Deutsche Gesellschaft für die Vereinten Nationen e.V.

UN-BASIS-INFORMATIONEN 61

Konflikte im Cyberspace

GEEIGNET FÜR UN im Klassenzimmer

DYNAMIKEN ZWISCHENSTAATLICHER CYBER-KONFLIKTE

Immer mehr Staaten entwickeln offensive Cyber-Fähigkeiten, um in vernetzten Gesellschaften Schäden verursachen zu können. Seit den frühen 2000ern gibt es in den Vereinten Nationen Versuche, diese Entwicklung einzudämmen. Zwar haben sich Staaten grundsätzlich darauf geeinigt, dass das Völkerrecht auch zur Eindämmung digitaler Konflikte gilt, allerdings gibt es keine Einigung über die genaue Umsetzung. Unterschiedliche Interessen, Ordnungsvorstellungen und die Charakteristika digitaler Technologien erschweren bisher die Schaffung rechtlich bindender Verträge oder eines Cyber-Rüstungskontrollregimes.

Informations- und Kommunikationstechnologien (IKT) haben in bewaffneten Konflikten schon immer eine Rolle gespielt. Durch die Vernetzung von IT-Systemen über das Internet, aber auch durch die Durchdringung des physischen Raums mit Hilfe von Computern (›Internet der Dinge‹ – IoT) oder industriellen Steuerungssystemen, steigt die Verwundbarkeit moderner Gesellschaften durch Cyber-Angriffe. Intelligente Energienetze basieren auf feinabgestimmter Computer-Steuerung, ebenso wie autonome Fahr- und Flugzeuge. Durch diese Vernetzung kommt es vor, dass immer mehr zivile Einrichtungen durch den Missbrauch von IKT zu Schaden kommen. Daneben bietet der durch das Internet geschaffene Kommunikationsraum, der Cyberspace, zahlreiche Möglichkeiten an Landesgrenzen und staatlichen Kontrollorganen vorbei, auf gesellschaftliche Diskurse in anderen Staaten einzuwirken. Die weltweite Verbreitung dieser Technologien hat somit Auswirkungen auf die kollektive Sicherheit, den Frieden und das Völkerrecht – allesamt Kernanliegen der UN. In der Vergangenheit haben die Vereinten Nationen bei der Regulierung und Eingrenzung neuer Waffentechnologien, etwa Giftgas, Kernwaffen oder Landminen, immer eine Rolle gespielt. Insofern stellt sich die Frage, welche Maßnahmen die UN unternehmen, um die Gefahr des Missbrauchs von IKT auf internationaler Ebene einzudämmen.

Cyber-Angriffe in Echtzeit, einschließlich Informationen über den Ursprung, die Art und das Ziel des Angriffs sowie die IP-Adresse des Angreifers, den geografischen Standort und die verwendeten Ports, werden auf einer Karte der für den Luftraum zuständigen Teil der US-Nationalgarde sichtbar gemacht.
Foto: Airman Magazine/Flickr (CC BY-NC 2.0)

Unter Cyber-Fähigkeiten versteht man die Fähigkeit zum Ausführen von Cyber-Angriffen, also das Eindringen in ein fremdes IT-System, mit dem Ziel der Spionage, der Beeinflussung und/oder Sabotage. Physische Zerstörung von Maschinen, Stromausfälle durch Cyber-Angriffe, aber auch die Beeinflussung gesellschaftlicher Diskurse, mittels IT-gestützter Desinformationsoperationen, sind damit möglich geworden. Offensive Cyber-Fähigkeiten spielen mittlerweile in zahlreichen Konflikten eine Rolle. Angetrieben durch diese Bedrohungen rüsten Staaten im Digitalen auf und erschaffen eigene militärische Cyber-Kommandos. Da Cyber-Angriffe durch das Internet eine globale Reichweite haben, sind Rüstungswettläufe und die daraus entstehenden Sicherheitsdilemmata im Informationszeitalter nicht mehr regional begrenzt, sondern tendenziell global. Es wird geschätzt, dass um die 100 Staaten über offensive Cyber-Fähigkeiten verfügen. Die Anzahl von Cyber-Angriffen ist in den letzten 20 Jahren um ein Vielfaches angestiegen. Diese verursachen jährlich geschätzte Kosten in Höhe von 600 Milliarden US-Dollar. Die Nutzung dieser Fähigkeiten ist dabei weitgehend unreguliert, sodass hier die Gefahr von Fehlwahrnehmungen und Eskalationen besteht. Große Cyber-Vorfälle wie ›WannaCry‹ (2017) oder ›Not-Petya‹ (2017), die hunderttausende IT-Systeme befielen, zeigen die Gefahr, die von Rüstungswettläufen ausgeht. Beide Vorfälle basierten auf einer Angriffssoftware der USA, die Drittparteien nutzten. Solche Begleitschäden werden in Zukunft mit höherer Intensität und höherer Frequenz auftreten.

REGULIERUNGSVERSUCHE VON CYBER-KONFLIKTEN

Bemühungen, die negativen Effekte von Informationstechnologien zu begrenzen, wurden erstmals im Jahr 1998 von Russland unternommen, das die Entwicklungen des Kosovo-Krieges kritisch beäugte und in dem erste Cyber-Fähigkeiten verwendet wurden. Russland reichte eine Resolution in der UN-Generalversammlung ein, in der die destabilisierenden Effekte von Informationstechnologien für die Sicherheit von Staaten dargestellt wurden. Es setzte sich dafür ein, dass UN-Mitgliedstaaten und der UN-Generalsekretär diesbezüglich Positionen erarbeiten sollten, um internationale Prinzipien zum Schutz globaler informationstechnologischer Systeme zu entwickeln. Seitdem hat Russland immer wieder ähnliche Resolutionen mit dem Ziel eingereicht, einen völkerrechtlich bindenden Vertrag zu schaffen, der die Nutzung des Cyberspace für militärische Zwecke hätte unterbinden sollen. Ein solcher bindender Cyber-Vertrag existiert aber aufgrund zahlreicher konzeptioneller und politischer Probleme bisher nicht.

