Die Ressourcen der Sicherheitsbehörden sollten deshalb für die Ermittlung der Urheber illegaler Inhalte und deren Löschung eingesetzt werden. Zu diesem Zweck sind u.a. auch private Hotlines zu fördern, die Meldungen der Internetnutzer über illegale Inhalte entgegennehmen und an die jeweiligen Host-Provider weiterleiten. Aufgrund der in Europa geltenden Haftungsregeln müssen die Host-Provider diese Inhalte nach Kenntniserlangung löschen, um eine eigene Strafbarkeit zu vermeiden.[419] Private Hotlines haben hier den Vorteil, dass sie sich anders als staatliche Ermittlungsbehörden unmittelbar an ausländische Host-Provider oder Ermittlungsbehörden wenden können.

Da sich die technischen Möglichkeiten zur Sperrung von Inhalten im Internet laufend weiterentwickeln, sind die Fortschritte in diesem Bereich, insbesondere hinsichtlich des Einsatzes von Deep-Packet-Inspections, genau zu beobachten. Unter rechtlichen Gesichtspunkten wird dabei zu prüfen sein, inwieweit neue Sperrverfahren nach den Grundsätzen des BVerfG in Rechtspositionen der Betroffenen eingreifen.[420] Gegenwärtig sind jedoch keine überzeugenden Gesichtspunkte für eine Änderung der vorliegenden Empfehlungen zu erkennen.

IV. Koordination der nationalen Strafrechtssysteme

Der in der bisherigen Analyse zu Tage getretene Gegensatz zwischen den territorialen Grenzen der *nationalen* Strafrechtsordnungen und der *transnationalen* Internetkriminalität kann nur mit einem transnational wirksamen Strafrecht aufgelöst werden. Mögliche Weiterentwicklungen des bestehenden Regelungsrahmens speziell für das Internet liegen in der extraterritorialen Ausdehnung des eigenen nationalen Strafrechtssystems. Diese Erweiterung kann sowohl im Bereich des nationalen *Strafanwendungsrechts* erfolgen (unten 1.) als auch im Bereich der nationalen *Strafverfolgungsgewalt* mit transnationalen Eigenermittlungen im globalen Cyberspace (2.). Ein transnationales Strafrecht lässt sich ansonsten durch eine verbesserte Koordination der nationalen Strafrechtssysteme schaffen. Eine solche Koordination ist sowohl mithilfe der klassischen Amts- und Rechtshilfe möglich als auch mit der Weiterent-

[419] Zu diesen Verantwortlichkeitsregelungen oben C.I.6.
[420] Vgl. BVerfG BvR 1372/07 vom 17. 2. 2009, Rn. 19.

wicklung internationaler und supranationaler Regelungen und Organisationen (3.).[421]

1. Strafanwendungsrecht

a) Problemstellung

Das nationale Strafanwendungsrecht erfordert für die meisten Straftaten im Internet keine besonderen Regelungen, da die Delikte auf physisch existierenden Computersystemen begangen werden, die als Ort der Handlung oder des Erfolgs einen Tatort nach §§ 3, 9 StGB begründen können. Schwierigkeiten mit dem Territorialitätsprinzip ergeben sich im Wesentlichen nur für abstrakte Gefährdungsdelikte, insbesondere im Bereich der illegalen Inhalte, bei denen der „zum Tatbestand gehörende Erfolg" i.S.v. § 9 StGB nur schwer in Deutschland zu konstruieren ist. Hier stellt sich die Frage, ob das deutsche Strafrecht (evtl. sogar verstärkt) Anwendung finden soll, wenn auf ausländischen Servern Inhalte gespeichert sind, die in Deutschland mit einem „Mausklick" abrufbar und nach deutschem Recht strafbar sind.[422] Denn aus dem nationalen Blickwinkel ist es zunächst schwer verständlich, wenn die gleichen Inhalte in körperlicher Form – beispielsweise in Zeitschriftenpublikationen – verfolgt werden, in der noch leichter zugänglichen Form von Angeboten auf Servern dagegen nicht.

