Delikte in der digitalen Sphäre

Die Vereinten Nationen im Kampf gegen Cyberkriminalität

Tatiana Tropina · Nicolas von zur Mühlen

Tatiana Tropina, geb. 1979, ist Wissenschaftliche Referentin am Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg.

Nicolas von zur Mühlen, geb. 1982, ist Leiter des Referats ›Informationsrecht und Rechtsinformatik‹ am Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg.

Die Bekämpfung der Cyberkriminalität ist aufgrund des globalen Charakters dieses Deliktsbereichs durch die Aktivitäten einer Vielzahl internationaler Akteure geprägt. Diese lassen sich nicht einem Bereich der Strafverfolgung zuordnen, sondern betreffen auch andere Rechtsregime sowie diverse außerrechtliche Maßnahmen. Der Beitrag beleuchtet die Rolle der Vereinten Nationen im Rahmen dieses komplexen Gesamtsystems.

Das rasante Wachstum der digitalen Wirtschaft, die elektronische Vernetzung der Infrastruktur und die digitale Durchdringung des Alltags haben in den letzten Jahrzehnten dazu geführt, dass die Informationsgesellschaft maßgeblich vom ordnungsgemäßen Funktionieren von Computersystemen und der Sicherheit der hierauf gespeicherten Daten abhängig ist. Um in der von unkörperlichen Werten dominierten modernen Welt einen Schaden großen Ausmaßes anzurichten, bedarf es in der Regel nicht einmal mehr eines physischen Zugangs zu Systemen oder Speichermedien: Durch Ausnutzung von Sicherheitslücken und den Einsatz von Schadsoftware können Daten aus der Ferne zerstört, verändert oder hinzugefügt werden. Straftaten, die über Kommunikationsnetze begangen werden, stellen daher eine anhaltende Bedrohung nicht nur für Einzelpersonen und Unternehmen dar, sondern für die Wirtschaft und die Gesellschaft im Ganzen. Dies gilt nicht nur in den Fällen, in denen Informationssysteme das eigentliche Ziel eines Angriffs sind, sondern auch dann, wenn diese lediglich ein Werkzeug zur Begehung von Straftaten darstellen. Diese Bedrohung wird in den nächsten Jahren – nicht zuletzt durch das sich bereits abzeichnende ›Internet der Dinge‹ – mit zunehmender Vernetzung und steigender Abhängigkeit von moderner Informationstechnologie weiter ansteigen.

Eine effektive Prävention, Bekämpfung und Verfolgung von Cyberkriminalität bedarf einer Vielzahl unterschiedlicher Maßnahmen, die nicht nur technische, organisatorische und personelle Vorkehrungen umfassen, sondern auch die Sensibilisierung durch Aufklärung, die Weiterentwicklung des Straf-, Zivil- und Verwaltungsrechts, die Schaffung von Rahmenbedingungen für öffentlich-private Partnerschaften, Maßnahmen der regulierten Selbstregulierung und die Erzeugung von Anreizen zur Selbstregulierung der Wirtschaft. Diese Ansätze müssen kombiniert angewandt werden, um eine effektive Antwort auf die Herausforderungen der Cyberkriminalität zu finden. Darüber hinaus ist aufgrund des globalen Charakters dieser Problematik eine Harmonisierung des rechtlichen Rahmens von zentraler Bedeutung, sowohl um sichere Häfen für Straftäter zu beseitigen als auch um grenzüberschreitende Ermittlungen und die Kooperation zwischen Strafverfolgungsbehörden unterschiedlicher Staaten zu ermöglichen.[1] Aus diesem Grund gehört im Bereich der Bekämpfung der Cyberkriminalität die Erarbeitung internationaler Standards mit dem Ziel der Harmonisierung rechtlicher Rahmenbedingungen zu den zentralen Anliegen, mit denen sich internationale Organisationen wie die Vereinten Nationen in den letzten Jahren beschäftigt haben.

Was ist Cyberkriminalität?