Im Jahr 2002 wurde durch den früheren UN-Generalsekretär Kofi Annan eine Gruppe von Regierungsexpertinnen und -experten der Vereinten Nationen für Entwicklungen auf dem Gebiet der Information und Telekommunikation im Kontext der internationalen Sicherheit (UN GGE) ins Leben gerufen. Das Ziel dieser UN GGE war es, Konzepte für die Sicherheit globaler IT-Systeme zu entwickeln. Sie traf sich erstmalig im Jahr 2004. Die Gruppe bestand aus 15 Personen der UN-Mitgliedstaaten, inklusive den fünf ständigen Mitglieder im Sicherheitsrat (P5). Die übrigen Mitglieder wurden auf Basis geografischer Verteilung ausgewählt. Seitdem ist die Gruppe auf 25 angewachsen. Die Sitzungen finden in einem geschlossenen Rahmen statt und es gibt keine Zwischenberichte. Die Gruppe wird von einem Vorsitz geleitet und bestimmt weitgehend selbst über die Agenda. Innerhalb des UN-Systems gehört die UN GGE zum ersten Ausschuss der Generalversammlung für Abrüstung und internationale Sicherheit. Andere Internet-Themen wie Cyber-Spionage, Internet Governance und Datenschutz sind daher nicht Agenda der UN GGE. Das Ziel aller UN GGEs ist es seither, Berichte zu erstellen, auf die sich alle Mitglieder verständigen können. Dieses Vorhaben scheiterte bereits mit dem ersten Bericht im Jahr 2005. Die erste UN GGE konnte in der Frage, ob das Völkerrecht und das humanitäre Völkerrecht alle Sicherheitsaspekte von Informationstechnologien und deren bösartige Nutzung in Gänze abdecken könne, keine Einigung erzielen.

ÜBERSICHT ÜBER BISHERIGE UN GGEs

JAHRE	GRUPPE	RESOLUTION	BERICHT
2004/2005	1. UN GGE	A/RES/58/32	A/60/202 (keine Einigung)
2009/2010	2. UN GGE	A/RES/60/45	A/65/201
2012/2013	3. UN GGE	A/RES/66/24	A/68/98
2014/2015	4. UN GGE	A/RES/68/243	A/70/174
2016/2017	5. UN GGE	A/RES/70/237	A/72/327 (keine Einigung)
2019/2021	6. UN GGE	A/RES/73/266	
2019/2020	OEWG*	A/RES/73/27	

*Offene Arbeitsgruppe, Quelle: UN-Büro für Abrüstungsfragen (UNODA)

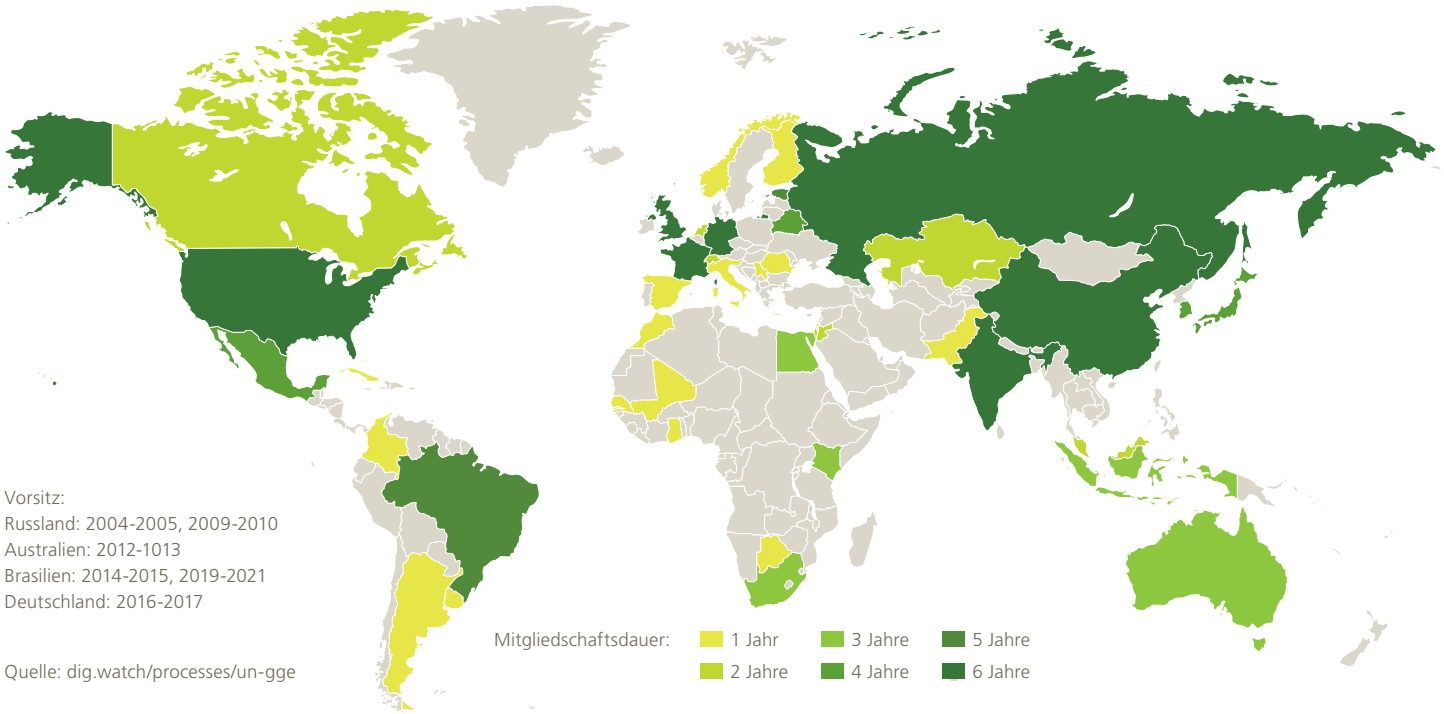
Gegen Ende des Jahres 2005 rief die Generalversammlung die zweite Expertenrunde ein, die im Jahr 2010 einen einstimmig verabschiedeten Bericht samt Empfehlungen vorlegte. Die Relevanz der UN GGE hatte sich zwischenzeitlich mit den Cyber-Angriffen auf Estland im Jahr 2007 und im Georgienkonflikt ein Jahr später, beide mutmaßlich durch russische Angriffe verursacht, verschärft. Treffend stellte der Bericht fest, dass IKT eine stärkere Rolle bei Konflikten spielen, wie schwierig es ist, die Urheber von Cyber-Angriffen zu ermitteln und wie fehlende Verhaltensstandards das Risiko für Fehlwahrnehmungen und Instabilitäten verschärfen. Um daraus entstehende Sicherheitsrisiken wie Eskalationen durch Fehlwahrnehmungen zu verhindern sollten gemeinsame Normen für angemessen staatliches Verhalten im Cyberspace, sowie vertrauensbildende Maßnahmen entwickelt werden. Konkrete, legale Prinzipien wurden indes nicht vorgelegt. Die zweite UN GGE entwickelte fünf Empfehlungen für vertrauensbildende Maßnahmen, um das Risiko von Fehlwahrnehmungen nach Cyber-Vorfällen zu reduzieren:

- Die Diskussionen um Normen staatlichen Verhaltens sollten fortgesetzt werden, um das Risiko von Angriffen auf kritische Infrastrukturen zu reduzieren.
- Nationale Sichtweisen sollen über die Nutzung von IKT in Konflikten ausgetauscht werden.
- Nationale Cyber-Sicherheitsmaßnahmen, Strategien und bewährte Verfahrensweisen sollen ausgetauscht werden.
- Der Aufbau eigener Kapazitäten zum Schutz von IT-Systemen in Entwicklungsländern soll gestärkt werden.
- Gemeinsame Begriffe und Definitionen sollen entwickelt werden.

