Erschienen in: Zeitschrift für internationale Strafrechtsdogmatik : ZIS ; 7 (2012), 8-9. - S. 458-465

Einseitiges Strafanwendungsrecht und entgrenztes Internet?*

Von Akad. Rätin a.Z. Dr. **Liane Wörner**, LL.M. (UW-Madison), Gießen

The paper questions, whether the subordination of criminal law to national state systems can cope with the – by nature – un-restricted and un-limited internet and its possibilities to act international. Neither total observation of all kinds of websites and internet forum seems to be even possible nor can this be called an achievable aim in respect of societal democratic orders. Efforts to restrict „the internet" fail. A coordinated approach by national states reconfiguring their national criminal laws in respect of the challenges of internet-crimes may be a solution and result in the release of International contractual provisions. But, agreeing on what shall be punished will not solve any conflicts of jurisdiction, because the Internet is a „boundless ocean". International coordination will require reconsidering what to protect on the one side and to reconsider national jurisdictional rules of choice of forum on the other side. In the end a transnational approach on choice of forum addresses national states as well as (directly) state citizens. Transnational power on choice of forum therefore cannot be a one-way-street, but a democratic process resulting in provisions. This will have to result in reinterpreting rules of national jurisdictions away from a one-side-viewed national sovereignty to transnational solidarity and transnational citizens.

I. Einführung: Das entgrenzte Internet

Die Informationsplattform Internet ist aus unserem Leben nicht mehr wegzudenken. Wir verhalten uns zu ihr, mit *Callas*, „fast schon wie Fische zum Wasser: Wir merken nicht, dass es uns umgibt. Wir schwimmen einfach drin."[1] Faktisch sind die mehr als drei Milliarden Webseiten des world wide web (www) mit über 150.000 verschiedenen newsgroups und ca. 25.000 verschiedenen Chatkanälen im Internet Relay Chat (IRC) jedenfalls auf Basis der derzeitigen Netzstruktur zur Feststellung von Straftaten längst nicht mehr vollständig überwachbar,[2] noch wäre dies erstrebenswert. Der anhaltende Trend zur „globalen Verbreitung digitaler Informationen", ob per peer to peer oder mittels „Cloud Computing", jeweils anonymisiert und kryptiert, stellt die Ermittler vor immer neue Herausforderungen.[3] Die Nutzung des Internets zu kriminellen Zwecken entwickelt sich zu *dem* Kriminalitätsphänomen des 21. Jahrhunderts.[4]

1. Piraten und Hacker

Dabei erinnert die aktuelle Diskussion um das Internet an das Zeitalter romantisch verklärter Piraterie und Freibeuterei des 16. und frühen 17. Jh. n. Chr. Der Vergleich mag überraschen, doch er ist rasch erklärt: Die Piraten, so ambivalent, wie wir sie heute verstehen, kamen mit der Entdeckung der terra incognita, der neuen Welt Amerikas.[5] Schätze wollten geborgen, neue Kommunikations- und Handelswege gefunden und neues Terrain erschlossen werden. Angelockt vom Reichtum der großen Handelsschiffe gab mancher seine ehrbare Stellung auf, um in den ungesicherten Meeren als Pirat sein „Glück zu machen". Mit Entdeckung der Weite des noch nicht erschlossenen Raums begann das goldene Zeitalter der Piraterie. Doch auch die Staatsmächte Europas wollten sich am Reichtum beteiligten und verteilten „Kaperbriefe" – also Lizenzen für Piraten zum Bestehlen und Berauben ausländischer Handelsschiffe im staatlichen Auftrag.[6]

Die terra incognita von heute ist das world wide web. Mit seiner Freigabe an die Welt 1989[7] begann die Schatzsuche. Was von *Tim Berners-Lee* am Cern/Schweiz für den einfachen und schnellen Austausch von Forschungsergebnissen gedacht war, ist heute unsere Hauptkommunikationsplattform und

---

* Vortrag im Rahmen des AIDP-Symposiums „Cybercrime: Ein deutsch-türkischer Rechtsdialog" an der Bilgi-Universität Istanbul, Türkei (13.-15.10.2011). Der Vortragsstil wurde weitgehend beibehalten.

[1] *Callas*, Die Zeit v. 29.9.2011, S. 29 (aus dem Englischen übersetzt v. *Thomas Fischermann*).

[2] So die Zentralstelle für anlassunabhängige Recherchen in Datennetzen (ZaRD) beim Bundeskriminalamt (BKA), unter: http://bka.de/nn_205994/DE/ThemenABisZ/Deliktsbereiche/InternetKriminalitaet/InternetrechercheZaRD/zard__node.html?__nnn=true (12.7.2012).

[3] So auch die ZaRD auf ihrer Internetseite unter „Perspektiven". Zur Zunahme des cloud computing vgl. Bundesamt für Sicherheit in der Informationstechnik (BSI), Die Lage der IT-Sicherheit in Deutschland 2011, BSI-Lagebericht IT-Sicherheit 2011, 2011, S. 38 ff., auch im Internet abrufbar unter: http/www.bsi.bund.de/ContentBSI/Publikationen/Lageberichte/bsi-lageberichte.html (12.7.2012).

[4] S. nur BKA, Bundeslagebild Cybercrime 2010, 2010, S. 5 ff., insb. S. 7; Bundesministerium des Inneren, Polizeiliche Kriminalstatistik 2010, Stand: April 2011, S. 8: Erhebungen zum Tatmittel Internet erfolgen seit 2010 in allen Bundesländern über eine entsprechende Sonderkennung. Die Steigungsrate liegt allein von 2009 auf 2010 bei durchschnittlich 8,1 %. Vgl. auch *Hecker*, Europäisches Strafrecht, 3. Aufl. 2010, § 11 Rn. 97 f. Zur Entwicklung schon *Valerius*, Ermittlungen der Strafverfolgungsbehörden in den Kommunikationsdiensten des Internet, 2004, S. 20 f.; *Böckenförde*, Die Ermittlung im Netz, 2003, S. 1 ff., insb. S. 7 f., spricht von „Netzkriminalität".

[5] Seefahrer gab es freilich bereits zuvor, doch entspann sich der eigentliche Kampf um die Meere gerade mit der Entdeckung der „neuen Welt".

[6] Zur rechtlichen Einordnung ausführlich *Kretschmer*, Globalisierung und Strafrecht, Grundlagen transnationaler Strafbegründung: Recht – Geschichte – Ökonomie – Politik (noch unveröff.), A. I. 3.-5. (Manuskript S. 9-27 ff.).