Bevor auf den relevanten internationalen Rahmen und die Aktivitäten der Vereinten Nationen eingegangen wird, soll zunächst die Bedeutung des Begriffs der Cyberkriminalität näher umrissen werden.[2] Trotz des Umstands, dass seit über zwei Jahrzenten auf internationaler Ebene intensiv über die Problematik der Cyberkriminalität diskutiert wird, gibt es in den relevanten internationalen Instrumenten trotz der vielfachen Benutzung dieses Begriffs – wie insbesondere im Rahmen des Übereinkommens über Computerkriminalität des Europarats von 2001 – keine feste Definition. Die Bedeutung hängt letztlich vom jeweiligen Kontext ab: Soweit es um die spezifischen Straftatbestände geht, die dem Deliktsbereich der Cyberkriminalität im materiellen Recht zugerechnet werden, beziehen sich die meisten der internationalen und regionalen Instrumente auf die Straftaten gegen die Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Computerdaten und -systemen, computerbezogene Straftaten wie die computerbezogene Fälschung und den computerbezogenen Betrug, inhaltsbezogene Straftaten und Straftaten mit Bezug zu Kinderpornografie und Kindesmissbrauch.[3] Während die internationalen Instrumente im Bereich des materiellen Strafrechts dadurch einen größtenteils übereinstimmenden und spezifischen Deliktskatalog regeln, ist der Anwendungsbereich verfahrensrechtlicher Bestimmungen sehr viel weitgehender. Denn anders als bei Vorgaben zum materiellen Recht, wo in der Regel abschließend spezifische strafbare Handlungen benannt werden, kann durch eine breite Herangehensweise im Bereich des Verfahrensrechts sichergestellt werden, dass die Vorgaben zu Eingriffsbefugnissen bei Ermittlungen im Bereich

aller Straftaten Anwendung finden können, in denen digitale Beweismittel eine Rolle spielen. Dies ist nicht nur bei den zuvor genannten spezifischen Delikten der Cyberkriminalität der Fall, sondern aufgrund der fortschreitenden Durchdringung des Alltags mit Informations- und Kommunikationstechnologie bei nahezu allen Straftaten.

Schwierigkeiten bereitet zudem auch immer öfter die Abgrenzung der Aktivitäten internationaler Organisationen im Bereich der Strafverfolgung zu anderen Bereichen des Sicherheitsrechts, wie dem Polizeirecht, dem Kriegsrecht und dem Geheimdienstrecht.[4] Waren diese Rechtsregime früher noch klar voneinander abgrenzbar, ist in den letzten Jahren, insbesondere im Bereich der Cyberkriminalität und der Terrorismusbekämpfung, ein Verschwimmen der Grenzen dieser Disziplinen hin zu einem allgemeinen präventiven Sicherheitsrecht zu beobachten, das sich auch auf der Ebene internationaler Abkommen widerspiegelt.[5]

Internationale Ansätze zur Bekämpfung der Cyberkriminalität

Die internationalen Ansätze zur Bekämpfung der Cyberkriminalität stellen ein komplexes Gesamtsystem dar, in dem internationale und regionale Akteure agieren und das aus verbindlichen Abkommen und nicht bindenden Modellgesetzen sowie Best-Practice-Konzepten besteht.

Der Ruf nach einer Harmonisierung der strafrechtlichen Bestimmungen zur Computerkriminalität und einer Förderung der Zusammenarbeit der Strafverfolgungsbehörden in diesem Sektor wurde erstmals im Jahr 1986 laut, als im Rahmen des Berichts einer Expertengruppe der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (Organisation for Economic Co-operation and Development – OECD) erste Maßnahmen unternommen wurden, die einzelnen Elemente computerspezifischer Straftaten zu systematisieren.[6] Weitere Entwicklungen in den letzten zwei Jahrzehnten führten zur Schaffung sowohl verbindlicher als auch nicht bindender internationaler Instrumente durch den Europarat, die Europäische Union (EU), die Gemeinschaft unabhängiger Staaten, die Afrikanische Union und die Arabische Liga. Diese Instrumente beeinflussten sich in ihrer Entstehung weitgehend untereinander, wobei die maßgebliche Rolle das Übereinkommen über Computerkriminalität des Europarats spielt. Dennoch weisen alle im Bereich der Cyberkriminalität relevanten 19 multilateralen Instrumente – abgesehen von einigen mehr oder weniger gemeinsamen Kernbestimmungen – teils signifikante Unterschiede auf.[7]

Zusätzlich zur Entwicklung rechtlicher Standards im Bereich des Strafrechts befasst sich eine Reihe anderer internationaler Organisationen und Behörden auf unterschiedlichen Ebenen mit dem Problem der Cyberkriminalität. Die Gruppe der Sieben (G7), die Organisation amerikanischer Staaten (Organization of American States – OAS), die Asiatisch-Pazifische Wirtschaftsgemeinschaft (Asia-Pacific Economic Cooperation – APEC), die OECD, der Verband Südostasiatischer Nationen (Association of Southeast Asian Nations – ASEAN), Interpol und Europol sowie eine Reihe weiterer Organisationen beschäftigen sich diesbezüglich mit einer Vielzahl rechtlicher und außerrechtlicher Vorhaben, wie etwa der Harmonisierung des gesetzlichen Rahmens, der Verbesserung personeller und institutioneller Strukturen, der Ausbildung und der allgemeinen Sensibilisierung.