Eine solche verstärkte Ausdehnung des deutschen Strafrechts auf ausländische Server würde nicht zwingend in die Souveränitätsrechte fremder Staaten eingreifen. Denn nach internationalem Recht kann das nationale Strafanwendungsrecht grundsätzlich auch auf Sachverhalte angewandt werden, die auf dem Territorium eines Drittstaats stattfinden oder einen anderen Bezug zu diesem aufweisen. Das Völkerrecht setzt der nationalen Strafgewalt zwar durch das gewohnheitsrechtliche Prinzip der Nichteinmischung Grenzen.[423] Die Wahrnehmung einer extraterritorialen Strafgewalt gegenüber Drittstaaten oder deren Angehörigen stellt jedoch so lange keine Verletzung des Prinzips der Nichteinmischung dar, wie ein hinreichender Anknüpfungspunkt zwischen Straftat und staatlicher Strafgewalt besteht.[424]

---

[421] Zusammenfassend *Sieber,* ZStW 121 (2009), 1 (16 ff.).

[422] Vgl. oben C.IV.1.

[423] Grundlegend StIGH, *Lotus,* PCIJ Series A No. 10, S. 71 (90).

[424] Allgemein zur extraterritorialen Souveränitätsausübung IGH, *Nottebohm,* ICJ Reports 1955, 3, 4, 23; IGH, *Barcelona Traction,* ICJ Reports 1970, 1, 42; BVerfGE 63, 343 (369); 77, 137 (153). Insbesondere zur Strafgewalt BVerfGE 92, 277 (320 f.); BGHSt 27, 30 (32); 34, 334.

Ein solcher Anknüpfungspunkt liegt in der Regel vor, wenn eines der völkerrechtlichen Prinzipien des internationalen Strafrechts einschlägig ist.[425]

Die hieraus resultierenden Jurisdiktionskonflikte erfordern allerdings eine zurückhaltende Ausübung der extraterritorialen Strafgewalt[426] und eine Abwägung der Interessen der betroffenen Staaten. Maßgebliche Bedeutung hat dabei das Rangverhältnis der völkerrechtlichen Prinzipien des internationalen Strafrechts.[427] Aufgrund der völkerrechtlichen Bedeutung des Staatsterritoriums für die Begründung und Begrenzung der Hoheitsausübung[428] besteht ein genereller Vorrang des Territorialitätsprinzips.[429] Das Staatsschutzprinzip[430] ist dem Territorialitätsprinzip gleichrangig oder unmittelbar nachgeordnet. Eine maßvolle und durch berechtigte Schutzinteressen legitimierte Ausdehnung des deutschen Strafrechts auf ausländische Sachverhalte ist daher mit dem Völkerrecht grundsätzlich vereinbar.

Der Gesetzgeber könnte somit eine entsprechende Ausdehnung des deutschen Strafanwendungsrechts für die allgemeinen Gefährdungsdelikte im materiellen Recht durch eine Ergänzung der Gefährdungstatbestände um ein Gefährdungsmerkmal erleichtern, das im Fall der Deliktsbegehung einen zum Tatbestand gehörenden Erfolg i.S.v. § 9 StGB zur Folge hätte. Eine solche Lösung hätte den Vorzug, dass sie deliktsspezifisch erfolgen und dabei auch die völkerrechtliche Legitimation für die Einbeziehung der jeweiligen Auslandssachverhalte liefern würde. Weitere Optionen zur Ausdehnung des deutschen Strafanwendungsrechts wären die Modifikation des Erfolgsorts von § 9 StGB speziell für Straftaten im Internet, die Aufnahme einzelner Gefährdungsdelikte in die von § 5 StGB genannten Auslandstaten gegen inländische Rechtsgüter oder die Ausdehnung des Katalogs der Auslandstaten gegen international geschützte Rechtsgüter in § 6 StGB.

So wünschenswert eine solche Ausdehnung der Strafgewalt aus nationaler Sicht erscheinen mag, so problematisch ist sie jedoch aus

---

[425] *Jescheck/Weigend,* Lehrbuch des Strafrechts, 5. Aufl. (1996), S. 167; *Hailbronner,* in: Vitzthum, Völkerrecht, 4. Aufl. (2007), Rn. 144 ff.; *Verdross/Simma,* Universelles Völkerrecht, 3. Aufl. (2010), § 1183 f.

