Transnationale Verantwortung und Normemergenz im Cyberraum

Sebastian Harnisch und Kerstin Zettl

Zusammenfassung Steigende Konfliktpotenziale im digitalen Raum erfordern die Schärfung transnationaler Verantwortung, sie erschweren diese aber auch. Aus völkerrechtlicher Perspektive wurde die Norm der Sorgfaltsverantwortung für den Cyberraum bereits umfänglich diskutiert. Wir knüpfen aus politikwissenschaftlicher Perspektive an diese Debatte an, indem wir die Bedingungen für eine Normemergenz zunächst theoretisch diskutieren und sodann die Staatenpraxis im engeren (vier kurze Fallstudien) und im weiteren Sinne (auf der Grundlage eines neuen Heidelberger Konfliktdatensatzes) untersuchen. Unsere Befunde zeigen, dass es zwar Ansätze für eine retrospektive Norm der Sorgfaltsverantwortung gibt, aber bislang kaum prospektive Normwirkung erkennbar ist. Die Staatenpraxis zentraler staatlicher „Normunternehmer" verdeutlicht die bislang fehlende intersubjektive Anerkennung der Norm. Zudem legt der Abgleich mit systematisch erhobenen Cyber-Konfliktdaten der Jahre 2014–2016 nahe, dass insbesondere autoritäre Staaten wie Russland und China die regulative Wirkung der Norm durch den Einsatz von nicht-staatlichen Akteuren unterminieren. Insgesamt kann die noch im Frühstadium befindliche Normemergenz vor allem auf unterschiedliche Motivationen und Schwerpunktsetzungen der Normunternehmer in ihrem Agieren zurückgeführt werden.

S. Harnisch (✉)
Universität Heidelberg, Institut für Politische Wissenschaft, Heidelberg, Deutschland
E-Mail: Sebastian.harnisch@ipw.uni-heidelberg.de

K. Zettl
Institute of Political Science, Heidelberg University, Heidelberg, Deutschland

A. Seibert-Fohr (Hrsg.), *Entgrenzte Verantwortung*,
https://doi.org/10.1007/978-3-662-60564-6_11

1 Einleitung

Normen als geteilte Standards angemessenen Verhaltens in einer Gemeinschaft etablieren Akteursidentitäten. Normen werden durch Akteursverhalten aber auch (re-) produziert. Ganz gleich ob man die aus Normen entstehende Verantwortung als legitim oder legal ansieht, Normen regeln die Beziehungen zwischen Akteuren gleichen oder unterschiedlichen Status in einer (Rechts-)Gemeinschaft. Normen schaffen somit Verantwortung. Wie ist nun die Emergenz und Beschaffenheit von Verantwortung in neuen Politikfeldern wie jenem der Cybersicherheit zu erklären? Wer bestimmt über die Anpassung rivalisierender Normen und Verantwortlichkeiten? Wann wirkt sich die Schaffung neuer Verantwortung stabilisierend auf eine politische Gemeinschaft oder eine Rechtsgemeinschaft aus, wann nicht?

Verantwortung wird in den Sozialwissenschaften ganz allgemein als „das Einstehen eines Akteurs für die Folgen seiner Handlungen in Relation zu einer geltenden Norm“ verstanden.[1] Im Kontrast zum klassischen Pflichtbegriff umfasst Verantwortung in der Politikwissenschaft neben der Einhaltung der Norm auch die Berücksichtigung der Folgen der Normanwendung. In der politikwissenschaftlichen Teildisziplin der Internationalen Beziehungen wird Verantwortung daher nicht nur als erwartungsgesteuerte Zuständigkeit für die Normdurchsetzung selbst (prospektive Verantwortlichkeit), sondern auch als Zurechnungsfähigkeit der beabsichtigten und unbeabsichtigten Folgen der Normhandlung konzeptualisiert (retrospektive Verantwortung).[2]

Manche Verantwortung kann dabei einfach, schnell und präzise zugewiesen werden. Dies gilt beispielsweise, wenn spezifizierte Normen verantwortliche Akteure eindeutig identifizieren, dem Kontext angemessene Verhaltensvorschriften beinhalten und die Handlungsfolgen sich ganz überwiegend auf diese Normhandlung zurückverfolgen lassen. Andere Formen von Verantwortung, und dazu gehören jene im Cyberraum, können nicht oder noch nicht so eindeutig bestimmt werden. Verantwortung ist gleichsam an Normen im Frühstadium ihrer Entstehung gebunden oder wird mit anderen Gebotsformen (mehr oder minder stark) verknüpft, z. B. allgemeinen Handlungsprinzipien, Regeln oder nationalen Gesetzen.[3]

Verantwortung, zumal rechtliche Verantwortung, kann auch (bewusst) diffus auf mehreren Ebenen eines korporativen Akteurs verteilt sein oder werden. Sie kann zwischen privaten und öffentlichen Akteuren geteilt oder sie kann nur von oder innerhalb einer bestimmten Gruppe (z. B. Großmächten) erwartet werden.[4] Erschwerend kommt im Politikfeld Cybersicherheit hinzu, dass die technische und somit auch rechtliche und politische Zurechenbarkeit von Handlungen aufgrund

[1] Heidbrink, Definitionen und Voraussetzungen der Verantwortung, in: Heidbrink u. a. (Hrsg.), Handbuch Verantwortung, 2016, S. 5.

[2] Erskine, Making Sense of Responsibility in International Relations, in: Erskine (Hrsg.), Can Institutions Have Responsibilities?, 2003, S. 8.

[3] Finnemore, Cybersecurity and the Concept of Norms, 2017, S. 2.

[4] Bukanovsky u. a., Special Responsibilities: Global Problems and American Power, 2012.

komplexer Kausalketten erschwert werden kann oder sie durch die Verwendung autonom agierender Systeme grundsätzlich (und bewusst) in Frage gestellt wird.[5]

Cybersicherheit wird deshalb auch oft eine Sonderstellung unter den im Rahmen dieses Bandes behandelten Politik- und Rechtsgebieten zugesprochen. Der Umfang, die Schnelligkeit und die Verschwiegenheit über die Veränderungen im Akteursverhalten, die Beteiligung von nicht-staatlichen Akteuren an der Etablierung des Raumes sowie dessen Beschaffenheit (durch kommerzielle Dienste und elektronischen Code) dafür verantwortlich, dass keine hinreichende Attribution von Handlungen vorgenommen werden könne, welche eine Verantwortungszuweisung und rechtliche Sanktionierung erst ermögliche.[6]

Mit Finnemore und Hollis[7] geben wir zu bedenken, dass diese Einwände zwar weiter diskutiert werden sollten, die Wirkungen dieser Entwicklungen (Volumenaufwuchs, temporäre Volatilität und Handlungsintransparenz) jedoch keineswegs eindeutig, gleichgerichtet und distinkt im Vergleich zu anderen Politikfeldern sind oder dass Staaten ihren territorialen Regelungsanspruch für den Cyberraum vollständig aufgegeben hätten.[8] Vielmehr übertragen Regierungen bewusst staatliche Funktionen an nicht staatliche Akteure (z. B. Hackergruppen), üben diese mit ihnen gemeinschaftlich aus (z. B. mit Unternehmen aus der Cybersicherheitsbranche) oder dulden aktiv nicht staatliches Handeln, sodass die Frage nach transnationaler Verantwortung auch diese Akteure erfassen muss.[9]

Wir betonen daher in diesem Kapitel den emergenten Charakter von transnationaler Verantwortung im Cyberraum. In einem ersten Abschnitt diskutieren wir zunächst politikwissenschaftliche Erklärungen für die transnationale Norm- und Verantwortungsgenese und präsentieren dann empirische Evidenz dafür, dass Staaten (aber auch zunehmend nicht-staatliche Akteure) Verhalten zeigen, welches kongruent mit unterschiedlichen Formen einer Sorgfaltsverantwortung im Cyberraum ist. Im zweiten Abschnitt erörtern wir transnationale Verantwortung als sozialen Mechanismus, der jenseits von machtpolitischer Ungleichheit und formalrechtlicher Gleichheit die Entwicklung einer internationalen sozialen Ordnung mit unterschiedlichen Verantwortlichkeitsniveaus erklären kann. Abschn. 3 beschreibt sodann

[5] Erskine u. a., Beyond ‚Quasi-Norms', in: Osula u. a. (Hrsg.), International Cyber Norms: Legal, Policy & Industry Perspectives, 2016; Rauer, Distribuierte Handlungsträgerschaft, in: Daase u. a. (Hrsg.), Politik und Verantwortung: Analysen zum Wandel politischer Entscheidungs- und Rechtfertigungspraktiken, PVS-Sonderheft 52/2017, 2017, S. 436.

[6] Ney u. a., Cyber-Security beyond the Military Perspective, German Yearbook of International Law, Vol. 49, 2015, S. 51; Schaller, Internationale Sicherheit und Völkerrecht im Cyberspace: Für klarere Regeln und mehr Verantwortung, 2014, S. 5.

[7] Finnemore u. a., Constructing Norms for Global Cybersecurity, The American Journal of International Law, Vol. 110, Issue 3, 2016, S. 425 (456–562).

[8] Vgl. auch De Nardis, The Global War for Internet Governance, 2014; Kello, The Virtual Weapon and International Order, 2017.

[9] Vgl. Eichensehr, Public-Private Cybersecurity, Texas Law Review, Vol. 95, 2017, S. 467; Maurer, Cyber Mercenaries: The State, Hackers, and Power, 2018; Tsagourias, Non-State Actors, Ungoverned Spaces and International Responsibility for Cyber Acts, Journal of Conflict and Security Law, Vol. 21, Issue 3, 2016, S. 455.

konkret die Genese des Prinzips der Sorgfaltsverantwortung und seiner Anbindung an bestehende internationale und nationale Normen und Prinzipien, auch wenn die entsprechende Normentwicklung bislang sehr begrenzt geblieben ist. In Abschn. 4 präsentieren wir deskriptive statistische Befunde und Episoden staatlicher Zurückhaltung im Cyberraum, die plausibilisieren können, inwiefern und warum es zur Ausbildung einer transnationalen Sorgfaltsverantwortung kommen kann und wie diese derzeit konkret ausgestaltet ist. Wir argumentieren, dass das Konfliktverhalten und Konfliktniveau im Cyberraum bislang eine deutliche Zurückhaltung von staatlichen Akteuren bezüglich schwerwiegender Angriffe auf Kritische Infrastrukturen erkennen lässt. Dies zeugt von einer emergierenden Norm für den Cyberraum, die folgenschwere Angriffe auf Kraftwerke, Wasserversorgung etc. mit kinetischen Angriffen rechtlich gleichsetzt und entsprechende rechtliche Regeln der Offline-Welt (UN-Charta Art. 51) über den Waffeneinsatz (use-of-force) anwendet.

Gleichzeitig engagieren sich insbesondere autokratische Staaten vermehrt mit Hilfe nicht-staatlicher Hackergruppierungen bei der Destabilisierung demokratischer Staaten und unterwandern so die regulative Wirkung der noch in der Genese befindlichen Sorgfaltsverantwortungsnorm. Der fünfte Abschnitt schließlich fasst die Ergebnisse zusammen und liefert einen kurzen Ausblick, ob diese Entwicklung ungebrochen fortgeführt werden wird.

