

Dieses Kapitel beleuchtete die transnationale Dimension bei der Verfolgung von Cyberkriminalität. Wir haben zunächst aufgezeigt, dass es im Bereich der Internet-Beschwerdestellen und bei der Bekämpfung von Botnetzen zahlreiche Beispiele für gelungene Kooperationen gibt, die jenseits einer formal-juristischen Zusammenarbeit liegen.

Rechtlich ermöglicht die *Cybercrime-Konvention* des Europarats eine weit reichende internationale Harmonisierung der Straftatbestände und eine Vermeidung von Strafbarkeitslücken. Ziel weiterer Maßnahmen auf diesem Gebiet sollte sein, die Umsetzung und Wirksamkeit dieses Instruments zu stärken. Wenig zielführend sind hingegen neue Strafvorschriften oder auch eine Erhöhung der Mindeststrafrahmen.

Da jegliche Kommunikation im Internet zwischen Anfangs- und Endpunkten stattfindet, die sich einem bestimmten physischen Ort und daher einem Staatsgebiet zuordnen lassen, lässt sich ohne Weiteres mindestens ein Staat finden, dessen Strafrechtsordnung auf jede nur denkbare Internet-relevante Verhaltensweise Anwendung findet. Aufgrund der international zu verzeichnenden Tendenz zu extraterritorialer Anwendung des Strafrechts führt dies zu Kompetenzkonflikten. Diese sind besonders dann problematisch, wenn eine Rechtsordnung ein Verhalten unter Strafe stellt, und eine andere Rechtsordnung dasselbe Verhalten entweder verfassungsrechtlich schützt oder sogar gebietet.

Der Zugriff auf im Ausland befindliche Beweismittel ist auf verschiedenste Arten möglich: erstens *faktisch*, wenn auch rechtlich zu missbilligen aufgrund einer weit reichenden Kooperationsbereitschaft international tätiger Dienstleister, zweitens *rechtlich* durch Parallelermittlungen, Datenaustausch und Kontaktstellennetze – insbesondere das G8-Kontaktstellennetz ist hier zu nennen –, drittens durch klassische und moderne Rechtshilfeinstrumente. Besonders hervorzuheben ist hierbei die Möglichkeit zu einer schnellen, vorläufigen Sicherung von Daten, etwa durch die Europäische Sicherstellungsanordnung. Ein Direktzugriff und eine zu weit gehende Anerkennung ausländischer Entscheidungen ohne Missbrauchsprüfungen, wie sie derzeit auf europäischer Ebene diskutiert werden, drohen aber Kollateralschäden mit sich zu bringen, sei es für die Beschuldigtenrechte, sei es auch für Drittbetroffene wie Wirtschaftsunternehmen, die ein legitimes Geheimhaltungsinteresse insbesondere gegenüber ausländischen Stellen haben, um weniger Angriffsfläche für Wirtschaftsspionage zu bieten.

9. Handlungsempfehlungen: Neun Thesen

1. Ein sicheres Internet beginnt mit jedem Einzelnen.

Eine Vielzahl von Gefahren im Internet entstehen durch unzureichend geschützte Rechner, durch unsicheres Verhalten im Netz und durch unsicheres Verhalten an lokalen Arbeitsplatzrechnern. Das gilt selbst dann, wenn auf einem lokalen Computer (vermeintlich) keine »interessanten Daten« für Cyberkriminelle zu finden sein mögen, denn die feindliche Übernahme dieses Rechners und die Einbindung dieses Rechners in ein Botnetz ist ein wesentliches Werkzeug für die Begehung von Cyberkriminalität. Dieses Risiko – und die tatsächlichen Gefahren durch Cyberkriminalität – gilt es weitaus besser als bisher zu vermitteln.

Es ist für jeden Einzelnen dringend erforderlich, auf die Sicherheit seines Arbeitsplatzrechners, seiner privaten Computer und neuerdings auch seiner Smartphones zu achten. Hierzu dient unter anderem die häufig gepredigte Verwendung von Antiviren- und Sicherheitssoftware, die rasche Aktualisierung von Software, sobald Sicherheitslücken festgestellt wurden, und die Verwendung von verschiedenen, sicheren Passwörtern. Man sollte Software aus zweifelhaften Quellen sowie fremde USB-Sticks oder sonstige Datenträger nur zurückhaltend verwenden. Schließlich mag es auch nützlich sein, auf weniger häufig genutzte Hardware, Betriebssysteme und sonstige Software zurückzugreifen, denn je unterschiedlicher die Systeme, desto schwieriger wird es für Angreifer, eine Vielzahl von Computern erfolgreich anzugreifen.

Zudem sei jedem empfohlen, Auffälligkeiten und – erfolgreiche – Angriffe durch Cyberkriminelle auch zu melden. Hierfür gilt es geeignete Plattformen und Kommunikationskanäle zu entwickeln, so dass rasch ermittlungsrelevante Datenspuren ausgewertet werden können, aber auch, dass durch entsprechende empirische Forschungen ein verlässlicheres Bild der Cyberkriminalität gewonnen werden kann. Bei alledem ist auf die vertrauliche Bearbeitung solcher Meldungen zu achten, damit nicht Opfer – insbesondere Unternehmen – sogleich in die öffentliche Kritik geraten oder sogar von Nachahmungstätern erneut angegriffen werden.

Dieselben Grundsätze gelten auch für Behörden und Unternehmen: Durch automatisierte Sicherheitsaktualisierungen, durch *best practises* im Umgang mit informationstechnischen Systemen, durch die Beschäftigung von oder die externe Unterstützung durch IT-Sicherheitsexperten und auch durch eine ausreichende Schulung der Mitarbeiter lassen sich die Angriffspotentiale reduzieren. Zudem sollten Behörden und Unternehmen in Erwägung ziehen, sensible Daten komplett von Rechnern fernzuhalten, die auch mit dem Internet verbunden sind: So könnte etwa eine Arztpraxis die Patientendaten in einem lokalen Netzwerk zur Verfügung stellen; ein weiterer Rechner, der nicht an das

lokale Netzwerk angeschlossen ist, mag dann für die Internetnutzung dienen. Die zu beobachtenden Trends – etwa im Zuge der »elektronischen Gesundheitskarte« – sind jedoch gegenläufig, hin zu mehr Vernetzung über das Internet, und damit auch zu mehr Angriffsflächen.

Unterstützung zur Absicherung von Rechnern von Privatpersonen, von Behörden und Unternehmen bieten dabei unter anderem die CERTs und das Bundesamt für Sicherheit in der Informationstechnologie. Auch ein »nationales Cyber-Abwehrzentrum« und *public-private-partnerships* hin zu einem Austausch von Erfahrungen und Hinweisen auf aktuelle Bedrohungslagen sind zu begrüßen.

2. Es fehlen verlässliche kriminologische Daten über die Bedrohungslage durch Cyberkriminalität in Deutschland und Europa.

Cyberkriminalität ist in der Regel ökonomisch motivierte Kriminalität. Sie reicht dabei von der kostenlosen Nutzung urheberrechtlich geschützter Musik und Filme über Betrügereien bis hin zur Verwertung fremder Betriebsgeheimnisse durch Industriespionage. Hinzu treten die Verbreitung von kinderpornographischen und sonstigen verwerflichen, inkriminierten Schriften, aber auch Cybermobbing und -stalking sowie die Nutzung des Internets zur Kommunikation unter Terroristen. Cyberkriminalität ist aber *nicht* zur Gewaltkriminalität zu zählen und auch nicht mit dieser vergleichbar; Fälle schwerster Kriminalität finden nicht im Internet statt, sondern praktisch nur leichtere bis mittlere Kriminalitätsbereiche.

Ökonomisch motivierte Cyberkriminalität zeichnet sich aus durch einen hohen Grad an Organisation und an einer ausdifferenzierten Arbeitsteilung. Dabei sind die Kooperationen allerdings wenig hierarchisch und zum Teil nur sehr kurzfristig. Sie ist damit nicht gänzlich mit der klassischen »organisierten Kriminalität« vergleichbar; zudem gibt es keine verlässlichen Erkenntnisse darüber, dass es engere Verbindungen zwischen der traditionellen organisierten Kriminalität (etwa im Bereich Drogen- und Menschenhandel) und der digitalen Schattenwirtschaft gibt.

Eine Betrachtung des Umfangs und der Schäden der Cyberkriminalität wird durch verschiedene Faktoren erschwert, insbesondere durch das nur unzureichend analysierte Dunkelfeld. Wir empfehlen daher, umfangreiche und vertiefte empirisch-kriminologische Studien durchzuführen, die etwa auf der Grundlage des BCS (Allen et al., 2005; Wilson et al., 2006) fußen können. Doch auch betreffend der Verfolgung von Cyberkriminalität überwiegen anekdotische Darstellungen, etwa für die Notwendigkeit der Vorratsdatenspeicherung von Verbindungsdaten (vgl. etwa in KOM [2010] 385 endg. v. 20.7.2010). Eine evidenzbasierte Kriminalpolitik erfordert eine hinreichend verlässliche Datengrundlage, die dringend zu schaffen ist.

3. Soweit der technische Schutz reicht, ist rechtlicher Schutz nicht nötig.

Wo sich Angriffsmöglichkeiten für Cyberkriminelle reduzieren oder gänzlich vermeiden lassen, lässt sich auch Cyberkriminalität reduzieren oder ganz vermeiden. Daher ist es dringend erforderlich, den technischen Schutz von Hard- und insbesondere Software zu erhöhen. So reduziert der standardmäßige Einsatz von starker Kryptografie über die gesamte Kommunikation hinweg (*end-to-end*) die Gefahren, dass sensible Daten von Nachrichtenmittlern ausgelesen werden können. So dienen Restriktionen zum Zugriff auf Daten, ein technisch implementiertes »Vier-Augen-Prinzip« und weitere Maßnahmen dazu, die Risiken von Konkurrenzausspähung und Wirtschaftsspionage zu reduzieren.

Zudem ist die Diversität an Soft- und Hardware zu fördern: Ähnlich wie in der Biologie ist eine Monokultur anfälliger für Schädlinge, die sich auf technisch gleichartigen Systemen weitaus schneller verbreiten können als auf technisch unterschiedlichen Systemen. Zugleich erscheint es notwendig, Virtualisierungstechniken skeptischer als bisher zu betrachten: Nicht nur der Datenschutz lässt sich dabei schlechter bewerkstelligen, sondern es bieten sich auch weitaus mehr kriminelle Möglichkeiten. Mehr Nähe und mehr Bezug zur Hardware mag daher durchaus vorteilhaft sein, wobei dies nicht auf Kosten der soeben genannten Diversität gehen darf: So ist eine Abschottung von Hardware gegen die Verwendung alternativer Software zu vermeiden, denn diese Abschottung erhöht die Anfälligkeit der Informationstechnologie, anstatt sie zu minimieren.

Dennoch: der technische Schutz kann nicht perfekt sein, insbesondere nicht gegen gezielte Angriffe. Daher ist auch stets in Erwägung zu ziehen, das Internet nur als das zu betrachten, wofür es geschaffen wurde: als Raum für die interpersonale Kommunikation. Weitaus größere Gefahren drohen bei der Verwendung des Internets für die Prozesssteuerung oder zur Übermittlung sensibler Daten. Die Prozesssteuerung hochsensibler Systeme – sei es etwa in Flugzeugen oder bei Industrieanlagen – sollte daher nach Möglichkeit keine Verbindung mit dem Internet aufweisen. Ebenso ist kritisch zu hinterfragen, ob mehr internetbasierte Vernetzung – etwa im Gesundheitssektor, aber auch zur Steuerung jeglicher Geräte im Haushalt – wirklich vorteilhaft ist. Aus technischer Sicht spricht hier viel für eine komplette physische Trennung von bereichsspezifischen Netzwerken, etwa im Banken-, Gesundheits-, und Infrastruktursektor, aber auch in der Exekutive (»Entnetzung«; Gaycken & Karger, 2011). Weniger Vernetzung und voneinander getrennte Vernetzung ist *technisch* sicherer, dabei aber auch kostspieliger.

Insgesamt sind hoch entwickelte Gesellschaften sehr viel mehr auf sichere Informationstechnik angewiesen als die organisierte Kriminalität. Darum sollte der Staat technische Entwicklungen hin zu mehr Sicherheit, also etwa die umfassende Einführung starker Kryptographie bei der Kommunikation, aktiv unterstützen (Pfitzmann, 2007).

4. Das Internet ist kein rechtsfreier Raum.

Das Internet ist kein eigener Raum, sondern nur ein Kommunikationsnetz zwischen Endpunkten, die sich im physischen Raum befinden. Diese wiederum befinden sich in den verschiedenen Staaten der Welt, so dass stets ein konkreter Anknüpfungspunkt, ein Handlungsort, gegeben ist, wenn ein Krimineller über das Internet eine Straftat begeht. Daher findet auch stets zumindest eine Strafrechtsordnung Anwendung und kann diesen Straftäter zur Verantwortung ziehen – zumeist aber mehrere, da Staaten ihre Strafgewalt auch auf Sachverhalte im Ausland ausweiten.

International ist eine Harmonisierung der Straftatbestände zu verzeichnen: Jedenfalls die erheblichen Erscheinungsformen der Cyberkriminalität werden daher von immer mehr Staaten unter Kriminalstrafe gestellt. Von maßgeblichem Einfluss ist dabei die Cybercrime-Konvention des Europarats, der sich alle Staaten anschließen können. Anpassungsbedarf dieser Konvention – oder eine UN-Konvention gegen Cyberkriminalität – ist nicht gegeben, wohl aber ein internationaler politischer Konsens, gegen erhebliche Erscheinungsformen der Cyberkriminalität vorzugehen und Staaten, die sich dem nicht oder nur unzureichend anschließen, zur Mitwirkung zu überzeugen.

