SSOAR

Open Access Repository
www.ssoar.info

Internationale Sicherheit und Völkerrecht im Cyberspace: für klarere Regeln und mehr Verantwortung

Schaller, Christian

Veröffentlichungsversion / Published Version
Forschungsbericht / research report

Zur Verfügung gestellt in Kooperation mit / provided in cooperation with:
Stiftung Wissenschaft und Politik (SWP)

Empfohlene Zitierung / Suggested Citation:
Schaller, C. (2014). *Internationale Sicherheit und Völkerrecht im Cyberspace: für klarere Regeln und mehr Verantwortung.* (SWP-Studie, 18/2014). Berlin: Stiftung Wissenschaft und Politik -SWP- Deutsches Institut für Internationale Politik und Sicherheit. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-407923

Nutzungsbedingungen:
Dieser Text wird unter einer Deposit-Lizenz (Keine Weiterverbreitung - keine Bearbeitung) zur Verfügung gestellt. Gewährt wird ein nicht exklusives, nicht übertragbares, persönliches und beschränktes Recht auf Nutzung dieses Dokuments. Dieses Dokument ist ausschließlich für den persönlichen, nicht-kommerziellen Gebrauch bestimmt. Auf sämtlichen Kopien dieses Dokuments müssen alle Urheberrechtshinweise und sonstigen Hinweise auf gesetzlichen Schutz beibehalten werden. Sie dürfen dieses Dokument nicht in irgendeiner Weise abändern, noch dürfen Sie dieses Dokument für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, aufführen, vertreiben oder anderweitig nutzen.
Mit der Verwendung dieses Dokuments erkennen Sie die Nutzungsbedingungen an.

Terms of use:
This document is made available under Deposit Licence (No Redistribution - no modifications). We grant a non-exclusive, non-transferable, individual and limited right to using this document. This document is solely intended for your personal, non-commercial use. All of the copies of this documents must retain all copyright information and other information regarding legal protection. You are not allowed to alter this document in any way, to copy it for public or commercial purposes, to exhibit the document in public, to perform, distribute or otherwise use the document in public.
By using this particular document, you accept the above-stated conditions of use.

gesis Leibniz-Institut für Sozialwissenschaften

Mitglied der Leibniz-Gemeinschaft

SWP-Studie
Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale
Politik und Sicherheit

Christian Schaller

Internationale Sicherheit und Völkerrecht im Cyberspace

Für klarere Regeln und mehr Verantwortung

S 18
Oktober 2014
Berlin

Alle Rechte vorbehalten.
Abdruck oder vergleichbare Verwendung von Arbeiten der Stiftung Wissenschaft und Politik ist auch in Auszügen nur mit vorheriger schriftlicher Genehmigung gestattet.

SWP-Studien unterliegen einem Begutachtungsverfahren durch Fachkolleginnen und -kollegen und durch die Institutsleitung *(peer review)*. Sie geben ausschließlich die persönliche Auffassung der Autoren und Autorinnen wieder.

© Stiftung Wissenschaft und Politik, Berlin, 2014

SWP
Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

Ludwigkirchplatz 3–4
10719 Berlin
Telefon +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN 1611-6372

Inhalt

5 Problemstellung und Empfehlungen

7 Der Cyberspace als völkerrechtlich erfassbarer Raum

9 Ein Beispiel für internationale Kooperation: Die Bekämpfung von Cyberkriminalität

11 Im Völkerrecht totgeschwiegen: Cyberspionage

13 Eine neue Dimension: Das systematische Ausspähen privater Daten

15 Politische Einflussnahme mit Hilfe von Cybertechnologie

16 Cyberattacken zwischen Provokation und bewaffnetem Angriff

18 Der Ernstfall: Cyberattacken gegen kritische Infrastrukturen

20 Militärische Selbstverteidigung gegen Cyberattacken

21 Das Grundproblem: Nachweis und Zurechnung der Urheberschaft von Cyberattacken

23 Was bleibt? – Völkerrechtliche Due-Diligence-Pflichten im Umgang mit Cybertechnologie

25 Verantwortlichkeit und Gegenmaßnahmen bei Due-Diligence-Pflichtverletzungen

26 Völkerrechtspolitischer Ausblick: Spielräume für eine gezielte Normsetzung

31 Abkürzungsverzeichnis

Dr. iur. Christian Schaller ist stellvertretender Leiter der Forschungsgruppe Globale Fragen

Internationale Sicherheit und Völkerrecht im Cyberspace
Für klarere Regeln und mehr Verantwortung

Der Cyberspace ist ein virtueller Raum, in dem mit Hilfe digitaler Informations- und Kommunikationstechnologien über vernetzte Systeme Daten generiert, gespeichert, modifiziert und ausgetauscht werden. Teil der Cyberinfrastruktur ist das Internet. Die fortschreitende globale Vernetzung und wachsende Abhängigkeit von komplexen Technologien führt zu einer neuen Verwundbarkeit, von der alle Bereiche des staatlichen, wirtschaftlichen und gesellschaftlichen Lebens betroffen sind. Die Bandbreite möglicher Bedrohungen reicht von einfacher Cyberkriminalität und terroristischen Aktivitäten im Internet über das systematische Ausspähen privater Daten und Cyberspionage bis hin zur Sabotage kritischer Infrastrukturen mit unter Umständen katastrophalen Folgen für die Sicherheit eines Staates. Verstärkt wird das Bedrohungspotential dadurch, dass immer mehr Staaten Fähigkeiten in der Cyberkriegführung entwickeln und sich auf diese Weise neue Wege eröffnen, um geostrategische Interessen durchzusetzen.

Die Gewährleistung von Sicherheit im Cyberspace erfordert in erster Linie, dass öffentliche und private IT-Systeme und vor allem kritische Informationsinfrastrukturen besser vor Angriffen geschützt werden. Darüber hinaus gilt es zu verhindern, dass feindselige Akte im Cyberspace zwischenstaatliche Konflikte eskalieren lassen. Denn zum einen können Staaten und nichtstaatliche Akteure durch Cyberattacken mit geringem Aufwand großen Schaden anrichten, ohne dass ihnen eine Urheberschaft zweifelsfrei nachzuweisen ist. Zum anderen besteht die Gefahr, dass Staaten auf Cyberangriffe militärisch überreagieren, ohne genau zu wissen, wer für den Angriff verantwortlich ist. Umso wichtiger sind vertrauensbildende Maßnahmen und die Schaffung von Rechtssicherheit bei der Abwehr von Cyberbedrohungen.

In ihrer Cyberaußenpolitik setzt sich die Bundesrepublik Deutschland unter anderem für die Stärkung internationaler Normen ein, die ein verantwortungsvolles Miteinander der Staaten im Cyberspace gewährleisten sollen. Ziel ist es, einen Kanon von Verhaltensregeln zu entwickeln, der von möglichst vielen Regierungen mitgetragen wird. In dieser Studie wird der Frage nachgegangen, welche Vorgaben sich hierfür

aus dem Völkerrecht ableiten lassen. Allgemein anerkannt ist, dass die Wahrung von Frieden, internationaler Sicherheit und Stabilität im Cyberkontext grundsätzlich jenen völkerrechtlichen Normen und Prinzipien unterliegt, die bereits 1945 in der Charta der Vereinten Nationen niedergelegt wurden. Eine gewisse Unsicherheit herrscht jedoch darüber, wie einzelne Normen und Prinzipien im Lichte der spezifischen Herausforderungen des Cyberspace auszulegen sind.

Die Bekämpfung transnationaler Cyberkriminalität wirft aus völkerrechtlicher Sicht keine grundlegenden Probleme auf. Hier geht es vor allem darum, international einheitliche Straftatbestände zu definieren und eine möglichst lückenlose Verfolgung der Taten über Staatsgrenzen hinweg sicherzustellen. Schwierigere Rechtsfragen stellen sich im Zusammenhang mit nachrichtendienstlichen Aktivitäten im Cyberspace. Die systematische Überwachung der Korrespondenz von Privatpersonen stellt prinzipiell einen Eingriff in das Recht auf Privatsphäre dar. Unklar ist hingegen, in welchem Umfang die internationalen Menschenrechtsnormen Geheimdienste daran hindern, Angehörige anderer Staaten im Ausland auszuspähen. Gestritten wird auch darüber, ob das heimliche Eindringen in geschützte IT-Systeme und Netzwerke zu Spionagezwecken gegen das zwischenstaatliche Interventionsverbot verstößt. Traditionell üben die Staaten nämlich größte Zurückhaltung hinsichtlich der völkerrechtlichen Bewertung von Spionageaktivitäten. Sofern Cyberattacken jedoch darauf ausgelegt sind, Einrichtungen der Infrastruktur eines Staates lahmzulegen oder weitergehende Schäden zu verursachen, kann neben dem Interventionsverbot auch das Gewaltverbot nach Artikel 2 (4) der UN-Charta verletzt sein. Die USA nehmen für sich das Recht in Anspruch, notfalls mit konventioneller militärischer Gewalt auf Cyberattacken zu reagieren. Diese Ankündigung hat eine intensive Debatte darüber ausgelöst, wann Staaten im Falle von Cyberangriffen das Recht auf Selbstverteidigung nach Artikel 51 der UN-Charta zusteht. Das Augenmerk ist vor allem auf Szenarien gerichtet, in denen Steuerungssysteme kritischer Infrastrukturen angegriffen werden. In der Praxis dürfte es allerdings selbst für die USA äußerst schwierig sein, die Urheber einer professionell ausgeführten Cyberattacke rasch und verlässlich zu lokalisieren und zu identifizieren. Ein solcher Nachweis ist aber Grundvoraussetzung für eine völkerrechtliche Zurechnung des Angriffs. Sofern sich die Verantwortlichkeit im Einzelfall nicht eindeutig klären lässt – und die Nachweispflichten für die Inanspruchnahme des Selbstverteidigungsrechts in der Staatenpraxis nicht auf Dauer aufgeweicht werden –, verbieten sich gewaltsame Gegenschläge, durch die andere Staaten in ihrer geschützten Rechtssphäre betroffen sind. Dieses Verbot gilt auch für Reaktionen in Form von Cyberoperationen, soweit ihre Wirkung mit derjenigen konventioneller militärischer Maßnahmen vergleichbar ist. Die bloße Vermutung, dass ein bestimmter Staat hinter einer Cyberattacke steht, reicht jedenfalls nicht aus, um derartige Eingriffe völkerrechtlich zu legitimieren.

Kaum ein Staat dürfte in der Lage sein, die Cyberinfrastruktur in seinem Hoheitsbereich so abzusichern, dass nicht Teile dieser Einrichtungen manipuliert und für kriminelle Handlungen oder feindselige Akte gegen andere Staaten genutzt werden können. Möglicherweise ist ein Staat, in dessen Hoheitsbereich eine Attacke ihren Ursprung hat, sogar völkerrechtlich verantwortlich für Versäumnisse bei der Absicherung und Überwachung seiner Infrastruktur, für ein pflichtwidrig unterlassenes Einschreiten oder für mangelnde Kooperation bei der Abwehr und Aufklärung des Angriffs. Aus dem Völkerrecht lassen sich nämlich bestimmte Due-Diligence-Verpflichtungen ableiten, die daran anknüpfen, dass ein Staat Einrichtungen der Cyberinfrastruktur unterhält und Cybertechnologien nutzt. Obgleich darüber im Kern kein Dissens zwischen den Staaten besteht, ist es bislang nicht gelungen, Inhalt und Umfang der Verpflichtungen in einem offiziellen internationalen Rahmen zu präzisieren. An diesem Punkt müssten multilaterale Initiativen vorrangig ansetzen, um mehr Klarheit zu schaffen. Zur Konkretisierung der Pflichten bedarf es keines völkerrechtlich verbindlichen Abkommens. Ein formaler Rechtsetzungsprozess wäre äußerst langwierig und müsste hohe politische Hürden überwinden. Mehr Erfolg verspricht der von der Bundesregierung eingeschlagene Weg, gemeinsam mit anderen Staaten einen Kodex für verantwortungsvolles Verhalten im Cyberspace zu entwickeln. Langfristig können solche Initiativen dazu beitragen, dass sich neue völkergewohnheitsrechtliche Regeln herauskristallisieren.

Der Cyberspace als völkerrechtlich erfassbarer Raum

Die Bundesregierung betrachtet den Cyberspace als öffentlichen Raum und öffentliches Gut.[1] Dieses Verständnis entspricht der allgemeinen Auffassung, dass es sich beim Cyberspace um einen souveränitätsfreien Raum handelt, der allen Staaten gleichermaßen zur Nutzung offensteht. Kein Staat hat demnach das Recht, sich Teile dieses Raumes anzueignen oder andere Staaten von der Nutzung auszuschließen.[2] Obwohl der nichtgegenständliche und allgegenwärtige Charakter des Cyberspace das traditionell geographisch-raumbezogene Völkerrechtsdenken vor besondere Herausforderungen stellt,[3] besteht kein Zweifel daran, dass das geltende Völkerrecht auf Sachverhalte im Cyberspace Anwendung findet.[4]

Als virtueller und souveränitätsfreier Raum wird der Cyberspace grundsätzlich von der physisch lokalisierbaren Cyberinfrastruktur (Computer, Kabelnetze, Sendeanlagen und andere Einrichtungen) unterschieden, die staatlicher Souveränität unterliegt.[5] Allerdings drängt sich die Frage auf, bis zu welchem Punkt die im Cyberspace vorhandenen Daten noch dem öffentlichen virtuellen Raum zuzuordnen sind und wann sie zum geschützten Hoheitsbereich der Staaten zählen.

Bei der Ausübung ihrer Jurisdiktion[6] über Einrichtungen der Cyberinfrastruktur und deren Nutzer haben die Staaten bestimmte völkerrechtliche Rechte und Pflichten. Staatliche Souveränität, territoriale Integrität und politische Unabhängigkeit sowie das Interventionsverbot, das Gewaltverbot und andere in der Charta der Vereinten Nationen verankerte Prinzipien sind nämlich auch im Cyberkontext von großer Bedeutung. Im Verhältnis zwischen Staaten und Bürgern kommen zudem die internationalen Menschenrechtsnormen zum Tragen. Sie dienen unter anderem dem Schutz der Informationsfreiheit und der Privatsphäre.

Soweit Cyberoperationen als Mittel der Kriegführung genutzt werden, bestimmt sich der Rahmen des Zulässigen nach dem für bewaffnete Konflikte geltenden humanitären Völkerrecht. Dieses schreibt vor, welche Objekte vor Angriffen geschützt sind und welche Vorsichtsmaßnahmen getroffen werden müssen, um die Zivilbevölkerung zu schonen. Obgleich die Regeln des humanitären Völkerrechts prinzipiell flexibel genug sind, um den Besonderheiten der Cyberkriegführung Rechnung zu tragen, besteht erheblicher Klärungsbedarf, wie einzelne Vorschriften in solchen Situationen auszulegen sind.[7] Brisant ist etwa die Frage, ob und unter welchen Voraussetzungen Einrichtungen der zivilen Kommunikationsinfrastruktur zu einem legitimen Angriffsziel werden können.

Im alltäglichen Leben weitaus greifbarer ist die Bedrohung durch unterschiedliche Formen der Cyberkriminalität. Mit der Budapester Konvention von 2001 existiert bereits ein spezielles völkerrechtliches Regelwerk für die Bekämpfung von Straftaten im Cyberspace. Die Konvention sieht vor, dass bestimmte Taten in den Vertragsstaaten einheitlich unter Strafe zu stellen und zu verfolgen sind.

1 Vgl. die Stellungnahme Deutschlands, veröffentlicht im Bericht des UN-Generalsekretärs, *Developments in the Field of Information and Telecommunications in the Context of International Security*, Report of the Secretary-General, UN-Dok. A/68/156/Add.1, 9.9.2013, S. 7.

2 Wolff Heintschel von Heinegg, »Legal Implications of Territorial Sovereignty in Cyberspace«, in: Christian Czosseck/Rain Ottis/Katharina Ziolkowski (Hg.), *2012 4th International Conference on Cyber Conflict*, Tallinn: NATO CCDCOE, 2012, S. 7–19 (9).

