Überlegungen zur Einrichtung

eines

International Court for Cyber Crime

Denn der beste Weg die Zukunft zu gestalten, ist das Begreifen der Gegenwart

Prof. W. Kraft PhD

unter Mitarbeit von
Dr. Claudia Streit

Präambel

Der World Council for Law Firms and Justice hat es sich zur Aufgabe gemacht, sich für eine Evaluierung und Harmonisierung der Rechtssysteme rund um die Welt einzusetzen. Damit dieses Ziel nicht nur Vision bleibt, sind viele kleine und große Schritte erforderlich. Die vorliegenden Überlegungen zur Einrichtung eines International Court for Cybercrime sollen der Ausgangspunkt für eine internationale Initiative sein, die einen wichtigen Meilenstein auf dem langen Weg darstellt.

Entstanden ist die Idee im Zuge der Entwicklung eines Programms für eine international besetzte WCLF Konferenz zum Thema Internetkriminalität, die im kommenden Jahr in Hamburg stattfinden soll. Damit stand auch die Frage der internationalen Strafverfolgung und Rechtsdurchsetzung bei Vergehen im Cyberspace auf der Agenda. Offensichtlich ist das gegenwärtig hierfür vorhandene Instrumentarium der ungeheuer schnellen Entwicklung des Internets und den damit verbundenen neuartigen Straftaten mit internationaler Dimension nicht einmal annähernd gewachsen. Die Einrichtung eines Internationalen Strafgerichtshofs zur Verfolgung von Internetverbrechen könnte die vorhandene Lücke ganz oder teilweise schließen. Seine Verwirklichung erfordert viel Kompetenz, Einsatz und Mut – auch den Mut, überkommene Grenzen und Dogmen zu ignorieren und konsequent in die Zukunft zu denken.

Die nachstehenden Ausführungen können nur ein erster Hinweis auf den einzuschlagenden Weg sein. Den Anfang macht eine Bestandsaufnahme bestehender Initiativen. Sie zeigt, wie virulent das Thema ist, aber auch, wie weit die Vorstellungen über eine internationale Einigung auseinanderfallen. Die darauf folgende Bewertung der bisherigen Anstrengungen zur Vereinheitlichung der Rechtslage mündet in eine Skizzierung der Aufgaben, die eine WCLF Arbeitsgruppe zur Einrichtung eines International Court for Cybercrime wahrnehmen könnte. Eine solche Arbeitsgruppe könnte wichtige Brücken zu anderen Organisationen schlagen und wäre so in der Lage, ein weltweit sichtbares Zeichen für das Recht zu setzen.

Was die Zukunft betrifft,
so ist deine Aufgabe nicht,
sie vorauszusehen,
sondern sie zu ermöglichen.

Antoine de Saint-Exupéry

1. Was fällt unter den Begriff Cybercrime?

Die Begriffe „Cybercrime“ und „Internetkriminalität“ sind nicht ganz deckungsgleich – Cybercrime schließt sowohl die deutschen Begriffe Computerkriminalität als auch Internetkriminalität ein. In diesem Sinne wird er nachfolgend verwendet. Unter Cybercrime fallen demnach

- Verbrechen, bei denen ein Computer oder Computernetzwerk das ***Ziel*** des Angriffs ist.
- Verbrechen, bei denen ein Computer oder Computernetzwerk das ***Instrument*** des Angriffs ist.[1]

Zur ersten Kategorie gehören beispielsweise unerlaubter Zugriff auf Computer oder Computernetzwerke, Datendiebstahl, „Salamiangriffe“, Trojaner und sog. „logische Bomben“. Unter die zweite Kategorie fallen z. B. Verbrechen im Finanzbereich, der Verkauf illegaler Artikel, Verbreitung von Kinderpornographie, illegales Internetglücksspiel und Intellectual Property Vergehen.

Neben der Klassifikation nach Art des Verbrechens lässt sich eine weitere Unterteilung nach Opfern vornehmen. Cybercrimes können gegen

- ***Individuen*** (mit einer weiteren Unterscheidung nach Person und persönlichem Eigentum)
- ***Organisationen***
- oder die ***Gesellschaft insgesamt***

gerichtet sein. Unter die Verbrechen gegen Organisationen fallen u.a. unberechtigter Zugriff auf oder Kontrolle über ein Computersystem, unberechtigte Verschaffung und Besitz von Informationen sowie Cyberterrorismus gegen Regierungsorganisationen. Als gegen die Gesellschaft insgesamt gerichtet werden u. a. Verbreitung von Kinderpornographie, illegaler Handel mit Menschen oder Drogen sowie Verbrechen im Finanzsektor eingestuft.[2]

2. Uneinheitliche nationale Gesetzgebungen

Im Detail besteht keine globale Einigkeit darüber, welche Tatbestände im Cyberspace strafbar sein sollen. Zwar haben in den vergangenen 20 Jahren etliche Länder und regionale Organisationen Gesetzgebungen und Rechtsrahmen zur Bekämpfung von Cybercrime geschaffen. Aber auch wenn sich Gemeinsamkeiten abzeichnen, bleiben die Unterschiede zwischen den nationalen Gesetzgebungen signifikant. Dafür gibt es mehrere Gründe. Zum einen sind die Auswirkungen derselben Vergehen in den verschiedenen Ländern unterschiedlich stark zu spüren. Zum anderen gibt es aber auch Unterschiede in der Rechtsauffassung: Zum Beispiel ist das, was in einem Land unter illegale Inhalte fällt, in einem anderen Land vom Prinzip der Freiheit der Rede gedeckt.