Schwierigkeiten entstehen aber dadurch, dass auf manche Sachverhalte mehr als eine (Straf-)Rechtsordnung Anwendung findet. Soweit dies erhebliche Kriminalitätsformen – wie etwa die Verbreitung kinderpornographischer Schriften, *Phishing* oder schwerwiegende Urheberrechtsverletzungen – betrifft, sind die praktischen und rechtlichen Schwierigkeiten noch überschaubar. Anderes gilt aber in Bereichen, in denen unterschiedliche Wertvorstellungen aufeinander treffen – etwa das Glücksspiel oder die Abwägung Daten- und Geheimnisschutz gegen öffentliches Interesse betreffend. Hier sind neuartige Lösungsansätze zu diskutieren, etwa ein »Herkunftslandprinzip«, demzufolge alleine diejenige Rechtsordnung entscheidet, in der ein Akteur handelt. Ferner ist für sensible Bereiche – etwa dem Journalismus und der IT-Sicherheitsforschung – eine internationale Straffreistellung (*safe harbour*) zu schaffen, so dass sich etwa regierungskritische, insbesondere investigativ tätige Journalisten zumindest innerhalb Europas vor einer extensiven Strafverfolgung sicher fühlen können.

5. Das deutsche Strafrecht ist gut aufgestellt zur Verfolgung von Cyberkriminalität.

Die im deutschen Strafgesetzbuch und in weiteren Gesetzen zu findenden Strafbestimmungen sind weitestgehend ausreichend und adäquat zur Verfolgung von Cyberkriminalität. Nahezu jedes strafwürdige Verhalten unterfällt mindestens einem Straftatbestand und kann daher zu einem Strafverfahren gegen den oder die Täter führen. Auch die Strafrahmen sind ausreichend, zumal diese Strafrahmen in der öffentlichen und auch politischen Diskussion ohnehin überbewertet werden: Eine Erhöhung des gesetzlichen Strafrahmens hat keinerlei nennenswerte abschreckende Wirkung auf potentielle Täter.

Gleichwohl hat unsere Untersuchung gezeigt, dass ein gewisser Änderungsbedarf des materiellen Strafrechts, also der Tatbestände des Strafgesetzbuches, gegeben ist. Hervorzuheben sind drei Aspekte:

- Zum Schutz der Kinder und Jugendlichen ist der Erwerb von kinder- und jugendpornographischen Schriften unter Strafe zu stellen, um die ökonomischen Anreize zur Begehung solch verwerflicher Taten zu minimieren (s. oben 7.3.1., S. 90). Zugleich sind Streamingdienste auf Versender- und Empfängerseite besser zu erfassen (s. oben 7.3.1., S. 90). Das so genannte »Grooming«, also die sexuell motivierte Kontaktaufnahme von Pädokriminellen zu Kindern, ist entgegen einer landläufigen Meinung bereits weitgehend unter Strafe gestellt, nur in einem Randbereich – der Kontaktaufnahme via »Chats« – erscheint eine Anpassung der Gesetzeslage notwendig (s. oben 7.3.1., S. 92).

- Zur konsistenten Verfolgung des »Skimming«, dem Auslesen von Bankkarten durch Manipulation von Geldautomaten und Türöffnern, sowie des »Phishing«, dem Abgreifen oder Erschleichen von Kreditkarten- oder Zugangsdaten, ist eine geringfügige Ausweitung des Straftatbestands des »Vorbereitens des Computerbetrugs« angezeigt (s. oben 7.3.4., S. 107).

- Schließlich ist zum effektiven Schutz der Presse, aber auch der Wissenschaft und Forschung eine entsprechende Klarstellung in manchen Tatbeständen geboten, da sich bloß nachträglicher Rechtsschutz – etwa durch das Bundesverfassungsgericht im »Cicero«-Urteil (BVerfGE 117, 244) – als nicht ausreichend wirksam gezeigt hat. Daher regen wir an, den ohnehin diskutierten Gesetzentwurf zur Stärkung der Pressefreiheit auch auf die Veröffentlichung von Missständen in der Privatwirtschaft zu erstrecken (7.3.2., S. 97) und zudem explizite Straffreistellungsklauseln bei den Vorbereitungsdelikten für Belange der Wissenschaft und Forschung einzufügen (s. oben 7.3.6., S. 118).

6. Die forensischen und praktischen Möglichkeiten zur Verfolgung von Cyberkriminalität werden unterschätzt; sie gilt es fruchtbar zu machen.

Die Erfahrung zeigt: Auch Cyberkriminelle machen Fehler. Sie hinterlassen also unvermeidlich Spuren ihrer Taten. Im Gegensatz zu Spuren in der physischen Welt sind dies aber *digitale* Spuren. Im Vergleich zu physischen Spuren gibt es beim Umgang mit digitalen Spuren sowohl bei den Strafverfolgungsbehörden als auch bei den Gerichten kaum Erfahrungen. Aber die bisherigen Erkenntnisse der digitalen Forensik lassen erahnen, dass es eine Vielzahl von Spurenquellen gibt, die noch nicht hinreichend erschlossen wurden.

Insbesondere gilt dies auch für Spuren, die heute regelmäßig noch außerhalb des Zugriffs der Strafverfolgungsbehörden liegen, wie etwa verschlüsselte Festplatten oder verschlüsselte Datencontainer. Mit verschiedenen technischen Kniffen wie etwa einer Hauptspeicheranalyse von Systemen im Ruhezustand wird man in Zukunft auch Zugang zu diesen Daten erhalten können. Dafür ist ein offener Zugriff, also etwa im Rahmen einer Hausdurchsuchung, vollkommen ausreichend.

Der verdeckte Zugriff auf ein informationstechnisches System birgt aus forensischer Sicht viele Probleme und besitzt auch aufgrund der Universalität von Software eine enorme Eingriffstiefe. Er ist aus Sicht der Strafverfolgungsbehörden aufgrund seiner vermeintlichen Einfachheit jedoch außerordenlich attraktiv. Allerdings sollten erst dann die Möglichkeiten eines verdeckten Zugriffs näher in Betracht gezogen werden, wenn die Grenzen dessen erreicht sind, was man durch eine offene und nachprüfbare forensische Untersuchung in Erfahrung bringen kann.

Um den Stand des Wissens im Bereich der digitalen Forensik auszubauen, muss offene und auch offensive Forschung im Bereich der Cyberkriminalität gefördert werden. Gerade offensive Forschung, etwa in den Bereichen Hacking und Reverse Engineering, ist in Deutschland an den Hochschulen unterentwickelt. Obwohl es national eine sehr aktive »Hacker-Szene« gibt, wurden wesentliche technische Erkenntnisse im Bereich der Cyberkriminalität von Wissenschaftlern aus dem Ausland publiziert. Die in Deutschland unzweifelhaft vorhandene junge technische Expertise im »Hacking« muss für die offene Forschung an den Hochschulen und in Unternehmen gewonnen werden. Wenige zusätzliche, außertariflich bezahlte Technikerstellen bei der Polizei reichen hierfür nicht aus. Einerseits müssen sich die Strafverfolgungsbehörden, insbesondere Bundeskriminalamt und die Landeskriminalämter, stärker der Kooperation mit den Hochschulen und der Industrie öffnen. Andererseits müssen die Hochschulen bereit sein, sich stärker anwendungsbezogenen Forschungsthemen zuzuwenden.

Zur langfristigen Sicherung möglichst hoher Standards bei Ermittlungen im Cyberspace benötigen wir ein flächendeckendes Angebot wissenschaftlich orientierter und berufsbegleitender Ausbildungsprogramme im Bereich der digitalen Forensik. Diesbezüglich sei einerseits auf die verschiedenen Programme der EU – etwa *Falcone*, *AGIS* und *ISEC* – verwiesen, andererseits auf die Studiengänge in diesem Gebiet, etwa am University College Dublin oder an der Hochschule Albstadt-Sigmaringen.

Eine verbesserte Nutzung der Ermittlungsmöglichkeiten bietet zur Verfolgung von Cyberkriminalität ein hohes Potential. Schließlich ist Cyberkriminalität vor allem ökonomisch motivierte und lässt sich daher weitaus besser minimieren als zwangsgesteuerte, triebgesteuerte oder ideologisch motivierte Kriminalität. Eine verbesserte Nutzung der forensischen Möglichkeiten erhöht einerseits den technischen Aufwand, den Cyberkriminelle selbst betreiben müssen. Andererseits erhöht sie auch die von den Cyberkriminellen sehr genau wahrgenommene Überführungswahrscheinlichkeit (Kshetri, 2010, Kapitel 2.6).

Schließlich ist es notwendig, illegale Zahlungsströme und Geldwäsche zu unterbinden. Dies scheint wie in anderen Bereichen der Kriminalität ein effektives Mittel: Da Cyberkriminelle nunmehr erhebliche Schwierigkeiten haben, ihre Gelder zu waschen (Florêncio & Herley, 2010), reduzieren sich auch die ökonomischen Anreize, solche Straftaten zu begehen.

7. Die prozessualen Möglichkeiten zur Verfolgung von Cyberkriminalität sind besser als ihr Ruf.

Auch das deutsche Strafprozessrecht ist gut aufgestellt zur Verfolgung von Cyberkriminalität. Insbesondere die ökonomisch motivierte Kriminalität lässt sich nicht nur durch Auswertung von Informationstechnologie nachverfolgen und gerichtsfest beweisen, sondern auch durch eine Auswertung der Zahlungsströme. Zwar reduzieren anonyme Zahlungsdienstleister dabei die Chancen, *alle* Beteiligten zur Rechenschaft zu ziehen, doch sinken bereits durch die Verfolgung der Finanzagenten die Anreize zur Begehung von Cyberkriminalität. Solche ökonomischen, direkten und indirekten Ansätze zur Minimierung von Cyberkriminalität gilt es auch weiterhin zu nutzen (vgl. auch Kshetri, 2010, Kapitel 2.6).

Der Zugriff auf und die Auswertung von Daten ist den Straverfolgungsbehörden in weit reichendem Umfang gestattet. Deren Möglichkeiten reichen von einer offenen Durchsuchung und Beschlagnahme über die verdeckte Überwachung der Telekommunikation hin zur Verpflichtung von unverdächtigen Dritten, jedenfalls auf gerichtliche Anforderung (vgl. 7.5.1., S. 135) Daten preiszugeben und nötigenfalls auch zu entschlüsseln. Dabei sind die faktischen Zugriffsmöglichkeiten noch größer als die rechtlichen Pflichten, denn international tätige Internetdienstleister kooperieren auf freiwilliger Basis in großem Umfang mit den Strafverfolgungsbehörden. Hier ist eine verstärkte rechtliche Absicherung zur Wahrung von Drittinteressen und zum Schutz gegen missbräuchliche Ausspähung von Daten geboten.

Dennoch bestätigten sich in dieser Untersuchung auch Schwächen des Strafprozessrechts, von denen drei herausgegriffen werden sollen:

- Die Zuordnung von den Ermittlungsbehörden bekannten, dynamisch vergebenen IP-Adressen zu Name und Anschrift der Kunden (Bestandsdatenabfrage) ist wenigstens für eine gewisse Zeit, aber nicht notwendigerweise für 6 Monate zu ermöglichen (s. oben 7.5.3., S. 148).
- Der Zugriff auf E-Mail-Kommunikation ist je nach Übertragungsstadium rechtlich anders zu handhaben, was erstens aus technischer Sicht arbiträr wirkt und zweitens praktische Schwierigkeiten aufwirft. Eine Vereinheitlichung der Zugriffsmöglichkeiten durch eine Änderung der Regelungen über die Postbeschlagnahme ist daher

anzuraten, zumal die elektronische Post vermehrt zum Ersatz für die herkömmliche, physische Post wird (s. oben 7.5.2., S. 142).

- Schließlich stellt die Verschlüsselung von Telekommunikation – etwa von Skype-Telefongesprächen – ein erhebliches rechtliches und auch praktisches Problem dar, wenn diese Verschlüsselung bereits auf dem Computer eines Verdächtigen erfolgt und eine Entschlüsselung zwischen den Endgeräten nicht erfolgen kann. Soweit hier eine Inpflichtnahme der Diensteanbieter scheitert, mag es notwendig werden, eine hinreichend tragfähige Rechtsgrundlage für eine Quellen-Telekommunikationsüberwachung einzuführen, denn diese ist in der Strafprozessordnung bislang nicht zu finden. Dabei sind allerdings rechtliche und technische Vorgaben vorzusehen, die der Eingriffstiefe gerecht werden (s. oben 7.5.2., S. 144).

8. Internationale Kooperationen zur Verfolgung von Cyberkriminalität sind erfolgversprechend.

Flexible internationale Kooperationen zur Verfolgung von Cyberkriminalität sind ein Erfolgsmodell:

Zu nennen sind hier erstens informelle Kooperationen, etwa in Forschungsverbünden zwischen Universitäten und Unternehmen zur besseren Erforschung und technischen Bekämpfung von Schadsoftware, aber auch im Verbund der *European Government CERTs*.

