Einleitung

In den vergangenen Jahren haben sich sowohl Tat- als auch Tätertypologien grundlegend weiterentwickelt. Täter nutzen zunehmend modernste Technik; neuartige Kriminalitätsphänomene ersetzen immer mehr klassische Deliktsformen.[1] Die Bandbreite der so entstandenen Deliktsarten ist beachtlich. Sie reicht von der Adaption bereits seit langem bekannter Straftaten (z. B. eBay-Betrugsfälle[2]) über technisch hoch anspruchsvolle Spezialdelikte (z. B. Eindringen in Computersysteme[3] oder den Einsatz von Botnetzen[4]) bis hin zu Angriffen auf kritische Infrastrukturen (z. B. im Cyberterrorismus).

Praktiker, die mit der Bekämpfung der Internetkriminalität befasst sind, stehen daher vor **neuen Herausforderungen**.[5] Diese betreffen zum einen die technischen Aspekte, zum anderen aber auch die rechtliche Handhabung der neuen Materie. Auf der praktischen Seite stellen sich zum Beispiel Probleme, wie sich digitale Beweismittel heute überhaupt auffinden lassen. In den Weiten des Internet lassen sich vielfältige Kommunikationsformen nutzen, etwa E-Mail-Verkehr oder Chaträume, die sich nur schwer überwachen lassen. Selbst falls ein solcher Dienst bereits in den Fokus von Ermittlungsbehörden gerückt sein sollte, lassen sich Maßnahmen mitunter technisch umgehen.[6] Die Internationalität des Netzes einerseits und die dem entgegengesetzte Beschränkung rechtlicher Maßnahmen auf das eigene nationale Territorium tun ihr Übriges, um die Verfolgung zu erschweren. Als ob dies nicht bereits genug wäre, lassen sich Nachrichten mit Hilfe von Verschlüsselungstechnologie so umformen, dass sie – selbst wenn sie abgefangen werden können – nicht ausgewertet werden können.

Die notwendigen **Tatwerkzeuge** dazu stehen im Internet frei zur Verfügung. Je nach gewünschtem Einsatzgebiet lassen sich Produkte zum Brechen von Passwörtern (oder gleich fertige Passwortlisten), Angriffswerkzeuge für die Sabotage von Servern ebenso herunterladen wie Tools, mit denen Kopierschutzmaßnahmen umgangen werden können.[7] Die Software ist größtenteils frei verfügbar und setzt meist kein besonderes Fachwissen voraus. Täter können daher nicht mehr lediglich raffinierte und technologieerfahrene Personen sein, sondern bereits Jugendliche, die ihre ersten eigenen Schritte im Internet unternehmen. Hinzu kommt, dass Schäden distanziert mittels Mausklick produziert werden können und sich Täter und Opfer nicht gegenüberstehen müssen. Psychologische Hemmschwellen sind daher häufig weit herabgesetzt oder gar nicht mehr vorhanden.

Eine **Kontrolle** ist demgegenüber kaum möglich. Zwar ist zu beobachten, dass eine immer weitergehende **Kriminalisierung von Vorbereitungshandlungen**[8]

1 Vgl. hierzu die Pressemitteilung des BKA vom 28.3.2008 zu den aktuellen Herausforderungen der Kriminalitätsbekämpfung, http://www.bka.de/pressemitteilungen/2008/pm080328.html [März 2009]. Danach sind sowohl bei der allgemeinen Informations- und Kommunikationskriminalität als auch speziell bei Straftaten mit dem Tatmittel Internet deutliche Zuwächse zu verzeichnen. Vgl. auch *Bär*, Handbuch zur EDV-Beweissicherung, Stuttgart 2007, S. 15.

2 Vgl. dazu ausführlich: Rn. 200 ff.

3 Vgl. dazu Rn. 89 ff.

4 Zu den Konsequenzen für die Strafverfolgung vgl. Rn. 38 ff. sowie *Gercke*, MMR 2008, 296.

5 Vgl. dazu grundlegend: Kap. 1.

6 So haben in der Vergangenheit einige Terroristen per E-Mail kommuniziert, ohne dass die Mails tatsächlich jemals das System verlassen hätten. Zu dieser „Al Qaeda-Masche" siehe näher unten Rn. 921.

7 Vgl. dazu Rn. 16.

8 Zur Vorfeldkriminalisierung vgl. Rn. 17.

eingeführt wird (z. B. der umstrittene „Hackerparagraph", § 202c StGB) oder darüber debattiert wird, wie der Zugriff auf als gefährlich oder unerwünscht angesehene Informationen verhindert werden kann (z. B. mit Hilfe von **Sperrmaßnahmen gegen kinderpornographische Inhalte im Internet**). Technisch sind derartige Vorgaben jedoch wirkungslos, da sie auf das nationale Territorium beschränkt bleiben. Im Einzelfall können sie sogar ins Gegenteil umschlagen.[9] Um überhaupt wirksam Internetstraftaten bekämpfen zu können, ist es daher erforderlich, Maßnahmen nicht nur auf nationaler Ebene zu entwickeln, sondern Vorgaben international zu harmonisieren. Insbesondere durch die Cybercrime Konvention des Europarates sowie durch den Rahmenbeschluss über Angriffe auf Informationssysteme ist auf internationaler Ebene bislang viel erreicht worden.[10] Diesen Entwicklungen sowie allgemein den Herausforderungen bei der Bekämpfung der Internetkriminalität widmen sich daher näher die ersten beiden Kapitel dieses Buches.

