VEREINTE NATIONEN

Zeitschrift für die Vereinten Nationen und ihre Sonderorganisationen
German Review on the United Nations

Herausgegeben von der
Deutschen Gesellschaft für die
Vereinten Nationen (DGVN)

Die Vereinten Nationen im Cyberraum

Aus dem Inhalt

BWV ·
BERLINER WISSENSCHAFTS-VERLAG

2 16
64. Jahrgang | Seite 49–96
ISSN 0042-384 X | M 1308 F

Den Cyberraum regieren – aber wie?

Liebe Leserinnen und Leser,

»Die Kriege der Zukunft werden Cyberkriege sein« – so Atefeh Riazi, Beigeordnete Generalsekretärin und Leiterin des Amtes für Informations- und Kommunikationstechnologie bei den Vereinten Nationen. Sie schlug im Dezember 2015 vor, Expertinnen und Experten als ›digitale Blauhelme‹ für die UN zu rekrutieren. Das Internet verändert die Welt. Die UN müssen im Zeitalter der Digitalisierung Antworten auf neue Bedrohungen finden und den Rahmen setzen, um Chancen für Entwicklung nutzbar zu machen. Die internationale Politik versucht, Regelwerke zu etablieren, die dem technologischen Fortschritt Rechnung tragen. Auf eine Harmonisierung nationaler Rechtssysteme und ein Übereinkommen für den Cyberraum im Rahmen der UN wartet man allerdings bisher vergebens.

Vor dem Hintergrund zunehmender Sicherheitsbedrohungen durch Cyberangriffe zeichnet **Tim Maurer** die Entwicklung der Debatte zum Thema Cybersicherheit bei den Vereinten Nationen nach. Mittlerweile werden Bedrohungen auf dem Gebiet der Informationssicherheit als eine der großen Herausforderungen des 21. Jahrhunderts anerkannt. Maurer sieht in den UN eines der maßgeblichen Foren, um Regelwerke voranzubringen. **Tatiana Tropina** und **Nicolas von zur Mühlen** halten es für unwahrscheinlich, dass die Vereinten Nationen bei der Bekämpfung von Cyberkriminalität eine Führungsrolle einnehmen. Ihre Empfehlung lautet, sich beim Erfahrungsaufbau und der technischen Unterstützung zu engagieren sowie mit regionalen Organisationen zu kooperieren. Aus Sicht von **Wolfgang Kleinwächter** hat der staatenzentrierte Ansatz für Internet Governance ausgedient. Anlässlich des im Dezember 2015 verlängerten Mandats für das Internet Governance Forum (IGF) stellt er die Frage: Wer regiert das Internet? Im ›Ökosystem Internet Governance‹ sieht Kleinwächter keinen Gegensatz zwischen Multistakeholderismus und Multilateralismus, sondern einen Übergang zu komplexeren Verhandlungsstrukturen. **Anja Mihr** plädiert – mit Blick auf die Menschenrechte – ebenfalls für einen Multistakeholder-Ansatz. Sie kommt zu dem Schluss, dass es der Staatengemeinschaft bisher nicht gelungen ist, Menschenrechte im Cyberraum ausreichend zu schützen. In einem weiteren Punkt sind sich beide Autoren einig: Die Regulierung des Internets steht noch am Anfang.

Liefert das humanitäre Völkerrecht einen ausreichenden Rechtsrahmen für den Einsatz von Autonomen Waffensystemen? **Markus Wagner** ist der Meinung, dass die technologischen Voraussetzungen für einen Einsatz, der mit völkerrechtlichen Prinzipien in Einklag steht, momentan noch nicht gegeben sind. Unabhängig von technischen Möglichkeiten muss beantwortet werden, ob eine weitere Autonomisierung wünschenswert ist und wer die Verantwortung für den Einsatz autonomer Waffen trägt.

Sie halten heute die erste Ausgabe der Zeitschrift Vereinte Nationen unter der neuen Leitung der Redaktion in Händen. Ich freue mich darauf, die Zeitschrift mit Monique Lehmann und dem Redaktionsbeirat zu gestalten, den angestoßenen Reformprozess weiterzuführen und Ihnen eine interessante und qualitativ hochwertige Berichterstattung zu bieten.

Ich wünsche eine anregende Lektüre.

Sylvia Schwab

Sylvia Schwab, Leitende Redakteurin
schwab@dgvn.de

VEREINTE NATIONEN 64. Jahrgang | 2016 | Heft 2

Die Vereinten Nationen im Cyberraum

Inhalt

Cybersicherheit in einem komplexen Umfeld

Transatlantische Divergenzen und diplomatische Errungenschaften*

Tim Maurer

Die internationale Gemeinschaft ist zunehmend besorgt angesichts von häufiger auftretenden Vorfällen im Cyberraum in den vergangenen Jahren. Die Vereinten Nationen sind eines der zentralen Foren, in denen mögliche Regelwerke für den Cyberraum diskutiert werden. Dieser Beitrag analysiert die bisherigen Verhandlungen bei den Vereinten Nationen und zeigt zukünftige Herausforderungen auf. So wird vor allem die effektive Umsetzung der jüngsten Vereinbarungen für die Strategie, eine Regelung über freiwillige Normen zu erzielen, entscheidend sein.

Ein Cyberangriff verursachte in der Westukraine im Dezember 2015 einen Stromausfall. Die Auswirkungen waren gering, denn wenige Stunden nach Einsetzen des Stromausfalls stellten die Betreiber auf manuelle Kontrolle um. Es war nicht der erste Stromausfall während des Konflikts. Nur wenige Wochen zuvor wurde durch eine Bombenexplosion ein weitaus längerer Stromausfall auf der Halbinsel Krim ausgelöst. Dennoch ist der Vorfall erwähnenswert, denn es ist der erste bekannte Fall, bei dem während eines Konflikts ein Stromausfall durch Schadsoftware verursacht wurde. Nur ein Jahr zuvor machte der amerikanische Präsident Barack Obama mit Nordkorea erstmals einen Staat für einen Hackerangriff – auf die Firma Sony Pictures Entertainment – öffentlich verantwortlich. Der Stromausfall in der Westukraine ist also lediglich der jüngste in einer Reihe bekannter Vorfälle, die die Verschlechterung des Umfelds der Cybersicherheit aufzeigen.

Angesichts der gegenwärtigen Entwicklungen ist die Weltgemeinschaft zunehmend alarmiert und die diplomatischen Bemühungen in diesem Bereich werden verstärkt. Die Vereinten Nationen sind ein Hauptforum für die Diskussion zum Thema Cybersicherheit. In Bezug auf Cybersicherheit im Zusammenhang mit der Wahrung des Weltfriedens und der internationalen Sicherheit finden die Diskussionen im Ersten Ausschuss der UN-Generalversammlung, dem Ausschuss für Abrüstung und internationale Sicherheit, statt. Seit dem ersten, von Russland im Jahr 1998 eingereichten Resolutionsentwurf diskutiert der Erste Ausschuss die »Entwicklungen auf dem Gebiet der Informationstechnik und der Telekommunikation im Kontext der internationalen Sicherheit«[1]. Doch erst mit dem Amtsantritt von Präsident Obama im Jahr 2009 wurde die Debatte intensiver geführt. Mit der Verschiebung der außenpolitischen Prioritäten der USA unter Obama hin zu mehr internationalem Engagement war die amerikanische Regierung bereit, Ideen hinsichtlich internationaler Regeln zu Cybersicherheit und, seit neuestem, auch die Vision einer »internationalen Cyberstabilität« aktiv zu diskutieren.[2]

Innerhalb der letzten acht Jahre gab es in diesem Bereich verschiedene wichtige diplomatische Bemühungen. Die fünf ständigen Mitglieder des UN-Sicherheitsrats (China, Frankreich, Großbritannien, Russland und die USA) haben zusammen mit zehn weiteren Mitgliedstaaten in einem Bericht im Jahr 2010 anerkannt, dass die »bestehenden und potenziellen Bedrohungen auf dem Gebiet der Informationssicherheit zu den wichtigsten Herausforderungen des 21. Jahrhunderts gehören«[3]. Drei Jahre später erkannte eine ähnliche Gruppe an, dass das Völkerrecht auch online Anwendung findet und Informations- und Kommunikationstechnologien (information and communication technologies – ICTs) positiv beeinflusst.[4] Dies war ein bedeutender Wendepunkt, nachdem verschiedene Staaten zuvor die Anwendung des Völkerrechts angefochten hatten und sich stattdessen für die Entwicklung eines neuen Gesetzes für den Cyberraum einsetzten. Ein weiterer, im Konsens verabschiedeter Bericht, der im Jahr 2015 von einer Gruppe von 20 UN-Mitgliedstaaten vorgelegt wurde, hat neue Erkenntnisse zur Anwendung des bestehenden Völkerrechts und der Normen, die den Cyberraum regeln sollen, geliefert.[5]

Besonders hervorzuheben ist, dass all diese Empfehlungen in den Berichten der Gruppe von Regierungssachverständigen für Entwicklungen auf dem Gebiet der Informationstechnik und Telekommunikation im Kontext der internationalen Sicherheit (GGE), die von UN-Generalsekretär Kofi Annan auf

Tim Maurer, geb. 1984, leitet die Cyber Policy Initiative des Carnegie Endowment for International Peace in Washington, D.C., und ist Nonresident Fellow des Global Public Policy Institute (GPPi) in Berlin.

Übersetzung aus dem Englischen von Monique Lehmann.

* Dieser Beitrag beruht auf der Veröffentlichung von Tim Maurer, Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security?, Discussion Paper 2011-11, Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge 2011, www.belfercenter.ksg.harvard.edu/experts/2304/tim_maurer.html

1 UN Doc. A/RES/53/70 v. 4.12.1998.

2 White House. International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World, Washington, D.C., 2011; Department of State, International Security Advisory Board. Report on A Framework for International Cyber Stability, Washington, D.C., 2014.

3 UN Doc. A/65/201 v. 30.7.2010, S. 2.

4 UN Doc. A/68/98 v. 24.6.2013, S. 8.

5 UN Doc. A/70/174 v. 22.7.2015.

Die bisherigen Normen zur Anwendung des Völkerrechts im Cyberraum besitzen kaum rechtliche Gültigkeit.

Ersuchen der Mitgliedstaaten eingerichtet wurde, festgehalten sind. Bislang wurden diese Berichte jedoch nicht von den UN-Mitgliedstaaten als Resolution verabschiedet. Der jüngste Bericht wurde lediglich »begrüßt«. Aus diesem Grund besitzen sie selbst als sogenanntes ›Softlaw‹ nach dem Völkerrecht kaum rechtliche Gültigkeit. Vielmehr beruhen die Normen, die in diesen Dokumenten dargelegt sind, auf Freiwilligkeit. Ihre Umsetzung hängt vom politischen Willen der einzelnen Staaten und der internen Kohärenz ihrer Bürokratie ab. Dieser Beitrag zeichnet den Verlauf der Diskussionen in den Vereinten Nationen nach, der in vier Phasen untergliedert ist. Ergänzend liefert er eine Analyse der jüngsten Entwicklungen sowie einen Ausblick.

Mit der auslaufenden Amtszeit der Regierung Obama bleibt offen, in welche Richtung sich diese Agenda unter einer neuen amerikanischen Regierung zukünftig entwickeln wird. Eine neue, fünfte GGE wird im Herbst 2016 zusammentreffen. Es bleibt zudem abzuwarten, ob die Gruppe mit nunmehr 25 Mitgliedstaaten die Legitimität der GGE-Berichte stärken wird, um eine breite Unterstützung durch die UN-Mitgliedstaaten zu erreichen, oder ob sie sich darauf konzentrieren wird, das Thema inhaltlich weiter voranzubringen. Eine entscheidende Aufgabe wird außerdem sein, die Bestimmungen aus den früheren Berichten zu operationalisieren, sie mit Bedeutung zu füllen und somit tatsächlich das Sicherheitsumfeld zu verbessern. Nicht zuletzt wird die internationale Gemeinschaft der Frage nachgehen müssen, was nach dem fünften GGE-Treffen folgen wird. Es scheint wenig Interesse zu bestehen, ein sechstes Treffen in gleicher Form einzuberufen. Wird sich die GGE zu einer ergebnisoffenen Arbeitsgruppe oder einem anderen institutionellen Rahmenwerk entwickeln? Wie wird sie zudem nichtstaatliche Akteure etwa aus dem Industriebereich, der Zivilgesellschaft oder aus dem technischen Umfeld einbeziehen?

Historischer Hintergrund: Die UN und Cybersicherheit

Der Erste Hauptausschuss der UN-Generalversammlung steht seit Ende der neunziger Jahre im Mittelpunkt der Debatte zum Thema Cybersicherheit.

In einem Schreiben vom 23. September 1998 an den UN-Generalsekretär Annan forderte der russische Außenminister Igor Sergejewitsch Iwanow die Verteilung eines Resolutionsentwurfs zu Entwicklungen auf dem Gebiet der Informationstechnik und der Telekommunikation im Kontext der internationalen Sicherheit.[6] Seitdem hat die russische Regierung dem Ersten Hauptausschuss der UN-Generalversammlung jährlich eine Resolution zu diesem Thema vorgelegt. »Russland beabsichtigt, einen internationalen Rechtsrahmen aufzustellen, um die Anwendung von Informationstechnologien zu Zwecken, die nicht mit den Missionen zur Wahrung von Stabilität und Sicherheit einhergehen, zu verhindern«, erklärte der russische Verteidigungsminister Sergei Borissowitsch Iwanow einige Jahre später.[7] Der russische Vorschlag für ein Übereinkommen zur Informationssicherheit traf jedoch auf deutliche Skepsis. Laut Ronald Deibert, Professor für Politikwissenschaft und Direktor des Citizen Lab der Universität Toronto, drängte »Russland auf eine Rüstungskontrolle im Cyberraum beziehungsweise auf die Kontrolle von Informationswaffen. Die meisten Menschen sehen dies als unaufrichtig an und ich tendiere dazu, mich dem anzuschließen. Ein Großteil der Beobachterinnen und Beobachter bewertet dies als einen Versuch Russlands, die Vorherrschaft der USA in der virtuellen Sphäre zu beschränken. Russland ist weitaus mehr besorgt über Farbrevolutionen und die Mobilisierung durch Dissidenten und Menschenrechtsgruppen im Internet – und versucht, alle Möglichkeiten der USA, derartige soziale Bewegungen zu unterstützen, zu beseitigen, – als dass es sich um den Schutz des Internets sorgt.«[8] Laut der Berichterstatterin des Wall Street Journals Siobhan Gorman betrachteten die USA ein Abkommen als verfrüht aufgrund von Bedenken, ein solches Abkommen könne nicht verhindern, dass Staaten wie Russland und China Dritte dazu nutzen könnten, es zu unterlaufen.[9]

Die Diskussion im Rahmen der Vereinten Nationen über Cybersicherheit kann allgemein in zwei große Stränge unterteilt werden: auf der einen Seite handelt es sich um Verhandlungen, die sich auf die politisch-militärische Dimension von Cybersicherheit konzentrieren, auf der anderen Seite um solche, die den kriminellen Missbrauch von Informationstechnologie zum Gegenstand haben.[10] Dieser Beitrag beschränkt sich auf den politisch-militärischen Aspekt, der die potenzielle Nutzung von (Informations-) Technologien und Maßnahmen für Zwecke umfasst, die nicht mit den Zielen der Wahrung der Stabilität und Sicherheit einhergehen und stattdessen möglicherweise die Sicherheit von Staaten gefährden.[11] Bislang hat sich der UN-Sicherheitsrat nicht mit diesem Thema befasst. Stattdessen standen der Erste Hauptausschuss der UN-Generalversammlung und der zuvor genannte Prozess seit dem ersten Resolutionsentwurf im Jahr 1998 im Mittelpunkt der Debatte.

Phase 1: Der Anfang (1998 bis 2004)

Im Anschluss an den Brief des russischen Außenministers an den UN-Generalsekretär wurde der Resolutionsentwurf am 4. Dezember 1998 von der UN-Generalversammlung ohne förmliche Abstimmung angenommen.[12] Die Resolution für ein »Übereinkommen zur internationalen Informations- und Telekommunikationssicherheit«[13] konzentrierte sich auf folgende Schlüsselelemente: Zunächst benannte sie das militärische Potenzial von Informations- und Telekommunikationstechnologien[14] und zum ersten Mal wurden in einem UN-Dokument Bedenken geäußert, dass »diese Technologien mit dem Ziel der Wahrung der internationalen Stabilität und Sicher-

heit unvereinbar sind«.[15] Zweitens betonte es die Notwendigkeit, Cyberkriminalität und Cyberterrorismus zu verhindern, und drittens wurden die Mitgliedstaaten gebeten, dem Generalsekretär ihre Auffassungen hinsichtlich einer Definition der grundlegenden Begriffe im Zusammenhang mit der Informationssicherheit und der Ausarbeitung »internationaler Grundsätze« mitzuteilen.[16] In den Folgejahren hat die russische Regierung diesen Resolutionsentwurf als Hauptbefürworter weiterhin vorgelegt. Er wurde schließlich von der Generalversammlung angenommen, allerdings ohne dass weitere Maßnahmen eingeleitet wurden. Einzig einige Mitgliedstaaten haben dem UN-Generalsekretariat Berichte vorgelegt, um entsprechend der Resolution Informationen zu teilen. Zusammengefasst kann gesagt werden: Die Resolution ruhte.

Phase 2: Strittige Politik (2005 bis 2008)

Im Jahr 2005 fand innerhalb des Ersten Hauptausschusses ein Wandel statt. Es war die zweite Amtszeit des amerikanischen Präsidenten George W. Bush und die Beziehungen zwischen den USA und den Vereinten Nationen erreichten nach dem gescheiterten Weltgipfel im Jahr 2005 ihren historischen Tiefpunkt. Der von Russland vorgelegte Resolutionsentwurf wurde verabschiedet und zum ersten Mal in seiner Geschichte förmlich abgestimmt. Die USA waren der einzige Staat, der am 28. Oktober 2005 gegen die Resolution stimmte.[17] Der Resolutionsentwurf wurde im Jahr 2006 nicht mehr allein von Russland eingebracht.[18] Armenien, Belarus, China, Kasachstan, Kirgisistan, Myanmar, Tadschikistan und Usbekistan reichten den Resolutionsentwurf mit ein und in den Folgejahren schlossen sich weitere Staaten an.[19] Etwa zur gleichen Zeit, im Jahr 2007 nach einem Hackerangriff gegen Estland und im Jahr 2008 während des georgisch-russischen Krieges, füllte der Begriff ›Cyberkrieg‹ die Schlagzeilen großer Tageszeitungen. Während der wissenschaftliche Diskurs darüber, was ›Cyberkrieg‹ bedeutet, bis heute andauert, schafften die Schlagzeilen derweil mehr öffentliche Aufmerksamkeit. Sie trugen dazu bei, dass sich das Bewusstsein politischer Entscheidungsträgerinnen und Entscheidungsträger für das Thema erhöhte, und lenkten es beispielsweise auf die Diskussion, ob ein Cyberangriff die Anwendung des Artikels 5 der Nordatlantikvertragsorganisation (NATO) auslösen könnte.[20]

Phase 3: Von der Spaltung zur Beteiligung (2009 bis 2013)

Während die Medien zunehmend über die weltweiten Bedrohungen der Cybersicherheit berichteten, wurde die Bush-Regierung von der Regierung unter Präsident Obama abgelöst. Die Obama-Regierung verfolgte nicht nur eine Politik des Neustarts in Bezug auf Russland, sondern auch in den Vereinten Nationen. Die New York Times berichtete, dass im November 2009 eine »russische Delegation, geleitet von General Vladislav P. Sherstyuk, einem stellvertretendem Sekretär des Sicherheitsrats und ehemaligem Leiter der Nationalen Sicherheitsbehörde Russlands, mit amerikanischen Vertreterinnen und Vertretern des Nationalen Sicherheitsrats, des Außen- und des Verteidigungsministeriums sowie des Ministeriums für Innere Sicherheit in Washington, D.C., zusammentraf. Insider verwiesen darauf, dass beide Seiten bei der Beseitigung von Unstimmigkeiten, die lange Zeit beide Staaten spalteten, Fortschritte erzielten. Zwei Wochen später erklärten sich die USA in Genf bereit, die Themen Cyberkrieg und Cybersicherheit mit Vertreterinnen und Vertretern des UN-Ausschusses für Abrüstung und internationale Sicherheit zu diskutieren.«[21]

Im Zuge dieser Entwicklungen wurden seit Oktober 2009, wie in der Zeit vor dem Jahr 2005, die Resolutionsentwürfe im Ersten Hauptausschuss ohne förmliche Abstimmung angenommen. Darüber hinaus legte die Obama-Regierung im Januar 2010 ein Positionspapier vor, mit dem Ziel, die verschiedenen Parteien enger zusammenzubringen.[22] Einige Zeit später erklärte Richard Clarke, ehemaliger Son-

Während der wissenschaftliche Diskurs darüber, was ›Cyberkrieg‹ bedeutet, bis heute andauert, verschafften die Schlagzeilen in den Jahren 2007 und 2008 öffentliche Aufmerksamkeit und trugen dazu bei, dass sich das politische Bewusstsein für das Thema erhöhte.

6 Anatolij A. Streltsov, International information security: description and legal aspects, United Nations Institute for Disarmament Research (UNIDIR), Geneva 2007.

7 Christopher A. Ford, The Trouble with Cyber Arms Control, The New Atlantis. A Journal of Technology & Society. Vol. 29/2010, S. 65.

8 Ronald Deibert, Tracking the emerging arms race in cyberspace, Bulletin of the Atomic Scientists, Vol. 67, Isssue 1, 2011, S. 6.

9 Siobhan Gorman, U.S. Backs Talks on Cyber Warfare, The Wall Street Journal, 4.6.2010.

10 UN-Dok. A/RES/55/63 v. 4.12.2000, ausführlich zu Cyberkriminalität: Tatiana Tropina/Nicolas von zur Mühlen, in diesem Heft, S. 56–60.

11 UN Doc. A/RES/53/70 v. 4.12.1998.

12 Ebd.

13 John Markoff, Step Taken to End Impasse Over Cybersecurity Talks, The New York Times, 16.7.2010.

14 Anatolij A. Streltsov, a.a.O. (Anm. 6).

15 UN-Dok. A/RES/53/70 v. 4.12.1998, S. 2.

16 Zur Relevanz von Definitionen in dieser Debatte siehe Analyse von Tim Maurer/Robert Morgus, ›Cybersecurity‹ and Why Definitions Are Risky, The International Relations and Security Network, 10.11.2014, www.isnblog.ethz.ch/intelligence/cybersecurity-and-the-problem-of-definitions

17 UN Doc. A/60/452 v. 16.11.2005.

18 UN Doc. A/C.1/61/L.35 v. 11.10.2006.

19 Ebd.

20 Ian Traynor, Russia Accused of Unleashing Cyberwar to Disable Estonia, The Guardian, 16.5.2007.

21 John Markoff/Andrew E. Kramer, In Shift, U.S. Talks to Russia on Internet Security, The New York Times, 13.12.2009.

22 John Markoff, a.a.O. (Anm. 13).

derberater für Cybersicherheit von George W. Bush, in seinem Buch: »Vielleicht sollte ich zugeben, dass ich den russischen Vorschlag abgelehnt habe. […] In den Vereinten Nationen standen die USA mit ihrer Ablehnung der Cybergespräche beinahe allein. Wir sagten ›Nein‹ […] und wir haben jetzt mehr als eine Dekade lang ›Nein‹ gesagt […] es ist an der Zeit, dass die USA ihre Position bezüglich einer Kontrolle von Cyberwaffen überprüfen.«[23] Der grundlegende politische Wandel aufgrund des Wechsels der amerikanischen Regierung hatte dazu geführt, dass die USA den Resolutionsentwurf zum ersten Mal miteinbrachten, nachdem sie in der Zeit von 2005 bis 2008 dagegen stimmten.

Angesichts des vorangegangenen politischen Klimas war der Bericht der GGE aus dem Jahr 2010 ein wichtiger symbolischer Meilenstein und ein diplomatischer Erfolg.

Phase 4: Erste Vereinbarungen und substanzielle Fortschritte (2013 bis 2015)

Mit den diplomatischen Bemühungen entfalteten sich inhaltliche Diskussionen zum Thema Cybersicherheit. Im Jahr 2004 hatte der Erste Hauptausschuss die erste GGE eingerichtet, in der Hoffnung, dass diese kleinere Gruppe, bestehend aus nur 15 Vertreterinnen und Vertretern der UN-Mitgliedstaaten, mehr Fortschritte erzielen würde. Doch diese erste GGE, die im Jahr 2005 einen Bericht vorlegen sollte, scheiterte letztlich, eine gemeinsame Position vorzubringen. »Das größte Hindernis lag in der Frage, ob das Völkerrecht und das humanitäre Völkerrecht die Sicherheitsaspekte internationaler Beziehungen in Fällen des feindlichen Einsatzes von ICT zu politisch-militärischen Zwecken ausreichend regeln.«[24] Eine zweite GGE wurde im Jahr 2009 eingerichtet – ein weiteres Zeichen für den Wandel, der mit der neuen amerikanischen Regierung einherging. Dieses Mal einigte sich die Gruppe und gab in einer ersten Vereinbarung bekannt, dass »bestehende und potenzielle Bedrohungen auf dem Gebiet der Informationssicherheit zu den größten Herausforderungen des 21. Jahrhunderts gehören«[25]. Die Bedrohung wurde demnach als groß genug eingeschätzt, um ein Risiko für den internationalen Frieden und die nationale Sicherheit darzustellen.

Die internationale Gemeinschaft kam überein, dass das Völkerrecht sowohl online als auch offline Anwendung finden muss.

Angesichts des vorangegangenen politischen Klimas war der Bericht der GGE aus dem Jahr 2010 ein wichtiger symbolischer Meilenstein und ein diplomatischer Erfolg. In einem Artikel der Washington Post wurde konstatiert, dass »eine Gruppe von Staaten – einschließlich China, Russland und den USA – zum ersten Mal die Bereitschaft signalisiert hat, sich gemeinsam dabei zu unterstützen, Bedrohungen durch Angriffe auf ihre Computernetzwerke einzudämmen«. Es wurde darin weiter betont, »dass die Russen im Jahr 1998 einen Vorschlag für ein Übereinkommen vorgebracht hatten, der die Nutzung des Cyberraums für militärische Zwecke untersagt«. Zitiert wurde zudem Robert Knake, der die neuen Entwicklungen als einen »Bestandteil der Strategie der Obama-Regierung, sich diplomatisch zu beteiligen«, versteht. Mit den Worten eines Mitarbeiters aus Regierungskreisen: »Es entwickelt sich zunehmend ein Bewusstsein dafür, dass es notwendig ist, die Risiken international anzugehen.«[26]

Inhaltlich war der Bericht der GGE aus dem Jahr 2010 jedoch sehr vage formuliert. Ein erster substanzieller Durchbruch fand nur drei Jahre später statt. In einer Resolution, die neben Russland nun von weiteren 26 Staaten eingebracht wurde, wurde der UN-Generalsekretär aufgefordert, im Jahr 2012 eine neue GGE einzurichten und der 68. UN-Generalversammlung im Jahr 2013 einen Bericht vorzulegen.[27] Diese neue GGE ging über die ursprüngliche Vereinbarung hinaus und hob in ihrem Bericht im Jahr 2013 besonders hervor, dass »das Völkerrecht, insbesondere die Charta der Vereinten Nationen, Anwendung findet und maßgeblich zur Wahrung des Friedens und der Stabilität beiträgt sowie eine offene, sichere, friedliche und für alle zugängliche Struktur der Informations- und Kommunikationstechnologien (information and communication technologies – ICTs) fördert.«[28] Mit anderen Worten: Was Streltsov vor beinahe zehn Jahren als das »größte Hindernis« auf dem Weg zu einem Konsensbericht beschrieben hatte, war nun beseitigt. Die internationale Gemeinschaft, so auch China, Russland und die USA, kam überein, dass das Völkerrecht sowohl online als auch offline Anwendung finden muss. Erwähnenswert ist, dass dieses Zugeständnis damit dem generellen Umdenken der internationalen Gemeinschaft entsprach. So kam beispielsweise auch der UN-Menschenrechtsrat im Jahr 2012 zu dem Schluss, dass »die gleichen Rechte, die Menschen offline genießen, auch online zu schützen sind«[29].

Die diplomatischen Bemühungen in Bezug auf Cybersicherheit wurden seit der Amtsaufnahme der amerikanischen Regierung im Jahr 2009 verstärkt. Angesichts der besorgniserregenden Medienberichte über das sich verschlechternde Sicherheitsumfeld wurden neue inhaltliche Vorschläge in Umlauf gebracht. Im Jahr 2011 veröffentlichte die amerikanische Regierung ihre ›Internationale Strategie für den Cyberraum‹, während China und Russland mit der Shanghaier Organisation für Zusammenarbeit (Shanghai Cooperation Organization – SOC) zusammenarbeiteten, um den Entwurf für einen ›Internationalen Verhaltenskodex für die Informationssicherheit‹ zu erstellen.[30] Deutlich wurde, dass die amerikanische Regierung nun zwar bereit war, sich an dem Thema zu beteiligen, doch die Unstimmigkeiten der neunziger Jahre blieben weiter bestehen.

Laut Joseph Nye »strebte Russland seit mehr als einem Jahrzehnt nach einem Übereinkommen für eine internationale Kontrollinstanz über das Internet, das die Täuschung mit oder die Einbettung von schädlichen Codes verbietet, die im Falle eines Krieges aktiviert werden könnten. Die Amerikaner wen-

deten jedoch ein, dass Maßnahmen zur Verhinderung von Angriffen wiederum die Maßnahmen zur Verteidigung gegen tatsächliche Angriffe beeinträchtigen können. Zudem wäre es unmöglich, diese zu verifizieren oder zu erzwingen. Darüber hinaus wehrten die Vereinigten Staaten Vereinbarungen ab, die die Zensur des Internets durch autoritäre Regierungen legitimieren könnten. Dennoch nahmen die USA formelle Gespräche mit Russland auf. Doch selbst die Fürsprecherinnen und Fürsprecher eines internationalen Gesetzes für die Verwendung von Informationstechnologien stehen einem multilateralen Vertrag ähnlich den Genfer Konventionen, der – angesichts der zukünftigen technologischen Unbeständigkeit – spezifische und detaillierte Vorschriften enthalten würde, skeptisch gegenüber. Sie vertreten die Ansicht, dass gleichgesinnte Staaten Regeln festlegen könnten, die sich mit der Zeit zu Normen herausbilden könnten.«[31]

Für viele Beobachter war es somit überraschend, dass die fünfte GGE aus dem Schatten des GGE-Berichts aus dem Jahr 2013 trat und inhaltlich mehr Substanz entwickelte. Nicht nur wurde die Gruppe von 15 auf 20 Mitgliedstaaten erhöht. Vor dem Hintergrund des Konflikts in der Ukraine traf sie auch auf starke geopolitische Spannungen. Zur Halbzeit des Prozesses schätzten einige Mitglieder der Gruppe die Chance, ein Abkommen zu erreichen, auf 50 Prozent ein. Die GGE verabschiedete letztlich einen neuen Konsensbericht, in dem eine Reihe spezifischer Normen umrissen werden, beispielsweise zum Schutz von autorisierten Notfallteams und hinsichtlich wichtiger Infrastrukturen.

Wohin geht der Weg?

Die fünfte GGE wird im Herbst 2016 zusammentreffen – was gleichzeitig den Auftakt der fünften Phase markiert. Nachdem in den letzten Jahren erste Vereinbarungen und erhebliche Fortschritte erzielt wurden, steht die internationale Gemeinschaft vor einer wichtigen Herausforderung: Wie kann die Legitimität dieser Vereinbarungen erhöht und wie können diese umgesetzt werden, sodass die Sicherheitslage tatsächlich verbessert werden kann?