[7] Ursprung des Internets ist das bereits 1966/69 vom amerikanischen Verteidigungsministerium eingerichtete ARPAnet (Advanced Research Projects Agency). Zur Geschichte des Internets vgl. *Blancke*, APuZ 30-31/2005, 24 (25); *Valerius* (Fn. 4), S. 1 ff., insb. S. 4, 9.; *Böckenförde* (Fn. 4), S. 3. Der erste Browser stand 1993 kostenfrei zur Verfügung.

bestimmt unsere Handelswege. Auch heute gibt manch einer eine „ehrbare“ Stellung auf, um als „Anonymous“ Sicherheitslücken in der Kommunikationsplattform Facebook aufzuspüren[8] oder mittels des Software-Trojaners Katusha die Handelswege vieler Millionen Bankkunden zu durchkreuzen.[9] Es ist das goldene Zeitalter der Hacker, wie man jene Online-(Daten-)Piraten zu nennen pflegt.[10] Facebook ruft nach Sicherheit und verteilt ebenso wie viele Staatsmächte „Hacker-briefe“.[11] Der amerikanisch-israelische Computerwurm stuxnet wird 2010 („staatlich verordnet“) in eine Urananreicherungsanlage im Iran „eingepflanzt“ und manipuliert dort den Steuerungschip der Zentrifugen und damit das Atombombenprogramm des Iran insgesamt.[12] Das Internet als „wichtigste Infrastruktur unserer Zeit“ scheint zur Gefahr für Wohlstand und Sicherheit zu mutieren und steht vor dem Neubau.[13] Unklar ist mithin, was es überhaupt gegen wen zu schützen gilt.[14]

2. Weltmeer und Datenmeer

Die Piraterie ist heute weltweit geächtetes und international verfolgtes Delikt. Das Seerechtsübereinkommen der Vereinten Nationen von 1982[15] verpflichtet die Staaten zur gemeinsamen Bekämpfung der Piraterie auf den Weltmeeren. Doch sind damit nicht alle Probleme der internationalen Piraterie gelöst. Der seit dem 17. Jahrhundert anerkannte, wenn auch in seinen Grenzbereichen nicht unumstrittene, Grundsatz der Freiheit der Weltmeere[16] beschränkt die staatliche Hoheitsausübung bis heute auf Schiffe unter eigener Flagge. Die 1927 in Istanbul begründete „Lotus-Regel“ stellt eine Vermutung für die staatliche Handlungsfreiheit aufgrund staatlicher Souveränität auf. Denn nachdem am 2.8.1926 das französische Postschiff Lotus auf hoher See mit der Boz-Kurt kollidiert war und dabei acht türkische Seeleute ihr Leben verloren, entschied der Ständige Internationale Gerichtshof (StIGH) zugunsten der türkischen Souveränität:[17]

„International law governs relations between independent States. The rules of law binding upon States therefore emanate from their own free will [...]. Restrictions upon the independence of States cannot therefore be presumed.“

Für staatlich zulässiges Handeln bedarf es danach keiner völkerrechtlichen Erlaubnisnorm. Es darf nur kein völkerrechtliches Verbot entgegenstehen.[18] Und der souveräne Staat kann nicht zur Handlung verpflichtet werden. Die hieraus resultierenden Probleme in der Bekämpfung der internationalen Piraterie zeigt (beispielhaft) die Entführung des von der deutschen Reederei verwalteten Tankers Longchamp im Januar 2009 vor der Küste Somalias. Die Staatsanwaltschaft in Hamburg ermittelte wegen Angriffs auf den Luft- und Seeverkehr (§ 316c dStGB). Doch die deutsche Zuständigkeit für das in Deutschland verwaltete, unter der Flagge der Bahamas mit indonesischem Kapitän und philippinischer Mannschaft zwischen Norwegen und Vietnam verkehrende und von somalischen Piraten überfallene Schiff war keineswegs klar. Die deutsche Marine erklärte sich schließlich nach Prüfung für unzuständig.[19] Einseitige Souveränitätskonzepte helfen hier nicht weiter.

---

[8] *Fischermann/Hamann*, Die Zeit v. 8.9.2011, S. 27.

[9] Dazu: *Gatzke*, Kriminalistik 2012, 75; Zeitungsbericht *Katusha*, Weser-Ems-Zeitung v. 1.11.2010 (business-on, http://www.business-on.de/druckansicht/14_80_15512.html [28.2.2012]). Die exemplarische Aufzählung ist nicht abschließend. Zu den „Daten-Piraten“ sind neben Einzelpersonen und Personenzusammenschlüssen ebenso auch Unternehmen, Unternehmensgruppen und Staaten zu zählen, soweit sie im Umgang mit ihnen zugänglichen oder ihnen überlassenen Daten in Individualrechte eingreifen oder diese beschränken.

[10] Auf die zu den Piraten von damals bestehende gleichlaufende Ambivalenz machen nun etwa auch *Robertz/Rüdiger*, (Kriminalistik 2012, 79) aufmerksam.

[11] Zum Facebook-Aufruf s.a. *Fischermann/Hamann*, Die Zeit v. 8.9.2011, S. 27. Zum jährlichen Facebook-Hacker Cup: http://www.facebook.com/video/video.php?v=10100106817149407 (12.7.2012).

[12] Vgl. dazu BSI (Fn. 3), S. 28 f. Es kursieren bereits neue stuxnet-ähnliche Schadprogramme wie Duqu (*Höll/Krüger/Martin-Jung*, Süddeutsche Zeitung v. 20.10.2011, S. 5).

[13] *Fischermann/Hamann*, Die Zeit v. 8.9.2011, S. 27 (im Titel); *dies.*, Zeitbombe Internet, 2011, S. 25 ff., insb. S. 28.

[14] Zu definitorischen Problemen des Begriffs „Computerkriminalität“ vgl. bereits *Hilgendorf*, JuS 1997, 323 („Datennetzkriminalität“); *Sieber*, Computerkriminalität und Strafrecht, 1977, S. 184, 188 („Sammelsurium“); *ders.*, Legal Aspects of Computer-Related Crime in the Information Society, 1998, S. 24 ff.; *ders.*, in: Sieber/Brüner/Satzger/von Heintschel-Heinegg (Hrsg.), Europäisches Strafrecht, 2011, Kap. 6 Rn. 1-6 zum weiten Bereich der Computer- und Internetkriminalität und den definitorischen Problemen.

[15] Seerechtsübereinkommen der Vereinten Nationen („United Nations Convention on the Law of the Sea“) v. 10.12.1982, auch in Deutschland in Kraft seit 16.11.1994 (BGBl. II 1994, S. 1798; BGBl. II 1995, S. 602); basierend auf dem Genfer Übereinkommen über die Hohe See v. 29.4.1958, in Kraft seit 30.9.1962, in Deutschland seit dem 25.8.1973 (BGBl. II 1972, S. 1089, 1091; BGBl. II 1975, S. 843).

[16] Völkervertraglich anerkannt erst mit Art. 2 des UN-Übereinkommens über die Hohe See v. 29.4.1958 (UNCLOS I) sowie in Art. 87 ff. des UN-Seerechtsübereinkommens v. 10.12.1982 (UNCLOS III). Zur geschichtlichen Entwicklung vgl. auch *Kretschmer* (Fn. 6), B. III. (Manuskript S. 270 f.).

[17] Vgl. StIGH, Urt. v. 7.9.1927 – PCIJ Ser. A No. 10 (S.S. Lotus [Frankreich v. Türkei]), im Internet abrufbar unter: http://www.worldcourts.com/pcij/eng/decisions/1927.09.07_lotus.htm (12.7.2012).