2 Normen und transnationale Verantwortung in den Internationalen Beziehungen

Normen und die mit ihnen verbundenen Identitäten sowie transnationale Verantwortung sind konzeptionell eng miteinander verwoben. Obwohl sie in der Sozialwissenschaft lange unabhängig voneinander behandelt wurden, werden sie hier in ihrer Wechselwirkung betrachtet. Normen verweisen als „kollektive Verhaltensstandards auf der Grundlage einer gegebenen Identität“[10] unmittelbar auf eine Identifikation mit einer bestimmten Gruppe von Akteuren und den in der Gruppe geltenden Werthaltungen hin. Die entsprechende Forschung hat gezeigt, dass die Kommunalität einer Norm, d. h. die Größe der gebundenen Gruppe, in einem Spannungsverhältnis zur Spezifizität der Norm, d.h. der Präzision des ver- und/oder gebotenen Verhaltens, steht.[11] Im Falle der Sorgfaltsverantwortung stellt sich daher zunächst die Frage, welche Gruppe von Staaten sich als gebunden erklärt hat und ob diese Bindung nur von staatlichen und nur für staatliche Akteure, beispielsweise im Rahmen der UN oder einer Regionalorganisation wie der Shanghai Cooperation Organization, anerkannt wird.

[10] Katzenstein (Hrsg.), The Culture of National Security: Norms and Identity in World Politics, 1996, S. 5.

[11] Legro, Which Norms Matter? Revisiting the „Failure“ of Internationalism, International Organization, Vol. 51, Issue 1, 1997, S. 31.

Der Begriff der Verhaltensstandards einer Norm nimmt Bezug auf deren regulative und konstitutive Wirkung. Regulativ wirken Normen, indem sie Verhalten vorschreiben, verbieten oder erlauben. Konstitutiv wirken Normen, indem sie Rechte zuweisen und dadurch Autorität und sogar Akteursschaft etablieren.[12] Der Begriff des Verhaltensstandards weist also daraufhin, dass unterschiedliche Erwartungshaltungen aus einer Norm erwachsen können. Regeln sind sehr spezifische *ex ante* Erwartungen über ein bestimmtes Verhalten in einer eng umgrenzten Situation, während Standards zumeist *ex post* Einschätzungen über das erwartete Verhalten bezeichnen.[13]

Normen entfalten ihre Wirkung als kollektive Verhaltensstandards durch die intersubjektive Anerkennung der Gruppenmitglieder. Normen genießen daher kontrafaktische Gültigkeit, d. h. ein Bruch führt nicht zu ihrer unmittelbaren Eliminierung. Aber das Ausmaß und die Art ihrer Umstrittenheit (Contestation) kann trotzdem ihre Gültigkeit erheblich beeinträchtigen. So entsteht ein Horizont an möglichen Verhaltensdispositionen eines Individuums in einer Gruppe, welcher sich zwischen individueller Nonkonformität einerseits und vollständiger, kollektiver Konformität aller Gruppenmitglieder andererseits aufspannt (vgl. Abb. 1 unten).

Die bisherige Normenforschung zeigt nun einerseits, dass bestimmte Staaten (bzw. Regimetypen) zu „*unaufrichtiger Konformität*“ neigen,[14] d. h. diese erkennen eine Norm zwar an, missachten aber die Erwartungen an regelgerechtes Verhalten. Solche Staaten trachten danach, die konstitutive Wirkung der Norm (als verlässliches Mitglied der Staatengemeinschaft zu gelten) von der regulativen Wirkung (normkonformes Verhalten zu zeigen) zu trennen. Die Forschung zeigt weiterhin, dass erst wenn sich diese Staaten „argumentativ selbstverstricken“, d. h. die Lücke zwischen Anspruch und Wirklichkeit offen zu Tage tritt, die Möglichkeit einer

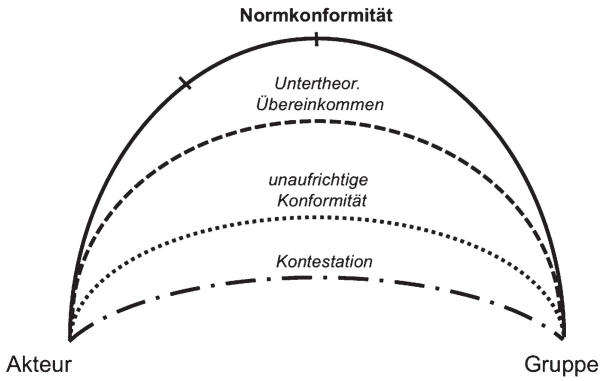

Abb. 1 Spektrum von Normkonformität und Nonkonformität. (Quelle: eigene Erstellung)

[12] Jepperson u. a., Norms, Identity and Culture in National Security, in: Katzenstein (Hrsg.), The Culture of National Security: Norms and Identity in World Politics, 1996, S. 33 (54).

[13] Finnemore u. a., Constructing Norms for Global Cybersecurity, The American Journal of International Law, Vol. 110, Issue 3, 2016, S. 425 (441).

[14] Simmons, Mobilizing for Human Rights, 2009.

nachholenden Konformitätsanpassung besteht, denn in diesem Fall droht die Reputation des Akteurs – die konstitutive Wirkung der Normanerkennung – verloren zu gehen.[15]

Darüber hinaus weist die politikwissenschaftliche Normenforschung darauf-hin, dass Staaten sich aus ganz unterschiedlichen Motiven normkonform verhalten können. Cass Sunstein hat dafür den Begriff des „untertheoretisierten Übereinkommens“[16] (incompletely-theorized agreement) geprägt. Ein Beispiel mag dies verdeutlichen: Während Softwarehersteller die Norm, schadhaften Code offenzulegen und Sicherheitslücken zu füllen (disclosure/patching), aus kommerziellen Gründen schützen, und dabei von Experten unterstützt werden, die solche Lücken gezielt suchen und dann ihr Wissen darüber verkaufen, erwarten staatliche Institutionen deren Offenlegung und Beseitigung, um Schaden vom jeweiligen Gemeinwesen abzuwenden. Regierungen können solche Sicherheitslücken aber auch temporär geheim halten, um sie später als „Waffen“ (sog. Zero-Day-Exploits) in einem Cyberkonflikt einzusetzen.[17]

Verantwortung bezeichnet in diesem Zusammenhang nun jene soziale Praxis, wonach ein Akteur für eine Handlung gemessen an einer Norm rechenschaftspflichtig ist. Konkret bedeutet dies, dass er/sie aufgefordert sein kann, die Folgen seiner Handlung im Vorhinein zu erwägen und dann entsprechend zu handeln, um normkonform zu handeln (Prospektive Verantwortung). Oder derjenige kann nachträglich für eine getätigte oder unterlassene Erwägung der Handlungsfolgen zur Rechenschaft gezogen werden (Retrospektive Verantwortung). Erstere Konstellation wird in der Politikwissenschaft als weiter, letztere als enger Verantwortungsbegriff betrachtet.

Entscheidend für das Zusammenwirken von Norm und Verantwortung sind daher zwei Dimensionen: Zum einen steht in Frage, ob der Akteur überhaupt die Folgen seiner Handlungen vor deren Einsetzen erkennen konnte. Diese Verantwortungsfähigkeit kann entweder durch Akteurscharakteristika (Alter, Bildungsstand, andere Einschränkungen) oder die (technische) Unvorhersehbarkeit der Folgen einer Handlung beeinträchtigt werden. Zum anderen kann der Ausgangspunkt der Verantwortungszuweisung variieren. So kann ein Akteur zwar kausal, nicht aber rechtlich verantwortlich für eine Folge sein. Oder eine Akteurin ist moralisch für die Folgen ihrer Handlung verantwortlich, aber nicht kausal. Beide Dimensionen sind daher für eine (transnationale) Verantwortungsbestimmung essenziell (vgl. Abb. 2 unten stehend).

Für die empirische Bestimmung der kausalen und konstitutiven Wirkung der transnationalen Verantwortung sind daher die (rechtlichen) Normen, an welche die jeweilige Verantwortung angebunden ist, besonders bedeutsam. Denn zum einen

[15] Risse, Konstruktivismus, Rationalismus und Theorien Internationaler Beziehungen, in: Hellmann u. a. (Hrsg.), Die neuen Internationalen Beziehungen: Forschungsstand und Perspektiven in Deutschland, 2003, S. 99 (115).

[16] Sunstein, Incompletely Theorized Agreements in Constitutional Law, University of Chicago Public Law & Legal Theory Working Paper No. 147, 2007.

[17] Finnemore u. a., Constructing Norms for Global Cybersecurity, The American Journal of International Law, Vol. 110, Issue 3, 2016, S. 425 (444).

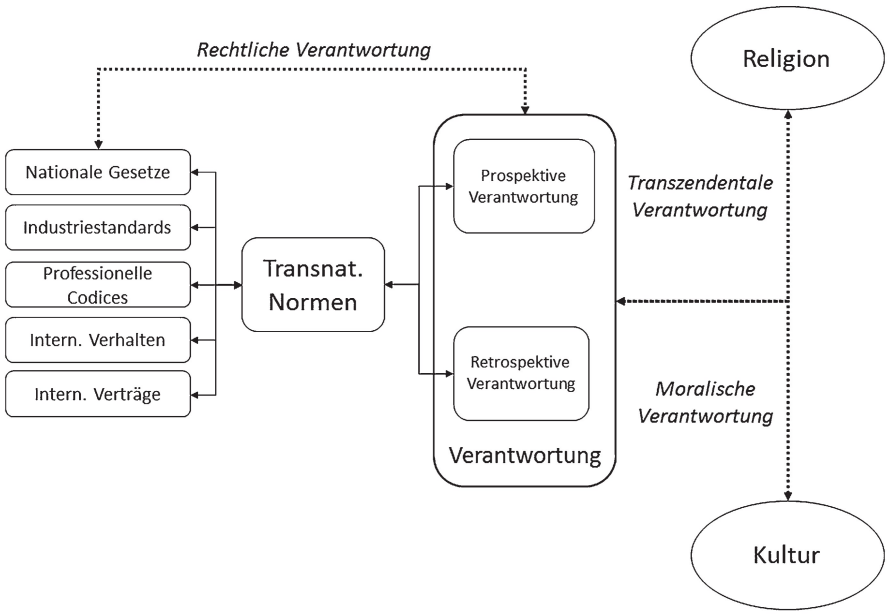

Abb. 2 Zusammenwirken und Situierung von Normen und Verantwortung. (Quelle: eigene Erstellung)

entscheidet die Art und Stärke der Bindung mit darüber, ob die jeweilige Norm das jeweilige Verhalten stabilisiert und/oder Akteure reifiziert, d. h. diese erneut mit Handlungsautorität zum legitimen Handeln in einer Gruppe ausstattet. Zum anderen ist für die Genese politischer und rechtlicher Verantwortlichkeit wichtig, inwiefern der staatliche (oder auch nicht-staatliche) Akteur unmittelbar selbst oder nur mittelbar durch das Zusammenwirken mit anderen (staatlichen) Akteuren Verantwortung durch eine Norm (oder andere Verhaltensregeln) zugesprochen bekommt.[18]

3 Normemergenz und transnationale Verantwortung im Cyberraum

Verbindliches Recht und (politische) Normen sind soziale Konstruktionen, deren Befolgung auf die intersubjektive Anerkennung durch Akteure angewiesen ist. Während verbindliches Recht aber auf dessen Setzung und Durchsetzung durch legitime Autorität beruht, entstehen durch politische Normen dezentrale und emergente soziale Ordnungen.[19] In ihrer Entstehungsphase können politische Normen

[18] D'Aspremont u. a., State Responsibility between Non-State Actors and States in International Law: Introduction, Netherland International Law Review, Vol. 62, 2015, S. 49.

[19] Osula u. a., Introduction, in: Osula u. a., (Hrsg.), International Cyber Norms: Legal, Policy & Industry Perspectives, NATO CCD COE Publications, Tallinn, 2016, S. 11.

zwar durch sog. Normunternehmer propagiert werden. Ihr Aufstieg und Fall geht aber primär auf dezentrale Praktiken der Sanktionierung – von der Bloßstellung nonkonformen Verhaltens bis zum Gruppenausschluss – durch diverse Gruppenmitglieder zurück.[20] Die Stärke einer Norm und der daran angebundenen Verantwortung lassen sich also an den wiederkehrenden normkonformen Handlungspraktiken oder den Rechtfertigungen und Verschleierungen nonkonformen Verhaltens abschätzen. Insbesondere das Gewährenlassen eines Normbruchs durch (nicht-)staatliche Akteure kann dazu dienen, den Anschein von Normkonformität und damit der konstitutiven Wirkung der Norm zu wahren, während die Konsequenzen der regulativen Wirkung, die Kosten der Verhaltensbeschränkung, umgangen werden.