Die jüngsten Ereignisse werfen auch die Frage auf, inwiefern die bestehenden Vereinbarungen zu interpretieren sind und was im Falle von Verstößen passiert. Die Vereinbarung, die sich insbesondere auf wichtige Infrastrukturen konzentriert, besagt zum Beispiel, dass »kein Staat ICT-Aktivitäten durchführen oder wissentlich unterstützen sollte, die den völkerrechtlichen Verpflichtungen widersprechen oder bewusst darauf abzielen, wichtige Infrastrukturen zu beschädigen oder auf andere Weise die Nutzung und den Betrieb wichtiger Infrastrukturen beeinträchtigen, die Dienstleistungen für die Öffentlichkeit bieten«[32]. Welchen Unterschied macht die Formulierung »sollte nicht« gegenüber der Formulierung »darf nicht« aus, beispielsweise in dem hypothetischen Fall, der Stromausfall in der Ukraine wäre das Ergebnis einer staatlich unterstützten Handlung? Was wären die Konsequenzen?

Um ihre Legitimität zu erhöhen, wurde die neue GGE nun auf 25 Mitgliedstaaten erweitert. Daneben hat eine beträchtliche Anzahl von Staaten gegenüber dem UN-Generalsekretariat ihr Interesse an einer Beteiligung zum Ausdruck gebracht. Die Auswahl der GGE-Mitglieder wird ein wichtiger Indikator sein und eine bedeutende Rolle bei der Einbindung der UN-Mitgliedstaaten spielen. Wagt man jedoch einen Blick über die fünfte GGE hinaus, wie wird sich der Prozess zukünftig gestalten? Wird die GGE eine ergebnisoffene Arbeitsgruppe werden? Oder wird sie in ein anderes institutionelles Gefüge übergehen und möglicherweise nichtstaatliche Akteure einbinden? Wie wird sie mit anderen gegenwärtig stattfindenden Diskussionen umgehen, zum Beispiel in Bezug auf China und Wirtschaftsspionage und den damit verbundenen jüngsten bilateralen Aussagen und den Darlegungen der Gruppe der 20 (G20)? Wie verhält sich die GGE hinsichtlich der Diskussion zu Überwachung im Dritten Hauptausschuss der Generalversammlung? Die Herausforderung wird sein, eine Balance zwischen einem integrativen Prozess mit zunehmender Beteiligung und gleichzeitigem inhaltlichem Fortschritt zu erreichen.

Eine dringliche Herausforderung ist die wachsende Kluft zwischen den diplomatischen Errungenschaften und der sich kontinuierlich verschlechternden Sicherheitslage.

Eine umfassendere und zunehmend dringliche Herausforderung ist die wachsende Kluft zwischen den diplomatischen Errungenschaften und der sich kontinuierlich verschlechternden Sicherheitslage. Neben staatlichen Akteuren und Fragen der Kohärenz des innenpolitischen Vorgehens fordern auch nichtstaatliche Akteure mehr Mitsprache. Damit stellt sich auch die Frage, welche Institution das geeignete, schnellste und effektivste Forum ist, um die Diskussionen voranzubringen.

23 Richard A. Clarke/Robert Knake, Cyber War: The Next Threat to National Security and What to Do About It, New York 2010, S. 218–219.

24 Anatolij A. Streltsov, a.a.O. (Anm. 7), S. 6–7.

25 UN Doc. A/65/201 v. 30.7.2010, S. 6.

26 Ellen Nakashima, 15 Nations Agree to Start Working Together to Reduce Cyberwarfare Threat, The Washington Post, 17.7.2010.

27 UN Doc. A/65/405 v. 9.11.2010, S. 5.

28 UN Doc. A/68/98 v. 24.6.2013, S. 8.

29 Library of Congress, U.N. Human Rights Council: First Resolution on Internet Free Speech, 12.7.2012.

30 White House. International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World, Washington, D.C., 2011; UN Doc. A/66/359 v. 14.9.2011.

31 Joseph S. Nye Jr., Cyberpower, Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge 2010, S. 18.

32 Ebd.

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

Bedrohte Menschenrechte im Cyberraum

Anja Mihr

Die Umsetzung grundlegender Freiheitsrechte, sozialer und wirtschaftlicher Menschenrechte und der Ziele für nachhaltige Entwicklung (Sustainable Development Goals – SDGs) sind ohne das Internet heute nicht mehr denkbar. Jedoch gelang es der Staatengemeinschaft bislang nicht, Menschenrechte sowohl offline als auch online ausreichend zu schützen und zu fördern. Daher verabschiedete die UN-Generalversammlung im Dezember 2015 eine Resolution, die der Förderung und dem Schutz der Menschenrechte im Internet neue Regeln geben soll.

Im digitalen Zeitalter wird der internationale Menschenrechtskodex der Vereinten Nationen immer dann bemüht, wenn Regierungen bei der Bekämpfung von Sicherheitsrisiken im Internet nicht weiterkommen. Menschenrechte sind häufig das letzte Mittel beim Miteinander im ›staatenlosen‹, anarchischen Cyberraum[1]. Wenn staatliche Behörden und die nationale Rechtsprechung es nicht schaffen, Internetkriminalität zu verhindern, appellieren staatliche Stellen gerne an die individuelle Verantwortung des Nutzers. Dementsprechend sollte jeder Nutzerin und jedem Nutzer der freie Zugang zu Informationen, Schutz der Privatsphäre, Chancen der persönlichen, beruflichen und privaten Entwicklung, das Recht auf Meinungsfreiheit sowie auf Arbeit und Gesundheit gewährt werden. Im Umkehrschluss sollten Nutzerinnen und Nutzer damit verantwortungsbewusst umgehen.

Zu den Regierungen als einzige maßgebliche Akteure, die diese Rechte schützen, fördern oder verletzen, sind andere Akteure hinzugekommen: Nutzerinnen und Nutzer, private Unternehmen oder kriminelle Organisationen. Sie alle sollen miteinander Frieden, Freiheit und Sicherheit des Internets aushandeln und damit für einen allen gleichermaßen zugänglichen Internetzugang im Cyberraum Sorge tragen. Der Staat als einziger Garant für den Schutz der Menschenrechte im Internet hat sich *de facto* schon lange von dieser Rolle verabschiedet.

Heute zählen die Sicherheitsrisiken und die Verletzung der grundlegenden Freiheitsrechte im Cyberraum zu den Prioritäten jeder gesellschaftspolitischen Debatte. Dem tragen die hastigen Aktivitäten der Vereinten Nationen spätestens seit der Gründung des Internet Governance Forums (IGF) im Jahr 2005 Rechnung.[2] Trotz aller Appelle und Resolutionen internationaler Organisationen in den letzten Jahren und der wiederholten Beteuerung aller staatlichen und nichtstaatlichen Akteure, dass Menschenrechte sowohl offline als auch online gültig seien, gelang es der Staatengemeinschaft nicht, das Menschenrecht auf Privatsphäre zu harmonisieren. Auch die im Jahr 2013 verabschiedete ›Charta der Menschenrechte und Prinzipien für das Internet‹ im Auftrag des IGFs änderte daran zunächst nichts.[3] Die UN hofften, die Ursachen dafür mit einer neuen Resolution zu benennen und Anreize zu schaffen, diese zu beheben.

Aus Anlass einer Evaluierung des IGFs durch die Gruppe der Vereinten Nationen für die Informationsgesellschaft (United Nations Group on the Information Society – UNGIS) verabschiedete die UN-Generalversammlung im Dezember 2015 die umfassende Resolution 70/125 zu Multistakeholder-Ansätzen und Teilhabe im Internet.[4] Entsprechend dieser Resolution soll eine Informationsgesellschaft aufgebaut werden, die die nachhaltige Entwicklung und die Lebensqualität jedes Einzelnen fördert. Das Internet, so die Staatenvertreterinnen und Staatenvertreter, spiele dabei mehr denn je eine wesentliche Rolle und die Informations- und Kommunikationstechnologie leiste einen bereichsübergreifenden Beitrag, schnellere Fortschritte bei den Zielen für nachhaltige Entwicklung zu erwirken. Nur wenn private Nutzerinnen und Nutzer, Unternehmen, Wissenschaftlerinnen und Wissenschaftler sowie Regierungen zusammenarbeiten, gelingt die Umsetzung der Ziele für nachhaltige Entwicklung (Sustainable Development Goals – SDGs). Betrachtet man die Tragweite und Ehrgeizigkeit dieser Ziele, so hängt letztlich auch die Zukunft und das Weiterbestehen der Vereinten Nationen von der Verwirklichung der Ziele ab.

Dr. Anja Mihr, geb. 1969, ist Gründerin und Leiterin des HUMBOLDT-VIADRINA Centers on Governance through Human Rights in Berlin. Sie vertritt zudem den Franz-Haniel Chair of Public Policy an der Willy-Brandt-School of Public Policy der Universität Erfurt.

1 Als Cyberraum (Cyberspace) wird ein virtueller mehrdimensionaler Raum bezeichnet, der mithilfe von Computern oder mobiler Technologie ›betreten‹ werden kann. Das Internet ist ein Netzwerk von Dienstanbietern, Plattformen oder Nutzerinnen und Nutzern, die im Cyberraum kommunizieren und sich vernetzen.

2 Siehe zur Gründung: Wolfgang Kleinwächter, Globalisierung und Cyberspace. Der Weltgipfel über die Informationsgesellschaft weist den Weg, VN, 1–2, 2006, S. 38–44, sowie www.intgovforum.org

3 Siehe dazu Internet Rights and Principles Coalition, Die Charta der Menschenrechte und Prinzipien für das Internet, United Nations, 2013, www.internetrightsandprinciples.org/site/wp-content/uploads/2014/06/IRPC_booklet_29May2014_German.pdf

4 Vgl. UN-Dok. A/RES/70/125 v. 16.12.2015.

Resolution 70/125 sieht die Neuverteilung von Verantwortlichkeiten, Entscheidungsbefugnissen, Einfluss und der Systemordnung vor. Ziel ist es, das Internet neutral, für alle zugänglich und sicher zu machen sowie Cyberkriminalität und Cyberterror zu verhindern. Gleichzeitig soll der Zugang zum Internet die persönliche Entwicklung aller Menschen ermöglichen. Jeder Mensch hat eine Rolle und Verantwortung, so die Resolution, nicht nur Regierungen. Waren es bis dato vor allem Regierungen und staatliche Einrichtungen, die im Sinne der Menschenrechte verantwortlich zu handeln hatten, ist diese Verantwortung in den letzten Jahren fast schleichend an andere, zumeist private und nichtstaatliche Akteure abgegeben worden.[5] Noch existieren allerdings weder lokal, regional, international, global noch ›cyberal‹ entsprechende Umsetzungs- und Einhaltungsmechanismen. Als Erfolg ist immerhin zu werten, dass sich Staaten wie China, Russland, Singapur, die Türkei oder die USA davon verabschiedet haben, zu glauben, sie könnten das Internet allein kontrollieren. Internet Governance ist Multistakeholder-Governance: Jeder Akteur darf bei der Norm- und Regelsetzung mitmischen und übernimmt Verantwortung bei der Einhaltung oder Nichteinhaltung dieser Regeln. Was für Wissenschaftlerinnen und Wissenschaftler sowie internetaffine Personen keine neue Erkenntnis ist, war auf Staatenebene noch bis letztes Jahr umstritten. Nicht umsonst ist im Jahr 2015 zum ersten Mal beim jährlich tagenden Internet Governance Forum das Thema Menschenrechte und Verantwortung auf die Agenda gekommen. Auch das NATO Cooperative Cyber Defence Centre of Excellence in Tallin, das sich zuvor ausschließlich mit Sicherheitsfragen befasst hat, beschäftigt sich seit letztem Jahr mit dem Thema.[6]

Waren es bis dato vor allem Regierungen, die im Sinne der Menschenrechte verantwortlich zu handeln hatten, ist diese Verantwortung in den letzten Jahren zumeist an private und nichtstaatliche Akteure abgegeben worden.

Die Resolution liest sich daher wie ein lang überfälliges Eingeständnis der Realität. In Zeiten von nicht zu lokalisierenden Nutzern und Domainbesitzern, von Hasspredigern, Terrornetzwerken und Anbietern von Kinderpornografie wäre es fatal, auf nationalstaatliche Kompetenz in Fragen von Sicherheit und Frieden zu beharren. Internet Governance beruht entsprechend des Vorschlags der UNGIS auf dem Multistakeholder-Ansatz für erstens mehr Verantwortlichkeit aller Akteure, zweitens mehr Transparenz und Freiheitsrechte für alle Nutzerinnen und Nutzer und drittens mehr Teilhabe von Akteuren durch Cybertools, wie zum Beispiel das Internet, Smartphones und andere mobile Geräte. Kurz: Internet Governance bedeutet verantwortungsbewusster Umgang aller Akteure im Internet. Wer diesen Umgang einfordern, einhalten oder überwachen soll, ist noch offen. Genau darum geht es jedoch bei dem Thema Menschenrechte im Cyberraum und damit auch im Internet. Wer hat die Interpretationshoheit, wer darf daran teilhaben und wer setzt die Ergebnisse im Anschluss daran um? Welche globalen, unabhängigen, transparenten und rotierenden Mechanismen braucht es, um allen Akteuren gerecht zu werden? Auch hier versucht die UN-Generalversammlung seit dem Jahr 2013, ein multistakeholder-basiertes Governance-System zu schaffen.[7]

Die Pflicht, die Menschenrechte im Cyberraum zu schützen, wird aus dem Prinzip der territorialen Souveränität abgeleitet.

Warum Internet Governance?

Bereits in Resolution 68/167 zu Sicherheitsfragen und der Privatsphäre im Internet aus dem Jahr 2013 forderte die Generalversammlung die Regierungen auf, Maßnahmen zu ergreifen und die Menschenrechte auf der ›Datenautobahn‹ zu schützen.[8] Es sollten ›Verkehrsregeln‹ für die Nutzung des virtuellen Raums eingeführt werden. Entsprechend den internationalen Menschenrechtsrechtsverträgen soll das Sammeln und die Weiterverarbeitung von persönlichen Daten unter gleichen und für alle nachvollziehbaren Kriterien offen gelegt werden. Was sich damals noch wie Wunschdenken anhörte, hat in den letzten zwei Jahren durch unzählige nationale und einige internationale Gerichtsentscheidungen an Format gewonnen. Es handelt sich dabei um Präzedenzfälle, die möglicherweise den Weg zu einem internationalen ›Cyber- oder Internetgerichtshof‹ bereiten könnten.

Denn die Möglichkeiten nationaler Gerichtsbarkeit im Fall von Internetkriminalität sind schon lange ausgeschöpft. Das neue globale Rechts- oder Leitungssystem ist jedoch noch nicht etabliert und legitimiert, geschweige denn souverän.[9] Internationale Rechtssysteme wie die des Seerechts, der Raumfahrt oder der extraterritorialen Verpflichtungen sind noch staatenzentriert, werden jedoch oft als Beispiele für die zukünftige Entwicklung einer ›Cyberjustiz‹ zu Rate gezogen. Nationale Grenzen, Staatszugehörigkeiten oder ein Eintrag in ein Handels- und Vereinsregister in einem bestimmten Land spielen dann keine Rolle mehr, sondern allein die Tat und die Verantwortlichkeit – so der Wunsch der Visionäre: eine ›geteilte Verantwortlichkeit‹, wie sie bereits seit langem im Klima- und Menschenrechtsregime Thema ist.[10]

Die Pflicht, die Menschenrechte im Cyberraum zu schützen, wird aus dem Prinzip der territorialen Souveränität abgeleitet. Der Internationale Gerichtshof (IGH) in Den Haag hat argumentiert, dass aufgrund der (bisherigen) territorialen Souveränität Menschenrechte im Cyberraum zu schützen seien, wenn Unternehmen ihre Server innerhalb der eigenen Staatsgrenzen betreiben. Da diese Server stets auch physisch lokalisiert sind, müssen Regierungen aktiv werden – auch wenn sie damit nur beschränkt Rechte schützen.[11] Während Unternehmen wie Google, Twitter, Youtube oder Facebook die Verantwortung für ihre Angebote tragen müssen – egal in welchem Land oder auf See –, sollten Staaten die Betreiber von Servern zur Verantwortung ziehen,

auch wenn deren Angebot nicht die eigene Bevölkerung betrifft.

Als Reaktion auf die Debatte, ob Internet-Souveränität und -Legitimität staatliche Institutionen schwächt oder stärkt, hat der damalige UN-Sonderberichterstatter über die Förderung und den Schutz des Rechts auf Meinungsfreiheit und freie Meinungsäußerung Frank William La Rue bereits im Jahr 2013 empfohlen, die Kommunikations-, Daten- und Informationsflüsse zu überprüfen. Es solle untersucht werden, inwiefern diese nicht nur Freiheit einschränken, sondern auch die Grundwerte einer demokratischen Gesellschaft angreifen. Allerdings sollten nur unabhängige, durch die UN initiierte Überprüfungsmechanismen darüber befinden.[12]

Schülerinnen und Schüler der Rhodes Park School in Lusaka, Sambia, bereiten im Computerlabor im Rahmen eines Projekts des Insitute for International Cooperation and Development (IICD) einen Lernzirkel vor. Foto: IICD/flickr.com

Chancen für die Menschenrechte

Am Ende überrascht es wenig, dass die UN-Generalversammlung das Internet kurz nach der Verabschiedung der 17 SDGs im September 2015 als Wegbereiter für deren Verwirklichung benannt hat. Ob Bildung, Armutsbekämpfung, Gesundheit, Frieden und Gerechtigkeit, Bekämpfung des Klimawandels oder der Geschlechterungleichheit: Ohne Zugang zum Internet sind diese Ziele nicht zu verwirklichen. In Resolution 70/125 wird deshalb der Multistakeholder-Prozess als Chance für einen holistischen, auf Menschenrechten basierenden Weg zur Umsetzung der SDGs gesehen. Der Entscheidungs- und Umsetzungsprozess soll ermöglichen, dass sowohl Frauen als auch Männer gleichen und neutralen Zugang zum Internet haben. Bislang sind nur knapp 40 Prozent aller Internetnutzer Frauen. Zudem sollen entsprechend Resolution 70/125 in den nächsten Jahren mindestens zwei Milliarden Menschen erstmalig Zugang erhalten, vor allem in den Entwicklungsländern. Erst dann hätten die SDGs eine reelle Chance, ansatzweise bis zum Jahr 2030 realisiert zu werden.

Dies ist jedoch nur in Zusammenarbeit mit internationalen, nationalen, lokalen und privaten oder zivilgesellschaftlichen Akteuren über das Internet möglich. Nur im ›cyberalen‹ Raum können alle ihr Menschenrecht auf Informationszugang, freie Meinungsäußerung und Teilhabe an gesellschaftlichen Prozessen als Schlüssel für ihre berufliche Entwicklung, zur Teilhabe an wissenschaftlichem Fortschritt, zur Bildung, zur Gesundheit und gesunder Umwelt, zum Ausleben ihrer Kultur oder zur Geschlechterneutralität nutzen. Das Völkergewohnheitsrecht kann die Grundlage sein, diese globalen Werte und Normen auch in jene Länder zu übermitteln, die internationale Menschenrechtsverträge nicht ratifiziert haben. Ein neutrales Internet, wie es die Teilnehmenden des IGF im November 2015 in Brasilien gefordert haben, ist dabei nur die technische Voraussetzung, die jedoch von staatlichen Behörden allein nicht gewährleistet werden kann.[13]

Alle Akteure sind laut Generalversammlung verpflichtet, nicht nur in ihren eigenen Ländern, sondern auch in von Krieg, Gewalt, Armut und Naturkatastrophen gebeutelten Ländern in ein neutrales Internet zu investieren. So wie einst der Straßen-, Hafen- oder Schienenbau der Schlüssel zum Wiederaufbau oder zur Entwicklung einer Gesellschaft war, ist es heute die freie, neutrale und allen zugängliche ›Datenautobahn‹. Unternehmen wie Microsoft oder

5 Ronald J. Deibert/Masashi Crete-Nishihata, Global Governance and the Spread of Cyberspace Controls, Global Governance, 18/2012, S. 339–361.

6 Vgl. Dokumentation zum Workshop on ›Human Rights in Cyberspace‹ des NATO Cooperative Cyber Defence Centre of Excellence unter www.ccdcoe.org/workshop-human-rights-cyberspace.html

7 Tim Maurer, Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cybersecurity, Discussion Paper #2011–11, Belfer Center for Science and International Affairs Harvard Kennedy School, www.belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf

8 Vgl. UN-Dok. A/RES/68/167 v. 18.12.2013.

9 Zu den rechtlichen Rahmenbedingungen: Tatiana Tropina/Nicolas von zur Mühlen, in diesem Heft: S. 56–60.

10 Jaqueline Lipton, Rethinking Cyberlaw. A New Vision for Internet Law, Cheltenham 2015.

11 Wolff Heintschel von Heinegg, Legal Implications of Territorial Sovereignty in Cyberspace, in: Christian Czosseck/Rain Ottis/Katharina Ziolkowski (Eds.), 4th International Conference on Cyber Conflict, Tallinn 2012, S. 7–13, www.ccdcoe.org/publications/2012proceedings/CyCon_2012_Proceedings.pdf

12 UN Doc. A/HRC/23/40 v. 17.4.2013.

13 Siehe dazu Internet Governance Forum, The 10th Internet Governance Forum (IGF), Chair's Summary, 10.–13. November 2015, João Pessoa, Brasilien, www.intgovforum.org/cms/10th%20IGF%20Chairs%20Summary_Finalv2.pdf

Google können nicht mehr frei entscheiden, ob sie in ein Land investieren oder ihre Dienstleistung anbieten wollen, sondern sind quasi dazu verpflichtet, zu investieren und am Gemeinwohl orientiert zu handeln. Gleichzeitig wird im letzten Abschnitt der Resolution 70/125 beim Thema Internet Governance davon ausgegangen, dass selbst autokratische Regime sich dem Multistakeholder-Ansatz öffnen und damit zumindest minimale Good-Governance-Standards umsetzen. Denn um Datenfreiheit und Datenschutz in Zukunft zu garantieren, braucht es ein Mindestmaß an Transparenz, Rechenschaftslegung und Partizipation durch und mit privaten und staatlichen Akteuren.

Es geht um das Thema, wie viel Schutz, Zugang oder Begrenzung von Freiheit für eine Gesellschaft gut sind und wann unter dem Vorwand ›Sicherheit‹ die freie Entwicklung eingeschränkt wird.

Unternehmen wie Microsoft und SAP, Anbieter wie Google und Yandex sowie soziale Netzwerke wie Facebook, Renren in China oder d1g.com in den arabischen Ländern sollten überall verfügbar beziehungsweise frei zugänglich sein. Neutral bedeutet auch, dass jeder Mensch gleichen und freien Zugang zu Informationen und Kommunikation erhält, der für seine Entwicklung notwendig ist. Zusatzangebote sollen über das Mindestangebot hinaus den Unternehmen ihren Profit garantieren. Der ungehinderte Zugang in Landes- und Minderheitensprachen sowie ein ortsunabhängiger Zugang mit allen Endgeräten gehören ebenfalls dazu. Freier und kostenloser Zugang zu den neusten Anbaumethoden von Getreide in Afrika südlich der Sahara in lokalen Dialekten ist dabei ebenso wichtig wie freier Zugang für Jugendliche zu Informationen und Bildungsangeboten, ohne dabei permanenter Werbung und Manipulation ausgesetzt zu sein. Gerade beim Kampf gegen die rasante Klimaveränderung und ihre dramatischen Folgen kann ein neutrales, politik-, religions- und kommerziell unabhängiges Internet viel bewirken.

Ob bei der Bekämpfung und Aufklärung von Ebola in Westafrika oder dem Zika-Virus in Lateinamerika: Das Internet ist auch beim Recht auf Gesundheit nicht mehr wegzudenken. Junge Menschen erhalten über das Internet Chancen auf Bildung und Ausbildung, die sie sich offline niemals hätten leisten können. Dabei setzen Anbieter nicht mehr auf Computer als Zugangstechnik, sondern auf Smartphones mit Satelliten- oder gar drohnengesteuertem Zugang zum Internet.

Es gibt keine Notwendigkeit für eine eigene digitale Menschenrechtscharta. Vielmehr gilt es, ein effizienteres Internet-Governance-Regime aufzubauen.

Der Austausch zwischen Kulturen kann zu mehr Frieden beitragen. Gleichzeitig erhalten jedoch auch autoritäre Regierungen, radikale und religiöse Hassparteien Zugang zu den Nutzerinnen und Nutzern und können diese beeinflussen. Es geht immer um das Thema, wie viel Schutz, Zugang oder Begrenzung von Freiheit für eine Gesellschaft gut sind und wann unter dem Vorwand ›Sicherheit‹ die freie Entwicklung eingeschränkt wird. Diese Diskussion ist so alt wie die Idee der Menschenrechte selbst und nicht allein auf das Internet beschränkt. Sie wird im Cyberraum allerdings stärker geführt, da es hier (noch) kein Steuerungs- und Sanktionssystem gibt. Die Kommunikation im Internet ist oft anonym, was nicht nur die vielbeschriebenen Risiken, sondern auch Chancen birgt. Mehr Frauen, Mädchen und Angehörige von marginalisierten Gruppen beteiligen sich an politischen Debatten im Internet. Es bietet denjenigen Zugang, die sich aufgrund gesellschaftlicher Zwänge und Diskriminierung bislang nicht trauten, sich am politischen Prozess zu beteiligen. Die Frauenbewegungen in Saudi-Arabien, die Blogger-Bewegung in Bangladesch oder die Aktivisten des ›Arabischen Frühlings‹ und die Indio-Bewegung ›Amazonas Watch‹ sind ohne den freien Zugang zum Internet nicht denkbar. Menschen mit Behinderung erhalten Zugang zur beruflichen und politischen Teilhabe, ohne dass dabei alltägliche Hemmnisse ein Hindernis darstellen. Angehörige von ethnischen oder religiösen Minderheiten mischen sich in politische Debatten ein, um ihr Land, ihre Kultur und ihre Ressourcen zu schützen, und sie profitieren von der internationalen Solidarität.

Es gibt daher keine Notwendigkeit für eine eigene digitale Menschenrechtscharta, wie noch vor wenigen Jahren diskutiert. Vielmehr gilt es, ein effizienteres Internet-Governance-Regime aufzubauen. Dabei einigen sich private, öffentliche oder internationale Akteure gemeinsam auf Kriterien, denen entsprechend sie einen Teil des Cyberraums ›besiedeln‹ und ihre Rollen und Verantwortlichkeiten festlegen. Bei Nichteinhaltung drohen selbst auferlegte Sanktionen – erst dann kann der Multistakeholder-Ansatz funktionieren. Bislang ist jedoch offen, wer festlegt, welche Akteure sich in welcher Weise an diesem Aushandlungsprozess beteiligen.

Negative Auswirkungen des Internets auf die Menschenrechte

Vor allem der Schutz der Privatsphäre und privater Daten ist ein Kernanliegen von Internet Governance. Der Missbrauch oder Diebstahl von privaten Gesundheits- und Kreditkartendaten oder Cybermobbing führten bereits in vielen Fällen zum existenziellen Ruin einzelner Nutzer und nicht selten zu Todesfällen, ohne dass die Täter erkannt oder verurteilt werden konnten. Privatsphäre ist jener persönliche Raum, in dem wir unsere Persönlichkeit selbstbewusst und frei entwickeln und unsere Fähigkeiten und Möglichkeiten ausschöpfen, unsere Gesundheit erhalten sowie soziale Beziehungen mit Familie und Freunden ohne Einfluss von außen unterhalten können.[14] Daher bedeutet Privatsphäre im Cyberraum, das Internet als Werkzeug für private Zwecke zu verwenden, ohne zu fürchten, dass Dritte ohne Zustimmung auf unsere Daten zugreifen, sie verkaufen oder öffentlich machen. Hier wird deutlich, warum die UN-Generalversammlung den Multistakeholder-Ansatz

so hoch bewertet, denn private Unternehmen sind häufig die einzigen Akteure, die Daten von potenziellen Tätern zugänglich machen können. Gleichzeitig haben Regierungen die Sorge, ihren Einfluss auf Unternehmen zu verlieren, da diese sich im Cyberraum zunehmend staatlicher Kontrolle entziehen.

Freiheits- und Persönlichkeitsrechte im Internet sind beim Datenschutz, bei der Cybersicherheit, der Cyberüberwachung oder dem Cyberkrieg durch Cyberviren besonders zu schützen. Staatliche und nichtstaatliche Akteure sind an dieser Kriminalität im Internet gleichermaßen beteiligt. Gesetzesvorhaben wie der amerikanische ›Stop Online Piracy Act‹ (SOPA) beziehungsweise der PROTECT IP Act, das amerikanische Überwachungsprojekt PRISM oder das multilaterale Handelsübereinkommen zur Bekämpfung von Produkt- und Markenpiraterie (Anti-Counterfeiting Trade Agreement – ACTA) gehören zu den unzähligen verzweifelten Versuchen, die staatliche Kontrolle über den grenzenlosen Datenfluss wiederzuerlangen. Es ist ein Wettlauf gegen die Zeit, den staatliche Stellen allein nicht gewinnen können.

Andere Grundfreiheiten und Menschenrechte, die in diesem Zusammenhang behandelt werden, sind der freie Ausdruck des Glaubens, der politischen Meinung, von Forschungsdaten, geistigem Eigentum, der freie und gleichberechtigte Zugang zu Informationen und der Schutz der Privatsphäre. Darüber hinaus geht es um den Schutz und die Sicherheit, frei von Belästigung und Verfolgung im Internet zu agieren. Geistiges Eigentum und Kreativität müssen geschützt werden, gleichzeitig jedoch der Gemeinschaft im Sinne ihrer Entwicklung in angemessener Weise zugeführt werden.[15] Oberstes Prinzip dabei ist, dass die veröffentlichten Mitteilungen und Informationen die Menschenrechte anderer nicht verletzen. Dies ist Abwägungssache und bis dato lag die Entscheidung darüber allein in der Hand nationaler oder internationaler Gerichte.

Das oft proklamierte ›Recht auf Internet‹, das den Privatpersonen jederzeit den Zugang zum Internet ermöglichen soll, und das ›Recht auf Vergessen‹, das sicherstellt, dass private Daten privat bleiben und jederzeit gelöscht werden können, sind inzwischen Bestandteil von Internet Governance geworden, ohne dass es einer eigenen Internetcharta oder Ähnlichem bedurfte. Der Gerichtshof der Europäischen Union (EuGH) hat im Mai 2014 eine Grundsatzentscheidung getroffen, die diesen Ansatz untermauert.[16] Allerdings gilt die Entscheidung nur für die EU und eine globale Lösung steht noch aus. Dies gilt auch für die Entscheidung des EuGH aus dem Jahr 2015 zum Thema ›sicherer Hafen‹ für Datenübermittlung in die USA.[17] Dies sind Präzedenzfälle, auf die sich zukünftige Rechtsprechungen berufen werden. Grundsätzlich geht es bei all diesen Entscheidungen um die anteilige Verantwortung verschiedener Akteure, Staaten, Unternehmen sowie Nutzerinnen und Nutzer beim Schutz der Daten im Internet.

Im Jahr 2011 hat die Forschungsabteilung des Europäischen Gerichtshofs für Menschenrechte bereits eine klare Richtung vorgegeben, indem sie dem Datenschutz eine prinzipielle Vorrangstellung einräumte.[18] Es hängt viel davon ab, wer über die Grenzen der Informationsfreiheit entscheidet. Je mehr diese Akteure im Sinne des Multistakeholder-Ansatzes in Zukunft am Aushandeln dieser Rechtsgrundsätze beteiligt sind, desto wahrscheinlicher wird dieses Ergebnis von den Nutzern angenommen.

Nach Bekanntwerden vieler Fälle von Cyberspionage und Internetkriminalität im Jahr 2013 betonte der damalige UN-Sonderberichterstatter über die Förderung und den Schutz des Rechts auf Meinungsfreiheit und freie Meinungsäußerung, dass Datenschutz und Meinungsfreiheit miteinander verknüpft seien. Ohne ausreichende Gesetzgebung und Rechtsnormen zur Gewährleistung der Privatsphäre können Sicherheit und Anonymität der Kommunikation für Journalistinnen und Journalisten, Menschenrechtsaktivisten und Whistleblower nicht gewährleistet werden.[19] Dass Regierungen Verfahren gegen den Whistleblower Edward Snowden, den Wikileaks-Gründer Julian Assange oder gegen die Plattform netzpolitik.org eingeleitet haben, war eine Bankrotterklärung der nationalen Sicherheitsapparate und Rechtsysteme, die allesamt mit ihrer neuen Rolle im Multistakeholder-System überfordert sind.