[18] Zur Interpretation kurz auch *Hobe*, Einführung in das Völkerrecht, 9. Aufl. 2008, S. 619 f.

[19] Vgl. Hamburger Abendblatt v. 30.1.2009, im Internet unter: http://www.abendblatt.de/wirtschaft/article596093/Deutsche-Marine-Wir-sind-fuer-die-Longchamp-nicht-zustaendig.html (12.7.2012). Zum Verfahrensausgang: Spiegel-online v. 28.3.2009, abrufbar unter: http://www.spiegel.de/panorama/justiz/somalia-entfuehrter-deutscher-gastanker-longchamp-wieder-frei-a-616040.html (12.7.2012).

Auch im aktuellen Datenmeer des www bestehen Jurisdiktionskonflikte wegen strafbarer Handlungen im Internet. Höchst fraglich ist es, ob sich ein „goldenes Zeitalter des Hackertums“ mit einer Invasion gegen das Internet beenden ließe[20] oder ob eher ein Umdenken und gegebenenfalls ein Neustrukturieren seiner Kommunikationsformen und Datenübertragungswege – seien es Facebook oder „library.nu“[21] – angezeigt sind. Eine rechtliche Begrenzung der terra incognita Internet tut gut und not. Man sollte aber nicht erwarten, dass mit Mitteln des Strafrechts über seine grundsätzlich friedenssichernde Funktion hinaus[22] mittels Datensicherheit ein kriminalitätsfreier Raum geschaffen würde. Denn das veränderte auch *im* und *über das* Internet die Wertegesellschaft in eine Sicherheitsgesellschaft. Fraglich ist nun einerseits, inwieweit eine rechtliche Begrenzung des Internet möglich erscheint (II.), wie einseitig – im Sinne von staatlichen Formen abhängig – das Strafanwendungsrecht (III.) ist und wie sich beide Komponenten miteinander verbinden lassen (III./IV.)

II. (Faktische) Begrenzungsversuche

Neben aktuell geplanten staatlichen Versuchen zur nationalstaatlich betriebenen Begrenzung des world wide web etwa durch das (deutsche) Nationale Cyber-Abwehrzentrum in Bonn[23] mit einer Softwareschutzhülle gegen Hacker[24] oder dem von EU-Justizkommissarin Viviane Reding gerade erarbeiteten EU-Datenschutzrahmengesetz[25] – *Jon Callas* prophezeit sogar die staatliche Übernahme der sozialen Internetnetzwerke (von google bis facebook)[26], – stand lange die an anderer Stelle angedachte Begrenzung des Internets durch die Weiterentwicklung von peer to peer-Systemen in „zuverlässige Netze“.[27]

Der peer to peer-Schutz ist jedenfalls für die Kriminalitätsbekämpfung wenig zielführend. Nach der Idee des peer to peer-accountable soll Zutritt nur dem gewährt werden, der sich als identifizierbar, vertrauenswürdig und zuverlässig erweist. Die Nutzer sollen untereinander verantwortlich sein und frei von staatlichem Zugriff entscheiden, in welchem System sie „leben“ möchten: in einem mit mehr Regulierung oder in einem, in dem ein jeder einen jeden belügt und betrügt. Mittels verlässlicher Reputationssysteme und Schutztools könne man beide unterscheiden.[28] Diese dezentrale „Internet-Governance“[29] entspricht einer informationellen Selbstbestimmung der Internetuser. Doch der Kriminelle wird sich kaum freiwillig in einem Netz von Betrügern und Lügnern tummeln, sondern gerade Zugang zu einem speziellen peer to peer-accountable suchen. Den an staatliche Hoheitsgrenzen auch noch gebundenen Ermittlungsorganen und Justizen fällt dann unter ungleich erschwerten Bedingungen die Durchsetzung des Opferschutzes zu. Die Balance zwischen informationeller Selbstbestimmung und Opferschutz im Internet erscheint kaum haltbar.[30] Den entwickelten cloud-Systemen haften insoweit die gleichen Probleme an.[31] Denn der vermeintlich höchste Datenschutz, etwa in einer besonders gesicherten „zuverlässigen cloud“, beinhaltet gerade den Zugriffsreiz. Zugleich erschwert die Vielzahl an Usern und an clouds die Sicherungsmöglichkeiten.[32]

Auch der Blick auf einen aktuellen Fall[33] zeigt, dass die faktische territorial-staatliche Begrenzung des Internets nicht funktioniert: Die Ermittler der EK-Katusha, benannt nach dem von den Tätern eingesetzten Trojaner, sprengten eine internationale Hacker-Bande in einem der umfangreichsten Ermittlungsverfahren gegen Verbreiter von Schadsoftware. In 39 Telekommunikationsüberwachungsmaßnahmen ermittelten sie ca. 670 sogenannte Finanzagenten in über 100 Botnetzen mit über 50 Servern, die für die acht Hauptverdächtigen – zwei Deutsche, ein Brite und fünf estnische Staatsbürger – tätig waren. In Deutschland wurden ca. 400.000 mit dem Katusha-Trojaner infizierte PCs festgestellt, weltweit ca. 2,5

[20] So der Vorschlag von *Fischermann/Hamann*, Die Zeit v. 8.9.2011, S. 27; *dies.* (Fn. 13), S. 33 ff., 234 ff.

[21] Das angeführte Bsp. „www.library.nu“ (12.7.2012) ist als Beispiel für ein lange Zeit funktionierendes Webportal gewählt, welches umfassend den Down- und teilweise Upload von belletristischer und vor allem auch wissenschaftlicher Literatur ermöglichte. Juristisch unbehelligt blieb es lange vor allem, weil hier national verschieden Betreiber, Webhost und Server*standort* zusammenwirkten und hieraus – wenn man so will – ein negativer Jurisdiktionskonflikt entstand. Seit Ende 2011 war die Seite gesperrt, ist inzwischen aber offiziell mit google und Amazon verbunden legal zugänglich. Nachfolger existieren bereits.

[22] Hierzu grundlegend auch *Kretschmer* (Fn. 6), B. I. sowie B. III. und C.IV. (Manuskript S. 186, S. 278 ff. und S. 458 ff.).

[23] Kurz NCAZ, gegründet am 23.2.2011.

[24] Vgl. *Fischermann/Hamann* (Fn. 13), S. 231 ff., 243 ff.; dazu *dies.*, Die Zeit v. 8.9.2011, S. 27 (S. 29).

[25] *Hammann/Tatje*, Die Zeit v. 29.9.2011, S. 28.

[26] *Callas*, Die Zeit v. 29.9.2011, S. 29. *Fischermann/Hamann* (Fn. 13), S. 240 ff. plädieren für eine Datendiät etwa mittels einer Zentralstelle für Lizenzen im Umgang mit persönlichen Daten (*dies.* [Fn. 13], S. 240), die die Verwendung persönlicher Daten für den Einzelnen nach dessen Wünschen konkret lizensiert.

[27] Deutlich *Dyson*, APuZ 30-31/2005, 3.