Zweitens sind die Erfolge der Internet-Service-Provider lobend zu erwähnen, die weitaus effektivere Ergebnisse bei der Löschung von »Phishing«-Seiten und von kinderpornographischen Inhalten zeigen als polizeilich initiierte Maßnahmen. Solche Modelle einer Selbstregulierung eines Internets der Bürger und eines Internets der Zivilgesellschaft sind freiheitsschonend und daher stets als mildere Alternative zu staatlichen Eingriffen in Erwägung zu ziehen, zumal eine inhaltsbezogene Regulierung des Internets ohne breite Mitwirkung der technischen Akteure des Internets aussichtslos erscheint.

Drittens ermöglichen es das G8-Kontaktstellennetz und vergleichbare Netzwerke des Europarats und der Europäischen Union, rasch transnational Beweismittel vorläufig zu sichern. Auch wenn der spätere Transfer von Beweismitteln nach dem klassischen Rechtshilferecht einige Zeit in Anspruch nehmen kann, so handelt es sich bei einer vorläufigen Sicherung um eine effektive Maßnahme, da sie der Flüchtigkeit elektronischer Daten entgegenwirkt. Zudem ist auch auf den regen Informationsaustausch zwischen Strafverfolgungsbehörden hinzuweisen, etwa bei Parallelermittlungen oder über Europol und Eurojust. So nützlich diese Möglichkeiten auch derzeit für die Verfolgung von Cyberkriminalität sind, so sind dennoch vertiefte rechtliche Analysen notwendig, ob bei Parallelermittlungen und bei informellem transnationalen Informationsaustausch die Beschuldigtenrechte und die Belange von Drittbetroffenen ausreichend geschützt werden.

9. Die Staatengemeinschaft ist nicht machtlos gegenüber der Cyberkriminalität.

Durch effektive Nutzung der forensischen und praktischen Möglichkeiten zur Verfolgung von Cyberkriminalität, durch die Stärkung informeller und formeller Kooperationen zwischen privaten Akteuren und zwischen Strafverfolgern, und durch eine Harmonisierung der Strafbestimmungen ist es den Staaten möglich, effektiv gegen ökonomisch motivierte Cyberkriminalität und auch gegen weitere Formen der Cyberkriminalität vorzugehen. Im Gegensatz zu etwa Brenner (2009a) sind wir daher nicht der Auffassung, dass der Nationalstaat in Zeiten des Cyberspace um sein Überleben kämpft.

Gänzlich lässt sich aber Cyberkriminalität ebenso wenig ausschließen wie sonstige Kriminalitätsformen. Dies ist auch nicht wünschenswert, da nur eine »Wagniskultur« (vgl. Gerhold, 2010, S. 28) freiheitlich ist; gleichwohl gilt es aber, die Risiken zu minimieren. Eine Rückbesinnung darauf, dass das Internet der interpersonalen Kommunikation dient und dass das diesbezügliche Gefahrenpotential begrenzt und leichter beherrschbar ist, wäre hierzu ein wesentlicher erster Schritt. Wo aber über das Internet Prozesse in Industrieanlagen oder in sicherheitskritischer Infrastruktur gesteuert werden, wo mit dem Internet verbundene Rechner auch für solche Zwecke eingesetzt werden, steigt das mit Cyberkriminalität verbundene Risiko erheblich. Ebenso sind für sensible Daten alternative Kommunikationsnetze in Erwägung zu ziehen, nicht nur im militärischen Bereich, sondern etwa im Gesundheitswesen, im Bankensektor und auch in der Exekutive. Dies würde in einem zweiten Schritt auch verdeutlichen, dass ein immer komplexer werdendes System zugleich auch ein immer weniger überschaubares und zugleich immer größeres Risiko mit sich trägt. Diverse Software, diverse Systeme und auch diverse, voneinander getrennte Netzwerke reduzieren die Gefahren der Cyberkriminalität hingegen in erheblichem Maße.

Zwar mag es sein, dass Staaten in Zeiten des Cyberspace Inhalte – das heißt Meinungsäußerungen, wahre und unwahre Tatsachenbehauptungen, aber auch grausame, schreckliche und verwerfliche Inhalte – mitunter nur schlechter kontrollieren können, ebenso wie den wirtschaftlichen Exklusivitätsanspruch von Urheberrechtsinhabern. Doch auch hier erscheint die wahrgenommene Bedrohungslage eine übertriebene zu sein:

Erstens ist auf einen internationalen Grundkonsens hinzuweisen, etwa bezogen auf die Verwerflichkeit kinderpornographischer Schriften, aber auch bezogen auf die Schädlichkeit evidenter und erheblicher wirtschaftlicher Verstöße etwa des »Phishing«. Je schwerer solche Kriminalitätsformen sind, desto eher ist eine Bereitschaft *aller* relevanten Akteure zu verzeichnen, technisch und rechtlich in maßvoller Weise gegen diese Verstöße vorzugehen.

Zweitens aber ist stets in Erinnerung zu halten, dass ein solches, freies und freiheitliches Internet überlegen ist: Die von Arbeitnehmern, ja von der Gesellschaft geforderte größere

Mobilität und Flexibilität erfordert es, zum Ausgleich umfassende Kommunikationsmöglichkeiten frei von staatlicher Überwachung zu haben. Das Internet und die technischen Möglichkeiten zum freien Meinungs- und Informationsaustausch ermöglichen neuartige Demokratisierungs- und Teilhabeprozesse.

Daher erscheint es notwendig, mit einer solchen Kontrollreduktion über Inhalte umzugehen zu lernen. Das heißt für Staaten und Unternehmen, auf eine veränderte »interessierte Öffentlichkeit« zu reagieren und von sich aus die demokratische Teilhabe zu fördern. Das heißt für Künstler und Unternehmen, adäquate, leicht bedienbare Angebote zum Erwerb urheberrechtlich geschützter Werke anzubieten. Das heißt für Eltern, ihre Kinder im Umgang mit dem Internet, mit sozialen Netzwerken und den Medien angemessen zu erziehen. Und es bedeutet auch, dass die vom Staat vermittelte Werteordnung sich neu orientieren muss: Weg von einer freien »Verfügbarkeit von Daten«, hin zu einer Datensparsamkeit. Der Staat muss seinen Bürgern vorleben, dass Daten schützenswert sind, und dass sparsam mit Daten umzugehen ist. Um dieses den Bürgern zu vermitteln, sollte der Staat selbst mehr Respekt vor den Daten der Bürger zeigen. Respekt zeigen bedeutet hier auch, nicht alle Eingriffe, die denkbar und verfassungsgemäß wären, auch umzusetzen, sondern dem Bürger auch über das verfassungsrechtlich gebotene Minimum hinaus Freiräume und Freiheiten zu belassen.

Literaturverzeichnis

Akerlof, G. A. (1970). The market for lemons: qualitative uncertainty and the market mechanism. *The Quarterly Journal of Economics*, *84*, 488–500.

Albrecht, P.-A. (2005). *Kriminologie: eine Grundlegung zum Strafrecht* (3. Aufl.). München: Beck.

Aleph One. (1996). Smashing the stack for fun and profit. *Phrack Magazine*, *7* (49), File 14.

Allen, J., Forrest, S., Levi, M., Roy, H. & Sutton, M. (2005). *Fraud and technology crimes: findings from the 2002/03 british crime survey and 2003 offending, crime and justice survey*. Home Office. Verfügbar unter http://www.homeoffice.gov.uk/rds/pdfs05/rdsolr3405.pdf (Online Report 34/05)

Ambos, K. (2009). Anmerkung zu EuGH JZ 2009, 466. *JZ*, 468–471.

Arai, Y. (2009). Economic analysis of software patents. *IIP Bulletin*, 92–95.

Aust, S. (2008). *Der Baader-Meinhof-Komplex*. Hamburg: Hoffmann und Campe.

Bächer, P., Kötter, M., Holz, T., Dornseif, M. & Freiling, F. C. (2006). The nepenthes platform: An efficient approach to collect malware. In D. Zamboni & C. Krügel (Hrsg.), *Recent advances in intrusion detection, 9th international symposium, RAID 2006, Hamburg, Germany, September 20-22, 2006, proceedings* (S. 165–184). Berlin: Springer.

Baldus, M. (2008). Der Kernbereich privater Lebensgestaltung – absolut geschützt, aber abwägungsoffen. *JZ*, 218–227.

Bamford, J. (2002). *Body of secrets: anatomy of the ultra-secret National Security Agency*. New York: Anchor Books.

Bandyopadhyay, T., Mookerjee, V. S. & Rao, R. C. (2009). Why IT managers don't go for cyber-insurance products. *Communications of the ACM*, *52*, 68-73.

Bär, W. (2007a). 12. Kapitel. Computerkriminalität. In H.-B. Wabnitz & T. Janovsky (Hrsg.), *Handbuch des Wirtschafts- und Steuerstrafrechts.* München: Beck.

Bär, W. (2007b). Anmerkung zu BGH MMR 2007, 237. *MMR*, 239–242.

Bär, W. (2007c). EDV-Beweissicherung im Strafverfahren bei Computer, Handy, Internet. *DRiZ*, 218–221.

Bär, W. (2007d). *Handbuch zur EDV-Beweissicherung*. Stuttgart: Boorberg.

Baumann, J., Weber, U. & Mitsch, W. (2003). *Strafrecht: Allgemeiner Teil* (11. Aufl.). Bielefeld: Gieseking.

Bayer, U., Habibi, I., Balzarotti, D., Kirda, E. & Kruegel, C. (2009). A view on current malware behaviors. In *2nd USENIX workshop on large-scale exploits and emergent threats (LEET).* Berkeley: USENIX Association.

Beck, S. (2009). Internetbeleidigung de lege lata und de lege ferenda. Strafrechtliche Aspekte des »spickmich«-Urteils. *MMR*, 736–740.

Becker, C. & Meinicke, D. (2011). Die sog. Quellen-TKÜ und die StPO – Von einer »herrschenden Meinung« und ihrer fragwürdigen Entstehung. *StV*, 50–52.

Berghel, H. & Hoelzer, D. (2006). Digital village: Disk wiping by any other name. *Communications of the ACM*, *49* (8), 17–21.

Bessen, J. & Hunt, R. M. (2004). *An empirical look at software patents. working paper no. 03-17/r.* Verfügbar unter http://www.researchoninnovation.org/swpat.pdf

Bessen, J. & Hunt, R. M. (2007). An empirical look at software patents. *Journal of Economics and Management Strategy*, *16*, 157–189.

Beukelmann, S. (2008). Die Online-Durchsuchung. *StraFo*, 1–8.

Beulke, W. & Meininghaus, F. (2007). Anmerkung zu BGH StV 2007, 60. *StV*, 63–65.

Bier, S. (2005). Kampf gegen Cyberkriminalität. *DuD*, *29*, 473–477.

Bieszk, D. & Sadtler, S. (2007). Mobbing und Stalking: Phänomene der modernen (Arbeits-)Welt und ihre Gegenüberstellung. *NJW*, 3382–3387.

Blankenburg, D. (2010). Quo vadis §§ 106, 108a UrhG? Strafrechtlicher Urheberrechtsschutz nach dem BVerfG-Urteil zur Vorratsdatenspeicherung. *MMR*, 587–591.

Blazakis, D. (2010). Interpreter exploitation. In *4th USENIX workshop on offensive technologies.* Berkeley: USENIX.

Bleisteiner, S. (1999). *Rechtliche Verantwortlichkeit im Internet: unter besonderer Berücksichtigung des Teledienstegesetzes und des Mediendienste-Staatsvertrags*. Köln: Heymanns.

Böckenförde, T. (2003). *Die Ermittlung im Netz: Möglichkeiten und Grenzen neuer Erscheinungsformen strafprozessualer Ermittlungstätigkeit*. Tübingen: Mohr Siebeck.

Böckenförde, T. (2008). Auf dem Weg zur elektronischen Privatsphäre. Zugleich Besprechung von BVerfG, Urteil v. 27.2.2008 – »Online-Durchsuchung«. *JZ*, 925–939.

Böhlke, D. & Yilmaz, O. (2008). Auswirkungen von § 202c StGB auf die Praxis der IT-Sicherheit. *CR*, 261–266.

Böhme, R. (2005). Cyber-insurance revisited. In *Proceedings of the fourth annual workshop on the economics of information security (WEIS).*

Böhme, R. & Holz, T. (2006). The effect of stock spam on financial markets. In *Proceedings of the sixth workshop on the economics of information security (WEIS).*

Böhme, R. & Kataria, G. (2006). Models and measures for correlation in cyber-insurance. In *Proceedings of the fifth annual workshop on the economics of information security (WEIS).*

Böhme, R. & Schwartz, G. (2010). Modeling cyber-insurance: Towards a unifying framework. In *Proceedings of the ninth workshop on the economics of information security (WEIS).*

Bolduan, G. (2008). Digitaler Untergrund. *Technology Review (Deutschland)*, 27–34.

Bolot, J. & Lelarge, M. (2008). A new perspective on internet security using insurance. In *Proceedings of the 27th conference on computer communications (infocom)* (S. 1948–1956). Phoenix.

Borges, G., Schwenk, J., Stuckenberg, C.-F. & Wegener, C. (2011). *Identitätsdiebstahl und Identitätsmissbrauch im Internet: Rechtliche und technische Aspekte*. Berlin: Springer.

Borges, G., Stuckenberg, C.-F. & Wegener, C. (2007). Bekämpfung der Computerkriminalität. Zum Entwurf eines Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität. *DuD*, 275–278.