Das ›Recht auf Internet‹ und das ›Recht auf Vergessen‹ sind Bestandteil von Internet Governance geworden.

Ausblick

Die rund 3,5 Milliarden Nutzerinnen und Nutzer des Cyberraums machen die Hälfte der Weltbevölkerung aus. Der Cyberraum ist ein grenzenloser öffentlicher Raum ohne Regierung, in dem Menschen, unabhängig von ihrer Staatsbürgerschaft, ethnischen Herkunft, politischen Orientierung, ihrem Geschlecht oder sonstigem Hintergrund kommunizieren und interagieren. Dies erinnert fast schon an ein ›Failed state‹-Szenario. Gleichzeitig ist die

14 Anja Mihr, Good Cyber Governance. The Human Rights and Multi-Stakeholder Approach, in: Georgetown Journal of International Affairs, 2014, S. 24–34.

15 Vgl. Marcia V.J. Kran/Geraldine Fraser-Moleketi, Global Consultation on Governance and the Post-2015 Framework: Concept Note, 7.10.2012, www.worldwewant2015.org/node/277876

16 Urteil des EuGH, C-131/12, 13.5.2014.

17 Urteil des EuGH, ECLI:EU:C:2015:650, 6.10.2015.

18 Declaration by the Committee of Ministers on Internet Governance Principles, Adopted by the Committee of Ministers on 21 September 2011.

19 Heintschel von Heinegg, a.a.O (Anm. 11).

Drei Fragen an **Thomas Fitschen**

Was sind die wichtigsten Themenfelder der Cyber-Außenpolitik der Bundesregierung und wo finden sich die Vereinten Nationen in der digitalen Agenda?

Die deutsche Cyber-Außenpolitik hat drei Kernziele: Erstens wollen wir erreichen, dass die wirtschaftlichen Chancen der Digitalisierung in Deutschland und in weniger entwickelten Teilen der Welt genutzt werden. Zweitens setzen wir uns dafür ein, dass die Menschenrechte online wie offline geschützt werden. Hierzu zählt unser Engagement zum Schutz der Privatsphäre. Dies ist nur möglich, wenn wir – drittens – gemeinsame Lösungen für neue Bedrohungen finden. Vertrauensbildung und die Stärkung des Völkerrechts sind die entscheidenden Stichworte. Unsere Aktivitäten in den UN, in der Europäischen Union und in Organisationen wie der OSZE spiegeln sich in der ›Digitalen Agenda‹ wider. Für Deutschland ist besonders wichtig, dass die Kontrolle über das Internet dem Multistakeholder-Prinzip folgt. Wir müssen sicherstellen, dass das Netz offen und nicht fragmentiert bleibt. Auch die ›digitale Spaltung‹ zwischen den Industrie- und Entwicklungsländern muss beseitigt werden. Das ist auch der Auftrag der Überprüfungskonferenz WSIS+10 im Dezember 2015.

Deutschland hat mit Brasilien bei den Vereinten Nationen Initiativen zum Schutz der Menschenrechte im Cyberraum eingebracht. Was wurde erreicht?

Im Jahr 2013 haben Deutschland und Brasilien eine Initiative zum Schutz der Privatsphäre im digitalen Zeitalter in der Generalversammlung gestartet. In einer im Dezember 2014 verabschiedeten Resolution stellte die Generalversammlung fest, dass die (Menschen-)Rechte, die alle im täglichen Leben haben, auch online geschützt werden müssen. Das klingt ganz einfach, aber in den Jahren zuvor hätten längst nicht alle Staaten dieser Aussage zugestimmt. Auch bei den Beschlüssen des Menschenrechtsrats, die im Jahr 2015 zur Einsetzung eines Sonderberichterstatters über das Recht auf Privatheit führten, waren unsere beiden Länder die treibenden Kräfte. Wir haben die entsprechenden Entscheidungen vorbereitet und in mehreren Paneldiskussionen in Genf und New York auch den Austausch mit Wissenschaft und Zivilgesellschaft ermöglicht. Uns war klar, dass das Thema politisch sensibel ist. Aber in langen Verhandlungen konnten wir erreichen, dass am Ende alle Staaten zustimmten.

Die Bundesregierung möchte ein ›Völkerrecht des Netzes‹ definieren. Welche Rolle spielen die Vereinten Nationen?

Die Vereinten Nationen sind der wichtigste Ort für den Dialog über diese Frage. Die Generalversammlung hat bereits mehrere Gruppen von Regierungssachverständigen eingesetzt, die eine Bestandsaufnahme machen und den Staaten Empfehlungen unterbreiten sollten. In diese Gruppe hat der UN-Generalsekretär auch einen deutschen Experten aus dem Cyber-Koordinierungsstab des Auswärtigen Amtes berufen. Nach schwierigen Anfangsjahren kam die Gruppe im Jahr 2015 zu dem Schluss, dass die Normen des Völkerrechts auch im Cyberraum gelten, und machte Vorschläge für Grundregeln verantwortlichen Verhaltens von Staaten sowie für Maßnahmen zur Vertrauensbildung. Auch dies war nicht selbstverständlich und setzt dem zwischenstaatlichen ›Verkehr‹ im Netz wichtige Leitplanken.

Dr. Thomas Fitschen, geb. 1959, ist seit 2015 der Beauftragte im Auswärtigen Amt für die Vereinten Nationen, Cyber-Außenpolitik und Terrorismusbekämpfung.

›Internetgemeinde‹ die am schnellsten wachsende Bevölkerungsgruppe in der Geschichte der Menschheit in einem fast anarchischen Cyberraum. Internet Governance ist daher zu Recht als Weg aus dem Dilemma erkannt worden, jedoch steckt sie noch in den Kinderschuhen.

Die Internetnutzer, von denen zwei Drittel in sogenannten entwickelten Ländern leben, erledigen im Cyberraum ihre täglichen Geschäfte, tauschen Wissen, organisieren Kampagnen und ihr Privatleben. Dies alles ohne gemeinsame grenzüberschreitende Regeln, Gesetze, Regierung, Durchsetzungs- oder Kontrollmechanismen, Gerichte oder Polizei, die die Aktivitäten der Menschen in diesem Bereich schützen könnten.

Beachtlich scheint es, dass es eine Staatenallianz aus den Vereinigten Arabischen Emiraten (VAE) und Lettland war, die den Multistakeholder-Prozess bislang vorantrieb. Demokratieschwache Länder wie die VAE, Pakistan, China oder Nigeria, in denen es keine freie Zivilgesellschaft, jedoch eine schnell wachsende junge Internetgemeinde gibt, die alle bisherigen Normen der Gesellschaft in Frage stellt, setzen sich für einen Multistakeholder-Ansatz ein, um diesen kontrollieren zu können. Dies kann als ein Zugeständnis gewertet werden. Allerdings ist fraglich, ob die Staatenvertreter im Dezember 2015 wirklich einen Multistakeholder-Ansatz im Sinne des Begriffs vor Augen hatten oder nicht eher einen staatenzentrierten Ansatz, bei dem lediglich die eine oder andere Internetfirma zurate gezogen werden kann, wann immer es öffentlichkeitswirksam wäre.

Allen Bemühungen zum Trotz, die *terra incognita* Cyberraum zivilisiert zu ›besiedeln‹ und diesem Raum einheitliche Regeln und Vorschriften zu geben, steht Internet Governance noch am Anfang. Das Internet- oder Cyberregime ist allerdings neben dem Klimaregime das am schnellsten wachsende globale Regime. Es ist gerade einmal 20 Jahre her, dass John Perry Barlow im Jahr 1996 die erste ›Unabhängigkeitserklärung des Cyberspace‹ veröffentlichte.[20] In dieser Erklärung wies er bereits auf die Gefahren hin, über die wir uns heute weltweit Sorgen machen. Barlow war sich sicher, dass die Internetgemeinde ihre eigenen Gesellschaftsverträge entwickeln werde, um zu bestimmen, wie sie mit den Problemen umgehen solle. Für ihn stand dabei allerdings stets fest, dass die Problemlösung auf Grundlage der Menschenrechte gefunden werden müsse. Er sollte Recht behalten.

20 John Perry Barlow, A Declaration of the Independence of Cyberspace, Davos 1996, www.eff.org/cyberspace-independence

Wer regiert das Internet?

Internet Governance auf dem Prüfstand

Wolfgang Kleinwächter

Der Cyberraum mit rund 3,2 Milliarden Internetnutzerinnen und -nutzern ist in den letzten Jahren zunehmend zu einem Feld politischer Kontroversen geworden. Dabei stehen sich zwei Konzepte gegenüber: Auf der einen Seite wollen einige Regierungen Fragen das Internet betreffend in einem multilateralen völkerrechtlichen Vertrag regeln. Auf der anderen Seite steht das Konzept des Multistakeholderismus. Diesem entsprechend hat sich, der Vielschichtigkeit des ›Ökosystems Internet Governance‹ folgend, ein dezentraler Mechanismus entwickelt, an dem staatliche und nichtstaatliche Akteure auf verschiedenen Ebenen für unterschiedliche Themen zuständig sind. Das im Jahr 2005 gegründete Internet Governance Forum (IGF) ist die wichtigste globale Plattform für diese Diskussion. Das Mandat des IGFs wurde im Dezember 2015 von der UN-Generalversammlung bis zum Jahr 2025 verlängert.

Seit knapp zwei Jahrzehnten ist das Thema ›Internet Governance‹ Gegenstand heftiger politischer Kontroversen. Das Internet entwickelte sich in den siebziger und achtziger Jahren im Schatten staatlicher Regulierung und zwischenstaatlicher Verhandlungen. Zunächst finanziert vom amerikanischen Verteidigungsministerium entstand es als ein grenzüberschreitendes privatwirtschaftlich organisiertes ›Netz von Netzwerken‹. In der Diskussion um die ›Neue Weltinformations- und Kommunikationsordnung‹ (NWIKO), die die Diplomatie der Vereinten Nationen der achtziger Jahre – vor allem in der Organisation der Vereinten Nationen für Erziehung, Wissenschaft und Kultur (United Nations Educational, Scientific and Cultural Organization – UNESCO) – prägte, spielte das Internet keine Rolle.

Der Begriff ›Internet Governance‹ wurde in den frühen neunziger Jahren im Rahmen der Initiative für eine Informationsinfrastruktur (National Information Infrastructure – NII) der Regierung unter Bill Clinton zur Beschreibung der primär technischen Selbstregulierungsmechanismen des Internets eingeführt. Ein Schlagwort der Zeit war ›Governance without Governments‹. Ergebnis dieser Diskussion war die Gründung der Organisation für die Vergabe von Internetdomainnamen (Internet Corporation for Assigned Names and Numbers – ICANN) im Jahr 1998. Regierungen sind bei der ICANN beratend eingebunden. Empfehlungen des ›Governmental Advisory Committee‹ (GAC), dem mittlerweile 150 Regierungen angehören, sind für das ICANN-Direktorium nicht bindend.[1]

UN-Weltgipfel zur Informationsgesellschaft

Die politische Diskussion zu Internet Governance begann erst im Jahr 2002 mit dem Weltgipfel über die Informationsgesellschaft (World Summit on the Information Society – WSIS).[2] Eine Vielzahl von Staaten, allen voran China und Russland, forderte die Schaffung einer zwischenstaatlichen Regierungsaufsicht über das Internet im Rahmen der Vereinten Nationen. Dies stieß auf viel Opposition und man konnte sich beim ersten Gipfeltreffen im Dezember 2003 in Genf nicht einmal auf eine Definition von Internet Governance einigen.

Die im Jahr 2004 eingesetzte Arbeitsgruppe Internet-Verwaltung (Working Group on Internet Governance – WGIG) kam zu dem Schluss, dass das Internet zu komplex sei, um von einer Organisation allein verwaltet zu werden. Die vorgeschlagene Definition, die beim zweiten WSIS-Gipfel im Jahr 2005 in Tunis von den 191 UN-Mitgliedstaaten akzeptiert wurde, geht von einem dezentralen Multistakeholder-Modell aus, bei dem alle Akteure eingebunden sind. Entscheidungen sollen weitgehend im Konsens zwischen allen Betroffenen und Beteiligten (shared decision making procedures) getroffen werden.[3]

Die Definition differenziert zwischen der Entwicklung des Internets im engeren (technischen) Sinne und der Nutzung des Internets im weiteren (politischen) Sinne. In Tunis wurde das Internet Governance Forum (IGF) gegründet. Die Funktion des IGF besteht darin, die komplexen Querschnittsprobleme des Internets aus der Perspektive aller Akteure zu diskutieren, um Entscheidungsträger zu befähigen, vernünftige Beschlüsse zu fassen. Das IGF selbst hat kein Verhandlungsmandat.[4]

Wolfgang Kleinwächter, geb. 1947, ist Professor für Internetpolitik und -regulierung an der Universität Aarhus, Mitglied des ICANN-Direktoriums und Sonderbotschafter der NETMundial-Initiative (NMI).

1 Siehe Statuten der ICANN, 24. Juni 2011, www.icann.org/resources/pages/bylaws-2012-02-25-de

2 Siehe zur Vorgeschichte und Entwicklung des WSIS-Gipfels: Wolfgang Kleinwächter, Globalisierung und Cyberspace. Der Weltgipfel über die Informationsgesellschaft weist den Weg, VN, 1–2/2006, S. 38–44.

3 Report of the UN WGIG, Château de Bossey, 25. Juli 2005, www.wgig.org/WGIG-Report.html; William J. Drake (Ed.), The Working Group on Internet Governance: 10th anniversary reflections, 2015, www.apc.org/en/system/files/IG_10_Final.pdf

4 Siehe Tunis-Agenda für die Informationsgesellschaft, 18.11.2015, www.un.org/depts/german/conf/wsis-05-tunis-doc-6rev1.pdf

Was macht die ICANN?

Die Internet Corporation for Assigned Names and Numbers (ICANN) ist eine internationale Organisation, die als gelungenes Beispiel für die Praxistauglichkeit und den Erfolg des Multistakeholder-Ansatzes gilt. Sie koordiniert die Aufgaben der Internet Assigned Numbers Authority (IANA) und ist für die Verwaltung und Verteilung von IP-Adressen zuständig. Internetnutzerinnen und -nutzer benötigen diese Adresse, um über das Netz miteinander Kontakt aufnehmen zu können. Sie entscheidet zudem über die Einführung neuer Top-Level-Domains (etwa .de, .org, .berlin). Am 14. März 2014 gab die amerikanische Handelskammer bekannt, dass die IANA endgültig an die Multistakeholder-Gemeinschaft unter Leitung der ICANN übergeben werden soll. Zur Umsetzung wurde von der ICANN eine Koordinierungsgruppe eingesetzt, deren Vorschlag bei der 55. ICANN-Tagung im März 2016 verabschiedet wurde.

Dieser mehrstufige und flexible Mechanismus hat sich seither bewährt, zumal innerhalb der letzten zehn Jahre das sogenannte ›Ökosystem Internet Governance‹ erheblich gewachsen ist. Dieses System wird immer wieder mit dem Regenwald verglichen.[5] Im Regenwald leben Hunderte von Spezies zusammen, die alle voneinander abhängig sind. Niemand kann den Regenwald als Ganzes kontrollieren oder beherrschen. Unverantwortliches Verhalten kann jedoch Teile des Regenwalds zerstören und alle leiden an den Folgen.

In den letzten Jahren ist es immer wieder zu einer Konfrontation zwischen Regierungen gekommen, die einen rein staatlichen Regulierungsmechanismus bevorzugen, und Regierungen, die auf eine Weiterentwicklung des Multistakeholder-Prinzips setzen.

Im ›Ökosystem Internet Governance‹ koexistieren gleichfalls Hunderte von Mechanismen – teils staatlich, teils nichtstaatlich, teils fremdreguliert, teils selbstreguliert – die einerseits selbstständig operieren, andererseits abhängig vom Funktionieren anderer Akteure sind. Ein solcher ›Multilayer-Multiplayer-Mechanismus‹ fordert ein hohes Maß an gegenseitigem Verständnis und Rücksichtnahme sowie eine verbesserte Kommunikation, Koordination und Zusammenarbeit (enhanced cooperation) sowohl innerhalb als auch zwischen den einzelnen Akteursgruppen auf globaler, regionaler und nationaler Ebene. Das Internet verdankt seine Dynamik dem Grundsatz der ›zulassungsfreien Innovation‹ (innovation without permission). Dabei kommt dem sogenannten ›Do no harm‹-Prinzip – der Vermeidung von unbeabsichtigten Negativeffekten für unbeteiligte Parteien – eine zentraler Bedeutung zu. Auch hier ist das enge Zusammenwirken staatlicher und nichtstaatlicher Akteure essentiell.

Die zur Lösung von internetbasierten politischen, wirtschaftlichen, kulturellen, sozialen und rechtlichen Problemen benötigten Diskussionsinstrumente und Verhandlungsebenen gehen insofern weit über die traditionellen diplomatischen Mechanismen hinaus, wie sie beispielsweise das System der Vereinten Nationen zur Verfügung stellt. Insofern war es logisch, dass das zunächst skeptisch betrachtete IGF zunehmend Unterstützung bekam und bald regionale und nationale IGFs folgten. Das bedeutet auf der anderen Seite nicht, dass die bestehenden Möglichkeiten des UN-Systems für das Internet irrelevant sind. Gerade die letzten Jahre haben gezeigt, dass sowohl die UN-Generalversammlung und ihre Ausschüsse als auch die UN-Sonderorganisationen sehr gute sachbezogene Beiträge zur Beantwortung von Internet Governance-Fragen leisten können.

Bei der ersten Sitzung der WGIG im Jahr 2004 in New York hatte der damalige UN-Generalsekretär Kofi Annan gefordert, Innovationen nicht den Technikern zu überlassen, sondern auch im politischen Bereich innovativ zu handeln.[6] Das Multistakeholder-Modell, das sich seit mehr als zehn Jahren als Grundlage für Internet Governance etabliert hat, ist eine solche politische Innovation.

Es gibt jedoch nicht wenige Regierungen, die diesem Modell mit großem Misstrauen begegnen. Sie sehen in der dem Modell innewohnenden Pflicht zur gleichberechtigten Zusammenarbeit mit nichtstaatlichen Akteuren, die letztlich in einer Aufteilung von Entscheidungsmacht mündet, einen Verlust nationaler Souveränitätsrechte. Die wachsende Komplexität des ›Ökosystems Internet Governance‹ ist allerdings eine Tatsache, an der niemand vorbeikommt. Eine primär an nationalen Interessen orientierte Internetpolitik trägt das Risiko einer Fragmentierung des Internets in sich – mit negativen Folgen für Innovation, Wachstum, Schaffung von Arbeitsplätzen, kulturelle und soziale Entwicklung sowie die individuellen Menschenrechte.

Multilateralismus versus Multistakeholderismus

Trotzdem ist es in den letzten Jahren im Rahmen der Vereinten Nationen immer wieder zu einer Konfrontation zwischen Regierungen gekommen, die einen rein staatlichen Regulierungsmechanismus in Form von multilateralen Verträgen bevorzugen, und Regierungen, die auf eine Weiterentwicklung des Multistakeholder-Prinzips setzen.

Ein Höhepunkt dieser Auseinandersetzung war die Weltweite Konferenz für internationale Fernmeldedienste (World Conference on International Telecommunications – WCIT) im Dezember 2012 in Dubai. Dort versuchte eine große Gruppe von Staaten das Internet den zwischenstaatlichen Regeln des grenzüberschreitenden Fernmeldeverkehrs zu unterwerfen. Dies wurde von Australien, der Europäischen Union (EU), Japan, den USA und zahlreichen Entwicklungsländern abgelehnt. Die Folge war, dass es zu einer Spaltung kam. Zwar wurde in der endgültigen Fassung der Vollzugsordnung für internationale Fernmeldedienste (International Telecommunication Regulations – ITR) das Internet weitgehend ausgespart, dennoch unterzeichneten nur weniger als die Hälfte der ITU-Mitgliedstaaten die neu-

en ITRs.[7] Auch die Überprüfungskonferenz WSIS+10 im Dezember 2015 drohte an dieser Auseinandersetzung zu scheitern.[8]

Dieser Streit ist kontraproduktiv, da er weniger auf einer sachlichen Basis als auf ideologischen Positionen basiert. Im Grunde genommen gibt es keinen Gegensatz zwischen Multilateralismus und Multistakeholderismus. Es geht vielmehr darum, von Verhandlungen innerhalb einer Akteursgruppe zu Verhandlungen zwischen allen Akteursgruppen zu gelangen. Das Multistakeholder-Prinzip bei Internet Governance steht demnach für einen Prozess des Übergangs von einfachen zu komplexen Verhandlungsstrukturen. Nur so kann man dem ständig an Komplexität gewinnenden Thema Internet Governance gerecht werden. Einfache Modelle – Entscheidungen auf der Basis absoluter Souveränität – stoßen an ihre Grenzen und funktionieren nicht mehr. Die Komplexität des Internets, wo Kategorien von Raum und Zeit keine Rolle spielen, verlangt die Einbeziehung aller betroffenen und beteiligten Gruppen in den Prozess, der immer mehr ›von unten‹ organisiert wird.

Die Entstehung des Multistakeholder-Modells ist insofern das Ergebnis einer natürlichen Entwicklung, die die wachsende Komplexität von modernen Gesellschaften widerspiegelt. Kein Akteur – weder Regierungen noch die Privatwirtschaft – kann heute alleine eine vernünftige Internetpolitik entwickeln. Eigene Interessen kann man nicht mehr mit einfachen Mehrheiten ›durchboxen‹. Dabei verschwinden weder das völkerrechtliche Vertragssystem noch nationale Souveränität und Interessen. Beide sind jedoch mehr denn je in eine Multistakeholder-Umgebung eingebettet und die Ausübung von klassischen Souveränitätsrechten verändert sich.

Dies erfordert weitaus komplexere Mechanismen als die des Politikbetriebs des vergangenen Jahrhunderts. Notwendig ist ein neues Verständnis von globaler Teilhabe, gemeinsamer Wahrnehmung von Verantwortung und kollaborativer Souveränität. Im Internet gibt es keinen Königsweg und keine zentrale Autorität. Lösungen müssen von Fall zu Fall entsprechend der spezifischen Natur des jeweiligen Problems in einem Diskussionsprozess erarbeitet werden, an dem alle Gruppen in einem offenen und transparenten Verfahren gleichberechtigt beteiligt sind.

Internet Governance Makrokosmos 2015: Der Überprüfungsprozess WSIS+10

Auf der globalen Bühne wird Internet Governance heute primär beim Internet Governance Forum thematisiert. Eine wesentliche Rolle spielt auch die UN-Generalversammlung:

- Der Ausschuss für Abrüstung und internationale Sicherheit (Erster Ausschuss) diskutiert internetrelevante Sicherheitsfragen, darunter vertrauensbildende Maßnahmen zur Stärkung der Cybersicherheit. Das wichtigste Untergremium ist eine Gruppe von Regierungssachverständigen (Group of Governmental Experts – GGE), die zuletzt im Juni 2015 einen Bericht vorgelegt hat.[9]
- Der Wirtschafts- und Finanzausschuss (Zweiter Ausschuss) diskutiert die Umsetzung der WSIS-Beschlüsse und ist für das IGF zuständig. Er erhält Unterstützung von der Kommission für Wissenschaft und Technologie im Dienste der Entwicklung (Commission on Science and Technology for Development – CSTD), die jährlich die Fortschritte beim WSIS evaluiert. Die Kommission hat im Jahr 2013 die Arbeitsgruppe zur Untersuchung des in der Tunis-Agenda enthaltenen Mandats des Weltgipfels über die Informationsgesellschaft zur Verstärkung der Zusammenarbeit (Working Group on Enhanced Cooperation – WGEC) eingerichtet.[10]
- Der Ausschuss für soziale, humanitäre und kulturelle Fragen (Dritter Ausschuss) diskutiert die menschenrechtlichen Aspekte, insbesondere die Umsetzung der Rechte auf freie Meinungsäußerung und den Schutz der Privatsphäre.[11] Der UN-Menschenrechtsrat (Human Rights Council – MRR) hat mit der Einsetzung eines Sonderberichterstatters über das Recht auf Privatheit im Jahr 2015 einen konstruktiven Beitrag für den Schutz individueller Menschenrechte geleistet.[12] Die Schaffung dieses Postens geht auf eine deutsch-brasilianische Initiative in der Generalversammlung zurück.[13]

Das Multistakeholder-Prinzip bei Internet Governance steht für einen Prozess des Übergangs von einfachen zu komplexen Verhandlungsstrukturen.

5 Siehe Wolfgang Kleinwächter, Internet Regulierung: So undurchschaubar wie ein Regenwald, Frankfurter Allgemeine Zeitung, 14.8.2015.

6 Siehe Wolfgang Kleinwächter, WSIS, ICANN, GBDe: How Global Governance is Changing in the Information Age, in: Bart De Schutter/Johan Pas (Eds.), About Globalisation: Views of the Trajectory of Mondialisation, Brussels 2004, S. 205–226; Wolfgang Kleinwächter, Multi-Stakeholder Internet Governance, in: Wolfgang Benedek/Veronika Bauer/Matthias C. Kettemann, Internet Governance and the Information Society: Global Perspectives and European Dimensions, Utrecht 2008, S. 20.

7 Siehe International Telecommunication Union, International Telecommunication Regulations, Dubai 2012, www.itu.int/en/wcit-12/Pages/default.aspx

8 UN Doc. A/70/L.33 v. 13.12.2015.

9 UN Doc. A/70/174 v. 22.7.2015.

10 Informationen zur WGEC: www.unctad.org/en/Pages/CSTD/WGEC.aspx

11 Ausführlich zu Menschenrechten im Cyberraum: Anja Mihr, in diesem Heft, S. 61–66.

12 Siehe Wolfgang Kleinwächter, Internet Governance Outlook 2016: Cooperation & Confrontation, CircleID, 11.1.2016, www.circleid.com/posts/20160111_internet_governance_outlook_2016_cooperation_confrontation/

13 UN Doc. A/HRC/27/37 v. 30.6.2014.

Nicht unerheblich sind mittlerweile auch die Aktivitäten anderer UN-Organisationen: Die Internationale Fernmeldeunion (International Telecommunication Union – ITU), die Weltorganisation für geistiges Eigentum (World Intellectual Property Organization – WIPO), die Welthandelsorganisation (World Trade Organization – WTO), die Internationale Arbeitsorganisation (International Labour Organization – ILO) und andere haben angefangen, sich in ihrem jeweiligen Kompetenzbereich tiefgehender mit dem Internet zu befassen. Erst im Januar 2016 hat die Weltbank beim Weltwirtschaftsforum (World Economic Forum – WEF) in Davos einen umfassenden Bericht unter dem Titel ›Digitale Dividenden‹ vorgelegt, der Empfehlungen enthält, wie die nächsten zwei Milliarden Menschen Zugang zum Internet erhalten können.[14] Koordiniert werden die einzelnen Aktivitäten von der Gruppe der Vereinten Nationen für die Informationsgesellschaft (UN Group on the Information Society – UNGIS), einem Gremium, dem mittlerweile fast 30 verschiedene UN-Institutionen angehören.[15]

Die wichtigsten Ereignisse im Jahr 2015 waren die Zehnte Jahrestagung des Internet Governance Forums im brasilianischen João Pessoa im November und die Überprüfungskonferenz WSIS+10 in New York im Dezember. Beide Ereignisse waren miteinander verknüpft. Die UN-Generalversammlung und die Überprüfungskonferenz WSIS+10 mussten über die Verlängerung des IGF-Mandats entscheiden. Wie in den vergangenen Jahren erwies sich das Zehnte IGF als eine gewinnbringende Veranstaltung, bei der alle relevanten Themen in Bezug auf das Internet auf den Tisch kamen und kritisch untersucht wurden. In João Pessoa wurden Themen wie Cybersicherheit und Cyberkrieg, wirtschaftliche Aspekte wie Digitaler Handel und Datenschutz in Handelsverträgen sowie der erweiterte Zugang zum Internet, auch unter komplizierten nationalen wirtschaftlichen Bedingungen (Zero-Rating) bei Wahrung der individuellen Menschenrechte, behandelt. Detailliert diskutiert wurden auch neue technische Entwicklungen wie ›Cloud Computing‹, ›Big Data‹ und das ›Internet der Dinge‹. Selbstverständlich spielte die von der ICANN und der amerikanischen Regierung vorangetriebene Übergabe der Funktionen der IANA eine große Rolle. Rund 3000 Expertinnen und Experten aus aller Welt, die offline und online teilnahmen – darunter viele Regierungsmitglieder, Botschafterinnen und Botschafter, Unternehmensverantwortliche, nichtstaatliche Organisationen (NGOs) und technische Institutionen – verliehen dem Zehnten IGF ein hohes Maß an Kompetenz und Glaubwürdigkeit. Einmal mehr erwies sich das Format als hilfreich für eine ebenso offene wie tiefgründige Diskussion, die nicht durch den Zwang, ein Konsensdokument verhandeln zu müssen, eingeengt wurde.

Trotz der demonstrierten Funktionsfähigkeit des Multistakeholder-Modells beim Zehnten IGF war auch die WSIS+10-Überprüfungskonferenz überschattet von der Auseinandersetzung zwischen Multilateralisten und Multistakeholderisten.

Insofern fiel es der vier Wochen später in New York stattfindenden Überprüfungskonferenz WSIS+10 leichter, grünes Licht für eine Verlängerung des IGF-Mandats zu geben. Das IGF hatte im Jahr 2005 zunächst ein Mandat für fünf Jahre erhalten. Im Jahr 2010 war es um weitere fünf Jahre verlängert worden. Nun hat die UN-Generalversammlung entschieden, das IGF bis ins Jahr 2025 fortzuführen. Es erhielt gleichzeitig den Auftrag, die Prozesse weiterzuentwickeln und mehr ›greifbaren Output‹ zu produzieren. Trotz der demonstrierten Funktionsfähigkeit des Multistakeholder-Modells beim Zehnten IGF war auch die WSIS+10-Überprüfungskonferenz überschattet von der Auseinandersetzung zwischen Multilateralisten und Multistakeholderisten. Am Schluss wurde ein vernünftiger Kompromiss gefunden, indem beide Begriffe gleichberechtigt im Abschlussdokument zu WSIS+10 erscheinen.[16]

Ein weiteres wichtiges und kontroverses Thema war die Cybersicherheit. Die Anzahl von Cyberattacken hat auch im Jahr 2015 zugenommen. Cyberkriminalität, Cyberterrorismus, ja Cyberkrieg, ist zum Vokabular politischer Streitigkeiten geworden. Bei den Vereinten Nationen beschäftigt sich die GGE im Rahmen des Ersten Ausschusses der Generalversammlung mit diesem Thema. Auch dort stehen sich zwei Gruppen gegenüber. Die Mitglieder der Shanghaier Organisation für Zusammenarbeit (Shanghai Cooperation Organisation – SCO), der unter anderem China und Russland angehören, fordern seit Jahren die Ausarbeitung eines Übereinkommens zur Stärkung der Sicherheit im Cyberraum. Die USA und die EU lehnen jedoch ein neues völkerrechtliches Instrument ab, da sie befürchten, dass ein solcher Vertrag zu Einschränkungen und Zensur führen könnte. Sie laden Brasilien, China, Indien, Russland und andere Staaten ein, dem Übereinkommen über Computerkriminalität des Europarats aus dem Jahr 2001 beizutreten. Diese lehnen bisher ab, da sie bei der Ausarbeitung des Übereinkommens nicht beteiligt gewesen seien und ihnen einige Klauseln nicht gefielen. Immerhin konnte man sich in der GGE auf einige vertrauensbildende Maßnahmen einigen: Dazu gehören der Austausch von nationalen Strategien zur Cybersicherheit, die Zusammenarbeit von ›Computer Emergency Response Teams‹ (CERTs) und die Schaffung eines Informationssystems[17] in Anlehnung an das ›Rote Telefon‹, das in den sechziger Jahren zwischen den USA und der Sowjetunion zur Vermeidung eines Nuklearkriegs eingerichtet wurde.[18]

Die Übergabe der Verantwortung für die Funktionen der IANA

Bei der ICANN stand im Jahr 2015 die Übergabe der Funktionen der IANA im Mittelpunkt. Im April 2014 hatte die amerikanische Regierung ange-

kündigt, den Vertrag mit der IANA nicht erneuern zu wollen. Nach der Gründung der ICANN im Jahr 1998 hatte die ›National Telecommunication and Information Administration‹ (NTIA) des amerikanischen Handelsministeriums die Aufsicht über die IANA übernommen. Schon damals hatte die Regierung unter Bill Clinton angekündigt, diese Aufsicht früher oder später der Internetgemeinschaft zu übergeben.