3.1 Normemergenz im wissenschaftlichen und gesellschaftlichen Diskurs

Analysiert man nun die Genese und Ausprägung von Normen, die transnationale Verantwortung im Cyberraum konstituieren können, ergibt sich folgendes Bild: Ein Teil transnationaler Cyber-Verantwortung wird in der Forschungsliteratur auf bestehende völkerrechtliche Verträge und Gewohnheitsrecht zurückgeführt, die mittels Analogieschluss nun auch im Cyberraum angewendet werden.[21] Dies gilt zuvorderst für das humanitäre Völkerrecht, das die Begrenzung der Anwendung von Gewalt (use of force) regelt. Zwar verbleiben die meisten Cyberkonflikte unterhalb der Gewaltschwelle (s. u. Abschn. 4), aber die Analogie zum humanitären Völkerrecht hat trotzdem in Wissenschaft und Politik deutlich mehr Aufmerksamkeit erfahren als andere Rechtsgebiete.[22]

Unterscheidet man mit der Forschungsliteratur grob nach retrospektiver und prospektiver Verantwortlichkeit im Cyberraum, so ist retrospektive Verantwortung für staatliche, in Teilen aber auch nicht-staatliche Akteure, vergleichsweise eindeutig und umfassend geregelt.[23] Sie wird im Allgemeinen aus den Artikelentwürfen der UN-Völkerrechtskommission zur Staatenverantwortlichkeit von 2001 (ASR) abgeleitet.[24] Danach sind Staaten für „international schädigende Handlungen“ gegen-

[20] Frost, Ethics in International Relations: A Constitutive Theory, 1. Auflage, 1996.

[21] Liu, State Responsibility and Cyberattacks: Defining Due Diligence Obligations, Indonesian Journal of International & Comparative Law, Vol. 4, 2017, S. 191; Marauhn, Customary Rules of International Environmental Law, in: Ziolkowski (Hrsg.), Peacetime Regime for State Activities in Cyberspace – International Law, Foreign Affairs and Cyber-Diplomacy, 2013, S. 465.

[22] Shackelford u. a., Unpacking International Law on Cybersecurity Due Diligence, Chicago Journal of International Law, Vol. 17, Issue 1, 2016, S. 1 (3).

[23] Antonopoulos, State Responsibility in Cyberspace, in: Tsagourias u. a., (Hrsg.), Research Handbook on International Law and Cyberspace, 2015, S. 55; Schmitt u. a., The Nature of International Law Cyber Norms, Tallinn Paper No. 5, Special Expanded Issue, 2014.

[24] ILC, Responsibility of States for Internationally Wrongful Acts, Yearbook of the International Law Commission, Vol. II, Part Two, 2001, S. 26.

über Geschädigten verantwortlich, wenn sie diesen gegenüber bestehende Verpflichtungen verletzt haben. Solche schädigenden Akte können Handlungen oder Unterlassungen sein. Sie müssen dem Staat zurechenbar sein und dessen völkerrechtliche Verpflichtungen verletzen (Art. 2). Ist dies der Fall, so muss der Staat die schädigende Handlung unterlassen oder eine unterlassene Handlung aufnehmen und für den entstandenen Schaden Wiedergutmachung leisten.

In eng umgrenztem Umfang können Staaten auch für die Handlungen nichtstaatlicher Akteure auf ihrem Territorium verantwortlich gemacht werden. Dies gilt dann, wenn nicht staatliche Akteure in Ausübung staatlicher Aufgaben handeln, unter direkter staatlicher Kontrolle stehen oder eine nachträgliche staatliche Anerkennung vorliegt.[25] Sofern die schädigende Handlung nicht eingestellt wird, darf der Geschädigte sogar „Gegenmaßnahmen" in begrenztem Umfang ergreifen. Diese Gegenmaßnahmen dürfen aber nur auf Normeinhaltung durch den Schädigenden zielen (Verhaltensänderung) und nicht auf dessen Bestrafung. Da staatliche oder nicht-staatliche Cyberoperationen zahlreiche und unterschiedliche internationale Normen verletzen können, muss neben der Normsetzung vor allem auch die Staatenpraxis zeigen, welche Operationen legitimer Weise welche Gegenmaßnahmen nach sich ziehen dürfen.[26]

Eine prospektive Verantwortungsnorm ist für den Cyberraum bislang nicht etabliert worden.[27] Vielmehr finden sich im wissenschaftlichen Diskurs[28] und der Staatenpraxis lediglich vermehrt Hinweise auf eine im Entstehen begriffene „Sorgfaltsverantwortung im Cyberraum".[29] Noch, so unser Befund, ist die Norm im zwi-

[25] Seibert-Fohr, Die völkerrechtliche Verantwortung des Staats für das Handeln von Privaten: Bedarf nach Neuorientierung?, in: Zeitschrift für ausländisches öffentliches Recht und Völkerrecht, Bd. 73, 2013, S. 38 (42).

[26] Vgl. z. B. Jensen u. a., A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer? Texas Law Review, Vol. 95, 2017, S. 1555.

[27] Vgl. für eine Sachstandsbeschreibung der Due-Diligence-Norm in unterschiedlichen Bereichen des Völkerrechts: ILA Study Group Due Diligence 2014, 2016, sowie für den Cyberraum: Schmitt (Hrsg.), Tallinn Manual 2.0 on the international law applicable to cyber operations, 2017.

[28] Vgl. für die wissenschaftliche Debatte: Bendiek, Sorgfaltsverantwortung im Cyberraum: Leitlinien für eine deutsche Cyber-Außen- und Sicherheitspolitik, 2016; Bannelier-Christakis, Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?, in: Mälksoo u. a., Baltic Yearbook of International Law, Vol. 14, 2014, S. 23; Gross, Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-Incidents, Cornell International Law Journal, Vol. 48, 2015, S. 481; Jensen u. a., A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer? Texas Law Review, Vol. 95, 2017, S. 1555; Liu, State Responsibility and Cyberattacks: Defining Due Diligence Obligations, Indonesian Journal of International & Comparative Law, Vol. 4, 2017, S. 191; Ney u. a., Cyber-Security beyond the Military Perspective, German Yearbook of International Law, Vol. 49, 2015, S. 51; Schmitt, In Defense of Due Diligence in Cyberspace, Yale Law Journal Forum, Vol. 125, 2015, S. 68; Schmitt, Tallinn Manual 2.0 on the international law applicable to cyber operations, 2017; Shackelford u. a., Toward a Global Cybersecurity Standard of Care? Texas International Law Journal, Vol. 50, 2015, S. 303; Shackelford u. a., Unpacking International Law on Cybersecurity Due Diligence, Chicago Journal of International Law, Vol. 17, Issue 1, 2016, S. 1.

[29] Bendiek, Sorgfaltsverantwortung im Cyberraum: Leitlinien für eine deutsche Cyber-Außen- und Sicherheitspolitik, 2016.

schenstaatlichen Völkerrechtsdiskurs und in der Staatenpraxis nicht weiträumig in die Phase der „Normkaskadierung“ oder gar der „Norminternalisierung“ eingetreten.

Die Sorgfaltsverantwortung verpflichtet die Staaten im Cyberraum (in Friedenszeiten) dafür Sorge zu tragen, dass von ihrem Territorium keine Handlungen ausgehen, welche die Rechte anderer Staaten verletzen, bspw. durch Individuen, kriminelle Netzwerke, Hackergruppen oder organisierte Aufstandsgruppen.[30] Rechtstheoretisch geht die Genese der Norm auf die Trennung zwischen staatlichem und privatem Handeln zurück. Diese begründet den Schutz des Individuums gegen staatliche Bevormundung einerseits und die beschränkte Zurechenbarkeit privater Handlungen im völkerrechtlichen Verkehr andererseits.[31] Die zunehmende Verschränkung staatlicher und nicht-staatlicher Handlungen im Cyberraum bewirkt nun, z. B. durch private Bereitstellung öffentlicher Infrastruktur und die Teilung oder Übertragung staatlicher Funktionen an private Akteure, dass sich die Grenze beschränkter Zurechenbarkeit im Völkergewohnheitsrecht, u. a. durch die Staatenpraxis und Spruchpraxis internationaler Gerichte, immer weiter verschiebt.[32]

Im engeren Sinne enthält die Sorgfaltsverantwortungsnorm erstens die *Verpflichtung (obligation) zu warnen*. Diese Verpflichtung geht auf die Entscheidung des IGH (1949) „Corfu Channel“ (U.K. vs. Albania) zurück, in der der Gerichtshof eine Verantwortung Albaniens anerkannte, die britische Marine vorab über Seeminen in ihren Territorialgewässern informieren zu müssen, die zwei britische Kriegsschiffe versenkt hatten. Zweitens entschied ein Schiedsgericht in „Trail Smelter“ (U.S. vs. Canada) 1941, dass Staaten eine *Verantwortung haben, „Schaden zu vermeiden“ (Do-No-Harm)*. Die Entscheidung betraf die grenzüberschreitenden Abgase eines US-amerikanischen Hüttenwerks, die erhebliche Umweltschäden auf kanadischem Territorium hervorriefen. Schließlich entschied der IGH in „Nicaragua“ (Nicaragua vs. U.S.) 1986, dass Staaten eine *Verpflichtung zur Nicht-Intervention* haben, d. h. sie dürfen nicht in die inneren Angelegenheiten eines anderen Staates i. S. „der Wahl eines politischen, wirtschaftlichen, sozialen oder kulturellen Systems sowie der Formulierung der Außenpolitik“[33] eingreifen.

[30] Schmitt, In Defense of Due Diligence in Cyberspace, Yale Law Journal Forum, Vol. 125, 2015, S. 68 (68).

[31] Seibert-Fohr, Die völkerrechtliche Verantwortung des Staats für das Handeln von Privaten: Bedarf nach Neuorientierung?, in: Zeitschrift für ausländisches öffentliches Recht und Völkerrecht, Bd. 73, 2013, S. 38 (40).

[32] Eichensehr, Public-Private Cybersecurity, Texas Law Review, Vol. 95, 2017, S. 467, ILA Study Group, ILA Study Group on Due Diligence, Second Report, 2016, S. 2.

[33] International Court of Justice, Military and Paramilitary Activities in and against Nicaragua (Nicaragua vs. United States of America), ICJ Reports 1986, S. 27.