Die internationalen Ansätze zur Bekämpfung der Cyberkriminalität stellen ein komplexes Gesamtsystem aus Akteuren, Abkommen, Modellgesetzen sowie Best-Practice-Konzepten dar.

In diesem komplexen und vielschichtigen Umfeld kommt nicht den Vereinten Nationen die wegweisende Rolle bei der Schaffung internationaler Standards zu, sondern dem Europarat. Seit der Verabschiedung des Übereinkommens über Computerkriminalität im Jahr 2001 ist dieses Instrument zum führenden Maßstab für die rechtlichen Entwicklungen auf der internationalen Ebene geworden: Alle nachfolgenden internationalen Ansätze wurden durch dieses Übereinkommen mehr oder weniger beeinflusst und haben sich teilweise explizit auf dieses berufen, zudem sind ihm auch mehrere außerhalb Europas gelegene Staaten beigetreten. Damit ist es das einzige verbindliche Abkommen im Bereich der Computerkriminalität, das eine überregionale Bedeutung besitzt.

Das Übereinkommen über Computerkriminalität ist das einzige verbindliche Abkommen von überregionaler Bedeutung.

1 Vgl. dazu Ulrich Sieber, Mastering Complexity in the Global Cyberspace: The Harmonization of Computer-Related Criminal Law, in: Mireille Delmas-Marty/Mark Pieth/Ulrich Sieber (Hrsg): Les chemins de l'har-monisation pénale – Harmonising Criminal Law, Paris 2008, S. 127ff.

2 Im deutschsprachigen Sprachraum werden für den hier relevanten Deliktsbereich oft die Begriffe des Computer-, des Internet- und des Informationsstrafrechts synonym gebraucht.

3 Für eine phänomenologische Darstellung dieser Deliktsbereiche siehe Ulrich Sieber, Straftaten und Strafverfolgung im Internet, Gutachten Teil C, in: Verhandlungen des 69. Deutschen Juristentages, München 2012, S. 18ff.

4 Siehe dazu Tatiana Tropina/Cormac Callanan, Self- and Co-regulation in Cybercrime, Cybersecurity and National Security, Berlin 2015, S. 4f.

5 Dies zeigt sich etwa an der Einführung von Straftatbeständen, die bereits im Vorfeld der strafrechtlichen Tatbegehung ansetzen, wie beispielsweise Art. 6 des Übereinkommens zur Cyberkriminalität, der die Verbreitung bestimmter Software unter Strafe stellt.

6 OECD, Computer-Related Criminality: Analysis of Legal Policy in the OECD Area, Report DSTI-ICCP 84.22, 18.4.1986.

7 Für eine detaillierte Liste und Analyse der 19 Instrumente siehe UNODC, Comprehensive Study on Cybercrime, S. 63ff., www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

Die Aktivitäten der Vereinten Nationen

Cyberkriminalität war in der Vergangenheit mehrfach Gegenstand diverser Resolutionen der Generalversammlung und des Wirtschafts- und Sozialrats der Vereinten Nationen (Economic and Social Council – ECOSOC). Eine der ersten Resolutionen der Generalversammlung zu dieser Problematik wurde im Dezember 2000 verabschiedet.[8] Sie rief die Mitgliedstaaten dazu auf, auf nationaler Ebene stärkere Bemühungen zur Vermeidung sicherer Häfen für Straftäter zu unternehmen und die Koordinierung auf internationaler Ebene zu verbessern. Darüber hinaus wurde im selben Jahr mit der Resolution 55/59 der UN-Generalversammlung die Kommission für Verbrechensverhütung und Strafrechtspflege (Commission on Crime Prevention and Criminal Justice – CCPCJ) damit mandatiert, Antworten auf das Problem der Cyberkriminalität zu finden.[9] Weitere Ansätze, die sich mit dem Missbrauch von Informationstechnologie im Kontext der Organisierten Kriminalität beschäftigen, befinden sich in den Resolutionen 56/121 und 63/195 der UN-Generalversammlung.[10] Trotz dieser Vorstöße bezeichnete der ECOSOC in seiner Resolution 2009/22 das Übereinkommen über Computerkriminalität des Europarats als das einzige internationale Instrument, dass die Delikte des computerspezifischen Betrugs, der computerbezogenen Fälschung und andere Formen der Cyberkriminalität spezifisch aufgreift.[11] Auf die Nutzung des Internets speziell als Mittel zur Planung und Finanzierung terroristischer Aktivitäten und zur Werbung für terroristische Vereinigungen wurde zudem in mehreren Resolutionen des UN-Sicherheitsrats hingewiesen.[12]