[28] *Dyson*, APuZ 30-31/2005, 3.

[29] *Dyson*, APuZ 30-31/2005, 3.

[30] So die ZaRD auf ihrer Internetseite unter „Perspektiven“.

[31] Der durch den 2008 neu eingeführten § 110 Abs. 3 StPO erlaubte Zugriff auf die Cloud-Daten führt insbesondere zu einer „Online-Durchsuchung light“; zu den Zugriffsmöglichkeiten ausführlich und krit. s. *Schlegel*, HRRS 2008, 23, und *Bär*, ZIS 2011, 53 (54 f.), vor allem auch zu den praktischen Problemen des transnationalen Zugriffs; zu Recht kritisiert *Bär*, a.a.O., die Vorschriften der Cyber Crime Convention als insoweit unzureichend.

[32] *Fischermann/Hamann* (Fn. 13), S. 243 schlagen deshalb vor, mittels internationaler Bestimmungen festzulegen, dass die gespeicherten Cloud-Daten auf Superspeichern dort lagern sollen, wo die Menschen leben, um deren Daten es geht. Allerdings lassen sich auch Lebensmittelpunkte heute nicht mehr einfach bestimmen.

[33] Die Hauptverhandlungen, zuletzt gegen die fünf estnischen Beschuldigten, liefen am 30.9.2011 und endeten mit einem Vergleich.

Mio. Mittels des Trojaners wurden die Onlinebankgeschäfte der betroffenen Kunden so manipuliert, dass erst nach der Eingabe aller Daten durch die Kunden einschließlich der Transaktionsnummern der Bank (TAN) eine Umleitung der Überweisung unter Änderung des Überweisungsbetrags auf ein anderes Konto erfolgte. Den deutschen Ermittlern gelang es in enger Zusammenarbeit mit den estnischen und den britischen Behörden, einen Schaden in Höhe von 1,2 Mio. Euro abzuwenden.[34] Weder die international zusammengesetzte Tätergruppe noch die ebenso international betroffenen Kunden, noch die nunmehr ebenfalls international zusammenwirkenden Ermittler lassen sich faktisch noch in nationalstaatliche territorial erfassbare Grenzen „pressen".

Beschränkungen sind damit allenfalls bezogen auf den Datenfluss und seine Sicherungen denkbar. Im Übrigen ist das Internet entgrenzt. Publikationen im Internet sind grundsätzlich ebenso weltweit zugänglich wie weltweit Datenzugriffe möglich sind.[35] Rechtliche – auch strafrechtliche und im Besonderen strafanwendungsrechtliche – Regelungen müssen hierauf reagieren.

III. Einseitiges Strafanwendungsrecht oder Internationales Internetstrafrecht für alle?

Internationale Verfahren wie Katusha fordern die nationale Straftatverfolgung der Zukunft heraus.[36] Dabei gilt es einerseits zu klären, was im Internet überhaupt verfolgt werden kann und darf und welche Maßnahmen hierfür ergriffen werden dürfen.[37] Neben jene zu klärenden, teils auch faktischen Fragen, tritt unmittelbar eine weitere: Welches Strafrecht soll gelten?

1. „Das Rechtsnetz" – Auf hoher See der Rechte

Art. 22 der Cybercrime Convention des Europarats (2001)[38] knüpft für die festzulegende Gerichtsbarkeit an die völkerrechtlich anerkannten Anknüpfungspunkte, insbesondere der Territorialität, des Flaggengrundsatzes und der aktiven Personalität, an. Eine dezidierte Darstellung aller Strafanknüpfungspunkte ist hier freilich nicht zu leisten und auch nicht gewollt.[39] Vielmehr steht ihre Anwendbarkeit für das Internet in Frage und damit die Grundsatzfrage, ob das www Sonderregulierungen erfordert und inwieweit sich völkerrechtlich anerkannte Prinzipien nutzen lassen.

Insoweit kann zunächst festgehalten werden, dass die Statusüberprüfung des „CyberCrime@IPA Projektes" mit der Türkei eine grundsätzliche Übereinstimmung der türkischen Strafanwendungsvorschriften der Art. 8-13 türkStGB mit den Anforderungen der Cybercrime Convention feststellt.[40] Doch die Strafanwendungsfrage beim transnationalen und internationalen Datenmissbrauch bei facebook, mittels stuxnet oder Katusha löst das nicht. Während Art. 23-34 der Cybercrime Convention die Zusammenarbeit bei den Ermittlungen, Rechtshilfe und Auslieferung betreffen, bleibt die „Ausübung der Strafgerichtsbarkeit durch eine Vertragspartei nach ihrem innerstaatlichen Recht" nach Art. 22 Abs. 4 Cybercrime Convention ausdrücklich vorbehalten.

Das ist nicht unproblematisch, wie der Blick ins deutsche Strafanwendungsrecht zeigt. Denn das deutsche Strafrecht ist für seine extensive Auslegung weit bekannt.[41] An ihm soll offenbar „die Welt genesen", kritisierte *Hilgendorf* schon 1997 die Strafverfolgung im Internet.[42] Weil sich aber im territorial entgrenzten Internet weder der Datenzugriff noch die Datenmanipulation an staatliche Grenzen halten, entsteht im Hinblick auf die Zuweisung der nationalstaatlichen Gerichtsbarkeit nahezu zwangsläufig eine Jurisdiktionskonkurrenz. Auf-

[34] Genauer Schaden: 1.202.362,00 €. Ein Schaden in Höhe von 438.180,00 € ist gleichwohl entstanden und konnte nicht mehr verhindert werden. Die nachweislichen von den Tätern manipulierten Überweisungen belaufen sich auf einen Gesamtbetrag in Höhe von 1.640.542,00 €; zu öffentlich zugänglichen Verfahrensinformationen vgl. *Gatzke*, Kriminalistik 2012, 75; Zeitungsbericht *Katusha*, Weser-Ems-Zeitung v. 1.11.2010 (Fn. 9).

[35] So auch schon *Hilgendorf*, ZStW 113 (2001), 650 (651). *Valerius* (Fn. 4), S. 141, spricht vom globalen Dorf und seinen Bürgern als „Netizen" (net citizens).

[36] Ebenso schon *Hilgendorf*, ZStW 113 (2001), 650 (651).

[37] Ausführlich bereits *Böckenförde* (Fn. 4) spricht vom eigenen „Ermittlungsraum", S. 9, 167 ff.; *Valerius* (Fn. 4), S. 21 ff., insb. S. 26 ff. Zu den auftretenden faktischen wie rechtlichen Problemen vgl. auch die Beiträge im Rahmen dieses Projekts in dieser Ausgabe von *Groß*, ZIS 2012, 466, und *Rettenmaier/Palm*, ZIS 2012, 469.

[38] Übereinkommen über Computerkriminalität v. 23.11.2001. Die deutsche Fassung ist im Internet abrufbar unter: http://conventions.coe.int/treaty/ger/treaties/html/185.htm (12.7.2012).