Das dritte Kapitel befasst sich konkret mit den wichtigsten **materiellen Vorgaben** des Internetstrafrechts. Aufgrund einer zunehmenden Digitalisierung fällt eine Abgrenzung zwischen klassischem Strafrecht und Internetstrafrecht immer schwerer, denn viele Straftaten lassen sich mit Hilfe des Internet begehen. Gleichwohl lassen sich die Normen an den Kategorien unterscheiden, die auch in der Cybercrime Konvention gewählt wurden:

- Die so genannten **CIA-Delikte** betreffen nicht den amerikanischen Nachrichtendienst, sondern bezeichnen Straftaten gegen die Vertraulichkeit, Integrität und Verfügbarkeit von Computerdaten und -systemen (confidentiality, integrity, availability). Sie stellen den Kernbereich der Computerstraftaten im engeren Sinne dar.
- **Computerbezogene Straftaten** sind eigentlich Auffangdelikte. Sie sollen verhindern, dass eine Strafbarkeit alleine deshalb entfällt, weil eine Tat nicht gegen die Freiheit des menschlichen Willens gerichtet ist, sondern gegen die automatisierte Entscheidung eines Computers. Daher fallen insbesondere die Vorschriften des Computerbetrugs und der Verfälschung beweiserheblicher Daten in diese Kategorie. Betrugsfälle bei Online-Auktionen haben in der Presse immer wieder die Aufmerksamkeit auf sich gezogen.
- Bei der Bekämpfung der **inhaltsbezogenen Straftaten** geht es nicht um eine spezielle Handlungsform. Vielmehr bietet das Internet Vorteile, wenn es darum geht, bestimmte – vom Rechtssystem nicht erwünschte – Inhalte zu erlangen und weiter zu verbreiten. Insbesondere der Kampf gegen die Kinderpornographie hat zu einer weit ausgedehnten Strafbarkeit geführt.
- Als vierte Kategorie sind die Delikte zu nennen, die im Zusammenhang mit der **Verletzung von Schutzrechten** stehen. Insbesondere der fortwährende Kampf zwischen der Industrie, die ihre Inhalte – zum Teil mit technischen Schutzmaßnahmen – vor einer illegalen Verbreitung zu schützen sucht und Anwendern, die derartige Einschränkungen unterbinden möchten, haben dazu geführt, dass die Delikte dieser Kategorie immer wieder in den Fokus der allgemeinen Aufmerksamkeit gelangt sind. Weltumspannende Tauschbörsen scheinen dabei einen unbegrenzten und unkontrollierbaren Zugang zu neuesten Filmen und Musiktiteln zu ermöglichen.

Bei der Aufklärung von Fällen in allen vier Kategorien spielt zunächst der **Provider** die wichtigste Rolle. Er ist zum Beispiel die zentrale Anlaufstelle, wenn es darum geht, eine IP-Adresse zu ermitteln, die den Anschluss des Täters identifi-

9 Sperrlisten, mit denen in mehreren Ländern kinderpornographische und sonstige dort illegale Inhalte gesperrt werden sollen, sind zum Beispiel an die Öffentlichkeit gelangt. Mit Hilfe dieser Listen lassen sich die unerwünschten Inhalte unmittelbar aufrufen, selbst wenn sie in Suchmaschinen nicht zugänglich sein sollten. Zu den rechtlichen Problemen der Sperrung von Internetinhalten, vgl. *Sieber/Nolde,* Sperrverfügungen im Internet, Berlin 2008.

10 Vgl. zu den internationalen Harmonisierungsbestrebungen: Kap. 2.

zieren kann. Bei illegalen Inhalten kann der Provider unmittelbar tätig werden und ein weiteres Angebot unterbinden, auch wenn der eigentliche Urheber nicht ermittelbar ist. Insbesondere im Bereich von technischen Kontrollmaßnahmen zur Unterbindung von Urheberrechtsverletzungen sowie von Zugriffen auf kinderpornographische und terroristische Inhalte wird die Einbeziehung der Provider gegenwärtig intensiv diskutiert.

Die unmittelbar daran anschließende Frage nach dem Umfang einer **Haftung von Providern** spielt demgemäß eine große Rolle. Zwar gibt das TMG eine klare Regelung für eine gestaffelte Verantwortlichkeit vor, in der Praxis werden diese Grenzen aber durch die Rechtsprechung zunehmend verwischt, z. B. durch die Anwendung der Störerhaftung. Insbesondere in Konstellationen, in denen der eigentliche Täter nur schwer zu ermitteln oder zu fassen ist, z. B. bei offenen drahtlosen Netzwerken oder bei frei zugänglichen Meinungsforen, scheinen einige Entscheidungen vom Wunsch getragen zu sein, wenigstens *irgendjemanden* zur Verantwortung ziehen zu können.[11] Das vierte Kapitel setzt sich daher intensiv mit der Frage der Verantwortlichkeit der Diensteanbieter und den unterschiedlichen Ansichten der Rechtsprechung zu verschiedenen Angebotsformen auseinander.

Abschließend werden im fünften Kapitel die Fragen des Internetstrafprozessrechts behandelt. Dies betrifft zunächst den Zugriff auf Bestandsdaten, Verkehrsdaten und Inhaltsdaten. Bereits hierbei zeigen sich eine Reihe von **prozessualen Fragen,** die hohe Praxisrelevanz besitzen und dennoch bis jetzt nicht zufriedenstellend gelöst sind. Aus dem Bereich der Bestandsdaten sei zum Beispiel die Frage nach der richtigen Norm für Zugriffe auf Name und Adresse des Nutzers einer dynamischen IP-Adresse genannt. Im Bereich der Verkehrsdaten bleiben nach der Einführung der Vorratsdatenspeicherung und dem Urteil des Bundesverfassungsgerichts ebenfalls viele Fragen offen. Bei den sensiblen Inhaltsdaten schließlich schien zeitweilig beinahe mehr ungeklärt als gesichert: angefangen bei der richtigen Grundlage für Zugriffe auf gespeicherte E-Mails über die Möglichkeiten, verschlüsselte Daten im Wege eines heimlichen Online-Zugriffs oder einer Quellen-Telekommunikationsüberwachung zu erlangen bis hin zum Einsatz von Passwörtern, die in anderem Zusammenhang ermittelt wurden, stellen sich vielfältigste Fragen. Zudem stehen den Nutzern durch vielfältige Umgehungs- und Verschleierungsmöglichkeiten Optionen zur Verfügung, Ermittlungen deutlich zu erschweren oder sogar unmöglich zu machen.