Zwei weitere UN-Institutionen beschäftigen sich mit der Cyberkriminalität: die ITU und das UNODC.

Im Schwerpunkt beschäftigen sich mit der Problematik der Cyberkriminalität jedoch zwei weitere Institutionen der Vereinten Nationen: Die Internationale Fernmeldeunion (International Telecommunication Union – ITU) und das Büro der Vereinten Nationen für Drogen- und Verbrechensbekämpfung (United Nations Office on Drugs and Crime – UNODC).

Durch die im Jahr 2001 verabschiedete Resolution 56/183 der UN-Generalversammlung wurde die ITU damit beauftragt, einen Weltgipfel zur Informationsgesellschaft (World Summit on the Information Society – WSIS) abzuhalten.[13] Im Rahmen dieses Gipfels wurde im Jahr 2003 ein Aktionsplan verabschiedet, der auch Maßnahmen zur Gewährleistung von Vertrauen und Sicherheit bei der Nutzung von Informations- und Kommunikationstechnologie zum Gegenstand hatte und insbesondere Regierungen sowie den privaten Sektor dazu aufrief, Cyberkriminalität und sonstigen Missbrauch von Kommunikationstechnologie zu verhindern und zu verfolgen.[14] Die ITU wurde bei der Fortsetzung des Weltgipfels im Jahr 2006 damit beauftragt, eine Vermittlerrolle bei der Umsetzung dieser Maßnahmen des Aktionsplans einzunehmen. Im Rahmen dieser Aufgabe rief die ITU im Jahr 2007 die ›Agenda für weltweite Cybersicherheit‹ (Global Cybersecurity Agenda) ins Leben, die verschiedene Ebenen, wie beispielsweise rechtliche Maßnahmen und internationale Kooperation, zum Gegenstand hat.[15] Hervorzuheben sind zudem zwei weitere Aktivitäten der ITU, die während des WSIS-Forum im Jahr 2009 präsentiert wurden: Die Publikation ›Cybercrime Guide for Developing Countries‹ und ein Modellgesetz für eine Gesetzgebung zu Cyberkriminalität.[16] Letzteres wurde dahingehend kritisiert, dass die ITU damit als Organisation, die sich eigentlich originär mit technischen Aspekten der Telekommunikation beschäftigt, die rechtspolitisch geprägte Domäne der Entwicklung von Modellgesetzen betreten habe.[17] Das Modellgesetz selbst wurde von der amerikanischen Rechtsanwaltskammer (American Bar Association – ABA) entwickelt und enthielt einige Bestimmungen, die sowohl teils von bestehenden internationalen Standards abwichen als auch mehrere kontroverse Fragen nicht einbezogen. Ob das Modellgesetz für Entwicklungsländer tatsächlich von Nutzen ist, wurde daher angezweifelt.[18] Dennoch war die ITU in der Folge an der Erarbeitung rechtlicher Rahmenentwürfe beteiligt: Ab dem Jahr 2008 führte die ITU zusammen mit der EU einige Projekte zur Entwicklung von Modellgesetzen auch im Bereich der Cyberkriminalität durch, unter anderem für afrikanische, karibische und pazifische Staaten.[19]