[426] Vgl. IGH, *Barcelona Traction,* separate opinion *Fitzmaurice,* ICJ Reports 1970, 1 (Rn. 70).

[427] *Ambos,* in: MüKo-StGB, Vor §§ 3–7, Rn. 55 m.w.N. (Fn. 406). Vgl. auch Empfehlung 20 der Versammlung des Europarats („Draft European Convention on Conflicts of Jurisdiction in Criminal Matters", 1965).

[428] Vgl. allein Art. 2 Abs. 1, Abs. 4, Abs. 7 UN-Charta.

[429] Siehe dazu rechtsvergleichend *Ryngaert,* International Criminal Law Review 9 (2009), 187 ff.

[430] Vgl. *Jescheck/Weigend,* FN 425, S. 169.

der übergeordneten internationalen Perspektive. Dies gilt vor allem wegen der damit verbundenen Nachahmungseffekte in anderen Staaten und der daraus resultierenden Normkollisionen: Würden andere Rechtsordnungen einer solchen extraterritorialen Regelung mit ihren speziellen Straftatbeständen folgen, so käme es im Internet zum Geltungsanspruch einer Vielzahl unterschiedlicher nationaler Strafbestimmungen für illegale Inhalte. Der Verurteilung des australischen Staatsbürgers *Toeben* in Deutschland wegen Volksverhetzung und Verbreitung der Auschwitz-Lüge auf einem australischen Computer[431] könnten dann rasch entsprechende Strafverfahren anderer Staaten gegen Unternehmer, Verleger und Journalisten folgen, deren Alkoholwerbung, erotische Bilder oder politische Publikationen auf deutschen Servern nach ausländischen Rechtsordnungen strafbar sind. Da eine solche Entwicklung für den globalen Cyberspace schädlich wäre, sollte die Ausdehnung des Strafanwendungsrechts auf ausländische Computersysteme vermieden und durch gemeinsame internationale Lösungen ersetzt werden.

b) Empfehlung zum Strafanwendungsrecht im Internet

Die Anwendung einer Vielzahl unterschiedlicher nationaler Strafvorschriften auf illegale Inhalte im Internet muss nach Möglichkeit verhindert werden. Die zum Schutz des nationalen Territoriums notwendige Ausdehnung des Strafanwendungsrechts auf ausländische Server sollte daher so weit wie möglich im Rahmen internationaler Vereinbarungen erfolgen, die einen Katalog von strafrechtlichen Mindestvorschriften für alle Staaten definieren. Die Bundesrepublik Deutschland sollte sich dafür einsetzen, dass die Vereinten Nationen (UNODC) zusammen mit anderen internationalen und regionalen Institutionen (insbes. des Europarats) auf der Grundlage der bereits bestehenden Abkommen entsprechende Mindestvorschriften entwickeln, für die dann besonders in Bezug auf das Internet ein erweitertes Universalitätsprinzip gelten kann. Ohne einen solchen internationalen Konsens ist eine extraterritoriale Ausdehnung des nationalen Strafanwendungsrechts auch nicht durchsetzbar.

Das notwendige internationale Regelwerk erfordert – ähnlich wie andere regionale und internationale Empfehlungen für strafrechtliche Mindeststandards – auch Vorschriften über das Verhältnis und den Vorrang der parallel anwendbaren nationalen Strafanwendungsvorschriften. Diese Metaregeln sollten vom Vorrang des Territorialitätsprinzips ausgehen, jedoch auch das Schutzprinzip für nationalstaat-

[431] *BGH*, NJW 2001, 624 ff.

liche Interessen sowie Praktikabilitätsgründe des durchzuführenden Strafverfahrens berücksichtigen.[432]

Da derartige Kollisions- und Koordinationsnormen nicht präzise definiert werden können, müssen sie durch prozedurale und institutionelle Regelungen ergänzt werden, um eine Mehrfachverfolgung zu verhindern. Hierzu sollte das Netzwerk der bereits bestehenden internationalen Kontaktpunkte zur Verfolgung von Cybercrime unter Mitwirkung der Vereinten Nationen, Interpol und regionaler Organisationen ausgebaut werden.