3 Andreas von Arnauld, *Völkerrecht*, Heidelberg u.a. 2012, S. 335.

4 Vgl. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN-Dok. A/68/98*, 24.6.2013, Absatz 19ff.

5 Die Souveränität eines Staates erstreckt sich auch auf den staatlichen Luftraum und das Küstenmeer einschließlich des darunter liegenden Meeresbodens. Unter dem Schutz staatlicher Souveränität stehen zudem Schiffe, Luftfahrzeuge und Weltraumobjekte, die souveräne Immunität genießen. Träger souveräner Immunität sind Plattformen (unabhängig von ihrem Aufenthaltsort), die ausschließlich staatlich und nicht zu Handelszwecken genutzt werden. Darunter fallen insbesondere Kriegsschiffe und militärische Luftfahrzeuge sowie nicht kommerziell genutzte Satelliten.

6 Jurisdiktion bedeutet, dass ein Staat in Bezug auf bestimmte Sachverhalte Gesetze erlassen und vollziehen darf und dass seine Gerichte über Rechtsfragen entscheiden können. Jurisdiktion bezieht sich auf alle Bereiche des privaten Rechtsverkehrs, des Strafrechts und des Verwaltungsrechts.

7 Zu Rolle des humanitären Völkerrechts im Falle von Cyberkonflikten siehe unten, S. 31.

In welchem Umfang Staaten die Aktivitäten im Cyberspace regulieren und sanktionieren dürfen, hängt von der Reichweite ihrer Jurisdiktion ab. Die Jurisdiktion eines Staates erstreckt sich zunächst auf alle natürlichen und juristischen Personen sowie auf Objekte innerhalb seines Territoriums (Territorialitätsprinzip).[8] So kann jeder Staat in seinem Hoheitsbereich beispielsweise Zugangs- und Nutzungsbeschränkungen für Einrichtungen der Cyberinfrastruktur erlassen, Sicherheitsstandards für Unternehmen vorschreiben oder bestimmte Handlungen unter Strafe stellen. Aus dem Territorialitätsprinzip folgt unter anderem, dass ein Staat seine Strafgerichtsbarkeit auch dann ausüben kann, wenn die Folgen einer strafbaren Handlung, die auf seinem Hoheitsgebiet begangen wird, einen anderen Staat betreffen (subjektive Territorialität) oder wenn eine Tat, die im Ausland ihren Ursprung hat, substantielle Auswirkungen auf das Inland hat (objektive Territorialität). Ähnlich weitreichend ist das Schutzprinzip, das es den Staaten gestattet, Auslandstaten zu verfolgen, die sich gegen ihre nationale Sicherheit richten, etwa bei Cyberangriffen auf Verteidigungseinrichtungen.[9] Ein weiterer wichtiger Anknüpfungspunkt ist die Staatsangehörigkeit. In der Praxis kann die gleichzeitige Anwendung dieser Prinzipien durch verschiedene Staaten zu gravierenden Jurisdiktionskonflikten führen. Gelöst werden müssen diese auf zwischenstaatlicher Ebene nach Maßgabe der bestehenden Kollisionsregeln.[10] Grundsätzlich gilt jedoch, dass ein Staat seine Gesetze nicht eigenmächtig im Hoheitsbereich anderer Staaten vollziehen darf, selbst wenn der sachliche Anwendungsbereich eines Gesetzes an Vorgänge im Ausland anknüpft. Aus diesem Grund spielen spezielle Kooperationsabkommen bei der Abwehr von Cyberbedrohungen eine besonders wichtige Rolle.

8 Vorrichtungen der Cyberinfrastruktur an Bord von Schiffen, Luftfahrzeugen und Weltraumobjekten unterliegen grundsätzlich der Jurisdiktion des Flaggenstaates bzw. desjenigen Staates, in dem das Fahrzeug oder Objekt registriert ist. Soweit eine solche Plattform keine souveräne Immunität genießt, kann sie unter bestimmten Voraussetzungen auch dem Zugriff anderer Staaten unterliegen. Dies betrifft insbesondere Fälle, in denen sich ein Schiff oder Luftfahrzeug im territorialen Hoheitsbereich eines anderen Staates befindet.

9 Bernard H. Oxman, »Jurisdiction of States«, in: Rüdiger Wolfrum (Hg.), *Max Planck Encyclopedia of Public International Law*, Online Edition, Oxford u.a. 2014, Rn. 22ff, <http://opil.ouplaw.com/home/EPIL>.

10 Benedikt Pirker, »Territorial Sovereignty and Integrity and the Challenges of Cyberspace«, in: Katharina Ziolkowski (Hg.), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, Tallinn: NATO CCDCOE, 2013, S. 189–216 (196ff).

Ein Beispiel für internationale Kooperation: Die Bekämpfung von Cyberkriminalität

Im Bereich der Cyberkriminalität ist grundsätzlich zwischen zwei Kategorien von Delikten zu unterscheiden: Zur ersten Kategorie zählen Straftaten, die einen unerlaubten Eingriff in öffentliche oder private IT-Systeme, Computernetzwerke, Datenbanken oder Webseiten darstellen und die Integrität der betreffenden Systeme sowie die Vertraulichkeit von Daten beeinträchtigen. Solche Angriffe können etwa darin bestehen, dass sich eine Person mit Hilfe spezieller Programme unbefugt Zugang zu einem System verschafft, Datenübermittlungen abfängt und Manipulationen vornimmt, um andere zu schädigen oder sich selbst Vorteile zu verschaffen. Typische Beispiele sind das Lahmlegen von Servern (Denial-of-Service-Attacken), Online-Erpressungen in Verbindung mit Schadsoftware, der Diebstahl digitaler Identitäten (zum Beispiel durch Phishing) sowie Manipulationen zu Betrugszwecken im Zusammenhang mit Online-Banking und Internethandel.[11] Die zweite Kategorie umfasst Delikte, bei denen das Internet lediglich als Plattform genutzt wird, um bestimmte verbotene Inhalte zu verbreiten (content-related cybercrime), etwa Kinderpornographie oder volksverhetzende Inhalte. Darunter fallen aber auch Aktivitäten von Terroristen, die auf diesem Wege Anhänger rekrutieren und Anleitungen zum Bau von Bomben veröffentlichen.[12]

Einen Überblick über die technischen Entwicklungen im Bereich der Cyberkriminalität gibt die Europäische Agentur für Netz- und Informationssicherheit (European Union Agency for Network and Information Security, ENISA) in ihren jährlichen Analysen. Nach Einschätzung der ENISA besteht die größte Gefahr derzeit in sogenannten Drive-by Downloads (dem unerwünschten Herunterladen von Schadsoftware durch das Anschauen präparierter Webseiten). Weitere typische Phänomene sind das Einschleusen von Würmern, Trojanern und anderen Codes sowie die Nutzung von Botnetzen (Netzwerke manipulierter Computer, die unter fremder Kontrolle im Verbund operieren) für Denial-of-Service-Attacken, die auf eine Überlastung von Servern abzielen.[13] Bereits anhand dieser Beispiele wird klar, dass der Übergang von »einfacher« Cyberkriminalität zu schwerwiegenderen Cyberattacken fließend ist, denn solche Cybertools lassen sich gegen unterschiedlichste Ziele einsetzen. Im Extremfall können sie sogar als Mittel der Kriegführung dienen. Soweit in späteren Kapiteln von Cyberattacken die Rede ist, geht es meist um Angriffe, deren Bedrohungspotential weitaus höher ist als die Gefahr, die von einfacher Cyberkriminalität ausgeht.

Die Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung ist ebenso wie die Verfolgung von Straftaten eine klassische Domäne nationalen Rechts. Geht es um die Bekämpfung transnationaler Kriminalität und terroristischer Akte, spielt auch das Völkerrecht eine wichtige Rolle. Ein bewährter Ansatz besteht darin, dass sich Staaten in regional oder international verbindlichen Verträgen darauf verständigen, bestimmte Straftatbestände in nationales Recht zu übernehmen und die Voraussetzungen zu schaffen, um solche Taten zu verfolgen. Zu diesem Zweck werden regelmäßig spezielle Informations- und Kooperationspflichten vereinbart. Beispiele sind die UN-Konvention gegen transnationale organisierte Kriminalität, das Abkommen zur Bekämpfung der Terrorismusfinanzierung und weitere Verträge, die eine einheitliche Kriminalisierung spezieller terroristischer Handlungen vorsehen. Im Rahmen des Europarats wurde 2001

11 Nach einer Auflistung des Bundeskriminalamts umfasst Cyberkriminalität im engeren Sinne folgende im deutschen Strafgesetzbuch verankerte Tatbestände: Computerbetrug, Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten, Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung, Datenveränderung und Computersabotage sowie das Ausspähen und Abfangen von Daten einschließlich Vorbereitungshandlungen. Das Bundeskriminalamt umschreibt diese Delikte als Straftaten, die sich gegen das Internet, weitere Datennetze, informationstechnische Systeme oder deren Daten richten bzw. mittels solcher Informationstechnik begangen werden. Bundeskriminalamt, *Cybercrime Bundeslagebild 2012*, <www.bka.de/nn_205994/DE/ThemenABisZ/Deliktsbereiche/InternetKriminalitaet/Lagebilder/lagebilder__node.html?nnn=true>.

12 Vgl. UN Office on Drugs and Crime, *Comprehensive Study on Cybercrime*, Draft, New York, Februar 2013, S. 16ff, <www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf>.

13 European Union Agency for Network and Information Security, *ENISA Threat Landscape 2013. Overview of Current and Emerging Cyber-threats*, Heraklion, 11.12.2013, <www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/etl2013>.

in Budapest die bereits erwähnte Konvention gegen Cyberkriminalität verabschiedet, zu deren Vertragsparteien auch Deutschland gehört.[14] In dieser Konvention sind bestimmte Straftaten gegen die Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Computerdaten und Computersystemen definiert.[15] Erfasst werden unter anderem das Eindringen in fremde Computersysteme, das unbefugte Abfangen von Datenübermittlungen, die Manipulation von Computerdaten, das Sabotieren von Computersystemen sowie der Missbrauch (Herstellung, Verbreitung und Besitz) von Computerprogrammen und Zugangscodes, um solche Straftaten zu begehen. Zudem enthält das Budapester Abkommen Vorschriften zur Bekämpfung von Computerbetrug und computerbezogenen Fälschungen. Da es bei den genannten Straftatbeständen nicht auf die Motivation der Täter ankommt, lassen sich sowohl wirtschaftlich als auch politisch oder ideologisch motivierte Taten unter diese Bestimmungen fassen, etwa Aktionen sogenannter Hacktivisten oder Taten mit terroristischem Hintergrund. Außerdem enthält die Konvention Vorgaben zur Kriminalisierung und Verfolgung einer Reihe von Taten mit Bezug zu Kinderpornographie sowie bestimmter Urheberrechtsverletzungen. Ein Zusatzprotokoll von 2003 dehnt den Anwendungsbereich der Konvention zudem auf rassistische und fremdenfeindliche Handlungen im Cyberspace aus.

Neben den genannten Straftatbeständen finden sich in der Budapester Konvention verfahrensrechtliche Bestimmungen zur Sicherung, Herausgabe, Durchsuchung, Beschlagnahme und Erhebung strafrechtlich ermittlungsrelevanter Computerdaten sowie zur Begründung nationaler Gerichtsbarkeit und zur internationalen Zusammenarbeit (insbesondere zur Auslieferung, Rechtshilfe und Einrichtung nationaler Kontaktstellen). Obgleich das Budapester Abkommen prinzipiell auch Staaten zum Beitritt offensteht, die nicht Mitglied des Europarats sind, haben bisher erst sechs nichteuropäische Staaten von dieser Möglichkeit Gebrauch gemacht.[16]

Solche völkerrechtlichen Verträge sind ein wichtiges Instrument, um ein möglichst einheitliches internationales Vorgehen gegen transnational operierende kriminelle Akteure zu gewährleisten. Angesichts der Tatsache, dass terroristische Organisationen zunehmend auch im virtuellen Raum aktiv sind, könnte das Budapester Abkommen als Vorbild für künftige Regelungen dienen, um solche Aktivitäten gezielter zu bekämpfen.

14 Convention on Cybercrime (23.11.2001, in Kraft getreten am 1.7.2004); Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems (28.1.2003, in Kraft getreten am 1.3.2006).

15 Besondere Sensibilität erfordert dabei allerdings der Umgang mit technischen Verfahren, die zur Sicherung von Computersystemen erforderlich sind, wie etwa das Suchen nach Sicherheitslücken durch »freundliches Hacken«. Für solche Aktivitäten, die zum Teil im Grenzbereich strafrechtlicher Verbote stattfinden, muss unbedingt die nötige Rechtssicherheit geschaffen werden.

16 Aktuell haben 42 Staaten die Konvention ratifiziert, darunter auch sechs nichteuropäische Staaten: Australien, Dominikanische Republik, Japan, Mauritius, Panama und USA. Zum aktuellen Stand siehe Council of Europe, *Convention on Cybercrime*, <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG>.

Im Völkerrecht totgeschwiegen: Cyberspionage

Staatliche Spionage kann darauf gerichtet sein, an wirtschaftlich relevante Informationen zu gelangen, aber auch vertrauliche Regierungsinformationen betreffen oder einen militärischen Hintergrund haben. Cyberspionage ist dadurch gekennzeichnet, dass öffentlich nicht zugängliche Daten, die auf Computern oder in Netzwerken gespeichert sind oder über drahtlose Kommunikationssysteme übertragen werden, heimlich oder unter Vortäuschung falscher Tatsachen mit Hilfe von Cyberoperationen abgeschöpft werden.[17]

In den nationalen Rechtsordnungen finden sich durchgängig Vorschriften, die den Staat vor Spionage schützen sollen und entsprechende Handlungen unter Strafe stellen. Gleichwohl ist das Ausspähen ausländischer Regierungen und Wirtschaftsunternehmen gängige Praxis und kein Staat hat ein Interesse daran, dass international verbindliche Regelungen seinen Handlungsspielraum auf diesem Gebiet einschränken. So üben die Staaten traditionell größte Zurückhaltung, wenn es darum geht, solche Aktivitäten völkerrechtlich zu bewerten. Die US-Regierung beispielsweise hat im Februar 2013 eine Strategie zur Bekämpfung des Diebstahls US-amerikanischer Handelsgeheimnisse veröffentlicht, die vor allem auf diplomatische Schritte, eine Stärkung des Schutzes der Unternehmen und auf nationale Gesetzgebung baut. Die völkerrechtliche Dimension des Diebstahls von Handelsgeheimnissen jedoch wird in der Strategie nicht erwähnt.[18] Aufgrund dieser zögerlichen Haltung der Staaten hat sich im Völkergewohnheitsrecht bislang keine Norm herausgebildet, die Spionage *per se* untersagen würde. Lediglich in einigen Bereichen wie dem Diplomaten- und Konsularrecht,[19] dem Seerecht[20] oder dem Recht internationaler bewaffneter Konflikte[21] setzt sich das Völkerrecht in begrenztem Umfang mit spionagerelevanten Aktivitäten auseinander. Außerdem stellen Übergriffe wie das illegale Eindringen ausländischer Agenten in fremdes Staatsgebiet oder unerlaubte Überflüge von Aufklärungsflugzeugen eine Verletzung des völkerrechtlichen Interventionsverbots dar – ohne

17 Katharina Ziolkowski, »Peacetime Cyber Espionage – New Tendencies in Public International Law«, in: Ziolkowski (Hg.), *Peacetime Regime for State Activities in Cyberspace* [wie Fn. 10], S. 425–464 (428ff).

18 Executive Office of the President of the United States, *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets*, Washington, D.C., Februar 2013, <www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf>.