Doch das Internet steht nicht nur einseitig Straftätern zur Verfügung. Auch die Strafverfolgungsbehörden können es für ihre Zwecke einsetzen – und tun dies auch erfolgreich. Eine **Nutzung durch Strafverfolger** ist zum Beispiel bei Fahndungsaufrufen im Internet möglich. Anders als klassische Plakate können Internetfahndungen jederzeit aktualisiert und auch um weitere multimediale Elemente ergänzt werden, z. B. um Überwachungsvideos, alternative Bildentwürfe etc. Die Möglichkeiten, die sich hier mit Hilfe neuer Medien bieten, werden gegenwärtig noch nicht ausgereizt,[12] die Erfolge um die Fahndung nach „Vico“ erscheinen aber aussichtsreich.[13]

Ein weiterer Vorteil, der sich bei der Bekämpfung der Internetkriminalität bietet, ist die Tatsache, dass Täter trotz scheinbarer Anonymität faktisch viel mehr Spuren hinterlassen, als gemeinhin angenommen wird. Diese lagern zum Teil

11 Vgl. hierzu näher *Brunst,* Anonymität im Internet, Berlin 2009, S. 370 ff. m. w. N.

12 Ein besonderes Problem bei der Internetfahndung ist die Aktivität, die von Nutzern verlangt wird, um das Fahndungs“plakat“ anzusehen. Vgl. hierzu näher unten Rn. 940 ff. Andere Formen des Einsatzes neuer Medien, wie z. B. die SMS-Fahndung, waren in der Vergangenheit ebenfalls an der fehlenden Beteiligungsbereitschaft gescheitert. Zur Einstellung der SMS-Fahndung, vgl. etwa http://www.golem.de/0501/35424.html.

13 Vgl. hierzu näher Rn. 940 ff.

bei Providern und erlauben die Rückverfolgung von Tätern. Zum Teil können diese auch auf den Rechnern der Tatverdächtigen wiederhergestellt werden, selbst wenn sie scheinbar bereits gelöscht waren. Es ist daher davon auszugehen, dass Computerforensik – und auch Gegenmaßnahmen, sog. Anti-Forensik – in der Zukunft eine noch größere Bedeutung erlangen werden.