Im Dezember 2011 wurde die dritte UN GGE einberufen, mit dem Ziel konkrete Normen und Prinzipien für verantwortliches Staatenverhalten zu entwickeln. Der Bericht wurde im Jahr 2013 veröffentlicht und stellte zum ersten Mal fest, dass Völkerrecht im Allgemeinen und die UN-Charta im Speziellen für den Cyberspace gelten. Daher gilt auch im Cyberspace das Souveränitätsprinzip: Das heißt, Staaten sind für Cyber-Aktivitäten in ihrem Territorium verantwortlich. Aus diesem Grund sind Aktivitäten zu unterlassen, die die Souveränität anderer Staaten verletzen. Parallel dazu stellte eine Resolution der UN-Generalversammlung fest, dass die Menschenrechte offline wie online gelten. Aus diesem sich abzeichnenden Rechtsverständnis lassen sich konkrete Normen über angemessenes staatliches Handeln im Cyberspace ableiten: Der Schutz von IKT muss Hand in Hand mit dem Schutz von Menschenrechten gehen. Ferner sollen Staaten keine Proxy-Akteure, also Drittakteure im staatlichen Auftrag (›Cyber-Söldner‹), für illegale Cyber-Aktivitäten nutzen und dafür sorgen, dass von ihrem Territorium keine völkerrechtswidrigen Akte ausgehen. Mit dem Bericht der UN GGE erkannten die USA sowie China und Russland diese Prinzipien an. Neben vertrauensbildenden Maßnahmen gibt der Bericht Empfehlungen für den Aufbau von Kapazitäten zum Schutz von IKT ab.

Die vierte UN GGE wurde im Dezember 2013 ins Leben gerufen und lieferte im Jahr 2015 ihren einstimmig angenommenen Bericht ab. Das Dokument bestätigte einige der Elemente vergangener Berichte

UN GGE-MITGLIEDSTAATEN 2019-2021



und Resolutionen der Generalversammlung und bestimmte sie näher. Dazu gehört das Prinzip, dass Staaten rechtlich verantwortlich für die IKT in ihrem Territorium sind, dass sie das Souveränitätsprinzip inklusive der Nichteinmischung in die inneren Angelegenheiten anderer Staaten beachten sollten und dass Konflikte im Cyberspace mit friedlichen Mitteln beigelegt werden sollen. Ein zentrales Element ist auch die Berücksichtigung anderer Resolutionen, die das Recht auf Privatsphäre im Cyberspace anerkennen. Bezüglich der Verwendung von Cyber-Fähigkeiten in Konflikten stellte der Bericht fest, dass die Prinzipien der Menschlichkeit sowie die Notwendigkeit, Verhältnismäßigkeit und Zuordnung bei Cyber-Angriffen genau so gelten wie bei konventionellen Angriffen. Diese Prinzipien des humanitären Völkerrechts bedeuten, dass Cyber-Angriffe zwischen zivilen und militärischen Zielen unterscheiden müssen, sie nicht unnötiges menschliches Leid hervorrufen dürfen, sie nur zur Erlangung konkreter militärischer Ziele verwendet werden dürfen und der Einsatz von Waffen im Verhältnis zu dessen Zielen stehen muss. Erste inhaltliche Konflikte tauchten bei der Frage auf, wie genau diese Prinzipien bei Cyber-Angriffen umzusetzen beziehungsweise messbar zu machen seien. Ferner verständigten sich die Mitglieder darauf, dass Staaten keine Proxy-Akteure einsetzen dürfen, die international schädigende Akte verüben. Der Einsatz dieser Akteure unter staatlicher Steuerung, Aufsicht oder Tolerierung ist ein allgegenwärtiges Element von Cyber-Angriffen. Der UN GGE-Bericht beinhaltete auch erstmals das Prinzip der Sorgfaltsverantwortung. Es überträgt Staaten die Verantwortung, dass ihr nationales Territorium nicht zur Verübung von völkerrechtswidrigen Handlungen genutzt wird. Wenn also eine kriminelle Hackergruppe vom eigenen Territorium operiert und weltweit Schäden anrichtet, wäre der Staat dafür verantwortlich, sofern er diese Akteure identifizieren kann.

Darüber hinaus entwickelte der Bericht aus dem Jahr 2015 eine Liste von Normen und vertrauensbildenden Maßnahmen, etwa dass sich Staaten gegenseitig beim Informationsaustausch bei Cyber-Vorfällen und bei digitaler Strafverfolgung unterstützen sollen. Gleichzeitig sollen sie die Menschenrechte im digitalen Raum beachten, keine Aktivitäten durchführen, die kritische Infrastrukturen wie die Stromversorgung in anderen Ländern beeinträchtigen oder gar globalen Lieferketten von IT-Systemen aktiv schaden. Ferner sollen die ›digitalen Feuerwehren‹, die Computersicherheits-Ereignis- und Reaktionsteams (CERT), die Schadensminimierung nach Cyber-Vorfällen durchführen, nicht geschädigt oder gar für illegale Aktivitäten missbraucht werden. Die CERTs können entweder öffentlich, privatwirtschaftlich oder individuell organisiert sein.

Im Dezember 2015 wurde die fünfte UN GGE eingerichtet. Ziel war es, die zuvor aufgetauchten inhaltlichen Konflikte anzusprechen und herauszuarbeiten, wie genau das Völkerrecht bei der staatlichen Verwendung von IKT anzuwenden sei. Allerdings stellten sich diese als zu groß heraus, sodass im Jahr 2017 kein Bericht vorgelegt werden konnte.

KONFLIKTE UM DIE REGULIERUNG VON CYBER-KONFLIKTEN

Mit der fünften UN GGE begann das gemeinsame Verständnis darüber, dass das Völkerrecht auch im Cyberspace gelte, zu bröckeln. Im Verhalten einiger Mitgliedstaaten zeichnete sich eine Blockadehaltung bei der Weiterentwicklung des Prozesses ab. Zwar herrscht weiterhin Einigkeit darin, dass das Völkerrecht im Cyberspace gelte, aber wie genau die darin enthaltenden Prinzipien umzusetzen sind, sorgte für Streit. Inhaltliche Unterschiede zwischen westlichen Staaten und insbesondere China, Russland und Kuba bestanden in der Frage, inwiefern das Recht auf Selbstverteidigung sowie Gegenmaßnahmen zur Beantwortung von Cyber-Angriffen nach der UN-Charta im Cyberspace Anwendung finden können. Westliche Staaten vertreten die Position, dass das gesamte Völkerrecht gelte, während Staaten wie China und Russland hier nur auf bestimmte Aspekte wie Souveränitätsrechte bestehen. Sie argumentieren, dass Aspekte des Völkerrechts den Realitäten von IKT nicht gerecht werde und daher neue Rechtsprinzipien entwickelt werden müssten.