19 Das Wiener Übereinkommen über diplomatische Beziehungen von 1961 bietet einen gewissen Schutz der jeweiligen Mission vor Ausspähung durch den Empfangsstaat (Unverletzlichkeit der Räumlichkeiten, Archive, Schriftstücke und amtlichen Korrespondenz einer Mission, Artikel 22, 24, 27). Auf der anderen Seite verbietet das Übereinkommen nicht ausdrücklich Spionage durch Mitglieder des diplomatischen Personals im Empfangsstaat, sondern trägt zumindest implizit dem Umstand Rechnung, dass die Grenze zwischen Diplomatie und Spionage in der Praxis häufig nicht trennscharf zu ziehen ist. Immerhin wird in Artikel 3 des Übereinkommens anerkannt, dass es zu den Aufgaben einer diplomatischen Mission gehört, sich mit allen rechtmäßigen Mitteln über Verhältnisse und Entwicklungen im Empfangsstaat zu unterrichten und darüber an die eigene Regierung zu berichten. Allerdings findet sich in Artikel 41 die Vorgabe, dass Diplomaten trotz ihrer Vorrechte und Immunität die Gesetze des Empfangsstaates zu beachten haben, sich nicht in innere Angelegenheiten einmischen dürfen und dass die Räumlichkeiten der Mission nicht in einer Weise benutzt werden dürfen, die mit den Aufgaben der Mission unvereinbar ist. Um Spionage vorbeugen und auf konkrete Fälle reagieren zu können, hat der Empfangsstaat insbesondere die Möglichkeit, jederzeit und ohne Angabe von Gründen ein Mitglied des diplomatischen Personals zur *persona non grata* zu erklären. In einem solchen Fall muss der Entsendestaat die betreffende Person abberufen oder ihre Tätigkeit bei der Mission beenden. Darüber hinaus kann der Empfangsstaat etwa den Personalbestand einer diplomatischen Mission begrenzen (Artikel 11), verhindern, dass Missionsbüros an anderen Orten innerhalb seines Staatsgebiets eingerichtet werden (Artikel 12), und die Bewegungsfreiheit von Diplomaten aus Gründen der nationalen Sicherheit in bestimmten Zonen einschränken (Artikel 26).

20 Das Seerecht verwehrt Schiffen, auf denen bestimmte spionagerelevante Handlungen vorgenommen werden, das Recht auf friedliche Durchfahrt im Küstenmeer (Artikel 19 des Seerechtsübereinkommens der Vereinten Nationen von 1982).

21 Das Recht internationaler bewaffneter Konflikte sanktioniert Spionageakte von Angehörigen der Streitkräfte einer Konfliktpartei, indem es den betreffenden Personen unter bestimmten Voraussetzungen den Kriegsgefangenenstatus entzieht (Artikel 46 des ersten Zusatzprotokolls von 1977 zu den Genfer Abkommen).

dass damit Spionage als solche international geächtet wäre.[22]

Umstritten ist, ob auch das virtuelle Einbrechen in Computersysteme oder Netzwerke, deren Server sich in einem fremden Hoheitsbereich befinden, als Souveränitätsverletzung zu werten ist.[23] Betrachtet man solche staatlich veranlassten Eingriffe als Ausübung von Hoheitsgewalt und Anmaßung fremder Jurisdiktion, lässt sich durchaus argumentieren, dass dadurch Souveränität verletzt wird.[24] Immerhin können solche Aktionen Veränderungen des Datenbestands zur Folge haben, etwa wenn digitale Spuren einer solchen Operation verwischt oder Zugänge für künftige Operationen gelegt werden. Eine Gruppe internationaler Experten hat 2013 auf Einladung des NATO-Exzellenzzentrums für Cyberverteidigung (Cooperative Cyber Defence Centre of Excellence, CCDCOE) in Tallinn ein Handbuch verfasst (Tallinn Manual), das den aktuellen Stand des Völkerrechts im Hinblick auf verschiedene Aspekte der Cyberkriegführung widerspiegeln soll und in dem auch zur Cyberspionage Stellung genommen wird.[25] Dabei handelt es sich weder um ein NATO-Dokument noch um ein Papier von Staaten, sondern um ein wissenschaftliches Forschungsvorhaben. In dem Handbuch heißt es unter anderem, das Eindringen in fremde Computersysteme zu Spionagezwecken verstoße nicht *per se* gegen das Interventionsverbot, weil es an einem interventionstypischen Zwangscharakter fehle, selbst wenn virtuelle Schutzmechanismen wie eine Firewall oder Passwortbarrieren überwunden werden müssten.[26] Andere Autoren stufen Cyberspionage jedoch als massive Bedrohung der nationalen Sicherheit ein und versuchen sogar, das Selbstverteidigungsrecht im Lichte dieser Bedrohung neu zu interpretieren.[27] Verwiesen wird besonders darauf, dass auf dem Wege der Cyberspionage binnen Sekundenbruchteilen Unmengen von Daten abgeschöpft werden könnten. Die Obama-Administration hat in ihrer internationalen Cyberspace-Strategie von 2011 unter dem Aspekt der Abschreckung jedenfalls angedeutet, dass die USA nicht nur gegen Angriffe auf ihre Netze, sondern auch gegen deren Ausforschung (computer network exploitation) notfalls mit aller Härte vorgehen werden.[28] Im Übrigen ist aber nicht erkennbar, dass die Staaten tatsächlich dazu tendieren, Cyberspionage als Verletzung des Interventionsverbots zu ächten.

22 Simon Chesterman, »Secret Intelligence«, in: Wolfrum (Hg.), *Max Planck Encyclopedia of Public International Law* [wie Fn. 9], Rn. 14ff.

23 Vgl. Ziolkowski, »Peacetime Cyber Espionage« [wie Fn. 17], S. 458f.

24 Vgl. Heintschel von Heinegg, »Legal Implications of Territorial Sovereignty in Cyberspace« [wie Fn. 2], S. 11f.

25 Michael N. Schmitt (Hg.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, New York: Cambridge University Press, 2013.

26 Ebd., S. 44f.

27 Vgl. z.B. Alexander Melnitzky, »Defending America against Chinese Cyber Espionage through the Use of Active Defenses«, in: *Cardozo Journal of International and Comparative Law*, 20 (2012) 2, S. 537–570.

28 The White House, *International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World*, Washington, D.C., Mai 2011, S. 13, <www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>.

Eine neue Dimension: Das systematische Ausspähen privater Daten

Staatliche Nachrichtendienste scheinen in immer größerem Umfang auch damit beschäftigt zu sein, private Daten von Bürgerinnen und Bürgern im In- und Ausland auszuspähen, indem sie die Telekommunikation, den E-Mail-Verkehr und Internetaktivitäten systematisch überwachen. Zu den prominentesten Beispielen zählen die Aktivitäten der US-amerikanischen NSA (National Security Agency), unter anderem mit ihren Programmen »PRISM« und »Boundless Informant«. Aber auch der britische Nachrichtendienst GCHQ (Government Communications Headquarters) ist insoweit jüngst in die Schlagzeilen geraten.

Während im Völkerrecht keinerlei Vorschriften existieren, die zwischenstaatliche Spionage grundsätzlich verbieten, ist das Ausspähen privater Daten unter Menschenrechtsgesichtspunkten höchst problematisch. Bereits die Allgemeine Erklärung der Menschenrechte, die von der UN-Generalversammlung 1948 verabschiedet wurde und in weiten Teilen Völkergewohnheitsrecht widerspiegelt, enthält in Artikel 12 Garantien zum Schutz der Privatsphäre. Auf vertraglicher Ebene ist die Privatsphäre unter anderem durch die Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) von 1950 und den Internationalen Pakt über bürgerliche und politische Rechte von 1966 (Zivilpakt) geschützt.

Gemäß Artikel 8 EMRK hat jede Person das Recht auf Achtung ihrer Privatsphäre und Korrespondenz. Der Europäische Gerichtshof für Menschenrechte hat dieses Recht im Zusammenhang mit nachrichtendienstlichen Überwachungsmaßnahmen mehrfach konkretisiert.[29] Eine geheime Überwachung von Bürgern durch staatliche Stellen kann gemäß Artikel 8 Absatz 2 der Konvention nur zulässig sein, wenn sie in einem hinreichend bestimmten Gesetz geregelt und unbedingt notwendig ist, um demokratische Institutionen zu schützen. Auch breiter angelegte Überwachungsmaßnahmen können danach zulässig sein, soweit angemessene und wirksame Garantien gegen Missbrauch vorgesehen sind.[30] Nach Artikel 1 EMRK sichern die Vertragsparteien die in der Konvention enthaltenen Rechte aber nur Personen zu, die ihrer Hoheitsgewalt unterstehen (»everyone within their jurisdiction«). Ein Staat, der Personen gleich welcher Staatsangehörigkeit auf seinem eigenen Territorium überwacht (etwa indem er auf Server zugreift, die sich auf seinem Staatsgebiet befinden), übt Hoheitsgewalt aus und ist dabei in jedem Fall an Artikel 8 EMRK gebunden. Schwieriger zu beantworten ist die Frage, ob diese Bindung auch dann besteht, wenn Personen im Ausland ausgespäht werden. Nach der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte übt ein Staat außerhalb seines Territoriums Hoheitsgewalt aus, wenn er entweder effektive Kontrolle über ein bestimmtes Gebiet oder über eine bestimmte Person hat. Der bisherigen Rechtsprechung liegt jedoch ein physisches Verständnis von Kontrolle zugrunde, das sich nicht ohne weiteres auf die Überwachung digitaler Kommunikation übertragen lässt. In der Literatur wird daher zum Teil versucht, den Begriff der Kontrolle im Cyberkontext so weit zu fassen, dass auch bestimmte Formen virtueller Kontrolle darunter fallen,[31] etwa jemand anhand seiner Korrespondenz »durchleuchtet« wird. Andere Autoren stellen darauf ab, dass nicht nur die Erfassung von Daten einen Eingriff darstellt, sondern auch jede weitere Verarbeitung, Verwendung und Weitergabe dieser Daten. Danach könne eine außerhalb des eigenen Staatsgebiets stattfindende Überwachungsmaßnahme, die nur allgemein den Internetverkehr kontrolliert, vielleicht nicht in jedem Einzelfall als Ausübung von Hoheits-

29 European Court of Human Rights, *Klass and others v. Germany*, Application no. 5029/71, Judgment, 6.9.1978; *Case of Rotaru v. Romania*, Application no. 28341/95, Judgment, 4.5.2000; *Weber and Saravia v. Germany*, Application no. 54934/00, Decision as to the Admissibility, 29.6.2006; *Case of Liberty and others v. The United Kingdom*, Application no. 58243/00, Judgment, 1.7.2008; *Case of Kennedy v. The United Kingdom*, Application no. 26839/05, Judgment, 18.5.2010.

30 Vgl. Helmut Philipp Aust, *Stellungnahme zur Sachverständigenanhörung am 5.6.2014 im 1. Untersuchungsausschuss der 18. Wahlperiode des Deutschen Bundestages*, S. 7f, <www.bundestag.de/bundestag/ausschuesse18/ua/1untersuchungsausschuss/-/280848>, mit Verweisen zu den jeweiligen Entscheidungen des Europäischen Gerichtshofs für Menschenrechte.

31 Anne Peters, »Surveillance without Borders: The Unlawfulness of the NSA-Panopticon, Part II«, *EJIL: Talk!* (Blog of the European Journal of International Law), 4.11.2013, <www.ejiltalk.org/surveillance-without-borders-the-unlawfulness-of-the-nsa-panopticon-part-ii/>.

gewalt angesehen werden; der Charakter der Maßnahme wandele sich aber spätestens dann, wenn die Daten in Datenbanken auf dem eigenen Staatsgebiet gespeichert und weiterverarbeitet würden.[32]

Obgleich die Überwachungsmaßnahmen durch die NSA und andere amerikanische Geheimdienste nicht nach der EMRK, sondern nach dem Internationalen Zivilpakt zu beurteilen sind, stellen sich im Wesentlichen dieselben menschenrechtlichen Fragen. Gemäß Artikel 17 des Zivilpaktes darf niemand willkürlichen oder rechtswidrigen Eingriffen in seine Privatsphäre ausgesetzt werden. In den Schutzbereich dieser Vorschrift fällt auch digitale Korrespondenz. Die Staaten sind nicht nur selbst an dieses Verbot gebunden, sondern haben aktiv dafür Sorge zu tragen, dass Personen in ihrem Hoheitsbereich vor solchen Eingriffen durch andere Staaten sowie durch nichtstaatliche Akteure geschützt sind. Zu diesem Zweck müssen die Staaten Gesetze erlassen, die Art und Umfang zulässiger Eingriffe genau definieren.[33]

Eine flächendeckende und verdachtsunabhängige Überwachung der elektronischen Kommunikation von Bürgern ist mit Artikel 17 des Zivilpaktes jedenfalls nicht vereinbar. Im April 2014 hat der für den Pakt zuständige UN-Menschenrechtsausschuss seine Bedenken gegen die Praxis der USA in einer Stellungnahme veröffentlicht.[34] Unter anderem hat der Ausschuss gefordert, dass alle Überwachungsaktivitäten, gleichgültig ob innerhalb oder außerhalb der USA, durch öffentlich zugängliche Gesetze präzise geregelt und verhältnismäßig sein müssen. Außerdem müssten effektive Vorkehrungen gegen Missbrauch getroffen, das bestehende Aufsichtssystem in den USA reformiert und betroffenen Personen in Missbrauchsfällen wirksamer Rechtsschutz gewährt werden.

Gemäß Artikel 2 (1) des Zivilpaktes ist jeder Vertragsstaat verpflichtet, die in dem Pakt anerkannten Rechte allen in seinem Gebiet befindlichen und seiner Hoheitsgewalt unterstehenden Personen (»all individuals within its territory and subject to its jurisdiction«) zu gewähren. Der UN-Menschenrechtsausschuss hat bereits 2004 klargestellt, dass die Verpflichtungen gegenüber allen Personen bestehen, die sich unter der Gewalt oder effektiven Kontrolle (»anyone within the power or effective control«) eines Vertragsstaates befinden. Unerheblich ist, ob sich die betreffende Person tatsächlich auf dem Territorium der jeweiligen Vertragspartei aufhält.[35] Zur Auslegung des Merkmals der effektiven Kontrolle kann insoweit auf die Ausführungen zu Artikel 8 EMRK verwiesen werden. Im Falle der Abhöraktionen durch die USA kommt hinzu, dass die überwachte Kommunikation – selbst wenn es sich um Personen in Deutschland und anderen europäischen Staaten handelt – im Regelfall über Unternehmen erfolgt, die in den USA registriert sind und deren Server amerikanischer Jurisdiktion unterstehen. Die USA (ebenso wie Israel) indes zeigen sich unbeeindruckt von der Rechtsmeinung des UN-Menschenrechtsausschusses und des Internationalen Gerichtshofs zur extraterritorialen Anwendbarkeit des Internationalen Zivilpaktes. Sie vertreten die Position, dass der Zivilpakt keinerlei extraterritoriale Bindung entfaltet, sondern nur Personen innerhalb des eigenen Staatsgebiets schützt.[36] Derzeit ist nicht absehbar, wie diese grundlegenden juristischen Differenzen im transatlantischen Verhältnis überwunden werden könnten. Solange die beschriebenen Ungewissheiten weiterhin bestehen, dürften Bürgerinnen und Bürger in Europa, die ihre privaten Daten US-Firmen anvertrauen, jedenfalls kaum effektiv vor einer Überwachung durch amerikanische Behörden geschützt sein.

32 Aust, *Stellungnahme* [wie Fn. 30], S. 13f. Eine ähnliche Argumentation – wenngleich in einem anderen rechtlichen Kontext – hat das Bundesverfassungsgericht in seinem Urteil zum Verbrechensbekämpfungsgesetz/G 10 vertreten: Entscheidung vom 14.7.1999 – 1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95 (BVerfGE 100, 313), Absätze 173–176.

33 Human Rights Committee, International Covenant on Civil and Political Rights, *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, UN-Dok. A/43/40, Annex VI, 28.9.1988.