Kapitel 1: Herausforderungen bei der Bekämpfung der Internetkriminalität

Literatur: *Bär,* Öffentlichkeitsfahndung im Internet, CR 1997, 422 ff.; *ders.*, Wardriver und andere Lauscher – Strafrechtliche Fragen im Zusammenhang mit WLAN MMR 2005, 434 ff.; *Bäumler*, AN-ON Projekt in Schleswig-Holstein zur Anonymität im Internet, DuD 2001, 316; *Beck/Kreißig,* Tauschbörsen-Nutzer im Fadenkreuz der Strafverfolgungsbehörden, NStZ 2007, 304 ff.; *Bellare/Rogaway*, Introduction to Modern Cryptography, 2005; *Beulke/Meininghaus*, Anmerkung zum Urteil des BGH zur heimlichen Online-Durchsuchung, StV 2007, 63 ff.; *Bizer*, Kryptokontroverse. Vertraulichkeit in der Telekommunikation, DuD 1996, 5 ff.; *ders.*, Rechtliche Bedeutung der Kryptographie, DuD 1997, 203 ff.; *Böckenförde*, Ermittlungen im Netz, 2003; *Boese*, Die verfassungsrechtlichen Grundlagen des Satzes „Nemo tenetur se ipsum accusare", GA 2002, 98 ff.; *ders.* Nemo tenetur – Rekonstruktion eines Verfahrensgrundsatzes NStZ 1997, 361 ff. *ders.*, Nemo tenetur – Rekonstruktion eines Verfahrensgrundsatzes 415 ff.; *Bohn/Coroama/Langheinrich/Mattern/Rohs,* Living in a World of Smart Everyday Objects – Social, Economic, and Ethical Implications, Journal of Human and Ecological Risk Assessment, Vol. 10, S. 763 ff.; *Borges/Stuckenberg/Wegener*, Bekämpfung der Computerkriminalität, Das 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität, DuD 2007, 275 ff.; *Bräuer*, Anmerkung zu „Identitätsdiebstahl" von Karl Rihaczek, DuD 11/2004, DuD 2005, 24; *Breyer,* Die Cyber-Crime-Konvention des Europarates, DuD 2001, 592 ff.; *ders.*, Vorratsdatenspeicherung von IP-Adressen durch Access Provider, DuD 2003, 491 ff.; *Buermeyer,* Die „Online-Durchsuchung". Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme, HRRS 2007, 154 ff.; *Caronni*, Anonymität – Die Kehrseite der Medaille, DuD 1998, 1 ff.; *Casey*, Digital Evidence and Computer Crime, 2004; *Claessens/Prenelle/Vandewalle*, Solutions for Anonymous Communication on the Internet, in Security Technology, IEEE 33rd Annual International Camahan Conference, 1999, S. 298 ff.; *Cornelius*, Zur Strafbarkeit des Anbietens von Hackertools. Was nach dem 41. Strafrechtsänderungsgesetz noch für die IT-Sicherheit getan werden darf, CR 2007, 682 ff.; *Diehl*, Kryptographiegesetzgebung im Wandel. Von begrenzten Schlusselängen zur Schlusselherausgabe, DuD 2008, 243 ff.; *Dietz/Richter*, Netzzugänge unter Internet Service Providern, CR 1998, 528 ff.; *Dix*, Regelungsdefizite der Cyber-CrimeKonvention und der E-TKÜV, DuD 2001, 589; *ders.*, Vorratsspeicherung von IP-Adressen. Anmerkung zur Bewertung der Praxis von der T-Online International AG durch das Regierungspräsidium Darmstadt, DuD 2003, 234 ff.; *Dobbertin*, Digitale Fingerabdrücke Sichere Hashfunktionen für digitale Signaturen, DuD 1997, 82 ff.; *Dornfest/Bausch/Calishain*, Google Hacks: Tips & Tools for Finding and Using the World's Information, 2006; *Eichelberger*, Das Blockieren einer Internet-Seite als strafbare Nötigung. Zugleich eine Besprechung von AG Frankfurt am Main, Urt. v. 1.7.2005 – 991 Ds 6100 Js 226314/01 (Online-Demo) DuD 2006, 490 ff.; *Ernst*, Das neue Computerstrafrecht, NJW 2007, 2661 ff.; *ders./Seichter*, Die Störerhaftung des Inhabers eines Internetzugangs, ZUM 2007, 513 ff.; *Federrath/Golembiewski*, Speicherung von Nutzungsdaten durch Anonymisierungdienste im Internet. Welche strafprozessualen Vorschriften zur Überwachung der Telekommunikation sind auf Anonymisierungsdienste anwendbar?, DuD 2004, 486 ff.; *ders./Hansen*, Anonym – total (l)egal?, DuD 2003, 126; *Fox/Kelm*, Computer-Forensik, DuD 2004, 491; *Gajek/Schwenk/Wegener*, Identitätsmissbrauch im Onlinebaning, DuD 2005, 639 ff.; *Gercke*, Die Entwicklung der Rechtsprechung zum Internetstrafrechts im Jahr 2003, ZUM 2005, 443 ff.; *ders.*, Die Entwicklung des Internetstrafrechts im Jahr 2004, ZUM 2005, 612 ff.; *ders.*, Die Entwicklung des Internetstrafrechts im Jahr 2005, ZUM 2006, 284 ff.; *ders*, Die Entwicklung des Internetstrafrechts im Jahr 2007, ZUM 2008, 545 ff.; *ders.,* Update Strafrecht, in Taeger/Wiebe, Von AdWords bis Social Networks – Neue Entwicklungen im Informationsrecht, 2008, S. 431 ff.*; ders.*, The Slow Awake of a Global Approach Against Cybercrime, CRi 2006, 140 ff.; *ders.*, National, Regional and International Approaches in the Fight Against Cybercrime, CRi 2008, 7 ff.; *ders.*, Die Speicherung von Nutzungsdaten. Zwischen effektiver Kriminalitätsbekämpfung und Privatsphäre, DuD 2002, 477 ff.; *ders.*, Anmerkung zum Urteil des AG Frankfurt zur Strafbarkeit einer „Online-Demo", MMR 2005, 868 f.*; ders.,* Die Bekämpfung der Internetkriminalität als

