Kongressbericht: Cyberkriminalität als internationale Herausforderung

Thirteenth United Nations Congress on Crime Prevention and Criminal Justice vom 12.04.-19.04.2015 in Doha, Katar

Von Wiss. Mitarbeiter **Adrian Haase**, Berlin*

Im April 2015 trafen sich in Doha Vertreter internationaler Organisationen, Delegationen der Mitgliedstaaten der Vereinten Nationen, Vertreter von beratenden Nichtregierungsorganisationen sowie Experten aus Wissenschaft und Praxis auf Einladung des United Nations Office on Drugs and Crime (UNODC) und des Gastgeberstaates Katar. Die fünfjährlich stattfindenden Kongresse zum Thema Kriminalität der Vereinten Nationen beschäftigen sich seit 1955 insbesondere mit der Bekämpfung und Verhinderung transnationaler Kriminalitätserscheinungen, dem Schutz der Menschenrechte bei der Kriminalitätsbekämpfung und im Strafvollzug sowie der weltweiten Implementierung und Förderung von Grundsätzen der Rechtsstaatlichkeit. Im Rahmen ihrer jeweiligen offiziellen Eröffnungsansprachen adressierten der Generalsekretär der Vereinten Nationen Ban Ki-Moon, der Generaldirektor der Vereinten Nationen in Wien und Exekutivdirektor von UNODC Yuri Fedotov sowie der Emir von Katar Scheich Tamim bin Hamad Al Thani drängende Fragen des Internationalen Strafrechts und der Kriminalitätsbekämpfung. Waren in früheren UN-Kriminalitätskongressen noch mehrheitlich Themen der globalen Standards thematisiert worden, wurde bereits bei den Eröffnungsreden des Doha-Kongresses deutlich, dass Fragen der internationalen Zusammenarbeit bei der Bekämpfung von transnationalen Kriminalitätserscheinungen abermals an Bedeutung gewonnen haben.

I. Doha-Kongress und Cyberkriminalität

Als Leitmotiv des 13. Kongresses diente die „Integration von Kriminalitätsbekämpfung und Strafrechtspflege in die zukünftige Agenda der Vereinten Nationen um sozialen und ökonomischen Herausforderungen bestmöglich begegnen zu können, die Förderung der Rechtsstaatlichkeit auf nationaler und internationaler Ebene sowie die öffentliche Teilhabe am Prozess der Kriminalitätsbekämpfung“.[1] Das Leitmotiv wurde in vier Teilbereiche (Implementierung und Förderung von Rechtsstaatlichkeit, Menschenhandel, Bekämpfung moderner Kriminalitätserscheinungen und zivilgesellschaftliche Teilhabe bei der Kriminalitätsverhütung) gegliedert und sowohl auf Regierungsebene (High-Level-Segments) als auch auf Fachebene (Expert-Level-Segments) bearbeitet.[2]

In ihren jeweiligen Eröffnungsstatements identifizierten sowohl die Vertreter der UN-Mitgliedstaaten als auch der Internationalen Organisationen Cyberkriminalität als moderne Kriminalitätsform par excellence und knüpften damit an die Vorarbeiten der vorangegangenen Kongresse in Bangkok (Thailand)[3] im Jahre 2005 und Salvador de Bahia (Brasilien)[4] im Jahre 2010 an. Dabei wiesen sie auf die Relevanz der Anstrengungen gegen Cyberkriminalität im internationalen Verbund hin, da sowohl Täter als auch Opfer in allen Ländern der Erde zu finden seien. Im Rahmen des Salvador-Kongresses wurde eine Studie zum globalen Phänomen der Cyberkriminalität in Auftrag gegeben, die zwischenzeitlich als „Comprehensive Study on Cybercrime“[5] erschienen ist und derzeitig in die Amtssprachen der Vereinten Nationen übersetzt wird. Viele der darin untersuchten Bereiche und Kernergebnisse fanden sich auch auf der Agenda des Doha-Kongresses wieder. Insbesondere die internationale Zusammenarbeit bei Bekämpfung und Verfolgung von Cyberkriminalität sowie die elektronische Beweiserhebung, -speicherung und -verwertung spielten eine zentrale Rolle.