3.2 Normemergenz im zwischenstaatlichen Diskurs

In der zwischenstaatlichen Völkerrechtsdebatte ist die Sorgfaltsverantwortung eingehend diskutiert worden, u. a. auch deshalb, weil die Staatengemeinschaft wiederholt die Relevanz von Cyberangriffen für die internationale Sicherheit und den Weltfrieden anerkannt hat.[34] Ein tragfähiger Konsens konnte jedoch in den zentralen Foren der Vereinten Nationen, der Expertengruppe der Regierungen zu Cybersicherheit (UN GGE) sowie der Völkerrechtskommission (ILC), bislang nicht erzielt werden. Im Gegenteil: Die bislang letzte Expertengruppe unter deutschem Vorsitz (2016/2017) beendete ihre Arbeit ohne Abschlussbericht. Berichten zufolge konnten die beteiligten Staaten keine Einigung über die weitere Festschreibung rechtlicher Standards, insbesondere im Bereich des Humanitären Völkerrechts und des Rechts auf Selbstverteidigung, erzielen.[35]

Die Vereinten Nationen haben seit 2005 sechs UN-Gruppen von Regierungsexperten zur Informationssicherheit (UN GGE) einberufen. Für die Genese der Sorgfaltsverantwortung sind insbesondere die Diskussionen und der Bericht von 2015 einschlägig. Nach langen und kontroversen Debatten über die Bedeutung staatlicher Souveränität und deren Einschränkung durch entsprechende Pflichten konnte sich die UN-GGE 2015 lediglich darauf verständigen, dass die Sorgfaltsverantwortung eine rechtlich unverbindliche Norm darstelle.[36] Diese umschließe:

> „Staaten sollten nicht bewusst erlauben, dass ihr Territorium für völkerrechtswidrige Handlungen durch Informations- und Kommunikationstechnologien genutzt wird. Insoweit akzeptieren Staaten die Notwendigkeit, das Prinzip der Sorgfaltsverantwortung im Cyberraum zu respektieren, wenngleich es unbestimmt bleibt, ob dies eine rechtliche Verpflichtung ist oder nicht."[37]

Staaten werden zudem von der Expertengruppe ermuntert, miteinander zu kooperieren, um zu verhindern, dass schadhafte Informations- und Kommunikationsaktivitäten von ihrem Territorium gegenüber anderen Territorien ausgehen.[38]

Die von der International Law Association (ILA) eingesetzte Expertengruppe zur Cybersicherheit weist darüber hinaus darauf hin, dass eine solche Sorgfaltsverantwortung auch aus der Gründungscharta der Internationalen Telekommunikationsunion (ITU) abgeleitet werden könne. Diese sehe für ihre Mitglieder die Verantwortung vor, für die Aufrechterhaltung, den Schutz, sowie die unterbrechungsfreie Nutzung aller ICT-Verbindungen und Anlagen Sorge zu tragen. Besondere Geltung

---

[34] Ziolkowski, General Principles of International Law as Applicable in Cyberspace, in: Ziolkowski (Hrsg.), Peacetime Regime for State Activities in Cyberspace – International Law, Foreign Affairs and Cyber-Diplomacy, 2013, S. 135 (168, Fn. 241) m. w. N.

[35] Korzak, UN GEE on Cybersecurity: The End of an Era? – What the apparent GGE failure means for international norms and confidence-building measures in cyberspace, The Diplomat, 2017.

[36] Vgl. Kaljurand, United Nations Group of Governmental Experts: The Estonian Perspective, in: Osula u. a. (Hrsg.), International Cyber Norms: Legal, Policy & Industry Perspectives, 2016, S. 111 (121).

[37] Eigene Übersetzung von UN GGE, UN Doc. A/70/174, 2015, § 13(c).

[38] Ebda., § 17(e).

hätte diese Verantwortung in jenen Bereichen, wo sie den Erhalt des Lebens zu Lande, zu Wasser, in der Luft, im Weltraum sowie der epidemiologischen Kommunikation der Weltgesundheitsorganisation (WHO) betrifft. Zudem schreibe die ITU-Charta vor, die schadhafte Unterbrechung der Rundfunkübertragung zu verhindern.[39]

Eine Sonderstellung unter den internationalen Expertenberichten nimmt das sog. Tallinn-Manual ein, dessen zweiter Bericht „Tallinn 2.0“[40] sich explizit mit der Sorgfaltsverantwortung auseinandersetzt. Mit Unterstützung der niederländischen Regierung wurde auf Einladung vom „NATO Cooperative Cyber Defence Centre of Excellence“ (NATO CCD COE) unter der Leitung von Michael Schmitt eine internationale Expertengruppe zusammengerufen. Diese Gruppe hat es sich zur Aufgabe gemacht, bestehende internationale Rechtsnormen auf ihre Anwendbarkeit im Cyberraum hin zu überprüfen.[41] Es lässt sich gleichwohl argumentieren, dass schon die Feststellung bestimmter Regeln (Rules) und die dazugehörige völkerrechtliche Diskussion den Rahmen der Anwendung und Interpretation überschreiten und auf eine Neubewertung und Neuetablierung von Normen zusteuern.[42]

Das Tallinn Manual 2.0 diskutiert insbesondere zwei Normen bzgl. der Sorgfaltsverantwortung. Als „General Principle“ der Due-Diligence-Norm wird als „Rule 6“ statuiert:

> „A State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences.“

Übereinstimmend stellt die Expertengruppe fest, dass diese Norm noch nicht rechtlich verbindlich sei. Sie könne aber doch als politisch verbindlich aus der Souveränitätsnorm sowie dem Völkergewohnheitsrecht abgeleitet werden. In dieser Interpretation fordert die Norm keine aktiven präventiven Maßnahmen, sondern einen angemessenen Standard an Wachsamkeit sowie an Gegenmaßnahmen, die vernünftigerweise von dem Staat verlangt werden können.[43] Dies schließt insbesondere auch sog. Transitstaaten ein.[44] In dieser Interpretation schließt die Norm das Verhalten nicht-staatlicher Akteure auf dem Territorium des Staates oder einem Territorium unter seiner Kontrolle (Okkupationsgebiete, Botschaften etc.) ein.

Deutlich kontroverser wurde in der Tallinn-Gruppe diskutiert, welcher Art die „unrechtmäßigen Handlungen“ sein müssen, um von der Norm erfasst zu werden.

---

[39] Fidler u. a., ILA Study Group Report on Cybersecurity, Terrorism and International Law, 2016, S. 63.

[40] Schmitt, Tallinn Manual 2.0 on the international law applicable to cyber operations, 2017.

[41] Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare, 2013, S. 1; Schmitt, Tallinn Manual 2.0 on the international law applicable to cyber operations, 2017, S. 1.

[42] Mačák, From Cyber Norms to Cyber Rules: Re-engaging States as Lawmakers, Leiden Journal of International Law, Vol. 30, Issue 4, 2017, S. 877.

[43] Schmitt, Tallinn Manual 2.0 on the international law applicable to cyber operations, 2017, S. 41–42.

[44] Vgl. Reinisch u. a., Mitigating Risks, German Yearbook of International Law, Vol. 54, 2015, S. 101.

So sind Handlungen, die auf eine Blockade oder Entstellung von Webseiten abstellen, nur dann oberhalb der Erheblichkeitsschwelle (serious adverse consequences) anzusiedeln, wenn Kritische Infrastrukturen (inkl. Banken und Medien) oder kritische Regierungsdienste (Steuern, Wahlen, Notfallversorgung) betroffen sind.[45] Die bloße Verbreitung von Regierungsgeheimnissen oder Falschinformationen durch Hackergruppen unter Duldung von Regierungsstellen fällt demnach nicht unter die Due-Diligence-Norm.[46]

Die zweite Norm, Rule 7 des Tallinn Manual 2.0, fordert weitergehende Verantwortung für „angemessene Maßnahmen" des Staates, um die unrechtmäßigen Handlungen zu unterbinden.

> „The principle of due diligence requires a State to take all measures that are feasible in the circumstances to put an end to cyber operations that affect a right of, and produce serious adverse consequences for, other states."[47]

Deutlich umstrittener als Rule 6, wirft dieser Regelvorschlag die Frage auf, wann genau der Staat Maßnahmen ergreifen muss, um seiner Verantwortung gerecht zu werden: Wenn zukünftig eine Handlung erwartbar erscheint (präventiv), wenn eine Handlung unmittelbar bevorsteht (präemptiv) oder wenn die Handlung bereits begonnen hat?[48] Die Gruppe war sich einig, dass „konstruktives Wissen" Grundlage der Sorgfaltsverantwortung ist und deshalb allenfalls eine Pflicht zu präemptiven Handeln abgeleitet werden könne. Es folgt, dass die Gruppe weder eine generelle Pflicht zur kontinuierlichen Überwachung (Monitoring), noch zur innerstaatlichen rechtlichen Verankerung der Sorgfaltsverantwortung, noch zur zwischenstaatlichen Kooperation in der Unterbindung als Teil der Norm anerkennt.[49]

3.3 Normemergenz, Sorgfaltsverantwortung und Staatenpraxis

Im folgenden Abschnitt diskutieren wir kurz vier Episoden staatlicher Praxis im Hinblick auf die Norm der Sorgfaltsverantwortung. Die Auswahl der Akteure, USA, Russland, Deutschland & EU und der Volksrepublik China, wurde auf folgender Grundlage getroffen: Die Staaten/Akteure sollten über starke Cyberkapazitäten und -verwundbarkeiten verfügen, unterschiedlichen Regimetypen und Rechtssystemen angehören und in der Vergangenheit durch eigene Initiativen substanziellen Einfluss auf die Normbildung im Bereich der Cybersicherheit genommen haben.

---

[45] Schmitt, Tallinn Manual 2.0 on the international law applicable to cyber operations, 2017, S. 38.

[46] Schmitt, Tallinn Manual 2.0 on the international law applicable to cyber operations, 2017, S. 37.

[47] Ebda. S. 43.

[48] Ebda. S. 44.

[49] Ebda. S. 48.

Die USA

Die Vereinigten Staaten haben auf nationaler und internationaler Ebene erhebliche Anstrengungen unternommen, um eine (zunächst rechtlich unverbindliche) Norm der Sorgfaltsverantwortung zu etablieren. Diese Bemühungen sind jedoch zumindest partiell von den Auseinandersetzungen um die Überwachungspraktiken der National Security Agency (NSA) konterkariert worden, die u. a. von dem Whistleblower Edward Snowden seit 2013 aufgedeckt wurden (s. u.).

Die Obama-Administration hat erstmals in der International Strategy for the Cyberspace[50] gefordert, dass „Staaten ihre Verantwortung anerkennen und entsprechend handeln sollten, sodass ihre Informationsinfrastruktur geschützt wird und ihre nationalen Systeme vor Schaden und Missbrauch gesichert würden".[51] Ausdrücklich spricht die Strategie davon, verantwortungsbewusstes Verhalten im Cyberraum auf internationaler Ebene zu fördern. Dies soll u. a. durch den Aufbau eines globalen Netzes von Computer-Emergency-Response-Teams (CERT) geschehen, und indem auf nationaler Ebene eingefordert wird, dass nicht staatliche Akteure (u. a. Universitäten und Unternehmen) ihrer Verantwortung nachkommen, ihre Netzwerke zu pflegen und zu sichern.[52]

Die US-Regierung hat gezielt mehrere bi- und multilaterale Foren genutzt, um nationale Cyberstrategien im Rahmen der Organisation für Amerikanische Staaten (OAS) und der Afrikanischen Union (AU) auf die Sorgfaltsverantwortung zu verpflichten und in Kapazitätsbildungsprogrammen mit subsaharischen Staaten Afrikas, den gemeinsamen Einsatz von Computer Security Incident Response Teams (CSIRT) zu üben. Zudem konnten die USA ein gemeinsames Kommuniqué der G-20 (inklusive Chinas) erwirken, in dem die generelle Anwendbarkeit des Völkerrechts auf den Cyberraum anerkannt wird.[53]

US-Außenminister John Kerry betonte in seiner Rede über Freiheit und Sicherheit im Internet im Jahr 2015 insbesondere die Bedeutung der Verantwortung der Staaten für die Stabilität des Cyberraumes:

> „As I've mentioned, the basic rules of international law apply in cyberspace. Acts of aggression are not permissible. And countries that are hurt by an attack have a right to respond in ways that are appropriate, proportional, and that minimize harm to innocent parties. We also support a set of additional principles that, if observed, can contribute substantially to conflict prevention and stability in time of peace. We view these as universal concepts that should be appealing to all responsible states, and they are already gaining traction."[54]

Neben zahlreichen bilateralen Cyber-Dialogen hat sich die US-Regierung auch in Gesprächen mit der VR China für vertrauensbildende Maßnahmen und die Begrenzung von Cyberespionage-Angriffen eingesetzt. Besonders interessant ist daran, dass die US-Exekutive sich dabei immer privater Internet-Firmen bediente, um

[50] White House, International Strategy for Cyberspace, 2011.

[51] Ebda, S. 10.

[52] Ebda, S. 7–11.

[53] DOS, Department of State International Cyberspace Policy Strategy, 2016.