Herausforderung für die Strafverfolgungsbehörden, MMR 2008, 291 ff.; *ders.,* Heimliche Online-Durchsuchung: Anspruch und Wirklichkeit. Softwarebasierte Ermittlungsinstrumente zum heimlichen Zugriff auf Computerdaten, CR 2007, 245 ff.; *ders.*, Die Protokollierung von Nutzerdaten. Zu den Ermittlungsmaßnahmen gegen JAP nach § 100 g/h StPO, DuD 2004, 210 ff.; *ders.*, Einführung in das Internetstrafrecht, JA 2007, 839 ff.; *ders*., Die Strafbarkeit von „Phishing" und Identitätsdiebstahl. Eine Analyse der Reichweite des geltenden Strafrechts, CR 2005, 606 ff.; *ders*. Internet-related Identity Theft, 2007 – abrufbar unter: http://www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_ Technical_cooperation/CYBER/567%20port%20id-identity%20theft%20paper%20 22%20nov%2007.pdf; *ders.,* Die Cybercrime Konvention des Europarates. Bedeutung und Tragweite ihres völkerrechtlichen Einflusses auf das Straf- und Strafverfahrensrecht in Deutschland, CR 2004, 782 ff.; *ders.,* Analyse des Umsetzungsbedarfs der Cybercrime Konvention – Teil 1: Umsetzung im Bereich des materiellen Strafrechts, MMR 2004, 728 ff.; *ders.,* Analyse des Umsetzungsbedarfs der Cybercrime Konvention – Teil 2: Die Umsetzung im Bereich des Strafverfahrensrechts, MMR 2004, 801 ff.; *ders.*, The Slow Awake of a Global Approach Against Cybercrime, CRi 2006, 140 ff.; *ders*., National, Regional and International Approaches in the Fight Against Cybercrime, CRi 2008, 7 ff.; *Geschonneck*, Computer Forensik, 2006; *Gietl,* Störerhaftung für ungesicherte Funknetze – Voraussetzungen und Grenzen, MMR 2007, 630 ff.; *Gröseling/Höfinger,* Hacking und Computerspionage – Auswirkungen des 41. StrÄndG zur Bekämpfung der Computerkriminalität, MMR 2007, 549 ff.; *dies*, Computersabotage und Vorfeldkriminalisierung – Auswirkungen des 41. StrÄndG zur Bekämpfung der Computerkriminalität, MMR 2007, 626 ff.; *Grosskopf*, Anmerkung zum Urteil des LG Hamburg: Störerhaftung des Internetanschlussinhabers für Urheberrechtsverletzungen CR 2007, 122 ff.; *Gruhl*, Private Investigation im Bereich der IuK Kriminalität. Zulässigkeit und Verwertbarkeit der Sachverhaltsaufklärung durch Geschädigte oder Dritte, DuD 2005, 399 ff.; *Gusy*, Polizeirecht, 2006; *Hamm*, Kryptokontroverse, DuD 1997, 186 ff.; *Hansen/Pfitzmann*, Online-Durchsuchung, DRiZ, 2007, 225 ff.; *Heidrich*, Die T-Online-Entscheidung des RP Darmstadt und ihre Folgen, DuD 2003, 237 ff.; *Hilgendorf*, Gibt es ein „Strafrecht der Risikogesellschaft?" – Ein Überblick, NStZ 1993, 10 ff.; *Hoeren,* Das Internet für Juristen – eine Einführung, NJW 1995, 3295 ff.; *Hofmann*, Die Online-Durchsuchung – staatliches „Hacken" oder zulässige Ermittlungsmaßnahme?, NStZ, 2005, 121 ff.; *Hornung*, Anmerkung zum Beschluss des BGH zur heimlichen Online-Druchsuchung, CR 2007, 144 f.; *ders*. Ermächtigungsgrundlage für die Online-Durchsuchung. Verfassungsrechtliche Anforderung an und Grenzen für den heimlichen Zugriff auf IT-Systeme im Ermittlungsverfahren, DuD 2007, 575 ff.; *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1; *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, CRi 2006, 94 f.; *Huhn/Pfitzmann*, Technische Grundlagen jeder Kryptoregulierung, DuD 1996, 23 ff.; *Jahn/Kudlich,* Anmerkung zum Beschluss des BGH (Ermittlungsrichter) v. 25.11.2006 – 1 BGs 184/06 und v. 28.11.2006 – 1 BGs 186/2006, JR 2007, 57 ff.; *Kelm/Kossakowski*, Zur Notwendigkeit der Kryptographie. Warum die Praxis für Kryptographie und gegen Regulierung spricht, DuD 1997, 192 ff.; *Kelsey*, Hacking into International Humanitarian Law: The Principle of Distinction and Neutrality in the Age of Cyber Warfare, Michigan Law Review, Vol. 106, S. 1427 ff. *Kerr*, Searches and Seizutre in a Digital World, Harvard Law Review, Vol. 119; *Kitz*, Der Gewaltbegriff im Informationszeitalter und die strafrechtliche Beurteilung von Onlineblockaden, Zugleich Anmerkung zu OLG Frankfurt am Main, Beschluss vom 22. Mai 2006 – 1 Ss 319/05, ZUM 2006, 730 ff.; *Klewitz-Hommelsen*, Recht auf Anonymität? Oder Anspruch auf Transparenz?, DuD 2003, 159 ff.; *Knupfer* in Schriftenreihe der Strafverteidigervereinigung, Bd. 27, 139 ff.; *König*, Kinderpornographie im Internet, 2003; *Köpsell/Federrath/Hansen*, Erfahrungen mit dem Betrieb eines Anonymisierungsdienstes, DuD 2003, 139 ff.; *Köpsell/Miosga*, Strafverfolgung trotz Anonymität, Rechtliche Rahmenbedingungen und technische Umsetzung, DuD 2005, 403 ff.; *Kupfrian/Hoppen*, Datenverlust und Datenrettung. Technische Möglichkeiten und Grenzen, CR 2007, 819 ff.; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004; *Leutheusser-Schnarrenberger*, Vorratsdatenspeicherung – Ein vorprogrammierter Verfassungskonflikt, ZRP 2007, 9 ff.; *Lipson*, Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues, 2002; *Long/Skoudis/van Eijkelenborg* Google Hacking for Penetration Testers, 2005; *Meisel*, Die Erhebung von Kundendaten beim Kauf von Prepaid-Produkten, DuD 2004, 426 ff.; *Neumann,* Die elektronischen Schlapphüte kommen. Was soll, was kann und wozu nützt eine Online-Durchsuchung, DRiZ 2007, 226 ff.; *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005; *Nora/Minc*, Die Informatisierung der Gesellschaft, 1979; *Pätzel,* Das Internet als Fahndungs-