[39] Zu den Anknüpfungspunkten vgl. etwa *Ambos*, Internationales Strafrecht, 3. Aufl. 2011, §§ 1-4, insb. § 4 mit Übersicht in Rn. 23; *Satzger*, Internationales und Europäisches Strafrecht, 5. Aufl. 2011, § 5; *Hecker* (Fn. 4), § 2 Rn. 12 ff.; *Eser*, in: Schönke/Schröder, Strafgesetzbuch, Kommentar, 28. Aufl. 2010, Vor §§ 3-9 Rn. 11 ff.; *Werle/Jeßberger* in: Laufhütte/Rissing-van Saan/Tiedemann (Hrsg.), Strafgesetzbuch, Leipziger Kommentar, Bd. 1, 12. Aufl. 2007, § 3 Rn. 24 ff.; *L. Wörner/M. Wörner*, in: Sinn (Hrsg.), Jurisdiktionskonflikte bei grenzüberschreitend organisierter Kriminalität, 2012, S. 203 (S. 227 ff.).

[40] www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/CountryProfiles/cyber_cp_Turkey_2011_January.pdf (12.7.2012). Project on Regional Cooperation in Criminal Justice: Strengthening capacities in the fight against cybercrime, s. jp.coe.int/CEAD/JP/Default.asp?TransID=204 (12.7.2012).

[41] Schon *Eser*, in: Leipold (Hrsg.), Rechtsfragen des Internet und der Informationsgesellschaft aus deutscher und japanischer Sicht, Symposium der rechtswissenschaftlichen Fakultäten der Albert-Ludwigs-Universität Freiburg und der Städtischen Universität Osaka, 2002, S. 303 (S. 321 ff.).

[42] *Hilgendorf*, NJW 1997, 1873 (1874); zur vielfach aufgenommenen These vgl. auch: *Jofer*, Strafverfolgung im Internet, 1999, passim; *Roggan*, KJ 2001, 337.

grund der weithin anerkannten Ubiquitätsthese[43] werden für den in einem Staat an einem Computer handelnden Hacker schon dann mehrere Gerichtsbarkeiten zuständig, wenn diese Handlung in anderen Staaten einen Erfolg herbeiführt, sei es der Verlust, der Missbrauch oder die Manipulation von Daten. Der in einer Beschränkung auf die staatliche Territorialität gedachte Strafanknüpfungspunkt führt so unter Gleichbehandlung aller Handlungs- und Erfolgsorte einer Internetstraftat zu einer „globalen Strafrechtskonkurrenz".[44] Der Territorialitätsschutz verwandelt sich mit Beachtung des Internet-Erfolgsorts im deutschen – wie im Übrigen auch im türkischen – Strafrecht in einen passiven Personalschutz für alle Internetuser.[45]

Aus deutscher Perspektive ließe sich jene globale Konkurrenz jedenfalls für die sog. Inhaltsdelikte[46] zwar weitgehend reduzieren. Wird nämlich für die Strafbarkeit schon an den zu verbreitenden Kommunikations- bzw. Dateninhalt angeknüpft, wie im Fall des Verbreitens pornographischer Dateien (§§ 184 ff. dStGB) oder von volksverhetzenden Äußerungen (§ 130 dStGB), kann nur auf den Handlungsort abgestellt werden, wenn sich die Strafbarkeit in Form bereits abstrakter Gefährdung in der Handlung erschöpft.[47] Auf den Eintritt eines Erfolgs, den Eintritt einer auch nur konkreten Gefährdung, kommt es dann für die Strafbarkeit nicht an, § 9 Abs. 1 Var. 3 dStGB ist nicht einschlägig. Globale Strafrechtskonkurrenz im Internet ließe sich so also sehr einfach durch Vorverlagerung auf eine „Internetstrafbarkeit" schon bei abstrakter Gefährdung jeglicher krimineller Kommunikation verhindern. Denn dann käme es mangels erforderlichen Deliktserfolgs nur auf die Handlung an. Doch das wäre nicht nur rechtsstaatlich bedenklich, es erscheint auch im Ergebnis wohl nicht wünschenswert, wie die Diskussion um den Fall Toeben und die Verbreitung der sog. „Ausschwitzlüge" im Internet zeigt.[48]

Es gilt vielmehr einerseits zwischen bloß abstrakten Gefährdungsdelikten und Eignungsdelikten, die jedenfalls eine Eignung zu eine potentiellen Gefährdung durch die Handlung erfordern (auch: potentielle Gefährdungsdelikte), strikt zu trennen: Für erstere ist schon ihre Zulässigkeit überhaupt fraglich,[49] für zweitere kann § 9 Abs. 1 Var. 3 dStGB über die Eignung zur potentiellen Gefahr tatsächlich anwendbar werden.[50] Andererseits – und das ist hier entscheidend – besteht aber eben gerade kein grenzüberschreitender Konsens für Äußerungsdelikte, sondern die Strafbarkeit wird in den nationalen Rechtskulturen unterschiedlich beurteilt. Dem angloamerikanischen Rechtskreis ist die mit Äußerungsdelikten verbundene Einschränkung des free speech-Grundsatzes, wie im Fall Toeben, sogar eher befremdlich.[51] So wird hier letztlich einseitig souverän über die extensive Auslegung der Vorschriften des deutschen Strafanwendungsrechts die deutsche Strafbarkeit für Fälle eröffnet, in denen der Täter an der Computertastatur in seinem Heimatland handelt, unabhängig davon, wie diese Handlung dort strafrechtlich bewertet wird. Unproblematisch ist dies eben nur, wenn wie im Fall der Verbreitung von Kinderpornographie die Strafwürdigkeit solcher Handlungen international anerkannt ist.[52] Im Übrigen ist zunächst zu klären, was es im Internet gegen wen zu schützen gilt. Und dass die Lösung über restriktive oder extensive Auslegungen der Strafanwendungsvorschriften, etwa des § 9 Abs. 1 Var. 3 dStGB, für strafbare Handlungen im und über das Internet nicht trägt, zeigt schon der Blick auf die Äußerungsdelikte etwa der Beleidigung: Für die strafbare Beleidigung (§ 185 dStGB), wegen des Zugangserfordernisses ein Erfolgsdelikt, gilt, dass auch bei der über das Internet in Deutschland wahrnehmbaren Beleidigung eines amerikanischen Kommilitonen durch einen kalifornischen Studenten das deutsche Strafrecht eröffnet werden müsste.[53]

Daneben wird das deutsche Strafrecht im Falle gegebener aktiver Personalität oder in stellvertretender Strafrechtspflege

[43] Vgl. nur die Landesberichte in der rechtsvergleichenden Studie von *Sinn* (Hrsg., Fn. 39), passim. Die Ubiquitätsthese gilt auch im türkischen Strafrecht nach Art. 8 Abs. 1 türkStGB.

[44] Deutlich schon *Eser* (Fn. 41), S. 303 (S. 321, 324), der deshalb für ein Abstellen nur auf den Handlungsort plädiert (S. 325).

[45] Vgl. ähnlich schon *Eser* (Fn. 41), S. 303 (S. 324); *Sieber*, NJW 1999, 2065 (2066).