Damit internationale Ermittlungen und Strafverfolgung funktionieren können, ist jedoch ein gewisser Grad an gemeinsamem Verständnis und Harmonisierung der Gesetzgebung erforderlich.[3] Bestehende Rechtshilfeabkommen basieren in sehr vielen Ländern auf dem Prinzip der „dual criminality“: Nur

---

1 Referiert nach M. Ayilyath, Cyber Crimes and the Legal Framework against it – International and Indian Perspectives, Oktober 2010, S. 1 [= Ayilyath 2010]. Die dritte Kategorie – Verbrechen, bei denen ein Computer(netzwerk) nur zufällig eine Rolle spielt – wird hier außer Acht gelassen, da sie für einen Internationalen Strafgerichtshof nicht relevant ist.

2 Ayilyath 2010, S. 2

3 Draft Topics des Wiener Treffens der UN Expert Group on Cybercrime vom 17.-21.01.2011, UNODC/CCPCJ/EG.4/2011/2, [= UNODC Expert Group 2011], S. 8/9

wenn ein Tatbestand in beiden Ländern rechtswidrig ist, findet Rechtshilfe statt. Außerdem ist nur im Fall einer grundsätzlichen Einigung das Zustandekommen einer internationalen Gesetzgebung in Form eines völkerrechtlichen Abkommens und eine Rechtsprechung durch ein internationales Gericht überhaupt denkbar.[4]

3. Internationale Strafverfolgung derzeit

Grundsätzlich existieren vier Quellen für eine Rechtsgrundlage internationaler Zusammenarbeit bei der Verbrechensbekämpfung. Auslieferungen, gegenseitige Rechtshilfe und Zusammenarbeit bei Beschlagnahmungen können zum einen auf der Grundlage internationaler oder regionaler Abkommen zur Verfolgung bestimmter Verbrechen stattfinden. In diese Kategorie fällt beispielsweise die European Convention on Cybercrime. Dann kommen regionale Verträge zur internationalen Zusammenarbeit bei der Verbrechensbekämpfung generell in Frage, also z.B. bereits bestehende Auslieferungs- oder Rechtshilfeabkommen. Weiterhin können bilaterale Abkommen desselben Inhalts sowie nationales Recht eine fallweise internationale Zusammenarbeit zulassen.[5]

Schließlich sind auch Abkommen teilweise einschlägig, die die gegenseitige Anerkennung von in nationaler Rechtsprechung ergangenen Urteilen zum Gegenstand haben. Zu nennen wären hier insbesondere die „The Hague Convention on Foreign Judgments in Civil and Commercial Matters“ aus dem Jahr 1971 sowie die „EC Convention on Jurisdiction and the Enforcement of Judgment in Civil and Commercial Matters“ aus dem Jahr 2000.[6] Angesichts der geringen Zahl der Unterzeichner dieser Abkommen[7] lässt sich jedoch bereits erahnen, wie schwer sich die Nationalstaaten mit der Aufgabe ihrer Souveränität in der Rechtsprechung tun.

Die derzeit vorhandenen Möglichkeiten der Rechtshilfe und internationalen Zusammenarbeit bei der Bekämpfung von Cyberverbrechen werden überwiegend als ungenügend bewertet.[8]

4. Bestehender internationaler Rechtsrahmen

Es scheint allgemein anerkannt zu sein, dass die Council of Europe Convention on Cybercrime– neben dem Commonwealth Model Law on Cybercrime – den umfassendsten Ansatz für einen internationalen Rechtsrahmen entwickelt hat, da sie sowohl das Strafrecht und das Verfahrensrecht abdeckt, als auch Fragen der internationalen Zusammenarbeit aufgreift.[9]

Die Konvention definiert eine große Anzahl von Cyberverbrechen, unter anderem illegalen Zugriff, illegale Eingriffe, Daten- und Systemanipulation, Betrugsdelikte, Delikte im Zusammenhang mit Kinderpornographie und Urheberrechtsdelikte.[10] Eine Aufzählung der Einzelheiten des Abkommens

---

4 Ähnlich gelagert ist die Problematik bei der angedachten und im Vertrag von Lissabon als Ziel aufgenommenen Einführung eines Europäischen Staatsanwalts, die auch deshalb keine Fortschritte macht, weil es selbst in der EU an einer einheitlichen strafrechtlichen Grundlage fehlt. Vgl. hierzu z.B. Silke Nürnberger, Die zukünftige Europäische Staatsanwaltschaft – eine Einführung, in: ZJS 5/2009, S. 494-505

5 UNODC Expert Group 2011, S. 12

6 Ayilyath 2010, S. 8

7 Die EC Convention wurde beispielsweise nur von der Tschechischen Republik, Estland, Zypern, Lettland, Litauen, Ungarn, Malta, Polen sowie Slowenien und der Slowakischen Republik unterschrieben.