Sitzung des Innovationsdialogs ›Digitale Technologien & Internationale Sicherheit‹ des Instituts der Vereinten Nationen für Abrüstungsforschung (UNIDIR) im Jahr 2019 in Genf. Der Dialog untersucht Technologien, wie etwa künstliche Intelligenz, Quanteninformatik und das Internet der Dinge, die derzeit noch nicht offiziell auf der multilateralen Abrüstungsagenda stehen.
Foto: UN Photo/Jean-Marc Ferré

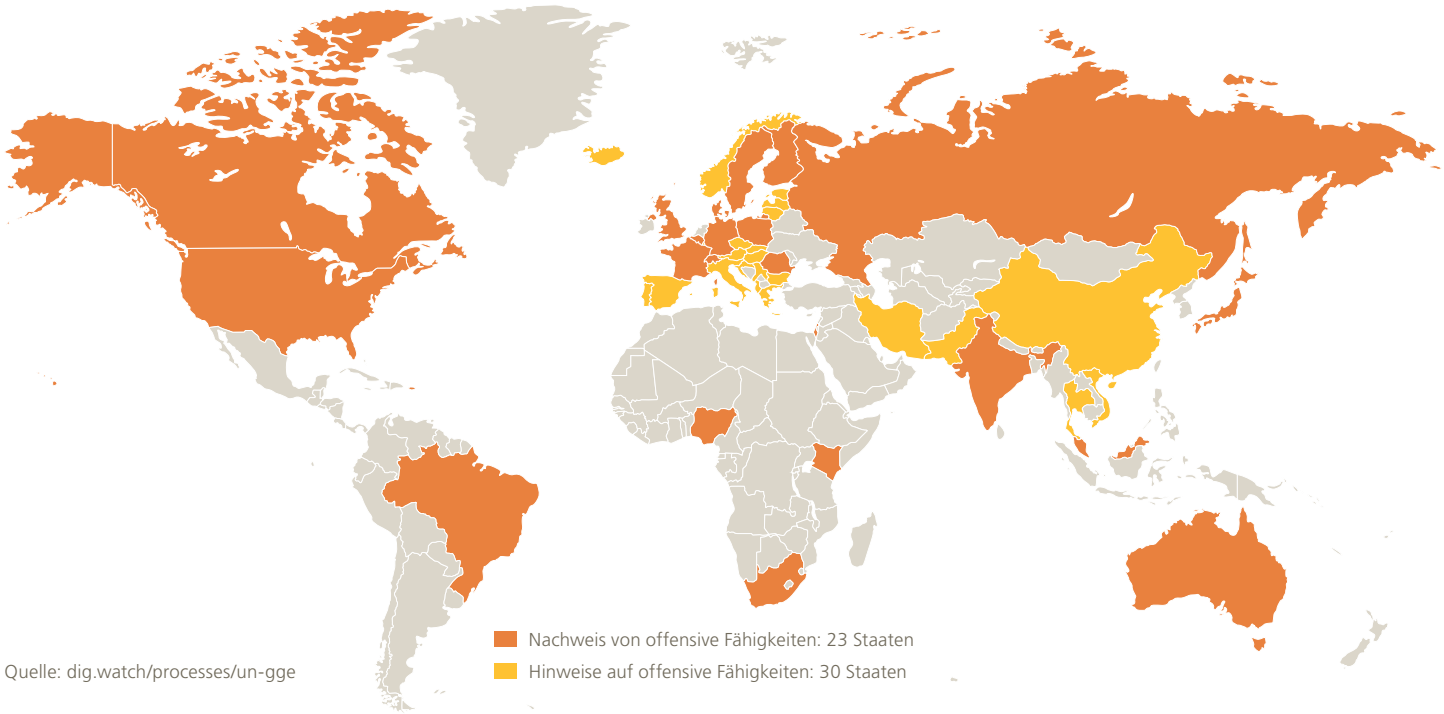
Ein Konfliktpunkt dabei war, inwiefern die im Jahr 2015 erstellten Bericht vereinbarten Prinzipien des humanitären Völkerrechts konkret gelten sollen. Wie sind diese Kriterien bei Cyber-Angriffen zu bemessen? Kann in globalen, dezentralen Netzen überhaupt sinnvoll zwischen zivilen und militärischen Zielen unterschieden werden? Ab wann ist ein Cyber-Angriff verhältnismäßig? Ferner stellt sich die Frage, inwiefern das Völkerrecht auf Cyber-Angriffe anwendbar ist, die in Friedenszeiten stattfinden. Denn mittlerweile besteht ein Trend hin zu ›hybriden Operationen‹, die insbesondere seit dem Jahr 2014 verstärkt von Russland ausgehen und Staaten in unmittelbarer Nachbarschaft betreffen. Derartige Operationen zielen weniger auf technische Sabotage ab, sondern auf psychologische Effekte und die Beeinflussung von Öffentlichkeiten in anderen Staaten. Dabei setzt man auf bewährte Techniken der Propaganda und Desinformation und paart diese mit neuen Möglichkeiten von IKT, etwa der massenhaften Verbreitung von Inhalten in sozialen Netzwerken, Verschwörungstheorien und dem Einsatz von ›Memes‹, also die Verbreitung kleiner Medieninhalte in Form von Text-Bild-Kombinationen. Da diese Operationen verdeckt stattfinden und nicht notwendigerweise einen militärischen Charakter haben, greift hier das Völkerrecht nicht, da dieses sich im Wesentlichen auf bewaffnete Konflikte konzentriert. Eine offene Frage dabei ist, ob der Einsatz solcher Desinformationskampagnen, die keine physischen Schäden oder wirtschaftliche Verluste erzeugen, eine Verletzung des Souveränitätsprinzips von Staaten darstellen.

Ein Problem dabei ist, dass Cyber-Angriffe sehr unterschiedliche Eigenschaften und Effekte haben können. Ein konkrete Uneinigkeit besteht darin, dass die Definition eines bewaffneten Angriffs und der Anwendung von Gewalt als zentrale Prinzipien der UN-Charta bei IKT unklar sind. Ab wann ist ein Cyber-Angriff eine Gewaltanwendung? Westliche Völkerrechtlerinnen und Völkerrechtler argumentieren, dass ein Cyber-Angriff dann als bewaffneter Angriff zu werten ist, wenn er in Umfang und Effekten die Eigenschaften eines kinetischen Angriffs erreicht. Konkret bedeutet dies eine physische Zerstörung und den Verlust von Menschenleben. Allerdings gibt es auch hier Grauzonen. Wenn ein Cyber-Angriff ein Stromkraftwerk nicht physisch zerstört, sondern nur zeitweise deaktiviert, würde dann das Recht auf Selbstverteidigung greifen? Wie sieht es mit Störungen aus, die Wirtschaftsprozesse lahmlegen und Milliarden an Kosten verursachen, die etwa von ärmeren Staaten nicht ohne Weiteres gedeckt werden können? Wer entscheidet darüber, ob ein Cyber-Angriff in einem anderen Land als bewaffneter Angriff oder Gewaltanwendung zu werten ist?