Nachdem die ICANN in den letzten Jahren erfolgreich gewachsen ist, hielt die Regierung unter Barack Obama im Jahr 2014 offensichtlich die Zeit für gekommen, dieses Kapitel abzuschließen, da die Kritik an der Sonderrolle der USA immer wieder geäußert wurde. Direkt nach der Ankündigung der amerikanischen Regierung hatte die ICANN die Weichen für die Übergabe der Funktionen der IANA gestellt und eine Koordinierungsgruppe (IANA Stewardship Transition Coordination Group – ICG) gebildet.[19]

Dabei zeigte sich, dass die Detailfragen komplexer waren als erwartet. Bei den rein technischen Aspekten konnte relativ rasch eine Einigung darüber erzielt werden, dass der Status quo erhalten bleiben solle. Der endgültige Vorschlag, der in Dublin im Oktober 2015 verabschiedet wurde, sieht lediglich vor, dass die ›Post Transition IANA‹ (PTI) als eine selbstständige Unterorganisation der ICANN die Funktionen der IANA übernehmen wird. Die PTI wird dabei von einem ständigen Ausschuss (Customer Standing Committee – CSC) beaufsichtigt und einem regelmäßigen Überprüfungsprozess (IANA Function Review Process – IFR) unterzogen.[20]

Politische Probleme entstanden beim Vorhaben, die Aufsicht durch die amerikanische Regierung durch eine multistakeholder-basierte Aufsicht zu ersetzen. Es galt, einen Mechanismus zu finden, der garantiert, dass eine unabhängige ICANN sich nicht verselbstständigt, Machtmissbrauch ermöglicht oder von einzelnen Interessengruppen eingenommen wird. Zwar war man sich im Grunde einig, dass in einer neuen ICANN eine Art von ›Gewaltenteilung‹ zwischen dem ICANN-Vorstand und der ICANN-Gemeinschaft bestehen müsse. Offen war jedoch, wie Entscheidungsmacht neu verteilt werden sollte. Dabei ging es um die Änderung der Statuten, die strategische Planung, das Budget oder die Abwahl von ICANN-Direktoren. Die eine Seite schlug ein sogenanntes ›Membership-Modell‹ vor. Demnach sollte ein neues Gremium Entscheidungen des ICANN-Vorstands anfechten und Direktoren abberufen können sowie Zuständigkeiten für das Budget oder Änderungen in den Statuten erhalten. Kritiker des ›Membership-Modells‹ sahen in der Schaffung einer zweiten Kammer einen Unsicherheitsfaktor, der das Risiko neuer Machtkämpfe oder die Gefahr einer lähmenden Pattsituation in sich trage. Sie bevorzugten einen kleineren Schritt in Form eines sogenannten ›Designatoren-Modells‹. Das ›Designatoren-Modell‹ beinhaltet viele Aspekte des Membership-Modells – insbesondere Einspruchsrechte der Gemeinschaft sowie das Recht, ICANN-Direktoren abzusetzen. Dies hat den Vorteil, dass formell keine neue Institution geschaffen wird.

Das Gesamtpaket wurde bei der 55. ICANN-Tagung im März 2016 in Marrakesch verabschiedet und muss nun von der NTIA und dem amerikanischen Kongress bewertet werden. Der IANA-Vertrag ist ein sogenannter ›Sunset-Vertrag‹ und kann ohne eine spezifische Zustimmung auslaufen. Sollte es keine gravierenden Einwände geben, würde das neue Modell mit dem Auslaufen des bestehenden IANA-Vertrags am 30. September 2016 an dessen Stelle treten.[21] Nicht ausgeschlossen werden kann jedoch, dass das Thema in den amerikanischen Wahlkampf hineingezogen wird und es dadurch zu Verzögerungen kommt. Eine letzte Möglichkeit wäre eine Verlängerung des Vertrags bis zum 31. Dezember 2016. Scheitert auch das, liegt es in den Händen der neuen amerikanischen Regierung, ob sie an der Übergabe der IANA festhält oder das ganze Verfahren noch einmal neu aufrollt. Der gegenwärtige Vertrag kann bis zum 30. September 2019 problemlos von der amerikanischen Regierung verlängert werden. Im Interesse der ICANN und ihrer Gemeinschaft wäre ein Schlussstrich unter diese zähe Debatte mehr als wünschenswert. Dann könnte sich die ICANN wieder seinen eigentlichen Aufgaben – der Weiterentwicklung des Marktes zu Domainnamen und der Gewährleistung von Stabilität und Sicherheit im System der Domainnamen – zuwenden.

Es galt, einen Mechanismus zu finden, der garantiert, dass eine unabhängige ICANN sich nicht verselbstständigt, Machtmissbrauch ermöglicht oder von einzelnen Interessengruppen eingenommen wird.

14 World Bank, World Development Report 2016: Digital Dividends, New York 2016, www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2016/01/13/090224b08405ea05/2_0/Rendered/PDF/Worldodevelopmoooodigitalodividends.pdf In deutscher Sprache ist eine Kurzfassung verfügbar: www.pubdocs.worldbank.org/pubdocs/publicdoc/2016/1/112781453827891613/WDR-2016-MainMessages-GERMAN-Final.pdf

15 Übersicht der UNGIS-Mitglieder: www.ungis.org/Members.aspx

16 UN Doc. A/70/L.33 v. 13.12.2015, S. 13.

17 Siehe Adam Segal, The UN's Group of Governmental Experts on Cybersecurity, Net Politics, 13.4.2015, www.blogs.cfr.org/cyber/2015/04/13/the-uns-group-of-governmental-experts-on-cybersecurity/

18 Ausführlich zu den bisherigen Verhandlungen: Tim Maurer, in diesem Heft, S. 51–55.

19 Informationen zur ICG: www.ianacg.org/

20 IANA Stewardship Transition Coordination Group (ICG), Proposal to Transition the Stewardship of the Internet Assigned Numbers Authority (IANA) Functions from the U.S. Commerce Department's National Telecommunications and Information Administration (NTIA) to the Global Multistakeholder Community, Juli 2014, S. 3–4.

21 Zur Übergabe der Funktionen der IANA und zum ›Konsensus von Marrakesch‹: www.icann.org/stewardship-accountability

Internet Governance: Zukünftige Akteure und Initiativen

Die beiden wichtigsten Konferenzen auf globaler Ebene werden im Jahr 2016 in Mexiko stattfinden. Im Juni 2016 wird die Ministerkonferenz der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (Organisation for Economic Co-operation and Development – OECD) in Cancún die Themen Cybersicherheit und Digitale Wirtschaft diskutieren. Im November 2016 wird Mexiko Gastgeber des Elften Internet Governance Forums sein.

Das Thema Cybersicherheit wird auch bei den großen Gipfeltreffen im Vordergrund stehen: Das Treffen der Gruppe der 7 (G7) findet im Mai 2016 in Japan statt, das Treffen der Gruppe der 20 (G20) im September 2016 in China. Die BRICS-Staaten (Brasilien, Russland, Indien, China, Südafrika), die sich bei ihrem letzten Gipfeltreffen im russischen Ufa für ein internationales Übereinkommen zu Cybersicherheit ausgesprochen haben, treffen sich im Sommer 2016 in Indien. Das Thema wird auch während der Generaldebatte der 71. UN-Generalversammlung im Herbst 2016 relevant werden.

Neben zwischenstaatlichen Verhandlungen haben sich immer mehr Multistakeholder-Plattformen gebildet, von denen ein nicht unerheblicher Einfluss auf die globale Internet Governance-Politik ausgeht.

Nicht minder brisant wird sich das Thema Datenschutz im Internet entwickeln. Nach den Urteilen des Europäischen Gerichtshofs (EuGH) muss das sogenannte ›Safe Harbor-Abkommen‹ neu ausgehandelt werden. Dies ist zwar zunächst eine bilaterale Angelegenheit zwischen den USA und der EU, hat jedoch schon lange eine globale Dimension. Möglicherweise wird sich auch die WTO zukünftig mit dem Thema ›Digitaler Handel‹ beschäftigen. Der erste Bericht des Sonderberichterstatters über das Recht auf Privatheit Joseph Cannataci ist Ende März 2016 erschienen. UNESCO, WIPO und ITU werden sich weiter mit dem Thema Internet Governance befassen. Gespannt kann man sein, was die neu gegründete Forschungsgruppe ›Study Group 20‹ der ITU zum Thema ›Internet der Dinge‹ zu sagen haben wird.[22]

Neben diesen mehr oder minder offiziellen, meist zwischenstaatlichen Verhandlungen haben sich immer mehr Multistakeholder-Plattformen gebildet, von denen ein nicht unerheblicher Einfluss auf die globale Internet Governance-Politik ausgeht. Die ›NETMundial-Initiative‹ (NMI), die aus der Konferenz ›NETMundial‹ im Jahr 2014 im brasilianischen São Paulo entstanden ist, sieht sich als eine Plattform für Projekte zur Umsetzung der São Paulo-Prinzipien und der ›São Paulo Roadmap‹. Dem Koordinierungsrat der NMI gehören unter anderem die amerikanische Wirtschaftsministerin Penny Pritzker, der Vizepräsident der Europäischen Kommission Andrus Ansip und der chinesische Internetminister Lu Wei an. Geleitet wird die NMI von fünf Ko-Vorsitzenden, darunter Eileen Donahoe, Director of Global Affairs bei Human Rights Watch, und Jack Ma, Gründer und Vorstandsvorsitzender der Alibaba Group. Angedacht wird eine NETMundial+5-Überprüfungskonferenz im Jahr 2019, eventuell in Kooperation mit dem 14. IGF.[23]

Das Weltwirtschaftsforum, das auch in die NMI involviert ist, hat mit der Initiative ›Future of the Internet‹ (FII) ein eigenes Projekt ins Leben gerufen. Beim Davoser Weltwirtschaftsforum Ende Januar 2016 fanden einige Workshops zu Internet Governance statt, darunter die Themen ›Fragmentierung des Internets‹[24] und ›Digitaler Handel‹. Die Global Internet Governance Commission (GIGC), die unter Leitung des ehemaligen schwedischen Ministerpräsidenten und Außenministers Carl Bildt vor zwei Jahren gegründet wurde, wird im Sommer 2016 ihren Bericht vorlegen. Darin wird unter anderem ein neuer ›Digitaler Sozialer Pakt‹ vorgeschlagen.[25] Dies ähnelt dem Vorschlag des Präsidenten des Europäischen Parlaments Martin Schulz zur Ausarbeitung einer ›Charta für Digitale Grundrechte‹.[26] Eine ›Global Commission on the Stability of Cyberspace‹ wird gegenwärtig vom niederländischen Außenministerium vorbereitet.

Die Anzahl der Akteure und Initiativen wird sich weiter erhöhen. Ende des Jahres 2015 hat die chinesische Regierung in Wuzhen die Zweite Welt-Internet-Konferenz mit mehr als 2000 Teilnehmenden aus über 100 Staaten veranstaltet und die ›Wuzhen Internet Initiative‹ (WII) gegründet. Chinas Präsident Xi Jinping hatte bei der Eröffnung der Konferenz verkündet, dass das Prinzip der Cybersouveränität das oberste Prinzip für Internet Governance sein müsste.[27]

22 Informationen zur SG20: www.itu.int/en/ITU-T/studygroups/2013-2016/20/Pages/default.aspx

23 Siehe Kleinwächter, a.a.O. (Anm. 12).

24 Siehe William Drake/Vinton G. Cerf/Wolfgang Kleinwächter, Internet Fragmentation: An Overview, Future of the Internet Initiative White Paper, World Economic Forum, Genf 2016, www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf

25 Global Commission on Internet Governance, Toward a Social Compact for Digital Privacy and Security, April 2015, www.cigionline.org/sites/default/files/gcig_special_report_web.pdf

26 Siehe Martin Schulz, EU-Parlamentspräsident fordert Ausweitung der Grundrechte, ZEIT ONLINE, 26.11.2015, www.zeit.de/digital/datenschutz/2015-11/martin-schulz-datenschutz-digitalisierung

27 Zur Eröffnungsrede von Präsident Xi Jiping siehe www.wuzhenwic.org/2015-12/16/c_47580.htm

Die Zukunft der Kriegsführung?

Autonome Waffensysteme als Herausforderung für das Völkerrecht

Markus Wagner

Der Umgang mit Autonomen Waffensystemen (AWS) ist keine Zukunftsmusik mehr, sondern stellt für das Völkerrecht und die internationale Politik eine große Herausforderung dar. Der Beitrag skizziert die rechtlichen Voraussetzungen des humanitären Völkerrechts für die Verwendung von AWS und kommt zu dem Ergebnis, dass derzeit einem Einsatz von AWS erhebliche Bedenken gegenüberstehen. Der Beitrag schließt mit einer Beschreibung möglicher zukünftiger Regelungsansätze für AWS.

Für viele mag die Debatte um sogenannte Autonome Waffensysteme (AWS) wie Zukunftsmusik erscheinen. Gemeint sind damit Systeme, die in der Lage sind, ohne direkte menschliche Einflussnahme Entscheidungen über den Waffeneinsatz und dessen Modalitäten zu treffen. In der Tat steht der Diskurs um AWS in Deutschland noch am Anfang. Dies liegt vor allem daran, dass die Auseinandersetzung um den Einsatz von bewaffneten ferngesteuerten Drohnen in Deutschland spät eingesetzt hat. Die Diskussion wurde schließlich umso heftiger geführt und hat wenig Raum für Fragen über die rechtliche Zulässigkeit und die politische Erwünschtheit von AWS gelassen. Andernorts wird über diese Fragen – sowohl in der Wissenschaft als auch in der Öffentlichkeit – bereits seit geraumer Zeit diskutiert. Der vorliegende Beitrag soll dazu dienen, die sich durch AWS stellenden rechtlichen und politischen Herausforderungen zu skizzieren und erste Denkanstöße hinsichtlich der Möglichkeit einer völkerrechtlichen Regulierung zu liefern.

Entwicklung und Begrifflichkeit Autonomer Waffensysteme

Die seit Ende des 19. Jahrhunderts erfolgten technologischen Errungenschaften sind im Hinblick auf die Entwicklung von AWS von besonderer Bedeutung. Zu beachten ist jedoch, dass eine Vermengung der Analyse von ferngesteuerten Drohnen mit AWS die unterschiedlichen Herausforderungen, die beide Systeme aufwerfen, vernachlässigt.[1]

Vorstufen zur Entwicklung von AWS lassen sich schon zu Ende des 19. Jahrhunderts finden, als Nikola Tesla ein Patent für ein ferngesteuertes und bewaffnetes Schiff erlangte.[2] Jedoch fanden weder Teslas Erfindung noch die bis zum Ende des Zweiten Weltkriegs entwickelten Systeme wie der von Charles Kettering entwickelte und erprobte unbemannte Flugkörper (Kettering Bug) aus Großbritannien oder der von der Wehrmacht eingesetzte kabelgesteuerte Goliath-Panzer weite Verbreitung.[3] Verbesserte Satelliten- und Kommunikationstechnologie ermöglichte seit den 1970er Jahren den Einsatz ferngelenkter unbemannter Fluggeräte zu Aufklärungszwecken im südlibanesischen Bekaa Tal durch die israelischen Streitkräfte.[4] Insbesondere nach dem 11. September 2001 stieg die Bedeutung von ferngelenkten Kampfdrohnen an. Dies lässt sich auch an der Anzahl der unbemannten Systeme des amerikanischen Verteidigungsministeriums ablesen, die im Zeitraum von 2002 bis 2010 von 167 auf über 7000 stieg.[5] Mittlerweile setzen eine Vielzahl anderer Staaten ähnliche Systeme routinemäßig ein. Die öffentliche Debatte hat sich gerade auch an der Verwendung ferngelenkter Drohnen im Zusammenhang mit gezielten Tötungen entzündet.[6]

Der Begriff ›Autonome Waffensysteme‹ hat unterschiedliche Definitionen erfahren. Ihnen ist jedoch gemein, dass sie ein großes Maß an Unabhängigkeit von menschlicher Intervention und eine Entscheidung aufgrund des dem System zugrunde liegenden Algorithmus erfordern.[7] Damit ist auch klargestellt, dass der Begriff nicht moralphilosophisch zu verstehen ist, sondern die Entscheidungen eines AWS unabhängig von menschlichem Zutun während eines

Prof. Markus Wagner, geb. 1976, ist Associate Professor an der University of Miami. Er lehrt und forscht in den Bereichen Internationales Recht, Verfassungsrecht und Vergleichendes Recht.

1 Siehe dazu: Robert Frau, Der Einsatz von Drohnen. Eine völkerrechtliche Betrachtung, Vereinte Nationen, 3/3013, S. 99–103.

2 Nikola Tesla, Method and Apparatus for Controlling Mechanism of Moving Vessels or Vehicles, U.S. Patent No. 613809 A vom 1.7.1898, www.perma.cc/9D7H-WLLH

3 Laurence R. Newcome, Unmanned Aviation: A Brief History of Unmanned Aerial Vehicles, American Institute of Aeronautics and Astronautics, Reston 2004, S. 13–14; Kendra Cook, The Silent Force Multiplier: The History and Role of UAVs in Warfare, Aerospace Conference, Institute of Electrical and Electronics Engineers, Big Sky 2007, S. 2.

4 Ralph Sanders, An Israeli Military Innovation: UAVs, Joint Force Quarterly, 2002/2003, S. 114.

5 Jeremy Gertler, U.S. Unmanned Aerial Systems, Congressional Research Service, 2012, S. 2.

6 Siehe generell David Kretzmer, Targeted Killing of Suspected Terrorists: Extra-Judicial Executions or Legitimate Means of Defence?, The European Journal of International Law, Vol. 16, 2005, S. 171; Nils Melzer, Targeted Killing in International Law, Oxford 2008.

7 Markus Wagner, The Dehumanization of International Humanitarian Law: Legal, Ethical and Political Implications of Autonomous Weapon Systems, Vanderbilt Journal of Transnational Law, Vol. 47, 2014, S. 1371.

Einsatzes beschreibt.[8] Autonome Systeme unterscheiden sich von derzeit bereits eingesetzten ferngesteuerten oder automatisierten Waffensystemen vor allem im Hinblick auf den Grad ihrer Unabhängigkeit. Diese in der öffentlichen Debatte häufig übersehene Unterscheidung hat in rechtlicher und in politischer Hinsicht grundlegende Bedeutung.

Die bekanntesten Beispiele für ferngesteuerte Waffensysteme sind luftbasierte Systeme. Entsprechende landgestützte Systeme befinden sich ebenfalls im Einsatz und finden häufig beim Aufspüren und bei der Beseitigung von Sprengfallen Verwendung, können aber auch selbst Waffenträger sein.[9] In geringerem Umfang werden auch ferngelenkte seegestützte Systeme eingesetzt.[10] Automatisierte Systeme folgen oftmals vorgegebenen Wegpunkten im Fall von Aufklärungsdrohnen oder greifen, im Fall von Marschflugkörpern, ein vor dem Einsatz ausgewähltes Ziel an. Andere Systeme reagieren auf bestimmte Reize, wie die Hitze eines Flugzeugtriebwerks oder Schraubengeräusche von Wasserfahrzeugen. Der menschliche Anteil besteht darin, dem System vor dem Einsatz die notwendigen Daten zur Verfügung zu stellen. Ferngesteuerte oder automatisierte Systeme unterscheiden sich von AWS dadurch, dass die Entscheidung über deren Einsatz von Menschen getroffen wird. Allerdings werden während eines Einsatzes die Einzelentscheidungen über einen Angriff, dessen Zeitpunkt, die Verwendung von Waffen oder anderer Angriffsmodalitäten dem der AWS zugrunde liegenden Software überlassen.[11] Zudem sind AWS in der Lage, unter einer Reihe von unterschiedlichen Möglichkeiten diejenige auszuwählen, die das Einsatzziel am besten erreicht. Sie haben einen viel höheren Grad an Unabhängigkeit als ferngelenkte oder automatische Systeme und üben Ermessen aus. Für einen Einsatz ist damit eine Software Voraussetzung, die solche Ermessensentscheidungen tatsächlich treffen und dies in Übereinstimmung mit den relevanten Regeln des Völkerrechts bewerkstelligen kann.

Für einen Einsatz von AWS ist eine Software Voraussetzung, die Ermessensentscheidungen treffen und dies in Übereinstimmung mit den relevanten Regeln des Völkerrechts bewerkstelligen kann.

Auch wenn AWS sich noch im Entwicklungsstadium befinden, kann es als gesichert gelten, dass autonome Systeme in absehbarer Zeit zum Einsatz kommen werden. Die Argumente für die Entwicklung und den Einsatz von AWS sind teilweise mit denjenigen identisch, die schon im Hinblick auf ferngelenkte Systeme vorgebracht wurden, gehen zum Teil aber darüber hinaus. Diese beinhalten eine über das menschliche Vermögen hinausgehende Einsatzdauer, eine genauere Zielbekämpfung, die Schonung der eigenen Soldatinnen und Soldaten und die fehlende emotionale Reaktion von Operateuren, wie zum Beispiel Angst oder Wut.[12] Beispiele für Systeme mit Fähigkeiten, die einen höheren Grad an Autonomie aufweisen, befinden sich bereits im Einsatz oder werden getestet. Dazu gehören luftgestützte Systeme, die nach Darstellung des Herstellers Ziele selbstständig suchen oder eigenständig einen Flug absolvieren können sowie defensive Luftverteidigungssysteme oder Patrouillensysteme.

Aus Sicht des Völkerrechts stellt sich vor allem die Frage, ob die Entscheidung über den Einsatz von Waffen ohne menschliches Zutun zulässig ist.

Diese Unterscheidung zwischen den verschiedenen Graden an Autonomie (ferngelenkt, automatisiert und autonom) erleichtert die Beschreibung der verschiedenen Kategorien. Darüber hinaus besteht kein Grund, warum ein System in einer Situation nicht ferngesteuert werden sollte und in anderen Situationen autonom agiert. Zuletzt ist noch zu bedenken, dass ein System möglicherweise auch dann als autonom einzustufen ist, wenn eine menschliche Kontrolle zumindest formal noch gegeben ist. Dies ist zum Beispiel der Fall, wenn ein Operateur eine Vielzahl von Systemen zu überwachen hat oder eine Situation eintritt, in der Informationen nicht verarbeitet werden. Dieses Szenario ist nicht rein theoretisch, sondern ereignete sich beim Abschuss eines iranischen Flugzeugs über dem Persischen Golf im Jahr 1988.[13]

Rechtliche Überlegungen

Aus Sicht des Völkerrechts stellt sich bezüglich AWS vor allem die Frage, ob die Entscheidung über den Einsatz von Waffen ohne menschliches Zutun zulässig ist. Es bestehen wohl kaum ernsthafte Bedenken gegen den Einsatz von autonomen Systemen etwa im Bereich des Minenräumens oder zur Rettung von Personen in gefährlichen Situationen ohne Feindkontakt (beispielsweise die Rettung aus nuklear verseuchtem Gebiet). Konkret sollen hier zwei grundlegende Eckpfeiler des humanitären Völkerrechts besprochen werden: das Unterscheidungsgebot und das Prinzip der Verhältnismäßigkeit.[14] Außer Betracht bleiben somit Fragen hinsichtlich

8 Robin Geiss, Die völkerrechtliche Dimension autonomer Waffensysteme, Friedrich-Ebert-Stiftung, Juni 2015, S. 6.

9 Elizabeth Quintana, The Ethics and Legal Implications of Military Unmanned Vehicles, Royal United Services Institute for Defence and Security Studies, 2008, S. 2.

10 Ebd., S. 6.

11 Vgl. International Committee of the Red Cross, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, Geneva 2011, S. 38ff. Siehe auch United States Department of Defense, Directive 3000.09, Autonomony in Weapon Systems, 2012; Human Rights Watch, Losing Humanity: The Case Against Killer Robots, 2012, S. 2.

12 United States Department of Defense, a.a.O. (Anm. 11), S. 7–15; Ronald Arkin, Governing Lethal Behavior in Autonomous Robots, Boca Raton 2009, S. 205ff.

13 Scott Sagan, Rules of Engagement, in: Alexander L. George (Ed.), Avoiding War: Problems of Crisis Management, Boulder 1991, S. 460.

14 Artikel 36 (1. Zusatzprotokoll), der den Vertragsparteien eine Pflicht auferlegt, neue Waffensysteme auf ihre Vereinbarkeit mit dem humanitären Völkerrecht zu überprüfen. Siehe Geiss, a.a.O. (Anm. 8), S. 14–15; Wagner, a.a.O. (Anm. 7), S. 1384.

der Zulässigkeit über den Eintritt in einen bewaffneten Konflikt. Die verwendeten militärischen Mittel spielen für diese Frage nur in hier nicht relevanten Ausnahmefällen eine Rolle.

Das humanitäre Völkerrecht enthält nicht nur eine Reihe genauer Regelungen, sondern auch weitreichende Prinzipien, welche die Konfliktführung regeln. Dabei ist zu beachten, dass Kombattanten dem Grundsatz nach zu jeder Zeit angegriffen werden dürfen. Von Ausnahmen abgesehen, besteht jedoch ein Verbot des Angriffs auf Zivilisten.[15] Dabei wird auf einen Ausgleich zwischen der militärischen Notwendigkeit und dem Gebot des humanen Umgangs mit der Zivilbevölkerung hingewirkt.[16] Unklarheit besteht jedoch darin, wo in diesem Spannungsverhältnis die Grenze zum Rechtsbruch zu ziehen ist. Das humanitäre Völkerrecht verfolgt dabei – von wichtigen Ausnahmen abgesehen[17] – den Ansatz, nicht Waffen als solche zu verbieten, sondern stellt auf deren konkreten Einsatz im Einzelfall ab. Bei der Bewertung kommt es nicht auf das Resultat des Angriffs an, sondern auf die zum Befehls- beziehungsweise Angriffszeitpunkt für den Befehlshaber vorliegende Situation. Die Frage der Zulässigkeit von AWS kann nur dann positiv beantwortet werden, wenn die zugrunde liegende Software in der Lage ist, diese recht abstrakten Regeln im konkreten Fall richtig anzuwenden. Problematisch ist vor allem Folgendes: Auf Algorithmen basierenden Computerprogrammen ist es bislang kaum möglich, Entscheidungen mit qualitativem Charakter zu fällen. Wie später noch gezeigt wird, sind die Entscheidungen nicht nur hinsichtlich des Verhältnismäßigkeitsprinzips, sondern auch bezogen auf das Unterscheidungsgebot qualitativer Natur.

Das Unterscheidungsgebot

Wie soeben angedeutet, müssen an Konflikten beteiligte Parteien zwischen Zivilisten und Kombattanten beziehungsweise zivilen Objekten und militärischen Zielen unterscheiden.[18] Darüber hinaus verbietet das Zusatzprotokoll zu den Genfer Abkommen vom 12. August 1949 über den Schutz der Opfer internationaler bewaffneter Konflikte (1. Zusatzprotokoll) Angriffe auf für die Zivilbevölkerung lebensnotwendige Objekte ebenso wie auf Anlagen und Einrichtungen, die sogenannte ›gefährliche Kräfte‹ enthalten (zum Beispiel Staudämme oder Nuklearanlagen).

Während diese Regeln auf den ersten Blick recht eindeutig erscheinen, zeigt die Praxis, dass die Unterscheidung zwischen zivilen und militärischen Zielen oftmals sehr komplex ist. Man denke an Brücken oder die Stromversorgung, die zwar grundsätzlich zivile Objekte darstellen, allerdings in bestimmten Fällen einen großen militärischen Nutzen aufweisen können. Ähnliche und noch größere Probleme stellen sich in sogenannten ›asymmetrischen Konflikten‹, in denen Kämpfer nicht eindeutig identifizierbar und nur schwer von der Zivilbevölkerung zu unterscheiden sind. Solche direkt an Kampfhandlungen teilnehmenden Personen fallen nicht unter den Schutz für Zivilisten, sondern gelten als legitime Ziele, solange sie dauerhaft an Kampfhandlungen teilnehmen.[19] Jedoch ist zu bedenken, dass das Tragen einer Waffe nicht ausreichend ist, um eine Person nicht als Zivilisten einzustufen. Es könnte sich um eine Waffe zum Eigenschutz oder zur Jagd handeln. Entscheidend ist mithin der Kontext, in der eine solche Entscheidung getroffen wird.

Problematisch ist, dass es auf Algorithmen basierenden Computerprogrammen bislang kaum möglich ist, Entscheidungen mit qualitativem Charakter zu fällen.

Die AWS zugrunde liegende Software muss in der Lage sein, diese unterschiedlichen Situationen zu meistern. Die Entscheidungen werden auf der Basis von programmierten Merkmalen eines bestimmten Objekts getroffen.[20] Sobald eine vorher bestimmte Anzahl von Übereinstimmungen mit den vorgegebenen Merkmalen und damit eine bestimmte Gewissheit über das Vorliegen eines militärischen Zieles erreicht ist, könnte der Angriff von einem AWS durchgeführt werden. Ein solcher Abgleich kann – abhängig vom Objekt – von mechanischer Natur sein und auf einer quantitativen Analyse basieren. Auch wenn man AWS – wohl begründet – skeptisch gegenübersteht, wird man zugestehen müssen, dass die zukünftige technische Entwicklung in der Lage sein wird, derartige Entscheidungen mit immer größerer Sicherheit zu treffen.[21]

Die Praxis zeigt, dass die Unterscheidung zwischen zivilen und militärischen Zielen sehr komplex ist.

Selbst wenn man einen entsprechenden technischen Fortschritt als möglich ansieht, bleibt zu bedenken, dass eine große Anzahl von Auseinanderset-

15 Melzer, a.a.O. (Anm. 6).

16 Michael Schmitt, Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance, Virginia Journal of International Law, Vol. 50, No. 4, 2010, S. 795; Darren M. Stewart, New Technology and the Law of Armed Conflict, International Law Studies, Vol. 87, 2011, S. 272.

17 Beispiele für derartige Verbote sind das Verbot von Antipersonenminen, Streubomben oder blendenden Laserwaffen.

18 Artikel 48, 1. Zusatzprotokoll: »Um Schonung und Schutz der Zivilbevölkerung und ziviler Objekte zu gewährleisten, unterscheiden die am Konflikt beteiligten Parteien jederzeit zwischen der Zivilbevölkerung und Kombattanten sowie zwischen zivilen Objekten und militärischen Zielen; sie dürfen daher ihre Kriegshandlungen nur gegen militärische Ziele richten.«

19 International Committee of the Red Cross, Interpretative Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law, Geneva 2009, S. 70ff.

20 Michael Lewis/Katia Sycara/Paul Scerri, Scaling Up Wide-Area-Search Munition Teams, IEEE Intelligent Systems, Vol. 24., 2009, S. 10.

21 Siehe zum Streit um die Erfordernis einer Verhältnismäßigkeitsprüfung Stefan Oeter, Methods and Means of Combat, in: Dieter Fleck (Hrsg.), The Handbook of International Humanitarian Law, 2. Auflage, Oxford 2008, S. 119, 201ff.

Bereits heutzutage können defensive Waffensysteme wie das PATRIOT-Raketenabwehrsystem autonom agieren. Berlin, 2012. Foto: Sivi Steys/flickr.com

zungen nicht mehr auf dem Schlachtfeld von Soldatinnen und Soldaten geführt werden, die eindeutig von Zivilisten zu unterscheiden sind. Vielmehr finden viele Einsätze in unübersichtlichen und zum Teil dicht besiedelten Gebieten statt. Gerade in diesen Situationen sind Entscheidungen in einem komplexen Kontext zu treffen. Für AWS bedeutet dies, dass sie nicht nur auf abstrakter Ebene zwischen zivilen und militärischen Zielen unterscheiden, sondern auch im konkreten Fall unter sich ändernden Umständen korrekt handeln müssen. Die Software müsste zudem in der Lage sein, bei Unsicherheit in der Beurteilung, ob ein Ziel zivilen oder militärischen Charakter hat, einen Angriff abzubrechen.