8 Diese Ansicht wird von deutschen Internetstrafrechtsexperten, auch aus dem Kreis des WCLF, geteilt: Vgl. bspw. Dr. Jürgen-P. Graf, Aktuelle Rechtsprechung des BHG zu Fragen der Internetkriminalität, Vortrag bei der Deutschen Richterakademie, 27.3.2010, S. 64

9 UNODC Expert Group 2011, S. 16, gemeinsam mit vielen anderen.

10 Ayilyath 2010, S. 7

würde hier zu weit führen. Im Zusammenhang mit der Idee eines Internationalen Strafgerichtshof für Cyberdelikte ist jedoch interessant, dass sich die Unterzeichner verpflichten, die Rechtsinstrumentarien und Verfahrensweisen, die zur Verfolgung von Cyberverbrechen erforderlich sind, einzuführen. Außerdem werden die Unterzeichner zur Einführung einer gesetzlichen Vorschrift zur Datenspeicherung verpflichtet, damit im Falle von strafrechtlichen Untersuchungen auf solche Daten zugegriffen werden kann. Darüber hinaus muss ein Unterzeichnerland seine zuständigen Institutionen dazu ermächtigen, unter definierten Bedingungen zum Zweck von Ermittlungen auf Computersysteme zugreifen zu können.[11] Schließlich besagt Kapitel III, dass die der Konvention angehörenden Parteien bei der Strafverfolgung so weit wie möglich miteinander kooperieren sollen, wobei diese Zusammenarbeit auf der Basis einer einheitlichen oder reziproken Gesetzgebung erfolgen soll.[12]

5. Arbeitsgruppen zur Schaffung wirksamer Instrumente zur Rechtsdurchsetzung auf internationaler Ebene

- ***UN Kommission zur Verbrechensvorbeugung und Strafgerichtsbarkeit (UNODC) – Regierungsübergreifende Expertengruppe zur Internetkriminalität***

  Die regierungsübergreifende Expertengruppe der UNODC zur Internetkriminalität wurde 2010 eingerichtet und hat die Aufgabe, Möglichkeiten zu prüfen, effektiv gegen Internetkriminalität vorzugehen. Sie soll ermitteln, wie sich vorhandene juristische Instrumente stärken lassen bzw. neue nationale und internationale juristische oder anderweitige Mittel gegen Internetkriminalität vorschlagen. Die Agenda des ersten (und bislang einzigen) Treffens der Gruppe[13] beschäftigte sich mit den folgenden juristischen Themenkomplexen: Harmonisierung der Gesetzgebung, substantielles Strafrecht, Ermittlungsinstrumente, internationale Kooperation bei der Rechtsdurchsetzung, Sicherung elektronischer Beweise, Haftung von Internetserviceprovidern. Aber auch nichtjuristische Mittel und Strategien wurden angesprochen, unter anderem technische Unterstützungsmöglichkeiten und die Abwehrstrategien des privaten Sektors gegen Internetkriminalität. Das erste Treffen diente vor allem einer Bestandsaufnahme, welche Themenkomplexe überhaupt und in welchem Umfang bzw. welcher Tiefe von der Expertengruppe bearbeitet werden sollen und erbrachte daher keine konkreten Handlungsvorschläge. Die Einrichtung eines internationalen Gerichtshofs für Cyberverbrechen taucht indes in der ausführlichen Agenda nicht auf.

  Einerseits ist der umfassende Ansatz der Initiative zu begrüßen, andererseits besteht sichtbar die Gefahr, dass sich die Expertengruppe jahrelang mit Bestandsaufnahmen beschäftigen wird und die Erarbeitung konkreter Vorschläge dabei in den Hintergrund gerät.