2. Grenzüberschreitende Eigenermittlungen im globalen Cyberspace

a) Problemstellung

Der grenzüberschreitende Charakter der mithilfe des Internets begangenen Delikte erfordert nicht nur eine transnationale Rechtsgeltung für die strafrechtliche Aburteilung *(jurisdiction to adjudicate),* sondern vor allem auch eine transnationale Rechtsdurchsetzung *(jurisdiction to enforce).* Im Vergleich zu anderen Kriminalitätsformen bietet das Internet hier besondere Möglichkeiten, strafprozessuale Aufklärungsmaßnahmen über Datenleitungen im Ausland selbst vorzunehmen. Den – für viele Staaten verlockenden – Möglichkeiten transnationaler Eigenermittlungen im globalen Cyberspace setzt die Souveränität der betroffenen Staaten völkerrechtliche Grenzen. Für die Beurteilung von transnationalen Internetermittlungen und als Grundlage für zukünftige internationale Aktivitäten ist daher zunächst eine differenzierende Analyse des einschlägigen Völkerrechts erforderlich, die in der bisherigen Diskussion noch weitestgehend fehlt.[433]

b) Ermittlungsgrenzen des allgemeinen Völkerrechts

aa) Souveränitätseingriff

Hoheitliche Maßnahmen im Ausland zur Durchsetzung innerstaatlichen Rechts ohne Ermächtigung des Drittstaats greifen grund-

---

[432] Zu den entsprechenden Kollisionsregeln und dem Grundsatz des *ne bis in idem Eser,* in: Sieber/Brüner/Satzger/v. Heintschel-Heinegg (Hg.), FN 9, § 36.

[433] Vgl. die Ansätze bei *Gercke,* Rechtswidrige Inhalte im Internet, 2010, S. 171; *Seitz,* Yale Journal of Law & Technology 2004–2005, 23 (35 f.).

sätzlich in dessen völkerrechtliche Souveränität ein.[434] Zu diesen Hoheitsmaßnahmen gehören auch grenzüberschreitende Ermittlungsmaßnahmen.[435] Denn der souveräne Staat kann – wie auch die Rechtshilfeabkommen zeigen – allein darüber entscheiden, ob strafrechtliche Ermittlungsmaßnahmen auf seinem Territorium erfolgen sollen. Zu den – die Souveränität tangierenden – Hoheitsmaßnahmen gehören auch grenzüberschreitende Ermittlungsmaßnahmen über das Internet, da sie Datenverarbeitungsprozesse auf Servern verursachen, die auf fremdem Territorium stehen. Dabei ist völkerrechtlich unerheblich, dass sich der Amtsträger nicht physisch auf fremdem Territorium befindet. Auch vom Inland in das Ausland hineinreichende Maßnahmen – z. B. mit technischen Systemen – greifen in die Souveränität des Drittstaats ein.[436] Für einen Souveränitätseingriff reicht es aus, dass eine hoheitliche Maßnahme indirekt Lebensbereiche des anderen Staats betrifft, für die dieser in Ausübung seiner Souveränität allein regelungs- und entscheidungsbefugt ist.[437] Mit dem zunehmenden Cloud-Computing verlieren allerdings die Interessen des Staates, in dem die Daten (zufällig) gespeichert sind, Bedeutung gegenüber den Interessen des Staates, auf dessen Territorium die Daten kontrolliert werden.

Damit stellt sich bei grenzüberschreitenden Online-Ermittlungsmaßnahmen die Frage, ob und unter welchen Voraussetzungen derartige Eingriffe gerechtfertigt sein können. Dies erfordert eine differenzierende Betrachtung verschiedener Sachverhaltskonstellationen und Rechtfertigungsgründe.

bb) Zugriff auf öffentlich zugängliche Daten

Eine *völkervertragliche* Rechtfertigung für Zugriffe auf *öffentlich zugängliche* Daten folgt für die Vertragsstaaten aus Art. 32 a der Cybercrime-Konvention.[438] Ein solcher Zugriff auf öffentlich zugängliche Daten könnte ungeachtet des Speicherorts auch für Nichtvertragsstaaten *völkergewohnheitsrechtlich* begründet werden, wenn in der Staatengemeinschaft eine entsprechende Rechtsüberzeugung

[434] Grundlegend StIGH, *Lotus,* PCIJ Series A No. 10, S. 4 (18); *Island of Palmas*-Fall, Reports of International Arbitral Awards (1949), S. 829 (838). Ebenso BGHSt 45, 188 (192).