Gleichzeitig übte das UNODC sein Mandat im Bereich der Verbrechensprävention und der Strafjustiz aus. In ihrer Resolution 65/230 beauftragte die Generalversammlung die CCPCJ damit, eine Offene zwischenstaatliche Arbeitsgruppe von Experten einzusetzen, um eine umfassende Studie über das Problem der Cyberkriminalität und die Umgangsweise der Mitgliedstaaten, der internationalen Gemeinschaft und des privaten Sektors damit zu erarbeiten.[20] Diese sollte Informationen über die einschlägigen nationalen Gesetze, Best-Practice-Konzepte, technische Lösungen und die internationale Zusammenarbeit erheben, um damit die Optionen zur Stärkung bestehender Regelungen und Vorschläge zur Erarbeitung neuer rechtlicher Antworten für den Umgang mit dem Problem der Cyberkriminalität zu finden. Im Mai 2011 unterzeichneten das UNODC und die ITU eine Absichtserklärung, die Mitgliedstaaten zukünftig in vier Schwerpunkten gemeinsam zu unterstützen: der Beurteilung bestehender Institutionen und Abläufe, der Entwicklung neuer und Überprüfung bestehender Gesetze, bei technischen Fragen und im Bereich des Erfahrungsaufbaus.[21] Darüber hinaus unterstützte das UNODC die in Resolution 60/288 verabschiedete globale Strategie der Vereinten Nationen zur Terrorismusbekämpfung, in der die Mitgliedstaaten beschlossen haben, die Erscheinungs-

formen des Terrorismus im Internet auf internationaler und nationaler Ebene zu bekämpfen und das Internet als Werkzeug zu benutzen, um die Ausbreitung des Terrorismus zu verhindern.[22] Eine Studie des UNODC hierzu wurde im Jahr 2012 veröffentlicht.[23]

Die Studie zu Cyberkriminalität des UNODC

Den umfassendsten Vorstoß der Vereinten Nationen im Bereich der Cyberkriminalität stellt die auf Grundlage der Resolution 65/230 erstellte Studie zu Cyberkriminalität des UNODC dar. Methodisch wurde diese Studie insbesondere auf der Grundlage ausführlicher Fragebögen erstellt, die an die Mitgliedstaaten, zwischenstaatliche Organisationen, ausgewählte Repräsentanten der Privatwirtschaft und Forschungseinrichtungen versandt wurden. Das Ziel der Studie lag darin, Möglichkeiten zu untersuchen, um existierende Ansätze zur Bekämpfung der Cyberkriminalität zu stärken und neue nationale sowie internationale rechtliche oder alternative Lösungsoptionen im Rahmen des Mandats des UNODC vorzuschlagen. Die Arbeit an der Studie, in deren Rahmen hauptsächlich Gesetze, Statistiken und die Antworten auf die Fragebögen ausgewertet wurden, wurde in den Jahren 2011 bis 2013 durchgeführt, die Veröffentlichung der Studie erfolgte im Februar 2013.[24]

Die Studie stellt bis heute wahrscheinlich die umfassendste Momentaufnahme des globalen Umgangs mit der Computerkriminalität und der diesbezüglichen Gesetzgebung dar. Sie kam zu dem Ergebnis, dass nach wie vor eine Fragmentierung und eine daraus folgende unzureichende Harmonisierung der Gesetzgebung auf nationaler Ebene und der verschiedenen Instrumente auf internationaler Ebene vorliegt, sowohl im materiellen Recht als auch im Prozessrecht.[25] Auch wurden die derzeit bestehenden Mechanismen der internationalen Kooperation für unzureichend erachtet, um in der gebotenen Zeit dem flüchtigen Charakter elektronischer Beweismittel gerecht zu werden. Darüber hinaus wurde im Bereich der präventiven Maßnahmen ein Bedarf an zusätzlichem Erfahrungsaufbau, Aufklärungskampagnen sowie öffentlich-privaten Partnerschaften diagnostiziert und die Integration der Strategien zur Bekämpfung der Cyberkriminalität in den breiteren Kontext der Cybersicherheit vorgeschlagen. Zur Lösung dieser Problembefunde schlug der Bericht die Entwicklung von Modellgesetzen vor. So sollten im Bereich des materiellen Rechts Vorschläge für eine Harmonisierung der Kernstraftatbestände der Cyberkriminalität (Straftaten gegen die Integrität, Vertraulichkeit und Zugänglichkeit von Computersystemen und Daten) sowie klassischer computerbezogener Delikte erfolgen. Für den Bereich des Prozessrechts wurden insbesondere Ermächtigungen zur umgehenden Sicherung von Daten und zur Erlangung von gespeicherten Daten und Echtzeitdaten vorgeschlagen, ebenso wie Richtlinien für den Umgang mit der Problematik grenzüberschreitender Ermittlungen. Empfohlen wurde zudem die Entwicklung neuer Abkommen auf internationaler Ebene, die neben der Kooperation bezüglich der Erlangung digitaler Beweismittel auch das materielle Strafrecht, das Prozessrecht und Fragen der Zuständigkeit im Rahmen grenzüberschreitender Ermittlungen zum Gegenstand haben sollen. An außerrechtlichen Maßnahmen wurden insbesondere die Unterstützung von Entwicklungsländern sowie die Stärkung der Kooperation von Staaten mit dem privaten Sektor und Forschungseinrichtungen angeregt.