In Bezug auf das Unterscheidungsgebot bestehen große Unsicherheiten, ob die derzeitige technologische Entwicklung den Einsatz von AWS ermöglichen kann.

Darüber hinaus ist die Unterscheidung zwischen Zivilisten und denjenigen, die direkt an Kampfhandlungen teilnehmen, schon für Menschen mit Schwierigkeiten behaftet. Im Gegensatz zu einer Vielzahl von Objekten können Entscheidungen zwischen Zivilisten und Kombattanten nicht nur auf Grundlage quantitativer Analysen getroffen werden. Vielmehr kommt in diesen Situationen qualitativen Merkmalen eine besondere Bedeutung zu.[22] Schon in Bezug auf das Unterscheidungsgebot bestehen somit große Unsicherheiten, ob die derzeitige technologische Entwicklung den Einsatz von AWS ermöglichen kann.

Das Prinzip der Verhältnismäßigkeit

Das Prinzip der Verhältnismäßigkeit verursacht im Hinblick auf seine Umsetzung durch AWS noch größere Schwierigkeiten, da es sich nur schwer auf abstrakter Ebene definieren lässt.[23] Das Prinzip wird nicht ausdrücklich im 1. Zusatzprotokoll erwähnt, sondern kommt in einer Reihe von Bestimmungen, wie zum Beispiel Artikel 51(5)(b) und Artikel 57(2) zum Ausdruck.

Die erste Vorschrift verbietet Angriffe, bei denen der militärische Vorteil nicht im Verhältnis zu den zivilen Verlusten steht.[24] Entscheidend sind hierbei die Umstände des Einzelfalls.[25] Der Begriff drückt die Spannung zwischen den in bewaffneten Konflikten widerstreitenden Interessen aus: auf der einen Seite die Erreichung des militärischen Zieles, auf der anderen Seite der Schutz der Zivilbevölkerung beziehungsweise ziviler Objekte. Es kann somit aus rechtlicher Sicht unbedenklich sein, wenn bei einem Angriff eine relativ hohe Anzahl von zivilen Opfern verursacht wurde, solange zum Zeitpunkt des Angriffs die abzusehende Anzahl von Opfern nicht außer Verhältnis zum konkreten und vorhergesagten militärischen Vorteil steht.

Aufgrund der unsicheren Konturen des Verhältnismäßigkeitsprinzips stellt sich die Frage, ob es überhaupt möglich ist, dieses korrekt zur Anwendung zu bringen. Dies betrifft nicht nur die Zielauswahl selbst, sondern auch die Wahl der Angriffsmethoden und der Angriffsmittel. Die Entscheidung über einen Angriff beziehungsweise dessen konkrete Umstände basieren auf den Entscheidungen und den Gewichtungen, die im Steuerprogramm von AWS festgelegt sind. Eine Vielzahl dieser Erwägungen sind qualitativer Natur. Einen numerischen Wert für die Wertigkeit eines Zieles anzugeben und damit festzulegen, wie viele Menschenleben hierfür geopfert werden dürfen, ist nicht möglich.[26] Verstärkt wird

22 Siehe Wagner, a.a.O. (Anm. 7), S. 1392.

23 William Boothby, Weapons and the Law of Armed Conflict, Oxford 2009, S. 79; Yoram Dinstein, The Conduct of Hostilities Under the Law of International Armed Conflict, 2. Auflage, Cambridge 2010, S. 131; William Fenrick, The Rule of Proportionality and Protocol I in Conventional Warfare, Military Law Review, Jg. 98, 1982, S. 97. Im Englischen wird der Begriff ›excessive‹ verwendet, der nach allgemeiner Ansicht gleichbedeutend mit »disproportionate« ist.

24 Artikel 51(5)(b), 1. Zusatzprotokoll: »Unter anderem sind folgende Angriffsarten als unterschiedslos anzusehen: [...]; b) ein Angriff, bei dem damit zu rechnen ist, dass er auch Verluste an Menschenleben unter der Zivilbevölkerung, die Verwundung von Zivilpersonen, die Beschädigung ziviler Objekte oder mehrere derartige Folgen zusammen verursacht, die in keinem Verhältnis zum erwarteten konkreten und unmittelbaren militärischen Vorteil stehen.«

25 Gary Solis, The Law of Armed Conflict: International Humanitarian Law in War, New York 2010, S. 273.

26 Dinstein, a.a.O. (Anm. 23), S. 132f.; Thomas Franck, On Proportionality of Countermeasures in International Law, American Journal of International Law, Vol. 102, 2008, S. 729; Michael Bothe/Karl Josef Partsch/Waldemar Solf, New Rules for Victims of Armed Conflicts: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949, The Hague 1982, S. 310.

die Problematik dadurch, dass keine der widerstreitenden Interessen – Erreichung des militärischen Zieles und Schutz der Zivilbevölkerung – statisch ist. Vielmehr treten in der Praxis häufig Situationen auf, in denen sich nicht nur der Wert eines Zieles für die Erreichung eines militärischen Vorteils ändert, sondern auch die Anzahl der möglicherweise betroffenen Zivilistinnen und Zivilisten.

Derzeit ist daher davon auszugehen, dass trotz technologischer Fortschritte Entscheidungen durch AWS nicht den soeben erörterten Vorschriften entsprechen. Dies bedeutet, dass die Anwendungsmöglichkeit von AWS so gering ist, dass sie für eine Vielzahl von Kampfhandlungen nicht herangezogen werden könnten, oder andere, schon bestehende Waffensysteme diese Aufgaben erfüllen.[27]

Das politische Für und Wider

Die juristische Debatte bettet sich in eine breitere Auseinandersetzung um das Für und Wider der derzeitigen und zukünftigen Entwicklung und des Einsatzes von AWS ein. Neben der Frage der Verringerung der psychologischen Hemmschwelle für die am Einsatz beteiligten Soldatinnen und Soldaten[28] ist ein häufiges Argument, dass die Verwendung von AWS die Entscheidung über eine kriegerische Auseinandersetzung oder dessen Fortführung auf politischer Ebene insofern beeinflusst, als dass menschliches Leid zumindest für diejenige Kriegspartei verringert wird, die AWS in ihren Arsenalen hat.[29] Auch wenn kriegerische Auseinandersetzungen in absehbarer Zeit nicht durch Armeen von AWS geführt werden,[30] ist dieses Argument zumindest im Hinblick auf Demokratien nicht von der Hand zu weisen.

Dieses veränderte politische Risiko wird sogar von denjenigen zugestanden, die AWS positiv gegenüber eingestellt sind.[31] Damit wird der Tatsache Rechnung getragen, dass das humanitäre Völkerrecht seinen Ursprung gerade in der Bemühung hat, das menschliche Leid in bewaffneten Konflikten zumindest einzudämmen. Diese Entwicklung einer Verringerung des Risikos für die Soldaten lässt sich seit geraumer Zeit beobachten. So wurden im Rahmen des Kosovo-Konflikts oder des Libyen-Konflikts im Jahr 2011 keine Bodenstreitkräfte eingesetzt. Das Risiko für die eigenen Truppen ist unter diesen Umständen ungleich geringer und eventuelle Verluste sind leichter zu erklären.

Die Gegenseite argumentiert, dass eine Verweigerung eines solchen technologischen Fortschritts und der damit jedenfalls angenommenen höheren Präzision moralisch nicht vertretbar sei.[32] Jedoch ist derzeit nicht ersichtlich, ob der nötige technologische Fortschritt und die vom humanitären Völkerrecht geforderte Präzision überhaupt möglich sind. Geht man jedoch davon aus, dass bewaffnete Konflikte so weit wie möglich zu vermeiden sind oder die Entscheidung über den Eintritt in einen Konflikt zumindest hohe politische Kosten mit sich bringen sollte, dann sind Verweise auf technologischen Fortschritt oder eine höhere Präzision nur bedingt überzeugend.

Zukunftsszenarien: Regulierung als Alternative zu Ächtung oder Abwarten?

Aufgrund der raschen technologischen Entwicklung kommt einer frühzeitigen Debatte über die rechtlichen und gesellschaftspolitischen Herausforderungen entscheidende Bedeutung zu. Es findet schon jetzt eine Weichenstellung für die Zukunft statt und damit über die Frage, ob AWS in künftigen bewaffneten Konflikten zum Einsatz kommen. Einige Autoren gehen von einer Art Unabwendbarkeit der technologischen Entwicklung aus.[33] In der Tat ist nicht zu leugnen, dass eine solche schleichende Indienststellung von Systemen mit autonomen Fähigkeiten möglich und sogar wahrscheinlich ist.

Dennoch hat sich eine rege Debatte über die Zukunft von AWS entwickelt. Grob lassen sich die Vorschläge in drei Kategorien unterteilen und reichen von Ächtung bis hin zu milden Kontrollmechanismen. Eine Reihe von nichtstaatlichen Organisationen (NGOs) und in der Öffentlichkeit stehenden Personen treten für eine Ächtung mit den oben schon erwähnten Argumenten ein.[34] Dabei werden häufig Parallelen zu den Verboten von Antipersonenminen und blendenden Laserwaffen gezogen. Zu beachten ist jedoch, dass es sich bei AWS um klassische Technologien mit doppeltem Verwendungszweck (dual-use technology) handelt und eine Vielzahl von

Die Anwendungsmöglichkeit von AWS ist so gering, dass sie für eine Vielzahl von Kampfhandlungen nicht herangezogen werden könnten, oder andere, schon bestehende Waffensysteme diese Aufgaben erfüllen.

27 Boothby a.a.O. (Anm. 23), S. 233.

28 Peter W. Singer, Wired For War, New York 2009, S. 395–96; UN Doc. A/HRC/23/47 v. 9.4.2013.

29 Sarah Kreps/John Kaag, The Use of Unmanned Aerial Vehicles in Contemporary Conflict: A Legal and Ethical Analysis, Polity, Vol. 44, 2012, S. 281f.; Frank Sauer/Niklas Schörnig, Killer Drones: The ›Silver Bullet‹ of Democratic Warfare?, Security Dialogue, Vol. 43, 2012, S. 370. Siehe zur Diskussion Wagner, a.a.O. (Anm. 7), S. 1420.

30 Kenneth Anderson/Matthew Waxman, Law and Ethics for Robot Soldiers, Policy Review, Dezember 2012 und Januar 2013, www.hoover.org/research/law-and-ethics-robot-soldiers

31 Siehe beispielsweise Marco Sassòli, Autonomous Weapons and International Humanitarian Law: Advantages, Open Technical Questions and Legal Issues to be Clarified, International Legal Studies, Vol. 90, 2014, S. 323.

32 Anderson/Waxman, a.a.O. (Anm. 30).

33 Anderson/Waxman, a.a.O. (Anm. 30). Siehe hierzu auch Noel E. Sharkey, The Evitability of Autonomous Robot Warfare, International Review of the Red Cross, Vol. 94, 2012, S. 787.

34 Siehe insbesondere Campaign to Ban Killer Robots, die eine Reihe von NGOs bündelt: www.stopkillerrobots.org/

Errungenschaften auch im zivilen Bereich von hohem Nutzen sind.[35] Als Vermittlungsversuch hat insbesondere der UN-Sonderberichterstatter über außergerichtliche, summarische oder willkürliche Hinrichtungen Christof Heyns ein Moratorium ins Spiel gebracht.[36] Diese innerstaatlichen Moratorien sollen die Phase bis zur Festlegung eines völkerrechtlich verbindlichen Rahmens für AWS überbrücken, der von einem interdisziplinär zusammengesetzten Gremium ausgearbeitet werden soll. Ein solches Moratorium soll unter anderem Folgendes untersagen: Die Durchführung von Testverfahren, die Produktion, den Bau, den Erwerb sowie den Einsatz von AWS. Der derzeit fehlende rechtliche Rahmen rechtfertige ein solches Vorgehen, wobei dieses Argument stärker auf den politischen Willen von Staaten abzuzielen scheint. Bislang ist jedoch nicht ersichtlich, dass dieser Vorschlag breites Gehör gefunden hat.

Die Vorschläge zur Zukunft der AWS lassen sich in drei Kategorien unterteilen und reichen von Ächtung bis hin zu milden Kontrollmechanismen.

Die Debatte hat sich in eine Richtung verschoben, die eine Regulierung von AWS zum Ziel hat. Die Ansätze unterscheiden sich dabei im Grad der Kontrolle, die über AWS ausgeübt werden soll. Unter dem Schlagwort ›sinnvolle menschliche Kontrolle‹ (meaningful human control) lassen sich die Bemühungen im Rahmen des Übereinkommens über das Verbot oder die Beschränkung des Einsatzes bestimmter konventioneller Waffen, die übermäßige Leiden verursachen oder unterschiedslos wirken können (CCW), zusammenfassen.[37] Die Offenheit der Formulierung könnte eine Einigung auf internationaler Ebene erleichtern und als Einfallstor für weitere Regulierung dienen. Es ist jedoch noch völlig unklar, was unter einer ›sinnvollen menschlichen Kontrolle‹ zu verstehen ist. Weitgehende Einigkeit scheint insofern zu bestehen, dass die Tötung von Menschen immer unter menschlicher Kontrolle stattzufinden hat. Es scheint leicht möglich, dass Staaten dies unterschiedlich interpretieren: von einer strikten Kontrolle, bei der jeglicher Waffeneinsatz von einem Menschen gesteuert werden muss, bis hin zu einer reinen Überwachungsfunktion, in der, wenn überhaupt, ein Mensch eingreifen muss, um den Waffeneinsatz zu verhindern. Abhängig davon, wie viele AWS von einem Menschen zu kontrollieren sind und wie komplex die Kampfsituation ist, kann man sich vorstellen, dass die Kontrolldichte dabei gering ausfällt. Der Ansatz des US-Verteidigungsministeriums, der eine ›angemessene menschliche Beurteilung‹ (appropriate levels of human judgment) als Maßstab festlegt,[38] ist wohl mit einem solch weiten Verständnis einer ›sinnvollen menschlichen Kontrolle‹ gleichzusetzen. Es gibt derzeit keinerlei Einigkeit über die Frage, wo auf dem soeben beschriebenen Spektrum die Grenze von rechtlicher Zulässigkeit zur rechtlichen Unzulässigkeit anzusiedeln ist. Klar scheint, dass die von den USA vertretene Ansicht zu weit geht, da die Angemessenheit eines Einsatzes, wie oben schon beschrieben, stark von den Umständen des Einzelfalls abhängt und nur bedingt objektivierbar ist.

Unter dem Schlagwort ›sinnvolle menschliche Kontrolle‹ lassen sich die Bemühungen im Rahmen des Übereinkommens über das Verbot oder die Beschränkung des Einsatzes bestimmter konventioneller Waffen (CCW) zusammenfassen.

Für eine noch geringere Kontrolle plädieren Vorschläge, welche die Entwicklung von AWS nicht oder nur eng begrenzt einschränken wollen.[39] Dieser Ansatz erfolgt vor dem Hintergrund einer großen Offenheit gegenüber neuen technologischen Errungenschaften und verfolgt das Ziel der (Nicht-)Regulierung durch unverbindliche Richtlinien.

Schlussbetrachtung

Auch wenn nicht zu erwarten ist, dass AWS in naher Zukunft Menschen in großem Maßstab in kriegerischen Auseinandersetzungen ersetzen werden, bedarf es einer Befassung mit dieser Thematik auf breiter gesellschaftlicher Ebene. Die Vorteile von Autonomie im zivilen Bereich sind vielversprechend, auch wenn sie zweifelsohne mit eigenen Problem behaftet ist. Inwieweit jedoch der Prozess einer weiteren Autonomisierung von Kriegswaffen wünschenswert ist, ob Entscheidungen über den Einsatz von Waffen und mithin über Leben und Tod aufgrund eines Algorithmus getroffen werden sollen und wer die Verantwortung für ihren Einsatz trägt, sind Fragen, die Vorrang vor technischen Möglichkeitserwägungen haben sollten. Auch wenn aus den genannten Gründen ein Moratorium nicht erfolgversprechend sein mag, ist der zugrunde liegende Gedanke der Vorsorge zu begrüßen und eine vertiefte Debatte wünschenswert.

35 Rebecca Crootof, The Killer Robots Are Here: Legal and Policy Implications, Cardozo Law Review, Vol. 36, 2015, S. 1883ff.

36 UN Doc. A/HRC/23/47, a.a.O. (Anm. 28), S. 22.

37 United Nations, 2015 Meeting of Experts on LAWS, www.unog.ch/80256EE600585943/(httpPages)/6CE049BE22EC75A2C1257C8D0o513E26?OpenDocument

38 United States Department of Defense, a.a.O. (Anm. 11).

39 Arkin, a.a.O. (Anm. 11); Anderson/Waxman, a.a.O. (Anm. 30).

Aus dem Bereich der Vereinten Nationen

Sozialfragen und Menschenrechte

Beratender Ausschuss des Menschenrechtsrats: 14. und 15. Tagung 2015

- **Zwei Fortschrittsberichte vorgelegt**
- **›Geierfonds‹ und Menschenrechte**
- **Selbstverständnis als Ideengeber behauptet**

Norman Weiß

(Dieser Beitrag setzt den Bericht von Norman Weiß, Beratender Ausschuss des Menschenrechtsrats: 12. und 13. Tagung 2014, VN, 5/2015, S. 226, fort.)

Der **Beratende Ausschuss (Advisory Committee – AC)** des **UN-Menschenrechtsrats (MRR)** besteht aus 18 in ihrer persönlichen Eigenschaft tätigen Sachverständigen. Das Gremium kommt in der Regel zu zwei Tagungen im Jahr für maximal zehn Arbeitstage in Genf zusammen. Der AC soll den Menschenrechtsrat der Vereinten Nationen durch die Bereitstellung von Expertenwissen unterstützen, erstellt nach Aufforderung durch den Rat wissenschaftliche Studien und berät ihn forschungsbasiert. Im Jahr 2015 kam der AC zu zwei Tagungen in Genf zusammen: vom 23. bis 27. Februar (14. Tagung) und vom 10. bis 14. August 2015 (15. Tagung). Im Folgenden werden die wichtigsten Ergebnisse beider Tagungen thematisch zusammengefasst.

Zwei Arbeitsgruppen legten ihre Fortschrittsberichte vor, die diskutiert wurden und im Lichte der Beratungen abgeschlossen werden sollen: Dies betrifft die Förderung von Menschenrechten durch Sport und das Olympische Ideal (Empfehlung 14/1) und das Thema Menschenrechte und Kommunalverwaltung (Empfehlung 14/2). Die Arbeit am Thema Unbegleitete minderjährige Flüchtlinge (Empfehlung 15/2) wurde weitergeführt. Auf Empfehlung des MRR wurde ein neues, im vergangenen Jahr vom AC angeregtes Thema in Angriff genommen: ›Geierfonds‹ (vulture funds) und Menschenrechte (Empfehlung 14/3); der AC setzte zunächst eine Arbeitsgruppe ein. Als ›Geierfonds‹ werden Hedgefonds und Private Equity Fonds bezeichnet, die auf den Erwerb von Anleihen und Aktien zahlungsfähiger Unternehmen und Staaten spezialisiert sind. Der Beratende Ausschuss diskutierte mögliche Auswirkungen dieser Aktivitäten auf die Menschenrechte während der 14. Sitzung auf der Grundlage eines Konzeptpapiers und der Stellungnahme externer Expertinnen und Experten. Es solle der Entwurf eines Fortschrittsberichts fertiggestellt werden, der dem MRR in seiner 31. Sitzung vorzulegen sei. Mit Empfehlung 15/1 nahm er dann den Entwurf eines Fortschrittsberichts zur Kenntnis und bat den UN-Menschenrechtsrat um eine Verlängerung der Befassungszeit bis Herbst 2016.

Der AC entschied mit Empfehlung 14/4, seine Rolle als Think Tank ernster zu nehmen und sich hierfür verstärkt Anregungen aus der Wissenschaft und der Zivilgesellschaft zu holen. Darüber hinaus möchte er eventuelle thematische Lücken in der Tätigkeit des MRR identifizieren und darauf aufbauende Problemskizzen erarbeiten sowie diese in einer Reihe von Reflexionspapieren (reflection paper series) veröffentlichen. Dies wurde in den Empfehlungen 15/4 und 15/5 konkretisiert. Da dieses Thema bereits im Jahr 2014 (Empfehlung 13/8) behandelt wurde, hat sich das Selbstverständnis, als Ideengeber zu fungieren, erkennbar behauptet.

Auf der 15. Tagung im August wurde ein vorläufiger Entwurf diskutiert, der mögliche thematische Lücken in der Arbeit des Menschenrechtsrats identifizierte. Außerdem wurden die in Empfehlung 14/5 in Auftrag gegebenen ersten Problemskizzen als neue Forschungsvorschläge präsentiert: Whistleblowing und Menschenrechte, Klimaflucht und Menschenrechte, Menschenrechte als Querschnittsthema in der Post-2015-Entwicklungsagenda, regionale Menschenrechtsschutzmechanismen und die Einrichtung eines globalen Beschwerdeforums für Fälle von Blasphemie. Diese wurden zur Kenntnis genommen und sollen weiter diskutiert werden. Gleichzeitig wurden mit Empfehlung 15/5 weitere erste Problemskizzen in Auftrag gegeben: Zum Einfluss von Siedlerkolonialismus auf Menschenrechte, zum ideellen Ansatz von sozialen Rechten im Rahmen nachhaltiger Entwicklung sowie zu Jugend und Menschenrechten. Ausdrücklich soll auch eine Problemskizze zum Thema ›Erhöhung der Bedeutung des Menschenrechtsrats: Effizienz – Effektivität – Umsetzung – Follow-up‹ angefertigt werden.

Auf den ersten Blick fällt die Arbeit des Beratenden Ausschusses im Jahr 2015 mager aus, da sich alle Arbeiten noch im Vorschlags-, Entwurfs- und Bearbeitungsstadium befinden. Bei genauerem Hinsehen zeigt sich jedoch, dass der Ausschuss an den durchaus wichtigen Themen Menschenrechte und Kommunalverwaltung, Unbegleitete minderjährige Flüchtlinge sowie ›Geierfonds‹ und Menschenrechte weiterarbeitet. Diese betreffen unterschiedliche Aspekte von Menschenrechtsverletzungen, können aber auch Möglichkeiten der Prävention in den Blick nehmen. Dazu gehören eine gute Verwaltungsführung und verantwortungsvolles Wirtschaften, beides wichtige Elemente einer Staats- und Gesellschaftstruktur, die Menschenrechte achtet und schützt.

Der Beratende Ausschuss sieht sich – das wurde auf beiden Sitzungen des Jahres 2015 deutlich – als Diskussionsforum und Ideengeber. Dass dabei auch recht spezifischen Fragestellungen nachgegangen wird, zeigen die Vorschläge, sich mit dem Einfluss von Siedlerkolonialismus auf die Menschenrechte und einem globalen Beschwerdeforum für Fälle von Blasphemie zu befassen. Die Verknüpfung von klima- und entwicklungspolitischen Fragestellungen mit dem Thema Jugend zeigt eine sinnvolle, langfristig orientierte Perspektive auf, die bei aller Notwendigkeit, sich mit tagesaktuellen Fragestellungen befassen zu müssen und zu wollen (Whistleblowing und Menschenrechte, Unbegleitete minderjährige Flüchtlinge), in die richtige Richtung weist.

Menschenrechtsausschuss: 113. bis 115. Tagung 2015

- **Keine Veränderung bei Anzahl ratifizierender Staaten**
- **Verletzungen der Paktrechte durch Russland**
- **Individualbeschwerden gegen Abschiebungen von Beschwerdeführenden**

Birgit Peters

(Dieser Beitrag setzt den Bericht von Birgit Peters, Menschenrechtsausschuss: 110. bis 112. Tagung 2014, VN, 4/2015, S. 180f., fort.)

Im Jahr 2015 trafen sich die 18 Expertinnen und Experten des **Menschenrechtsausschusses (Committee on Civil and Political Rights – CCPR)**, dem Organ, das über die Einhaltung der Verpflichtungen der Mitgliedstaaten des Internationalen Paktes über bürgerliche und politische Rechte (kurz: Zivilpakt) wacht, wie gewohnt zu drei Tagungen in Genf (113. Tagung: 16. März bis 2. April; 114. Tagung: 29. Juni bis 24. Juli; 115. Tagung: 19. Oktober bis 6. November 2015). Nachdem die Amtszeit zahlreicher Ausschussmitglieder Ende 2014 ausgelaufen war, kam der CCPR im Jahr 2015 in neuer Besetzung zusammen. Wiedergewählt wurden Yadh Ben Achour (Tunesien), Yuji Iwasawa (Japan) und Margo Waterwal (Suriname). Neu in den Ausschuss gewählt wurden Sarah Cleveland (USA), Olivier de Frouville (Frankreich), Ivana Jelic (Montenegro), Duncan Laki Muhumuza (Uganda), Mauro Politi (Italien) und Photini Pzartzis (Griechenland).

Auch dieses Mal nutzten die Ausschussmitglieder die durch die UN-Generalversammlung im Jahr 2014 zugebilligte zusätzliche Sitzungszeit, um über die anhängigen Individualbeschwerden zu entscheiden. Dabei kann der Ausschuss erste Erfolge verbuchen: Während zu Beginn des Jahres 2015 noch 456 Beschwerden vor dem Ausschuss anhängig waren, konnte der CCPR im Rahmen der Sitzungen 106 Antworten auf individuelle Beschwerden verfassen und damit die anhängigen Beschwerden auf 350 reduzieren. Allerdings besteht nur begrenzt Hoffnung, dass sich damit die Anzahl der noch anhängigen Beschwerden weiter abbauen lässt. Bis Ende des Jahres 2014 wurden mit 191 neuen Beschwerden doppelt so viele Beschwerden wie im Jahr 2013 registriert. Zwar liegen für das Jahr 2015 noch keine Zahlen vor, sodass nicht einzuschätzen ist, ob es sich dabei um ein einmaliges Hoch oder einen Trend handelt. Dennoch stellt die Handhabung und Entscheidung über die anhängigen Individualbeschwerden den CCPR vor große Herausforderungen. Möglicherweise könnte hier die Einführung von Pilotentscheidungen helfen, wie sie bereits vor dem Europäischen Gerichtshof für Menschenrechte (EGMR) üblich sind. Sie erlauben die Bescheidung einer Vielzahl ähnlich gelagerter Fälle in einem einzigen Verfahren. Doch werden auch andere Vertragsorgane, wie der Ausschuss gegen Folter (CAT) oder der Ausschuss für die Beseitigung der Rassendiskriminierung (CERD), verstärkt von Individualklägerinnen und -klägern in Anspruch genommen. Insofern stellt sich die Frage, ob der zu Beginn dieses Millenniums vorgebrachte Vorschlag eines Weltgerichtshofs für Menschenrechte nicht erneut diskutiert werden sollte (beispielsweise dazu: Manfred Nowak, Ein Weltgerichtshof für Menschenrechte, VN, 5/2008, S. 205–211). Er könnte nicht nur die Verfahrensvoraussetzungen für die Annahme von Beschwerden vereinheitlichen, sondern würde auch als einzig zuständiges Organ über Individualbeschwerden zur Verletzung der Menschenrechtspakte entscheiden.

Die Anzahl der Staaten, die den Zivilpakt ratifiziert hat, blieb im Vergleich zum Vorjahr unverändert. 168 Staaten sind Mitglied des Paktes. 115 Staaten haben das erste Fakultativprotokoll des Zivilpakts, das die Individualbeschwerde erlaubt, ratifiziert. Auch diese Zahl blieb im Jahr 2015 unverändert. Ebenso sind dem zweiten Fakultativprotokoll, das die Todesstrafe verbietet, keine neuen Mitglieder beigetreten. Die Anzahl der Vertragsstaaten blieb auch hier unverändert bei 81.

Staatenberichte

Auf seiner 113. Tagung beschäftigte sich der Ausschuss mit den Staatenberichten der Côte d'Ivoire, Kambodschas, Kroatiens, Monacos, Russlands und Zyperns. Im Rahmen der 114. Tagung verfasste der CCPR Abschließende Bemerkungen zu den Staatenberichten Frankreichs, Kanadas, Mazedoniens, Spaniens, Usbekistans, Venezuelas und des Vereinigten Königreichs. Schließlich diskutierten die 18 Expertinnen und Experten des Ausschusses auf ihrer 115. Sitzung die Staatenberichte Benins, Griechenlands, Iraks, der Republik Korea, Österreichs, San Marinos und Surinams. Beispielhaft soll hier auf die Abschließenden Bemerkungen zu den Berichten Russlands, Venezuelas und Österreichs eingegangen werden.

Russland hatte dem CCPR seinen siebten Staatenbericht zur 113. Tagung vorgelegt. Der CCPR lobte legislative Reformen, insbesondere Erleichterungen für die Registrierung politischer Parteien, sowie den Beitritt zum Übereinkommen über die Rechte von Menschen mit Behinderungen sowie zum Fakultativprotokoll zum Übereinkommens über die Rechte des Kindes betreffend den Verkauf von Kindern, die Kinderprostitution und die Kinderpornografie. Der Ausschuss zeigte sich jedoch besorgt über die Haltung und Handlungen Russlands in der Donbass-Region sowie in Südossetien. Der Ausschuss betonte, Russland übe dort erheblichen Einfluss aus, der mit effektiver Kontrolle gleichzusetzen sei. Daher solle der Staat auch die Verantwortung für die dortigen Verletzungen der Paktrechte übernehmen. Auch bezüglich der Autonomen Republik Krim mahnte der Ausschuss die Verantwortung Russlands an. Dem Staat seien die dortigen Verletzungen der Paktrechte, insbesondere durch gewaltsames Verschwindenlassen, Entführungen, die willkürliche Inhaftierung der ›Krim-Verteidigungsgruppen‹ sowie die Misshandlung und Einschüchterung von Journalistinnen und Journalisten, zuzurechnen. Darüber hinaus gebe es in Russland zahlreiche weitere Fälle von Verstößen gegen die Paktrechte, etwa im Bereich der Diskriminierung von Minderheiten, von Trans- und Homosexuellen oder im Bereich der Selbstbestimmungs- und Verwaltungsrechte indigener Bevölkerungsgruppen. Russland solle die Verantwortung für diese Verletzungen übernehmen und sie rückhaltlos aufklären.

Hinsichtlich des vierten Staatenberichts **Venezuelas** zur 114. Tagung des CCPR hob der Ausschuss hervor, dass der Staat diverse legislative Initiativen zur Verbesserung der Garantie der Paktrechte getroffen habe. So wurde ein Ministerium für die Angelegenheiten indigener Bevöl-

kerungsgruppen eingerichtet sowie eines für Frauen und die Gleichbehandlung der Geschlechter. Dennoch seien die Rechte indigener Gruppen nach Artikel 27 des Paktes gefährdet, insbesondere dann, wenn es um den Abbau von Rohstoffen in Venezuela gehe. Der CCPR habe keine Informationen darüber erhalten, dass indigene Gruppen bei staatlichen Beschlüssen zur Durchführung von Projekten zum Rohstoffabbau beteiligt worden seien. Auch gebe es keine Anzeichen dafür, dass die betroffenen Bevölkerungen diesen Projekten hätten zustimmen können. Schließlich seien nichtstaatliche Organisationen (NGOs), die dem CCPR Kommentare zum Bericht Venezuelas gesendet hätten, durch den Präsidenten der Nationalversammlung öffentlich diskreditiert worden. Dies verletze das im Pakt nach Artikel 19 garantierte Recht auf freie Meinungsäußerung.