Böse, M. (2006). Die Europäisierung der Strafvorschriften gegen Kinderpornografie. In A. Hoyer, H. E. Müller, M. Pawlik & J. Wolter (Hrsg.), *Festschrift für Friedrich-Christian Schroeder zum 70. Geburtstag* (S. 751–760). Heidelberg: C.F. Müller.

Braum, S. (2009). »Parallelwertungen in der Laiensphäre«: Der EuGH und die Vorratsdatenspeicherung. *ZRP*, 174–177.

Bremer, K. (2002). Radikal-politische Inhalte im Internet – ist ein Umdenken erforderlich? *MMR*, 147–152.

Brenner, S. W. (2002). Organized cybercrime? How cyberspace may affect the structure of criminal relationships. *North Carolina Journal of Law & Technology*, *4* (1), 1–41.

Brenner, S. W. (2009a). *Cyberthreats: The emerging fault lines of the nation state*. New York: Oxford University Press.

Brenner, S. W. (2009b). *Remote murder?* Verfügbar unter http://cyb3rcrim3.blogspot.com/2009/02/remote-murder.html

Brenner, S. W. (2010). *Cybercrime: criminal threats from cyberspace*. Santa Barbara: Praeger.

Brenner, S. W. & Clarke, L. L. (2005). Distributed security: Preventing cybercrime. *John Marshall Journal of Computer and Information Law*, *23*, 659–709.

Brodowski, D. (2009). Strafprozessualer Zugriff auf E-Mail-Kommunikation. Zugleich Besprechung zu BVerfG, Beschl. v. 16. 6. 2009 – 2 BvR 902/06 sowie zu BGH, Beschl. v. 31. 3. 2009 – 1 StR 76/09. *JR*, 402–412.

Brodowski, D. (2010a). Anmerkung zu BVerfG JR 2010, 543. *JR*, 546–550.

Brodowski, D. (2010b). EU actions on cybercrime and cybercrime investigations. In M. Bellini, P. Brunst & J. Jähnke (Hrsg.), *Current issues in IT security* (S. 145–161). Berlin: Duncker & Humblot.

Brodowski, D. (2010c). Strafrechtsrelevante Entwicklungen in der Europäischen Union – ein Überblick. *ZIS*, 749–761.

Brodowski, D. (2010d). Strafrechtsrelevante Entwicklungen in der Europäischen Union – ein Überblick. *ZIS*, 376–386.

Brodowski, D. (2011). Anmerkung zu HansOLG Hamburg, Urt. v. 15.2.2010 – 2 – 27/09 (REV). *StV*, 105–108.

Brunst, P. W. (2009a). Anmerkung zu BVerfG CR 2009, 584. *CR*, 591–593.

Brunst, P. W. (2009b). *Anonymität im Internet – rechtliche und tatsächliche Rahmenbedingungen: zum Spannungsfeld zwischen einem Recht auf Anonymität bei der elektronischen Kommunikation und den Möglichkeiten zur Identifizierung und Strafverfolgung*. Berlin: Duncker & Humblot.

Buermeyer, U. (2007a). Die Online-Durchsuchung – Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme. *HRRS*, 154–166.

Buermeyer, U. (2007b). Die »Online-Durchsuchung«. Verfassungsrechtliche Grenzen des verdeckten hoheitlichen Zugriffs auf Computersysteme. *HRRS*, 329–327.

Bundesamt für Justiz. (2009). *Übersicht Telekommunikationsüberwachung (Maßnahmen nach § 100a StPO) für 2008.*

Bundesamt für Justiz. (2010). *Übersicht Telekommunikationsüberwachung (Maßnahmen nach § 100a StPO) für 2009.*

Bundesamt für Sicherheit in der Informationstechnik. (o. J.). *BSI: Startseite.* Verfügbar unter https://www.bsi-fuer-buerger.de/

Bundeskriminalamt. (2010). *Polizeiliche Kriminalstatistik 2009: Bundesrepublik Deutschland*. Wiesbaden: Bundeskriminalamt.

Burchard, C. & Brodowski, D. (2010). Art. 50 Charta der Grundrechte der Europäischen Union und das europäische ne bis in idem nach dem Vertrag von Lissabon. *StraFo*, 376–386.

Bussmann, K.-D., Krieg, O., Nestler, C., Salvenmoser, S., Schroth, A., Theile, A. et al. (2009). *Wirtschaftskriminalität 2009: Sicherheitslage in deutschen Großunternehmen.* Verfügbar unter http://www.pwc.de/de/risiko-management/assets/Studie-Wirtschaftskriminal-09.pdf

Chaos Computer Club. (2008). Attrappe des Fingerabdrucks von Wolfgang Schäuble. *Die Datenschleuder* (92).

Chiesa, R., Ciappi, S. & Ducci, S. (2009). *Profiling hackers – the science of criminal profiling as applied to the world of hacking*. Boca Raton: CRC.

Cornelius, K. (2007). Zur Strafbarkeit des Anbieters von Hackertools. *CR*, 682–688.

Cova, M., Kruegel, C. & Vigna, G. (2008). There is no free phish: An analysis of »free« and live phishing kits. In *Proceedings of the 2nd conference on USENIX workshop on offensive technologies.* Berkeley: USENIX.

CSI/FBI. (2006). *Computer crime and security survey*. San Francisco: Computer Security Institute.

Dannecker, G. (2005). Die Dynamtik des materiellen Strafrechts unter dem Einfluss europäischer und internationaler Entwicklungen. *ZStW*, *117*, 697–748.

Dederer, H.-G. (2010). Konsistente Glücksspielregulierung. Eckpunkte aus den Sportwetten-Urteilen des EuGH vom 8.9.2010. *EuZW*, 771–774.

Degenhart, C. (2010). Anmerkung zu BVerfG JZ 2010, 298. *JZ*, 306–310.

Deiseroth, D. & Derleder, P. (2008). Whistleblower und Denunziatoren. *ZRP*, 248–251.

Devadas, S. (2009). Physical unclonable functions and secure processors. In C. Clavier & K. Gaj (Hrsg.), *Cryptographic hardware and embedded systems – CHES 2009, 11th international workshop, Lausanne, Switzerland, September 6-9, 2009, proceedings* (S. 65). Berlin: Springer.

DFN-CERT Services GmbH. (o. J.). *CERT-Verbund.* Verfügbar unter http://www.cert-verbund.de/

Dingledine, R., Mathewson, N. & Syverson, P. F. (2004). Tor: The second-generation onion router. In *13th USENIX security symposium* (S. 303–320). Berkeley: USENIX.

Dornseif, M. (2005). *Phänomenologie der IT-Delinquenz: Computerkriminalität, Datennetzkriminalität, Multimediakriminalität, Cybercrime, Cyberterror und Cyberwar in der Praxis*. Unveröffentlichte Dissertation, Rechts- und Staatswissenschaftliche Fakultät der Rheinischen Friedrich-Wilhelms-Universität Bonn.

DTI. (2004). *Information security breaches survey*. London: Department of Trade and Industry.

Duttge, G., Hörnle, T. & Renzikowski, J. (2004). Das Gesetz zur Änderung der Vorschriften über die Straftaten gegen die sexuelle Selbstbestimmung. *NJW*, 1065–1072.

eco – Verband der deutschen Internetwirtschaft e.V. (o. J.). *Anti-Botnet-Beratungszentrum.* Verfügbar unter http://www.botfrei.de

eco – Verband der deutschen Internetwirtschaft e.V. & Freiwillige Selbstkontrolle Multimedia-Diensteanbieter. (o. J.). *Internet-Beschwerdestelle.* Verfügbar unter http://www.internet-beschwerdestelle.de

Eichelberger, J. (2004). Sasser, Blaster, Phatbot & Co. – alles halb so schlimm? Ein Überblick über die strafrechtliche Bewertung von Computerschädlingen. *MMR*, 594–597.

Eicker, A. (2010). *Die Prozeduralisierung des Strafrechts: zur Entstehung, Bedeutung und Zukunft eines Paradigmenwechsels*. Bern: Stämpfli.

Eisele, J. (2005). Strafrechtlicher Schutz vor unbefugten Bildaufnahmen. *JR*, 6–11.

Eisele, J. (2010). Zur Strafbarkeit von sog. »Kostenfallen« im Internet. *NStZ*, 193–199.

Ellis, E. (Hrsg.). (1999). *The principle of proportionality in the laws of europe*. Oxford: Hart.

EMR/provet. (2009). *Die Zulässigkeit einer Kulturflatrate nach nationalem und europäischem Recht.* Verfügbar unter http://www.gruene-bundestag.de/cms/netzpolitik/dokbin/278/278059.kurzgutachten_zur_kulturflatrate.pdf

Endrass, J., Urbaniok, F., Hammermeister, L. C., Benz, C., Elbert, T., Laubacher, A. et al. (2009). The consumption of Internet child pornography and violent and sex offending. *BMC Psychiatry*, *9:43*.

Engelberth, M., Freiling, F. C., Göbel, J., Gorecki, C., Holz, T., Hund, R. et al. (2010). The inmas approach. In *Proceedings 1st european workshop on internet early warning and network intelligence (EWNI'10).*

Ernst, S. (2003). Hacker und Computerviren im Strafrecht. *NJW*, 3233–3239.

Ernst, S. (2009). Recht kurios im Internet – Virtuell gestohlene Phönixschuhe, Cyber-Mobbing und noch viel mehr. *NJW*, 1320–1322.

Ernst, S. & Spoenle, J. (2008). Zur Srafbarkeit des Schwarz-Surfens. *CR*, 439–442.

Eser, A. (2000). Sanktionierung und Rechtfertigung durch Verfahren. In P.-A. Albrecht et al. (Hrsg.), *Winfried Hassemer zum sechzigsten Geburtstag. Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft – Sonderheft.* Baden-Baden: Nomos.

Esser, R. (2010). Urheberrechtsverletzungen durch Tauschbörsennutzer im Internet. *GA*, 65–83.

Ester, M. & Benzmüller, R. (2010). *Underground economy – update 04/2010.* G Data. Verfügbar unter http://www.gdata.de/uploads/media/GData_Whitepaper_04_2010_GER_Screen.pdf (G Data Whitepaper 04/2010)

European Financial Coalition against Commercial Sexual Exploitation of Children Online. (2010). *14 months on: A combined report from the European Financial Coalition.* Verfügbar unter http://tinyurl.com/67b6q5r

eurostat. (2011). *8 Februar 2011 – »Safer Internet Day«: Fast ein Drittel der Internetnutzer in der EU27 war von einem Computervirus betroffen.* Verfügbar unter http://europa.eu/rapid/pressReleasesAction.do?reference=STAT/11/21&format=HTML&aged=0&language=DE&guiLanguage=de

Fallmann, H., Wondracek, G. & Platzer, C. (2010). Covertly probing underground economy marketplaces. In C. Kreibich & M. Jahnke (Hrsg.), *Detection of intrusions and malware, and vulnerability assessment, 7th international conference, DIMVA 2010, Bonn, Germany, July 8-9, 2010. proceedings* (S. 101–110). Berlin: Springer.

Fangerow, K. & Schulz, D. (2010). Die Nutzung von Angeboten auf www.kino.to. Eine urheberrechtliche Analyse des Film-Streamings im Internet. *GRUR*, 677–682.

Fawzi, N. (2009). *Cyber-Mobbing. Ursachen und Auswirkungen von Mobbing im Internet.* Baden-Baden: Nomos.

Fischer, T. (2011). *Strafgesetzbuch und Nebengesetze* (58. Aufl.). München: Beck.

Florêncio, D. & Herley, C. (2010). Phishing and money mules. In *Proceedings IEEE international workshop on information forensics and security (WIFS).*

Fossi, M., Johnson, E., Turner, D., Mack, T., Blackbird, J., McKinney, D. et al. (2008). *Symantec report on the underground economy: July 07–june 08.* Verfügbar unter http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008-14525717.en-us.pdf

Foucault, M. (1994). *Überwachen und Strafen: die Geburt des Gefängnisses*. Frankfurt am Main: Suhrkamp.

Frank, T. (2004). *Zur strafrechtlichen Bewältigung des Spamming*. Berlin: Logos.

Franklin, J., Perrig, A., Paxson, V. & Savage, S. (2007). An inquiry into the nature and causes of the wealth of internet miscreants. In P. Ning, S. D. C. di Vimercati & P. F. Syverson (Hrsg.), *Proceedings of the 2007 ACM conference on computer and communications security, CCS 2007, Alexandria, Virginia, USA, October 28-31, 2007* (S. 375–388). New York: ACM.

Freiling, F. C. (2010). *Wie repräsentativ sind die Messdaten eines Honeypot?* (Bericht Nr. TR-2010-001). Universität Mannheim, Institut für Informatik.

Freiling, F. C., Holz, T. & Mink, M. (2008). Reconstructing people's lives: A case study in teaching forensic computing. In O. Göbel, S. Frings, D. Günther, J. Nedon & D. Schadt (Hrsg.), *IT-incidents management & IT-forensics - IMF 2008, conference proceedings, September 23-25, 2008, Mannheim, Germany* (S. 125–142). Bonn: GI.

Freiling, F. C., Holz, T. & Wicherski, G. (2005). Botnet tracking: Exploring a root-cause methodology to prevent distributed denial-of-service attacks. In S. D. C. di Vimercati, P. F. Syverson & D. Gollmann (Hrsg.), *Computer security – ESORICS 2005, 10th european symposium on research in computer security, Milan, Italy, September 12-14, 2005, proceedings* (S. 319–335). Berlin: Springer.

Furedi, F. (2002). *Culture of fear*. London: Continuum.