[54] Kerry, Text of John Kerry's Remarks in Seoul on Open and Secure Internet, 2015.

staatliche Funktionen zu übernehmen. Zunächst assistierten öffentliche Stellen offensichtlich der Cybersicherheitsfirma „Mandiant“, als diese im Februar 2013 ein weitverzweigtes Netz von kommerziellen Cyberespionage-Aktivitäten auf die Einheit 61398 der Volksbefreiungsarmee in Shanghai zurückverfolgte (auch als Advanced Persistent Threat 1: APT1 bekannt). In der Abfolge einigten sich dann die US-amerikanische und chinesische Regierung im September 2015 darauf, dass „keine der beiden Regierungen Versuche unternehmen oder wissentlich unterstützen werde, cyber-gestützten Diebstahl von intellektuellem Eigentum, inklusive Handelsgeheimnissen oder vertraulichen Unternehmensinformationen, mit der Intention einen Wettbewerbsvorteil für Wirtschaftsunternehmen oder Wirtschaftssektoren zu erwirken“.[55] Beide Parteien verständigten sich außerdem darauf, einen hochrangigen Cyber-Dialog einzurichten, um weitere drängende Probleme zu adressieren. Im Nachgang erklärten sich dann wiederum zahlreiche US-Cybersicherheitsfirmen bereit, die Einhaltung des Moratoriums durch chinesische Stellen zu überwachen.[56]

Auf nationaler Ebene hat die Obama-Administration die Kritische Infrastruktur zum „strategic national asset“ erklärt und damit Angriffe auf diese als „militärische Angriffe“ auf die USA selbst gewertet. In der Nationalen Sicherheitsstrategie von 2017 wird diese Position von der Trump-Administration gestärkt.[57] Durch exekutive Anordnung hat die Obama-Administration auch das „National Institute of Standards and Technology“ (NIST) angewiesen, ein Rahmenprogramm zu entwickeln, das für den Privatsektor nationale best-practice Vorsorgeregeln zum Schutz ihrer ICT-Netzwerke etabliert.[58] Zudem wurden im NCCIC Cyber Incident Scoring System Notfälle der höchsten Dringlichkeitsstufe als „an imminent threat to the provision of wide-scale critical infrastructure services, national government stability, or the lives of U.S. persons“[59] charakterisiert.

In der Zusammenschau der Maßnahmen zeigt sich, dass die US-Regierung unter Barack Obama als Normunternehmer für die Norm der Sorgfaltsverantwortung in zahlreichen bi- und multilateralen Foren agierte. Die US-Staatenpraxis zeigt dabei ein distinktes Muster: Während die Norm als allgemeines völkerrechtliches Prinzip unterhalb der rechtlichen Verbindlichkeit propagiert wurde, setzte sich die Regierung bei der Schutzverantwortung für kommerzielle Interessen für deutlich weitergehende Regelungen ein. Sie nutzte dabei offensiv die bereits bestehenden Verflechtungen zur US-Cybersicherheitsindustrie, um die Involvierung staatlicher Stellen in Fragen der Attribution und des Monitorings von normwidrigem Verhalten zu vermeiden.

[55] White House, Office of the Press Secretary, FACT SHEET: President Xi Jinpings State Visit to the United States, 2015.

[56] Eichensehr, Public-Private Cybersecurity, Texas Law Review, Vol. 95, 2017, S. 467 (490–492).

[57] White House, National Security Strategy of the United States, 2017, S. 13.

[58] NIST, Framework for Improving Critical Infrastructure Cybersecurity, 2014.

[59] NCCIC, US-CERT Federal Incident Notification Guidelines, 2016.

Die Volksrepublik China

Die chinesische Regierung hat spätestens seit 1998, insbesondere aber seit dem Amtsantritt von Staats- und Parteichef Xi Jinping (2013), den Versuch unternommen, die Volksrepublik China zu einer vollwertigen „Cybermacht" zu entwickeln. Austin[60] identifiziert dabei drei distinkte Entwicklungsphasen: Die Entwicklung grundlegender Prinzipien zur Informationssicherheit (1998–2005), die Normgenese für militärische Cyberkonflikte (2006–2013) sowie den materiellen Ausbau zur Cyber(super)macht (seit 2014). Neben diesem zeitlichen Entwicklungsmuster heben vor allem US-amerikanische Autoren die enge Verknüpfung zwischen Regierungsstellen und diversen nicht-staatlichen Akteuren, d. h. halbstaatlichen Unternehmen, Universitäten und Hackergruppen, hervor, welche Chinas Verhaltensprofil bezüglich der Sorgfaltsverantwortung prägen könnte.[61]

Die Besonderheiten der chinesischen Cyberpolitik enden hier nicht. Im Vergleich zu den USA sprechen manche Autoren gar von einen „Kampf zweier Cyber-Zivilisationen".[62] Richtig ist, dass die chinesische Regierung mehrheitlich den Begriff der Informationssicherheit (oder auch Netzwerksicherheit) verwendet und damit der Informationsgehalt bzw. die Informationsdurchlässigkeit zum Gegenstand der Sicherheitspolitik erhoben wird.[63] Darüber hinaus vertritt die chinesische Regierung konsequent die Vorstellung eines souveränen „nationalen Cyberraumes", dessen Abgrenzung gegenüber äußeren Einflüssen und Kontrollierbarkeit nach innen mit Verve und erheblichem technischen und personellen Aufwand betrieben wird.[64] Bemerkenswert ist ferner, dass nach Jahren der primär kommerziellen Betrachtung des Cyberraumes, Peking seit dem Bekanntwerden des Stuxnet-Angriffs (2010) die militärische Dimension des Internets sehr viel stärker betont, eine Reihe strategischer Dokumente verfasst, eigene Institutionen geschaffen und internationale Vereinbarungen getroffen hat, welche dem weitgesteckten chinesischen nationalen Sicherheitsbedürfnis entsprechen.[65]

Seit dem Jahr 2000 hat die Volksrepublik die Etablierung einer auf „gemeinsamer Sicherheit" beruhenden Cyberordnung gefordert. Dieser Ordnungsentwurf zielt auf die Beschränkung militärischer Cyberinstrumente, die Zurückdrängung von Informationskriminalität und Terrorismus sowie die gleichzeitige Unterstützung der Entwicklungs- und Schwellenländer beim Aufbau einer Kritischen Informations-

[60] Austin, International Legal Norms in Cyberspace: Evolution of China's National Security Motivations, in: Osula u. a., (Hrsg.), International Cyber Norms: Legal, Policy & Industry Perspectives, 2016, S. 171.

[61] Williams, The ‚China, Inc.+' Challenge to Cyberspace Norms, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 1803, 2018.

[62] Hoffman, A Clash of Cyber Civilisations, ChinaFile, 2018.

[63] Cai, Cybersecurity in Chinese Context: Changing Concepts, Vital Interests and Cooperative Willingness, 9th Berlin Conference on Asian Security (BCAS), 14–16. Juni 2015.

[64] Yuen, Becoming a Cyber Power: China's Cybersecurity Upgrade and its Consequences, China Perspectives, Vol. 2, 2015, S. 53.

[65] Jong-Chen, China's Evolving Cybersecurity and Cyber Development Strategy, The International Bureau of Asian Research, 2017.

infrastruktur. In zahlreichen bi- und plurilateralen Foren, darunter der UN-Generalversammlung, der ICANN, dem APEC-Telekommunikationsministertref fen, dem World Summit on the Information Society, der ASEAN-China Strategic Partnership for Peace and Prosperity und der UN Group of Governmental Experts (UN GGE), setzte sich der chinesische Vertreter jeweils für die Anwendung des Völkerrechts einschließlich der UN-Charta im Cyberraum ein.[66]

Ein besonderer Schwerpunkt lag dabei auf der Kooperation mit Russland und den Staaten Zentralasiens. 2007 unterzeichneten die Staats- und Regierungschefs der Mitgliedstaaten der Shanghaier Organisation für Zusammenarbeit (SOZ oder SCO) einen Aktionsplan zur Informationssicherheit. Dieser wurde 2009 in einen Vertrag umgewandelt, der u. a. in Art. 3 zur Kooperation bei der gemeinsamen Bekämpfung von Cyberbedrohungen aufruft und die gemeinsame Propagierung internationaler Normen fordert. Diese Maßnahmen sollen fünf zentrale Bedrohungen minimieren, wie sie im Annex 2 des Vertrages beschrieben sind: 1) die Entwicklung und den Einsatz von Informationswaffen sowie die Vorbereitung und Durchführung eines Informationskrieges; 2) Informationsterrorismus; 3) Informationskriminalität; 4) den Gebrauch einer dominanten Stellung im Informationsraum zur Schädigung der Interessen und Sicherheit anderer Staaten; und 5) die Verbreitung von Informationen, welche die sozio-politische, sozio-ökonomische, spirituelle, moralische und kulturelle Umwelt anderer Staaten negativ beeinflusst.[67]

2011 unterstützte China sodann den Vorstoß Russlands zur Etablierung eines „International Code of Conduct for Information Security“ im UN-Rahmen (siehe unten). Dieser wurde der UN-Generalversammlung in veränderter Form 2015 erneut vorgelegt. Er stellt für China insofern ein Novum dar, als dass er proaktiv für eine internationale Normierung wirbt und in §§ 2, 7 u. 8 auch Pflichten für die Volksrepublik selbst und ihre Verbündeten schafft. Danach müssen die Rechte von Individuen in der Offline-Welt auch in der Online-Welt geschützt werden (§§ 2, 7), alle Staaten müssen die gleiche Rolle spielen sowie die gleiche Verantwortung bei der internationalen Governance des Internets, seiner Sicherheit, Kontinuität und Stabilität tragen. Zudem sei die Entwicklung des Internets so voranzutreiben, dass ein multilateraler, transparenter und demokratischer Governance-Mechanismus geschaffen wird, der die gleichmäßige Verteilung von Ressourcen, den Zugang für alle und die stabile und sichere Funktionsfähigkeit des Internets gewährleistet (§§ 2, 8).[68]

Diese globale Normbildung wurde 2015 durch ein bilaterales Cyber-Kooperationsabkommen mit Russland flankiert. Die Vereinbarung ist einerseits bemerkenswert, weil sie nicht nur eine gegenseitige Verpflichtung zum Schutz vor Cyberattacken beinhaltet, sondern gleichzeitig auch ein gegenseitiges Versprechen statuiert, nicht widerrechtlich in die Informationsressourcen und Netzwerke des

[66] Segal, Chinese Cyber Diplomacy in a New Era of Uncertainty, Hoover Working Group on National security, Technology, and Law, Aegis Paper Series No. 1703, 2017.

[67] SCO, Agreement between the Governments of the Member States of the Shanghai Cooperation Organization in the Field of International Information Security, 2009.

[68] UN General Assembly, UN Doc. A/69/723, 2015.