[435] BGHSt 45, 188 (192).

[436] Grundlegend *Trail Smelter,* Reports of International Arbitral Awards Vol. III (1938), S. 1905 (1965). Vgl. IGH, *Legality of the threat or use of nuclear weapons,* ICJ Reports 1996, 226 ff. (Rn. 29). Ebenso BGHSt 45, 188 (192); *Verdross/Simma,* FN 425, § 456.

[437] IGH, *Military and paramilitary activities in and against Nicaragua,* ICJ Reports 1986, S. 14 ff. (Rn. 205, 241, 251).

[438] Dazu oben C. IV.2.b).

(opinio iuris) vorherrschte und diese durch eine allgemeine Übung der Staatengemeinschaft *(consuetudo)* bestätigt würde.[439] Da keine präzisen öffentlichen Informationen über die (Internet-)Ermittlungsmethoden der nationalen Strafverfolgungsbehörden und deren Beurteilung vorliegen, lassen sich derzeit jedoch keine abschließenden Aussagen zu den entsprechenden Rechtsüberzeugungen und Übungen treffen.[440] Angesichts der heute selbstverständlichen weltweiten Nutzung des Internets, der häufig fehlenden Kenntnis der Nutzer über den Speicherort abgerufener Daten sowie der geringen Eingriffsintensität einer Abfrage öffentlicher Daten im globalen Cyberspace spricht jedoch viel für eine entsprechende Rechtsüberzeugung und Übung der Staatengemeinschaft.

cc) Zugriff auf nichtöffentlich zugängliche Daten

Beim Zugriff auf *nichtöffentlich zugängliche* Daten folgt eine *völkervertragsrechtliche* Rechtfertigung aus Art. 32 b) der Cybercrime-Konvention für deren Vertragsstaaten, wenn die zugriffsberechtigte Person ihre rechtmäßige und freiwillige Zustimmung zum Zugriff auf die Daten durch ausländische Ermittler erteilt hat.[441]

Eine hierüber hinausgehende *völkergewohnheitsrechtliche Rechtfertigung* des Zugriffs auf nichtöffentliche Daten im Rahmen grenzüberschreitender Ermittlungsmaßnahmen scheidet derzeit aus. Verlässliche Angaben zu einer solchen Übung liegen nicht vor. Vielmehr bestehen durchgreifende Zweifel an dieser Rechtsauffassung: Gegen die Annahme einer Art. 32 b) der Cybercrime-Konvention entsprechenden völkergewohnheitsrechtlichen Regel spricht zunächst, dass schon unter den Vertragsstaaten der Cybercrime-Konvention keine Einigkeit über Auslegung und Grenzen der Vorschrift besteht,[442] so dass eine völkergewohnheitsrechtlich relevante einheitliche Rechtsauffassung fehlt. Dagegen spricht auch, dass die Zustimmung der zugangsberechtigten (Privat-)Person zum Zugriff auf ihre Daten durch eine ausländische Hoheitsgewalt die Souveränitätsverletzung des betroffenen Staates nicht beseitigen kann, da das Individuum nicht über

---

[439] Art. 38 Abs. 1 lit. b) IGH-Statut. Zur – im Einzelfall auch kurzen Dauer der Übung siehe IGH, *North Sea Continental Shelf,* ICJ Reports, 1969, 3 (43).

[440] Vgl. dazu auch *Charney,* Washington Law Review 61 (1986), 971 ff. Siehe dazu auch *United States Department of Justice,* Searching and Seizing Computers and obtaining electronic evidence in criminal investigations, S. 56.

[441] Dazu oben C. IV.2.b).