34 Human Rights Committee, International Covenant on Civil and Political Rights, *Concluding Observations on the Fourth Periodic Report of the United States of America*, UN-Dok. CCPR/C/USA/CO/4, 23.4.2014.

35 Human Rights Committee, International Covenant on Civil and Political Rights, *CCPR General Comment No. 31 [80]: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant*, UN-Dok. CCPR/C/21/Rev.1/Add.13, 26.5.2004, Absatz 10.

36 Human Rights Committee, International Covenant on Civil and Political Rights, *Summary Record of the 1405th Meeting: United States of America*, UN-Dok. CCPR/C/SR.1405, 24.4.1995, Absatz 20; U.S. Department of State, *U.S. Observations on Human Rights Committee General Comment 31*, Washington, D.C., 27.12.2007, <http://2001-2009.state.gov/s/l/2007/112674.htm>; U.S. Department of State, *Fourth Periodic Report of the United States of America to the United Nations Committee on Human Rights Concerning the International Covenant on Civil and Political Rights*, Washington, D.C., 30.12.2011, <www.state.gov/j/drl/rls/179781.htm>, Absatz 505.

Politische Einflussnahme mit Hilfe von Cybertechnologie

Die Anonymität des Cyberspace und die zunehmende Vernetzung staatlicher Informationsinfrastrukturen eröffnen nicht nur neue Wege, um unentdeckt an sensible Daten von Regierungen zu gelangen. Auch die politischen Geschicke der Staaten lassen sich durch Cyberoperationen mehr oder weniger offen beeinflussen. Greift ein Staat direkt oder indirekt in innere oder äußere Angelegenheiten ein, die in die ausschließliche Zuständigkeit eines anderen Staates fallen, so liegt darin grundsätzlich ein Verstoß gegen das völkerrechtliche Interventionsverbot. Diese Norm gilt jedoch ausschließlich im zwischenstaatlichen Verhältnis, so dass das illegale Hacken staatlicher Netze durch Privatpersonen nicht als verbotene Intervention zu werten ist, sofern nicht ein Staat als Auftraggeber im Hintergrund steht.[37] Auf das Problem der völkerrechtlichen Zurechnung von Cyberakten wird weiter unten noch ausführlicher einzugehen sein.[38]

Die UN-Generalversammlung hat 1970 die Friendly-Relations-Deklaration verabschiedet, die zu großen Teilen Völkergewohnheitsrecht widerspiegelt. Dort heißt es, dass kein Staat Maßnahmen ergreifen darf, um einen anderen Staat zu zwingen, sich ihm bei der Ausübung seiner souveränen Rechte unterzuordnen.[39] In seiner Nicaragua-Entscheidung von 1986 hat der Internationale Gerichtshof die Ausübung von Zwang als das wesentliche Element einer verbotenen Intervention beschrieben.[40] Diese Entscheidung, die bis heute als wegweisend angesehen wird, betrifft Fälle, in denen Staaten versuchen, eine Veränderung der politischen Strukturen in anderen Staaten zu erzwingen, vor allem indem sie militärische und paramilitärische Aktivitäten unterstützen. Nach Auffassung des Internationalen Gerichtshofs kann die Unterstützung von Oppositionskräften durch Waffenlieferungen und Training sogar gegen das Gewaltverbot nach Artikel 2 (4) der UN-Charta verstoßen.[41] Diese Bewertung lässt sich durchaus auf den Cyberkontext übertragen, etwa wenn Aufständische von ausländischen Geheimdiensten die nötigen Werkzeuge erhalten und darin geschult werden, Cyberattacken zu starten. Die bloße Finanzierung solcher Gruppen stellt als solche allerdings keine Verletzung des Gewaltverbots dar, sondern lediglich eine völkerrechtswidrige Intervention.[42]

Von einer Verletzung des Interventionsverbots ist zum Beispiel auch dann auszugehen, wenn mit Hilfe von Cyberoperationen etwa Wahlergebnisse manipuliert oder falsche Informationen gestreut werden, um die Bevölkerung in einem anderen Staat gegen die eigene Regierung aufzuwiegeln und bewaffnete Unruhen zu entfachen oder einen Regimesturz herbeizuführen.[43] Solche Maßnahmen ähneln in ihrer Wirkung herkömmlichen Formen subversiver Intervention durch Radio- und Rundfunkpropaganda.[44] Vor allem Russland und China betonen bei ihren Bemühungen um eine Kodifizierung von Normen zur Cybersicherheit immer wieder das Recht der Staaten, ihren »Informationsraum« vor äußerer Einflussnahme zu schützen.[45]

37 Terry D. Gill, »Non-Intervention in the Cyber Context«, in: Ziolkowski (Hg.), *Peacetime Regime for State Activities in Cyberspace* [wie Fn. 10], S. 217–238 (233).

38 Dazu ausführlicher ab S. 21.

39 UN General Assembly, *Resolution 2625 (XXV), Declaration on Principles of International Law Concerning Friendly Relations and Cooperation among States in Accordance with the Charter of the United Nations*, UN-Dok. A/RES/2625 (XXV), 24.10.1970, Annex, Prinzip III (Concerning the Duty not to Intervene in Matters within the Domestic Jurisdiction of any State), Absatz 2.

40 International Court of Justice, *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Merits, Judgment, 27.6.1986, ICJ Reports 1986, S. 14–150 (108) [Absatz 205].

41 Ebd., S. 119.

42 Vgl. Schmitt (Hg.), *Tallinn Manual* [wie Fn. 25], S. 46. Der Internationale Gerichtshof hat in seiner Nicaragua-Entscheidung sogar die finanzielle Unterstützung von Rebellengruppen als klaren Verstoß gegen das Interventionsverbot angesehen, obgleich sich durchaus diskutieren lässt, ob durch eine solche Form der Unterstützung tatsächlich Zwang auf den Zielstaat ausgeübt wird. International Court of Justice, *Nicaragua v. United States of America* [wie Fn. 40], S. 124 (Absatz 242).

43 UN General Assembly, *Declaration on Principles of International Law Concerning Friendly Relations* [wie Fn. 39]. Dazu Pirker, »Territorial Sovereignty and Integrity and the Challenges of Cyberspace« [wie Fn. 10], S. 201.

44 Dazu Philip Kunig, »Intervention, Prohibition of«, in: Wolfrum (Hg.), *Max Planck Encyclopedia of Public International Law* [wie Fn. 9], Rn. 24.

45 Zur russischen und chinesischen Position siehe unten, S. 27f.

Cyberattacken zwischen Provokation und bewaffnetem Angriff

Das Spektrum von Cyberattacken gegen staatliche und private Einrichtungen reicht vom Testen von Sicherheitslücken über gezielte Provokationen bis hin zur Schädigung von Computersystemen und größeren Sabotageakten, mit denen wichtige Bereiche des öffentlichen Lebens lahmgelegt werden können. Handelt es sich bei den Tätern um private Hacker, die nicht im Auftrag staatlicher Stellen aktiv sind, greifen die internationalen Regelungen der Budapester Konvention zur Bekämpfung von Cyberkriminalität.[46] Geht eine solche Attacke jedoch von einem Staat aus, könnte zudem eine Verletzung des völkerrechtlichen Interventionsverbots und des Gewaltverbots vorliegen.

Ein alltägliches Phänomen sind die zahllosen Angriffe, die Computersystemen von Unternehmen und staatlichen Institutionen gelten, auf den virtuellen Raum beschränkt sind und allenfalls geringe materielle Schäden zur Folge haben. Solche Attacken können unter ungünstigen politischen Vorzeichen dennoch zwischenstaatliche Spannungen hervorrufen.

Nach geltendem Völkerrecht darf der verletzte Staat nämlich bestimmte Gegenmaßnahmen (countermeasures, traditionell als Repressalie bezeichnet) ergreifen. Das Recht zu Gegenmaßnahmen erlaubt es ausnahmsweise, eigentlich völkerrechtswidrige Handlungen vorzunehmen, um ein völkerrechtswidriges Delikt abzustellen, gewissermaßen als Mittel zur Selbsthilfe gegen Völkerrechtsbrüche.[47] Die Maßnahmen müssen allerdings unterhalb der Schwelle des Gewaltverbots bleiben und verhältnismäßig sein. Außerdem muss der verletzte Staat bestimmte prozedurale Voraussetzungen beachten. Nach Auffassung der Völkerrechtskommission sind die Gegenmaßnahmen zu beenden, sobald der verantwortliche Staat seinen Verpflichtungen nachgekommen ist.[48]

Verursacht ein Sabotageakt größere materielle Schäden, kann sogar das völkerrechtliche Gewaltverbot nach Artikel 2 (4) der UN-Charta verletzt sein.[49] Artikel 2 (4) schützt den Staat in seiner territorialen Integrität vor jeglicher Gewaltanwendung durch andere Staaten. Dabei spielt es keine Rolle, ob sich die Gewalt gegen öffentliche oder private Objekte auf dem Hoheitsgebiet richtet. Nach allgemeiner Auffassung verletzt eine Cyberattacke das völkerrechtliche Gewaltverbot, sofern deren Auswirkungen qualitativ und quantitativ mit den Folgen kinetischer Gewaltanwendung vergleichbar sind.[50] Im Tallinn-Handbuch von 2013 ist eine Reihe von Indizien aufgelistet, die im Einzelfall dafür sprechen, dass eine Cyberoperation als verbotene Gewaltanwendung im Sinne von Artikel 2 (4) der UN-Charta zu bewerten ist. Dazu zählen der Eintritt eines physischen Schadens an Personen oder Sachen, eine unmittelbare Kausalität zwischen Handlung und Schadenseintritt sowie eine unmittelbare zeitliche Nähe des Schadenseintritts.[51]

Die USA vertreten traditionell die Auffassung, dass jede völkerrechtswidrige Gewaltanwendung den betroffenen Staat dazu berechtigt, notwendige und verhältnismäßige Maßnahmen zur Selbstverteidigung zu ergreifen. Dies würde nach amerikanischer Lesart bedeuten, dass der angegriffene Staat notfalls auch

46 Zur Budapester Konvention siehe oben, S. 9f.

47 Von Arnauld, *Völkerrecht* [wie Fn. 3], S. 164.

48 Artikel 49ff der Artikelentwürfe der Völkerrechtskommission der Vereinten Nationen zur Staatenverantwortlichkeit: International Law Commission, »Responsibility of States for Internationally Wrongful Acts«, in: *Yearbook of the International Law Commission*, 2001, Vol. II, Part Two, S. 26–143; veröffentlicht auch als Annex zu UN General Assembly, *Resolution 56/83, Responsibility of States for Internationally Wrongful Acts*, 12.12.2001, UN-Dok. A/RES/56/83, 28.1.2002.

49 Zur Anwendbarkeit des Gewaltverbots und des Selbstverteidigungsrechts auf Cyberoperationen vgl. umfassend Nils Melzer, *Cyberwarfare and International Law*, Genf: United Nations Institute for Disarmament Research (UNIDIR), 2011, <http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf>.

50 Vgl. Schmitt (Hg.), *Tallinn Manual* [wie Fn. 25], S. 45ff; Matthew C. Waxman, »Cyber-Attacks and the Use of Force: Back to the Future of Article 2 (4)«, in: *Yale Journal of International Law*, 36 (2011) 2, S. 421–459 (431ff); Michael N. Schmitt, »Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework«, in: *Columbia Journal of Transnational Law,* 37 (1999), S. 885–937 (912ff).

51 Weitere Indizien finden sich bei Schmitt (Hg.), *Tallinn Manual* [wie Fn. 25], S. 48ff. Bei dieser Auflistung handelt es sich jedoch nicht um einen abschließenden verbindlichen Kriterienkatalog. Die Verfasser des Tallinn-Handbuchs gehen lediglich davon aus, dass solche Faktoren eine Rolle spielen können, wenn staatliche Stellen eine Einschätzung darüber treffen sollen, ob das Gewaltverbot im Einzelfall verletzt wurde.

mit konventionellen Militärschlägen auf eine solche Cyberattacke reagieren darf. Der Internationale Gerichtshof hat jedoch in seiner Nicaragua-Entscheidung dargelegt, dass die Schwelle zum bewaffneten Angriff im Sinne von Artikel 51 der UN-Charta erst dann überschritten ist, wenn die Gewaltanwendung ein bestimmtes Ausmaß erreicht und ihre Folgen besonders schwerwiegend sind.[52] Anders als die USA orientieren sich viele andere Staaten und die Mehrheit der Völkerrechtler an dieser prinzipiellen Unterscheidung. Sie gehen davon aus, dass ein Recht auf Selbstverteidigung erst dann gegeben ist, wenn die Anwendung von Gewalt eine gewisse Schwelle überschreitet und dadurch zu einem bewaffneten Angriff wird.[53]

Die Denial-of-Service-Attacken beispielsweise, die 2007 empfindliche Störungen des Regierungs- und Finanzsektors in Estland bewirkt haben, werden als Intervention unterhalb der Schwelle des Gewaltverbots bewertet (sofern es sich dabei tatsächlich um einen staatlich veranlassten Eingriff gehandelt haben sollte).[54] Auch der offensichtlich in staatlicher Regie erfolgte Stuxnet-Angriff auf das iranische Atomprogramm, der 2010 entdeckt wurde, lässt sich hinsichtlich seiner Intensität und Zielrichtung als Intervention einstufen. Einige Experten sprechen sogar davon, dass diese Attacke angesichts der verursachten physischen Schäden bereits die Schwelle eines bewaffneten Angriffs im Sinne von Artikel 51 der UN-Charta erreicht habe.[55] Allerdings wird auch darüber diskutiert, ob es sich bei der Stuxnet-Operation um eine völkerrechtlich legale Gegenmaßnahme in Reaktion auf das völkerrechtswidrige Verhalten Irans im Atomstreit gehandelt haben könnte.[56]

52 International Court of Justice, *Nicaragua v. United States of America* [wie Fn. 40], S. 101ff (Absatz 191ff). Vgl. auch International Court of Justice, *Case Concerning Oil Platforms (Islamic Republic of Iran v. United States of America)*, Judgment, 6.11.2003, ICJ Reports 2003, S. 161–219 (187) [Absatz 51].

53 Vgl. z.B. Yoram Dinstein, *War, Aggression and Self-Defence*, 5. Auflage, Cambridge: Cambridge University Press, 2011, S. 207ff; vgl. auch Michael N. Schmitt, »International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed«, in: *Harvard International Law Journal Online*, 54 (2012), S. 13–37, <www.harvardilj.org/wp-content/uploads/2012/12/HILJ-Online_54_Schmitt.pdf>.

54 Gill, »Non-Intervention in the Cyber Context« [wie Fn. 37], S. 234.

55 Vgl. den Hinweis auf die Debatte bei Schmitt (Hg.), *Tallinn Manual* [wie Fn. 25], S. 58.

56 Gill, »Non-Intervention in the Cyber Context« [wie Fn. 37], S. 235. Ablehnend Marco Roscini, »Cyber Operations as Nuclear Counterproliferation Measures«, in: *Journal of Conflict & Security Law,* 19 (2014) 1, S. 133–157.

Der Ernstfall: Cyberattacken gegen kritische Infrastrukturen

In der Abschlusserklärung des NATO-Gipfels von Wales haben die Staats- und Regierungschefs im September 2014 erstmals bekräftigt, dass die Hauptaufgabe der NATO, die kollektive Verteidigung, auch die Verteidigung gegen Cyberangriffe einschließe. Solche Attacken könnten die nationale und euro-atlantische Sicherheit und Stabilität bedrohen und ihre Auswirkungen könnten ebenso schwerwiegend sein wie die eines konventionellen Angriffs. Wann eine Cyberattacke den Bündnisfall nach Artikel 5 des NATO-Vertrages auslöse, müsse im Einzelfall vom Nordatlantikrat entschieden werden.[57]

Es steht außer Zweifel, dass Cyberattacken unmittelbare und mittelbare zerstörerische Folgen haben können, die weitaus gravierender sind als die Wirkungen konventioneller Angriffe. Als besonders gefährlich werden grundsätzlich Cyberangriffe gegen Steuerungssysteme kritischer Infrastrukturen[58] eingeschätzt. Dadurch hervorgerufene Funktionsstörungen können sich katastrophal auswirken, etwa wenn es zu Ausfällen in der Flugsicherung kommt, das Trinkwasser verunreinigt wird, nukleare Strahlung oder gefährliche biologische und chemische Substanzen freigesetzt werden, Staudämme geflutet werden oder die Stromversorgung flächendeckend zusammenbricht.