Die Ergebnisse der Studie und die Empfehlungen wurden beim zweiten Treffen der Expertengruppe vom 25. bis 28. Februar 2013 in Wien diskutiert. Dabei haben zwar einzelne Mitgliedstaaten, die das Übereinkommen über Computerkriminalität nicht unterzeichnet oder nicht umgesetzt haben, eine von den Vereinten Nationen angeführte alternative Lö-

Den umfassendsten Vorstoß der Vereinten Nationen im Bereich der Cyberkriminalität stellt die Studie des UNODC aus dem Jahr 2013 dar.

8 UN-Dok. A/RES/55/63 v. 4.12.2000.

9 UN-Dok. A/RES/55/59 v. 4.12.2000.

10 UN-Dok. A/RES/56/121 v. 19.12.2001, UN-Dok. A/RES/63/195 v. 18.12.2008.

11 UN Doc. E/2009/22 v. 30.7.2009.

12 UN-Dok. S/RES/1735 v. 22.12.2006, UN-Dok. S/RES/2129 v. 17.12.2013, UN-Dok. S/RES/2199 v. 12.2.2015, UN-Dok. S/RES/2253 v. 17.12.2015.

13 Zum Überprüfungsprozess WSIS+10 siehe den Beitrag von Wolfgang Kleinwächter, in diesem Heft, S. 67–72.

14 WSIS-03/GENEVA/DOC/5-E v. 12.12.2003.

15 Siehe dazu Report of the Chairman of the High-Level Expert Group on the Measurement of Economic Performance and Social Progress (HLEG), www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf

16 ITU, Understanding Cybercrime: A Guide for Developing Countries, Genf 2009.

17 Marco Gercke/Tatiana Tropina, From Telecommunication Standardisation to Cybercrime Harmonisation? ITU Toolkit for Cybercrime Legislation, Computer Law Review International, 5/2009, S. 136–140.

18 Ebd.

19 Vgl. die Übersicht zu den Projekten unter www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/Pages/default.aspx

20 UN-Dok. A/RES/65/230 v. 21.12.2010.

21 Vgl. zu den einzelnen Bereichen www.itu.int/en/ITU-D/Cybersecurity/Pages/UNODC.aspx

22 UN-Dok. A/RES/60/288 v. 20.9.2006.

23 UNODC, Use of Internet for Terrorist Purposes, www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

24 UNODC, Comprehensive Study in Cybercrime, a.a.O. (Anm. 7).

25 Eine Zusammenfassung der Ergebnisse und der Vorschläge ist abrufbar unter www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_E.pdf

sung unterstützt.[26] Es kam jedoch zu keiner Einigung hinsichtlich der Entwicklung neuer Abkommen auf internationaler Ebene. Grund dafür war im Wesentlichen die Besorgnis, dass durch auf einen breiteren internationalen Konsens angelegte Vorstöße die hohen Standards abgesenkt werden könnten, die durch den Europarat mit dem Übereinkommen über Computerkriminalität geschaffen wurden.[27] Eine breite Einigung wurde jedoch dahingehend erzielt, die Rolle des UNODC im Bereich des Erfahrungsaufbaus und der technischen Unterstützung zu stärken und die Studie zur weiteren Berücksichtigung an die CCPCJ weiterzuleiten. Das UNODC nahm die Ergebnisse des zweiten Treffens der Expertengruppe zum Anlass, um in Resolution 22/8 eine entsprechende Empfehlung abzugeben.

Im Ergebnis ist dem UNODC mit der Studie zu Cyberkriminalität somit zwar gelungen, ein umfassendes Bild des globalen Umgangs mit diesem Deliktsbereich zu zeichnen. Dennoch sind die wesentlichen politischen Ziele des UNODC, die Studie und ihre Ergebnisse als einen Rahmen für weitere Verhandlungen über die Schaffung neuer Abkommen in diesem Bereich zu nutzen, erfolglos geblieben.