Österreich reichte seinen fünften Staatenbericht vor der 115. Tagung ein. Die Expertinnen und Experten zeigten sich erfreut über ein neues Gesetz, das die Diskriminierung von Lesben, Schwulen, Bisexuellen und trans- und intergeschlechtlichen Menschen (LSBTI) verbietet. Auch habe Österreich Folter als eigenständiges Verbrechen im Strafgesetzbuch anerkannt. Besorgnis äußerten die Expertinnen und Experten gegenüber der geringen Anzahl von Frauen, die politische Ämter oder Aufsichtsratspositionen bekleideten. Hier solle der Staat Maßnahmen ergreifen. Ebenso habe Österreich eine gestiegene Anzahl von Fällen rassistischer Propaganda gegen Minderheiten wie Roma, Juden, Migrantinnen und Migranten sowie Asylsuchende zu verzeichnen. Dazu seien diese Gruppen im politischen wie im privaten Leben in Führungspositionen unterrepräsentiert. Schließlich gebe es Berichte, dass die österreichische Polizei sogenannte ›ethnische Profilerstellungen‹ durchführe und gezielt Personen aufgrund ihrer Herkunft oder Hautfarbe im Zusammenhang mit Verdachtsmomenten über verübte oder geplante Straftaten überprüfe. Österreich müsse Maßnahmen ergreifen, die gegen die Verbreitung rassistischer Meinungen vorgingen. Minderheiten müssten ermuntert werden, sich stärker im öffentlichen Leben zu engagieren. Die ›ethnische Profilerstellung‹ hingegen verstoße gegen den Gleichbehandlungsgrundsatz. Daher müsse Österreich hier klare Mittel ergreifen, um diese Maßnahmen zu unterbinden.

Individualbeschwerden gegen geplante Abschiebungen

Auf allen drei Tagungen behandelte der CCPR zahlreiche Fälle gegen europäische Staaten, Australien und Neuseeland, die Abschiebungen von Beschwerdeführenden in ihre Heimatstaaten betrafen. Probleme aus der gegenwärtigen globalen Migrationsbewegung werden dementsprechend auch vor dem CCPR virulent.

Es ist eine allgemein anerkannte Auslegung, dass die Abschiebung oder Rückführung einer Person in ein Land, in dem sie einer ernsthaften Gefahr durch drohende Folter oder unmenschliche Behandlung ausgesetzt ist, eine Verletzung des Folterverbots und des Verbots unmenschlicher Behandlung darstellt. Dies ist in Artikel 7 des Zivilpakts garantiert. Auch der Ausschuss hat diese Auslegung von Artikel 7 in seiner allgemeinen Bemerkung Nr. 31 zu Artikel 7 des Paktes anerkannt. Allerdings hat der Ausschuss dort auch dargelegt, dass die Gefahr die Beschwerdeführenden persönlich treffen und eine ernsthafte Gefahr irreparabler Schäden bestehen müsse. Dazu sei die allgemeine Menschenrechtssituation in dem Land zu bewerten, in das der oder die Beschwerdeführende zurückgeführt werden solle.

In einigen Fällen war das Vorbringen einer solchen Gefahr unbegründet. Im Fall Z gegen Dänemark betonte der Ausschuss, die Entscheidung der dänischen Behörden über die Abschiebung des Beschwerdeführenden obliege den Staaten. Um einen Verstoß gegen Artikel 7 geltend zu machen, müsse der Beschwerdeführende beweisen, dass die Entscheidung willkürlich und unvernünftig gewesen ist.

Dagegen sah der Ausschuss die Voraussetzungen einer Gefährdung der Beschwerdeführerin im Fall Osayi Omo-Amenaghawon gegen Dänemark als gegeben an. Hier hatte die Beschwerdeführende geltend gemacht, sie sei als Opfer einer gewaltsamen Verschleppung nach Dänemark gelangt und dort zur Prostitution gezwungen worden. Sie habe später in einem Strafprozess gegen die Täter ausgesagt und müsse befürchten, dass die Täter selbst oder ihre Komplizen sie bei einer Rückkehr nach Nigeria bedrohen würden. Da die dänischen Behörden den Asylantrag von Omo-Amenaghawon ausschließlich aufgrund der allgemeinen Menschenrechtslage in Nigeria und nicht nach der speziellen Situation und Schutzbedürftigkeit von Omo-Amenaghawon als Opfer einer Verschleppung beurteilt hätten, sah der Ausschuss Artikel 7 des Zivilpakts verletzt.

Abgesehen von einer Verletzung von Artikel 7 kann bei Abschiebungen auch eine Verletzung des Rechts auf Familie von Beschwerdeführenden nach Artikel 17 vorliegen. Dies ist etwa der Fall, wenn ein Staat verweigert, einem Familienmitglied Aufenthalt auf seinem Staatsgebiet zu gewähren. Der Fall von Mansour Leghaei und anderen gegen Australien illustriert eine solche Situation. Dabei handelt es sich um einen iranischen Familienvater, der im Jahr 2010 von Australien nach Iran abgeschoben werden sollte. Seine Tochter wurde in Australien geboren, seine beiden Söhne hatten die australische Staatsangehörigkeit. Zum Zeitpunkt der Ausweisung war die Tochter des Beschwerdeführers noch minderjährig. Leghaei war zunächst im Jahr 1994 mit einem temporären Visum nach Australien eingereist. Er hatte im Jahr 1996 eine dauerhafte Aufenthaltserlaubnis sowie den Nachzug seiner Familie nach Australien beantragt. Dies wurde ihm durch die zuständigen Behörden verweigert. Diese beriefen sich auf eine Entscheidung des australischen Verfassungsschutzes, nachdem der Beschwerdeführende eine Bedrohung für die nationale Sicherheit darstelle. Die Originaldokumente, die Grundlage dieser Entscheidung waren, wurden dem Beschwerdeführer nicht zur Verfügung gestellt und die Gründe für die Entscheidung des Verfassungsschutzes wurden Leghaei nicht mitgeteilt. Dazu erfuhr Leghaei über die gesamte Zeit seines Aufenthalts in Australien nie, dass er eine Gefährdung für die australische Sicherheit darstelle. Der Ausschuss entschied, dass der Beschwerdeführende langfristige Familienbindungen in Australien etabliert habe. Seine alleinige Ausweisung bedeute ein Auseinanderreißen der Familie. Für seine Ausweisung habe der australische Staat keine triftigen Gründe angeführt, die einen derartig schweren Eingriff in das Familienleben des Beschwerdeführenden rechtfertigen würden. Der Ausschuss sah daher Artikel 17 des Zivilpakts verletzt.

Rechte des Kindes: 68. bis 70. Tagung 2015

- **Somalia tritt Übereinkommen bei**
- **USA einziger Staat, der Kinderrechtskonvention nicht ratifiziert hat**
- **Erste Beschwerde nach Mitteilungsverfahren geprüft**

Stefanie Lux

(Dieser Beitrag setzt den Bericht von Stefanie Lux über die 65. bis 67. Tagung 2014, VN, 3/2015, S. 133f., fort.)

Seit Ende der neunziger Jahre war in vielen Kommentaren zum Übereinkommen zu lesen, alle Staaten außer Somalia und den Vereinigten Staaten von Amerika hätten das **Übereinkommen über die Rechte des Kindes** (kurz: **Kinderrechtskonvention**) ratifiziert. Lediglich aufgrund der Ratifizierung des Übereinkommens durch neu anerkannte Staaten wie Montenegro, Palästina, Timor-Leste und zuletzt Südsudan im Januar 2015 änderte sich die Anzahl der Beitrittsstaaten. 25 Jahre nach dem Inkrafttreten des Übereinkommens trat Somalia der Kinderrechtskonvention im Oktober 2015 bei. Nach dem Sturz von Mohamed Siad Barre im Jahr 1991 hatte Somalia viele Jahre keine funktionierende Zentralregierung, die das Übereinkommen hätte ratifizieren können. Die nach Verabschiedung der Verfassung im Jahr 2012 gewählte Regierung unter Hassan Sheikh Mohamud wird zunehmend international anerkannt. Mittlerweile hat die Regierung nicht nur die Kinderrechtskonvention, sondern auch das Übereinkommen zur Beseitigung der schlimmsten Formen der Kinderarbeit der Internationalen Arbeitsorganisation (International Labour Organisation – ILO) ratifiziert. Kinderrechtsexpertinnen und -experten zeigten sich trotzdem enttäuscht, da Somalia in einem weitreichenden Vorbehalt erklärt hatte, nicht an Bestimmungen der Kinderrechtskonvention gebunden zu sein, die nicht mit den Prinzipien der islamischen Scharia vereinbar sind. Menschenrechtsexpertinnen und -experten und die Ausschüsse der UN-Menschenrechtsverträge, wie hier der **Ausschuss für die Rechte des Kindes (CRC)**, halten diese Vorbehalte für unzulässig.

Nach den Beitritten Südsudans und Somalias sind die USA nunmehr der weltweit einzige Staat, der die Kinderrechtskonvention nicht ratifiziert hat. Die Regierung hatte das Übereinkommen bereits im Jahr 1995 unterzeichnet, allerdings kam die für die Ratifizierung notwendige Zweidrittelmehrheit im Senat bisher nicht zustande. Aus völkerrechtlicher Perspektive wird jetzt die Frage interessant, ob es sich bei einem Menschenrechtsübereinkommen, das alle Staaten bis auf einen weltweit ratifiziert haben, nicht bei einem großen Teil seiner Bestimmungen um Völkergewohnheitsrecht handelt. Wäre dies der Fall, könnten diese Bestimmungen auch für die USA bindend sein. Die einzigen Konventionen seit Ende des Zweiten Weltkriegs, die universell ratifiziert wurden, sind die Genfer Konventionen aus dem Jahr 1949. Deren Inhalte werden gemeinhin als Völkergewohnheitsrecht betrachtet.

Auch den im Jahr 2000 verabschiedeten Protokollen zur Kinderrechtskonvention ist bereits eine große Mehrheit der Staaten beigetreten: Bis Ende 2015 hatten 162 Staaten das Protokoll betreffend die Beteiligung von Kindern in bewaffneten Konflikten (OPAC) und 171 das Protokoll betreffend Kinderhandel, Kinderprostitution und Kinderpornografie (OPSC) ratifiziert. Zudem waren Ende 2015 22 Staaten dem im Jahr 2012 verabschiedeten Protokoll betreffend ein Mitteilungsverfahren beigetreten, zuletzt Argentinien, Chile, Finnland, Tschechien und die Mongolei.

Mitteilungsverfahren

Auf seiner 69. Tagung entschied der Ausschuss das erste Mal über eine Mitteilung entsprechend dem im Jahr 2014 in Kraft getretenen dritten Fakultativprotokoll. Im Fall Abdul-Hamid Aziz gegen Spanien hatte der Beschwerdeführer geklagt, die spanischen Behörden hätten ihm den speziellen Schutz für Minderjährige verwehrt, da Mediziner ihn auf älter als im Pass angegeben geschätzt hatten. Der Ausschuss lehnte die Beschwerde als nicht zulässig ab, da sowohl die Ereignisse als auch alle richterlichen Entscheidungen vor Inkrafttreten des Protokolls in Spanien lagen. Nach Artikel 7 des Protokolls sind Mitteilungen nicht zulässig, die auf Tatsachen basieren, die vor Inkrafttreten des Protokolls eingetreten sind.

Auf seinen drei Tagungen im Jahr 2015 (68. Tagung: 12.1.–30.1., 69. Tagung: 18.5.–5.6. und 70. Tagung: 14.9.–2.10.2015) prüfte der Ausschuss insgesamt 44 Berichte, 24 zum Übereinkommen, zehn zum OPAC und zehn zum OPSC. Von den Berichten sollen im Folgenden jeweils einer exemplarisch vorgestellt werden.

68. Tagung

Auf der Frühjahrstagung prüfte der Ausschuss die Berichte aus der Dominikanischen Republik, Gambia, Irak, Jamaika, Kolumbien, Mauritius, Schweden, der Schweiz, Tansania, Turkmenistan und Uruguay. Zudem behandelte er die Berichte aus Kambodscha, Irak, Turkmenistan und Uruguay zum OPAC und OPSC sowie den Schweizer Bericht zum OPSC.

Bei Prüfung des Berichts aus der **Schweiz** bemängelte der Ausschuss die Übersetzung des zentralen Grundprinzips des Übereinkommens ›best interest of the child‹ in den deutschen Begriff ›Wohl des Kindes‹. Nach Einschätzung des CRC stimmt die Terminologie nicht überein, die ungleiche Bedeutung könne damit zu Unterschieden in der Umsetzung und Anwendung des Prinzips führen. Positiv bewertete der Ausschuss Kostenvergünstigungen bei den Krankenversicherungsprämien für Kinder aus Familien mit mittleren und niedrigen Einkommen. Jedoch sei in der Schweiz die kinderärztliche Versorgung zu stark zentralisiert und es fehle an Kinderärzten. Zudem seien die zunehmenden Übergewichts- und Fettleibigkeitsprobleme besorgniserregend. Sehr kritisch äußerte sich der CRC zur fehlenden Reglementierung des Einsatzes von Babyklappen und der damit einhergehenden steigenden Anzahl von Babyklappen. Diese Möglichkeit, Neugeborene anonym abzugeben, stelle einen Verstoß gegen die Artikel 6, 7, 8, 9 und 19 des Übereinkommens dar. Gesetzesänderungen zur Aufnahme von Pflegekindern wurden von den Sachverständigen gelobt. Sie bemängelten jedoch die fehlenden Daten und Informationen zu Kindern in Heimen und Pflegefamilien. Darüber hinaus gebe es bedeutende kantonale Unterschiede bei den Kriterien zur Auswahl der Familien und Dauer des Aufenthalts sowie der Qualität der Unterstützung und Begleitung der Pflegefamilien. Unverständnis äußerte der Ausschuss darüber, dass bei Kindern unter drei Jahren nur eine Heimunterbringung möglich ist und leibliche Eltern bei

Rückkehr des Kindes nur begrenzt Unterstützung erhalten. Trotz gesetzlicher Neuerungen im Jugendstrafrecht blieb der Ausschuss in seiner Bewertung kritisch. Zwar wurde das Alter für die Strafmündigkeit im Jahr 2007 von sieben auf zehn Jahre erhöht, dies liege aber weiterhin unter den international akzeptierten Standards. Seit dem Jahr 2001 regelt das Jugendstrafprozessrecht, dass Kinder während einer Untersuchungshaft und im Strafvollzug von erwachsenen Inhaftierten zu trennen sind. Dies, so der Ausschuss, sei nicht immer der Fall.

69. Tagung

Auf der Sommertagung behandelte der CRC die Berichte aus Äthiopien, Eritrea, Ghana, Honduras, Mexiko und den Niederlanden zur Kinderrechtskonvention. Mit Honduras und Laos wurden die Berichte zum OPAC und zum OPSC diskutiert. Zudem wurden der Bericht von Israel zum OPSC sowie der niederländische Bericht zum OPAC erörtert.

In **Äthiopien** wurden sowohl in der nationalen Menschenrechtskommission (Ethiopian Human Rights Commission) als auch bei der Institution des Bürgerbeauftragten (Ethiopian Institution of the Ombudsman) Abteilungen für Kinderrechte eingerichtet. Der Ausschuss lobte diese Entwicklung, bemängelte jedoch die fehlenden Informationen zur personellen und finanziellen Ausstattung dieser Gremien sowie zur Anzahl der behandelten Beschwerden und durchgeführten Untersuchungen. Zudem sei es sehr bedenklich, dass Kinder nur über ihre Eltern oder Erziehungsberechtigten eine Beschwerde vorbringen können. Dies sei besonders problematisch, wenn die Eltern die Rechte des Kindes verletzt haben. Die wirtschaftliche Entwicklung und entschlossenen Schritte zur Armutsbekämpfung im Land nahm der CRC positiv zur Kenntnis, zeigte sich jedoch besorgt über negative Auswirkungen von großen Investitionen und Projekten auf die Kinderrechte. Insbesondere kritisierten die Sachverständigen die Zwangsvertreibung von indigenen Familien in den Regionen Gambella, Benishangul-Gumuz, Somali und Afar, um Platz für große Agrarvorhaben zu schaffen.

Äthiopien hat mit der Errichtung einer Behörde zur Registrierung von Zivilstandsangelegenheiten wichtige Fortschritte in Sachen Geburtenregister zu verzeichnen. Der Ausschuss lobte die Entwicklung und riet, die Anstrengungen zu verstärken, da weiterhin in ländlichen Gebieten nur fünf Prozent aller Kinder über Geburtsurkunden verfügen würden. Positiv bewerte man die Bemühungen der Regierung, durch legislative Reformen und Aufklärungskampagnen die Beseitigung von schädlichen Praktiken wie weiblicher Genitalverstümmelung zu erreichen. Der Ausschuss zeigte sich äußerst besorgt über die weiterhin sehr hohe Anzahl von Mädchen, die Genitalverstümmelung erleiden. Dies zeige, dass das gesetzliche Verbot nicht ausreichend durchgesetzt werde. Er forderte die Regierung mit Nachdruck dazu auf, entsprechende Gesetze streng anzuwenden und dafür zu sorgen, dass die Täter strafrechtlich verfolgt und verurteilt werden. Im Bildungsbereich äußerte sich der CRC anerkennend zu den ansteigenden Einschulungsraten im Grundschulalter, der Förderung des Zugangs von Mädchen zu Schulbildung sowie der Entwicklung neuer Ausbildungsprogramme für Lehrer und insbesondere Lehrerinnen. Negativ wurde bewertet, dass das Recht auf kostenfreie verpflichtende Schulbildung noch nicht gesetzlich festgeschrieben ist und große regionale Unterschiede bei den Einschulungsraten bestehen.

70. Tagung

Auf seiner Herbsttagung beschäftigte sich der Ausschuss mit den Berichten aus Bangladesch, Brasilien, Chile, Kasachstan, Polen, Timor-Leste und den Vereinigten Arabischen Emiraten. Mit Kuba und Madagaskar besprach der CRC zudem die Berichte zum OPAC und zum OPSC sowie mit Brasilien den Bericht zum OPAC.

Bei Prüfung des Berichts aus **Brasilien** setzte sich der Ausschuss unter mehreren Gesichtspunkten mit der weit verbreiteten Gewalt gegen Kinder auseinander. Brasilien hat die weltweit höchste Rate an Tötungsdelikten gegen Kinder; die meisten Opfer sind männliche afro-brasilianische Jugendliche. Die Regierung hat zwar ein Programm für den Schutz von Kindern und Jugendlichen, deren Leben bedroht wird, verabschiedet. Der CRC forderte sie jedoch nachdrücklich dazu auf, entsprechende Programme zu verstärken und mit den notwendigen personellen, technischen und finanziellen Ressourcen auszustatten. Gleichzeitig äußerte sich der Ausschuss zutiefst besorgt über die hohe Anzahl von Kindern, die Banden angehören, die gezielte Rekrutierung von Kindern durch Banden und die Nutzung von Kindern für die Organisierte Kriminalität. Die Sachverständigen rieten der Regierung, eine umfassende Strategie umzusetzen, um Kinder davon abzuhalten, sich Banden anzuschließen, sowie betroffenen Kindern bei Ausstieg, Rehabilitation und Reintegration zu helfen. Die Regierung solle insbesondere die Ursachen der Rekrutierung wie Armut, Marginalisierung und hohe Schulabbruchraten angehen, Aufklärungskampagnen durchführen und einen im Senat anhängigen Gesetzentwurf zur Strafverschärfung für die Rekrutierung von Kindern durch Banden verabschieden.

Weiterhin setzte sich der CRC sehr kritisch mit der weit verbreiteten Gewalt durch die Militärpolizei und andere Polizeieinheiten, die vor allem gegen Straßenkinder und Kinder in den Armenvierteln gerichtet ist, auseinander. Er nannte unter anderem die Vorfälle im Rahmen der groß angelegten ›Befriedungsaktionen‹ in den Armenvierteln und den Militäreinsatz in Maré in Rio de Janeiro als Beispiele. Die Sachverständigen zeigten sich zutiefst besorgt über die hohe Anzahl an außerrechtlichen Tötungen von Kindern durch Militär- und Zivilpolizei und die weitgehende Straflosigkeit für schwere Kinderrechtsverletzungen. Weiterhin erwähnt wurden Berichte zu Folter und Verschwindenlassen von Kindern, insbesondere bei den Einsätzen in den Armenvierteln, sowie die Anwendung von körperlicher Gewalt, Tränengas und Pfefferspray während Zwangsräumungen für große Infrastrukturprojekte vor der Fußballweltmeisterschaft und den Olympischen Spielen. Die Regierung solle die genannten Fälle schnellstmöglich untersuchen und die Täter strafrechtlich zur Verantwortung ziehen. Der Ausschuss schlug zudem vor, gesetzliche Neuerungen vorzunehmen, um strengere Strafen durchzusetzen.

Positiv bewertete der CRC das im Jahr 2014 in Kraft getretene gesetzliche Verbot der körperlichen Bestrafung von Kindern. Die Ausschussmitglieder äußerten sich jedoch besorgt, dass dieses Verbot nicht ausreichend durchgesetzt wird. Körperliche Bestrafung werde immer noch weithin praktiziert und als Methode zur Disziplinierung von Kindern toleriert.

Rechtsfragen

Internationaler Strafgerichtshof: Tätigkeiten 2015

- Verhinderte Festnahme Omar al-Bashirs in Südafrika
- Ehemaliger Kindersoldat angeklagt
- Ermittlungen im Georgien-Konflikt

Mayeul Hiéramente

(Dieser Beitrag setzt den Bericht von Mayeul Hiéramente, Internationaler Strafgerichtshof, Tätigkeiten 2014, VN, 6/2015, S. 275f., fort. Siehe auch einführenden Beitrag des Autors, VN, 5/2014, S. 195ff.)

Der **Internationale Strafgerichtshof (IStGH)** beginnt ein neues Kapitel. Das Jahr 2015 – 17 Jahre nach der Unterzeichnung des Römischen Statuts zur Gründung des IStGH (**International Criminal Court – ICC**) und 13 Jahre nach Aufnahme der Tätigkeiten in Den Haag – markiert einen Wendepunkt in der Entwicklung des ›Weltstrafgerichts‹. Mit dem Umzug in die neuen Räumlichkeiten hat das Gericht, dem 123 Staaten beigetreten sind, ein architektonisches Zeichen für die Dauerhaftigkeit der internationalen Strafjustiz gesetzt. Nach der Einleitung formeller Ermittlungen zur Situation in Georgien verlässt die Anklage den afrikanischen Kontinent und verschafft dem universellen Geltungsanspruch des Gerichts Ausdruck. Es setzt damit auch inhaltlich ein Zeichen. Doch in Zeiten des Wandels holen den Gerichtshof und die Chefanklägerin Fatou Bensouda einige Verfahren ein, die unter der Ägide des ersten Chefanklägers Luis Moreno-Ocampo angestoßen wurden und das Gericht noch heute vor große Herausforderungen stellen – Herausforderungen, die eine umfassende Unterstützung durch die Weltgemeinschaft erfordern.

Al-Bashir in Südafrika

Das Ermittlungsverfahren gegen den amtierenden sudanesischen Präsidenten Omar al-Bashir ist trotz mangelnder Fortschritte der juristischen Aufarbeitung auch nach mehreren Jahren noch hochbrisant. Es scheint immer mehr zur Belastung des Gerichtshofs zu werden. Al-Bashir, der über Jahre hinweg erfolgreich den Festnahmeersuchen des Haager Gerichts trotzte und jede Kooperation seines Landes mit dem IStGH verweigert, entwickelt sich nach der Einstellung des Verfahrens gegen den kenianischen Präsidenten Uhuru Kenyatta zum größten Gegenspieler des Gerichts auf dem afrikanischen Kontinent. In der Riege der afrikanischen Staatsoberhäupter findet er stärkeren Zuspruch als je zuvor. Gelodert hat der Konflikt zwischen den Machthabern Afrikas und dem Gericht bereits seit Längerem. Aufgeflammt ist er im Jahr 2015 anlässlich eines Besuchs des sudanesischen Präsidenten in Südafrika – eines Unterzeichnerstaats des Römischen Statuts.

Im Hinblick auf ein im Juni 2015 anstehendes Gipfeltreffen der Afrikanischen Union (AU) hatte der Gerichtshof im Mai 2015 die südafrikanischen Behörden darüber in Kenntnis gesetzt, dass der IStGH eine Festnahme al-Bashirs – gegen den seit den Jahren 2009/2010 Haftbefehle vorliegen – erwarte, wenn dieser südafrikanisches Staatsgebiet betrete. Die südafrikanischen Behörden verwiesen ihrerseits auf die Immunität eines amtierenden Staatsoberhaupts vor nationalen Strafverfolgungsbehörden und signalisierten al-Bashir die Möglichkeit der Einreise. Nachdem al-Bashir für den AU-Gipfel eingetroffen war, mahnte der IStGH erneut eine Festnahme an. Diese Mahnung wurde durch die Strafjustiz in Pretoria aufgegriffen, die sich der Forderung der internationalen Richter anschloss. Während allerdings noch durch den Obersten Gerichtshof über die Angelegenheit beraten wurden, verließ al-Bashir über einen Militärflughafen das Land. Sowohl der Oberste Gerichtshof Südafrikas als auch die Richter in Den Haag kritisierten die Ermöglichung der Ausreise heftig und forderten die südafrikanische Regierung zur Stellungnahme auf. Die politische Reaktion ließ nicht lange auf sich warten. Im Rahmen des AU-Gipfeltreffens im Januar 2016 wurden zahlreiche Forderungen nach einem Austritt afrikanischer Staaten aus dem IStGH laut. Sofern einzelne Staaten einem solchen Aufruf Folge leisten, könnten sie die Zuständigkeit des IStGH zwar nicht für laufende Verfahren, aber doch in Zukunft einschränken und dem Gericht einen nicht nur symbolischen Rückschlag versetzen.

Ein Kindersoldat vor Gericht

Neben dem Sudan-Verfahren ist das Uganda-Verfahren wieder in den Mittelpunkt des Interesses gerückt. Die Ermittlungen gegen die Lord's Resistance Army (LRA) waren schon fast vergessen, als im Januar 2015 die erste Festnahme eines Angeklagten öffentlich bekannt wurde. Auch wenn sich der LRA-Anführer Joseph Kony weiterhin erfolgreich der Festnahme entziehen kann, so gelang es der Anklage des IStGH nunmehr mit Dominic Ongwen, einen Kommandeur wegen mutmaßlicher Verbrechen gegen die Menschlichkeit und Kriegsverbrechen vor Gericht zu stellen. Ihm werden Angriffe auf zahlreiche Lager von Binnenflüchtlingen im Jahr 2004 zur Last gelegt. Eine Besonderheit dieses Verfahrens ist, dass Dominic Ongwen zur Tatzeit noch keine 30 Jahre alt war und mutmaßlich als Kind selbst von der LRA zwangsrekrutiert wurde. Aufgrund der Tatsache, dass Ongwen den Großteil seines Lebens in der Rebellenbewegung verbracht und dort unter dem prägenden Einfluss von Joseph Kony und den Gewalterfahrungen des nordugandischen Konflikts ›Karriere‹ gemacht hat, wird ein komplexes Verfahren erwartet. Es wird aller Voraussicht nach aufschlussreiche Erkenntnisse über das Innenleben einer der bekanntesten afrikanischen Rebellengruppe liefern und, insbesondere im Rahmen der Strafzumessung, die Richter vor schwierige Abwägungsfragen stellen. Möglich ist, dass seitens der Verteidigung die Zurechenbarkeit und strafrechtliche Verantwortlichkeit Ongwens äußerst kritisch überprüft werden wird. Dies ist für internationale Strafgerichte durchaus Neuland. Klassischerweise beschäftigen sich die Gerichte vornehmlich mit dem Tatgeschehen; der Täter, dessen Geschichte, Motivation und Geisteszustand bleiben allzu oft unbeachtet. Das Verfahren wird Anlass geben, Fragen der individuellen Schuld für kollektives Unrecht detailliert zum Gegenstand zu machen.

Der Schutz von Kulturgütern

Juristisches Neuland wird der IStGH auch im Verfahren gegen Ahmad al-Faqi al-Mahdi betreten. Dem im September 2015 festgenommenen Beschuldigten werden Kriegsverbrechen wegen der Zerstörung bedeutender Kulturgüter in Mali zur Last

gelegt. Angesichts der massiven Zerstörung in und um Timbuktu und im Lichte der medial verbreiteten Sprengungen verschiedener Kulturdenkmäler in Palmyra und anderenorts in Syrien und Irak hat die Anklagebehörde den symbolischen Schritt unternommen, die Notwendigkeit des Schutzes von Kulturdenkmälern – auch mittels der *ultima ratio* des internationalen Strafrechts – zu unterstreichen. Der IStGH bringt damit zum Ausdruck, dass die Zerstörung von wichtigen Errungenschaften der Weltbevölkerung zum Schutz der kulturellen Vielfalt verhindert werden muss, und sendet ein Signal an die Weltöffentlichkeit, dass derartigem Verhalten nicht tatenlos zugeschaut werden darf. Der Schutz von Kulturgütern ist eine Aufgabe für die gesamte internationale Gemeinschaft, die über das Strafrecht weit hinausgeht. Im UN-System sind die UNESCO, aber auch der Sicherheitsrat gefordert (vgl. dazu von Schorlemer, VN, 1/2016, S. 3–8). Der Weckruf aus Den Haag ist ein erster Schritt, um die Thematik im Bewusstsein der Weltgemeinschaft zu verankern.

Mit dem Verfahren setzt die Anklagebehörde die Tradition fort, bei der Fallauswahl auch symbolische Akzente zu setzen. So hat etwa der erste Chefankläger Moreno-Ocampo bewusst Straftaten gegen Friedenssicherungskräfte und den Einsatz von Kindersoldaten zum Gegenstand von Strafverfahren gemacht, um diese Probleme auf die ›öffentliche Agenda‹ zu setzen. Der Internationale Strafgerichtshof für Ruanda hat mit den Medienprozessen die Rolle und Verantwortung von Journalisten (etwa Radio Télévision Libre des Milles Collines) hervorgehoben. Die Nachfolgeprozesse zum Nürnberger Hauptkriegsverbrecherprozess haben ebenfalls mittels themenbezogener Aufarbeitung des Systemunrechts die Verantwortlichkeiten bestimmter Gruppen (wie Ärzte und Juristen) besonders betont. Angesichts der begrenzten Kapazitäten der internationalen Strafjustiz und des Ausmaßes des begangenen Unrechts ist eine Selektion unvermeidbar. Eine flächendeckende Aufarbeitung ist nur in enger Zusammenarbeit mit nationalen und gegebenenfalls lokalen Institutionen möglich.

Das Verfahren in Georgien

Geografisch neues Terrain hat der Gerichtshof mit der Einleitung von Ermittlungen in Georgien betreten. Am 13. Oktober 2015 beantragte die Anklagebehörde die Einleitung eines formellen Ermittlungsverfahrens wegen möglicher Kriegsverbrechen und Verbrechen gegen die Menschlichkeit im Zuge der kriegerischen Auseinandersetzung im Jahr 2008 zwischen Georgien auf der einen und der Russischen Föderation und südossetischen Streitkräften auf der anderen Seite.

Der IStGH ist – da Georgien bereits im Jahr 2003 das Römische Statut ratifiziert hat – territorial für die Aufarbeitung von Völkerstraftaten auf dem Staatsgebiet Georgiens grundsätzlich zuständig. Aufgrund dieser territorialen Zuständigkeit gemäß Artikel 12 (2)(a) des Römischen Statuts ist die Anklage zudem befugt, gegen sämtliche Konfliktparteien zu ermitteln, auch wenn diese – wie die Russische Förderation – nicht Mitglied des IStGH sind. Die möglichen weltpolitischen Implikationen sind gewaltig. Zum ersten Mal seit der Schaffung des IStGH befindet sich die Anklagebehörde in der Position, konkret gegen Streitkräfte einer Vetomacht des UN-Sicherheitsrats ermitteln zu können. Dass auch die russische Beteiligung am Konflikt aufgearbeitet werden soll und kann, wurde durch die Anklagebehörde stets betont. Ob der IStGH tatsächlich bereit sein wird, den Konflikt mit einem derart schlagkräftigen Gegner zu suchen und gar russische Staatsbürger namentlich zu beschuldigen, bleibt abzuwarten.

Zum jetzigen Zeitpunkt reichen die von der Anklage vorgebrachten Beweise nach Ansicht der Vorverfahrenskammer I aus, um weitergehende Ermittlungen durchzuführen und die Grenzen von informellen Vorermittlungen zu formellen Ermittlungen zu überschreiten. Eine Zustimmung der Richter der Vorverfahrenskammer ist notwendig, wenn weder ein Mitgliedstaat noch der UN-Sicherheitsrat die Ermittlungen durch Verweisung an den IStGH eingeleitet haben. Die Zustimmung der Richter vom 27. Januar 2016 erlaubt es der Anklagebehörde, die einzelnen Sachverhalte aufzuarbeiten und konkrete Beschuldigte zu benennen. Sofern gegen diese Personen keine ernsthaften Strafverfolgungsbemühungen auf staatlicher Ebene erfolgen, kann der IStGH Strafverfahren einleiten und – sollte dies notwendig werden – Haftbefehle beantragen. Dies wird jedoch vermutlich noch einige Monate oder gar Jahre dauern. Insbesondere aufgrund des langjährigen Vorwurfs der Afrikazentriertheit ist dem Schritt zu formellen Ermittlungen in Georgien indes große strategische Bedeutung beizumessen.