Generell anerkannt ist, dass Cyberattacken die Schwelle zum bewaffneten Angriff im Sinne von Artikel 51 der UN-Charta überschreiten und damit die Anwendung des staatlichen Selbstverteidigungsrechts auslösen können. Die Reaktionen der Staatengemeinschaft auf die terroristischen Anschläge vom 11. September 2001 haben gezeigt, dass Angriffe durch nichtstaatliche Akteure ebenfalls unter Artikel 51 fassbar sind. Ob eine Cyberattacke die Schwellenvoraussetzungen eines bewaffneten Angriffs erfüllt, hängt nach herrschender Meinung wiederum davon ab, ob sie hinsichtlich ihrer Intensität und ihrer Folgen mit einem konventionellen bewaffneten Angriff vergleichbar ist. Davon ist jedenfalls auszugehen, wenn der Angriff zu Todesopfern, Verletzten oder erheblichen Sachschäden führt. Je unmittelbarer solche Folgen eintreten, desto eindeutiger lässt sich die Attacke als bewaffneter Angriff einstufen. Schwieriger ist dies im Falle von Cyberangriffen, die erst nach zahlreichen Zwischenschritten und geraumer Zeit oder in Intervallen schädliche Auswirkungen entfalten. Vor allem wenn Steuerungssysteme kritischer Infrastrukturen angegriffen werden, kann zwischen der ursächlichen Cyberattacke und dem Eintritt des Schadens eine beträchtliche Zeitspanne liegen.[59]

Höchst umstritten ist, ob Cyberattacken auch dann einen bewaffneten Angriff darstellen, wenn die Folgen nicht unmittelbar physischer Natur sind.[60] Sofern beispielsweise wichtige Finanz- und Handelssysteme über einen längeren Zeitraum zum Erliegen kommen und die Märkte zusammenbrechen, wären die mittelbaren Folgen für die Staatengemeinschaft kaum absehbar. Manche vertreten die Auffassung, dass Cyberangriffe, die die Funktionsfähigkeit kritischer Infrastrukturen beeinträchtigen, stets als bewaffnete Angriffe im Sinne von Artikel 51 zu werten sind – unabhängig davon, ob unmittelbar ein physischer Schaden eintritt.[61] Diese Sichtweise leistet jedoch einer Ausuferung des Selbstverteidigungsrechts Vorschub. Die Gegenposition geht davon aus, dass ein bewaffneter Angriff nur dann vorliegt, wenn die Attacke einen Kausalverlauf in Gang gesetzt hat oder setzen soll, der absehbar den Tod von Menschen oder beträchtliche Sachschäden nach sich zieht. Rein ökonomische Folgeschäden wären somit nicht ausreichend, um eine Cyberattacke als bewaffneten Angriff zu klassifizieren. Nach dieser Auffassung begründen zum Beispiel Angriffe, die ohne physische Zerstörung vorübergehend zivile Kommunikationseinrichtungen lahmlegen, grundsätzlich noch

57 NATO, *Wales Summit Declaration. Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Wales*, Press Release, 5.9.2014, <www.nato.int/cps/en/natohq/official_texts_112964.htm>.

58 Zur Definition kritischer Infrastrukturen vgl. Melzer, *Cyberwarfare and International Law* [wie Fn. 49], S. 14f.

59 Dazu Marco Roscini, »World Wide Warfare – *Jus ad bellum* and the Use of Cyber Force«, in: Armin von Bogdandy/Rüdiger Wolfrum (Hg.), *Max Planck Yearbook of United Nations Law*, 14 (2010), S. 85–130 (117ff).

60 Zu dieser Problematik vgl. Melzer, *Cyberwarfare and International Law* [wie Fn. 49], S. 14ff.

61 National Research Council of the National Academies, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, Washington, D.C., 2009, S. 254f.

kein Recht auf Selbstverteidigung.[62] Innerhalb der Expertengruppe, die das Tallinn-Handbuch verfasst hat, konnte in diesen Fragen allerdings keine Einigkeit erzielt werden.[63] Bis zum gegenwärtigen Zeitpunkt ist jedenfalls noch keine Cyberattacke von der internationalen Gemeinschaft eindeutig als bewaffneter Angriff im Sinne von Artikel 51 der UN-Charta bewertet worden.

62 Roscini, »World Wide Warfare« [wie Fn. 59], S. 115f.
63 Schmitt (Hg.), *Tallinn Manual* [wie Fn. 25], S. 56.

Militärische Selbstverteidigung gegen Cyberattacken

Das Selbstverteidigungsrecht, das in Artikel 51 der UN-Charta verankert ist, erlaubt die Anwendung militärischer Gewalt gegen einen bewaffneten Angriff. Auch defensive Cyberoperationen, die die Schwelle zur Gewaltanwendung im Sinne von Artikel 2 (4) der Charta überschreiten, können dadurch gerechtfertigt sein. In der Praxis jedoch lassen sich die Urheber einer Cyberattacke nur in den seltensten Fällen so eindeutig identifizieren, dass eine völkerrechtliche Zurechnung möglich wird. Daher ist kaum vorstellbar, wie ein Staat die hohen Nachweisanforderungen erfüllen kann, die für eine Inanspruchnahme des Selbstverteidigungsrechts gelten. Dies wird im nachfolgenden Kapitel noch ausführlicher erörtert. Da indes nicht gänzlich auszuschließen ist, dass die Zurechnung eines Angriffs im Einzelfall gelingt, sollen die Voraussetzungen für die Anwendung des Selbstverteidigungsrechts an dieser Stelle kurz skizziert werden.

Die Ausübung des Selbstverteidigungsrechts unterliegt den Grundsätzen der Notwendigkeit und Verhältnismäßigkeit. Notwendig ist die Anwendung von Gewalt zur Selbstverteidigung, wenn keine anderen Optionen zur Verfügung stehen, um den Angriff wirksam abzuwehren. Im Falle eines Cyberangriffs kann ein militärischer Gegenschlag folglich nur dann zulässig sein, wenn aktive oder passive Cyberabwehrmechanismen keinen ausreichenden Schutz bieten. Sofern die Anwendung von Gewalt notwendig ist, bestimmt sich das zulässige Ausmaß nach dem Verhältnismäßigkeitsprinzip. Lässt sich ein Angriff beispielsweise durch den gezielten Einsatz von Spezialkräften wirksam zurückschlagen, wäre eine großangelegte militärische Invasion unverhältnismäßig. Grundbedingung einer legitimen Ausübung des Selbstverteidigungsrechts ist zudem, dass der betreffende Einsatz auch tatsächlich der Abwehr eines Angriffs dient. Vergeltungsmaßnahmen sind durch das Selbstverteidigungsrecht nicht gedeckt. Prinzipiell gilt daher, dass die Abwehrhandlung in einer gewissen zeitlichen Nähe zum Angriff erfolgen muss.

Werden in einem sich anbahnenden militärischen Konflikt Kommunikations- und Waffensysteme eines Staates zum Ziel von Cyberattacken, kann dies ein Indiz dafür sein, dass ein konventioneller Angriff unmittelbar bevorsteht. Mittlerweile dürfte es gängige Praxis sein, dass Militärinterventionen durch Cyberoperationen vorbereitet und flankiert werden.[64] In einem solchen Fall kann sich der betroffene Staat in engen Grenzen auf ein Recht zu antizipatorischer Selbstverteidigung berufen, sofern er plausibel darlegt, dass tatsächlich unmittelbar mit einem Militärschlag zu rechnen ist. Dabei kommt es nicht darauf an, ob die Cyberattacke als solche bereits die Schwelle von Artikel 51 der UN-Charta überschreitet. Entscheidend ist, dass sie wesentlicher Bestandteil einer militärischen Operation ist, die bei ungehindertem Fortgang unmittelbar in einen militärischen Angriff mündet. Die Verhältnismäßigkeit der Verteidigung bestimmt sich in diesem Fall nicht nach der Intensität der Cyberattacke, sondern nach dem Ausmaß der militärischen Angriffsbedrohung.[65]

Anders gelagert sind Fälle, in denen ein Staat das Recht in Anspruch nimmt, sich präventiv gegen befürchtete Cyberangriffe zu verteidigen und zu diesem Zweck Teile der IT-Infrastruktur eines anderen Staates physisch zerstört oder durch Cyberoperationen ausschaltet. Um solche Maßnahmen als Selbstverteidigung rechtfertigen zu können, müsste der Staat nachweisen, dass er tatsächlich der Bedrohung einer unmittelbar bevorstehenden Cyberattacke von der Intensität eines bewaffneten Angriffs ausgesetzt ist und ihm in dieser Situation ein weiteres Abwarten nicht zugemutet werden kann. Wie schwer ein solcher Nachweis in der Praxis zu führen ist, wird im folgenden Kapitel erläutert.

64 Vgl. z.B. Eric Schmitt/Thom Shanker, »U.S. Debated Cyberwarfare in Attack Plan on Libya«, in: *The New York Times*, 17.10.2011, <www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html?_r=0>.
65 Schmitt (Hg.), *Tallinn Manual* [wie Fn. 25], S. 930ff; Roscini, »World Wide Warfare« [wie Fn. 59], S. 120ff.

Das Grundproblem: Nachweis und Zurechnung der Urheberschaft von Cyberattacken

Eine der größten Herausforderungen bei der Abwehr von Cyberattacken besteht darin, den Ursprung und die Urheber eines Angriffs zu ermitteln. Selbst wenn offensichtlich ist, dass eine Cyberattacke von regierungseigenen Servern ausgeht oder den Weg über die Cyberinfrastruktur eines bestimmten Staates nimmt, kann daraus nicht ohne weiteres geschlossen werden, dass der betreffende Staat an dem Angriff in irgendeiner Form aktiv beteiligt ist.[66] Der Cyberspace bietet Angreifern eine Vielzahl von Möglichkeiten, ihre wahre Identität zu verschleiern und falsche Spuren zu legen. Eine gängige Methode bei Denial-of-Service-Attacken ist zum Beispiel die Nutzung von Botnetzen. Hinzu kommt, dass die Daten von Cyberoperationen innerhalb kürzester Zeit über zahllose Server in unterschiedlichen Staaten geleitet werden können, ohne dass die betroffenen Transitstaaten davon unmittelbar Kenntnis erlangen. Auch das Anmieten von Servern im Ausland kann ein Weg sein, um Spuren zu verwischen. Gerade im Falle technologisch hochentwickelter Schadprogramme, die von professionellen Angreifern verwendet werden, sind die Rückverfolgungsmöglichkeiten äußerst begrenzt. Selbst wenn es gelingt, den Weg einer Attacke anhand der benutzten Server geographisch nachzuvollziehen oder einen bestimmten Programmierstil zu identifizieren, lässt sich auch mit Hilfe solcher Indizien allenfalls vermuten, wer hinter der Attacke steht. Je spezifischer und professioneller ein großangelegter Angriff wie im Falle von Stuxnet erfolgt, desto eher dürfte sich zumindest erahnen lassen, dass ein bestimmter Staat dafür verantwortlich ist.

Hacker, die sich durch eine Cyberattacke Zugriff auf ein System verschafft haben, benötigen mitunter längere Zeit, um den eigentlichen Angriff vorzubereiten. Zu dem Zeitpunkt, in dem eine Cyberattacke entdeckt wird, ist daher häufig nicht klar, worauf sie abzielt und mit welchen Folgen zu rechnen ist. Geht es beispielsweise um eine Aktion, mit der Systeme ausgespäht oder spätere Attacken vorbereitet werden sollen, oder ist tatsächlich bereits eine Kausalkette in Gang gesetzt worden, die physische Schäden nach sich ziehen wird?

In der Praxis erschweren diese Ungewissheiten die Abwehr konkreter Angriffe und machen rasche Reaktionen gegen die Urheber und deren Hintermänner nahezu unmöglich; und in rechtlicher Hinsicht laufen die allgemeinen Regeln, nach denen Staaten für völkerrechtswidrige Akte zur Verantwortung gezogen werden können,[67] unter solchen Bedingungen ins Leere. Voraussetzung ist nämlich, dass das betreffende Verhalten dem Staat juristisch zuzurechnen ist. Handeln zum Beispiel Privatpersonen oder Unternehmen faktisch im Auftrag eines Staates oder unter der Leitung oder Kontrolle staatlicher Stellen, so ist ihr Verhalten als Handlung des Staates zu werten.[68] Denkbar wäre etwa, dass ein Staat spezialisierte Firmen engagiert, um Cyberangriffe zu verfolgen oder aktiv zurückzuschlagen, oder sich zu Sabotagezwecken die Dienste privater Hackergruppen zunutze macht. In diesem Zusammenhang wird unter Völkerrechtlern seit langem darüber gestritten, in welchem Umfang ein Staat die Handlungen von Privatpersonen kontrollieren muss (»effective control« oder »overall control«), damit ihm deren Handlungen zugeschrieben werden können.[69]

Dieser Streit ist jedoch – wie alle theoretischen Überlegungen zur Anwendung etablierter Zurechnungskriterien – im Cyberkontext von untergeordneter Bedeutung, solange es den angegriffenen Staaten nicht einmal gelingt, die zugrundeliegenden Sachverhalte aufzuklären und die nötigen Nachweise zu führen. Gerade im Bereich der Cyberforensik besteht offenbar enormer Entwicklungsbedarf. Relevant sind daher andere Fragen: Bis zu welchem Grad beispielsweise muss ein Staat, der sich auf sein Selbstverteidigungsrecht beruft, beweisen, dass derjenige Staat, gegen

66 Vgl. Schmitt (Hg.), *Tallinn Manual* [wie Fn. 25], S. 34ff; Roscini, »World Wide Warfare« [wie Fn. 59], S. 102.

67 Vgl. die Artikelentwürfe der Völkerrechtskommission der Vereinten Nationen zur Staatenverantwortlichkeit [wie Fn. 48].

68 Vgl. Artikel 8 der Artikelentwürfe zur Staatenverantwortlichkeit [wie Fn. 48].

69 Zur Diskussion dieser Standards im Cyberkontext vgl. Scott J. Shackelford, »State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem«, in: Christian Czosseck/Karlis Podins (Hg.), *Conference on Cyber Conflict Proceedings 2010*, Tallinn: NATO CCDCOE, 2010, S. 197–208.

den sich die Verteidigung richtet, tatsächlich für den Angriff verantwortlich ist? Generell gilt: Je schwerwiegender die Anschuldigungen und je weitreichender die Konsequenzen, desto höher die Beweisanforderungen. In der Spruchpraxis internationaler Gerichte und Tribunale scheint sich – soweit es um Fragen der Staatenverantwortlichkeit im Zusammenhang mit der Anwendung bewaffneter Gewalt geht – ein Standard durchgesetzt zu haben, wonach die Beweislage klar und überzeugend (»clear and convincing«) sein muss.[70] Offen ist, was dieser Standard im Cyberkontext bedeutet und ob derart hohe Beweisanforderungen unter den beschriebenen Bedingungen überhaupt erfüllt werden können.[71] Zu diskutieren wäre auch darüber, wie eine Beweisführung im Falle von Cyberattacken aussehen könnte und welche Beweiskraft einzelnen Beweismitteln zukommen soll. Eine Absenkung der traditionellen Kriterien kann dazu führen, dass zwischenstaatliche Spannungen, die zunächst im Cyberspace ausgetragen werden, ohne Vorwarnung in militärische Auseinandersetzungen umschlagen, in die auch unbeteiligte Staaten schnell hineingezogen werden können.