- ***EU – US „Working Group on Cybersecurity und Cybercrime“***

  Die Vereinigten Staaten und die Europäische Union haben beim US-EU Gipfeltreffen im November 2010 in Lissabon eine „Working Group on Cybersecurity und Cybercrime“ ins Leben gerufen. Ihre Aufgabe ist die Entwicklung von gemeinsamen Herangehensweisen bei verschiedenen Problemen der Internetkriminalität und Internetsicherheit. Zu ihren Aufgaben gehört die Entwicklung eines gemeinsamen Kooperations- und Übungsprogramms bei kritischen Cybervorfällen[14],

[11] Ayilyath 2010, S. 6
[12] Ayilyath 2010, S. 7
[13] vom 17.-21. Januar 2011 in Wien
[14] Concept Paper der EU-US Working Group on Cyber-Security and Cyber Crime, April 2011, S. 1 [EU-US WG Concept Paper 2011]

sowie die Entwicklung von Public-Private Partnership Modellen für die Zusammenarbeit von Regierungsinstitution und Industrie bei der Herstellung von Internetsicherheit und Bekämpfung von Cyberkriminalität.[15] Besonders wichtig in diesem Zusammenhang ist ihr Auftrag, die Cybercrime Convention des Europäischen Rates voranzubringen: Neben einem Programm zum Beitritt aller EU-Mitgliedsstaaten soll sie auch die Zusammenarbeit mit Staaten außerhalb der EU voranbringen, damit diese die Standards der Konvention erfüllen und der Konvention ebenfalls beitreten.[16] Erwähnenswert sind noch der explizite Auftrag der Bekämpfung von Kinderpornographie im Netz sowie die Tatsache, dass Deutschland und die USA ihre Positionen in der oben genannten UNODC Cybercrime Expertengruppe miteinander abstimmen wollen.[17] Auch wenn die Arbeitsgruppe bislang noch keine Ergebnisse präsentieren kann, erscheinen ihre Zielsetzungen konkret und umsetzbar.

- ***EastWest Institute Cybercrime Legal Working Group: Initiative für einen Internationalen Strafgerichtshof***

  Einen Internationalen Strafgerichtshof für den Cyberspace (ICTC) fordert der norwegische Richter Stein Schjolberg, der sich des Themas im Rahmen einer Arbeitsgruppe des EastWest Institutes (EWI) angenommen hat (Cybercrime Legal Working Group).[18] Die Mitglieder der Arbeitsgruppe sind unabhängige und nicht regierungszugehörige Experten für Internetsicherheit und Internetkriminalität. Die Arbeitsgruppe hat den Auftrag, Empfehlungen für neue juristische Mittel zu erstellen, um Internetkriminalität und Cyberangriffe zu bekämpfen.

  Stein Schjolberg schlägt in seinem Paper[19] vor, den ICTC als Unterabteilung des Internationalen Strafgerichtshofs zu errichten, mit Sitz entweder ebenfalls in Den Haag oder aber in Singapur. Schjolberg vertritt die Auffassung, dass der ICTC durch diese Konstruktion vom Römischen Statut gedeckt wäre, da das Abkommen alle Vorrichtungen zur Ermittlung und Strafverfolgung vorsieht, die der Gerichtshof brauchen würde. Der Staatsanwalt könnte als unabhängiges Organ des Gerichtshofs Untersuchungen auch auf außerordentlicher Grundlage einleiten.

  Alternativ könnte ein Ad-hoc-Gericht in Frage kommen: Ein solches Tribunal müsste ein Gerichtshof der Vereinten Nationen sein, der durch eine Resolution des UN-Sicherheitsrats in Übereinstimmung mit Kapitel 7 der UN Charta eingesetzt wird. Als Vorbild dient Schjolberg das Internationale Strafgerichtstribunal für das frühere Jugoslawien (ICTY).

  Die Bestimmung des neuen Tribunals wäre die Verfolgung und Bestrafung von Internetverbrechen, die Rechtsprechung sollte für folgende Fälle gelten:

[15] EU-US WG Concept Paper 2011, S. 2
[16] EU-US WG Concept Paper 2011, S. 4
[17] EU-US WG Concept Paper 2011, S. 4 u. 5
[18] Das EastWest Institute (EWI) wurde 1980 gegründet, um auf der Basis eines Netzwerks von Einzelpersonen, Institutionen und Nationen die Kommunikation über die Grenze des Eisernen Vorhangs zu ermöglichen. Es versteht sich als „think-and-do-tank", der innovative Lösungen für dringende Sicherheitsprobleme entwickelt und deren Umsetzung anstößt. Dem EWI gehören zahlreiche prominente Persönlichkeiten aus Politik und Wirtschaft an.
[19] Stein Schjolberg: An International Criminal Court or Tribunal for Cyberspace (ICTC), May 2011, auffindbar unter www.cybercrimelaw.net [= Schjolberg 2011]

- Verletzungen von globalen Abkommen zur Cyberkriminalität
- Massive und koordinierte globale Cyberangriffe gegen wichtige Informationsinfrastruktursysteme

Das Tribunal hätte eine gegenüber nationalen Gerichten gleichwertige Rechtsprechung, könnte aber in seinem Ermessen die Vormachtstellung für sich in Anspruch nehmen und Untersuchungen sowie Verfahren zu jedem Zeitpunkt an sich ziehen.