Garfinkel, S. (2001). *Database nation: The death of privacy in the 21st century*. Cambridge: O'Reilly.

Garfinkel, S. L., Stallman, R. M. & Kapor, M. (1991). Why patents are bad for software. *Issues in Science and Technology*.

Gaycken, S. (2011). *Cyberwar: Das Internet als Kriegsschauplatz*. München: Open Source Press.

Gaycken, S. & Karger, M. (2011). Entnetzung statt Vernetzung. Paradigmenwechsel bei der IT-Sicherheit. *MMR*, 3-8.

Gazeas, N., Grosse-Wilde, T. & Kießling, A. (2009). Die neuen Tatbestände im Staatsschutzstrafrecht – Versuch einer ersten Auslegung der §§ 89a, 89b und 91 StGB. *NStZ*, 593–603.

Gercke, B. (2009a). Anmerkung zu BVerfG StV 2009, 623. *StV*, 624–626.

Gercke, B. (2009b). Zur Zulässigkeit sog. Transborder Searches – Der strafprozessuale Zugriff auf im Ausland gespeicherte Daten. *StraFo*, 271–274.

Gercke, M. (2005). Der Rahmenbeschluss über Angriffe auf Informationssysteme. *CR*, 468–472.

Gercke, M. (2007a). Cyberterrorismus – Aktivitäten terroristischer Organisationen im Internet. *CR*, 62–68.

Gercke, M. (2007b). Heimliche Online-Durchsuchung: Anspruch und Wirklichkeit. Der Einsatz softwarebasierter Ermittlungsinstrumente zum heimlichen Zugriff auf Computerdaten. *CR*, 245–253.

Gercke, M. (2008). Die Bekämpfung der Internetkriminalität als Herausforderung für die Strafverfolgungsbehörden. *MMR*, 291–298.

Gercke, M. (2009a). Die Entwicklung des Internetstrafrechts im Jahr 2008. *ZUM*, 526–538.

Gercke, M. (2009b). Europes legal approaches to cybercrime. *ERA-Forum*, 409–420.

Gercke, M. (2009c). Sind Raubkopierer Verbrecher? Die strafrechtliche Bewertung der Tauschbörsennutzung. *Juristische Arbeitsblätter*, 90–95.

Gercke, M. (2010a). Defizite des Schriften-Erfordernisses in Internet-bezogenen Sexual- und Pornographiedelikten: wie unkörperliche Übertragungsformen die Strafbarkeit von Online-Grooming und Online-Zugang zu Jugend- und Kinderpornographie reduzieren. *CR*, 798–803.

Gercke, M. (2010b). Impact of the lisbon treaty on fighting cybercrime in the EU: the redefined role of the EU and the change in approach from patchwork to comprehensiveness. *Computer Law Review International*, 75–80.

Gercke, M. (2010c). Strafrechtliche und strafprozessuale Aspekte von Cloud Computing und Cloud Storage. *CR*, 345–348.

Gercke, M. & Brunst, P. W. (2009). *Praxishandbuch Internetstrafrecht*. Stuttgart: Kohlhammer.

Gerhards, J. (2010). *(Grund-)Recht auf Verschlüsselung?* Baden-Baden: Nomos.

Gerhold, L. (2010). *Sicherheit in Zukunft. Explorationsstudie zu zukünftigen Anforderungen an die Sicherheitsforschung*. Berlin: Forschungsforum Öffentliche Sicherheit.

Gibson, W. (1984). Neuromancer. *New York: Berkley Communications Group*.

Göbel, J. (2010). Amun: Automatic capturing of malicious software. In F. C. Freiling (Hrsg.), *Sicherheit 2010: Sicherheit, Schutz und Zuverlässigkeit, Beiträge der 5. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI), 5.-7. Oktober 2010 in Berlin* (S. 177–190). Bonn: GI.

Göbel, J. & Holz, T. (2008). Rishi: Identifizierung von Bots durch Auswerten der IRC-Nicknamen. In *Proceedings of the 15th DFN-CERT workshop »Sicherheit in vernetzten Systemen«*.

Göbel, J., Holz, T. & Willems, C. (2007). Measurement and analysis of autonomous spreading malware in a university environment. In B. M. Hämmerli & R. Sommer (Hrsg.), *Detection of intrusions and malware, and vulnerability assessment, 4th international conference, DIMVA 2007, Lucerne, Switzerland, July 12-13, 2007, proceedings* (S. 109–128). Berlin: Springer.

Göbel, J. & Trinius, P. (2010). Towards optimal sensor placement strategies for early warning systems. In F. C. Freiling (Hrsg.), *Sicherheit 2010: Sicherheit, Schutz und Zuverlässigkeit, Beiträge der 5. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI), 5.-7. Oktober 2010 in Berlin* (S. 191–204). Bonn: GI.

Gödel, K. (1931). Über formal unentscheidbare Sätze der Principia mathematica und verwandter Systeme I. *Monats. für Math. und Phys.*, *38*, 173–198.

Goeckenjan, I. (2008). Phishing von Zugangsdaten für Online-Bankdienste und deren Verwertung. *wistra*, 128–136.

Gordon, L. & Loeb, M. (2006). *Managing cyber-security resources: A cost-benefit analysis*. New York: McGraw-Hill.

Gordon, S. & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, *2* (1), 13–20.

Grabenwarter, C. (2008). *Europäische Menschenrechtskonvention* (3. Aufl.). München: Beck.

Graf, J.-P. (2003). Kommentierung der §§ 201 ff. StGB. In W. Joecks & K. Miebach (Hrsg.), *Münchener Kommentar zum Strafgesetzbuch. Band 3: §§ 185–262 StGB*. München: Beck.

Graf, J. P. (2007). »Phishing« derzeit nicht generell strafbar! *NStZ*, 129–132.

Graf, J. P. (2010). Kommentierung der §§ 99 ff. StPO. In J. P. Graf (Hrsg.), *Beck'scher Online-Kommentar. Strafprozessordnung* (8. Aufl.). München: Beck.

Gräfin Tyszkiewicz, G. (2010). Skimming als Ausspähen von Daten gemäß § 202a StGB? *HRRS*, 207–213.

Gramespacher, T. & Wichering, U. (2010). Kommentar zur Entscheidung des LG Wuppertal vom 19.10.2010 (25 Qs-10 Js 1977/08-177/10; K&R 2010, 838) – Nulla poena sine lege: Zur Strafbarkeit der Nutzung offener WLAN-Netze. *K & R*, 840–842.

Gröseling, N. & Höfinger, F. M. (2007). Hacking und Computerstrafrecht – Auswirkungen des 41. StrÄG zur Bekämpfung der Computerkriminalität. *MMR*, 549–553.

Grützmacher, M. (2009). Kommentierung der §§ 69 ff. UrhG. In A.-A. Wandtke & W. Bullinger (Hrsg.), *Praxiskommentar zum Urheberrecht* (3. Aufl.). München: Beck.

Haft, F. (1987). Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. WiKG) – Teil 2: Computerdelikte. *NStZ*, 6–10.

Halderman, J. A., Schoen, S. D., Heninger, N., Clarkson, W., Paul, W., Calandrino, J. A. et al. (2009). Lest we remember: cold-boot attacks on encryption keys. *Commun. ACM*, *52* (5), 91–98.

Hansen, M. & Pfitzmann, A. (2007). Online-Durchsuchung. *DRiZ*, 225–228.

Härting, N. (2009). Beschlagnahme und Archivierung von Mails. E-Mail zwischen Telekommunikation, Datensatz und elektronischer Post. *CR*, 581–584.

Hassemer, I. M. & Ingeberg, T. (2008). Dual-Use-Software aus der Perspektive des Strafrechts (§ 202c StGB). *Der IT-Rechts-Berater*, 84–87.

Hassemer, W. (2001). Das Symbolische am symbolischen Strafrecht. In B. Schünemann, H. Achenbach, W. Bottke, B. Haffke & H.-J. Rudolphi (Hrsg.), *Festschrift für Claus Roxin zum 70. Geburtstag am 15. Mai 2001* (S. 1001–1019). Berlin: De Gruyter.

Hassemer, W. (2007). Prozeduralisierung, Wahrheit und Gerechtigkeit. In W. Hassemer (Hrsg.), *Erscheinungsformen des modernen Rechts*. Frankfurt a.M.: Klostermann.

Heger, M. (2008). Fünf Jahre §§ 152a Abs. 2, 263a Abs. 3 StGB: Ein Plädoyer für die Korrektur handwerklicher Mängel bei der innerstaatlichen Umsetzung von EU-Vorgaben. *ZIS*, 496–499.

Heghmanns, M. (2004). Musiktauschbörsen im Internet aus strafrechtlicher Sicht. *MMR*, 14–18.

Heghmanns, M. (2007). Strafbarkeit des »Phishing« von Bankkontendaten und ihre Verwertung. *wistra*, 167–170.

Heinrich, B. (2000). Anmerkung zu KG NStZ 2000, 533. *NStZ*, 533–534.

Heinrich, M. (2005). Neue Medien und klassisches Strafrecht – § 184b IV StGB im Lichte der Internetdelinquenz. *NStZ*, 361–366.

Heisenberg, W. (1984). *Physik und Philosophie* (4. Aufl.). Stuttgart: S. Hirzel Verlag.

Hektor, J. & Göbel, J. (2008). *Der Blast-o-Mat v4: Ein Ansatz zur automatischen Erkennung und Sperrung von Malware infizierten Computern.* Verfügbar unter http://edoc.hu-berlin.de/conferences/dfn2007/hektor-jens-101/PDF/hektor.pdf

Hennessy, J. L. & Patterson, D. A. (1990). *Computer architecture: A quantitative approach*. San Francisco: Morgan Kaufmann.

Herley, C. & Florêncio, D. (2009). Nobody sells gold for the price of silver: Dishonesty, uncertainty and the underground economy. In *Proceedings on the eighth workshop on the economics of information security (WEIS).*

Herzog, F. (1991). *Gesellschaftliche Unsicherheit und strafrechtliche Daseinsvorsorge: Studien zur Vorverlegung des Strafrechtsschutzes in den Gefährdungsbereich*. Heidelberg: v. Decker.

Hilgendorf, E. (2001). Neue Medien und Strafrecht. *ZStW*, *113*, 650–680.

Hilgendorf, E. (2006). Betrug im Internet. In K. Asada, H.-D. Assmann, Z. Kitagawa, J. Murakami & M. Nettesheim (Hrsg.), *Das Recht vor den Herausforderungen neuer Technologien* (S. 141–161). Tübingen: Mohr Siebeck.

Hilgendorf, E. (2009). Kommentierung der §§ 303a, 303b StGB. In H. Satzger, B. Schmitt & G. Widmaier (Hrsg.), *StGB. Strafgesetzbuch. Kommentar.* Köln: Heymanns.

Hilgendorf, E. (2010a). Ehrenkränkungen (»flaming«) im Web 2.0. Ein Problemaufriss de lege lata und de lege ferenda. *ZIS*, 208–215.

Hilgendorf, E. (2010b). Kommentierung der §§ 202a ff. StGB. In H. W. Laufhütte, R. Rissing-van Saan & K. Tiedemann (Hrsg.), *Strafgesetzbuch: Leizpiger Kommentar. Band 6: §§ 146 bis 210* (12. Aufl.). Berlin: De Gruyter.

Hilgendorf, E., Frank, T. & Valerius, B. (2005). *Computer- und Internetstrafrecht: ein Grundriss*. Berlin: Springer.

Hilgendorf, E. & Hong, S.-H. (2003). Cyberstalking. Eine neue Variante der Internetkriminalität. *K & R*, 168–172.

Hilgendorf, E. & Valerius, B. (in Druck). *Computer- und Internetstrafrecht: ein Grundriss* (2. Aufl.). Berlin: Springer.

Hill, A., Briken, P. & Berner, W. (2006). Pornographie im Internet – Ersatz oder Anreiz für sexuelle Gewalt? In Stiftung Deutsches Forum für Kriminalprävention (DFK) (Hrsg.), *Internet-Devianz* (S. 113–135). Berlin: DFK.

Hoeren, T. (2010). Anonymität im Web – Grundfragen und aktuelle Entwicklungen. *ZRP*, 251–253.

Hoffmann, J. (2006). Cyberstalking. In Stiftung Deutsches Forum für Kriminalprävention (DFK) (Hrsg.), *Internet-Devianz* (S. 103–111). Berlin: DFK.

Hoffmann-Riem, W. (2008). Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme. *JZ*, 1009-1022.

Hoffmann-Riem, W. (2009). Grundrechts- und Funktionsschutz für elektronisch vernetzte Kommunikation. *Archiv des öffentlichen Rechts*, *134*, 513–541.

Höfinger, F. M. (2009). Anmerkung zu BVerfG ZUM 2009, 745. *ZUM*, 751–753.

Holz, T., Engelberth, M. & Freiling, F. (2009). Learning more about the underground economy: A case-study of keyloggers and dropzones. In M. Backes & P. Ning (Hrsg.), *Computer security – ESORICS 2009: 14th european symposium on research in computer security.* Berlin: Springer.

Holz, T., Gorecki, C., Rieck, K. & Freiling, F. C. (2008). Measuring and detecting fast-flux service networks. In *Network and distributed system security symposium 2008: proceedings; February 10–13, 2008, San Diego, California.* Reston: Internet Society.

Holz, T., Steiner, M., Dahl, F., Biersack, E. & Freiling, F. C. (2008). Measurements and mitigation of peer-to-peer-based botnets: A case study on storm worm. In *First USENIX workshop on large-scale exploits and emergent threats, April 15, 2008, san Francisco, CA, USA, proceedings.* Berkeley: USENIX Association.