Vertragspartners einzudringen.[69] Andererseits setzt sie in Breite und Tiefe einen deutlich verbindlicheren Verhaltensstandard als jenen im UN GGE Endbericht von 2015, der parallel mit chinesischer Zustimmung verabschiedet wurde. Der UN GGE Bericht von 2015 schrieb freiwillige und nicht-bindende Normen in folgenden Bereichen fest:

- Staaten sollten die Kritische Infrastruktur anderer Staaten nicht mit dem Ziel angreifen, diese zu beschädigen.
- Staaten sollten nicht auf die Cybernotfallreaktionssysteme anderer Staaten zielen.
- Staaten sollten bei der Untersuchung von Cyberattacken und Cyberkriminalität, die von ihrem Territorium aus lanciert wurden, auf Verlangen anderer Staaten assistieren.[70]

Schließlich schloss die chinesische Regierung im September 2015 das bereits angesprochene bilaterale Übereinkommen mit den USA, nachdem die Obama-Administration mehrfach und öffentlich chinesische Spionageaktivitäten als ernsthafte Bedrohung der bilateralen Beziehungen bezeichnet hatte.[71]

Innerstaatlich bringt die Volksrepublik zwar viele der notwendigen administrativen und technischen Kompetenzen und Fähigkeiten mit, die notwendig sind, um transnationale Sorgfaltsverantwortung zu übernehmen.[72] Gleichzeitig zielt eine wachsende Anzahl von innerstaatlichen Cybersicherheitsnormen (zumindest partiell) darauf ab, durch die Etablierung eigener chinesischer Sicherheitsstandards, der Regierung ungehinderten Zugang zu Netzwerken kommerzieller und privater Akteure zu ermöglichen und auswärtige Anbieter, z. B. von Verschlüsselungssoftware, aus dem chinesischen Markt fernzuhalten.[73]

In der Summe zeigt die chinesische Haltung zur Sorgfaltsverantwortung daher ein gemischtes Verhaltensprofil. Zwar wird die VR über Zeit immer proaktiver in der Propagierung von beschränkenden Normen für expansives Cyberverhalten, insbesondere im militärischen Bereich, wo die USA einen technologischen Vorsprung genießen. Diese Beschränkungen sind aber wiederum regional und funktional begrenzt. So etabliert die VR einen Kreis „engerer Kooperationspartner“ in Zentralasien und Russland mit entsprechend verdichteten Verhaltensvorschriften, deren Normen aber allenfalls schrittweise universalisiert werden. Eine weitergehende Sorgfaltsverantwortung gegenüber anderen Staaten, Individuen oder Wirtschaftsakteuren ist mit dem umfassenden Gestaltungs- und Kontrollanspruch der kommu-

[69] Russian Federation, Agreement between the Government of the Russian Federation and the Government of the People’s Republic of China on cooperation in ensuring international information security, 2015.

[70] UN GGE, UN Doc. A/70/174, 2015.

[71] Chin, Inside the Slow Workings of the U.S.-China Cybersecurity Agreement, The Wallstreet Journal, 2016.

[72] Shackelford u. a., Operationalizing Cybersecurity Due Diligence, University of South Carolina Law Review, Vol. 67, Issue 1, 2016.

[73] Shackelford u. a., Unpacking International Law on Cybersecurity Due Diligence, Chicago Journal of International Law, Vol. 17, Issue 1, 2016, S. 1 (33).

nistischen Partei offensichtlich nur eingeschränkt oder zumindest nur langsam und schrittweise vereinbar.[74]

Deutschland/EU

Die Bundesrepublik verfolgt(e) sowohl national als auch im europäischen Rahmen einen kooperativen, vor allem auf die technische Sicherung Kritischer IT-Infrastrukturen ausgerichteten Cyber-Security-Ansatz. Dabei standen bislang auf nationaler und europäischer Ebene vertrauens- und sicherheitsbildende Maßnahmen, angestrebte Standardisierungsvereinbarungen für den rechtlichen Umgang mit Hard- und Software sowie die Anwendbarkeit des Völkerrechts auf den digitalen Raum im Mittelpunkt.[75]

Im Verbund mit den übrigen EU-Staaten setzt sich die Bundesrepublik auch für eine klare Verantwortungszuweisung für staatliches Handeln im Cyberraum ein. So heißt es im Rahmen der Cyber-Sicherheitsstrategie der EU von 2013 unter dem Punkt „Grundlagen der Cyber-Sicherheit“: „Im Cyberraum gelten dieselben Gesetze und Normen wie in anderen Lebensbereichen.“[76] Auf binnenstaatlicher Ebene findet sich die Norm staatlicher Verantwortung in der nationalen Cyber-Sicherheitsstrategie von 2016, welche entsprechende Aussagen aus der ersten Fassung von 2011 aufgreift. Im Zuge der Neufassung wurden Maßnahmen in vier verschiedenen Handlungsfeldern festgelegt, die einen multidimensionalen Due-Diligence-Ansatz für den digitalen Raum festlegen:

- Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung (u. a. Cyber-Alphabetisierung/Aufklärung, IT-Zertifizierungsmaßnahmen etc.),
- Gemeinsamer Auftrag von Staat und Wirtschaft (u. a. Sicherung der KI, Kooperation mit Providern und Unternehmen),
- Leistungsfähige und nachhaltige gesamtstaatliche Cyber-Sicherheitsarchitektur (u. a. Nationales Cyber-Abwehrzentrum stärken, Strafverfolgung intensivieren, defensive Cyber-Kapazitäten stärken, u. a. durch bereits bestehende CERTs),
- Aktive Positionierung Deutschlands in der europäischen internationalen Cyber-Sicherheitspolitik (u. a. aktive Gestaltung der EU-Politik/NATO-Politik, internationale Präsenz, Cyber-Capacity Building bilateral als auch regional, internationale Strafverfolgung stärken).[77]

[74] Vgl. Gechlik, Appropriate Norms of State Behavior in Cyberspace: Governance in China and Opportunities for US Businesses, Hoover Working Group on National Security, Aegis Series Paper No. 1706, 2017.

[75] Bendiek, Sorgfaltsverantwortung im Cyberraum: Leitlinien für eine deutsche Cyber-Außen- und Sicherheitspolitik, 2016, S. 29.

[76] EU-Kommission, Cybersicherheitsstrategie der Europäischen Union, 2013, S. 4.

[77] BMI, Cybersicherheitsstrategie für Deutschland, 2016, S. 10.

Deutlich erkennbar wird hier der auf defensive Cyber-Fertigkeiten und Ressourcen ausgerichtete deutsche Cyber-Sicherheitsansatz, der im Zuge der jüngsten Debatte um sog. „Hack-Back-Strategien“ kritisch diskutiert wurde.[78]

Im Koalitionsvertrag von 2018 wird dieses brisante Thema ebenso wie die mögliche Initiierung eines „Vulnerabilites Equities Process“ (VEP) ausgespart.[79] VEP bezeichnen eine von der vorherigen Bundesregierung erwogene Praxis der (potenziellen) Zurückhaltung digitaler Sicherheitslücken, sogenannter Zero-Day-Exploits.[80] Die massenhafte Ansammlung solcher Verwundbarkeiten, wie sie von der NSA, aber auch von anderen Geheimdienste seit längerem praktiziert wird,[81] untergräbt potenziell den bislang propagierten defensiven Sicherheitsansatz Deutschlands. Erschwerend käme hinzu, dass nicht nur die angestrebte Kooperation mit IT-Unternehmen in Frage gestellt werden könnte, sondern dass auch die staatliche Sorgfaltspflicht gegenüber den eigenen, aber auch fremden Bürgern tangiert wird, denn das Horten von IT-Sicherheitslücken birgt große und potenziell unabsehbare Gefahren für weite Teile der Internet-Community (siehe hierzu z. B. der Fall der Hackergruppierung „The Shadow Brokers“ versus NSA).

Im Kontrast zu diesen repressiven Maßnahmen stehen die stärker auf die Wirkung von IT-Resilienz und Prävention ausgerichteten Instrumente der Bundesrepublik sowie der EU.[82] So sieht das deutsche IT-Sicherheitsgesetz von 2015 im besonderen Maße den Schutz der Kritischen Infrastrukturen, konkret in Form einer allgemeinen Meldepflicht im Falle von Cyber-Attacken seitens der Betreiber an das BSI, vor. Auf EU-Ebene schließt die sogenannte Richtlinie zur Netz- und Informationssicherheit (NIS) an, welche von den Mitgliedstaaten spätestens bis Mai 2018 umgesetzt werden muss. Beide gesetzlichen Regelungen haben zum Ziel, Informations- und Kommunikationsstrukturen im Bereich der Kritischen Infrastrukturen zu stärken sowie weitergehende IT-Sicherheitsstandards zu schaffen.[83]

Schon seit langem nimmt die Bundesrepublik eine Art Vorreiterrolle im Datenschutz ein. Diese wurde auf nationaler Ebene vor allem durch die Genese des Grundrechts der „informationellen Selbstbestimmung“ im sogenannten Volkszählungsurteil von 1983 gestärkt, das durch zahlreiche nachgeordnete Datenschutzregelungen einfachgesetzlich konkretisiert wird.[84] Auch die EU (u. a. durch die EG-Richtlinie (95/46/EG) von 1995 und die EU-Datenschutzgrundverordnung, verabschiedet 2016) sowie der Europarat (Konvention 108 von 1981) setzen bis heute

[78] Vgl. Krempl, Cyberschläge: Bundesregierung prüft „Hack-Back-Strategie“ mit „digitalem Rettungsschuss“, heise online, 2017.

[79] Mirko Hohmann, Deutschland 4.0? Germany’s Digital Strategy Over the Next Four Years, Council on Foreign Relations, 2018.

[80] Vgl. Holland, Zero Days: Bundesregierung prüft das Zurückhalten von Sicherheitslücken, heise online, 2017.

[81] Townsend, China May Delay Vulnerability Disclosures for Use in Attacs, Securityweek, 2017.

[82] Bendiek, Sorgfaltsverantwortung im Cyberraum: Leitlinien für eine deutsche Cyber-Außen- und Sicherheitspolitik, 2016, S. 10.

[83] BSI, Gesetz zur Umsetzung der NIS-Richtlinie, 2017.

[84] Datenschutz Hessen 2008.

als Normunternehmer globale Standards im Bereich der Cyber-Sicherheit. Dies gilt insbesondere auch für den Umgang mit Drittländern und deren IT-Unternehmen, wie das 2016 ausgehandelte Privacy Shield-Abkommen als Nachfolge-Vereinbarung des umstrittenen Safe-Harbour-Abkommens zeigt.[85]

Insgesamt engagiert sich die Bundesregierung sowohl national als auch auf europäischer und internationaler Ebene als Normunternehmer zur Stärkung der staatlichen, aber auch privaten Verantwortlichkeit im Cyber-Space. Durch entsprechende Gesetzgebungen und Kooperationsinitiativen auf bilateraler und europäischer Ebene fördert die BRD gezielt die Entstehung von Due-Diligence-Regeln im digitalen Raum. Die zunehmende Anzahl ernsthafter Attacken, wie beispielsweise der sogenannte Bundestagshack 2015 oder die Cyber-Attacke auf die Netze des Bundes 2016–2018, schüren aber eine Debatte über offensive Komponenten in der deutschen Cyber-Sicherheitsstrategie, welche die regulative Wirkung der Due-Diligence-Norm nachhaltig schwächen könnte.

Russland

Russland bemüht sich bereits seit Ende der 1990er-Jahre, auf internationaler Ebene verbindliche Regelungen bezüglich des staatlichen Verhaltens im Cyber-Space zu etablieren. Diese Bemühungen waren überwiegend auf die Stärkung des Konzeptes der nationalen Souveränität ausgerichtet oder auf Bereiche, in denen eine stärkere internationale Verrechtlichung russischen Interessen entsprach. Maßnahmen zur Stärkung gemeinsamer Law-Enforcement-Initiativen waren dagegen eher selten.[86]

So stammt der erste Resolutionsentwurf der Russischen Föderation mit dem Titel „Developments in the Field of Information and Telecommunications in the Context of International Security" bereits von 1998. Hier ging es um die Idee eines Vertrages zur Kontrolle von Cyber-Waffen, um so die technologische Vormachtstellung der USA vertraglich einzuhegen.[87] Diese Bestrebungen erfuhren bis 2010, insbesondere von Seiten der USA, erwartungsgemäß keinerlei Unterstützung. Zu sehr unterschied sich der Ansatz Russlands, der nicht von „Cyber-Security" sondern von „Information Security" sprach, von jenem der USA und auch dem der meisten EU-Staaten. Nachdem 2010 die Obama-Administration erstmals den ursprünglichen Entwurf innerhalb der UN mitunterstützte, erweiterte Russland jedoch noch das eigene Engagement: Im Verbund mit China, Tadschikistan und Usbekistan propagierte es im September 2011 den „International Code of Conduct for Information

[85] EU-Kommission, European Commssion launches EU-U.S. Privacy Shield: Stronger Protection for Transatlantic Data Flows, 2016.