hilfsmittel der Strafverfolgungsbehörden, NJW 1997, 3131 ff.; *Peter*, Störer im Internet – Haften Eltern für Ihre Kinder, KR 2007, 371 ff.; *Rihaczek*, Identitätsdiebstahl, DuD 2004, 649; *Roessler*, PGP – „Kryptographie fürs Volk, DuD 1998, 377 ff.; *Roessler*, Anonymität im Internet, DuD 1998, 619 ff.; *Rost*, Zur gesellschaftlichen Funktion von Anonymität. Anonymität im soziologischen Kontext, DuD 2003, 155 ff.; *ders./Meints*, Authentisierung in Sozialsystemen. Identitytheft strukturell betrachtet, DuD 2005, 216 ff.; *Salgado*, Fourth Amendment Search and the Power of the Hash, Harvard Law Review, Vol. 119, S. 38 ff.; *Schaar/Landwehr*, Anmerkung zum Beschluss des BGH zur heimlichen Online-Durchsuchung, KR 2007, 202 ff.; *Schnabel*, Böse Zensur, guter Filter? – Urheberrechtliche Filterpflichten für Access-Provider, MMR 2008, 281 ff.; *Schneier,* Angewandte Kryptographie, 1996; *Schöttle*, Sperrverfügung im Internet: Machbar und verhältnismäßig?, KR 2007, 366 ff.; Seitz, Strafverfolgungsmassnahmen im Internet, 2004; *Soine*, Fahndung via Internet – 1. Teil, NStZ 1997, 166 ff.; *ders.*, Fahndung via Internet – 2. Teil, NStZ, 1997, 321 ff.; *Schreibauer/Hessel*, Das 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität, CR 2007, 616 ff.; *Schumann*, Das 41. StrÄndG zur Bekämpfung der Computerkriminalität, NStZ 2007, 675 ff.; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension – in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001; *Spiekermann*, Die Konsumenten der Anonymität. Wer nutzt Anonymisierungsdienste?, DuD 2003, 150 ff. *Steinhaus/Rosdale/de Pol*, Basiswissen Internet, 1999; *Teinbacher*, Strafbarkeit der Privatkopie von offensichtlich rechtswidrig hergestellten oder öffentlich zugänglich gemachten Vorlagen, GRUR 2008, 394 ff.; *Tinnefeld*, Online-Durchsuchung – Menschenrechte vs. virtuelle Trojaner, MMR 2007, 137 f.; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2005; *Valerius,* Der Weg zu einem sicheren Internet? Zum In-Kraft-Treten der Convention On Cybercrime, KR 2004, 513 ff.; *Wallsten*, Regulation and Internet Use in Developing Countries, 2002; *Warntjen*, Die verfassungsrechtlichen Anforderungen an eine gesetzliche Regelung der Online-Durchsuchung Jura 2007, 581 ff.; *Wigert*, Varying policy responses to critical information infrastructure protection (CIIP) in selected countries, Cybercrime and Security, IIB-1, S. 1 ff.; *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007; *Wolak/Finkelhor/Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005, S. 9, – abrufbar unter: http://www.missingkids.com/en_US/publications/NC144.pdf; *Willer/Hoppen*, Computerforensik – Technische Möglichkeiten und Grenzen CR 2007, 610 ff.

I. Einleitung

Für die Strafverfolgungsbehörden müssen eine Reihe von Rahmenbedingungen erfüllt sein, um Internetdelikte effektiv bekämpfen zu können.[1] Dazu zählen insbesondere: **1**

- Rechtliche Grundlagen im Bereich des materiellen Strafrechts und des Prozessrechts
- Adäquate Ausbildung und regelmäßiges Training
- Adäquate technische und personelle Ausstattung.

Die Gewährleistung der Rahmenbedingungen ist für Deutschland, ebenso wie für die übrigen europäischen Staaten insofern von zentraler Bedeutung, als der Transformationsprozess von den Industrie- zur **Informationsgesellschaften**[2] hier immer weiter voranschreitet.[3] Der Transformationsprozess ist dadurch gekennzeichnet, dass Information ebenso wie die zur Informationsvermittlung notwenige Informationstechnologie sowohl im wirtschaftlichen als auch im **2**

1 Zur Einführung in die Problematik vgl. *Gercke*, MMR 2008, 291 ff.

2 World Summit on the Information Society, Document WSIS-03/GENEVA/DOC/5-E, December 2003, abrufbar unter: http://www.itu.int/wsis/docs/geneva/official/poa.htm.

3 *Gercke*, JA 2007, 839.

gesellschaftlichen Bereich eine immer größere Rolle spielt.[4] Verdeutlichen lässt sich dies anhand der Popularität von Mobilkommunikation und Internetdiensten.[5] Ebenfalls kennzeichnend für die Informationsgesellschaft ist der **Transfer identitätsbezogener Elemente** in das Internet[6] – wie beispielsweise im Rahmen der derzeit besonders populären sozialen Netzwerke.[7]

1. Abhängigkeit der Gesellschaft von der Verfügbarkeit der Informationstechnologie

3 Mit dem damit einhergehenden Bedeutungszuwachs der Informationstechnologie sowohl im wirtschaftlichen, als auch im gesellschaftlichen Bereich geht eine zunehmende Abhängigkeit der Gesellschaft von der Kommunikationstechnologie einher.[8] Dies betrifft alle Bereiche, in denen Kommunikationstechnologie eingesetzt wird.[9] Der Umstand, dass Mobiltelefone, Kommunikationsnetze, Elektrizitätsversorgung, medizinische Geräte und Kraftfahrzeuge ohne eine funktionierende Informationstechnologie nicht genutzt werden können, verdeutlicht sowohl deren Stellenwert für die Gesellschaft, als auch das **Gefahrenpotential von Angriffen auf kritische Infrastruktur.**[10] Die zunehmende Vernetzung hat zu einer erheblichen Erweiterung der „kritischen Infrastruktur" geführt. Dass Angriffe auf kritische Informationsinfrastruktur erhebliche Auswirkungen auf die Gesellschaft und ihre Wirtschaft nach sich ziehen, wurde in den vergangenen Jahren mehrfach unter Beweis gestellt:

- **Angriffe auf Computersysteme in Estland**[11] im Jahr 2007 haben zur Folge gehabt, dass zentrale Internetdienste nicht verfügbar waren. Während der genaue Umfang der Beeinträchtigung nicht zuletzt aufgrund des vermuteten politischen Hintergrunds der Angriffe unterschiedlich dargestellt wird, besteht weitgehend Einigkeit darüber, dass die Angriffe die Verwundbarkeit der Informationsinfrastruktur unter Beweis gestellt haben.[12]
- Vergleichbar im Hinblick auf die Auswirkungen des **Computerwurms „Sasser",** der nach der Einspeisung in das Internet hunderttausende von Computersystemen weltweit infizierte und zur Konsequenz hatte, dass Fluglinien

4 Vgl. dazu grundlegend: *Nora/Minc*, Die Informatisierung der Gesellschaft, 1979; vgl. dazu ferner *Bär*, in: Wabnitz/Janovsky, Handbuch des Wirtschaftsstrafrecht, 2007, Kap. 12 Rn. 1.

5 Aktuellen Erhebungen zufolge nutzen derzeit mehr als 1,1 Mrd. Menschen das Internet. Vgl. „Internet World Stats" abrufbar unter: http://www.internetworldstats.com/stats.htm.

