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.