Die Uneinigkeit über Konzepte zum bewaffneten Angriff und Gewaltanwendung berührt auch die Frage, ob das Recht auf Selbstverteidigung der Staaten nach der UN-Charta im Artikel 51 bei Cyber-Angriffen greife. Konkret geht es darum, ob bei einem Cyber-Angriff durch einen Staat auf einen anderen mit digitalen Mitteln zurückgeschlagen werden, beziehungsweise ob mit diplomatischen oder wirtschaftlichen Gegenmaßnahmen oder gar mit konventionellen, militärischen Mitteln reagiert werden darf. Diese Diskussion ist insbesondere seit der Entwicklung von militärischen Cyber-Doktrinen vor allem in den USA, der Nordatlantikvertrags-Organisation (NATO) und Westeuropa in vollem Gange. Seit dem Jahr 2015 sieht die amerikanische Cyber-Doktrin vor, schwerwiegende Cyber-Angriffe, die physischen Schäden verursachen und/oder Menschenleben gefährden, auch physisch vergelten zu wollen (Prinzip der Gleichwertigkeit). Zudem behalte man sich das Recht vor, auf Cyber-Angriffe gegen die USA mittels digitaler Gegenangriffe (›hack back‹) reagieren zu wollen. Die NATO hat erklärt, dass ein Cyber-Angriff die kollektive Bündnisverteidigung auslösen kann, wenn dieser die Kriterien eines bewaffneten Angriffs erreicht. Auch die Cyber-Diplomatie-Instrumente der Europäischen Union (EU) aus dem Jahr 2017 sehen als Reaktion den Einsatz von diplomatischen und wirtschaftlichen Sanktionen vor. Insofern bleibt die Frage, ob auf digitale Desinformationsoperationen ein militärischer Gegenschlag oder eine digitale Gegenoperation ein legitimes Mittel sind.

China, Kuba und Russland warnen indes, dass eine Anerkennung des Selbstverteidigungsprinzips und das Prinzip der Gleichwertigkeit die Militarisierung des Cyberspace beschleunige. Das Prinzip der Gleichwertigkeit sei eine Gefährdung der kollektiven Sicherheit. Russland ist der Auffassung, dass ein konventioneller Waffeneinsatz kein angemessenes Reaktionsmittel auf Cyber-Angriffe darstelle, zumindest nicht ohne Genehmigung des UN-Sicherheitsrats. Andererseits werden China im Bereich der Cyber-Spionage und Russland im Bereich der Desinformationskampagnen, insbesondere im US-Wahlkampf im Jahr 2016, von westlichen Akteuren als konkrete Aggressoren im Cyberspace wahrgenommen. In deren Augen treiben China und Russland eben jene Militarisierung des Cyberspace voran, vor der sie mit Worten warnen. Westliche Staaten argumentieren, dass China, Russland und andere zugestimmt haben, dass die UN-Charta in Gänze für Cyber-Aktivitäten gelte, und das beinhaltet das Recht auf Selbstverteidigung.

STAATEN MIT OFFENSIVEN CYBER-FÄHIGKEITEN



Quelle: dig.watch/processes/un-gge

Unklarheit herrscht außerdem bei der Frage, inwiefern Cyber-Angriffe, die einen bevorstehenden Cyber-Angriff verhindern sollen, ein legitimes Mittel sein können. Die USA führen diese präventiven Cyber-Angriffe im Rahmen der neuen Cyber-Doktrin aus dem Jahr 2018 durch. Mit dem Konzept der ›Vorwärtsverteidigung‹ dringen US-Hackerinnen und -Hacker wissentlich in Infrastrukturen anderer Staaten in Friedenszeiten ein, um etwaige Angreifer in ihren eigenen Netzwerken zu beobachten. Damit sollen gegnerische Cyber-Angreifer permanent mit der Verteidigung eigener Netze gebunden werden, sodass sie selbst nicht angreifen können. Diese Doktrin entstand aus der Erkenntnis, dass bisherige defensive Konzepte wie Abschreckung im digitalen Raum nicht funktionieren und man insofern mit ständigen Gegenreaktionen beginnen müsse.

Ein Problem bei Gegenreaktionen nach Cyber-Vorfällen ist, dass die Urheberschaft von Cyber-Angriffen leicht gefälscht werden kann. Der Nachweis der Urheberschaft ist aber nach dem Völkerrecht oft eine Vorbedingung für Gegenmaßnahmen. Unklarheiten herrschen hier etwa über Beweisstandards, da der Nachweis der Urheberschaft oftmals auf nachrichtendienstlichen Quellen basiert, die nicht offengelegt werden können. Bei einem öffentlichen Beschuldigen eines Urhebers ist zudem die Transparenz und Legitimität von Akteuren nicht gegeben, etwa von privaten IT-Sicherheitsunternehmen, die am Nachweis der Urheberschaft beteiligt sind. Russland sieht in dem Versuch eines öffentlichen Nachweises über einen Cyber-Angriff ein »pseudo-legales Konzept«.

Ein letzter Streitpunkt berührt die Frage der Staatenverantwortlichkeit. Dass Staaten verantwortlich sind, wenn aus ihrem Territorium IKT für völkerrechtswidrige Akte genutzt werden, ist unstrittig. Allerdings ist die Umsetzung dieser Norm enorm komplex, da Staaten in der Regel nicht jeden Computer in ihrem Territorium überwachen können. Prinzipiell kann fast jeder Rechner zum Einleiten von Cyber-Angriffen oder zum Schreiben von Schadsoftware verwendet werden. Oftmals werden Computer sogar von unbeteiligten Drittakteuren gekapert und ohne Wissen der Besitzerin oder des Besitzers für Cyber-Angriffe zweckentfremdet. In Demokratien ist es zudem normativ problematisch, wenn der Staat die Computer seiner gesamten Bevölkerung überwachen wollte. Die Norm der Sorgfaltsverantwortung beinhaltet also viele Möglichkeiten für Staaten, sie zu umgehen oder glaubhaft abzustreiten, von illegalen Aktivitäten auf dem eigenen Territorium zu wissen.