Deutlich wurde zunächst, dass zwar noch immer Unklarheiten über den Cyberkriminalitätsbegriff herrschen, auf der Fachebene jedoch, wie auch in der „Comprehensive Study on Cybercrime“, ein umfassender und pragmatischer Ansatz gewählt wird. Cyberkriminalität liegt daher vor, wenn eine Tat durch oder gegen einen Computer, ein Computernetzwerk oder Daten verübt wird. Folglich betrafen die Cybercrime-Themen des Kongresses nicht nur die Kerndelikte des Computerstrafrechts wie Hacking und Computersabotage, sondern auch Inhaltsdelikte wie die Verbreitung von Kinderpornographie sowie werkzeugbasierte Delikte wie Computerbetrug,

* Der *Verf.* ist Wiss. Mitarbeiter am Alexander von Humboldt Institut für Internet und Gesellschaft und Kollegiat des Kompetenznetzwerks für das Recht der zivilen Sicherheit in Europa (KORSE).

[1] Das Leitmotiv, die Agenda und die einzelnen Schwerpunktthemen des „Thirteenth United Nations Congress on Crime Prevention and Criminal Justice“ gehen zurück auf die Resolution 67/184 der Generalversammlung der Vereinten Nationen vom 20. Dezember 2012; abrufbar unter: http://www.unodc.org/documents/crime-congress/13th_crime_congress/GAresolution/A-RES-67-184.pdf (6.7.2015).

[2] Im Rahmen des Kongresses wurde zwischen der High-Level-Ebene (Staats- und Regierungschefs sowie deren unmittelbare Vertreter), der Working-Level-Ebene (Mitglieder der Delegationen von UN-Mitgliedstaaten sowie der Internationalen Organisationen) und der Expert-Level-Ebene (insbesondere Forscher sowie Unternehmensvertreter) unterschieden.

[3] Bangkok-Declaration, Nr. 16; abrufbar unter: http://www.unodc.org/pdf/crime/congress11/BangkokDeclaration.pdf (6.7.2015).

[4] Salvador-Declaration, Nr. 39 ff.; abrufbar unter: http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/Salvador_Declaration/Salvador_Declaration_E.pdf (6.7.2015).

[5] United Nations (Hrsg.), Comprehensive Study on Cybercrime, 2013, abrufbar unter: http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (6.7.2015).

internetbasierter Drogenhandel und Identitätsdiebstahl. Obwohl hinsichtlich der transnationalen Kooperation insbesondere auch die Angleichung des materiellen und formellen Strafrechts weithin als förderlich angesehen wird, wurde deutlich, dass die globale Harmonisierung des Cyberstrafrechts gegenwärtig als Utopie bezeichnet werden muss. Waren selbst die Arbeiten an der UNODC-Studie noch von diesem Ansatz geprägt, hat sich in der Realität gezeigt, dass die Bedürfnisse und Interessenskonflikte der beteiligten Staaten oftmals so unterschiedlich bzw. erheblich sind, dass eine umfassende und globale Lösung nicht realistisch erscheint. Dementsprechend haben sich auch die politischen und wissenschaftlichen Anstrengungen und Ziele verschoben und konzentrieren sich nunmehr auf die Etablierung und Umsetzung bestehender Instrumente sowie den Aufbau und die Erweiterung von Kompetenzen bei Gesetzgebung und Strafverfolgung (sog. Capacity building).