Holzner, S. (2009). Klarstellung strafrechtlicher Tatbestände durch den Gesetzgeber erforderlich. *ZRP*, 177–178.

Honeynet Project. (2003). *Know your enemy: A profile.* Verfügbar unter http://old.honeynet.org/papers/profiles/cc-fraud.pdf

Hopf, K. & Braml, B. (2007). Virtuelle Kinderpornographie vor dem Hintergrund des Online-Spiels Second Life. *ZUM*, 354–363.

Hornick, A. (2008). Staatlicher Zugriff auf elektronische Medien. *StraFo*, 281–286.

Hörnle, T. (2001). Anmerkung zu BGH NStZ 2001, 305. *NStZ*, 309–311.

Hörnle, T. (2006). Anschlussdelikte als abstrakte Gefährdungsdelikte – Wem sind Gefahren durch verbotene Märkte zuzurechnen? In A. Hoyer, H. E. Müller, M. Pawlik & J. Wolter (Hrsg.), *Festschrift für Friedrich-Christian Schroeder zum 70. Geburtstag* (S. 477-495). Heidelberg: C.F. Müller.

Hörnle, T. (2008). Die Umsetzung des Rahmenbeschlusses zur Bekämpfung der sexuellen Ausbeutung von Kindern und der Kinderpornographie. *NJW*, 3521–3525.

Hörnle, T. (2010a). Anmerkung zu BVerfG JZ 2010, 298. *JZ*, 310–313.

Hörnle, T. (2010b). Anmerkung zu HansOLG NStZ 2010, 704. *NStZ*, 704–706.

Hornung, G. (2007). Ermächtigungsgrundlage für die Online-Durchsuchung? *DuD*, 575–580.

Hornung, G. (2008). Ein neues Grundrecht. Der verfassungsrechtliche Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme. *CR*, 299-306.

Hornung, G. (2009). Anmerkung zu BVerfG CR 2009, 673. *CR*, 677-679.

Hornung, G. & Schnabel, C. (2010). Anmerkung zu BVerfG DVBl 2010, 503. *Deutsches Verwaltungsblatt*, 824–833.

Hössle, M. (2010). Dynamische Softwarepatentierung. Neue Spruchpraxis zur Patentierung computerimplementierter Erfindungen auf nationaler und europäischer Ebene. *CR*, 559–564.

Howard, M., LeBlanc, D. & Viega, J. (2005). *19 deadly sins of software security: programming flaws and how to fix them*. New York: McGraw-Hill.

Höynck, T. (2008). Stumpfe Waffe? Möglichkeiten und Grenzen der Anwendung von § 131 StGB auf gewalthaltige Computerspiele am Beispiel »Der Pate – Die Don Edition«. *ZIS*, 206–217.

Höynck, T. & Pfeiffer, C. (2007). Verbot von »Killerspielen«? – Thesen und Vorschläge zur Verbesserung des Jugendmedienschutzes. *ZRP*, 91–94.

Hullen, N. (2008). Illegale Streaming-Filmportale im Internet. *Der IT-Rechts-Berater*, 230–232.

Hund, R., Holz, T. & Freiling, F. C. (2009). Return-oriented rootkits: Bypassing kernel code integrity protection mechanisms. In *18th USENIX security symposium* (S. 383–398). Berkeley: USENIX Association.

INHOPE. (o. J.). *Inhope – the international association of internet hotlines.* Verfügbar unter https://www.inhope.org/

Inman, K. & Rudin, N. (2000). *Principles and practice of criminalistics: The proefssion of forensic science*. Boca Raton: CRC.

Jahn, M. & Kudlich, H. (2007). Die strafprozessuale Zulässigkeit der Online-Durchsuchung. Zugleich Anmerkung zu den Beschlüssen des Ermittlungsrichters des Bundesgerichtshofes v. 25.11.2006 – 1 BGs 184/06 und v. 28.11.2006 – 1 BGs 186/2006. *JR*, 57–61.

Janssen, G. & Maluga, G. (2010). Kommentierung der §§ 16 ff. UWG. In W. Joecks & R. Schmitz (Hrsg.), *Münchener Kommentar zum Strafgesetzbuch. Band 6/1: Nebenstrafrecht II.* München: Beck.

Jeßberger, F. (2001). Anmerkung zu BGH JR 2001, 429. *JR*, 432–435.

Johnson, B., Grossklags, J., Christin, N. & Chuang, J. (2010). Are security experts useful? bayesian nash equilibria for network security games. In D. Gritzalis, B. Preneel & M. Theoharidou (Hrsg.), *Computer security – ESORICS 2010: 15th european symposium on research in computer security* (S. 588–606). Berlin: Springer.

Kaiser, G. & Schöch, H. (Hrsg.). (2001). *Kriminologie, Jugendstrafrecht, Strafvollzug* (5. Aufl.). München: Beck.

Kanich, C., Kreibich, C., Levchenko, K., Enright, B., Voelker, G. M., Paxson, V. et al. (2009). Spamalytics: An empirical analysis of spam marketing conversion. *Communications of the ACM*, *52* (9), 99–107.

Katz, L. (2002). Villainy and felony: A problem concerning criminalization. *Buffalo Criminal Law Review*, *6*, 451–481.

Kelker, B. (2009). Online-Demonstrationen – ein Fall »additiver Mittäterschaft«? *GA*, 86–97.

Keller, R. (2009). *Softwarebezogene Patente und die verfassungsrechtlichen Eigentumsrechte der Softwareautoren aus Art. 14 GG*. Göttingen: Sierke.

Kiethe, K. & Hohmann, O. (2006). Der strafrechtliche Schutz von Geschäfts- und Betriebsgeheimnissen. *NStZ*, 185–191.

Kinzig, J. (2004). Die Telefonüberwachung in Verfahren organisierter Kriminalität: Fehler bei der richterlichen Anordnung, Mängel des Gesetzes. *StV*, 560–567.

Király, A. (2010). Der Beamte als Whistleblower. Die Zulässigkeit von Korruptionsanzeigen nach den jüngsten Gesetzesänderungen. *Die öffentliche Verwaltung*, 894–897.

Kiviat, B. (2010). *Driver's licenses for the internet.* Verfügbar unter http://curiouscapitalist.blogs.time.com/2010/01/30/drivers-licenses-for-the-internet/

Klein, O. (2009). Offen und (deshalb) einfach – Zur Sicherstellung und Beschlagnahme von E-Mails beim Provider. *NJW*, 2996–2999.

Klip, A. (2009). *European criminal law*. Antwerpen: Intersentia.

Koch, A. (2006). *Strafrechtliche Probleme des Angriffs und der Verteidigung in Computernetzen*. Baden-Baden: Nomos.

Koch, F. A. (2010). Der Content bleibt im Netz – gesicherte Werkverwertung durch Streaming-Verfahren. *GRUR*, 574–578.

Köhne, M. (2004). Zombies und Kannibalen: Zum Tatbestand der Gewaltdarstellung (§ 131 Abs. 1 StGB). *GA*, 180–187.

Köpsell, S., Federrath, H. & Hansen, M. (2003). Erfahrungen mit dem Betrieb eines Anonymisierungsdienstes. *DuD*, *27* (3), 139–142.

Kshetri, N. (2006). The simple economics of cybercrimes. *IEEE Security & Privacy*, *4* (1), 33–39.

Kshetri, N. (2010). *The global cybercrime industry: economic, institutional and strategic perspectives*. Berlin: Springer.

Kudlich, H. (2001). Anmerkung zu BGH StV 2001, 395. *StV*, 397–399.

Kudlich, H. (2002). Anmerkung zu BGH JZ 2002, 308. *JZ*, 310–312.

Kudlich, H. (2004). Herkunftslandprinzip und internationales Strafrecht. *HRRS*, 278–284.

Kunreuther, H. & Heal, G. (2003). Interdependent security. *Journal of Risk and Uncertainty*, *26*, 231–149.

Kutscha, M. (2007). Verdeckte Online-Durchsuchung und Unverletzlichkeit der Wohnung. *NJW*, 1169–1172.

Kutscha, M. (2008). Mehr Schutz von Computerdaten durch ein neues Grundrecht? *NJW*, 1042–1044.

Lagodny, O. (2001). Anmerkung zu BGH JZ 2001, 1194. *JZ*, 1198–1200.

Lejeune, M. & Sieckmann, R. (2010). Softwarepatente in den USA und die aktuelle Entwicklung in Deutschland und der EU. *MMR*, 741–745.

Lenckner, T. & Eisele, J. (2010). Kommentierung der §§ 185 ff. StGB. In A. Schönke, H. Schröder & A. Eser (Hrsg.), *Strafgesetzbuch. Kommentar* (28. Aufl.). München: Beck.

Lenckner, T. & Winkelbauer, W. (1986). Computerkriminalität – Möglichkeiten und Grenzen des 2 WiKG. Teil 2. *CR*, 654–661.

Liesching, M. (2009). Anmerkung zu BVerfG MMR 2009, 178. *MMR*, 179–180.

Lober, A. (2005). Jugendschutz im Internet und im Mobile Entertainment. *K & R*, 65–71.

Lober, A. & Neumüller, C. (2010). Verkehrte Gewinnspielwelt? Zulässigkeit von Geschicklichkeits- und Glücksspielen in Internet und Rundfunk. *MMR*, 295–299.

Malamuth, N. M., Addison, T. & Koss, M. (2000). Pornography and sexual aggression: Are there reliable effects and can we understand them? *Annual Review of Sex Research*, *11*, 26–91.

Malek, K. (2005). *Strafsachen im Internet*. Heidelberg: C.F. Müller.

Malkus, M. (2010). Harry Potter und die Abmahnung des Schreckens. Die Höhe von Abmahngebühren bei Urheberrechtsverletzungen auf Tauschbörsen gem. § 97a Abs. 2 UrhG. *MMR*, 382–388.

Manske, M. (2007). *Tatort Internet – eine globale Herausforderung für die Innere Sicherheit.* Verfügbar unter http://bka.de/kriminalwissenschaften/herbsttagung/2007/kurzfassung_manske.pdf

Marberth-Kubicki, A. (2010). *Computer- und Internetstrafrecht* (2. Aufl.). München: Beck.

Merten, D. (2009). § 56 Grundrechtlicher Schutzstandard. In D. Merten & H.-J. Papier (Hrsg.), *Handbuch der Grundrechte in Deutschland und Europa. Band 3: Grundrechte in Deutschland: Allgemeine Lehren II.* Heidelberg: C.F. Müller.

Meyer, F. (2010). Rechtsstaat und Terrorlisten – Kaltstellung ohne Rechtsschutz? *HRRS*, 74–85.

Meyer-Goßner, L. (2010). *Strafprozessordnung mit GVG und Nebengesetzen* (53. Aufl.). München: Beck.

Michalke, R. (2008). Staatlicher Zugriff auf elektronische Medien. *StraFo*, 287–292.

Microsoft Inc. (2010). *Windows virtual pc: Home page.* Verfügbar unter http://www.microsoft.com/windows/virtual-pc/

Miller, C. (2007). The legitimate vulnerability market: Inside the secretive world of 0-day exploit sales. In *Proceedings of the sixth workshop on the economics of information security (WEIS).*

Mitnick, K. D. & Simon, W. L. (2002). *The art of deception: controlling the human element of security*. Indianapolis: Wiley.

Mitsch, W. (2005). *Recht der Ordnungswidrigkeiten* (2. Aufl.). Berlin: Springer.

Mitsch, W. (2007). Der neue Stalking-Tatbestand im Strafgesetzbuch. *NJW*, 1237–1242.

Möhrenschlager, M. (1986). Das neue Computerstrafrecht. *wistra*, 128–142.

Möhrenschlager, M. (2007). 13. Kapitel. Schutz von Geschäfts- und Betriebsgeheimnissen. In H.-B. Wabnitz & T. Janovsky (Hrsg.), *Handbuch des Wirtschafts- und Steuerstrafrechts.* München: Beck.

Möller, M. (2010). Der Gesetzgeber, das BVerfG, der BGH und § 97 a II UrhG: Missbrauchsbekämpfung nach Plan? *NJW*, 2999-3001.

Müller, H. E. (2010). Anmerkung zu HansOLG MMR 2010, 342. *MMR*, 342–345.

Müller, T., Dewald, A. & Freiling, F. C. (2010). AESSE: a cold-boot resistant implementation of AES. In M. Costa & E. Kirda (Hrsg.), *Proceedings of the third european workshop on system security, EUROSEC 2010, Paris, France, April 13, 2010* (S. 42–47). New York: ACM.

Nack, A. (2008). Kommentierung der §§ 94 ff. StPO. In R. Hannich (Hrsg.), *Karlsruher Kommentar zur Strafprozessordnung mit GVG, EGGVG und EMRK.* München: Beck.

Neuheuser, S. (2008). Die Strafbarkeit des Bereithaltens und Weiterleitens des durch »Phishing« erlangten Geldes. *NStZ*, 492–497.

Ohler, C. (2010). Anmerkung zu BVerfG JZ 2010, 611. *JZ*, 626–628.

Omitola, T. (2001). ACM fellow profile: Roger Needham. *Software Engineering Notes*, *26* (1).

Oracle Inc. (2010). *Virtualbox.* Verfügbar unter http://www.virtualbox.org/

Pagenkopf, M. (2009). Kommentierung der Art. 10, 11, 16a, 17, 18 GG. In M. Sachs (Hrsg.), *Grundgesetz. Kommentar.* (5. Aufl.). München: Beck.