Selbst wenn die Rückverfolgung einer Cyberattacke im Einzelfall möglich erscheint, dürfte das Verfahren außerordentlich zeitaufwendig sein. Die Ausübung des Selbstverteidigungsrechts unterliegt aber gewissen zeitlichen Grenzen. So soll die Verteidigungshandlung unmittelbar auf den Angriff erfolgen. Dies schließt zwar nicht aus, dass der angegriffene Staat gründliche Nachforschungen anstellt, bevor er eine militärische Verteidigung einleitet. Je mehr Zeit verstreicht, desto schwieriger wird es jedoch, die Gegenschläge unter das Selbstverteidigungsrecht zu fassen. Die beschriebenen Nachweis- und Zurechnungsprobleme haben jedenfalls zur Folge, dass die Staaten in den meisten Szenarien kaum in der Lage sein werden, die verfahrensmäßigen Voraussetzungen zu erfüllen, die für eine legitime Inanspruchnahme des Selbstverteidigungsrechts gelten.[72] Solange nicht mit klaren und überzeugenden Beweisen belegt werden kann, dass ein bestimmter Staat hinter einem Cyberangriff steht, sind weder konventionelle militärische Maßnahmen noch Cyberoperationen im Rahmen einer aktiven Verteidigung (active cyber defence), die die Schwelle zur Gewaltanwendung im Sinne von Artikel 2 (4) der UN-Charta überschreiten, durch das Selbstverteidigungsrecht gedeckt.

Angesichts dieser Probleme wird darüber diskutiert, ob sich Staaten gegebenenfalls auf Notstandsrechte berufen können, um Eingriffe in die Cyberinfrastruktur anderer Staaten zu rechtfertigen.[73] Für die Ausübung des Notstandsrechts kommt es gerade nicht darauf an, wer für die Gefahr verantwortlich ist. Damit stellen sich zwar keine Zurechnungsfragen, gleichzeitig steigt aber das Risiko einer missbräuchlichen Inanspruchnahme dieses Rechts. Deshalb wird in der Literatur gefordert, dass das Notstandsrecht nur in absoluten Ausnahmefällen zur Anwendung kommen dürfe, allenfalls wenn kritische Infrastrukturen unmittelbar angegriffen würden. Allerdings erschließt sich nicht, gegen wen und in welcher Form der betroffene Staat auf der Grundlage des Notstandsrechts in einem solchen Fall vorgehen sollte, wenn nicht einmal geklärt ist, aus welcher Richtung der Angriff kommt. Möglicherweise wäre es hilfreich, bestimmte Server zeitweilig abzuschalten oder Netzverbindungen zu kappen. In jedem Fall müsste aber plausibel dargelegt werden, dass tatsächlich keine anderen Mittel zur Verfügung stehen, um die Gefahr abzuwenden. Denn durch derart grob kalibrierte Notstandsmaßnahmen können auch unbeteiligte Staaten ernsthaft in Mitleidenschaft gezogen werden. Daher ist es kaum denkbar, dass ein Staat in Reaktion auf eine Cyberattacke jenseits der Voraussetzungen des zurechnungsgebundenen Selbstverteidigungsrechts einschneidende Maßnahmen gegen andere Staaten allein auf ein Notstandsrecht stützen kann.[74]

70 Robin Geiß/Henning Lahmann, »Freedom and Security in Cyberspace: Shifting the Focus away from Military Responses towards Non-forcible Countermeasures and Collective Threat-Prevention«, in: Ziolkowski (Hg.), *Peacetime Regime for State Activities in Cyberspace* [wie Fn. 10], S. 621–657 (624); Mary Ellen O'Connell, »Evidence of Terror«, in: *Journal of Conflict and Security Law*, 7 (2002) 1, S. 19–36; Thomas M. Franck, *Recourse to Force. State Action against Threats and Armed Attacks*, Cambridge: Cambridge University Press, 2002, S. 67f.

71 Geiß/Lahmann, »Freedom and Security in Cyberspace« [wie Fn. 70], S. 625.

72 Heike Krieger, »Krieg gegen anonymous. Völkerrechtliche Regelungsmöglichkeiten bei unsicherer Zurechnung im Cyberwar«, in: *Archiv des Völkerrechts*, 50 (2012) 1, S. 1–20 (20).

73 Vgl. Schmitt (Hg.), *Tallinn Manual* [wie Fn. 25], S. 39f. Nach Artikel 25 der Artikelentwürfe der Völkerrechtskommission zur Staatenverantwortlichkeit [wie Fn. 48] kann die Rechtswidrigkeit einer ansonsten völkerrechtswidrigen Handlung ausnahmsweise ausgeschlossen sein, wenn die Handlung die einzige Möglichkeit darstellt, um ein wesentliches Interesse vor einer schweren und unmittelbar drohenden Gefahr zu schützen, und wenn dadurch keine wesentlichen Interessen anderer Staaten ernsthaft beeinträchtigt werden (Notstand, state of necessity).

74 Dazu ausführlich Geiß/Lahmann, »Freedom and Security in Cyberspace« [wie Fn. 70], S. 644ff.

Was bleibt? – Völkerrechtliche Due-Diligence-Pflichten im Umgang mit Cybertechnologie

Zu den völkerrechtlichen Grundpflichten jedes Staates zählt, dafür zu sorgen, dass es innerhalb seines Hoheitsbereichs nicht zu Handlungen kommt, durch die andere Staaten in ihren Rechten verletzt werden.[75] Folglich darf ein Staat nicht wissentlich zulassen, dass auf seinem Territorium befindliche oder sonst von ihm kontrollierte Einrichtungen der Cyberinfrastruktur für Angriffe gegen andere Staaten missbraucht werden.[76] Dementsprechend muss der Staat einschreiten, wenn Erkenntnisse vorliegen, dass von Servern und Netzen, auf die er Zugriff hat, Cyberattacken ausgehen. Unter Völkerrechtlern wird davon gesprochen, dass die Regierung alle vernünftigerweise durchführbaren (»reasonably feasible«) Maßnahmen veranlassen müsse, um die Schädigungshandlung zu unterbinden.[77] Unter anderem seien auch private Internet-Service-Anbieter zur Gefahrenabwehr in Anspruch zu nehmen. In jedem Fall muss der Staat die von der Attacke betroffenen Staaten warnen und an der Abwehr und Aufklärung des Angriffs mitwirken, um den Schaden zu minimieren.

Weniger klar ist, in welchem Umfang die Staaten völkerrechtlich zu präventiven Maßnahmen verpflichtet sind. Die internationale Expertengruppe, die das Tallinn-Handbuch veröffentlicht hat, konnte sich in dieser Frage nicht auf eine gemeinsame Position verständigen.[78] Im Grunde ist die Forderung nachvollziehbar, dass die Staaten in ihrem Hoheitsbereich die notwendigen Vorkehrungen treffen müssen, um von vornherein zu verhindern, dass ihre Informations- und Kommunikationsinfrastruktur für Cyberangriffe und andere kriminelle Handlungen im Cyberspace missbraucht wird. Andererseits stoßen die Staaten dabei rasch an technische Grenzen. Dies entbindet sie aber nicht davon, ihren Hoheitsbereich mit einer gewissen Sorgfalt zu überwachen. Solche Due-Diligence-Pflichten existieren im Völkerrecht in den unterschiedlichsten Bereichen.[79] Dabei handelt es sich stets um kontextabhängige Handlungspflichten, nicht um die Pflicht, einen bestimmten Zustand herbeizuführen oder zu verhindern.[80]

Was die Identifizierung staatlicher Präventionspflichten im Zusammenhang mit der Nutzung des Cyberspace anbelangt, lassen sich vor allem Parallelen zum internationalen Umweltrecht ziehen. Der Internationale Gerichtshof hat 1996 in seinem Nuklearwaffengutachten betont, die Staaten seien generell verpflichtet sicherzustellen, dass Aktivitäten unter ihrer Hoheitsgewalt und Kontrolle mit der Umwelt vereinbar sind.[81] In einem Urteil von 2010 hat der Gerichtshof unter Verweis auf diesen Passus weiter ausgeführt, dass die Verpflichtung zur Prävention eine Pflicht zur Sorgfalt sei.[82] Darunter falle die Verabschiedung bestimmter Vorschriften ebenso wie deren wachsame Durchsetzung und die Ausübung administrativer Kontrolle über öffentliche und private Aktivitäten. Einige Autoren rekurrieren bei der Herleitung von Präventionspflichten im Cyberkontext auf das umweltrechtliche Vorsorgeprinzip.[83] Außerdem hat die

75 Vgl. International Court of Justice, *The Corfu Channel Case (United Kingdom of Great Britain and Northern Ireland v. Albania)*, Merits, Judgment, 9.4.1949, ICJ Reports 1949, S. 4–38 (22).
76 Schmitt (Hg.), *Tallinn Manual* [wie Fn. 25], S. 26. Diese Verantwortung erstreckt sich auch auf Einrichtungen der Cyberinfrastruktur, über die der Staat außerhalb seines Hoheitsgebiets rechtlich oder faktisch Kontrolle ausübt, etwa auf Militärstützpunkten oder in Botschaftsgebäuden im Ausland sowie auf Schiffen und in Luftfahrzeugen, die souveräne Immunität genießen [vgl. Fn. 5].
77 Schmitt (Hg.), *Tallinn Manual* [wie Fn. 25], S. 27.
78 Ebd.
79 Timo Koivurova, »Due Diligence«, in: Wolfrum (Hg.), *Max Planck Encyclopedia of Public International Law* [wie Fn. 9], Rn. 29ff.
80 Vgl. auch International Court of Justice, *Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgment, 26.2.2007, ICJ Reports 2007, S. 43–240 (220ff) [Absatz 428ff].
81 International Court of Justice, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, 8.7.1996, ICJ Reports 1996, S. 226–267 (242) [Absatz 29]. Vgl. auch UN General Assembly, *Report of the UN Conference on Environment and Development, Annex I (Rio Declaration on Environment and Development)*, Principle 2, UN-Dok. A/CONF.151/26, Vol. 1, 12.8.1992.
82 International Court of Justice, *Case Concerning Pulp Mills on the River Uruguay (Argentina v. Uruguay)*, Judgment, 20.4.2010, ICJ Reports 2010, S. 14–107 (79) [Absatz 197]: »[...] the obligation [...] to prevent [...] is an obligation to act with due diligence in respect of all activities which take place under the jurisdiction and control of each party«.
83 Thilo Marauhn, »Customary Rules of International Environmental Law – Can they Provide Guidance for Developing a Peacetime Regime for Cyberspace?«, in: Ziolkowski (Hg.),

Völkerrechtskommission der Vereinten Nationen im Jahr 2001 Artikelentwürfe zur Verhütung grenzüberschreitender Schäden bei gefährlichen Aktivitäten verabschiedet.[84] Darin geht es um Tätigkeiten, die völkerrechtlich nicht verboten sind, aber das Risiko beinhalten, durch physische Auswirkungen schwerwiegende grenzüberschreitende Schäden zu verursachen. Nach den Artikelentwürfen ist jeder Staat, in dessen Territorium oder unter dessen Jurisdiktion oder Kontrolle solche Aktivitäten stattfinden, verpflichtet, alle geeigneten Maßnahmen zu treffen, um Schäden zu verhindern, oder jedenfalls das Risiko zu minimieren. Zu diesem Zweck müssen die Staaten die erforderlichen legislativen, administrativen und sonstigen Maßnahmen treffen und geeignete Überwachungsmechanismen schaffen. Der im Einzelfall anzulegende Due-Diligence-Standard richtet sich nach dem Ausmaß des drohenden Schadens und dem Grad der Eintrittswahrscheinlichkeit. Zur Verfahrensweise enthalten die Artikelentwürfe zudem Kooperations-, Konsultations- und Informationspflichten sowie Vorgaben für Notfallsituationen. Wenigstens in dieser Hinsicht können die Artikelentwürfe als Vorbild dienen, um die Sorgfaltspflichten von Staaten bei der Nutzung des Cyberspace auszubuchstabieren. Ein weiterer wichtiger Orientierungspunkt sind die nationalen Cybersicherheitsstrategien. Darin sind zumindest einzelne Bereiche definiert, in denen Due Diligence eine Rolle spielt.[85]

Grundsätzlich sollte sich auf internationaler Ebene ein Verständnis durchsetzen, wonach für alle Staaten bestimmte Due-Diligence-Pflichten gelten. Im Einzelfall kommt es aber unter anderem darauf an, in welcher Form ein Staat von einer Cyberattacke betroffen ist, etwa ob sie von seinem Territorium ausgeht, über Server in seinem Hoheitsbereich weitergeleitet wird oder gegen Ziele in seinem Territorium gerichtet ist. Dabei ist zu berücksichtigen, dass nicht alle Staaten dieselben technologischen Möglichkeiten haben, um die Cyberinfrastruktur in ihrem Hoheitsbereich vor Missbrauch zu schützen. Ob ein Staat im Einzelfall seinen Due-Diligence-Pflichten nachgekommen ist, hängt daher auch davon ab, über welche Möglichkeiten er verfügt.[86] Darüber hinaus wird immer wieder der dynamische Charakter solcher Pflichten betont.[87] So lässt sich argumentieren, dass die Staaten ihre Systeme kontinuierlich überprüfen und dem neusten Stand der technologischen Entwicklung anpassen müssen.

Peacetime Regime for State Activities in Cyberspace [wie Fn. 10], S. 465–484; Krieger, »Krieg gegen anonymous« [wie Fn. 72], S. 5ff, 16ff.

84 International Law Commission, »Prevention of Transboundary Harm from Hazardous Activities«, in: *Yearbook of the International Law Commission*, 2001, Vol. II, Part Two, S. 144–170.

85 Die Cybersicherheitsstrategie der Bundesregierung hebt unter anderem folgende Bereiche hervor: Schutz kritischer Informationsinfrastrukturen, Verbesserung der Sicherheit bei der Nutzung privater und öffentlicher IT-Systeme, Optimierung der Zusammenarbeit staatlicher Stellen bei Schutz und Abwehr (Nationales Cyber-Abwehrzentrum, Nationaler Cyber-Sicherheitsrat), wirksame Kriminalitätsbekämpfung im Cyberspace, effektives Zusammenwirken der Staaten in Europa und weltweit, Einsatz verlässlicher und vertrauenswürdiger Informationstechnologie, Personalentwicklung, Instrumentarium zur Abwehr von Cyberangriffen. Bundesministerium des Innern, *Cyber-Sicherheitsstrategie für Deutschland*, Berlin, Februar 2011, <www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile>.

86 Vgl. Koivurova, »Due Diligence« [wie Fn. 79], Rn. 19.

87 Vgl. International Law Commission, »Prevention of Transboundary Harm« [wie Fn. 84], Article 3, Commentary, Absatz 11.

Verantwortlichkeit und Gegenmaßnahmen bei Due-Diligence-Pflichtverletzungen

Professionelle Angreifer werden sich im Einzelfall kaum davon abhalten lassen, mit Cyberattacken großen Schaden anzurichten, und es ist fast unmöglich, einem Staat die Beteiligung an einem Cyberangriff zweifelsfrei nachzuweisen. Dennoch ebnet die Konzentration auf Due-Diligence-Pflichten den Weg, Staaten für Versäumnisse bei der Absicherung ihrer Infrastruktur, für pflichtwidrig unterlassenes Einschreiten oder für mangelnde Kooperation bei der Abwehr und Aufklärung von Cyberattacken völkerrechtlich zur Verantwortung zu ziehen. Dadurch kann es gelingen, zumindest den alltäglichen Bedrohungen im Cyberspace wirksamer zu begegnen.[88] Unter dem Blickwinkel von Due Diligence spielt es keine Rolle, ob ein Staat in einem konkreten Fall tatsächlich Kenntnis davon hatte, dass seine Informations- und Kommunikationsinfrastruktur für eine Cyberattacke missbraucht wurde. Entscheidend ist vielmehr, dass mittlerweile jeder Staat über die mit der Nutzung von Cybertechnologie verbundenen Risiken informiert ist und in seinem Hoheitsbereich alle vernünftigerweise durchführbaren Sicherheitsvorkehrungen treffen muss.