Obwohl die Staatsanwaltschaft dieses Gerichtshofes weitreichende Vollmachten hätte und natürlich auch der Aufgabe entsprechend qualifiziert sein müsste, ist doch klar, dass eine effektive Ermittlungsarbeit nicht vom ICTC allein bewältigt werden könnte. Deshalb schlägt Schjolberg eine enge Kooperation mit INTERPOL vor, die seit den 1980er Jahren als führende Institution für Wissen über die Verfolgung von internationalen Cyberverbrechen gilt. Seit 1990 wurden bei INTERPOL regionale Arbeitsgruppen für Afrika, Asien / Südpazifik, Nord- und Südamerika, Europa sowie den Nahen Osten und Nordafrika eingerichtet, denen die Leiter oder erfahrene Mitglieder nationaler Einheiten zur Bekämpfung von Computerkriminalität angehören.

Gegenwärtig arbeitet INTERPOL an der Errichtung des Interpol Global Complex (IGC) in Singapur, der ab 2013/2014 mit ca. 300 Mitarbeitern seine Arbeit aufnehmen soll. Der ICG wird sich auf Entwicklung innovativer und zeitgemäßer Ermittlungsinstrumente für die weltweite Durchsetzung des Rechts konzentrieren. Insbesondere soll die effektive Bekämpfung von Cyberverbrechen gestärkt werden, damit wäre der IGC eine außerordentlich wichtige Initiative für die internationale Durchsetzung der Gesetze gegen Cyberkriminalität.[20]

Ergänzend schlägt Schjolberg die Einrichtung einer globalen virtuellen Taskforce vor, die aus Experten der weltweiten Informations- und Kommunikationsindustrie, Finanzdienstleistungsbranche, NGOs und der akademischen Welt besteht und partnerschaftlich mit Interpol zusammenarbeitet, um Cyberverbrechen effektiv zu bekämpfen und zu verhindern. Insbesondere soll diese Task Force in der Lage sein, auf Cyberangriffe schnell zu reagieren.[21]

Schjolbergs Vorschlag zur Einrichtung eines Gerichtshofes ist sehr detailliert ausgearbeitet – unter anderem hat er bereits einen Entwurf einer UN-Resolution sowie einen Entwurf für die Statuten des Gerichtshofs vorgelegt. Allerdings ignorieren seine Überlegungen die Arbeit anderer Initiativen – obwohl er sie eingangs kurz erwähnt - praktisch komplett.

6. Exkurs: Problematik der Täterermittlung und Beweisführung bei Cyberverbrechen

Bevor eine grundsätzliche Stellungnahme zu den vorgestellten Initiativen stattfindet, soll ein grundsätzliches Problem der Cyberkriminalität angerissen werden. Cybercrimes sind aufgrund der technologischen Voraussetzungen, unter denen sie begangen werden, enorm schwierig zu verfolgen. Die Techniken des heimlichen Zugriffs ermöglichen es Internetkriminellen, ohne Furcht vor rechtzeitiger Entdeckung zu agieren, von Verhaftung und strafrechtlicher Verfolgung ganz zu schweigen.[22] Es scheint so zu sein, dass die Täter im Cyberspace neue Angriffstechniken in einem so hohen Tempo

[20] Schjolberg 2011, S. 17
[21] Schjolberg 2011, S. 17/18
[22] Deloitte Center for Security and Privacy Solutions: Cyber crime: a clear and present danger. White Paper, 2010, S. 4 [= Deloitte White Paper 2010]

produzieren, dass selbst höchst entwickelte Sicherheitstechnik nicht Schritt halten kann.[23] Unter anderem aus diesem Grund bleibt eine naturgemäß unbekannte, aber sehr hoch geschätzte Zahl von Internetverbrechen ganz und gar unentdeckt.[24] Im Klartext: Je organisierter und entwickelter ein Angriff ist, umso schwieriger ist er aufzudecken und zu bestrafen.

Sandro Gaycken[25], Sicherheitsforscher an der FU Berlin, listet insgesamt vier Faktoren auf, die aus seiner Sicht die Verfolgung und Bestrafung von Cyberverbrechen praktisch unmöglich machen und damit die abschreckende Wirkung von Strafen – und natürlich auch eines internationalen Gerichtshofs – grundsätzlich in Frage stellen:

- *Die Flüchtigkeit der physischen Spuren*: Die relative Winzigkeit des Angriffes (zum Beispiel ein verseuchter USB Stick) bedingt, dass so gut wie keine physischen Spuren der angreifenden Person entstehen. Das gilt natürlich erst recht für Angriffe über das Internet.
- *Der „erzählte" Charakter des feindlichen Programms*: Damit ist gemeint, dass der Angreifercode selbst bewusst (in einer Sprache) konstruiert ist, und diese Konstruktion auch dazu benutzt werden kann, die Ermittler über den Ursprung des Codes in die Irre zu führen.
- *Die Mensch-Maschine-Gap*: Die Lücke zwischen Mensch und Maschine führt dazu, dass selbst dann, wenn man einen Angriff zu einem bestimmten Rechner zurückverfolgen kann, damit nichts darüber ausgesagt ist, wer den Rechner zum fraglichen Zeitpunkt mit welchem Motiv bedient hat.
- *Die Alltäglichkeit der Waffen im Cyberkrieg*: Es werden handelsübliche Technologien wie Rechner, Standard-USB-Sticks oder reguläre Programme eingesetzt, auch Programmierkenntnisse beweisen keine schlechten Absichten. Eine „Tatwaffe" kann also nicht gefunden werden.[26]

Hinzu kommt ein weiterer für die Täterermittlung bedenklicher Faktor: Autoren von Schadprogrammen und andere Cyberkriminelle lassen sich „mieten" und stellen ihre Fähigkeiten, Möglichkeiten und Produkte den eigentlichen Profiteuren des Verbrechens gegen Entgelt zur Verfügung.[27] Diese Art der Komplizenschaft lässt sich mit der eines angeheuerten Auftragskillers vergleichen – trotz der Schwere der Tat fehlt das persönliche Motiv, weshalb es oft sehr lange dauert oder überhaupt nicht gelingt, die „Vollstrecker" zu finden.

Diese sogenannte „non-attributability" von Cybercrimes, die aus den oben genannten Faktoren resultiert, wird in Expertenkreisen derzeit breit diskutiert.[28]

Als Gegenargument ist anzuführen, dass die IT-Forensik natürlich mit Hochdruck an der Lösung der genannten Probleme arbeitet und dabei durchaus Fortschritte verzeichnen kann. Neuere Forschungsarbeiten zu IT-forensischen Designaspekten einer sicheren Rechnerarchitektur widmen sich insbesondere dem Problem der Spurensicherung und damit einer Kernfrage der Täterermittlung und Beweisführung.[29] Es ist aber dennoch nicht von der Hand zu weisen, dass – zumindest bis dato – die Sicherheitsbemühungen und Strafverfolgungsmethoden den Tätern hinterherlaufen.

---

[23] Deloitte White Paper 2010, S. 5
[24] Deloitte White Paper 2010, S. 6
[25] Sandro Gaycken, Krieg der Rechner, in: Internationale Politik, März/April 2011, S. 88-95 [=Gaycken 2011]
[26] Gaycken 2011, S. 91-94
[27] Deloitte White Paper 2010, S. 5
[28] Zum Beispiel plant das Auswärtige Amt, u.a. in Zusammenarbeit mit der FU Berlin und UNIDIR, eine Konferenz zum Thema: Challenges in Cybersecurity,die im Dezember 2011 stattfinden soll. Hier wird in verschiedenen Panels – eines geleitet von Prof. Sylvia M. Kierkegaard – das Problem der non-attributability breit diskutiert.
[29] Vgl. z.B. Klaus Hildebrandt, Stefan Hummel, Igor Podebrand, IT-Forensik. Ausgewählte Aspekte zu Sicheren Rechnerarchitekturen, FAT und NTFS, Berlin 2011. Ohne hier auf Einzelheiten eingehen zu können sei angemerkt, dass diese Arbeit etliche Aspekte aufgreift, die die oben genannte Deloitte-Studie als Ursache unentdeckter Cyberangriffe thematisiert.

7. Evaluierung und Schlussfolgerung

Fast alle nennenswerten Initiativen zur internationalen Rechtsdurchsetzung im Bereich Cybersecurity und Cybercrime wurden in den Jahren 2010 und 2011 ins Leben gerufen.[30] Auch wenn sie unterschiedlich breit angelegt sind und sich in Teilbereichen thematisch ergänzen, sticht vor allem die mangelhafte Koordination ins Auge. Dieser Befund stimmt besonders nachdenklich, wenn man sich bewusst macht, dass der Inhalt der Initiativen ja gerade eine Verbesserung der internationalen Kooperation bis hin zu einheitlichem Handeln zum Zweck hat. Aus heutiger Sicht kann man wohl sehr viel Parallelarbeit und im Nachgang der Tätigkeit der Arbeitsgruppen enormen Abstimmungsbedarf bei der Zusammenführung der Ergebnisse erwarten. Zudem birgt insbesondere die Initiative der UNODC eindeutig die Gefahr der Verzettelung in einer Bestandsaufnahme. Positiv zu bewerten ist jedoch, dass alle Initiativen eine Einbeziehung des privaten Sektors erreichen wollen – die Notwendigkeit einer Zusammenarbeit nicht nur über Ländergrenzen, sondern auch über institutionelle Grenzen hinweg ist unbestritten. Alle Initiativen erkennen an, dass eine rein juristische Herangehensweise an das Problem Cybercrime keine Lösung verspricht.