II. Erfahrungen und neue Ansätze bei der Bekämpfung der Cyberkriminalität[6]

1. „Strengthening crime prevention and criminal justice responses to evolving forms of crime, such as cybercrime and trafficking in cultural property, including lessons learned and international cooperation“ (UNODC)[7]

Im ersten offiziellen UNODC-Veranstaltungsteil gingen *Han-Kyun Kim* (Korean Institute of Criminology), *Francesca Bosco* (United Nations Interregional Crime and Justice Research Institute), *Richard Frank* (International Cybercrime Research Center, Simon Fraser University) und *Khalid Hamad Al Mohannadi* (Gulf Countries Council, Criminal Information Center to Combat Drugs) der Frage nach, ob Cyberkriminalität noch als moderne Kriminalitätserscheinung einzustufen ist. Dafür sprächen zwar die relative Neuartigkeit der Computertechnologie und das stetige weltweite Wachstum an Cyberdelikten, allerdings würden vermehrt auch klassische Delikte mit informations- und kommunikationstechnologischen Tatmitteln durchgeführt. *Alexander Seger* (Europarat) merkte an anderer Stelle dazu an, dass man früher etwa davon ausgegangen wäre, jedes Land benötige eine bestimmte Anzahl von Cyberkriminalitätsexperten in den Strafverfolgungsbehörden für spezielle Deliktsformen, während heute kaum noch ein Verbrechen ohne die Beteiligung von modernen Technologien denkbar sei. Vielmehr kämen jene entweder bereits bei der Tatbegehung oder spätestens im Rahmen der elektronischen Beweiserhebung, -sicherung und -verwertung zur Anwendung.

2. „Cybercrime: The Global Response“ (UNODC)

Im zweiten offiziellen UNODC-Event ging es um die Professionalisierung und Koordinierung der bestehenden Instrumente zur Bekämpfung der Cyberkriminalität auf globaler Ebene. *Loide A. N. Lungameni* (Chief of the Organized Crime and Illicit Trafficking Branch, UNODC) vertrat dabei die Auffassung, dass eine tatsächliche Rechtsharmonisierung zukünftig weder möglich noch nötig für eine effektive Bekämpfung sei. Stattdessen setze man bei UNODC verstärkt auf institutionelle Kooperationen mit anderen internationalen Organisationen und der Privatwirtschaft. Insbesondere Interpol, Europol (European Cybercrime Center EC3), das Commonwealth Secretariat, die Weltbank und die Internationale Telekommunications Union (ITU) seien wertvolle Partner. Im weiteren Verlauf der Vorträge und Diskussionen wurden sodann die unterschiedlichen Schwerpunkte der einzelnen Akteure deutlich. Interpol, vertreten durch den Computerforensiker *Silvino Schlickmann Junior*, sieht seine Aufgabe vorwiegend in der Koordinierung und Unterstützung von nationalen und regionalen Polizeiorganisationen und stellt dafür einerseits Personal und andererseits Expertise zur Verfügung. Aktuelle Impulse verspricht sich Interpol von der neu formierten „Interpol Global Alliance against Cybercrime“ und dem Interpol Global Complex for Innovation in Singapur, das ganz auf die technische Dimension der Cybercrime-Bekämpfung konzentriert ist. Europol, vertreten durch den Vorsitzenden des Netzwerks Organisierte Kriminalität *Robert Črepinko*, stellte das im Jahre 2013 gegründete European Cybercrime Center vor und wies auf die Vorteile lokaler und regionaler Initiativen hin. Vor allem die Bündelung von Informationen über kriminelle Aktivitäten im Cyberraum sei für die nationalen Strafverfolgungsbehörden von unschätzbarem Wert. Die Weltbank, vertreten durch *Jinyong Chung*, sieht ihre Aufgabe maßgeblich in der Entwicklung eines Standardmodells zur Erkennung und Einordnung von Cyberdelikten mit wirtschaftlichem Bezug um auf den Ergebnissen basierend nationale und internationale Gegenmaßnahmen ergreifen zu können. Zum Schluss des Panels war es wiederum an der Vertreterin von UNODC mit dem „Cybercrime Repository“[8] ein vielversprechendes Arbeitsergebnis zu präsentieren. Dabei handelt es sich um eine internationale Datenbank mit den Rubriken „Cybercrime-Gesetzestexten“, „Cybercrime-Gerichtsurteilen“ und „Cybercrime: Lessons learned“. Die Vereinten Nationen greifen dadurch den vielfach geäußerten Wunsch kleiner Mitgliedstaaten auf, ihnen die Vorarbeiten und gewonnenen Erkenntnisse größerer Mitgliedstaaten in aufbereiteter Form zugänglich zu machen.