NEUE BEDROHUNGEN UND ENTWICKLUNGEN ZU DEREN BEGRENZUNG

Betrachtet man die Entwicklung der UN GGE im Kontext der Krise des Multilateralismus, also der internationalen Zusammenarbeit, und der Rückkehr nationalistischer Politik, so scheint sich der Raum für Einigungen zu verringern und sich die unterschiedlichen Standpunkte weiter voneinander zu entfernen. Dies betrifft insbesondere die Frage der legalen Konzepte wie Gewaltanwendung und bewaffneter Angriff sowie das Recht auf Selbstverteidigung. Insofern stellte sich mit dem Scheitern der fünften UN GGE die Frage, wie die gegenwärtige Blockade gelöst und die Zukunft des UN GGE-Prozesses aussehen kann.

Die UN-Generalversammlung richtete Ende des Jahres 2018 nicht nur die Fortführung des UN GGE-Prozesses unter brasilianischem Vorsitz ein, sondern etablierte eine zweite Arbeitseinheit, die Offene Arbeitsgruppe (OEWG) unter Vorsitz der Schweiz. Ihre Aufgabe ist es, den Dialog fortzuführen und Regeln, Normen und Prinzipien verantwortungsvollen, staatlichen Verhaltens im Cyberspace zu entwickeln. Die Agenda liest sich recht ähnlich zur UN GGE: In beiden UN-Gruppen geht es um die Frage, wie das Völkerrecht auf den Cyberspace anwendbar ist und wie Normen und vertrauensbildende Maßnahmen entwickelt werden können. Anders als die UN GGE, ist die OEWG offener gestaltet, sodass sich daran alle UN-Mitgliedstaaten beteiligen können. Auch Konsultationsgespräche mit der Privatwirtschaft, nichtstaatlichen Organisationen (NGOs) und der Wissenschaft sind geplant. Durch diese offene Struktur des Verhandlungsprozesses erhoffen sich einige Mitglieder, die Blockadehaltung, die die letzte UN GGE geplagt

Cyber-Kriegsführung und Überwachung von Cyber-Angriffen durch den für den Luftraum zuständigen Teil der US-Nationalgarde in Maryland im Dezember 2017. Foto: Airman Magazine/Flickr (CC BY-NC 2.0)

hat, zu überwinden. Erste Treffen haben in der zweiten Jahreshälfte 2019 mit über 100 UN-Mitgliedstaaten stattgefunden.

Grundsätzlich stellt sich die Frage, ob sich beide Gruppen eher ergänzen oder gar gegenseitig blockieren. Russland hatte schon angekündigt, die OEWG zu nutzen, um die UN GGE-Berichte mit allen 193 Mitgliedstaaten hinsichtlich ihrer Effektivität und Umsetzung überprüfen zu wollen. Es ist also denkbar, dass die OEWG die Einigkeit früherer UN GGEs untergräbt. Im besten Fall ergänzen sich aber beide Initiativen. Die USA sehen etwa die Rolle der OEWG eher darin, anderen Staaten die Arbeit der UN GGE näherzubringen, sowie bei der Umsetzung existierender Cyber-Normen behilflich zu sein. Die UN GGE soll indes die offenen, technischen Fragen des Völkerrechts angehen, sowie Prozeduren zur Umsetzung bereits ausgearbeiteter Normen entwickeln.

Neue Cyber-Normen und vertrauensbildende Maßnahmen sollen in den Regionalorganisationen wie der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE), beziehungsweise in Multi-Akteurs-Prozessen wie dem Pariser Friedensforum weiterentwickelt werden. Neben Staaten sind Unternehmen, NGOs und die Zivilgesellschaft in diese Prozesse integriert. Auch bei den Treffen der Gruppe der 7 (G7) spielt das Thema seit wenigen Jahren eine größere Rolle. Daneben werden in zahlreichen Regionalorganisationen wie der OSZE oder der Shanghaier Organisation für Zusammenarbeit (SCO) vertrauensbildende Maßnahmen entwickelt. Russland würde vertrauensbildende Maßnahmen lieber in der OEWG weiterentwickeln und die fragmentierten Regionalinitiativen hierin bündeln. Hier wird sich in Zukunft die Frage stellen, welche Organisation federführend werden wird.

Eine offene Frage ist darüber hinaus, inwiefern sich die OEWG oder die UN GGE mit benachbarten Themenfeldern befassen sollen, die nicht direkt in das Mandat der Gruppen fallen, aber dennoch Bedeutungen für die IT-Sicherheit haben. Internationale Tendenzen im Krieg gegen den Terrorismus und zur Bekämpfung von Cyber-Kriminalität – wie etwa das Aufweichen von Verschlüsselung zugunsten von Überwachung und Strafverfolgung und die Weiterentwicklung von Internet-Protokollen – berühren sowohl Aspekte von Privatsphäre, Datenschutz aber auch IT-Sicherheit.

Im UN GGE-Bericht aus dem Jahr 2015 gibt es eine breite Übereinstimmung darüber, dass der Schutz von Menschenrechten, Meinungsfreiheit, Privatsphäre und der freie Fluss von Informationen wichtig sind. Allerdings stellt sich heute die Frage, inwiefern die Verbreitung von Desinformation und falschen Nachrichten in den Aufgabenbereich der UN GGE gehören sollte. Es besteht die Gefahr, dass im Namen der Bekämpfung unliebsamer Internetinhalte das Recht auf freie Meinungsäußerung eingeschränkt und damit das Internet zensiert wird. Russland versucht dieses Thema in der OEWG zu verankern und China hat bereits ein Positionspapier zur Staatensouveränität im Cyberspace vorgelegt, was Staaten eine umfassende Kontrolle über Internet-Inhalte in ihrem Territorium geben soll. Gleichzeitig haben westliche Staaten ein Interesse an der Sicherung ihrer Wahlinfrastrukturen und der Beeinflussung des Informationsumfelds. Insofern gibt es gegenwärtig auch in westlichen Staaten ein Momentum zur Kontrolle von Internet-Inhalten, etwa bei bewusst irreführender Wahlwerbung. Die Frage ist, inwiefern demokratische Staaten der autoritären Versuchung der Kontrolle von Internet-Inhalten widerstehen und Normen wie den freien Fluss von Internet-Daten und die Meinungsfreiheit hochhalten oder sich darauf einlassen.