[442] *Council of Europe,* Committee of experts on the operation of European Conventions on co-operation in criminal mattters (PC-OC), replies on mutual legal assistance in computer-related cases, 1. 12. 2008 (PC-OC (2008) 09 rev), Stellungnahmen von Finnland (S. 14), Deutschland (S. 15), Lettland (S. 18), Slowakei (S. 37), Ukraine (S. 44).

die staatliche Souveränität dispositionsbefugt ist.[443] Eine über Art. 32 der Cybercrime-Konvention hinausgehende allgemeine völkergewohnheitsrechtliche Regel, die den grenzüberschreitenden Zugriff auf nichtöffentliche Daten ohne die Ermächtigung des betroffenen Staates zulässt, wird auch von vielen an der Cybercrime-Konvention nicht beteiligten Staaten abgelehnt.[444] Fälle eigenmächtiger Ermittlungen haben zu erheblichen diplomatischen Verstimmungen geführt.[445] Auch die oben dargestellte Streichung von Art. 21 im Vorschlag für einen Rahmenbeschluss über die Europäische Beweisanordnung von 2003 spricht – sogar innerhalb des Verhältnisses der EU-Mitgliedstaaten – gegen eine entsprechende Rechtsüberzeugung.[446]

Eine Rechtfertigung des grenzüberschreitenden Zugriffs auf nichtöffentliche und im Ausland gespeicherte Daten ist in üblichen Kriminalitätsfällen auch nicht aus *sonstigen völkerrechtlichen Rechtfertigungsgründen* abzuleiten. In Fällen „normaler" Kriminalität lassen sich grenzüberschreitende Online-Ermittlungen ohne die Zustimmung des betroffenen Drittstaats nicht als Ausübung des völkerrechtlichen Selbstverteidigungsrechts gemäß Art. 51 UN-Charta rechtfertigen. Ein solches Verteidigungsrecht setzt voraus, dass ein Staat Opfer eines „bewaffneten Angriffs" i. S. d. Art. 51 UN-Charta und dieser dem fraglichen Staat zurechenbar ist.[447] Ein Selbstverteidigungsrecht gemäß Art. 51 UN-Charta kommt daher allenfalls in den Fällen des Cyberwar in Betracht. Diskutiert wurde dies etwa anlässlich massenhafter DDoS-Angriffe gegen estnische Regierungs-Server sowie Computersysteme von Banken, Zeitungen und Unternehmen im Jahr 2007.[448] Auch der Angriff des Computerwurms Stuxnet auf die iranische Urananreicherungsanlage in Natanz[449] wird häufig mit dem Schlagwort „Cyberwar" in Verbindung gebracht. Allerdings ist hier offen, ob dieser Sabotageakt die notwendige Qualität für eine Qualifizierung als „bewaffneter Angriff" erreicht.[450]

---

[443] *Akehurst,* in: Weiler/Nissel (Hg.), International Law, Vol. III, 171 (173). Vgl. aber *United States Department of Justice,* FN 440, S. 56: "The U.S. view (and that of some other countries) is that prior consultation is not required to […]. (2) access materials in Country A with the voluntary consent of a person who has lawful authority to disclose the materials."

[444] SEV Nr. 185, Explanatory Report, FN 200, Nr. 293; *Council of Europe,* Cybercrime and Internet jurisdiction (discussion paper, 5. 3. 2009), S. 27 (Rn. 79), a. A. *Seitz,* Yale Journal of Law & Technology 2004–2005, 23 (45).

[445] Siehe dazu den Fall *Gorshkov-Ivanov: United States v. Ivanov,* 175 F. Suppl. 2 d 367 (D. Conn 2001); *United States v. Gorshkov,* 2001 WL 1 024 026 (W.D. Wash. 2001).

[446] Oben C. IV.2.b).

[447] Zur Zurechnung *Ipsen,* in: ders. (Hg.), Völkerrecht, 5. Aufl. (2004), S. 636 ff.

[448] Die estnische Regierung beschuldigte zunächst die russische Regierung, konnte hierfür jedoch keine Beweise liefern. Vgl. http://heise.de/-138 918.

[449] Dass Stuxnet tatsächlich die Anlage in Natanz zum Ziel hatte, gilt mittlerweile als gesichertes Wissen, siehe *Schneier,* Eintrag vom 23. 2. 2012, online verfügbar unter, http://www.schneier.com/blog/archives/2012/02/another_piece_o.html.

[450] Ähnliche Gründe sprechen auch gegen eine Rechtfertigung durch völkerrechtlichen rechtfertigenden Notstand. Hierfür wäre erforderlich, dass ein Staat eine schwerwiegende und unmittelbar bevorstehende Beeinträchtigung wesentlicher Inte-