[86] Vgl. Nocetti, Contest and Conquest: Russia and Global Internet Governance, International Affairs, Vol. 91, Issue 1, 2015, S. 111 (112).

[87] Vgl. Schmidt u. a., Zwischen nationaler Selbstbehauptung und Kooperationssignalen: Zur Einschätzung der neuen russischen Militärdoktrin, HSFK-Report, Bd. 1, 2010, S. 2.

Security“, dem nur eine Woche später der Vorschlag zu einer „Convention on International Information Security“ folgte.[88]

Bemühungen zur Etablierung einer Sorgfaltsverantwortung im Cyberraum waren von russischer Seite von Beginn an stärker auf die konstitutive Wirkungsebene der Norm gerichtet, um Regierungen klare Rechte und Kompetenzen zuzusprechen und einem drohenden Kontrollverlust entgegenzuwirken. In den Augen vieler westlicher Beobachter war und ist dieser Ansatz in erster Linie autokratischen Bestrebungen nach Kontrolle im analogen und digitalen Raum geschuldet und somit auch eine drohende Gefahr für die Freiheit des Internets und dessen Nutzer.[89]

Ende des Jahres 2017 reichte die russische Regierung den Entwurf einer „United Nations Convention on Cooperation in Combating Information Crimes“ ein, der als Gegenmodell zur „Budapest Convention on Cybercrime“ des Europarates von 2001 gelten kann. Der russische Vorschlag sieht umfassende staatliche Monitoring-Rechte vor.[90] Unterstützung erfuhr der Vorstoß von Seiten der übrigen BRICS-Staaten, in Form einer gemeinsamen Erklärung während des BRICS-Treffens in Xiamen.[91] Die Budapester Cyber-Crime-Konvention enthält aus russischer Sicht zu weitreichende Einschnitte in die staatliche Souveränität der Unterzeichnerstaaten. So wäre es bspw. Strafvollzugsbehörden anderer Staaten nach einer Ratifizierung durch Russland gestattet, umfassende Untersuchungen des digitalen Datenflusses auf russischem Territorium durchzuführen.[92]

Die folgende Darstellung des Cyberangriffs gegen das Democratic National Committee (kurz: DNC-Hack/Leak) aus dem Jahr 2016 wird hier als repräsentativ für einen Teil der russischen Staatspraxis im Cyberraum eingeführt: Zum einen verdeutlicht der Fall die oftmals problematische Balance zwischen prospektiver und retrospektiver Verantwortung; zum anderen zeigt er exemplarisch jene Hindernisse auf, die oftmals einer eindeutigen völkerrechtlichen Bewertung eines Cyber-Vorfalles im Wege stehen.

So kommt Schmitt zu der Auffassung, dass das Verhalten russischer Akteure während des US-Präsidentschaftswahlkampfes 2016 keine verbotene Intervention im Sinne des Verantwortungsgebots der ILC darstellte.[93] Ein manipulativer Angriff auf die IT-Wahl-Systeme einiger Bundesstaaten wäre dagegen laut UN-GGE vom Nichteinmischungsgebot des Nicaragua-Urteils sehr wohl erfasst gewesen. Das US-Präsidialamt interpretierte das Ausbleiben einer solchen direkten Einflussnahme

[88] Maurer, Cyber Norm Emergence at the United Nations, Belfer Center for Science and International Affairs, Discussion Paper 11, 2011, S. 3, 5.

[89] Vgl. Deibert, Tracking the Emerging Arms Race in Cyberspace, Bulletin of the Atomic Scientists, Vol. 67, Issue 1, 2011, S. 1 (6).

[90] Ignatius, Russia is pushing to control cyberspace. We should all be worried., The Washington Post, 2017.

[91] BRICS, Full Text of BRICS Leaders Xiamen Declaration, 2017.

[92] Vgl. Markoff u. a., In Shift, U.S. Talks to Russia on Internet Security, The New York Times, 2009.

[93] Schmitt, in: Nakashima, Russia's apparent meddling in U.S. election is not an act of war, cyber experts say, The Washington Post, 2017.

als Erfolg der eigenen Abschreckungsstrategie, welche Russland (angeblich) im Vorfeld über geheime Kanäle vor entsprechendem Verhalten gewarnt habe. In der Öffentlichkeit wurde indes spekuliert, dass ein direktes Vorgehen aufgrund der vorherigen indirekten Einflussnahme gar nicht mehr im russischen Interesse gelegen habe.[94] Die naheliegende Vermutung, die bereits erfolgte Entwicklung der Due-Diligence-Norm durch die UN GGE habe Russland davon abgehalten, direkte Manipulation (welche über die berichteten Störversuche hinaus gegangen wäre) an Hard-/Software des Wahlvorgangs vorzunehmen, kann indes wohl ausgeschlossen werden.

Die Reaktion der US-Regierung gibt aber Aufschluss über einige Besonderheiten des Konfliktaustrags mit Russland im Cyberraum, denn Anfang Oktober 2016 scheute sich die Obama-Administration, öffentlich die russische Regierung als Initiator zu identifizieren, zudem erfolgte die Attribution letztlich erst nach massivem öffentlichen Druck, u. a. durch wichtige US-Senatoren.[95] Die politische Reaktion der USA beschränkte sich (lange Zeit) auf Sanktionen gegen Geheimdienstakteure, involvierte russische Privatpersonen und angeblich geheimdienstlich genutzte Einrichtungen in den USA.[96]

In seiner Erklärung über die US-Sanktionen vom Dezember 2016 verwies Obama selbst auf den ambivalenten Status des Angriffs: Russland habe zwar gegen „established international norms of behavior“[97] verstoßen, jedoch – wie im Sinne der UN GGE – nicht gegen internationales Völkerrecht. Von Beobachtern wird die Existenz der nicht weiter spezifizierten Normverletzung jedoch u. a. wegen der mangelnden Akzeptanz durch Moskau angezweifelt. Eine abschreckende Wirkung einer bislang nicht etablierten Norm gegenüber Akteuren wie Russland (auch aufgrund fehlender Staatenpraxis) sei nicht zu erwarten.[98]

Konkret steht damit die fortwährende Forderung Russlands nach einer internationalen Verregelung des Kampfes gegen Cyber-Terroristen und -Kriminelle im direkten Widerspruch zur staatlichen Unterstützung bzw. Beauftragung von Hackergruppierungen wie Fancy Bear.[99] Die russische Regierung möchte offensichtlich bestimmte private Akteure mit Hilfe anderer Regierungen ausschalten, während sie die gleichen Regierungen mit Hilfe anderer quasi-privater Akteure attackiert, sodass die Lücke zwischen der konstitutiven und regulativen Wirkung der Sorgfaltsverantwortung immer weiter auseinanderstrebt.

---

[94] Vgl. Sanger, White House Confirms Pre-Election Warning to Russia over Hacking, The New York Times, 2016.

[95] Nakashima, U.S. government officially accuses Russia of hacking campaign to interfere with elections, The Washington Post, 2016.

[96] White House, Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment, 2016.

[97] Ebda.

[98] Vgl. Fidler, The U.S. Election Hacks, Cybersecurity, and International Law, Articles by Maurer Faculty, Vol. 2607, 2017, S. 341.

[99] Vgl. Hacquebord, Zwei Jahre Pawn Storm: Analyse einer mehr in den Mittelpunkt rückenden Bedrohung, 2017.

4 Konfliktverhalten staatlicher und nicht staatlicher Akteure: Befunde

Im folgenden Abschnitt kontrastieren wir die Ergebnisse der Analyse der Staatenpraxis mit den Befunden einer systematischen Erhebung des Cyberkonfliktverhaltens staatlicher und nicht staatlicher Akteure. Ausgangspunkt ist der Datensatz des Projektes „Zwischen Regulation und Furcht: Zur Klassifizierung von Cyberangriffen“, der seit 2016 am Institut für Politische Wissenschaft in Heidelberg aufgebaut wird.[100] Ziel ist es zu klären, inwiefern Entwicklungstrends der Norm auf das Verhalten staatlicher oder nicht-staatlicher Akteure als dyadische Interaktionen zurückgeführt werden können.

4.1 Heidelberger Datensatz zu Cyberkonflikten

Konventionelle gewalttätige Konflikte in der Offline-Welt werden seit Jahrzehnten systematisch, u. a. durch das Heidelberger Institut für Internationale Konfliktforschung (HIIK) analysiert.[101] Konflikte im Cyberraum haben dagegen bislang sehr viel weniger Aufmerksamkeit erfahren: Die Mehrzahl der entsprechenden Datensammlungen erfasst nur einseitige Cyberangriffe,[102] aber keine Konfliktinteraktionen zwischen zwei oder mehreren Akteuren in der Online-Welt.

Unter den einschlägigen Datensätzen stellt das *Dyadic Cyber Incident and Dispute Dataset 1.0* (DCIDD) von Valeriano und Maness,[103] neben dem 2017 initiierten *Cyber-Operations Tracker*,[104] den bislang umfassendsten Versuch dar, Cyberkonflikte zu identifizieren und zu vermessen. Für den Zeitraum zwischen 2000 und 2011 verzeichnen Valeriano und Maness insgesamt 111 Vorfälle, deren Analyse erste wichtige Erkenntnisse über Konfliktdynamiken und mögliche Zusammenhänge mit der Entwicklung der Sorgfaltsverantwortung gezeitigt hat. Valeriano und Maness stellen einerseits fest, dass die Mehrzahl der kodierten Konflikte einen stabil niedrigen Intensitätsgrad aufweisen und nicht eskalieren.[105] Andererseits weisen ihre Daten aus, dass Cyber- und Offline-Konflikte selten interagieren, das heißt Konfliktdynamiken (bislang) kaum von der einen in die andere Sphäre ‚überschwappen‘. Vielmehr sei (im Zeitraum 2001–2011) zu beobachten, dass hohe

[100] Steiger u. a., Conceptualising Conflicts in Cyberspace, Journal of Cyber Policy, Vol. 3, Issue 1, 2018, S. 77.

[101] HIIK, Konfliktbarometer 2016; COW, Data Sets 2017; UCDP 2017.

[102] Vgl. etwa CSIS, Significant Cyber Incidents 2017.

[103] Valeriano u. a., The Dynamics of Cyber Conflict between Rival Antagonists, 2001–11, Journal of Peace Research, Vol. 51, Issue 3, 2014, S. 347.

[104] CFR, Cyber Operations Tracker 2017.

[105] Valeriano u. a., The Dynamics of Cyber Conflict between Rival Antagonists, 2001–11, Journal of Peace Research, Vol. 51, Issue 3, 2014, S. 347 (359); Valeriano u. a., Cyber War versus Cyber Realities: Cyber Conflict in the International System, 2015, S. 214.

konventionelle Konfliktaktivität regelmäßig mit einem (artifiziell) niedrigen Online-Konfliktniveau einhergeht.[106]

Das *Dyadic Cyber Incident and Dispute Dataset 1.0* hat erste wichtige Grundlagen für die sozialwissenschaftliche Cyberkonfliktforschung gelegt. Die Systematik des Heidelberger Datensatzes (HD-CY.CON) zielt indes in wichtigen Bereichen über die des DCIDD hinaus: 1) Während der DCIDD 1.0[107] nur bestimmte Staatendyaden erfasst (jene die durch langjährige Offline-Konflikte geprägt sind), indexiert HD-CY.CON alle (potenziell möglichen) zwischenstaatlichen Konfliktdyaden und alle Konfliktdyaden mit nicht-staatlichen Akteuren, insbesondere auch (regierungsnahen) Hackergruppen, sodass staatlich delegierte oder gesponserte Konfliktaktivitäten nicht-staatlicher Akteure analysiert werden; 2) Die Konfliktintensitätsmessung des Heidelberger Ansatzes folgt einem induktiven Verfahren, das technische, (potenzielle) physische, und vor allem auch sozio-politische Auswirkungen der jeweiligen Cyber-Ereignisse erfasst, d.h. die Politisierung von Cyber-Verwundbarkeiten stärker in den Blick nimmt; 3) HD-CY.CON verwendet zudem neben westlichen Quellen zur Ereignisbestimmung auch solche in chinesischer und russischer Sprache, um eine mögliche regionale und sozio-kulturelle Voreingenommenheit besser erfassen und einordnen zu können.