Eine offene Frage ist zudem, wie UN GGE und OEWG mit der Weiterentwicklung von Cyber-Normen im Kontext des Aufweichens des Konsenses früherer UN GGEs weiter verfahren werden soll. Einerseits wird argumentiert, dass es besser wäre, Kritikerinnen und Kritiker bestehender Normen einzubinden und mit ihnen gemeinsam neue Normen zu entwickeln. Einige Staaten schlagen etwa vor, neue Normen zu schaffen, die die Integrität von Daten sichern oder den Missbrauch der Kerninfrastruktur des Internets verhindern sollen. Cyber-Normen werden unter anderem durch NGOs wie die Globale Kommission für Stabilität im Cyberspace, aber auch durch staatliche Initiativen wie den Pariser Aufruf für Vertrauen und Sicherheit im Cyberspace angetrieben. Ebenso treiben Wirtschaftsunternehmen Initiativen an. Zu nennen wäre hier Microsofts Initiative einer ›Digitalen Genfer Konvention‹ sowie die Verabschiedung eines Vertrags, der die Beteiligung von Unternehmen an Cyber-Konflikten minimieren soll. Daneben starteten Siemens und andere Unternehmen mit der ›Charta des Vertrauens‹ im Jahr 2018 eine ähnliche Initiative.

Andererseits wird argumentiert, dass bestimmte Staaten diese Prozesse ohnehin sabotieren und an keiner Lösung interessiert seien. Zu erwarten sei höchstens ein kleinster gemeinsamer Nenner. Daher könnte es sinnvoller sein, Koalitionen von gleichgesinnten Staaten zu bilden, die sich auf konkrete, umfassendere Normen einigen können. Insbesondere die USA scheinen ihren Schwerpunkt von der Entwicklung neuer Normen hin zur Umsetzung der bereits bestehenden Einigkeit zu verlagern. Ziel ist hierbei, dass eine ›Koalition der Guten‹ diese Normen umsetzt und Verstöße gegen diese Normen durch Dritte öffentlich

anprangert. Die UN-Abrüstungsagenda, die durch den UN-Generalsekretär António Guterres vorangetrieben wird, konzentriert sich vorwiegend auf die Umsetzung bereits bestehender Normen des UN GGE-Berichts aus dem Jahr 2015.

ÄCHTUNG VON CYBER-WAFFEN IN EINEM DIGITALEN RÜSTUNGS-KONTROLLREGIME?

Bei den bisherigen unterschiedlichen Maßnahmen zur Begrenzung von Cyber-Konflikten handelt es sich um völkerrechtlich nicht-bindende, vorwiegend normative Initiativen. Völkerrechtlich bindende, einklagbare Verträge oder gar ein rechtlich-bindendes Rüstungskontrollregime mit Überprüfungs- und Sanktionsmöglichkeiten für völkerrechtswidriges Verhalten im Cyberspace gibt es bisher nicht. Jedoch wird immer wieder die Notwendigkeit digitaler Rüstungskontrolle heraufbeschworen. Ähnlich wie Russland bereits seit dem Jahr 1998 fordert, solle entweder ein bindender ›Cyber-Vertrag‹ beziehungsweise eine Art Rüstungskontrollregime ausgearbeitet werden, was entweder Cyber-Angriffe verbietet oder Cyber-Waffen, ähnlich etwa wie Landminen, ächten soll.

Rüstungskontrollregime versuchen in der Regel, konkrete Waffentypen wie Atomwaffen oder Landminen zu begrenzen, zu ächten oder eskalatorisches Verhalten wie Waffentests oder die grenznahe Stationierung von Truppen zu verhindern. Das Ziel ist dabei die Verhinderung von Konflikten sowie die Entschleunigung von Rüstungswettläufen. In Rüstungskontrollregimen fassen die Mitgliedstaaten angemessenes und verbotenes Verhalten rechtlich zusammen und setzen sich selbst vertragliche Regeln, über deren Einhaltung dann verschiedene internationale Institutionen wachen. Dazu muss zunächst definiert werden, was unerwünschtes Verhalten ist und wie dieses gemessen werden kann, um eine Vertragsverletzung eines Mitgliedstaats überhaupt festzustellen. Diese Überprüfung wurde in traditionellen Rüstungskontrollregimen etwa durch Vor-Ort-Inspektionen von Fertigungsanlagen, Sensorik, Satellitenüberwachung und dem Austausch von Informationen bewerkstelligt. Wenn regelverletzendes Verhalten festgestellt wurde, folgen in umfassenderen Regimen häufig Sanktionen. Die Charakteristika digitaler Technologien erschweren allerdings die traditionellen Prinzipien von Rüstungskontrolle, sodass ein Cyber-Rüstungskontrollregime aus den folgenden Gründen unwahrscheinlich ist:

Ein Problem ist, dass Rüstungskontrollregime sich in der Regel auf sehr besondere Dinge konzentrieren, etwa die Anzahl erlaubter Atomsprengköpfe oder die Ächtung spezieller Waffengattungen wie Landminen. Bisher gibt es keinen Konsens darüber, was ein Cyber-Rüstungskontrollregime überhaupt kontrollieren sollen, also ob konkrete Waffentypen (›Cyber-Waffen‹) geächtet oder begrenzt werden sollen, oder ob es um das Eindämmen unerwünschten Verhaltens, wie etwa Cyber-Spionage oder -Sabotage gehen soll. Dies scheitert schon daran, dass es bisher zwar unterschiedliche Ansätze, aber keinerlei akzeptierte Definition einer Cyber-Waffe gibt. Cyber-Angriffe beschreiben eine Reihe verschiedener Praktiken mit unterschiedlichen Charakteristika. Das reicht vom Missbrauch legitimer Instrumente wie das massenhafte Versenden von Internetdatenpaketen mit lediglich störenden Effekten über Praktiken sozialer Manipulation zum Erlangen von Zugangsdaten (›phishing‹) bis hin zum Einsatz von Schadsoftware. Die meiste Schadsoftware wird zu kriminellen Zwecken erstellt und hat finanzielle Ziele, sodass diese nicht die Definition einer Waffe erfüllt. Allerdings kann Schadsoftware unter bestimmten Umständen auch physische Effekte verursachen, wenn zum Beispiel ein Waffensystem wie eine bewaffnete Drohne gehackt wird. Die Schwierigkeit besteht darin, eine Definition zu finden, die breit genug ist, um wirkliche Schadsoftware zu erfassen, aber gleichzeitig trennscharf genug ist, dass etwa legitime Software, die auch zur Verteidigung genutzt wird, nicht darunter fällt. Da Schadsoftware modular und wandelbar ist, ist eine solche Definition nur schwer zu finden.