Auffällig und bedenklich ist, dass bislang keine der genannten Initiativen das Problem der „non-attributability“ anspricht.

Für die überwiegende Mehrheit der Akteure ist die Cybercrime Convention des European Council die beste vorhandene Grundlage für die Schaffung eines internationalen Rechtsrahmens. Ihr haben sich bereits 47 Nationen angeschlossen, darunter auch vier (besonders wichtige) Nicht-EC-Mitglieder, nämlich die Vereinigten Staaten, Kanada, Japan und Südafrika. Auch die sehr weitgehenden Kooperationsanforderungen an die Unterzeichner gelten als aussichtsreiche Basis für die internationale Rechtsdurchsetzung.[31] Unterstützt wird die Konvention unter anderem von der Asia-Pacific Economic Cooperation, der Europäischen Union, INTERPOL und der Organisation Amerikanischer Staaten.[32] Gleichwohl gibt es verständliche Vorbehalte gegen einen Beitritt in etlichen der Staaten, die an der ursprünglichen Ausarbeitung der Konvention nicht beteiligt waren. Diese ließen sich jedoch möglicherweise dadurch ausräumen, dass neuen Unterzeichnern bei der Weiterentwicklung der Konvention entsprechende Mitspracherechte eingeräumt werden.[33]

Die grundsätzlichen Schwierigkeiten bei der Erzielung eines international einheitlichen Standards – nämlich das Gefälle zwischen den westlichen Staaten und den Entwicklungsländern, die grundsätzlich ablehnende Haltung der BRIC-Staaten[34], weitverbreitete Bedenken gegen Eingriffe in die staatliche Souveränität – kämen zweifellos bei einem kompletten Neustart von Verhandlungen erst Recht zum Tragen. Außerdem würden neue jahrelange Verhandlungen die Implementierung der bereits vorhandenen Reformvorhaben vermutlich deutlich verzögern.[35] Deshalb erscheint es aus jetziger Perspektive wenig sinnvoll, neue Verhandlungen ins Leben zu rufen, die wieder bei Null anfangen.

Auch wenn über seine Gestaltung mehr oder weniger gestritten wird – an der Notwendigkeit eines internationalen Rechtsrahmens zweifelt mittlerweile keiner mehr. Ist ein solcher geschaffen, könnte

---

30 Die Aktivitäten der International Telecommunication Union, einer Organisation der Vereinten Nationen, die u. a. 2009 in Zusammenarbeit mit der American Bar Association ein 69 Seiten starkes „Toolkit for Cybercrime Legislation“ veröffentlicht hat, laufen bereits seit einigen Jahren. Vgl. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf

31 Brian Harley, A Global Convention on Cybercrime?, März 2010, S. 3 [= Harley 2010]

32 Harley 2010, S. 4

33 Harley 2010, S. 4

34 Brasilien, Russland, Indien und China

35 Harley 2010, S. 4

auch ein Internationaler Gerichtshof effektiv operieren. Dieser Gerichtshof wäre aber wohl nicht der, für den sich die EWI Arbeitsgruppe um Stein Schjolberg einsetzt:

Vermutlich zur Abkürzung des wie oben beschrieben ohne Zweifel sehr langwierigen Procedere einer internationalen Einigung zur Verfolgung von Cybercrime soll Schjolbergs ICTC per Resolution des UN-Sicherheitsrats an den Internationalen Strafgerichtshof angedockt werden. Damit er vom Römischen Statut gedeckt ist, soll er nur für schwerste Verbrechen (analog zu Kriegsverbrechen und Verbrechen gegen die Menschlichkeit) zuständig sein, zu denen z.B. Kinderpornographiedelikte nicht zählen würden. Cyberverbrechen sind jedoch – auch wenn es natürlich terroristische und kriegsähnliche Attacken gibt, die ebenfalls verfolgt werden müssen – vor allem *Wirtschaftsverbrechen* transnationaler Natur. Mit einer so drastischen Einschränkung der abgedeckten Verbrechen, wie Schjolberg sie vorschlägt, würde ein Cybercrime Court den internationalen Aufgaben, die bewältigt werden müssen, auf keinen Fall gerecht.

Hinzu kommen die Hindernisse, die dem Internationalen Strafgerichtshof im Wege standen und teilweise immer noch stehen.[36] Unter anderem haben besonders wichtige Staaten wie die USA den Internationalen Strafgerichtshof bis heute nicht anerkannt. Mit China und Russland fehlen zwei weitere der fünf ständigen Mitglieder des Sicherheitsrats.[37] Dieses Erbe hätte eine Rechtsprechungsinstitution, die auf dem ICT aufbaut, von vorneherein als Bürde auf sich lasten.