6 Vgl. zu den digitalen Identitäten und den damit verbundenen datenschutzrechtlichen Risiken *Hansen/Meissner*, Verkettung digitaler Identitäten, 2007 – abrufbar unter: https://www.datenschutzzentrum.de/projekte/verkettung/2007-uld-tud-verkettung-digitaler-identitaeten-bmbf.pdf.

7 Vgl. z. B. www.myspace.com, www.facebook.com. Das Unternehmen Microsoft hat kürzlich für 240 Millionen US-Dollar einen knapp 2 % Anteil an der Online Community www.facebook.com erworben. Vgl. dazu Heise News vom 25.10.2007 – abrufbar unter: http://www.heise.de/newsticker/meldung/97934.

8 *Gercke*, MMR 2008, 291.

9 Vgl. dazu *Bohn/Coroama/Langheinrich/Mattern/Rohs,* Living in a World of Smart Everyday Objects – Social, Economic, and Ethical Implications, Journal of Human and Ecological Risk Assessment, Vol. 10, S. 763 ff.

10 Vgl. zur Gefährdung kritischer Infrastrukturelemente das Basisschutzkonzept des BMI für kritische Infrastruktur, 2005, S. 13 ff. sowie *Wigert*, Varying policy responses to critical information infrastructure protection (CIIP) in selected countries, Cybercrime and Security, IIB-1, S. 1.

11 *Toth*, „Estonia under cyber attack" – abrufbar unter: http://www.cert.hu/dmdocuments/Estonia_attack2.pdf; *Lewis*, „Cyber Attacks Explained", 2007 – abrufbar unter: http://www.csis.org/media/csis/pubs/070615_cyber_attacks.pdf; „A cyber-riot",

12 Zur völkerrechtlichen Bewertung des Angriffs, vgl. *Kelsey*, Hacking into International Humanitarian Law: The Principle of Distinction and Neutrality in the Age of Cyber Warfare, Michigan Law Review, Vol. 106, S. 1427 ff.

Flüge streichen mussten und Finanzdienstleister ihre Filialen schließen mussten.[13]
– Auch der **Verkehrssektor** ist aufgrund der starken Abhängigkeit von der Verfügbarkeit der Computertechnologie nicht von Angriffen verschont geblieben.[14] Erfolgreiche Angriffe auf die Flugkontrollsysteme eines Flughafens in den USA[15] haben das Risiko der Vernetzung kritischer Infrastruktur hervorgehoben.[16]

2. Die Gewährleistung einer effektiven Strafverfolgung

Das Erfordernis einer effektiven Strafverfolgung im Hinblick auf Internet- und Computerdelikte ist eine direkte Konsequenz des Transformationsprozesses zur Informationsgesellschaft.[17] Neben der Reaktion auf die zunehmende Abhängigkeit der Gesellschaft von der Informationstechnologie ist die Notwendigkeit einer **Analyse der Herausforderungen** der Bekämpfung der Internetkriminalität als Grundpfeiler für die Gewährleistung einer effektiven Strafverfolgung auch eine Reaktion auf die zunehmende Risikobereitschaft der Mitglieder der Informationsgesellschaft.[18] Wie bereits erwähnt, zeichnet sich die Informationsgesellschaft insbesondere durch die Bedeutung digitaler Identitäten aus. Deren Nutzung birgt Risiken. Einen Aspekt – die Auswirkung der Verkettung digitaler Identitäten – wurde jüngst in einer Studie des ULD thematisiert.[19] Weitere Risiken sind insbesondere mit dem Phänomen des Identitätsdiebstahls verbunden.[20] **4**

3. Möglichkeiten der Strafverfolgungsbehörden

Die Verbreitung der Informations- und Kommunikationstechnologie geht nicht nur mit einer Erhöhung des Risikos für Angriffe und der Schaffung neuer Deliktsformen[21] einher, sondern hat in der Vergangenheit auch maßgeblich an Einfluss auf die Möglichkeiten der Strafverfolgungsbehörden im Rahmen ihrer Ermittlungstätigkeit gewonnen.[22] **5**

In den letzten 20 Jahren hat sich der Funktionsumfang von Softwareprodukten in vielen Bereichen wesentlich erweitert. Dies betrifft neben Betriebssystemen **6**

---

13 Vgl. zu den Auswirkungen des Computerwurms Sasser vgl. Heise-News, Spätfolgen eines Computer-Virus, 4.1.2005 – abrufbar unter: http://www.heise.de/newsticker/meldung/54746.
14 *Gercke*, in: Tahmisoglu/Özen, Transportation Security Against Terrorism, 2009, S. 151 ff.
15 Vgl. zu den Angriffen gegen Worcester Airport: Critical Infrastructure Protection, Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain, September 2007, GAO-07-1036 – abrufbar unter: http://www.gao.gov/new.items/d071036.pdf.
16 Zu den Risiken der Vernetzung vgl. *Gercke*, Cyber-Attacks against Transportation Infrastructure, in: Tahmisoglu/Özen, Transportation Security Against Terrorism, 2009, S. 151 ff.
17 Vgl. zum Transformationsprozess: World Summit on the Information Society, Document WSIS-03/GENEVA/DOC/5-E, December 2003, abrufbar unter: http://www.itu.int/wsis/docs/geneva/official/poa.htm.
18 Zu den möglichen strafrechtlichen Reaktionen auf die mit der Risikogesellschaft einhergehenden Phänomene, vgl. *Hilgendorf*, NStZ 1993, 10 ff.
19 *Hansen/Meissner*, Verkettung digitaler Identitäten, 2007 – abrufbar unter: https://www.datenschutzzentrum.de/projekte/verkettung/2007-uld-tud-verkettung-digitaler-identitaeten-bmbf.pdf.
20 Zum Identitätsdiebstahl vgl. *Rihaczek*, DuD 2004, 649; *Bräuer*, DuD 2005, 24. *Rost/Meints*, DuD 2005, 216 ff.; *Gajek/Schwenk/Wegener*, DuD 2005, 639 ff.; *Gercke*, CR 2005, 606 ff.; *ders*. Internet-related Identity Theft, 2007 – abrufbar unter: http://www.coe.int.
21 Ein Beispiel für eine Deliktsform, die maßgeblich von der Entwicklung der Informationstechnologie profitiert hat, ist Spam. Gemäß Erhebungen der „Messaging Anti-Abuse Working Group" waren 2005 bis zu 85 % aller überprüften E-Mails Spam.
22 Zu den Möglichkeiten der Computerforensik vgl. einführend *Willer/Hoppen*, CR 2007, 610 ff.; Weiterführend: *Geschonneck*, Computer Forensik, 2006.