Panda Security. (2010). *The cyber-crime black market: Uncovered.* Panda Security. Verfügbar unter http://press.pandasecurity.com/wp-content/uploads/2011/01/The-Cyber-Crime-Black-Market.pdf

Peifer, K.-N. & Kamp, J. (2009). Datenschutz und Persönlichkeitsrecht – Anwendung der Grundsätze über Produktkritik auf das Bewertungsportal »spickmich.de«? *ZUM*, 185–190.

Perron, W. & Eisele, J. (2010). Kommentierung der §§ 174 ff. StGB. In A. Schönke, H. Schröder & A. Eser (Hrsg.), *Strafgesetzbuch. Kommentar* (28. Aufl.). München: Beck.

Peters, S. (2009). Der Tatbestand des § 238 StGB (Nachstellung) in der staatsanwaltlichen Praxis. *NStZ*, 238–243.

Petri, T. (2009). Anmerkung zu EuGH EuZW 2009, 212. *EuZW*, 214–215.

Pfitzmann, A. (2007). *Möglichkeiten und Grenzen der Nutzungsüberwachung von Informations- und Kommunikationssystemen in einer freiheitlichen demokratischen Gesellschaft.* Verfügbar unter http://dud.inf.tu-dresden.de/literatur/MoegGrenzderNutzuebIuK-Sys-V1-0.pdf (Fachkundige Stellungnahme im Verfahren um die so genannte Online-Durchsuchung vor dem Bundesverfassungegericht)

Popp, A. (2004). Von »Datendieben« und »Betrügern« – Zur Strafbarkeit des so genannten »phishing«. *NJW*, 3517–3518.

Popp, A. (2007). Computerstrafrecht in Europa. *Medien und Recht International*, 458–463.

Popp, A. (2008). § 202c StGB und der neue Typus des europäischen »Software-Delikts«. *GA*, 375–393.

Pouget, F., Dacier, M. & Pham, V. H. (2005). Leurre.com: on the advantages of deploying a large scale distributed honeypot platform. In *ECCE'05, E-Crime and Computer Conference, 29-30th March 2005, Monaco.*

Provos, N. & Holz, T. (2007). *Virtual honeypots: From botnet tracking to intrusion detection*. Upper Saddle River: Addison-Wesley.

Radmann, F. (2010). Kino.ko – Filmegucken kann Sünde sein. Zur Rechtswidrigkeit der Nutzung von (offensichtlich) illegalen Streaming-Filmportalen. *ZUM*, 387–392.

Radtke, H. & Steinsiek, M. (2010). Terrorismusbekämpfung durch Vorfeldkriminalisierung? – Das Gesetz zur Verfolgung der Vorbereitung schwerer staatsgefährdender Gewalttaten. *JR*, 107–109.

Rantala, R. (2010). Cybercrime against businesses. In M. Bellini, P. Brunst & J. Jähnke (Hrsg.), *Current issues in IT security* (S. 37–49). Berlin: Duncker & Humblot.

Reinbacher, T. & Wincierz, A. (2007). Kritische Würdigung des Gesetzentwurfs zur Bekämpfung von Kinder- und Jugendpornographie. *ZRP*, 195–198.

Rempe, C. (2010). Anmerkung zu BGH MMR 2010, 550. *MMR*, 552.

Rettenmaier, F. & Kopf, O. (2007). Der unlautere Abschluss und Widerruf von Fernabsatzverträgen – Betrug gemäß § 263 Abs. 1 StGB? *JR*, 226–231.

Robinson, P. & Harley, J. (2003). The role of deterrence in the formulation of criminal law rules: At its worst when doing its best. *Georgetown Law Journal*, *91*, 949-1002.

Röder, R. (2010). Nach der letzten Änderung des § 184b StGB: Ist das Verbreiten sog. »Posing«–Fotos weiterhin straflos? *NStZ*, 113–119.

Rogers, M. (2005). The development of a meaningful hacker taxonomy: A two dimensional approach. *CERIAS Tech Report*, *2005* (43). Verfügbar unter https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2005-43.pdf

Roggan, F. (2001). Am deutschen Rechtswesen soll die Welt genesen? Eine rechtspolitische Skizze zum Urteil des BGH vom 12.12.2000. *Kritische Justiz*, 337-340.

Röhl, C. & Bosch, A. (2008). Musiktauschbörsen im Internet. Eine rechtliche Bewertung aus aktuellem Anlass. *NJW*, 1415–1420.

Rombach, W. (1990). Killer-Viren als Kopierschutz. *CR*, 101–106.

Roßnagel, A. & Schnabel, C. (2008). Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und sein Einfluss auf das Privatrecht. *NJW*, 3534–3538.

Rotsch, T. (2010). Compliance und Strafrecht: Konsequenzen einer Neuentdeckung. In W. Joecks, H. Ostendorf, T. Rönnau, T. Rotsch & R. Schmitz (Hrsg.), *Recht – Wirtschaft – Strafe: Festschrift für Erich Samson zum 70. Geburtstag* (S. 141–160). Heidelberg: C.F. Müller.

Roxin, C. (2006). *Strafrecht Allgemeiner Teil, Band 1* (4. Aufl.). München: Beck.

Rüther, W. (2006). Betrugsdelikte im Internet: Zum aktuellen Stand des Wissens aus kriminologischer Sicht. In Stiftung Deutsches Forum für Kriminalprävention (DFK) (Hrsg.), *Internet-Devianz.* Berlin: DFK.

Rüther, W. (2007). *Das Internet als Gegenstand und Instrument kriminologischer Forschung.* Vortrag auf dem 12. Deutschen Präventionstag. Verfügbar unter http://www.praeventionstag.de/Dokumentation.cms/231

Rutkowska, J. (2004). *Red Pill ... or how to detect VMM using (almost) one CPU instruction.* Verfügbar unter http://invisiblethings.org/papers/redpill.html

Rutkowska, J. (2006). *Subverting vista kernel for fun and profit.* Black Hat Briefings, Las Vegas. Verfügbar unter http://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Rutkowska.pdf

Rux, J. (2007). Ausforschung privater Rechner durch die Polizei- und Sicherheitsbehörden. Rechtsfragen der Online-Durchsuchung. *JZ*, 285–295.

Sachs, M. & Krings, T. (2008). Das neue Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. *JuS*, 481–486.

Sadeghi, A.-R., Stüble, C. & Pohlmann, N. (2004). European multilateral secure computing base – open trusted computing for you and me. *DuD* (9), 548–554.

Satzger, H. (2009). Kommentierung der §§ 1 ff. StGB. In H. Satzger, B. Schmitt & G. Widmaier (Hrsg.), *StGB. Strafgesetzbuch. Kommentar.* Köln: Heymanns.

Satzger, H. (2010). *Internationales und Europäisches Strafrecht* (4. Aufl.). Baden-Baden: Nomos.

Schäfer, G. (2004). Kommentierung der §§ 94 ff. StPO. In P. Rieß (Hrsg.), *Löwe/Rosenberg: Die Strafprozeßordnung und das Gerichtsverfassungsgesetz. Großkommentar. Band 2: §§ 72–136 StPO* (25. Aufl.). Berlin: De Gruyter.

Scheffler, H. & Dressel, C. (2000). Die Insuffizienz des Computerstrafrechts. *ZRP*, 514–517.

Schiemann, A. (2010). Anmerkung zu BGH JR 2010, 497. *JR*, 498–500.

Schlegel, S. (2008). Online-Durchsuchung light – Die Änderung des § 110 StPO durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung. *HRRS*, 23–30.

Schnabel, C. (2009). Das Mikado-Prinzip. Die mittelbare Rasterfahndung als Mittel zur Umgehung gesetzlicher Vorschriften? *CR*, 426–430.

Schneider, G. (2010). Consequences of cloud computing. In M. Bellini, P. Brunst & J. Jähnke (Hrsg.), *Current issues in IT security* (S. 81–87). Berlin: Duncker & Humblot.

Schneier, B. (2006). *Beyond fear.* New York: Springer.

Schomburg, W. (2006). Kommentierungen. In W. Schomburg, O. Lagodny, S. Gleß & T. Hackner (Hrsg.), *Internationale Rechtshilfe in Strafsachen* (4. Aufl.). München: Beck.

Schöning, U. (1997). (3. Aufl.). Heidelberg: Spektrum Akademischer Verlag.

Schramm, M. & Wegener, C. (2011). Neue Anforderungen an eine anlasslose Speicherung von Vorratsdaten. Umsetzungsmöglichkeiten der Vorgaben des Bundesverfassungsgerichts. *MMR*, 9-13.

Schroeder, F.-C. (1990). Pornographieverbot als Darstellerschutz? *ZRP*, 299–301.

Schroeder, F.-C. (2009). Gesetzestechnische Mängel im Gesetz zur Umsetzung des EU-Rahmenbeschlusses zur Bekämpfung der sexuellen Ausbeutung von Kindern und Kinderpornographie. *GA*, 213–218.

Schubarth, M. (1987). Faustrecht statt Auslieferungsrecht? *StV*, 173–175.

Schumann, K. H. (2007). Das 41. StrÄndG zur Bekämpfung der Computerkriminalität. *NStZ*, 675–680.

Schuster, F. P. (2006). Telekommunikationsüberwachung in grenzüberschreitenden Strafverfahren nach Inkrafttreten des EU-Rechtshilfeübereinkommens. *NStZ*, 657–663.

Schwarzenegger, C. & Summers, S. J. (in Druck). *The emergence of EU criminal law: cyber crime and the regulation of the informations society*. Oxford: Hart.

Seidl, A. & Fuchs, K. (2010). Die Strafbarkeit des Phishing nach Inkrafttreten des 41. Strafrechtsänderungsgesetzes. *HRRS*, 85–92.

Shacham, H. (2007). The geometry of innocent flesh on the bone: return-into-libc without function calls (on the x86). In P. Ning, S. D. C. di Vimercati & P. F. Syverson (Hrsg.), *Proceedings of the 2007 ACM conference on computer and communications security, CCS 2007, Alexandria, Virginia, USA, October 28-31, 2007* (S. 552–561). New York: ACM.

Shetty, N., Schwartz, G., Felegyhazi, M. & Walrund, J. (2009). Competitive cyber-insurance and internet security. In *Proceedings of the eighth workshop on economics of information security (WEIS)*.

Sieber, U. (1999a). Die Verantwortlichkeit von Internet-Providern im Rechtsvergleich. *ZUM*, 196–213.

Sieber, U. (1999b). Internationales Strafrecht im Internet. Das Territorialitätsprinzip der §§ 3, 9 StGB im globalen Cyberspace. *NJW*, 2065–2073.

Sieber, U. (1999c). *Verantwortlichkeit im Internet: technische Kontrollmöglichkeiten und multimediarechtliche Regelungen. Zugleich eine Kommentierung von § 5 TDG und § 5 MDStV*. München: Beck.

Sieber, U. (2001). Die Bekämpfung von Hass im Internet. Technische, rechtliche und strategische Grundlagen für ein Präventionskonzept. *ZRP*, 97–103.

Sieber, U. (2008). Compliance-Programme im Unternehmensstrafrecht: ein neues Konzept zur Kontrolle von Wirtschaftskriminalität. In U. Sieber, G. Dannecker, U. Kindhäuser, J. Vogel & T. Walter (Hrsg.), *Strafrecht und Wirtschaftsstrafrecht* (S. 449–484). Köln: Heymann.

Sieber, U. (2009). Sperrverpflichtungen gegen Kinderpornografie im Internet. *JZ*, 653–662.

Simitis, S. (2009). Der EuGH und die Vorratsdatenspeicherung oder die verfehlte Kehrtwende bei der Kompetenzregelung. *NJW*, 1782–1786.

Spindler, G. (2004). Hyperlinks und ausländische Glücksspiele – Karlsruhe locuta causa finita? *GRUR*, 724–729.

Spindler, G. (2010). Online-Spiele auf dem Prüfstand des Gewerberechts. Zur Anwendbarkeit der §§ 33c, 33d GewO auf Online-Spiele. *K & R*, 450–458.

Spitzner, L. (2003). The honeynet project: Trapping the hackers. *IEEE Security & Privacy*, *1* (2), 15–23.

Spoenle, J. (2010). Underground economy. In M. Bellini, P. Brunst & J. Jähnke (Hrsg.), *Current issues in IT security* (S. 67–79). Berlin: Duncker & Humblot.

Steidle, R. & Pordesch, U. (2008). Im Netz von Google. Web-Tracking und Datenschutz. *DuD*, *35* (5), 324–329.

Stock, B., Göbel, J., Engelberth, M., Freiling, F. C. & Holz, T. (2009). Walowdac — Analysis of a peer-to-peer botnet. In *Proceedings 2009 european conference on computer and network defense (EC2ND)* (S. 13-20). New York: IEEE.

Stone-Gross, B., Cova, M., Cavallaro, L., Gilbert, B., Szydlowski, M., Kemmerer, R. A. et al. (2009). Your botnet is my botnet: analysis of a botnet takeover. In E. Al-Shaer, S. Jha & A. D. Keromytis (Hrsg.), *Proceedings of the 2009 ACM conference on computer and communications security, CCS 2009, Chicago, Illinois, USA, November 9-13, 2009* (S. 635–647). New York: ACM.

Stree, W. & Hecker, B. (2010). Kommentierung der §§ 303 ff. StGB. In A. Schönke, H. Schröder & A. Eser (Hrsg.), *Strafgesetzbuch. Kommentar* (28. Aufl.). München: Beck.