[46] Bei sog. *Inhalts*delikten besteht der kriminelle Charakter schon im *Inhalt* der Kommunikation selbst, auf das zur Verbreitung verwendete Medium kommt es nicht an. Das dürfte sogar die überwiegende Zahl im Internet begangener Delikte betreffen, *Hilgendorf/Frank/Valerius*, Computer- und Internetstrafrecht, 2005, Rn. 231.

[47] Ebenso deutlich *Hilgendorf/Frank/Valerius* (Fn. 46), Rn. 231, 234; vgl. auch *Rotsch*, ZIS 2010, 168 (170, 171).

[48] Vgl. BGHSt 46, 212 = NJW 2001, 624 = ZUM-RD 2001, 103 = MMR 2001, 228 m. Anm. *Clauß*, MMR 2001, 232, und Anm. *Hörnle*, NStZ 2001, 309, sowie auch *Vassilaki*, CR 2001, 260; *Heghmanns*, JA 2001, 276; *Jeßberger*, JR 2001, 429; *Lagodny*, JZ 2001, 1194; *Kudlich*, StV 2001, 395; *Hilgendorf/Frank/Valerius* (Fn. 46), Rn. 232.

[49] Krit. etwa *Baroke*, in: Sinn/Gropp/Nagy (Hrsg.), Grenzen der Vorverlagerung in einem Tatstrafrecht, 2011, S. 247 (S. 264 ff., 275 f. m.w.N.).

[50] So der BGH in BGHSt 46, 212; zust. *Clauß*, MMR 2001, 228 (232 f.). Die Anwendbarkeit von § 9 Abs. 1 dStGB über reine Erfolgsdelikte hinaus bejahen auch *B. Heinrich*, GA 1999, 72; *Sieber*, NJW 1999, 2065 (2067 ff.). Insgesamt lehnen dies ab: *Hilgendorf*, NJW 1997, 1873 (1875 f.); *Hilgendorf/Frank/Valerius* (Fn. 46), Rn. 232; *Cornils*, JZ 1999, 394 (395 f. m.w.N.). Grds. krit. jüngst *Rotsch*, in: Graf/Jäger/Wittig (Hrsg.), Wirtschafts- und Steuerstrafrecht, Kommentar, 2011, § 9 Rn. 19.

[51] Vgl. etwa *Whitman*, Yale Law Journal 109 (2000), 1279, worauf zu Recht auch *Hörnle*, NStZ 2011, 309 hinweist. Vgl. auch *Sieber*, NJW 1999, 2065.

[52] Ebenso deutlich *Hörnle*, NStZ 2011, 309.

[53] *Hilgendorf*, NJW 1997, 1873 (1876). Freilich kommt den deutschen Strafverfolgungsbehörden hier § 153c dStPO, insbesondere Abs. 1 Nr. 2 zu Hilfe (vgl. *L. Wörner/M. Wörner* [Fn. 39], S. 203 [S. 224] m.w.N.).

(§ 7 dStGB) zuständig,[54] wenn die Tat auch am Tatort – für das Internet wäre es besser zu formulieren: an irgendeinem der Tatorte – strafbar ist. Für das aktive Personalitätsprinzip geht die türkische Regelung in Art. 11 türkStGB darüber wohl noch hinaus und fordert keine identische Tatortnorm. Das gilt auch im deutschen Strafrecht, wenn von der Internetstraftat eines der besonders geschützten nationalen (§ 5 dStGB) oder internationalen (§ 6 dStGB) Rechtsgüter betroffen ist. Straffrei bleibt mithin nur, wem es gelingt, keines der wesentlichen Rechtsgüter zu verletzen und wer ohne Handlungs- und Erfolgsort in Deutschland eine straffreie Insel entdeckt, um eine dort straffreie Handlung so zu begehen, dass sie sich nicht als identische Tatortnorm auswirkt.

Die Zielrichtung dieser „Strafanwendungsregeln" ist klar. Ausgehend von der Grundannahme staatlicher Souveränität sollen sie die Verfolgbarkeit jedweder in den staatlichen Grenzen auftretender oder festgestellter Kriminalität sicherstellen. Sie stammen aus einer Zeit, in der das Reisen noch nicht Teil des Alltags, das Überwinden von Grenzen noch mit erheblichem Aufwand verbunden war. Während etwa *Eser* 2002 in seiner Typisierung der Internetstraftaten noch von solchen sprach, die mittels des Internets nur schneller begangen werden, und solchen, die tatsächlich nur im entgrenzten Internet möglich sind,[55] lautet die Frage 2012 bereits, welche Bedeutung der staatlichen Hoheitsgrenze im weltweiten Wirtschafts- und Handelsverkehr überhaupt noch beigemessen werden kann.[56] Die nationalen Strafanwendungsregeln sind mit ihrem staatssouveränen Ansatz nicht auf diese globale Herausforderung vorbereitet, weder im Internet noch auf hoher See.

2. Überlegungen zur Nautik des Rechts

Um *Callas*' „schwimmende Fische"[57] einzufangen, können wir nur Netze auswerfen. Auch hierzu gibt es bereits hinreichend Vorschläge.

Eine globale weltweite Zuständigkeit eines Staates liegt dabei weder im staatlichen Interesse noch ist sie staatlicherseits zu bewältigen,[58] Strafanwendungsvorschriften in diesem Sinne begrenzen die materielle Strafgewalt[59] und prozessuale Verfolgungsvorschriften geben zusätzlich Opportunitätsmöglichkeiten zum Absehen von der Verfolgung. Es dient vielmehr dem Selbstschutz des Staates, wenn er in seinem Hoheitsgebiet umfassend die eigene Strafgewalt ausübt.[60] Das Meer lässt sich nicht von einer Stelle aus befischen.

Umgekehrt lässt sich auch die vorhandene „gemeinsame Essenz" des Strafbaren nicht als „Weltstrafrecht deklamieren", sondern könnte allenfalls die „Grundlage für eine noch zu verfassende Strafrechtsordnung" bieten.[61] Allein es fehlt am gemeinsamen Gesetzgeber. Unklar ist also, wie ein solches Fischernetz gespannt werden sollte. Globalisiertes Strafrecht setzt vielmehr voraus, dass sich auf globaler Ebene eine Gemeinschaft gebildet hat, die unvollkommen, vielschichtig und vielfältig sein mag, die aber zumindest segmentär das Attribut verdient, globalisiert zu sein.[62]

Von deutscher Seite wird etwa drittens vorgeschlagen, die Anwendbarkeit der nationalen Strafrechte auf Internetstraftaten mittels restriktiver Auslegung gerade des Erfolgsbegriffs weitgehend zu beschränken[63] und entweder nur auf den Handlungsort abzustellen[64] *oder* nur einen mittels Push-Technologie auf deutsche Webseiten und Server bzw. in Deutschland zugänglichen Dateninhalt als Erfolg gelten zu lassen.[65] Und doch zielt der Ansatz, unter extensiver Auslegung mit jeder Zugriffsmöglichkeit auf strafrechtsrelevante, missbrauchte oder manipulierte Datenbestände im Internet auch einen Erfolgsort und die Strafanwendung zu bejahen,[66] (je-

[54] Vgl. *Eser* (Fn. 41), S. 303 (S. 307, krit. S. 325 f.); *Weigend*, in: Hohloch (Hrsg.), Recht und Internet, 2001, S. 85 (S. 87); *Sieber*, NJW 1999, 2065.