Weitere Hindernisse sind, dass Softwarecodes leicht über das Internet verbreitet werden, dass der Code immer wieder kopiert und somit nicht zerstört und faktisch auf jedem beliebigen Privatcomputer weltweit geschrieben werden kann. Digitale Waffen werden nicht in großen Fabriken hergestellt, die man aus dem All beobachten kann, sondern zuweilen auf Privatcomputern mittels kommerzieller Software. Zudem gibt es einen milliardenschweren schwarzen und grauen Markt für Schadsoftware, auf dem auch Regierungen Angriffssoftware für Cyber-Konflikte, zur Spionage von Gegnern oder zur Überwachung der eigenen Bevölkerung einkaufen. Diese Eigenschaften von Software führen dazu, dass man diese nicht ›zählen‹ und vergleichen kann, wie etwa bei traditionellen Rüstungskontrollverträgen. Cyber-Macht kann sehr schlecht quantifiziert werden, zumal die Mittel häufig in der Hand von Nachrichtendiensten liegen und daher unter hoher Geheimhaltung stehen. Viele Staaten erklären zudem nicht öffentlich, wie groß ihre Ausgaben für offensive Cyber-Fähigkeiten gegenüber defensiven Ausgaben sind, sofern man diese sinnvoll trennen kann. Neben

In Deutschland ist das Bundesamt für Sicherheit in der Informationstechnik (BSI) für das im Jahr 2011 gegründete Cyber-Abwehrzentrum (Cyber-AZ) zuständig. Letzteres soll Schutz- und Abwehrmaßnahmen im Cyberspace koordinieren. Dies betrifft Cyber-Spionage, Cyber-Ausspähung, Cyber-Terrorismus und Cyber-Kriminalität. Foto: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Digitale Souveränität verspricht Sicherheit für Staaten, sie kann aber auch eine Einschränkung von Grundrechten bedeuten. Foto: Yuri Samoilov/Flickr (CC BY 2.0)

diesen konzeptionellen Schwierigkeiten ist die zentrale Herausforderung allerdings die Überprüfung, die durch das bereits erwähnte Problem, den Urheber ausfindig zu machen, erschwert wird. Ein Cyber-Vertrag oder -Abkommen hätte somit wenig legale Bindekraft und könnte leicht von bösartigen Akteuren umgangen werden, ohne dass dies mittels handfester Beweise überprüft werden könnte.

Schwerer wiegt indes der Umstand, dass es zwischen demokratischen und autoritären Regimen grundsätzlich unterschiedliche Ordnungsvorstellungen darüber gibt, was durch ein solches Cyber-Regime reguliert werden soll. Für westliche Staaten steht die Ächtung von Cyber-Konflikten und Industriespionage im Vordergrund. Cyber-Sicherheit meint hier den Schutz von IT-Systemen und Gesellschaften vor Sabotage und Störungen. Autoritäre Staaten haben indes ein grundsätzliches anderes Verständnis des Problems: Ihnen geht es um Informationssicherheit, also den Schutz der Öffentlichkeit und des eigenen Machtapparats vor sogenannten Informationsangriffen, also der Verwendung von IKT zu Propagandazwecken und dem Handeln im Verborgenen, um Staaten zu destabilisieren. Hierbei steht weniger die Angst vor technischer Sabotage, als vielmehr vor sozialer Beeinflussung durch soziale Medien im Vordergrund. Die Farbrevolutionen im postsowjetischen Raum und der arabische Frühling, bei denen soziale Netzwerke und Informationstechnologien durch die Bevölkerung gegen die Regierung genutzt wurden, sind hier Gegenstand der Sorge. Westliche Staaten drängen aufgrund ihres Weltbildes hin zu Cyber-Rüstungskontrolle, da sie Cyber-Fähigkeiten vorwiegend als militärische Waffen interpretieren, die hochtechnisierte Gesellschaften lahmlegen können. Autoritäre Regime drängen indes auf Informationskontrolle, also die Überwachung und Kontrolle von Informationen in ihrem nationalen Teil des Internets. Diese Ordnungsvorstellung ist grundsätzlich inkompatibel mit demokratischen Normvorstellungen.

AUSBLICK

Die Aushandlung internationaler, bindender Verträge ist oftmals ein sehr langwieriger und schwieriger Prozess, in dem es immer wieder Rückschritte gibt. Ein bindender Cyber-Vertrag ist somit kurz- bis mittelfristig unwahrscheinlich. Die Erfahrung aus anderen Bereichen lehrt, dass internationale Verhandlungen häufig durch Krisen- und Schocks beschleunigt werden. Zynikerinnen und Zyniker argumentieren daher, dass Cyber-Fähigkeiten erst großflächige Zerstörung anrichten müssen, bevor Staaten sich zu deren Begrenzung überzeugen lassen. Optimistinnen und Optimisten verweisen auf breite zivilgesellschaftliche Initiativen, unterstützt durch Maßnahmen der IT-Industrie, wenn sie Staaten zu mehr Regulierung und Schaffung weiterer Normen drängen. Das Problembewusstsein existiert also und da ein Großteil aller IKT in Hand privater Unternehmen ist, haben diese hier größere Einflussmöglichkeiten. Dass sich zum Beispiel immer mehr Unternehmen verpflichten, sich nicht für staatliche Cyber-Angriffe missbrauchen zu lassen, ist hierbei ein wichtiges normatives Signal. Letztlich kann die Regulierung des globalen Cyberspace und die Eindämmung von Cyber-Konflikten nur global und durch das Mitwirken aller Beteiligten, ob Staaten, Unternehmen oder der Zivilgesellschaft, gelingen.

WEITERFÜHRENDE INFORMATIONEN

- Geneva Internet Platform, Digital Watch Observatory, UN GGE and OEWG: dig.watch/processes/un-gge
- Internet Governance Radar: internet-governance-radar.de
- Alexander Klimburg, The Darkening Web: The War for Cyberspace, New York 2017.
- Holger Niemann, Digitale Bedrohungen – eine Aufgabe für den UN-Sicherheitsrat?, dgvn.de/meldung/digitale-bedrohungen-eine-aufgabe-fuer-den-un-sicherheitsrat/
- Julia Pohle/Julius Lang, Digitale Souveränität als Frage der Selbstbestimmung im digitalen Raum, dgvn.de/meldung/digitale-souveraenitaet-als-frage-der-selbstbestimmung-im-digitalen-raum/
- Resolution der UN-Generalversammlung, Das Recht auf Privatheit im digitalen Zeitalter, UN-Dok. A/RES/68/167 v. 18.12.2013.

Weitere Informationen zu den Vereinten Nationen:
www.dgvn.de

Themenportale der DGVN
frieden-sichern.dgvn.de
menschenrechte-durchsetzen.dgvn.de
nachhaltig-entwickeln.dgvn.de

Deutsche Gesellschaft für die Vereinten Nationen e. V.
Zimmerstraße 26/27 | D-10969 Berlin
info@dgvn.de | www.dgvn.de
dgvn.e.V dgvn_de

ISSN: 1614-5453 | Stand: Januar 2020

Text: Dr. Matthias Schulze
Redaktion: Dr. Patrick Rosenow, Jana Krieg
Gestaltung: Cornelia Agel, sevenminds.de

Klimaneutral gedruckt auf 100%-Recycling-Papier
Gefördert durch das Auswärtige Amt

Klimaneutral Druckprodukt
ClimatePartner.com/11180-2001-1001