Der Umzug

Eine für das Tagesgeschäft nicht ganz unbeachtliche Entwicklung ist der Umzug des gesamten Gerichts aus den provisorischen Gebäuden in der Den Haager Vorstadt an die neue Wirkungsstätte in der Nähe des UN-Gefängnisses in Scheveningen. Das neue Gerichtsgebäude soll allen Beteiligten (Richter, Anklage, Verwaltung, Verteidigung) permanente Strukturen bieten, der zunehmenden Vergrößerung des Gerichts Rechnung tragen und nach außen das Bekenntnis der Mitgliedstaaten zur Dauerhaftigkeit der internationalen Strafjustiz verdeutlichen. Die Vorteile der neuen Strukturen sind nicht von der Hand zu weisen. Dennoch darf der feierliche Umzug nicht über die bestehenden Unsicherheiten und Herausforderungen hinwegtäuschen. So geht der Bezug der neuen Räumlichkeiten keinesfalls mit einer langjährigen Garantie eines ausreichenden Budgets einher. Die Konsequenz der Planungsunsicherheit: Zeitverträge, Personalengpässe und drohende Verzögerungen. Hinzukommt, dass die Anzahl der anhängigen Verfahren mit der Ausweitung der Ermittlungstätigkeit auf derzeit zehn Situationen sowie Vorermittlungen in weiteren sieben Ländern stetig zunimmt. Die Anforderungen an das Personal werden sich aufgrund der sprachlichen und kulturellen Diversifizierung der Verfahren (etwa Georgien, Palästina, Ukraine) ebenfalls deutlich erhöhen. Das Projekt ›Internationaler Strafgerichtshof‹ erfordert mehr als ein Gebäude. Nötig ist eine ausreichende und vor allem langfristig angelegte Finanzierung. Ohne die notwendige Unterstützung ist die internationale Strafjustiz zum Scheitern verurteilt. Hier ist auch Deutschland gefragt.

Verweise: Webseite des IStGH: www.icc-cpi.int; Webseite zum neuen Gerichtsgebäude: http://www.icc-permanentpremises.org/

Umwelt

Resolution gegen Wilderei und illegalen Wildtierhandel

- UN-Generalversammlung verabschiedet erste thematische Resolution
- Deutschland und Gabun initiieren Freundesgruppe

Jan Kantorczyk

Anfang Juli 2015 tötete ein amerikanischer Jäger den Löwen Cecil in Simbabwe, der dadurch internationale Bekanntheit erlangte. Die Tat rief einen Aufschrei der Entrüstung in den Medien und in den sozialen Netzwerken hervor. Sie warf zugleich ein Schlaglicht auf eine besorgniserregende und zunehmend gefährliche Entwicklung: Wilderei und illegaler Wildtierhandel bedrohen die Wildtierbestände in vielen Ländern, vor allem in Afrika. Im Jahr 2014 wurden über 20 000 Elefanten und über 1200 Nashörner auf dem afrikanischen Kontinent von Wilderern erlegt. Endgültige Zahlen für das Jahr 2015 liegen noch nicht vor. Es muss aber davon ausgegangen werden, dass ähnlich viele Elefanten und Nashörner der Jagd nach den Luxusgütern Elfenbein und Nashorn-Horn zum Opfer gefallen sind. Die Regierung Tansanias gab unlängst bekannt, dass sich die Elefantenpopulation des Landes binnen fünf Jahren um 60 Prozent durch Wilderei verringert habe. Wenn sich diese bedenkliche Entwicklung fortsetzt, könnte in zehn Jahren die Hälfte der afrikanischen Elefanten verschwunden sein. In einigen Regionen muss sogar ein Aussterben befürchtet werden.

Nicht nur ein Fall für den Artenschutz

Wilderei und illegaler Wildtierhandel bedrohen zahlreiche Tier- und Pflanzenarten, und nicht nur in Afrika. Auch das südamerikanische Vikunja, die zentralasiatische Schraubenziege, die karibische Große Fechterschnecke sowie Teakhölzer in Lateinamerika und Asien sind in ihrem Bestand gefährdet – trotz nationaler und internationaler Regelungen zum Artenschutz. Daneben schränken Umwelteinflüsse, Urbanisierungstendenzen und wirtschaftliche Aktivitäten wie Abholzung die natürlichen Lebensräume für wildlebende Tier- und Pflanzenarten immer weiter ein.

Doch nicht nur die Biodiversität ist bedroht. Wilderei und illegaler Wildtierhandel berauben Menschen ihrer Lebensgrundlage, gefährden Arbeitsplätze im Tourismus- und Servicebereich und erzeugen, einhergehend mit Korruption, soziale Probleme. Die zunehmende Militarisierung der Wilderei mit grenzüberschreitend operierenden, hochgerüsteten Banden bedroht auch die Stabilität und Sicherheit von Regionen und ganzen Staaten. Dies wurde vom Sicherheitsrat der Vereinten Nationen in mehreren Länderresolutionen anerkannt. Die Lage wird noch komplizierter durch den Umstand, dass die wichtigsten Absatzmärkte für illegale Wildtierprodukte in Asien und Nordamerika liegen. Das Horn von Nashörnern erzielt auf asiatischen Schwarzmärkten einen Preis von über 65 000 US-Dollar und ist damit wertvoller als Gold. Das Risiko einer Festnahme für Wilderer ist gering, ebenso das Strafmaß, werden sie doch einmal überführt, die Gewinnspanne dagegen hoch. Es liegen Erkenntnisse vor, dass sich terroristische Organisationen durch Erlöse aus dem illegalen Wildtierhandel finanzieren. Der verbotene Handel mit geschützten Tier- und Pflanzenprodukten rangiert weltweit an vierter Stelle in der Organisierten Kriminalität hinter Drogenhandel, Menschenhandel und Produktpiraterie. Der Umsatz wird auf mindestens zehn Milliarden US-Dollar pro Jahr geschätzt.

Der Weg in die Vereinten Nationen

Wilderei und illegaler Wildtierhandel sind wegen ihrer Komplexität und globalen Bedeutung eigentlich ein klassisches Thema für die Vereinten Nationen. Lange Zeit wurde es aber nur punktuell behandelt, etwa durch thematische Resolutionen des Wirtschafts- und Sozialrats der Vereinten Nationen (Economic and Social Council – ECOSOC), länderbezogene Resolutionen des Sicherheitsrats oder durch Projekte einzelner UN-Organisationen. Eine kohärente, gesamtheitliche und koordinierte Herangehensweise fehlte. Dies zu ändern, war das Ziel einer Initiative der Vertretungen Deutschlands und Gabuns bei den Vereinten Nationen.

Deutschland engagiert sich seit Jahren umweltpolitisch, entwicklungspolitisch und im Rahmen der Außen- und Sicherheitspolitik für ein wirksames Vorgehen gegen Wilderei und illegalen Wildtierhandel. Gabun ist die Heimat bedeutender Populationen von Waldelefanten und Gorillas, aber auch zahlreicher anderer Spezies. Seine Nationalparks sind immer wieder das Ziel von Wilderern.

Die gemeinsame deutsch-gabunesische Initiative führte am 30. Juli 2015 zur Verabschiedung der ersten Resolution der Generalversammlung (69/314) zur Bekämpfung des illegalen Wildtierhandels (›Tackling illicit trafficking in wildlife‹).

Der Weg dahin war lang. Den Anfang bildeten mehrere thematische Veranstaltungen, die die Vertretungen Deutschlands und Gabuns gemeinsam mit Organisationen der Vereinten Nationen, etwa dem Entwicklungsprogramm der Vereinten Nationen (UNDP), dem Umweltprogramm (UNEP) und dem Büro für Drogen- und Verbrechensbekämpfung (UNODC), sowie verschiedenen nichtstaatlichen Organisationen (World Wildlife Fund, Wildlife Conservation Society, TRAFFIC) seit Dezember 2012 organisierten. Im September 2013 leiteten der Staatspräsident Gabuns Ali Bongo Ondimba und der damalige Bundesaußenminister Guido Westerwelle während der Generaldebatte zur 68. Generalversammlung eine hochrangige Veranstaltung zu diesem Thema, auf der konkrete Empfehlungen hervorgebracht wurden. Auf Vorschlag Deutschlands und Gabuns zählten dazu die Gründung einer Freundesgruppe in New York und die Arbeit an einer Resolution der Generalversammlung.

Die UN-Freundesgruppe

Auf dieser Grundlage gründeten die Vertretungen Deutschlands und Gabuns im Dezember 2013 die UN-Freundesgruppe ›Wilderei und illegaler Wildtierhandel‹. (Poaching and illicit wildlife trafficking). Zur konstituierenden Sitzung auf Botschafterebene wurden strategisch wichtige Mitgliedstaaten eingeladen, insbesondere auch asiatische Zielländer des illegalen Wildtierhandels wie China, Malaysia, Thailand und Vietnam. Durch beharrliche Überzeugungsarbeit gelang es dabei, ursprüngliche Bedenken gegen die Ziele der Freundesgruppe zu zerstreuen.

Die Freundesgruppe setzt sich repräsentativ aus über 20 Herkunfts-, Transit- und Zielländern des illegalen Wildtierhandels zusammen. Alle Kontinente sind in ihr vertreten. Nach ihrer konstituierenden Sitzung nahm die Freundesgruppe, gelei-

tet von Deutschland und Gabun, zunächst eine Bestandsaufnahme vor und sondierte den Regelungsumfang der angestrebten Resolution. Dafür trat sie auch in einen Dialog mit Vertreterinnen und Vertretern relevanter Organisationen der Vereinten Nationen sowie mit dem Sekretariat des Übereinkommens über den internationalen Handel mit gefährdeten Arten freilebender Tiere und Pflanzen (CITES). Ein erster Textentwurf wurde im August 2014 erarbeitet. Dabei, aber auch im späteren Verlauf, erfolgte eine intensive Beratung mit internationalen Naturschutzorganisationen. Im September 2014 fand eine weitere hochrangige Veranstaltung am Rande der Generaldebatte unter Leitung von Präsident Ondimba und Bundesaußenminister Frank-Walter Steinmeier statt, an der weitere afrikanische Staatsoberhäupter und zahlreiche Ministerinnen und Minister teilnahmen. Sie erzeugte wichtige politische Unterstützung für die Initiative. Parallel organisierte die Gruppe diverse Veranstaltungen, um auf das Thema aufmerksam zu machen und für ein stärkeres internationales Engagement zu werben.

Die Verhandlungen

Während den folgenden Verhandlungen der Freundesgruppe über den Resolutionsentwurf traten wiederholt Differenzen zutage: vor allem beim Erfassungsgrad (alle Wildtierarten oder nur einzelne), bei der Erwähnung von Sicherheit und Stabilität im Kontext des illegalen Wildtierhandels, bei der Hervorhebung von Rechtsstaatlichkeit, dem Kampf gegen Korruption und einigen anderen Punkten. Wichtig war zu jedem Zeitpunkt, dass auch die asiatischen Mitglieder der Freundesgruppe das Ziel der Resolution grundsätzlich unterstützten und daher konstruktiv am Textentwurf mitarbeiteten. Nach zahlreichen Verhandlungsrunden und zusätzlichen bilateralen Kontakten in New York und den Hauptstädten einigte sich die Freundesgruppe im Mai 2015 schließlich auf einen Resolutionsentwurf.

Anschließend verhandelten alle UN-Mitgliedstaaten über den Entwurf, also auch diejenigen, die nicht Mitglied der Freundesgruppe sind. Dabei ergaben sich neue Aspekte: Argentinien, Island und Japan drängten zum Beispiel darauf, dass sich die Resolution klar vom Seerechtsübereinkommen abgrenzen müsse und Meerestiere nicht erfassen dürfe. Russland schlug, nicht konsensfähig, vor, ein Zusatzprotokoll für illegalen Wildtierhandel zum Übereinkommen der Vereinten Nationen zur grenzüberschreitenden organisierten Kriminalität (UNTOC) auszuarbeiten. Mitte Juli einigte sich schließlich auch der Kreis der 193 Mitgliedstaaten auf einen Resolutionstext, der dem Ambitionsgrad des von der Freundesgruppe erstellten Textes weitgehend entspricht. Somit war der Weg frei für die Suche nach Miteinbringern und die Annahme der Resolution in der Generalversammlung.

Die Verabschiedung der Resolution

Am 30. Juli 2015 verabschiedete das Plenum der Generalversammlung den Resolutionsentwurf, den 86 Staaten eingebracht hatten, im Konsens. Neben allen EU-Mitgliedstaaten finden sich auf der Liste der Miteinbringer Herkunfts-, Transit- und Zielländer des illegalen Wildtierhandels.

Die Resolution behandelt Wilderei und illegalen Wildtierhandel erstmals in ihrer gesamten Komplexität, als Bedrohung von nachhaltiger Entwicklung, Stabilität und Sicherheit. Sie erfasst die globale Dimension und spricht Herkunfts-, Transit- und Zielländer an. Sie ruft Mitgliedstaaten zu umfassenden nationalen Maßnahmen und besserer internationaler Zusammenarbeit auf. Ausdrücklich genannt werden eine bessere Strafverfolgung, eine stärkere internationale Zusammenarbeit im Kampf gegen Korruption und Geldwäsche sowie eine geringere Nachfrage nach illegalen Produkten. Die Vereinten Nationen werden zu einem koordinierten Vorgehen aufgefordert. Der Generalsekretär wird gebeten, die 70. Generalversammlung über globale Entwicklungen bei illegalem Wildtierhandel zu unterrichten und operative Handlungsvorschläge zu unterbreiten. Die Generalversammlung beschließt, sich jährlich mit der Problematik zu befassen.

Mit Verabschiedung der Resolution hat die Staatengemeinschaft gezeigt, dass sie die globale Dimension des illegalen Wildtierhandels erkannt hat und bereit ist, nicht nur national dagegen vorzugehen, sondern auch Verantwortung unter dem Dach der Vereinten Nationen zu übernehmen. Bundesaußenminister Frank-Walter Steinmeier und Bundesumweltministerin Barbara Hendricks begrüßten die Annahme der Resolution am 30. Juli 2015 in einer gemeinsamen Presseerklärung.

Die nächsten Schritte

Nach erfolgreicher Verabschiedung der Resolution rückt nun deren Umsetzung in den Blick. Im Januar 2016 haben unter Federführung von UNODC die Arbeiten am Bericht des Generalsekretärs begonnen. Dabei ist eine breite Konsultation mit den UN-Mitgliedstaaten und der Zivilgesellschaft vorgesehen. Die Vorlage des Berichts wird für Mai erwartet; die Debatte in der Generalversammlung wird im Juni oder Juli stattfinden.

In einem parallelen Handlungsstrang beginnt die Umsetzung der ›Agenda 2030 für nachhaltige Entwicklung‹. Sie enthält mehrere handlungsorientierte Unterziele, die auf ein Ende der Wilderei und des illegalen Handels mit geschützten Arten bis zum Jahr 2030 abzielen.

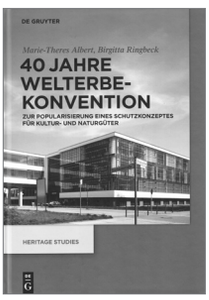
Eine weitere, neue Handlungsschiene betrifft den UN-Sicherheitsrat. Auf Initiative von Litauen und Angola hatte dieser am 30. November 2015 erstmals in einer offenen thematischen Veranstaltung den Zusammenhang zwischen dem illegalen Handel mit Klein- und Leichtwaffen und der Wilderei in Afrika untersucht. Auf Bestreben afrikanischer Staaten soll möglichst noch im Jahre 2016 eine förmliche Sitzung des Rates dazu stattfinden.

Die Freundesgruppe wird diese Prozesse aktiv mitgestalten. Sie plant, auf Basis des Berichts des Generalsekretärs und seiner Empfehlungen, eine Nachfolgeresolution auszuarbeiten, in Verhandlungen abzustimmen und den UN-Mitgliedstaaten im Juni oder Juli 2016 zur Annahme vorzulegen. Parallel wird sie durch Veranstaltungen und Erklärungen in Sitzungen diverser UN-Gremien auf aktuelle Entwicklungen bei Wilderei und illegalem Wildtierhandel hinweisen und für einen noch entschlosseneren Einsatz der Staatengemeinschaft werben.

Vor diesem Hintergrund besteht eine realistische Chance, den Schutz wildlebender Arten im Jahr 2016 auf globaler Ebene weiter zu verstärken – unter Führung der Vereinten Nationen. Diese Chance darf nicht ungenutzt verstreichen, damit sich Fälle wie der des Löwen Cecil und vieler namenloser Tiere nicht wiederholen und nachfolgende Generationen Wildtieren nicht nur in Lehrbüchern oder zoologischen Gärten begegnen.

Welterbe: Ambivalenz eines Erfolgsmodells

Andrea F. G. Raschèr



Marie-Theres Albert/
Birgitta Ringbeck

40 Jahre Welterbekonvention.
Zur Popularisierung eines Schutzkonzeptes für Kultur- und Naturgüter

Heritage Studies
Volume 2

Berlin/München/
Boston: Walter de
Gruyter 2015,
326 S., 39,95 Euro

Das Übereinkommen zum Schutz des Kultur- und Naturerbes der Welt der UNESCO von 1972 (Welterbekonvention) gehört zu den wichtigsten Rechtsinstrumenten der UNESCO. Ziel der Konvention, die vor mehr als 40 Jahren verabschiedet wurde, ist es, Welterbe von außergewöhnlichem universellem Wert zu schützen und für künftige Generationen zu erhalten. Die Publikation ›40 Jahre Welterbekonvention‹ zeigt auf, wie die Konvention angewendet wird, wo Probleme liegen und welche Weiterentwicklungen wünschbar wären. All dies gelingt, indem die Autorinnen, **Marie-Theres Albert** und **Birgitta Ringbeck**, eine beeindruckende Fülle an Daten und Fakten souverän zu ordnen verstehen. Ihre Ausführungen haben sie mit Bildern von Kulturerbestätten angereichert.

Angesichts der großen Popularität der Konvention gilt gemeinhin als unbestritten, dass die internationale Gemeinschaft damit ein herausragendes Instrument zum Schutz des Welterbes geschaffen hat. Bislang haben 191 Staaten die Konvention ratifiziert, und es wurden mehr als 1000 Stätten als Welterbe ausgezeichnet. In diesem Sinne kann die Konvention als Erfolgsmodell angesehen werden. Die Autorinnen der vorliegenden Publikation begnügen sich jedoch nicht damit, den Status quo als die großartige Errungenschaft darzustellen, die sie faktisch ist. Sie weisen Fehlentwicklungen nach, für die sie auch gleich Lösungsvorschläge bieten. Anhand aussagekräftiger Grafiken wird ein eklatantes Missverhältnis zwischen Zielen und Umsetzung der Konvention offenbar, betrachtet man die regionale Verteilung der Stätten oder die Kategorien, denen die Stätten zugeordnet werden. Insbesondere das Verhältnis zwischen den UNESCO-Stätten in Europa und den USA einerseits und dem, was geradezu als ›Rest der Welt‹ erscheint. Die bis heute ungebrochene Auffassung einer ›entwickelten‹ gegenüber einer ›unterentwickelten‹ Welt sowie die Unterscheidung einer ›repräsentativen Kultur‹ gegenüber der ›Natur‹ wird überdeutlich erkennbar. So finden sich erstaunlich viele Naturerbestätten in Afrika, den arabischen Staaten, Asien oder Lateinamerika, hingegen bemerkenswert wenige Kulturstätten. Dieses internationale Ungleichgewicht zementiert traditionelle Bilder von vermeintlich typischen ›euro-amerikanischen Kulturräumen‹ und ›Naturräumen von Entwicklungsländern‹. Hier wird offenkundig, dass eine europäische Vorstellung von Kultur durchgesetzt wird: Fußend auf einem konservativen, eurozentrischen Konzept der Mittelschicht wird Welterbe definiert und konstruiert. Die Grundlage für den Anspruch außergewöhnlichen und universellen Wertes bildet aber ein bildungsbürgerlicher materieller Kulturbegriff. Immaterielle Interpretationen von Stätten sind folglich nur bedingt möglich. In dieser Logik bleibt das europäische Erbe zwangsläufig konkurrenzlos und unbestritten.

Das Unterkapitel ›Welterbe und Politik‹ legt dar, dass eine Kulturstätte durch ›Popularisierung‹ förmlich zu einer Ware verkommt. Albert und Ringbeck illustrieren diese Veränderung anhand jüngerer Entscheidungen des Welterbekomitees: Als Richtlinie für eine schützenswerte Stätte gilt nicht mehr allein ihr außergewöhnlicher universeller Wert. Vielmehr scheint der Auswahl ein diffuses Konzept einer ›nationalen Marke‹ zugrunde zu liegen, die Prestige verleiht und insbesondere für bislang weniger bekannte Stätten ein wertsteigernder Faktor für die Tourismusentwicklung ist. Im Jahr 2011 wurde für 18 Stätten die UNESCO-Anerkennung beantragt. Die Beratergremien empfahlen, alle 18 zurückzuweisen. Dennoch haben die UNESCO-Staaten 15 davon als Welterbe akzeptiert. Honi soit qui mal y pense.

Im abschließenden Kapitel werden Lösungen für die Zukunft präsentiert. Eine erste Forderung ist, den Beteiligten vor Ort größeres Mitspracherecht einzuräumen. Denn was von der lokalen Bevölkerung akzeptiert wird, bietet zugleich eine gute Grundlage für die sozio-ökonomische Entwicklung der Orte und Gesellschaften, in denen diese Stätten liegen. Als nächste Herausforderung gilt es zu erforschen, ob und in welcher Weise kulturelle Vielfalt und kulturelles Erbe überhaupt konstruktiv zu vereinen sind. Schließlich fordern die Autorinnen, dass eine nachhaltige Nutzung von Erbe an mündige Bürgerinnen und Bürger zu übertragen sei, anstatt diese – wie bisher in Politik und Verwaltung üblich – bestenfalls als Zaungäste zuzulassen.

Die Publikation gibt für die Anwendung der Konvention zahlreiche Denkanstöße. Nicht zuletzt ortet das Werk Risiken an jenen Stellen, wo die Politik Anstalten macht, die Grundfeste der Konvention zu vereinnahmen. Die Autorinnen vertreten die Auffassung, dass es Ziel sein muss, transparente und partizipatorische Verfahren zu entwickeln, in deren Mittelpunkt die Wertschätzung und Vielfalt des Welterbes steht. Erst dann wird aus dem heute ambivalenten Erfolgsmodell ein wahres Erfolgsmodell.

Gegenwart und Zukunft der UN-Friedenssicherung

Manuela Scheuermann

60 Jahre unentwegt im Einsatz für den Frieden in der Welt – wer kann das schon von sich behaupten? Was im Jahr 1956 mit dem ersten Einsatz der Noteinsatztruppe der Vereinten Nationen (United Nations Emergency Force – UNEF I) begann, entpuppte sich im Laufe der Jahrzehnte als beispiellose Erfolgsgeschichte des internationalen Krisenmanagements. Dank der erstaunlichen Flexibilität und Anpassungsfähigkeit der Vereinten Nationen und der vielfältigen Unterstützung unterschiedlichster Partner steht das System der Friedenssicherung der Vereinten Nationen aktuell stärker denn je im Zentrum der weltweiten Friedensanstrengungen. Ein Ende dieses »Flaggschiff-Unternehmens« (Ban Ki-moon) ist – zum Glück für den Weltfrieden – nicht in Sicht.

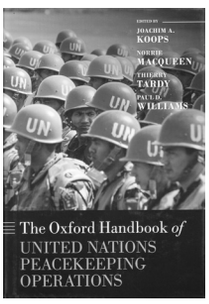
Zwei im Jahr 2015 erschienene Werke widmen sich der UN-Friedenssicherung mit dem Ansporn, zur Debatte um die Gegenwart und Zukunft des Systems beizutragen. Diesem Anspruch werden beide Bücher, allerdings auf sehr unterschiedlichen Wegen, gerecht.

Mit ›The Oxford Handbook of United Nations Peacekeeping Operations‹ legen **Joachim A. Koops**, **Norrie MacQueen**, **Thierry Tardy** und **Paul D. Williams** das erste umfassende Nachschlagewerk zur UN-Friedenssicherung vor. Die Herausgeber, die sich selbst seit Jahren intensiv mit dem Thema befassen, vereinigten dazu ein beeindruckendes Expertenkonsortium von 57 Wissenschaftlern, UN-Expertinnen und -Experten, Diplomaten und Militärangehörigen.

Im ersten von zwei Teilen beschäftigen sich die Autorinnen und Autoren mit den Konzepten und Perspektiven der Friedenssicherung. Bei der Auswahl der Themen demonstrierten die Herausgeber ein gutes Gespür, sprechen die Artikel doch die Kernfragen der Friedenssicherung an: Muss, beziehungsweise wie muss sich die »Buschfeuerkontrolle« (Dag Hammarskjöld) der internationalen Beziehungen ändern, um weiterhin für Sicherheit, Stabilität und Frieden sorgen zu können? Welche Chancen birgt die Partnerschaft mit Regionalorganisationen für die Friedenssicherung der UN? Unter welchen Bedingungen ist eine Friedensoperation tatsächlich erfolgreich? Im ersten, besonders lesenswerten Aufsatz besprechen Alex J. Bellamy und Paul D. Williams die gegenwärtigen und zukünftigen Trends von Friedensoperationen. Der Beitrag ist deshalb so herausragend, weil Bellamy und Williams den Blick nicht auf die Vereinten Nationen verengen. Sie beziehen in ihre vorwiegend quantitative Studie neben UN-geführten Einsätzen auch UN-mandatierte Missionen ein, also von den UN lediglich anerkannte Einsätze und Missionen außerhalb des UN-Systems, sofern sie die Kriterien einer Friedensoperation erfüllen. Zudem decken Bellamy und Williams mit Hilfe interregionaler Vergleiche häufig übergangene regionale Varianzen auf. Deshalb sind ihre Ergebnisse – im Ganzen sieben Trends – ein überaus wertvolles Korrigendum zu den vielen Untersuchungen, die ihre Resultate nicht mit den Strömungen außerhalb der spezifischen Wirklichkeit der Friedenssicherung abgleichen. Bellamy und Williams können mit Hilfe ihres umfangreichen Datensatzes beispielsweise der oftmals artikulierten These, die UN verlieren ihre Schlüsselrolle, den Befund entgegensetzen, dass die Weltorganisation auch langfristig fest im Zentrum dieser zunehmend verbreiteten Form des Krisenmanagements verbleiben wird.

Im zweiten Beitrag widmet sich Nigel G. White der Frage, wie Friedenssicherung völker- und menschenrechtlich verortet werden kann. Anschließend diskutieren Thierry Tardy und Joachim A. Koops die Partnerschaft mit Regionalorganisationen, die als Mitherausgeber ihren wissenschaftlichen Schwerpunkt im Bereich der Forschung zu internationalen Organisationen haben. Thomas G. Weiss führt den Komplex ›Friedenssicherung und humanitäre Interventionen‹ näher aus und Paul F. Diehl und Daniel Druckman gehen der (Un-)Möglichkeit der Evaluation von Friedensoperationen nach. Diehl und Druckman kritisieren, dass viele Studien zum Erfolg von Friedenssicherung in ihrer Aussagekraft beschränkt sind, da sie sich nur auf einen Indikator von Erfolg konzentrieren und grundsätzliche Überlegungen zur Perspektive von Erfolg ausblenden. Nach Ansicht der Autoren ist es ein beinahe unmögliches Unterfangen, eine Friedensoperation korrekt zu evaluieren. Die Welt der UN-Friedenssicherung ist schlichtweg zu komplex.

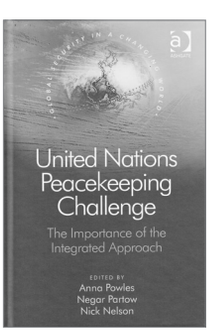
Steht der erste Teil des Buches für intelligente Analysen und erhellende Befunde, so wartet der zweite Teil mit gesammeltem und geordnetem Wissen auf. Denn allen 67 im Zeitraum von 1948 bis 2013 eingesetzten UN-Beobachtungs- und Friedenssicherungsmissionen steht ein eigenes, bis zu zehn Seiten umfassendes Kapitel zur Verfügung. Da (fast) alle Kapitel nach dem gleichen Schema aufgebaut sind und jedem Kapitel die wichtigsten Informationen in einem Kasten vorangestellt werden, lädt der Band zu systematischen Vergleichen der Missionen ein. Wei-



Joachim A. Koops/ Norrie MacQueen/ Thierry Tardy/Paul D. Williams (Hrsg.)

The Oxford Handbook of United Nations Peacekeeping Operations

Oxford: Oxford University Press 2015, 800 S., 95,00 brit. Pfund



Anna Powles/ Negar Partow/ Nick Nelson (Hrsg.)

United Nations Peacekeeping Challenge. The Importance of the Integrated Approach

London: Routledge 2015, 300 S., 65,00 brit. Pfund

terführende Literatur zum Ende der jeweiligen Kapitel wäre ein zusätzlicher Anreiz gewesen, das Werk in die Hand zu nehmen. Neben den Herausgebern, die relativ häufig als Autoren und Koautoren in Erscheinung treten, konnten hochrangige Verantwortliche der Missionen selbst gewonnen werden. So berichtet beispielsweise Alan Doss über seine Erfahrungen als ehemaliger Sonderbeauftragter des UN-Generalsekretärs und Leiter der Stabilisierungsmission der Organisation der Vereinten Nationen in der Demokratischen Republik Kongo (MONUSCO) und deren Vorgängermission MONUC. In der Gesamtschau ergibt sich so eine einzigartige Historie der UN-Friedenssicherung. Zwei Botschaften des zweiten Teiles lohnen näherer Betrachtung: Viele Entwicklungen in der Friedenssicherung, die gemeinhin der jüngeren Geschichte zugeschrieben werden, wie beispielsweise das robuste Mandat oder der Schutz der Zivilbevölkerung, hatten ihre Premiere bereits vor Ende des Kalten Krieges. Und jede Friedenssicherungsmission war – mehr oder weniger – erfolgreich.

Der Sammelband ›United Nations Peacekeeping Challenge. The Importance of the Integrated Approach‹, herausgegeben von **Anna Powels, Negar Partow** und **Nick Nelson**, verspricht dagegen den ›besonderen‹ Einblick. Ein Vorwort von Hervé Ladsous, dem amtierenden Leiter der Hauptabteilung Friedenssicherungseinsätze (Department of Peacekeeping Operations – DPKO), eröffnet den Band, der auf zwei gemeinsamen Veranstaltungen der neuseeländischen und US-amerikanischen Streitkräfte im September 2013 beruht. Zusammen mit der Abteilung Militär des DPKOs wurden die bessere Integration von truppenstellenden Staaten in UN-Missionen und der Einfluss von Krieg auf die mentale Gesundheit von Soldaten diskutiert.

Es ist das erklärte Ziel, zur Reformdebatte der UN-Friedenssicherung einen substanziellen Beitrag zu leisten. Dabei sollen nicht die altbekannten Herausforderungen besprochen, sondern wenig beachtete und kritische Themen in die Debatte integriert werden. Es ist – insbesondere bei den Abhandlungen über die mentale soldatische Gesundheit – zu erkennen, dass die Herausgeber nicht in der UN-Forschung beheimatet sind. Auch die übrigen zwanzig Autoren sind überwiegend hochrangige Militärangehörige, (Militär-)Psychologen und – vereinzelt – UN-Bedienstete wie der Leiter der Hauptabteilung Unterstützung der Feldeinsätze (Department of Field Support – DFS) oder Politikwissenschaftler. Der Sammelband ist vor allem aufgrund der dokumentierten Praxiserfahrung nicht nur für Wissenschaftlerinnen und Wissenschaftler, sondern gerade auch für Militärangehörige ein Konvolut an geballtem Wissen.