[55] *Eser* (Fn. 41), S. 303 ff.

[56] Auch *Hilgendorf/Frank/Valerius* (Fn. 46), Rn. 213, halten nationale Grenzen für „nahelos bedeutungslos" und betonen zusätzliche Aspekte der Globalität und der Verantwortlichkeit der Diensteanbieter.

[57] *Callas*, Die Zeit v. 29.9.2011, S. 29.

[58] *Kretschmer* (Fn. 6), spricht vom „Gebot der politischen Klugheit", B. III. (Manuskript S. 267).

[59] Ebenso *Böse*, in: Kindhäuser/Neumann/Paeffgen (Hrsg.), Nomos Kommentar, Strafgesetzbuch, Bd. 1, 3. Aufl. 2010, Vor § 3 Rn. 5.

[60] Vgl. ausführlich *Oehler*, Internationales Strafrecht, 2. Aufl. 1983, Rn. 125, 153.

[61] *Kretschmer* (Fn. 6), B. III. (Manuskript S. 265). Krit. für die Entwicklung eines Europäischen Strafrechts mit einem Europäischen Strafgesetzbuch auch *Rosenau*, ZIS 2008, 9 (16 ff.).

[62] Vgl. *Kretschmer* (Fn. 6), B. I. (Manuskript S. 186.). Zu den Gefahren der Entterritorialisierung von Strafgewalt auch *F. Meyer*, in: Beck/Burchard/Fateh-Moghadam (Hrsg.), Strafrechtsvergleichung als Problem und Lösung, 2011, S. 87 (S. 93 ff.).

[63] Vgl. *Hilgendorf*, NJW 1997, 1873 (insb. 1876 m.w.N.); *Kienle*, Internationales Strafrecht und Straftaten im Internet, 1998, S. 68, 173 ff., so dass auch bei klassischen Erfolgsdelikten und bei konkreten Gefährdungsdelikten ein durch eine Handlung im Ausland in Deutschland verursachter Erfolg nur dann strafbar sei, wenn die Handlung auch im Ausland unter Strafe stehe unter Berufung auf eine analoge Anwendung von § 7 StGB.

[64] So etwa der Vorschlag von *Eser* (Fn. 41), S. 303 (S. 325).

[65] Ausführlich zur einschränkenden Anwendbarkeit des deutschen Strafrechts nur bei Push-Inhalten insb. *Sieber*, NJW 1999, 2065 (2066, 2069). Vgl. ähnlich auch *Cornils*, JZ 1999, 394 (395 f., 397), die auch eine Neudefinition des Handlungsbegriffs nach Kriterien der Steuerung und Kontrolle vorschlägt.

[66] Vgl. so *B. Heinrich*, GA 1999, 72 (83 f.); *Martin*, Strafbarkeit grenzüberschreitender Umweltbeeinträchtigungen, 1989, S. 79 ff., 118 ff.; *Eser* (Fn. 41), S. 303 (S. 309); aber auch BGHSt 42, 235 (242) = NJW 1997, 138 und schon BGH NStZ 1990, 36 (37): Deutsches Strafrecht soll über § 9 Abs. 1 Var. 3 dStGB gelten, „sofern es im Inland zu der Schädigung von Rechtsgütern oder zu Gefährdungen kommt, deren Vermeidung Zweck der jeweiligen Strafvorschrift ist", somit über die Begriffsbildung des allgemeinen Strafrechts hinaus.

denfalls) in die richtige Richtung. Nur das verhindert das Entstehen zu großer Hohlräume in den Fischernetzen. Es soll eben nicht möglich sein, sich eine straffreie Insel zu suchen, um von dort einen Server auf einer anderen straffreien Insel, wo die Serverprovider nicht haftbar gemacht werden können, mit illegalen Daten zu versorgen, die dann weltweit unter Verstoß gegen Urheberrechte abrufbar sind (das Beispiel www.library.nu). Allein das darf nicht dazu führen, dass Jurisdiktionskonkurrenzen zu Lasten nur eines Staates ausgehen.[67] Dem käme dann mit der Verfolgungsmöglichkeit womöglich auch die Verfolgungspflicht zu.

Der Restriktionsansatz muss folglich ein anderer sein. Weit wesentlicher wird das gegenseitige Helfen (Rechtshilfe) bei der Verfolgung und Aburteilung von Straftaten. Das Prinzip der stellvertretenden Strafrechtspflege könnte so (wieder) an Bedeutung gewinnen.[68] Doch die Vorzeichen haben sich geändert. Als eine Art Vorreiter eröffnet § 22 Abs. 5 der Cybercrime Convention 2001, dass die Staaten im Falle der Jurisdiktionskonkurrenz gemeinsam durch Konsultation die Gerichtsbarkeit bestimmen sollen. Was hier beschrieben ist, ist keine Souveränitätsentscheidung, sondern ein staatliches Miteinander in Solidarität. Damit aber wird gerade das Kompetenzverteilungsprinzip, dass *Oehler* bereits in seinem Buch zum Internationalen Strafrecht v. 1983 vorgestellt hat,[69] zum Prinzip der Prinzipe.[70] In der Folge kann das einseitig staatliche Strafanwendungsrecht zum konsultativ vereinbarten internationalen Strafrecht werden. Das zu fordernde Umdenken betrifft sowohl das Verhältnis der jeweils nationalen Strafrechte zueinander als auch die Auslegung der nationalen Strafanwendungsprinzipien im Verhältnis von Bürger und Staat.[71]

So bleiben die nationalen Strafrechte national begrenzt, die völkerrechtlich anerkannten und im Einzelnen in den nationalen Strafrechten geregelten Strafanwendungsprinzipien bleiben anwendbar. Nur ordnen sie sich neu ein. Das bedeutet keine Hierarchie der Strafanwendungsprinzipien.[72] Es bedeutet aber, dass sie umzudenken sind in Begrenzungsrichtlinien zur Anwendbarkeit nationalen Strafrechts.[73] Denn „die Voraussetzungen zur Anwendung des Strafrechts auch auf extraterritoriale Sachverhalte im Pluralismus von Gesellschaften und zunehmender Globalisierung [haben] sich gewandelt".[74] Das betrifft das Verhältnis zwischen den Staaten ebenso wie gegenüber den Beschuldigten und Opfern. Denn letztere wählen mehr und mehr frei, in welchem System sie leben und wessen Regeln sie akzeptieren wollen (und zwar auch real und nicht nur im Internet). Das im Strafrecht in Deutschland noch vorherrschende Rechtsgüterschutzprinzip gelangt damit (erneut) an seine Grenzen. Es müsste letztlich die internationale Verfolgung aller staatlich geschützten Rechtsgüter fordern.[75] Um seiner Funktion zur Wahrung der Friedensordnung noch gerecht werden zu können, ist der Strafgesetzgeber heute mehr denn je auf die Mitwirkung der zu verpflichtenden Staatsbürger angewiesen. Es entsteht eine Solidargemeinschaft. Damit in dieser die Rechte des Beschuldigten und mit ihnen die Rechtsstaatlichkeit des materiellen Strafrechts nicht unter Beschuss geraten, bedarf es im zunehmenden Internationalisierungsprozess klarer Regelungen, die für den Beschuldigten vorhersehbar das materielle Recht bestimmen und ihn nicht zum Gegenstand mehrerer Strafrechte und Strafprozesse werden lassen. Nur dann bilden etwa die europäischen Grundgedanken einer Freizügigkeit der EU-Bürger sowie einer gegenseitigen Anerkennung weiter die Basis freiheitlich demokratischer Entwicklungen.[76]