Eine Verletzung von Due-Diligence-Pflichten im Zusammenhang mit einer Cyberattacke zieht bestimmte Rechtsfolgen nach sich. Der völkerrechtlich verantwortliche Staat ist nicht nur verpflichtet, die Schutzlücken umgehend zu schließen und bei der Abwehr und Rückverfolgung des Angriffs behilflich zu sein, sondern muss nach den Grundsätzen der Staatenverantwortlichkeit auch Wiedergutmachung leisten.[89] Darüber hinaus hat ein durch eine völkerrechtswidrige Handlung verletzter Staat prinzipiell das Recht, in verhältnismäßigem Umfang Gegenmaßnahmen zu ergreifen, um den verantwortlichen Staat zu veranlassen, seine Verpflichtungen zu erfüllen.[90] Denkbar wäre zum Beispiel eine zeitweilige Abschaltung von Servern oder die Trennung von Netzverbindungen. Inwieweit solche Aktionen tatsächlich als Gegenmaßnahmen zulässig sein können, ist noch weitgehend ungeklärt.[91] Fest steht jedenfalls, dass die Gegenmaßnahmen ihrerseits unterhalb der Schwelle des Gewaltverbots nach Artikel 2 (4) der UN-Charta bleiben müssen und nicht mit grundlegenden menschenrechtlichen Garantien kollidieren dürfen. Im Übrigen wird im Einzelfall genau zu prüfen sein, ob die Gegenmaßnahme verhältnismäßig ist – und zwar nicht im Hinblick auf die eigentliche Cyberattacke, sondern gegenüber der jeweiligen Due-Diligence-Verletzung, auf die reagiert wird. In der Praxis dürfte es allerdings äußerst schwierig sein, einem Staat ein entsprechendes Fehlverhalten nachzuweisen. Deshalb wird darüber diskutiert, ob möglicherweise eine Beweislastumkehr in Form einer widerlegbaren Vermutung sinnvoll wäre.[92] Demnach müsste der Staat, von dessen Territorium eine Cyberattacke ausgeht, nachweisen, dass er bei der Absicherung und Überwachung seiner Infrastruktur bestimmte international anerkannte Standards eingehalten hat. Insgesamt birgt eine Beweislastumkehr aber die nicht zu unterschätzende Gefahr des Missbrauchs und der Eskalation, da »unbeteiligte« Drittstaaten schnell in sicherheitspolitische Auseinandersetzungen zwischen anderen Staaten hineingezogen werden können. Dies könnte auch Deutschland treffen, wenn zum Beispiel US-Behörden deutsche Server lahmlegen, die als Drehkreuze für russische oder chinesische Botnetz-Attacken identifiziert wurden.

88 Geiß/Lahmann, »Freedom and Security in Cyberspace« [wie Fn. 70], S. 656f.

89 Artikel 28ff der Artikelentwürfe zur Staatenverantwortlichkeit [wie Fn. 48].

90 Zum Recht auf Gegenmaßnahmen siehe oben, S. 16.

91 Dazu ausführlich Geiß/Lahmann, »Freedom and Security in Cyberspace« [wie Fn. 70], S. 632ff.

92 Vgl. Wolff Heintschel von Heinegg, »Cyberspace – Ein völkerrechtliches Niemandsland?«, in: Roman Schmidt-Radefeldt/Christine Meissler (Hg.), *Automatisierung und Digitalisierung des Krieges. Drohnenkrieg und Cyberwar als Herausforderungen für Ethik, Völkerrecht und Sicherheitspolitik*, Baden-Baden 2012, S. 159–174 (172); Eneken Tikk, »Ten Rules for Cyber Security«, in: *Survival*, 53 (2011) 3, S. 119–132 (122).

Völkerrechtspolitischer Ausblick: Spielräume für eine gezielte Normsetzung

Die Schaffung eines friedlichen, sicheren, resilienten und offenen Umfeldes zur Nutzung des Cyberspace setzt voraus, dass sich die Staaten zunächst einmal über ihre Rechtspositionen austauschen. In Bereichen, in denen ein gewisser Konsens besteht, müssen aus dem geltenden Völkerrecht politisch akzeptable und praktisch umsetzbare Verhaltensregeln und Standards für einen verantwortungsvollen Umgang mit Cybertechnologie entwickelt werden. Ein solches Vorgehen hätte auf jeden Fall erhebliche vertrauensbildende Wirkung. Inhaltlich geht es dabei zum einen um den Schutz kritischer Informationsinfrastrukturen und die Absicherung öffentlicher und privater IT-Systeme weltweit. Beispielsweise müsste noch genauer umrissen werden, welche Einrichtungen zur kritischen Infrastruktur zählen und welche Maßstäbe im Einzelfall für Schutzvorkehrungen anzulegen sind. Zum anderen müssen die Staaten in der Lage sein, bei der Abwehr und Aufklärung von Cyberattacken sowie bei der Verfolgung damit einhergehender Straftaten wirksam zusammenzuarbeiten. Dies erfordert bestimmte Überwachungsmechanismen, Frühwarnsysteme und Kontaktstellen für einen geregelten Informationsaustausch sowie spezielle Kanäle für eine Kommunikation in Krisenfällen.

Der Verhandlungsrahmen in den Vereinten Nationen

Im Rahmen der Vereinten Nationen lassen sich die Verhandlungsinitiativen zu Fragen der Cybersicherheit grob in drei Stränge untergliedern: einen politisch-militärisch orientierten Strang, bei dem es um die Wahrung von internationaler Stabilität und Sicherheit geht; einen eher ökonomisch ausgerichteten Strang, der sich auf den kriminellen Missbrauch von Informationstechnologien konzentriert;[93] und einen auf die Einhaltung der Menschenrechte bezogenen Strang, der vor allem die Problematik staatlicher Überwachungsmaßnahmen aufgreift.

Maßgebende Akteure und Foren zur Behandlung cyberrelevanter Stabilitäts- und Sicherheitsfragen sind der Erste Ausschuss der UN-Generalversammlung (zuständig für Abrüstung und internationale Sicherheit), die Internationale Fernmeldeunion (International Telecommunication Union, ITU), das UN-Institut für Abrüstungsforschung (UN Institute for Disarmament Research, UNIDIR) und eine spezielle Arbeitsgruppe der vom UN-Sicherheitsrat geschaffenen Counter-Terrorism Implementation Task Force (CTITF).

Mit Cyberkriminalität beschäftigen sich vor allem der UN-Wirtschafts- und Sozialrat, das UN-Büro für Drogen- und Verbrechensbekämpfung (UN Office on Drugs and Crime, UNODC) und ein interregionales UN-Institut für Kriminalitätsforschung und Rechtspflege (UN Interregional Crime and Justice Research Institute, UNICRI).

Der dritte Verhandlungsstrang geht auf eine Initiative Deutschlands und Brasiliens aus dem Jahr 2013 zurück und ist im Dritten Ausschuss der UN-Generalversammlung (zuständig für soziale, humanitäre und kulturelle Angelegenheiten) angebunden. Im Zusammenhang mit der NSA-Affäre haben beide Staaten gemeinsam einen Resolutionsentwurf eingebracht, der sich mit dem Recht auf Privatheit im digitalen Zeitalter befasst und im Dezember 2013 von der Generalversammlung verabschiedet wurde.[94] In der Resolution wird betont, dass das unrechtmäßige oder willkürliche Überwachen und Abfangen von Kommunikation und Sammeln persönlicher Daten das Recht auf Privatheit sowie das Recht auf freie Meinungsäußerung verletzt. Ohne bestimmte Staaten zu verurteilen, bezieht sich die Resolution in erster Linie auf grenzüberschreitende und massenhafte Überwachungsmaßnahmen. Allgemein wird bekräftigt, dass die Rechte, die den Menschen »offline« zustehen, auch »online« geschützt werden müssten. Daher werden die Staaten unter anderem aufgefordert, ihre Überwachungspraxis und die zugrundeliegende Gesetzgebung im Lichte der einschlägigen Menschen-

93 Dazu ausführlich Tim Maurer, *Cyber Norm Emergence at the United Nations – An Analysis of the Activities at the UN Regarding Cyber-security*, Cambridge, MA: Harvard Kennedy School, Belfer Center, September 2011, <http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf>.

94 UN General Assembly, *Resolution 68/157, The Right to Privacy in the Digital Age*, 18.12.2013, UN-Dok. A/RES/68/167, 21.1.2014.

rechtsverpflichtungen zu überprüfen und unabhängige nationale Aufsichtsmechanismen zu schaffen. Auf Veranlassung der Generalversammlung hat der UN-Hochkommissar für Menschenrechte im Juni 2014 einen ersten Bericht zu den rechtlichen Aspekten dieser Problematik vorgelegt.[95] Parallel zum Dritten Ausschuss der Generalversammlung setzt sich auch der UN-Menschenrechtsrat in regelmäßigen Abständen mit den menschenrechtsbezogenen Auswirkungen staatlicher Überwachungsmaßnahmen auseinander.[96]

Kontroversen im Sicherheitskontext

Im Jahr 1998 hat die UN-Generalversammlung im Ersten Ausschuss zum ersten Mal eine Resolution über »Entwicklungen auf dem Gebiet der Information und Telekommunikation im Kontext internationaler Sicherheit« beschlossen.[97] Seitdem wird jährlich eine Folgeresolution verabschiedet, auf deren Basis bereits mehrmals eine Gruppe von Regierungsexperten eingesetzt wurde (Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, GGE). Nachdem in der Gruppe lange Zeit über grundlegende Fragen gestritten worden war, konnte 2010 ein erster Konsensbericht präsentiert werden.[98] Der zweite Bericht wurde im Juni 2013 veröffentlicht.[99] Die aktuelle Gruppe, in der Deutschland erneut vertreten ist, soll das Völkerrecht darauf abklopfen, inwiefern es sich im Zusammenhang mit der Nutzung solcher Technologien anwenden lässt.[100]

95 *The Right to Privacy in the Digital Age*, Report of the Office of the United Nations High Commissioner for Human Rights, UN-Dok. A/HRC/27/37, 30.6.2014.
96 Vgl. insbesondere den Bericht des Sonderberichterstatters Frank La Rue: UN Human Rights Council, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue*, UN-Dok. A/HRC/23/40, 17.4.2013.
97 UN General Assembly, *Resolution 53/70, Developments in the Field of Information and Telecommunications in the Context of International Security*, 4.12.1998, UN-Dok. A/RES/53/70, 4.1.1999.
98 UN-Dok. A/65/201, 30.7.2010. Die Berichte der Expertengruppen und weitere Informationen finden sich auf der Website des UN Office for Disarmament Affairs (UNODA), <www.un.org/disarmament/topics/informationsecurity/>.
99 UN-Dok. A/68/98*, 24.6.2013.
100 UN General Assembly, *Resolution 68/243*, 27.12.2013, UN-Dok. A/RES/68/243, 9.1.2014, Absatz 4. Der nächste Bericht der Expertengruppe soll 2015 veröffentlicht werden.

Soweit es um Aspekte internationaler Stabilität und Sicherheit im Cyberkontext geht, sind Russland und die USA traditionell Kontrahenten. Im Kern verfolgt Russland das Ziel, das Prinzip der Nichteinmischung im Cyberspace durchzusetzen und neue völkerrechtliche Regeln für eine Rüstungskontrolle im Hinblick auf Cyberwaffen zu schaffen. Die USA bemühen sich um ein möglichst offenes und freies Internet und um internationale Kooperation, die nichtstaatliche Akteure einbezieht. Den russischen Rüstungskontrollbestrebungen stehen die USA generell ablehnend gegenüber.

Der russische Vorstoß

Im September 2011 hat die russische Regierung einen Entwurf für eine Konvention zu internationaler Informationssicherheit veröffentlicht.[101] Definiert werden Hauptbedrohungen, grundlegende Prinzipien für die Gewährleistung internationaler Informationssicherheit, Maßnahmen zur Vermeidung und Lösung militärischer Konflikte im Informationsraum und zur Unterbindung terroristischer und sonstiger illegaler Aktivitäten in diesem Raum sowie übergreifende Kooperationspflichten der Staaten. Das Papier wurde jedoch sowohl wegen handwerklicher Mängel (etwa mangelnde Begriffsklarheit und irreführende Doppelungen mit bestehenden völkerrechtlichen Instrumenten) als auch wegen zahlreicher inhaltlicher Punkte kritisiert.[102] Vor allem liegt dem Entwurf ein Verständnis staatszentrierter »Informationssicherheit« zugrunde. Es geht davon aus, dass Staaten das Recht haben, ihren eigenen »Informationsraum« ohne Einflussnahme von außen zu gestalten und diesen Raum gegen Informationen zu schützen, die destabilisierende Wirkung haben könnten. In diesem Sinne wird in dem Entwurf auch davon gesprochen, dass »aggressive Informationskriegführung« ein Verbrechen gegen den Weltfrieden und die internationale Sicherheit dar-

101 *Concept of a Convention on International Information Security*, veröffentlicht unter anderem auf der Webseite der russischen Botschaft im Vereinigten Königreich, <http://rusemb.org.uk/policycontact/52>.
102 Conflict Studies Research Centre/Institute of Information Security Issues, *Russia's »Draft Convention on International Information Security«. A Commentary*, Watlington/Moskau, April 2012, <www.conflictstudies.org.uk/files/20120426_CSRC_IISI_Commentary.pdf>. Vgl. auch die offizielle Kritik von Seiten der US-Regierung im Ersten Ausschuss der UN-Generalversammlung: U.S. Department of State, *Statement by Delegation of the United States of America*, New York, 2.11.2012, <www.state.gov/t/avc/rls/200050.htm>.

stelle und die Staaten daher ein Recht auf Selbstverteidigung gegen aggressive Akte im Informationsraum hätten.[103] Ein solcher Ansatz, der den Staaten einen weiten Spielraum für Zensur und repressive Maßnahmen eröffnen würde, ist mit einem demokratischen Verständnis von Cybersicherheit nicht vereinbar.

Parallel zu diesem Konventionsentwurf hat Russland im September 2011 zusammen mit China, Tadschikistan und Usbekistan in der UN-Generalversammlung einen Resolutionsentwurf eingebracht, der einen internationalen Verhaltenskodex für Informationssicherheit beinhaltet.[104] Darin wird unter anderem bekräftigt, alle Staaten hätten das Recht, die Verbreitung solcher Informationen einzuschränken, die zu Terrorismus, Sezessionismus oder Extremismus anstacheln oder die politische, wirtschaftliche und soziale Stabilität von Staaten sowie ihr geistiges und kulturelles Umfeld unterminieren.

Streitpunkt Rüstungskontrolle

Der russische Konventionsentwurf ebenso wie der in der UN-Generalversammlung gemeinsam mit China eingebrachte Resolutionsentwurf enthalten konkrete Vorschriften gegen die Proliferation sogenannter Informationswaffen und verwandter Technologien. Dieser Aspekt wirft zusätzliche Probleme auf, denn bei digitalen Informations- und Kommunikationstechnologien handelt es sich grundsätzlich um Dual-Use-Technologien, die sowohl zivile als auch militärische Verwendung finden. Unklar ist zum einen, wie ein darauf gerichtetes Proliferationsverbot definitorisch gefasst und wie seine Einhaltung verifiziert und durchgesetzt werden könnte.[105] Zum anderen haben die USA ein starkes Interesse daran, ihren Spielraum bei der Entwicklung von Cyberkapazitäten nicht durch Regeln einzuschränken. Aus amerikanischer Sicht spielt auch der kommerzielle Aspekt bei der Erforschung und Nutzung derartiger Technologien eine zentrale Rolle. Angesichts dieser Hürden und Differenzen dürfte es eher schwierig sein, die Mechanismen traditioneller Rüstungskontrolle auf Cybertechnologien zu übertragen.