Die Strategie der Vereinten Nationen, sich im Erfahrungsaufbau und in der technischen Unterstützung einzusetzen, erscheinen momentan als passender Ansatz.

Die Bemühungen zur Harmonisierung der Gesetzgebung zu Cyberkriminalität werden daher weiterhin hauptsächlich im Rahmen verschiedener Vorstöße auf der Ebene regionaler Organisationen unternommen. So hat etwa die Afrikanische Union im Jahr 2014 ein Abkommen im Bereich der Cybersicherheit verabschiedet. Hauptakteur bleibt jedoch weiterhin der Europarat, der seine Position durch die Arbeit an Programmen im Erfahrungsaufbau stärkt und Leitfäden entwickelt, um die Anwendung der bestehenden Regelungen des Übereinkommens über Computerkriminalität zu erläutern.[28] Es verbleibt jedoch ein weiterer Bedarf an Harmonisierung: Während das relevante materielle Strafrecht, abgesehen von einzelnen noch bestehenden Fragmentierungen, in vielen Bereichen inzwischen harmonisiert ist, besteht noch größerer Harmonisierungsbedarf im Bereich des Strafprozessrechts, insbesondere hinsichtlich der Erlangung und des transnationalen Austauschs digitaler Beweismittel.

Auch das UNODC und die ITU setzen derzeit ihre Arbeit im Bereich des Erfahrungsaufbaus weiter fort. Der Umgang mit dem Problem der Cyberkriminalität ist weiterhin ein wichtiger Teil auf der Agenda des UNODC und war zuletzt Schwerpunkt des 13. Kongresses der Vereinten Nationen für Verbrechensverhütung und Strafrechtspflege in Doha im Jahr 2015. Im selben Jahr wurde zudem eine Studie über die Auswirkungen neuer Informationstechnologien in Bezug auf den Missbrauch und die Ausbeutung von Kindern veröffentlicht.[29] Darüber hinaus wurde im Mai 2015 auf der Internetseite des UNODC eine Datenbank zur Verfügung gestellt, die Gesetzgebung, Entscheidungen und sonstige Informationen der Mitgliedstaaten zum Bereich der Cyberkriminalität enthält.[30]

Ausblick

Insbesondere das UNODC und die ITU setzen derzeit ihren Beitrag im Rahmen der globalen Bemühungen zur Bekämpfung der Cyberkriminalität weiter fort. Dennoch ist es unwahrscheinlich, dass die UN in der näheren Zeit eine Führungsrolle in diesem Sektor erreichen wird. Jeder Vorstoß in Richtung eines neuen internationalen Abkommens würde auf der internationalen Ebene nur schwer einen Konsens erlangen können. Die Strategie der Vereinten Nationen, sich über die ITU und das UNODC im Erfahrungsaufbau und in der technischen Unterstützung einzusetzen, erscheinen daher momentan als passender Ansatz. Da die im Bereich der Cyberkriminalität relevanten Standards jedoch von anderen Organisation – wie insbesondere dem Europarat – entwickelt wurden und weiterhin umgesetzt werden, ist es für die Vereinten Nationen ratsam, mit diesen Organisationen zu kooperieren, um eine bessere Abstimmung und damit einen größeren Erfolg der Initiativen zu erreichen.

26 Vgl. etwa die russische Position während des Treffens der Expertengruppe zu Cyberkriminalität in Wien vom 17. bis 21. Januar 2011, www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/Presentations/Russia_1_Cybercrime_EGMJan2011.pdf

27 Im abschließenden Bericht wurde lediglich festgehalten, dass »verschiedene Ansichten bezüglich des Inhalts, der Erkenntnisse und der in der Studie dargestellten Optionen zum Ausdruck gebracht wurden.«, siehe UNODC, Report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in Vienna from 25 to 28 February 2013, www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_3_E.pdf

28 Siehe hierzu die Übersicht unter www.coe.int/en/web/cybercrime/guidance-notes

29 UNODC, Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children, www.unodc.org/documents/organized-crime/cybercrime/Study_on_the_Effects.pdf

30 Die Datenbank ist verfügbar unter www.unodc.org/cld/index-cybrepo.jspx