So divers wie die Autorenschaft, so facettenreich sind die besprochenen Themen und so unterschiedlich sind auch Stil und Qualität der Beiträge. Von exzellenten Aufsätzen von Ameerah Haq, Alex J. Bellamy, Jens Winther Andersen und William Flavin bis hin zu einem rein subjektiven Bericht eines traumatisierten Generals, von wiederholt eingestreuten fundierten Reformvorschlägen bis hin zu einem wirklich schlecht verfassten Schluss findet sich ein Kaleidoskop an Beiträgen. Immer im Mittelpunkt steht der Mitgliedstaat oder der einzelne Soldat beziehungsweise die einzelne Soldatin. Auch wenn das Buch im Untertitel den ›Integrated Approach‹ aufgenommen hat, findet die Auseinandersetzung mit dem vernetzten, integrierten, multidimensionalen Ansatz der Friedenssicherung vorwiegend im unbedingt empfohlenen ersten Teil statt. Der zweite Teil konzentriert sich auf die besonderen Herausforderungen der Landstreitkräfte angesichts des Wandels des internationalen Krisenmanagements. Die Autorinnen und Autoren betonen die Relevanz klarer, stabiler Mandate und finden mitunter harsche Worte für die UN-Friedenssicherung. So behauptet beispielsweise D. Craig Aitchison in seinem Beitrag, dass viele Mitgliedstaaten weiterhin auf andere Organisationen ausweichen würden, solange die UN nicht dasselbe kampferprobte und effiziente System wie die Organisation des Nordatlantikvertrags (NATO) eingerichtet habe.

Der dritte Teil hat sich ganz der Fürsorgepflicht gegenüber den Soldaten verschrieben. Posttraumatische Belastungsstörungen (PTBS) sind zweifellos ein wichtiges Thema für Militärangehörige und prinzipiell ist es notwendig, die UN-Friedenssicherung dafür zu sensibilisieren. Angesichts der Tatsache, dass PTBS in der Friedenssicherung aufgrund der seltenen Nähe zum Kampfgeschehen allenfalls vereinzelt vorkommen, hätte dieser Abschnitt jedoch deutlich kleiner ausfallen können. Teil vier trägt den vielversprechenden Titel ›Sharing Peace Operations Spaces‹, bleibt aber hinter der Erwartung, mehr über den integrierten Ansatz zu erfahren – bis auf die Analyse von William Flavin zur zivil-militärischen Zusammenarbeit – zurück.

Ist es der Fachfremde der Herausgeber geschuldet, dass sich in einige Artikel ärgerliche inhaltliche Fehler eingeschlichen haben? Polizisten werden als ›Grünhelme‹ betitelt, der unzweifelhaft hoch verdiente Ralph Bunche wird zum Generalsekretär der Vereinten Nationen und Vater der UN-Friedenssicherung erkoren und Lakhdar Brahimi erlangt erst mit seinem Bericht der Sachverständigengruppe für die Friedensmissionen der Vereinten Nationen aus dem Jahr 2008 Prominenz und Anerkennung in der UN-Friedenssicherung. Solche Fehler sollten in einem Buch, das im Vorfeld mit vielen Vorschusslorbeeren bedacht wurde, nicht vorkommen.

Der Sammelband ist vor allem dreierlei: Ein praktischer Ratgeber für Militärangehörige, Ermunterung und Ermahnung für die UN-Friedenssicherung und ein leiser Appell für mehr Partnerschaft, Teamarbeit und Führung in der Friedenssicherung.

Nach der Schlusskonferenz ist noch lange nicht Schluss

Jürgen Maier

Nick Reimer ist eine gute Darstellung der Geschichte der Klimakonferenzen gelungen – leicht verständlich auch für all diejenigen, die längst den Überblick über die vielen Details dieser Verhandlungen verloren haben. Kompakter und verständlicher kann man es wohl kaum schildern. Vor allem belässt es der Autor nicht bei den Ereignissen und ihren oberflächlichen Begleiterscheinungen, sondern er analysiert auch Hintergründe und Interessen. Pointiert bringt er dies auf den Punkt: »Dass auf den Klimagipfeln die Reduktion der Treibhausgase verhandelt wird, ist ein weitverbreiteter Irrtum. In den Verhandlungen spielt das allenfalls auch eine Rolle. In erster Linie aber geht es in der Klimadiplomatie um Wirtschaftskraft.« (S.95)

Bei allen Irrungen und Wirrungen der Konferenzen, die Reimer treffend beschreibt, wird er nicht müde, auch ihre Bedeutung für das System der Vereinten Nationen herauszuarbeiten. In einer Zeit wachsender internationaler Spannungen sind multilaterale Problemlösungsversuche alles andere als eine Selbstverständlichkeit. Der Autor zitiert den Schweizer Andreas Fischlin mit der Ansicht, es sei eine enorme kulturelle Leistung, dass hier Vertreter der gesamten Menschheit versammelt seien und sich auf 50, 100 Jahre hinaus Gedanken machten. (S.72)

Im Gegensatz zu vielen anderen, die die Klimaverhandlungen schon lange (manchmal auch zu lange) beobachten, neigt Reimer selten dazu, ihre Bedeutung zu überhöhen. Er beschreibt knapp, aber ungeschönt zahlreiche Fehlentwicklungen, die aus dem Kyoto-Protokoll entstanden sind. Unter der Überschrift »Wie der Klimaschutz zum Geschäft wurde« kann nachgelesen werden, welch krumme Geschäfte im Rahmen der ›flexiblen Klimaschutz-Mechanismen‹ abgewickelt werden und warum ausgerechnet Unternehmen wie RWE davon profitierten. »Mit dem ›Clean Development Mechanism‹ entstand ein völlig neuer Wirtschaftszweig«, der zum Klimaschutz allerdings nichts beiträgt, weil Emissionen nur auf dem Papier vermieden werden. (S.106ff.)

Auf dem Buchumschlag wird der Klimaforscher Hartmut Grassl zitiert »Wer wissen will, wie Klimadiplomatie funktioniert, kommt an diesem Buch nicht vorbei«. Dem ist nicht zu widersprechen. Dennoch beschleichen den kritischen Leser früher oder später Zweifel über ihre tatsächliche Bedeutung für den Klimaschutz: »Seit 20 Jahren arbeitet die Maschinerie der Klimadiplomaten an einer Lösung…« (S.85), und herausgekommen sind dabei nur steigende Emissionen. Dass Klimadiplomatie nicht funktioniert – diese Schlussfolgerung lässt der Autor jedoch nicht zu. Nur zwischendurch scheinen kurz Zweifel auf: »Lässt sich mit solchem Gefeilsche die Welt retten?« (S.154)

Wie so oft in der Literatur über den Klimaschutz gibt es auch bei Reimer eine merkwürdige Diskrepanz zwischen der Eindringlichkeit, mit der er die Bedrohung durch den Klimawandel beschreibt, und der Alternativlosigkeit der Klimakonferenzen, die er als einzigen Lösungsweg betrachtet. Auch das Apokalyptische vieler Autorinnen und Autoren, die sich intensiv mit Klimaverhandlungen befassen, kann er nicht ganz vermeiden – trotz des Kopenhagen-Fiaskos 2009, als mit einer Klimakonferenz gleich die ganze Welt gerettet werden sollte. Die Kapitelüberschrift »Schlusskonferenz: Warum Paris über die Zukunft der Demokratie entscheidet« (S.83) zeugt genau davon: Scheitere die 21. Vertragsstaatenkonferenz (COP-21) von Paris, drohe das »Ende einer Epoche« und das bedeute »Verteilungskämpfe, Überlebenskämpfe, kriegerische Auseinandersetzungen oder Weltkrieg. Unvorstellbar, was ein Scheitern bedeutet.« (S.88). Doch die COP-21 hat, obwohl sie anders als Kopenhagen einen Vertrag hervorbrachte, mitnichten die notwendigen Beschlüsse gefasst, um den gefährlichen Klimawandel aufzuhalten, wozu sich die Staaten schon mit der Klimarahmenkonvention 1992 verpflichtet hatten. Sie hat wieder vor allem den Prozess gerettet. Und nicht einmal das ist schon sicher: »Gibt es auch diesmal keine Mehrheit für den Klimaschutz in den USA, wird der neue Klimavertrag scheitern.«, prognostiziert der Autor (S.165). Klimaverhandlungen als Selbstzweck?

Soweit muss man nicht gehen. Dennoch wäre vielleicht das nächste spannende Buch eines, das die Bedeutung der Klimakonferenzen für den tatsächlichen Klimaschutz analysiert. So hat das deutsche Erneuerbare-Energien-Gesetz (EEG) womöglich mehr zum Klimaschutz beigetragen als alle Konferenzbeschlüsse. Es hat quasi im Alleingang einen Massenmarkt für Solar- und Windenergie geschaffen, der die Produktionskosten für diese Technologien stark gesenkt und damit ohne UN-Klimafonds weltweit wettbewerbsfähig gemacht hat. Heute machen diese Technologien in Afrika Energie auch für Arme erschwinglich und zerstören in Europa und den USA die Geschäftsmodelle der Produzenten von Kohle- und Atomstrom. Die Klimapolitik, die uns ohnehin noch Jahrzehnte begleiten wird, bleibt auch künftig ein lohnendes Thema für Analysen.

Nick Reimer

Schlusskonferenz: Geschichte und Zukunft der Klimadiplomatie

München: Oekom 2015, 208 S., 14,95 Euro

Dokumente der Vereinten Nationen

In der folgenden Übersicht sind die Resolutionen und Erklärungen des Präsidenten des Sicherheitsrats der Vereinten Nationen mit einer kurzen Inhaltsangabe und den (etwaigen) Abstimmungsergebnissen von **Oktober 2015 bis Januar 2016** aufgeführt. Die Dokumente sind alphabetisch nach Ländern, Regionen oder Themen sortiert. In der jeweiligen Rubrik erfolgt die Auflistung chronologisch (das älteste Dokument zuerst). Diese **Dokumente im Volltext** sind zu finden über die Webseite des Deutschen Übersetzungsdienstes:
www.un.org/Depts/german

Sicherheitsrat

	UN-Dok.-Nr.	Datum	Gegenstand	Abstimmungsergebnis
Afghanistan	S/RES/2255(2015) + Anlage	21.12.2015	Der Sicherheitsrat **beschließt, dass alle Staaten** im Hinblick **auf die als Taliban bezeichneten Personen und Einrichtungen** sowie auf die nach Resolution 1988(2011) in der Sanktionsliste benannten und mit den Taliban verbundenen Personen, Gruppen und Unternehmen, **die in dieser Resolution enthaltenen Maßnahmen,** wie das Einfrieren der Gelder und anderer finanzieller Vermögenswerte, **ergreifen werden**.	Einstimmige Annahme
Afrika	S/PRST/2015/24	8.12.2015	Der Sicherheitsrat **ermutigt das System der Vereinten Nationen und seine Partner zu weiteren Fortschritten bei der Umsetzung der Integrierten Strategie der Vereinten Nationen für den Sahel** mit dem Ziel, zur Bewältigung der sicherheitsbezogenen und politischen Herausforderungen beizutragen, die die Stabilität und die Entwicklung der Region bedrohen. Er **fordert die internationale Gemeinschaft auf, ihre Zusagen** im Hinblick auf die Ankurbelung des Wirtschaftswachstums, die Beseitigung der Armut und die Unterstützung von Reformen auf dem Gebiet der Regierungsführung **zu erfüllen**.	
Burundi	S/RES/2248(2015)	12.11.2015	Der Sicherheitsrat **fordert die Regierung Burundis** und alle Parteien **auf**, alle Arten von **Gewalt abzulehnen**. Unter nachdrücklicher Verurteilung der zunehmenden Fälle von Menschenrechtsverletzungen, **fordert der Rat die Regierung auf, alle Menschenrechte und Grundfreiheiten** für alle zu achten, **zu schützen und zu gewährleisten**.	Einstimmige Annahme
Côte d'Ivoire	S/RES/2260(2015)	20.1.2016	Der Sicherheitsrat **beschließt, die Militärkomponente der Operation der Vereinten Nationen in Côte d'Ivoire (UNOCI) bis zum 31. März 2016** von 5437 auf 4000 Militärangehörige **zu reduzieren**.	Einstimmige Annahme
Ehemaliges Jugoslawien	S/RES/2247(2015)	10.11.2015	Der Sicherheitsrat **fordert alle Behörden in Bosnien und Herzegowina auf, mit dem Internationalen Strafgerichtshof für das ehemalige Jugoslawien** und dem Internationalen Residualmechanismus für die *Ad-hoc*-Strafgerichtshöfe uneingeschränkt **zusammenzuarbeiten**. Er **ermächtigt die Mitgliedstaaten, bis 9. Oktober 2016 die multinationale Stabilisierungstruppe (EUFOR ALTHEA)** als Rechtsnachfolgerin der Stabilisierungstruppe (SFOR) unter gemeinsamer Führung **einzurichten**.	Einstimmige Annahme
Frauen	S/RES/2242(2015)	13.10.2015	Der Sicherheitsrat fordert die Mitgliedstaaten auf, die Strategien und die Ressourcenausstattung für die **Umsetzung der Agenda für Frauen und Frieden und Sicherheit** zu bewerten und diese weiter in ihre Strategiepläne einzubeziehen. Er **beschließt, Anliegen zum Thema** Frauen und Frieden und Sicherheit durchgängig **in alle länderspezifischen Situationen auf seiner Tagesordnung zu integrieren**. Der Rat **fordert zudem die Hauptabteilung Friedenssicherungseinsätze (DPKO) und die Hauptabteilung Politische Angelegenheiten (DPA) auf**, die notwendigen **geschlechtsspezifischen Analysen in alle Phasen der Planung**, der Mandatsfestlegung, der Durchführung, der Überprüfung und der Personalverringerung **einer Mission zu integrieren**.	Einstimmige Annahme
Friedenssicherung	S/RES/2250(2015)	9.12.2015	Der Sicherheitsrat **fordert die Mitgliedstaaten auf, zu prüfen, wie die inklusive Vertretung Jugendlicher in Entscheidungsprozessen auf allen Ebenen** in den lokalen, nationalen, regionalen und internationalen Institutionen und Mechanismen **zur Verhütung und Beilegung von Konflikten verstärkt werden kann**.	Einstimmige Annahme

Sicherheitsrat

	UN-Dok.-Nr.	Datum	Gegenstand	Abstimmungs-ergebnis
Friedenssicherungs-einsätze	S/PRST/2015/22	25.11.2015	Der Sicherheitsrat **stellt fest, dass der Bericht des Generalsekretärs (S/2015/682) Bereiche aufzeigt**, **in denen der Sicherheitsrat eine Schlüsselrolle zur Stärkung der Friedensmissionen** der Vereinten Nationen **spielen könnte**. Er begrüßt die Initiative des Generalsekretärs, eine **umfassende Überprüfung der UN-Friedensmissionen durchzuführen**, um Maßnahmen zur Stärkung der Rolle, der Kapazität, der Wirksamkeit, der Rechenschaftspflicht und der Effizienz des UN-Systems zu erwägen. Der Rat wird bei der Evaluierung, Mandatierung und Überprüfung von Friedensmissionen vermehrt eine Prioritätensetzung verfolgen.	
	S/PRST/2015/26	31.12.2015	Der Sicherheitsrat **ist sich bewusst, dass** anhaltende **Konsultationen mit dem Sekretariat und den truppen- und polizeistellenden Ländern unerlässlich sind, um zu einem gemeinsamen Verständnis über geeignete Maßnahmen und deren Auswirkungen auf das Mandat und die Durchführung eines Einsatzes zu gelangen.** Er stellt fest, dass die Erfahrung der truppen- und polizeistellenden Länder sowie ihre Kenntnis der Einsatzorte bei der Einsatzplanung sehr hilfreich sein können.	
Internationale Strafgerichte	S/PRST/2015/21	16.11.2015	Der Sicherheitsrat **erinnert an** seine Resolution 1966(2010) über **die Schaffung des Internationalen Residualmechanismus für die *Ad-hoc*-Strafgerichtshöfe** zu dem Zweck, die verbleibenden Aufgaben des Internationalen Strafgerichtshofs für das ehemalige Jugoslawien (ICTY) und des Internationalen Strafgerichtshofs für Ruanda (ICTR) zu erfüllen. Der Rat **ersucht den Mechanismus, bis zum 20. November 2015 einen Bericht über die Fortschritte bei seiner Arbeit vorzulegen**.	
	S/RES/2256(2015)	22.12.2015	Der Sicherheitsrat **begrüßt den Abschluss der richterlichen Arbeit des ICTR** nach dem Erlass seines letzten Urteils am 14. Dezember 2015 und die Auflösung des Gerichts am 31. Dezember 2015. Er **beschließt, die Amtszeit der ständigen Richter und Ad-litem-Richter beim ICTY** bis zum 31. März 2016 beziehungsweise 30. Juni 2016 oder bis zum Abschluss der zugewiesenen Fälle **zu verlängern**. Ferner **beschließt der Rat, Serge Brammertz für eine am 31. Dezember 2016 endende Amtszeit erneut zum Ankläger des ICTY zu ernennen**.	+14; -0; =1 (Russland)
Libyen	S/RES/2259(2015)	23.12.2015	Der Sicherheitsrat **begrüßt die Unterzeichnung des Libyschen politischen Abkommens** von Skhirat (Marokko) am 17. Dezember 2015, **das die Bildung einer Regierung der nationalen Eintracht vorsieht**, die aus dem Präsidentschaftsrat und dem Kabinett besteht. Der Rat **begrüßt** ferner **die Bildung des Präsidentschaftsrats und fordert diesen auf, zügig auf die Bildung einer Regierung hinzuarbeiten**.	Einstimmige Annahme
Nahost	S/RES/2257(2015)	22.12.2015	Der Sicherheitsrat **beschließt, das Mandat der Beobachtertruppe der Vereinten Nationen für die Truppenentflechtung (UNDOF) bis zum 30. Juni 2016 zu verlängern**.	Einstimmige Annahme
Ostafrikanisches Zwischenseengebiet	S/PRST/2015/20	9.11.2015	Der Sicherheitsrat **fordert die sofortige Wiederaufnahme der gemeinsamen Offensiveinsätze der Streitkräfte der Demokratischen Republik Kongo und der** Interventionsbrigade in Zusammenarbeit mit der **Organisation der Vereinten Nationen in der Demokratischen Republik Kongo (MONUSCO)**. Er f**ordert ferner die Regierung auf**, die erfolgreiche und fristgerechte Abhaltung von Wahlen, insbesondere der **Präsidentschafts- und Parlamentswahlen im November 2016, zu gewährleisten.**	
Somalia	S/RES/2245(2015)	9.11.2015	Der Sicherheitsrat **beschließt, dass das Büro der Vereinten Nationen zur Unterstützung der Mission der Afrikanischen Union in Somalia** (UNSOA) **die Bezeichnung ›Unterstützungsbüro der Vereinten Nationen in Somalia‹ (UNSOS) tragen soll**. Es wird dafür verantwortlich sein, die AMISOM, die Hilfsmission der Vereinten Nationen in Somalia (UNSOM) und die Somalische Nationalarmee zu unterstützen.	Einstimmige Annahme
	S/RES/2246(2015)	10.11.2015	Der Sicherheitsrat **unterstreicht, dass die somalischen Behörden die Hauptverantwortung im Kampf gegen Seeräuberei** und bewaffnete Raubüberfälle **vor der Küste Somalias tragen und begrüßt den Entwurf des Gesetzes über eine Küstenwache**, den die somalischen Behörden vorgelegt haben. Er fordert die Behörden nachdrücklich auf, weiter daran zu arbeiten, ohne Verzögerung einen umfassenden Katalog von Rechtsvorschriften zur Bekämpfung der Seeräuberei zu erlassen.	Einstimmige Annahme

Sicherheitsrat

	UN-Dok.-Nr.	Datum	Gegenstand	Abstimmungs-ergebnis
Sudan/Südsudan	S/RES/2251(2015)	15.12.2015	Der Sicherheitsrat **beschließt, das Mandat der Interims-Sicherheitstruppe der Vereinten Nationen für Abyei (UNISFA) bis zum 15. Mai 2016 zu verlängern**. Der Rat **verlangt, dass Sudan und Südsudan** im Einklang mit ihren Verpflichtungen aus dem Abkommen vom 20. Juni 2011 **dringend mit der Einrichtung der Verwaltung und des Rates des Gebiets Abyei beginnen**.	Einstimmige Annahme
	S/RES/2252(2015)	15.12.2015	Der Sicherheitsrat **beschließt, das Mandat der Mission der Vereinten Nationen in der Republik Südsudan (UNMISS) bis 31. Juli 2016 zu verlängern und die Truppenstärke** auf bis zu 13 000 Soldaten und 2001 Polizisten **zu erhöhen**. Die UNMISS hat das Mandat, alle erforderlichen Mittel einzusetzen, um ihre Aufgaben wahrzunehmen.	+13; -0; =2 (Russland, Venezuela)
Syrien	S/RES/2254(2015)	18.12.2015	Der Sicherheitsrat **bestätigt erneut, dass er das Genfer Kommuniqué vom 30. Juni 2012 billigt**. Er schließt sich der Gemeinsamen Erklärung über das Ergebnis der multilateralen Gespräche über Syrien vom 30. Oktober 2015 und der Erklärung der Unterstützungsgruppe vom 14. November 2015 an, **mit dem Ziel, die vollständige Umsetzung des Genfer Kommuniqués als Grundlage für einen politischen Übergang** unter syrischer Führungs- und Eigenverantwortung **und so die Beendigung des Konflikts in Syrien zu bewirken**. Der Rat betont, dass das syrische Volk über die Zukunft des Landes entscheiden wird.	Einstimmige Annahme
	S/RES/2258(2015)	22.12.2015	Der Sicherheitsrat verlangt, dass alle Parteien, insbesondere die syrischen Behörden, den Verpflichtungen nach dem Völkerrecht sofort nachkommen. Der Rat **beschließt, die Beschlüsse seiner Resolution 2165(2014) bezüglich humanitärer Hilfslieferungen und des** dem UN-Generalsekretär unterstellten **Überwachungsmechanismus bis zum 10. Januar 2017 zu verlängern**. Er ersucht die syrischen Behörden, alle von den UN und ihren Durchführungspartnern eingereichten Anträge betreffend Lieferungen, die Konfliktlinien überschreiten, wohlwollend zu prüfen.	Einstimmige Annahme
Terrorismus	S/RES/2249(2015)	20.11.2015	Der Sicherheitsrat **verurteilt die fortgesetzten schweren Menschenrechtsverletzungen und Verstöße gegen das humanitäre Völkerrecht sowie die barbarischen Akte der Zerstörung und Plünderung von Kulturerbe, die vom** Islamischen Staat in Irak und der Levante (**ISIL**, auch bekannt als Da'esh) **begangen werden**. Er **fordert die Mitgliedstaaten auf**, in dem unter der Kontrolle des ISIL stehenden Gebiet in Syrien und Irak alle **notwendigen Maßnahmen zu ergreifen** und ihre Anstrengungen zu verstärken und zu koordinieren**, um terroristische Handlungen zu verhüten und zu unterbinden**.	Einstimmige Annahme
	S/PRST/2015/25	16.12.2015	Der Sicherheitsrat **beklagt alle vom ISIL begangenen Akte des Menschenhandels** sowie alle begangenen Verstöße gegen das humanitäre Völkerrecht und Menschenrechtsverletzungen. Er **unterstreicht**, **dass bestimmte mit dem Menschenhandel verbundene Handlungen im Kontext bewaffneten Konflikts Kriegsverbrechen darstellen können**. Er **fordert die Mitgliedstaaten auf**, zu erwägen, **das Übereinkommen der Vereinten Nationen gegen die grenzüberschreitende Organisierte Kriminalität und das Zusatzprotokoll zur Verhütung, Bekämpfung und Bestrafung des Menschenhandels**, insbesondere des Frauen- und Kinderhandels, **zu ratifizieren beziehungsweise** ihnen **beizutreten**.	
	S/RES/2253 (2015) + Anlagen I, II	17.12.2015	Der Sicherheitsrat **beschließt, dass der Al-Qaida-Sanktionsausschuss** fortan **als ISIL (Da'esh)- und Al-Qaida-Sanktionsausschuss und die Al-Qaida-Sanktionsliste** fortan **als die ISIL (Da'esh)- und Al-Qaida-Sanktionsliste bezeichnet wird**. Er **beschließt, dass alle Staaten die** bereits mit den Resolutionen 1333(2000), 1390(2002) und 1989(2011) verhängten **Maßnahmen bezüglich des Einfrierens von Vermögenswerten, des Reiseverbots und der Waffenembargos im Hinblick auf ISIL, Al-Qaida und die mit ihnen verbundenen Personen**, Gruppen, Unternehmen und Einrichtungen **ergreifen**.	Einstimmige Annahme
Verfahren	S/PRST/2015/19	30.10.2015	Der Sicherheitsrat b**ekundet seine Absicht,** auch künftig **eine jährliche Ansprache über seine Arbeitsmethoden abzuhalten und** bekräftigt seine Entschlossenheit, **seine Arbeitsmethoden weiter zu prüfen**. Er unterstreicht, wie wichtig eine verstärkte Koordinierung und Zusammenarbeit zwischen den Hauptorganen der Vereinten Nationen sowie mit anderen zuständigen Organisationen ist.	

German Review on the United Nations | Abstracts

Volume 64 | 2016 | No. 2

United Nations in Cyberspace

Tim Maurer pp. 51–55

Cybersecurity in a Complex Environment

Transatlantic Divergences and Diplomatic Achievements

In December 2015, a cyber-attack caused a blackout in Western Ukraine. It was the first known blackout during a conflict to have been caused by malware. However, this is only the latest in a series of high-profile incidents in recent years that illustrate the deteriorating cybersecurity environment. The international community has become increasingly alarmed by these developments and has ramped up diplomatic efforts to address the problem. One of the key forums for these discussions is the United Nations. Dating back to a first draft resolution introduced in 1998, the First Committee has been discussing this issue for the past eight years, reaching several important diplomatic agreements along the way. This article outlines the history of this discussion by breaking it up into four different phases. As the Obama administration is nearing its end, it also examines which direction this agenda will take in the future.

Tatiana Tropina · Nicolas von zur Mühlen pp. 56–60

Crimes in the Digital Sphere

The United Nations' Fight against Cybercrime

Effective prevention, disruption and investigation of cybercrime require a wide variety of technical, organizational and legal measures. Due to the transnational nature of information and communications networks, the harmonization of legislation and procedural frameworks is necessary to avoid safe havens for cybercriminals, carry out cross-border investigations and collect electronic evidence. Therefore, international standard-setting and efforts to facilitate international cooperation in criminal investigations have become some of the central issues on the agenda of many international organizations. This article aims to provide an analysis of the role the United Nations has played, and still does play, in the efforts to build capacity and set standards to tackle the problem of cybercrime.

Anja Mihr pp. 61–66

Threatened Human Rights in Cyberspace

The Internet is a tool for the implementation of fundamental civil and political rights as well as social and economic human rights, particularly in the context of the realization of the Sustainable Development Goals (SDGs). But the international community has thus far not been able to protect and fully promote human rights offline or online. In the light of these challenges, the UN General Assembly has passed a resolution concerning the multi-stakeholder approach as a mechanism to implement, realize and protect globally agreed human rights norms and standards in cyberspace.

Wolfgang Kleinwächter pp. 67–72

Who Governs the Internet?

Internet Governance Being Tested

Cyberspace, with its 3.2 billion Internet users, has become a main subject of political controversy in recent years. On the one hand, a number of governments want to regulate all Internet-related issues through a multilateral, legally-binding instrument. On the other hand, the concept of 'multistakeholderism' gains more and more support. In the 'Internet Governance Ecosystem', numerous governmental and non-governmental players coexist and work hand in hand to manage various technical and non-technical issues. The UN-based Internet Governance Forum (IGF), established in 2005, is the main platform for discussion of those issues. In December 2015, the 70th UN General Assembly renewed its mandate until 2025.

Markus Wagner pp. 73–78

The Future of Warfare?

Autonomous Weapon Systems as a Challenge for International Law

The question of how to deal with autonomous weapon systems (AWS) is no longer academic. Indeed, there are contemporary challenges with respect to their compliance with international law. The article outlines the applicable international humanitarian law framework concerning AWS, specifically the principle of distinction and the principle of proportionality. It concludes that at this point, and despite impressive technological advances in autonomous technology, the deployment of autonomous weapon systems would be impermissible only for circumstances in which they are not needed. The article embeds the legal debate in the larger policy debate concerning AWS. Finally, it describes the current regulatory approaches under discussion and assesses their viability.

Impressum

Vereinte Nationen
Zeitschrift für die Vereinten Nationen und ihre Sonderorganisationen.
Begründet von Kurt Seinsch. ISSN 0042-384X
ISSN (Online): 2366-6773

Herausgeber:
Deutsche Gesellschaft für die Vereinten Nationen (DGVN), Berlin.

Leitung der Redaktion: Sylvia Schwab
Redaktion/DTP: Monique Lehmann

Redaktionsanschrift: Vereinte Nationen
Zimmerstr. 26/27, D–10969 Berlin
Telefon: +49 (0)30 | 25 93 75–10
Telefax: +49 (0)30 | 25 93 75–29
E-Mail: zeitschrift@dgvn.de
Internet: www.dgvn.de/zeitschrift-vereinte-nationen

Druck und Verlag:
BWV · Berliner Wissenschafts-Verlag GmbH
Markgrafenstraße 12–14, D-10969 Berlin
Telefon: +49 (0)30 | 84 17 70–0
Telefax: +49 (0)30 | 84 17 70–21
E-Mail: bwv@bwv-verlag.de
Internet: www.bwv-verlag.de

Erscheinungsweise: zweimonatlich
(Februar, April, Juni, August, Oktober, Dezember)

Bezugspreise des BWV:
Jahresabonnement Printausgabe 63,– Euro*
Jahresabonnement Onlineausgabe 63,– Euro
Jahresabonnement Print- und Onlineausgabe 79,– Euro*
Einzelheft 13,– Euro*
*Alle Preise inkl. MwSt., zzgl. Porto.

Bestellungen nehmen entgegen:
E-Mail: vertrieb@bwv-verlag.de
Tel.: +49 (0)30 | 84 17 70–22
Fax: +49 (0)30 | 84 17 70–21
sowie der Buchhandel.

Kündigung drei Monate vor Kalenderjahresende. Zahlungen im Voraus an:
BWV · Berliner Wissenschafts-Verlag GmbH,
Postbank Berlin, Konto Nr.: 28 875 101,
BLZ 100 100 10, IBAN DE 39 1001 0010 00288751 01,
SWIFT (BIC): PBNKDEFF.

Für **Mitglieder** der DGVN ist der Bezugspreis im Mitgliedsbeitrag enthalten.

Anzeigenverwaltung und Anzeigenannahme:
Berliner Wissenschafts-Verlag GmbH
Brigitta Weiss
Tel.: +49 (0)30 | 84 17 70–14
Fax: +49 (0)30 | 84 17 70–21
E-Mail: weiss@bwv-verlag.de

Vereinte Nationen wird auf Recycling-Papier aus 100% Altpapier gedruckt.

Deutsche Gesellschaft für die Vereinten Nationen

Landesverbände

Landesverband Baden-Württemberg
Vorsitzender:
Prof. Dr. Karl-Heinz Meier-Braun
karl-heinz.meier-braun@swr.de

Landesverband Bayern
Vorsitzende: Ulrike Renner-Helfmann
info@dgvn-bayern.de

Landesverband Berlin-Brandenburg
Vorsitzender: Dr. Lutz-Peter Gollnisch
info@dgvn-berlin.de

Landesverband Hessen
Vorsitzender: Dustin Dehez
info@dgvn-hessen.org

Landesverband Nordrhein-Westfalen
Vorsitzender:
Dr. Michael-Lysander Fremuth
kontakt@dgvn-nrw.de

Landesverband Sachsen,
Sachsen-Anhalt, Thüringen
Vorsitzender: Kai Ahlborn
info@dgvn-sachsen.de

Generalsekretariat
Dr. Lisa Heemann, Generalsekretärin
Deutsche Gesellschaft für die Vereinten Nationen
Zimmerstr. 26/27, D–10969 Berlin
Telefon: 030 | 25 93 75–0
info@dgvn.de | www.dgvn.de