und den klassischen Office-Produkten auch den Bereich der Computerforensik.[23] Sowohl die Zahl der Anbieter, als auch der Umfang der Analysemöglichkeiten hat sich erweitert.[24] So können Ermittlungsbehörden mithilfe entsprechender Softwareprodukte zahlreiche **automatisierte Auswertungen** vornehmen, die die Ermittlungstätigkeit beschleunigen können. Dazu zählen beispielsweise:

- Die automatisierte Auswertung der auf beschlagnahmten Mobiltelefonen gespeicherten Daten. Die Forensiksoftware ermöglicht dabei neben dem Auslesen des Telefonbuchs und des Kurznachrichtenspeichers auch die Auswertung von Internetzugriffen über das Mobiltelefon.
- Beschlagnahmte Speichermedien wie beispielsweise CDs, DVDs, USB-Sticks oder Festplatten lassen sich mit Hilfe von Forensiksoftware automatisch daraufhin überprüfen, ob **kinderpornographische Schriften**[25] gespeichert sind.[26] Aufgrund der weiterhin beschränkten Möglichkeiten einer automatisierten Bewertung von Bildern auf ihren pornographischen Inhalt erfolgt die Überprüfung Hashwert-basiert.[27] Dies hat im Ergebnis zur Folge, dass im Rahmen des automatisierten Verfahrens nur bekannte und nicht modifizierte Bilder und Filme gefunden werden können.
- Eine Analyse eines beschlagnahmten Rechners kann darüber hinaus Aufschluss über das Nutzungsverhalten des Eigentümers, die Verwendung von kabellosen (und ggf. im Rahmen von Durchsuchungsmaßnahen daher unentdeckt gebliebenen) externen Datenspeichern oder zum Einsatz von Verschlüsselungstechnologie geben.[28]

7 Ein weiteres Beispiel für den Einsatz der Informations- und Kommunikationstechnologie zu Ermittlungszwecken ist die **öffentliche Fahndung** nach Verdächtigen.[29] Über einen spektakulären Fahndungserfolg von Interpol aus dem Jahr 2007 wurde ausführlich in der Presse berichtet.[30] Experten des Bundeskriminalamts ist es gelungen, Bilder eines Pädophilen, die dieser unter Verwendung von Filtern einer Grafiksoftware in einer Weise verfremdet hatte, dass sein Gesicht nicht erkennbar war, dergestalt zu bearbeiten,[31] dass das Gesicht wieder erkennbar wurde und daraufhin ein Verdächtiger festgenommen werden konnte.[32] Während der 76sten Generalversammlung von Interpol haben die Delegierten einem Beschluss zugestimmt, der Interpol ermächtigt, die Internetfahndung als reguläres Instrument im Bereich der Bekämpfung von

23 *Willer/Hoppen*, CR 2007, 614 f.
24 *Fox/Kelm*, DuD 2004, 491.
25 Vgl. zu den Möglichkeiten und Grenzen der Überprüfung großer Datenbestände durch Spezialsoftware wie das Programm Perkeo vgl. *König*, Kinderpornographie im Internet, 2003, S. 231 f.
26 Zum Einsatz von Hashwert-basierte Analysen vgl. *Salgado*, Fourth Amendment Search and the Power of the Hash, Harvard Law Review, Vol. 119, S. 38 ff.; *Kerr*, Searches and Seizutre in a Digital World, Harvard Law Review, Vol. 119.
27 Vgl. zu Hashwerten (im Zusammenhang mit asymmetrischer Kryptographie) *Dobertin*, DuD 1997, 82 ff.
28 Vgl. zur Verschlüsselungstechnologie auch Rn. 47 ff.
29 Vgl. dazu *Pätzel,* NJW 1997, 3131 ff., *Soine*, NStZ 1997, 166 ff.; *ders.*, NStZ, 1997, 321 ff.; *Bär,* CR 1997, 422 ff.; *Gusy*, Polizeirecht, 6. Aufl., Rn. 275. Seitz, Strafverfolgungsmaßnahmen im Internet, 2004.
30 Vgl. z. B. Der Tagesspiegel, abrufbar unter: http://www.tagesspiegel.de/weltspiegel/Kinderschaender-Kinderpornos-Interpol;art1117,2400506; Interpol in Appeal to find Pedophile Suspect, The New York Times, 9.10.2007.
31 „Schwerer sexueller Missbrauch von Kindern – Interpol fahndet erstmals mit Bildern nach Tatverdächtigem", BKA – Pressemitteilung vom 8.10.2007.
32 Zum Verfahren vgl.: Interpol identifiziert Kinderschänder Vico, Der Tagesspiegel, abrufbar unter: http://www.tagesspiegel.de/weltspiegel/Kinderschaender-Kinderpornos-Interpol;art1117,2400506.