Auf der Grundlage des jetzigen Informationsstands könnte es eine Möglichkeit sein, dass der Council of Europe einen Gerichtshof einrichtet, der grundsätzlich für transnationale Verbrechen mit der notwendigen Schwere zuständig wäre, die in oder aus einem der Unterzeichnerstaaten verübt wurde. Der bisherige Weg der Angleichung nationaler Gesetzgebungen und gegenseitiger Rechtshilfe könnte durch eine solche Institution sinnvoll ergänzt werden. Voraussetzung hierfür wäre eine genügende Zahl von Unterzeichnerstaaten und damit Anpassung der Konvention an die Anforderungen der neuen Mitglieder – wozu ja bereits Initiativen laufen – und eine praktikable und klare Abgrenzung der Verbrechen, die von diesem Gerichtshof verfolgt und bestraft werden.[38] Zudem würden bei dieser Konstruktion die Harmonisierung des internationalen Rechts und die Einrichtung eines internationalen Gerichtshofs nicht nur parallel, sondern sogar Hand in Hand laufen. Die Mitglieder und Neuunterzeichner könnten sich im Prozess der Erweiterung auch über die Ausgestaltung und Befugnisse des Courts einigen.

Ein weiteres Argument für diese Anbindung wäre die explizite Unterstützung der Cybercrime Convention durch INTERPOL. Wie Stein Schjolberg richtig argumentiert, ist diese Institution derzeit am besten dafür gerüstet, die Ermittlungen und Strafverfolgung durch einen Internationalen Cybercrime Court zu unterstützen.

Bei der Erweiterung des Kreises der Unterzeichnerstaaten und der gleichzeitigen Etablierung des Gerichtshofs wären vor allem zwei Problemkreise im Auge zu behalten: Zum einen die unterschiedlichen Rechtsauffassungen vor allem im Bereich Intellectual Property, den der European Council explizit in die Konvention aufgenommen hat, und die verschiedene Länder vor einem Beitritt zurückschrecken lässt. Zum anderen das Maß, in dem die Nationen Souveränität in der Rechtsprechung abgeben müssten – ein wesentlicher Grund, warum beispielsweise die USA den Internationalen Strafgerichtshof in Den Haag bis dato nicht anerkannt haben. Beide Aspekte stellen mit Sicherheit erhebliche Hürden dar, deren Überwindung einige Zeit in Anspruch nehmen dürfte.

---

[36] Vgl. hierzu ausführlich den sehr lesenswerten Vortrag von Gregor Schirmer, Vom Internationalen Militärtribunal zum Haager Internationalen Gerichtshof – Fortschritt und Ernüchterung, gehalten am 12.10.2010 [= Schirmer 2010]

[37] Schirmer 2010, S. 12

[38] Jedenfalls sollten alle wesentlichen Verbrechen gegen die Gesellschaft insgesamt (vgl. Auflistung unter 1.) mit erfasst werden.

8. Einrichtung einer WCLF Arbeitsgruppe für einen International Court for Cybercrime

Es lassen sich verschiedene Anknüpfungspunkte für eine Mitarbeit des WCLF und, nach entsprechender Vertiefung, der Global Law Society erkennen. Als erste Maßnahme erscheint die Einrichtung einer Arbeitsgruppe zur weiteren Prüfung und Erarbeitung konkreter Vorschläge für einen an den Council of Europe angeschlossenen *International Court for Cybercrime* vielversprechend. Diese Arbeitsgruppe könnte sich unter anderem den folgenden Aufgaben widmen:

- Genauere Prüfung der Voraussetzungen, die für einen solchen auf der Cybercrime Convention fußenden Gerichtshof erfüllt sein müssen.
- Vorschläge für die Entwicklung eines Collective Codex (von vielen Ländern getragene Weiterentwicklung der Cybercrime Convention).
- Eingrenzung der Cyberverbrechen, die unter die Rechtssprechung des Gerichtshofs fallen sollen.
- Prüfung, welche Art der Rechtsprechung (subsidiär oder der nationalen Rechtsprechung übergeordnet) dem Gerichtshof zustehen soll.
- Konkrete Überlegungen zur Ausgestaltung des Courts (institutionell, personell, finanziell)
- Einbringen der Idee in die verschiedenen laufenden Initiativen
- Erarbeitung von Lobbyingvorschlägen
- Gewinnung weiterer Unterstützer

Dem Arbeitskreis könnten unter anderem die folgenden Mitglieder angehören:

Aus dem Kreis des WCLF:

Prof. Dr. Sylvia M. Kierkegaard, LL.M, LL.B, Southampton, Chair

Externe Experten (in alphabetischer Reihenfolge):

Prof. Dr. Susan W. Brenner, Dayton

Dr. Sandro Gaycken, Berlin

Prof. Dr. Dr. Eric Hilgendorf, Würzburg

Dr. Françoise Le Bail MSc, Generaldirektorin EU–Komm., Brüssel

Prof. Dr. Alexander Lorz LL.M, Düsseldorf