Stuckenberg, C.-F. (2006). Zur Strafbarkeit von »Phishing«. *ZStW*, *118*, 878–912.

Stuckenberg, C.-F. (2010). Viel Lärm um nichts? – Keine Kriminalisierung der »IT-Sicherheit« durch § 202c StGB. *wistra*, 41–46.

Suerbaum, J. (2010). Kommentierung der Art. 91a ff. GG. In V. Epping & C. Hillgruber (Hrsg.), *Beck'scher Online-Kommentar. Grundgesetz* (8. Aufl.). München: Beck.

Symantec. (2009). *Symantec global Internet security threat report.* Verfügbar unter http://www4.symantec.com/Vrt/wl?tu_id=gCGG1239137894536408O2

Tanenbaum, A. (1990). *Structured computer organisation* (3. Aufl.). Englewood Cliffs: Prentice Hall.

Thomas, R. & Martin, J. (2006). The underground economy: Priceless. *The USENIX Magazine*, *31* (6), 7–16.

Tiedemann, K. (1986). Die Bekämpfung der Wirtschaftskriminalität durch den Gesetzgeber. Ein Überblick aus Anlaß des Inkrafttretens des 2 WiKG am 1.8.1986. *JZ*, 865–874.

Többens, H. W. (2000). Wirtschaftsspionage und Konkurrenzausspähung in Deutschland. *NStZ*, 505–512.

Turing, A. M. (1936). On computable numbers, with an application to the Entscheidungsproblem. *Proc. London Math. Soc.*, *2* (42), 230–265. (See also correction Turing, 1937)

Turing, A. M. (1937). On computable numbers, with an application to the Entscheidungsproblem, A correction. *Procedings of the London Mathematical Society*, *43* (2), 544–546.

United Nations. (2010a). *Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime (working paper prepared by the secretariat).* Verfügbar unter http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_9/V1050382e.pdf

United Nations. (2010b). *Report of the twelfth United Nations congress on crime prevention and criminal justice.* Verfügbar unter http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_18/V1053828e.pdf

Valerius, B. (2003). Das globale Unrechtsbewusstsein. Oder – zum Gewissen im Internet. *NStZ*, 341–346.

Valerius, B. (2004). *Ermittlungen der Strafverfolgungsbehörden in den Kommunikationsdiensten des Internet.* Berlin: Logos.

Valerius, B. (2007a). Ermittlungsmaßnahmen im Internet. *JR*, 275–280.

Valerius, B. (2007b). Stalking: Der neue Straftatbestand der Nachstellung in § 238 StGB. *JuS*, 319–324.

Valerius, B. (2008). Zur Bedeutung des § 99 StPO im Zeitalter des Internets. Ein Plädoyer für eine Revision der §§ 99 ff. StPO. In E. Hilgendorf (Hrsg.), *Dimensionen des IT-Rechts.* Berlin: Logos.

Vec, M. (2002). Internet, Internationalisierung und nationalstaatlicher Rechtsgüterschutz. *NJW*, 1535–1539.

Vega, V. & Malamuth, N. M. (2007). Predicting sexual aggression: The role of pornography in the context of general and specific risk factors. *Aggressive Behaviour*, *33*, 104–117.

Vetter, J. (2002). *Gesetzeslücken bei der Internetkriminalität.* Hamburg: Dr. Kovač.

Vitzthum, W. (Hrsg.). (2007). *Völkerrecht* (4. Aufl.). Berlin: De Gruyter.

VMWare Inc. (2009). *VMWare ESX Server: Platform for virtualizing servers, storage and networking.* Verfügbar unter http://www.vmware.com/pdf/esx_datasheet.pdf

Vogel, J. (2004). *Einflüsse des Nationalsozialismus auf das Strafrecht.* Berlin: BWV.

Vogel, J. (2010). Kommentierung der §§ 242 ff. StGB. In H. W. Laufhütte, R. Rissing-van Saan & K. Tiedemann (Hrsg.), *Strafgesetzbuch: Leizpiger Kommentar. Band 8: §§ 242 bis 262* (12. Aufl.). Berlin: De Gruyter.

Vogel, J. (in Druck). Kommentierung der Art. 82 ff. AEUV. In E. Grabitz, M. Hilf & M. Nettesheim (Hrsg.), *Das Recht der Europäischen Union.* München: Beck.

Vogel, J. & Brodowski, D. (2009). Anmerkung zu OLG Hamburg StV 2009, 630. *StV*, 630–635.

Vömel, S., Holz, T. & Freiling, F. C. (2010). *I'd like to pay with your visa card: an illustration of illicit online trading activity in the underground economy* (Bericht Nr. TR-2010-004). Universität Mannheim, Institut für Informatik.

Wagner, E. (2008). Schutz der Privatheit – Informationsgesellschaft ohne Tabu? *DuD*, 736–740.

Wall, D. (2007). *Cybercrime*. Cambridge: Polity Press.

Wall, D. (2010). The organization of cybercrime and organized cybercrime. In M. Bellini, P. Brunst & J. Jähnke (Hrsg.), *Current issues in IT security* (S. 51–66). Berlin: Duncker & Humblot.

Warntjen, M. (2007). Die verfassungsrechtlichen Anforderungen an eine gesetzliche Regelung der Online-Durchsuchung. *JURA*, 581–585.

Weber, U. (1976). *Der strafrechtliche Schutz des Urheberrechts*. Tübingen: Mohr Siebeck.

Weichert, T. (2007). Bürgerrechtskonforme Bekämpfung der Computerkriminalität. *DuD*, 590–594.

Weidemann, M. (2010). Kommentierung der §§ 303 ff. StGB. In B. von Heintschell-Heinegg (Hrsg.), *Beck'scher Online-Kommentar. Strafgesetzbuch* (13. Aufl.). München: Beck.

Werthebach, E., Kersten, U., Nehm, K., Riotte, W., Matthias, K.-H. & Ritsert, R. (2010). *Kooperative Sicherheit: Die Sonderpolizeien des Bundes im föderalen Staat. Bericht und Empfehlungen der Kommission »Evaluierung Sicherheitsbehörden«*. Verfügbar unter http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/Sicherheit/Bundespolizei/werthebach_1.pdf

Wilson, D., Patterson, A., Powell, G. & Hembury, R. (2006). *Fraud and technology crimes. Findings from the 2003/04 british crime survey, the 2004 offending, crime and justice survey and administrative sources*. Home Office. Verfügbar unter http://www.homeoffice.gov.uk/rds/pdfs06/rdsolr0906.pdf (Online Report 09/06)

Wimmer-Leonhardt, S. (2007). Softwarepatente – eine »Never-Ending-Story«. *Wettbewerb in Recht und Praxis*, 273–281.

Wolff, H. (2008). Kommentierung der §§ 33 ff. StGB. In H. W. Laufhütte, R. Rissing-van Saan & K. Tiedemann (Hrsg.), *Strafgesetzbuch: Leizpiger Kommentar. Band 10: §§ 284 bis 305a* (12. Aufl.). Berlin: De Gruyter.

Wondracek, G., Holz, T., Platzer, C., Kirda, E. & Kruegel, C. (2010). Is the Internet for porn? An insight into the online adult industry. In *Proceedings of the ninth workshop on the economics of information security (WEIS)*.

Wright, C., Kleiman, D. & Sundhar R.S., S. (2008). Overwriting hard drive data: The great wiping controversy. In R. Sekar & A. K. Pujari (Hrsg.), *Information systems security, 4th international conference, ICISS 2008, Hyderabad, India, December 16-20, 2008. proceedings* (S. 243–257). Berlin: Springer.

Yuan, M. Y. (2006). A better copyright system? comparing welfare of indefinitely renewable copyright versus fixed-length copyright. *Economics of Innovation and New Technology*, *15*, 519–542.

Završnik, A. (2010). Criminal justice systems' (over)reactions to IT security threats. In M. Bellini, P. Brunst & J. Jähnke (Hrsg.), *Current issues in IT security* (S. 113–135). Berlin: Duncker & Humblot.

Zhuge, J., Holz, T., Song, C., Guo, J., Han, X. & Zou, W. (2008). Studying malicious websites and the underground economy on the chinese web. In *Proceedings of the seventh workshop on the economics of information security (WEIS)*.

Zöller, M. A. (2010). Willkommen in Absurdistan. Neue Straftatbestände zur Bekämpfung des Terrorismus. *GA*, 607–621.

Abkürzungsverzeichnis

a.A.	andere Auffassung
abl.	ablehnend
AblEG	Amtsblatt der Europäischen Gemeinschaften
AblEU	Amtsblatt der Europäischen Union
Abs.	Absatz
ACM	*Association for Computing Machinery*
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AG	Amtsgericht
Alt.	Alternative
Anm.	Anmerkung
Art.	Artikel
BDSG	Bundesdatenschutzgesetz
Beschl.	Beschluss
Bespr.	Besprechung
BGB	Bürgerliches Gesetzbuch
BGBl	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHSt	Entscheidungen des Bundesgerichtshofs in Strafsachen
BKAG	Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten
BR-Drs.	Bundesrats-Drucksache
BSI	Bundesamt für Sicherheit in der Informationstechnologie
BT-Drs.	Bundestags-Drucksache
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
ca.	*circa*
CD	*Compact Disc*
CERT	*Computer Emergency Response Team*
CR	Computer und Recht
CSI	*Crime Scene Investigation*
d.h.	das heißt
DDoS	*Distributed Denial of Service*
DNS	*Domain Name System*
DoS	*Denial of Service*
DRiZ	Deutsche Richterzeitung
DSL	*Digital Subscriber Line*
DuD	Datenschutz und Datensicherheit
DVD	*Digital Versatile Disc*
EGMR	Europäischer Gerichtshof für Menschenrechte

EJN	Europäisches Justizielles Netz
EMRK	Konvention zum Schutze der Menschenrechte und Grundfreiheiten
endg.	endgültig
EPÜ	Europäisches Patentübereinkommen
etc.	*et cetera*
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
f.	folgende
FBI	*Federal Bureau of Investigation*
ff.	fortfolgende
Fn.	Fußnote
GG	Grundgesetz
GI	Gesellschaft für Informatik e.V.
GPS	*Global Positioning System*
GR	Goldtammer's Archiv für Strafrecht
GRC	Charta der Grundrechte der Europäischen Union
GRUR	Gewerblicher Rechtsschutz und Urheberrecht
GVG	Gerichtsverfassungsgesetz
HRRS	Online-Zeitschrift für Höchstrichterliche Rechtsprechung im Strafrecht
Hrsg.	Herausgeber
HTTP	*Hypertext Transport Protocol*
i.d.R.	in der Regel
i.S.d.	im Sinne des
i.V.m.	in Verbindung mit
ICJ	*International Court of Justice*
IEEE	*Institute of Electrical and Electronics Engineers*
inkl.	inklusive
insb.	insbesondere
IP	*Internet Protocol*
IRC	*Internet Relay Chat*
IRG	Gesetz über die internationale Rechtshilfe in Strafsachen
IT	Informationstechnologie
jew.	jeweils
JMStV	Staatsvertrag über den Schutz der Menschenwürde und den Jugendschutz in Rundfunk und Telemedien
JR	Juristische Rundschau
JURA	Jura. Juristische Ausbildung
JuS	Juristische Schulung
JZ	Juristenzeitung

K&R	Kommunikation und Recht
KG	Kammergericht
KOM	Kommissionsdokument
krit.	kritisch hierzu
LG	Landgericht
m.	mit
m.w.N.	mit weiteren Nachweisen
MMR	Multimedia und Recht
MP3	*MPEG Audio Layer 3*
NJW	Neue Juristische Wochenschrift
NStZ	Neue Zeitschrift für Strafrecht
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
OWiG	Gesetz über Ordnungswidrigkeiten
PatG	Patentgesetz
PC	*Personal Computer*
PDF	*Portable Document Format*
PostG	Postgesetz
Rdn.	Randnummer
RGSt	Entscheidungen des Reichsgerichts in Strafsachen
RiStBV	Richtlinien für das Strafverfahren und das Bußgeldverfahren
RiVASt	Richtlinien für den Verkehr mit dem Ausland in strafrechtlichen Angelegenheiten
Rs.	Rechtssache
S.	Seite
s.	siehe
SDÜ	Schengener Durchführungsübereinkommen
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StraFo	Strafverteidiger-Forum
StV	Strafverteidiger
TKG	Telekommunikationsgesetz
TKÜV	Telekommunikations-Überwachungsverordnung
TMG	Telemediengesetz
UAbs.	Unterabsatz
UN	Vereinte Nationen
UrhG	Gesetz über Urheberrecht und verwandte Schutzrechte
Urt.	Urteil
USA	Vereinigte Staaten von Amerika
USB	*Universal Serial Bus*
usw.	und so weiter

UWG	Gesetz gegen den unlauteren Wettbewerb
v.	vom
VGH	Verwaltungsgerichtshof
vgl.	vergleiche
wistra	Zeitschrift für Wirtschafts- und Steuerstrafrecht
WLAN	*Wireless Local Area Network*
WpHG	Gesetz über den Wertpapierhandel
z.T.	zum Teil
ZIS	Zeitschrift für Internationale Strafrechtsdogmatik
ZKDSG	Gesetz über den Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten
ZRP	Zeitschrift für Rechtspolitik
ZStW	Zeitschrift für die gesamte Strafrechtswissenschaft
ZUM	Zeitschrift für Urheber- und Medienrecht
zutr.	zutreffend