3. „Capacity Building on Cybercrime“ (Europarat)

Der Vorsitzende des Cybercrime-Programms des Europarates *Alexander Seger* begann seinen Vortrag mit der Aussage, man sei froh, die Budapester Konvention[9] bereits im Jahre 2001 verhandelt zu haben, da heutzutage keinesfalls mehr mit

[6] Weiterführende Dokumente und Informationen zu den einzelnen Veranstaltungen finden sich unter: http://www.unodc.org/congress/en/documentation.html und http://www.un-congress.org//Sessions/AllSessions (6.7.2015).

[7] Die Internationalen Organisationen, Universitäten und Forschungsinstitute in den Klammerzusätzen übernahmen die Organisation und die Sitzungsleitung der jeweiligen Veranstaltung.

[8] Abrufbar unter: https://www.unodc.org/cld/index-cybrepo.jspx (6.7.2015).

[9] ETS Nr. 185 = BGBl. II 2008, S. 1242.

einem derartigen Konsens zu rechnen sei. Auch der Europarat lenke seine Anstrengungen daher auf die Umsetzung bestehender Instrumente. Zusätzlich machte er deutlich, dass nicht allein die Zahl der Unterschriften oder Ratifikationen ausschlaggebend für den Erfolg der Budapester Konvention seien, da vielfach nationale Gesetzgebungsinitiativen die Vorschriften der Budapester Konvention auch inoffiziell als Model-Gesetze heranzögen.

Staatsanwalt *Kritananda Naghee Reddy* für Mauritius und Staatssekretär *Geronimo Sy* für die Philippinen berichteten daraufhin über den Prozess der Kontaktaufnahme mit dem Europarat, über die Unterstützung bei der Umsetzung von Cyberkriminalitäts-Gesetzgebung und den damit verbundenen Schwierigkeiten bis hin zur aktuellen Begleitung und Zusammenarbeit bei der Verhütung und Aufklärung von Cyberdelikten. Insbesondere hoben die Vertreter der Schwellenländer hervor, dass Cyberkriminalität letztlich gar nicht mehr als moderne Verbrechenskategorie bezeichnet werden könne, sondern vielmehr entweder materiell oder formell im Wege digitaler Beweiserhebungen integraler Bestandteil vieler, auch herkömmlicher, Ermittlungsverfahren geworden sei.

4. „An International Perspective on Cybercrime: complexities and way forward" (O.P. Jindal Global University, Indien)

Auch *Indranath Gupta*, *Sanjeev P. Sahni* und *Brajesh Kumar* mit ihren jeweiligen Mitarbeitern erwarten keine Einigung im Hinblick auf eine globale Cybercrime-Konvention mehr. Auf Ebene der Vereinten Nationen sei man vor fünf Jahren beim Salvador-Kongress näher an einem solchen Instrument gewesen, als beim diesjährigen Doha-Kongress. Man gehe daher in Indien wissenschaftlich einen anderen Weg und entwickle ein Modell, um die Kosten von Cyberkriminalität benennen zu können, auch wenn diese nicht auf den ersten Blick monetär qualifizierbar seien. Durch einen solchen „cost-based-approach" erhoffe man sich ein verstärktes Bewusstsein in der Bevölkerung für die Verletzlichkeit vieler Lebensbereiche durch Cyberkriminalität schaffen zu können.

5. „Rule of Law and Internet Legislation" (Zhongnan University of Economics and Law, China)

Sowohl *Hanming Xu* (Zhongnan University of Economics and Law, China) als auch *Jian-ping Lu* (Beijing Normal University, China) setzten sich mit dem Zusammenhang der Machtverhältnisse im Internet und der Bekämpfung von Cyberdelikten auseinander. Sie kritisierten die Tatsache, dass der Einfluss auf die (Weiter-)Entwicklung des Internets nahezu ausschließlich in den USA monopolisiert sei. Zwar würden auch europäische Nationen darunter leiden, jedoch hätten diese effektive politische und wirtschaftliche Möglichkeiten, einem solchen Trend entgegenzuwirken, wie etwa die deutsch-französische Initiative zum Aufbau eines „europäischen Internets" zeige. Entwicklungs- und Schwellenländer hingegen seien massiv von den Entscheidungen der USA und der dort beheimateten Unternehmen abhängig. Durch diese Monopolisierung und den Erstzugriff auf Daten sei ein effektives Vorgehen gegen Cyberkriminalität oftmals nur dann möglich, wenn die Maßstäbe der USA und ihrer Partner übernommen würden.