Plädiert sei hier also für ein gemeinsames Fischernetzwerk, bei dem man freilich aufpassen muss, dass man nicht überfischt!

IV. Fazit

Was bedeutet dies in aller gebotenen Kürze: Piraten gab es immer und wird es weiter geben. Ebenso wird es sich mit den Hackern verhalten. Beide schwimmen in einem Meer an Freiheiten, dass eben auch kriminelle Möglichkeiten eröffnet. Das Internet ist entgrenzt und allenfalls im Hinblick auf die Datenverfügbarkeit, nicht aber territorial eingrenzbar. Das Strafrecht ist jedenfalls in seiner nationalen Ausformung territorial begrenzt. Beides passt nicht zusammen. Unklar ist dabei nicht nur, was es in concreto zu schützen gilt, sondern auch durch wen. Beide Sachfragen bedürfen der internationalen Verständigung, gerade weil sich der Datenverkehr und Informationsaustausch im Internet nicht an staatlichen Grenzen anhalten lässt.

Zur Lösung kommen genau drei Dinge in Frage: Entweder man begrenzt (1) das Internet unter Ausschluss bestimmter user und unter vollständiger user-Kontrolle, baut es also letztlich neu oder man entgrenzt (2) das Strafrecht bzw. die Strafrechte im Sinne eines Internetstrafrechts für alle Internetuser eines world wide web-Staates. Im ersten Fall wird letztlich der user entmündigt und seines derzeit faktischen Hauptkommunikationsmittels beraubt. Er wäre völlig überwacht. Der zweite Fall kommt einer Staatsentmündigung gleich. Schon welches Weltorgan hierüber zu befinden hätte, ist fraglich.

In einem hier angedachten dritten Ansatz wird das Kompetenzverteilungsprinzip zum Prinzip der Prinzipe unter einer neuen Ausrichtung der einseitigen Strafanwendungsrechte

[67] Dies wäre aber wohl derzeit nach extensiver Auslegung des Erfolgsbegriffs im deutschen Strafrecht tatsächlich der Fall, so auch *Sieber*, NJW 1999, 2065 (2067). Vgl. etwa *B. Heinrich*, GA 1999, 72 (76, 82); Einstellungsverfügung des Generalbundesanwalts MMR 1998, 93 (Obiter Dictum).

[68] Ebenso *Kretschmer* (Fn. 6), B. III. (Manuskript S. 262).

[69] Vgl. *Oehler* (Fn. 60), Rn. 134 ff., 682 ff.

[70] Deutlich insoweit *L. Wörner/M. Wörner* (Fn. 39), S. 203 (S. 255).

[71] Dass solches Umdenken auch im nationalen Strafrecht angezeigt ist, zeigen die Ausführungen von *Zabel*, JZ 2011, 617 zur „Governance" im Strafrecht.

[72] Dagegen ausführlich *L. Wörner/M. Wörner* (Fn. 39), S. 203 (S. 227 ff.).

[73] S.o.; ähnlich *Kretschmer* (Fn. 6), B. III. (Manuskript S. 264).

[74] *L. Wörner/M. Wörner* (Fn. 39), S. 203 (S. 255).

[75] Ausdrücklich schon *L. Wörner/M. Wörner* (Fn. 39), S. 203 (S. 235, 255).

[76] *L. Wörner/M. Wörner* (Fn. 39), S. 203 (S. 255).

nicht auf Basis eines rein staatlichen Souveränitätsgedankens, sondern auf Basis eines Solidaritätsgedankens gegenüber den eigenen Staatsbürgern und gegenüber den anderen Staaten. „We need traffic rules", heißt es bei *Ladeur*.[77] So soll etwa die Zuständigkeit für Gerichte in den USA betreffend Tätigkeiten im Internet nach US-amerikanischem Recht dann gegeben sein, wenn der Beschuldigte durch seine Handlung nicht nur geringfügige Auswirkungen (minimum contacts) auf den Staat, welcher die Zuständigkeit der Strafverfolgung für sich in Anspruch nimmt, herbeiführt.[78] Der im Bereich der Rechtshilfe bereits geforderten Solidarität bedarf es im Hinblick auf territorial entgrenzte transnationale und internationale Kriminalitätsbereiche auch für die Strafanwendungsrechte und auch in der Verständigung über die transnational zu schützenden Rechtsgüter selbst. Das sollte auf Dauer zu einem Umdenken weg von staatlich einseitig gedachter Souveränität führen. An Lotus anschließend könnte das die Nachricht von 2011 aus Istanbul sein.

[77] *Ladeur*, German Law Journal 2009, 1201 (1214): „ […] for the internet and the information society, not the protection of any data of a nomadic individualism which fights against any restriction of its autonomy. […] Hybridization and the proliferation of linkages through networks are two of the characteristics of the internet. Instruments for the protection of the variety of the internet and the limitation of state power in the network of networks should make use of these paradigmatic phenomena."

[78] Hervorgehend aus dem Verfahren „Pres-Kap v. System One Direct" (District Court of Appeal of Florida, Third District, Urt. v. 12.4.1994 – No. 93-1440), der ersten Entscheidung, in welcher sich US-Gerichte mit Zuständigkeitskonflikten im Internet beschäftigen mussten. Vgl. dazu *Primig*, Internationales Strafrecht und das Internet, 2002, S. 4 f. (unter: http://rechtsprobleme.at/doks/primig-1-internationales_strafrecht.pdf [12.7.2012]); *Kuner*, CR 1996, 454. Im Internet ist diese Entscheidung einsehbar unter: http://www.loundy.com/CASES/Pres-Kap_v_System_One.html (12.7.2012). S. zu den verschiedenen Bestimmungen des U.S.C. (United States Code) z.B.: http://uscode.house.gov/search/criteria.shtml (12.7.2012). Aus der Entscheidung: „It is settled law that an individual's contract with an out-of-state party alone can (not) automatically establish sufficient minimum contacts in the other party's home forum to support an assertion of in personam jurisdiction against the out-of-state defendant, even where, as here, the foreign defendant allegedly breaches that contract by failing to make the required payments in Florida."