Die humanitär-völkerrechtliche Dimension von Cyberoperationen

Werden Cyberoperationen in bewaffneten Konflikten durchgeführt oder lösen sie einen solchen Konflikt aus, kommt das humanitäre Völkerrecht zur Anwendung. Allerdings besteht auch in diesem Bereich großer Klärungsbedarf, wie einzelne Vorschriften ausgelegt werden sollen. Besonders heikel ist zum Beispiel die Frage, welche Einrichtungen der Cyberinfrastruktur im Konfliktfall als zivile Objekte vor Angriffen geschützt sind und welche Einrichtungen zu legitimen militärischen Zielen werden. Diese Fragen werden umfassend und detailreich im Tallinn-Handbuch erörtert.[106] In den allermeisten Punkten deckt sich der Inhalt des Handbuchs, das unter der Federführung des amerikanischen Völkerrechtsprofessors Michael N. Schmitt entstand, mit der Rechtsauffassung der USA.[107] Abzuwarten bleibt, wie sich andere Staaten zu dieser Vorlage positionieren werden. Vor allem von russischer und chinesischer Seite dürften abweichende Rechtsauffassungen zu erwarten sein. Die deutsche Bundesregierung hat zu den inhaltlichen Fragen bislang nicht öffentlich Stellung bezogen.[108] Einen wichtigen Beitrag zur Debatte über die Anwendbarkeit des humanitären Völkerrechts im Zusammenhang mit Cyberkriegführung leistet darüber hinaus vor allem das Internationale Komitee vom Roten Kreuz.

Die Strategie der USA

Ihre Vorreiterrolle bei der Identifizierung von Normen für den Cyberspace hat die amerikanische Regierung bereits 2011 in ihrer internationalen Cyberspace-Strategie deutlich unterstrichen. Darin wird bekundet, man werde mit gleichgesinnten Staaten daran arbeiten, nach Maßgabe des geltenden Völkerrechts Verhaltensregeln für den Cyberspace zu etablieren.

103 *Concept of a Convention on International Information Security* [wie Fn. 101], Article 5, Absatz 5ff, 19.
104 UN General Assembly, *International Code of Conduct for Information Security*, Annex to the Letter Dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General, UN-Dok. A/66/359, 14.9.2011.
105 Herbert S. Lin, »Arms Control in Cyberspace: Challenges and Opportunities«, in: *World Politics Review*, 6.3.2012, <www.worldpoliticsreview.com/articles/11683/arms-control-in-cyberspace-challenges-and-opportunities>.
106 Schmitt (Hg.), *Tallinn Manual* [wie Fn. 25], S. 73ff.
107 Vgl. Schmitt, »International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed« [wie Fn. 52].
108 Vgl. Deutscher Bundestag, Drucksache 17/13357, 29.4.2013.

Dafür müsse das Völkerrecht nicht neu erfunden werden. In dem Strategiepapier werden einige Aspekte deutlich hervorgehoben: die Freiheit der Meinungsäußerung und Vereinigung, den Schutz geistigen Eigentums, die Achtung der Privatsphäre, das Interesse an einer effektiven Verbrechensbekämpfung sowie das naturgegebene Recht der Staaten auf Selbstverteidigung gegen bestimmte aggressive Akte im Cyberspace. Überdies werden einige Verantwortungsbereiche als besonders relevant für die Herausbildung weiterer Normen identifiziert. So sollten die Staaten darauf hinarbeiten, globale Interoperabilität, Netzwerkstabilität, einen verlässlichen Zugang zum Internet und anderen vernetzten Technologien sowie die Einhaltung von Due-Diligence-Standards zum Schutz von Informationsinfrastrukturen zu gewährleisten. Insgesamt müssten nicht nur Staaten, sondern alle relevanten Akteure an diesen Prozessen teilhaben (Multi-Stakeholder-Ansatz).[109]

Was die eigene nationale Sicherheit betrifft, liegt ein Schwerpunkt der aktuellen Cybervölkerrechtspolitik der Obama-Administration darauf, der internationalen Staatengemeinschaft zu vermitteln, wie die USA das geltende *ius ad bellum* und *ius in bello* im Falle von Cyberangriffen und Cyberkonflikten anwenden. Vor allen Dingen lassen die USA keinen Zweifel daran, dass sie notfalls konventionelle militärische Mittel einsetzen werden, um sich gegen Cyberattacken zu verteidigen. In ihrer Cyberspace-Strategie von 2011 stellt die Obama-Regierung zudem klar, dass die USA für sich das Recht in Anspruch nehmen, gegebenenfalls auch Alliierten und Partnern militärisch gegen Cyberangriffe beizustehen, zumal solche Attacken Auswirkungen haben könnten, die weit über die Grenzen des angegriffenen Staates hinausgehen. In dem betreffenden Strategiepapier wird das Selbstverteidigungsrecht unter der Überschrift Abschreckung (deterrence) thematisiert.[110] Medienberichten zufolge hat Präsident Obama im Oktober 2012 eine geheime Direktive unterzeichnet, die dem Militär und Sicherheitsdiensten größere Handlungsspielräume bei der Bekämpfung von Cyberattacken verleiht. Danach sollen auch Cyberoperationen gegen ausländische Server und Netze zum Zwecke einer aktiven Verteidigung zulässig sein.[111]

In einer Grundsatzrede von 2012 zur Rolle des Völkerrechts im Cyberspace hat der damalige Rechtsberater des US-Außenministeriums, Harold Koh, erläutert, wie wichtig es für die USA ist, die eigene Rechtsauffassung zu diesen Fragen auf internationaler Ebene zu kommunizieren. Ziel müsse es sein, so viele Staaten wie möglich davon zu überzeugen, dass das Verhalten im Cyberspace bereits bestimmten Regeln unterliege. Umso effektiver könne man sich dagegen wehren, dass andere Staaten Regeln zu etablieren versuchten, die US-Interessen zuwiderliefen.[112] Für die USA geht es somit auch um Interpretationshoheit, nämlich um die Autorität, darüber zu befinden, wie das geltende Völkerrecht im Kontext sich abzeichnender Cyberkonflikte auszulegen ist. Gelänge es, die internationale Staatengemeinschaft zu überzeugen, dass sich die USA bei ihren Aktivitäten im Cyberspace an bestimmte Regeln hielten, könne dies laut Koh größere Handlungsspielräume eröffnen. Es ermögliche den USA, mit höherer Legitimität im Cyberspace aktiv zu werden, um nationale Interessen besser verfolgen zu können. Daher sei die Einhaltung des Völkerrechts im Cyberspace ein wichtiger Bestandteil des »Smart-Power«-Ansatzes in der US-Außenpolitik.[113]

»Verkehrsregeln« für den Cyberspace

Anders als im US-Strategiepapier wird in der britischen Cybersicherheitsstrategie die militärische Dimension von Cybersicherheit nahezu vollständig ausgeblendet. Soweit es um normative Fragen geht, setzt sich die britische Regierung ebenso wie die deutsche Bundesregierung in erster Linie für eine internationale Debatte über mögliche »Verkehrsregeln« im Cyberspace ein.[114] Im Rahmen regelmäßig

109 The White House, *International Strategy for Cyberspace* [wie Fn. 28], S. 9f, <www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>.
110 Ebd., S. 13f.
111 Ellen Nakashima, »Obama Signs Secret Directive to Help Thwart Cyberattacks«, in: *The Washington Post*, 14.11.2012, <www.washingtonpost.com/world/national-security/obama-signs-secret-cybersecurity-directive-allowing-more-aggressive-military-role/2012/11/14/7bf51512-2cde-11e2-9ac2-1c61452669c3_story.html>.
112 Vgl. U.S. Department of State, *International Law in Cyberspace*, Remarks by Harold Hongju Koh, USCYBERCOM Inter-Agency Legal Conference, 18.9.2012, <www.state.gov/s/l/releases/remarks/197924.htm>; mit Fußnoten veröffentlicht in: *Harvard International Law Journal Online*, 54 (2012), S. 1–12 (10ff), <www.harvardilj.org/wp-content/uploads/2012/12/Koh-Speech-to-Publish1.pdf>.
113 Ebd., S. 10.
114 Cabinet Office, *The UK Cyber Security Strategy. Protecting and Promoting the UK in a Digital World*, London, November 2011, <www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf>,

stattfindender internationaler Konferenzen versuchen die Staaten seitdem, diese Fragen wissenschaftlich aufzuarbeiten.[115] Vor allem bezüglich Art und Umfang staatlicher Due-Diligence-Pflichten besteht nach wie vor erheblicher Klärungsbedarf. Daher läge es nahe, dass sich die Regierungs-Expertengruppe der Vereinten Nationen in den kommenden Monaten schwerpunktmäßig mit dieser Thematik befasst. Das wäre aus praktischer Sicht weitaus sinnvoller als eine Konzentration auf die in der Völkerrechtswissenschaft bereits umfassend geführte, eher theoretisch relevante Debatte über die Anwendbarkeit des Gewaltverbots und des Selbstverteidigungsrechts. Denkbar ist aber auch, dass humanitär-völkerrechtliche Aspekte der Cyberkriegführung stärker in den Vordergrund rücken.[116] In jedem Fall sollten keine allzu hohen Erwartungen an das Ergebnis der Beratungen gestellt werden, da in der Gruppe zum Teil sehr konträre Regierungsstandpunkte aufeinanderprallen und Schlussfolgerungen nur veröffentlicht werden, soweit sie von einem Konsens aller beteiligten Vertreter getragen sind. Aus diesen Gründen werden andere multilaterale und bilaterale Foren immer mehr an Bedeutung gewinnen, wenn es darum geht, die Möglichkeiten für weitere vertrauensbildende Maßnahmen und die Etablierung normativer Standards auszuloten. Wichtig ist dabei auch, die menschenrechtliche Dimension enger mit der sicherheitspolitischen Dimension zu verknüpfen und auf der Suche nach gemeinsamen Spielregeln für die Nutzung von Cybertechnologie den Schutz der Privatsphäre nicht aus den Augen zu verlieren. Gerade in den transatlantischen Beziehungen ist dringend ein intensiver Austausch darüber erforderlich, wie sich legitime Sicherheitsbedürfnisse bei der Informationsgewinnung im Cyberspace besser mit menschenrechtlichen Garantien in Einklang bringen lassen.

Ein Forum, in dem das Spannungsverhältnis zwischen Sicherheit und Freiheit im Cyberspace zumindest auf grundsätzlicher Ebene erörtert werden könnte, ist die sogenannte Freedom Online Coalition (FOC), die 2011 von 14 Staaten (darunter Ghana, Kanada, Mexiko, Mongolei, Schweden und die USA) in Den Haag gegründet wurde.[117] Die Koalition, der mittlerweile auch Deutschland und zahlreiche weitere Staaten angehören, hat sich der Wahrung der Menschenrechte und Grundfreiheiten im Internet verschrieben. Sie arbeitet darauf hin, Beschränkungen der Meinungs- und Informationsfreiheit entgegenzuwirken und den Schutz der Privatheit im Internet zu verbessern. Vor allem hat sich die Koalition zum Ziel gesetzt, Menschen, die in einem repressiven Umfeld leben, bei der Ausübung ihrer Freiheitsrechte durch das Internet zu unterstützen. Ein weiteres Thema auf der Agenda ist die menschenrechtliche Verantwortung von Unternehmen im Online-Kontext. Obgleich es sich bei der Koalition um einen Zusammenschluss von Regierungen handelt, verfolgt die Initiative einen Multi-Stakeholder-Ansatz, der alle wichtigen Akteure mit einbezieht. Auch in anderen Bereichen, die den Umgang von Staaten mit Cybertechnologie betreffen, bieten solche informellen Initiativen eine Chance, gemeinsame Positionen zu erarbeiten und Normbildungsprozesse unterhalb der Schwelle völkerrechtlicher Verträge anzustoßen.

Das Bemühen um einen international akzeptierten Verhaltenskodex – gewissermaßen als Leitbild einer »globalen Kultur von Cybersicherheit«[118] – verspricht mehr Erfolg als jeder Versuch, einen vertraglichen Normsetzungsprozess in Gang zu bringen.[119] Die Aushandlung eines völkerrechtlichen Abkommens würde viele Jahre in Anspruch nehmen und wäre mit erheb-

S. 26; Cabinet Office, *The National Cyber Security Strategy. Our Forward Plans*, London, Dezember 2013, <www.gov.uk/government/uploads/system/uploads/attachment_data/file/265386/The_National_Cyber_Security_Strategy_Our_Forward_Plans_December_2013.pdf>, S. 9.

115 Beispielsweise hat das Auswärtige Amt in Zusammenarbeit mit der Universität Potsdam im Juni 2013 eine Konferenz unter dem Titel »Securing the Freedom and Stability of Cyberspace: The Role and Relevance of International Law« veranstaltet (International Berlin Cyber Conference III, 27. und 28.6.2013). Deren Hauptaugenmerk richtete sich darauf, die Due-Diligence-Pflichten von Staaten im Cyberkontext zu untersuchen.

116 Vgl. Detlev Wolter, *»The UN Takes a Big Step Forward on Cybersecurity«*, in: *Arms Control Today*, September 2013, <www.armscontrol.org/act/2013_09/The-UN-Takes-a-Big-Step-Forward-on-Cybersecurity>.

117 *Freedom Online Coalition, Joint Action for Free Expression on the Internet* (»The Hague Declaration«), Den Haag, 9.12.2011. Aktuelle Informationen unter <www.freedomonline.ee/about-us/Freedom-online-coalition>. Derzeit gehören der Koalition 23 Staaten an.

118 Vgl. unter anderem UN General Assembly, *Resolution 57/239, Creation of a Global Culture of Cybersecurity*, 20.12.2002, UN-Dok. A/RES/57/239, 31.1.2003.

119 Brigid Grauman, *Cyber-security: The Vexed Question of Global Rules. An Independent Report on Cyber-preparedness around the World*, Brüssel: Security & Defence Agenda, Februar 2012, <www.securitydefenceagenda.org/Contentnavigation/Library/Libraryoverview/tabid/1299/articleType/ArticleView/articleId/3063/SDA-report-Cybersecurity-The-vexed-question-of-global-rules.aspx>.

lichen politischen Unwägbarkeiten verbunden. Ein derart langwieriges Vorhaben hätte aller Voraussicht nach bestenfalls einen Minimalkonsens zum Ergebnis und dürfte mit der rasanten technologischen Entwicklung ohnehin kaum Schritt halten. Unabhängig davon wird sich das Völkergewohnheitsrecht im Umgang mit dem Cyberspace graduell weiterentwickeln. Voraussetzung für die Herausbildung neuen Völkergewohnheitsrechts ist, dass möglichst viele Staaten ihr Handeln an einer bestimmten Norm ausrichten und davon überzeugt sind, dass dies völkerrechtlich geboten ist. Welchen Weg das Völkerrecht im digitalen Zeitalter künftig einschlägt, wird entscheidend davon abhängen, inwieweit sich die Staaten überhaupt auf die angestoßenen Debatten einlassen und ihre Rechtsüberzeugungen äußern.

Abkürzungsverzeichnis

CCDCOE	Cooperative Cyber Defence Centre of Excellence
CTITF	Counter-Terrorism Implementation Task Force
EMRK	Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten
ENISA	European Union Agency for Network and Information Security (Europäische Agentur für Netz- und Informationssicherheit)
FOC	Freedom Online Coalition
GCHQ	Government Communications Headquarters
GGE	Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security
ICJ	International Court of Justice
ITU	International Telecommunication Union
NSA	National Security Agency (USA)
UNICRI	UN Interregional Crime and Justice Research Institute
UNIDIR	UN Institute for Disarmament Research
UNODA	UN Office for Disarmament Affairs
UNODC	UN Office on Drugs and Crime

Lektüreempfehlungen

Annegret Bendiek
Umstrittene Partnerschaft. Cybersicherheit, Internet Governance und Datenschutz in der transatlantischen Zusammenarbeit
SWP-Studie 26/2013, Dezember 2013

Annegret Bendiek
Kritische Infrastrukturen, Cybersicherheit, Datenschutz. Die EU schlägt Pflöcke für digitale Standortpolitik ein
SWP-Aktuell 35/2013, Juni 2013