Schließlich kritisierte *Xiaying Mei* (University of International Business and Economics, China) noch den (europäischen) Ansatz, persönliche Informationen grundsätzlich als Eigentum des jeweiligen Informationssubjekts zu betrachten. Gerade im Big Data Zeitalter sei dies weder rechtlich korrekt noch weiterführend. Es sei vielmehr zwischen privaten und öffentlichen Informationen zu unterscheiden, wobei zur Einordnung als Kriterien erstens der Informationsinhalt, zweitens das Informationsinteresse der Öffentlichkeit und drittens das Alters des Informationssubjekts heranzuziehen seien. Anhand dieser Parameter sei letztlich zu entscheiden, welche Informationen im ausschließlichen Verfügungsbereich des Informationssubjekts zu belassen sind und welche Daten den staatlichen Behörden oder der Allgemeinheit offen zugänglich gemacht werden dürfen.

6. „FIDUCIA – Research on Trust-Based Policy" (European Institute for Crime Prevention and Control)

Das EU-Forschungsprojekt FIDUCIA[10] erforscht die sog. vetrauensbasierte Kriminalitätsprävention. Insbesondere hinsichtlich moderner Kriminalitätserscheinungen wie Cyberkriminalität sei es nicht mehr ausreichend, bei normabweichendem Verhalten Sanktionen anzudrohen. Vielmehr sei normgerechtes Handeln durch die Stärkung des Vertrauens in Fairness und moralisch-ethische Integrität eines (Straf-) Verfahrens zu erzielen. Im FIDUCIA-Projekt sind unter Mitwirkung des Max-Planck-Instituts für ausländisches und internationales Strafrecht 13 europäische Forschungsinstitutionen versammelt, die seit 2012 ein Modell entwickelt haben, das den EU-Mitgliedstaaten und der Europäischen Union forschungsbasierte Gesetzgebungsvorschläge zur Kriminalitätsprävention bei Cyberdelikten unterbreiten soll.

III. Fazit und Ausblick

Der 13. UN-Kriminalitätskongress hat wieder einmal gezeigt, dass internationale Initiativen, Kooperationen und Forschungsprojekte weit über den aktuellen Stand politischer Konventionen und Vereinbarungen hinausreichen. Die Doha-Declaration[11] als offizielles Ergebnis des Kongresses ist der kleinste gemeinsame Nenner einer Staatengemeinschaft, die sich in vielen Aspekten globaler Kriminalitätsbekämpfung noch uneinig ist. Auf der Fachebene hingegen werden Akteure verschiedener Rechtskreise und Nationalitäten regelmäßig kooperativ tätig und entwickeln konkrete Lösungsansätze.

Nachdem die vergangenen UN-Kongresse noch von dem Geist des Suchens nach dem einen Instrument, der einen Konvention zur Bekämpfung der Cyberkriminalität getragen worden waren, hat sich die internationale Gemeinschaft von dieser Utopie mittlerweile verabschiedet. Stattdessen ist deutlich geworden, dass Informations- und Kommunikationstech-

[10] http://fiduciaproject.eu (6.7.2015).
[11] Als Entwurf abrufbar unter: http://www.unodc.org/documents/congress//Documentation/IN_SESSION/ACONF222_L6_e_V1502120.pdf (6.7.2015).

nologien bei sämtlichen, auch vermeintlich klassischen, Delikten zur Anwendung kommen. Daher ist vor allem der Aufbau technischer Expertise in der Fläche existenziell um modernen Begehungsformen effektiv entgegentreten zu können.