Staat A	Staat B	Staat als Angreifer**	Staatlich-gespons. Akteur als Angreifer	Hacktivist als Angreifer	Akteur unbekannt	N	Cyber-Intensität Ø***
Indien (7)****	Pakistan (16)	2	0	18	3	23	1
Russland (11)	USA (1)	4	3	2	3	12	1,75
Russland (6)	Ukraine (1)	3	2	1	1	7	3,07
Korea (0)	Nordkorea (7)	4	2	0	1	7	1,71
Iran (3)	Saudi-Arab. (3)	0	1	3	2	6	1,67
Gesamt		13	8	24	10	55	1,84

** Voraussetzung: Mindestens in einem Fall attribuierte staatliche Involvierung.*
*** Entspricht der jeweilig vorgenommenen Attribution.*
**** Skala reicht von 1 bis maximal 15.*
***** (x) = Anzahl der initiierten Angriffe.*
Das Sample umfasst derzeit insgesamt 428 Fälle für den Zeitraum 2014-2016.

Abb. 3 Die Top Fünf der Cyber-Konfliktdyaden 2014–2016 und deren Intensitäten.∗ (Quelle: HD-CY.CON; eigene Erstellung)

[106] Maness u. a., Cyber Spillover Conflicts: Transitions from Cyber Conflict to Conventional Foreign Policy Disputes? In: Friis u. a., (Hrsg.), Routledge Studies in Conflict, Security and Technology, 2016, S. 45 (60).

[107] Im Juli 2019 erschien der DCIDD 1.5 (2000–2016), welcher nun auch Cyberkonflikte zwischen Staaten ohne verbundener Offline-Rivalität erfasst. Die übrigen Limitationen, wie eine wenig ausdifferenzierte Erfassung der attribuierten Täter-Akteursschaft, bleiben jedoch bestehen.

Staat A	Staat B	HIIK-Intensität* Ø	Cyber-Intensität Ø	Staat als Angreifer	Staatlich-gespons. Akteur als Angreifer	Hacktivist als Angreifer	Akteur unbekannt	N
Indien (7)**	Pakistan (16)	3,15	1	2	0	18	3	23
Aserbaid. (4)	Armenien (5)	3	1,88	0	0	9	0	9
Russland (6)	Ukraine (1)	2,5	3,07	3	2	1	1	7
Iran (3)	Saudi-Arab. (3)	5***	1,67	0	1	3	2	6
Israel (0)	Palästina (4)	3	1	0	0	4	0	4
Gesamt		3,33	1,72	5	3	35	6	49

**Bezieht sich ausschließlich auf den Durchschnitt der vergebenen Intensitätswerte des HIIK für den Untersuchungszeitraum, im Falle einer Übereinstimmung zwischen Cyber- und Offline-Konflikt-Issue innerhalb der Dyade. Die Skala reicht von 1 bis maximal 5.*
***(x) = Anzahl der jeweilig initiierten Angriffe.*
**** Bezieht sich auf drei Fälle, in welchen die Cyber-Maßnahmen einen direkten Bezug zum Jemen-Konflikt hatten. Die HIIK-Intensität bezieht sich daher auf den dortigen Konflikt zwischen den vom Iran unterstützten Huthi-Rebellen auf der einen sowie der Regierung und dessen Verbündeten (u.a. Saudi-Arabien) auf der anderen Seite.*
Das Sample umfasst derzeit insgesamt 428 Fälle für den Zeitraum 2014-2016.

Abb. 4 Regionale Offline/Online-Konfliktdynamiken: Spillover-Effekte 2014–2016. (Quelle: HD-CY.CON; eigene Erstellung)

4.2 (Vorläufige) Befunde von HD-CY.CON (2014–2016)

Auf der Grundlage einer vorläufigen Auswertung der Cyberkonfliktdaten für den Zeitraum von 2014–2016 lassen sich nun folgende tentative Ergebnisse festhalten: Zum einen kann nach wie vor ein Trend festgestellt werden, wonach staatliche Akteure mit umfangreichen technischen Cyberkonfliktkapazitäten Selbstbeschränkung im Cybergewaltverhalten üben, das heißt auf den Gebrauch ihres *gesamten* Instrumentenspektrums verzichten. Dies spiegelt sich vor allem in der überwiegend niedrigen Konfliktintensität wider (Abb. 3). Zum anderen ist aber (zumindest im Zeitraum 2014–2016) eine deutlich erhöhte Cyberkonfliktinteraktion zwischen staatlichen und nicht-staatlichen Akteuren zu verzeichnen, die primär auf die USA und dortige Regierungsstellen abzielen, nicht aber auf diese beschränkt bleiben. So waren im Untersuchungszeitraum in 66 von insgesamt 428 Fällen ein politischer Akteur oder eine politische Institution der USA das jeweilige Angriffsziel.

Unsere Daten zeigen ferner, dass Hackergruppen, trotz der gegenläufigen Normbildung, kommerzielle Ziele angreifen und politische Prozesse beeinflussen. Sie zeigen aber auch, dass Angriffe oder Konfliktinteraktion unter Einbeziehung von Kritischen Infrastrukturen jedoch nach wie vor selten sind. So waren lediglich in ca. jedem zehnten Fall (44 von 428) Kritische Infrastrukturen unter den anvisierten Zielen. Es kann daher begründet vermutet werden, dass unilaterale Erklärungen, wie jene in der US-Sicherheitsstrategie, die einen Cyberangriff auf Kritische Infrastrukturen mit einem kinetischen Angriff gleichsetzen, eine einhegende Wirkung entfalten.

Auffällig ist in unseren Daten auch das Verhalten global agierender Hackerkollektive wie Anonymous, die immer häufiger in ideologisch motivierten Angriffen Staaten ins Visier nehmen, um diese für vorangegangenes Verhalten zu „bestrafen“

oder diese an ihre staatlichen Verantwortungen auf analoger sowie digitaler Ebene zu „erinnern“. So war das Kollektiv im Untersuchungszeitraum allein in 90 der insgesamt 428 kodierten Fälle der (selbst ernannte) „bekennende Täter“. Jedoch überschritten auch diese Angriffe, zumeist als DDoS-Attacken, überwiegend nicht das allgemein niedrige Intensitätsniveau und wurden in den betroffenen Staaten für gewöhnlich auch nicht politisiert. Für diesen Typ der Akteursgruppierung ist deshalb bislang weder eine retrospektive noch prospektive Wirkung der Sorgfaltsverantwortungsnorm nachweisbar. Lediglich im Falle der weltweit Aufsehen erregenden Attacke „OpAntiSec“ (Operation Anti Security) der Hackergruppierung LulzSec in Kooperation mit Anonymous wurde von transnationalen Strafverfolgungsmaßnahmen in den USA, Großbritannien und den Niederlanden berichtet.[108] Diese Kampagne zeichnete sich allerdings auch durch eine für Hacktivisten ungewöhnlich hohe Intensität aus, indem u. a. sehr sensible Daten geleakt wurden.[109]

Der von Valeriano und Maness bereits hergestellte Zusammenhang zwischen analogem und digitalem Konfliktaustrag wird durch die Daten von HD-CY.CON bestätigt. So partizipieren in Regionalkonflikten (siehe Abb. 4) verstärkt auch staatlich gesponserte Hackergruppierungen, selbst ernannte „Cyber-Armeen“ oder „patriotische Hacker“, die mit niedriger Intensität und ideologischer Ausrichtung vorgehen. Regionale Normetablierungsbemühungen, wie jene in Zentralasien, werden daher durch Cyber-Konfliktdynamiken teilweise konterkariert. Mögliche Erklärungen hierfür sind die zumeist sehr niedrigen Intensitätsstufen der Cyber-Konflikte, die mit der Einbindung von Hackergruppen verbundene Hoffnung zur Verschleierung staatlicher Verantwortung sowie die lange historische Animosität in vielen der Konfliktdyaden, die eine Konfliktregelung außerordentlich erschwert.

5 Fazit

Unsere Untersuchung zeigt, dass die Norm einer transnationalen Sorgfaltsverantwortung im Cyberraum noch in den Kinderschuhen steckt. Es ist daher fraglich, ob die Norm, verstanden als transnationale Verpflichtung zu warnen, Schaden zu vermeiden und nicht zu intervenieren, tatsächlich schon für die Akteursschaft von Staaten und nicht-staatlichen Akteuren konstitutiv und das Verhalten prägend wirkt. Noch fraglicher ist, ob eine prospektive Sorgfaltsverantwortung existiert, wenn gerade erst, wie im Falle der schädigenden Weitergabe von Nutzerdaten durch Facebook diskutiert, die retrospektive Sorgfaltsverantwortung innerhalb der Gemeinschaft demokratischer Rechtsstaaten etabliert wird. Da die Datenbasis unserer Analyse schmal ist, können unsere Schlussfolgerungen indes nur als vorläufig gelten.

Konkret feststellbar ist zunächst, dass es eine partiell sehr weit fortgeschrittene völkerrechtswissenschaftliche Debatte darüber gibt, inwiefern eine Sorgfaltsverantwortung analog zu anderen Rechtsgebieten für den Cyberraum abgeleitet werden

[108] Mills, FBI arrests 16 in Anonymous hacking investigation, cnet, 2011.

[109] Ward, Anti-Sec: Who are the world’s most wanted hackers?, bbc, 2012.

kann und inwiefern diese in der gewohnheitsrechtlichen Staatenpraxis und völkerrechtlichen Meinungsbildung bereits politische (aber nicht rechtliche) Bindung erlangt hat. Die Untersuchung der Staatenpraxis zeigt auch, dass die USA und die Bundesrepublik in unterschiedlich ausgeprägter Form als Normunternehmer für die Sorgfaltsverantwortung aufgetreten sind. Auffällig ist dabei, dass eine rechtliche Selbstbindung der US-Regierung durch die Obama-Administration keine Unterstützung erfuhr. Eine plausible Erklärung für diesen Befund lautet, dass mit einer formalen Selbstbindung erhebliche Umsetzungskosten für Regierung, Bürger und Unternehmen einhergehen dürften, um sicherzustellen, dass deren Online-Verhalten keine schädigende Drittwirkung entfaltet.

Auch konnten wir empirisch feststellen, dass die Sorgfaltsverantwortung von Russland und China anders, zumeist restriktiver diskutiert und noch eingeschränkter praktiziert wird. So findet sich die Verpflichtung zur Nicht-Intervention und zur Verantwortung, Schaden zu vermeiden, explizit (und rechtlich verbindlich) in bilateralen Vereinbarungen und jenen der Shanghaier Organisation für Zusammenarbeit. In der Staatenpraxis kann jedoch bislang nur eine Verschonung von Kritischen Infrastrukturen (mit wenigen Ausnahmen) sowie die Einhaltung funktional begrenzter Verzichtserklärungen für kommerzielle Cyberspionage zwischen einigen wichtigen Handelsmächten (USA, China, Deutschland, Großbritannien, Australien) nachgewiesen werden.

Kontrastiert man diese empirischen Befunde nun mit den Entwicklungstrends der internationalen Cyberkonfliktdynamiken, dann fällt zunächst einmal auf, dass die Sorgfaltsverantwortung, wenn sie denn von Regierungen für sich selbst anerkannt wird, noch keine erkennbare Wirkung für nicht-staatliche Akteure, insbesondere Hackergruppen, entfaltet hat. Plausibel ist vielmehr, dass insbesondere die russische und chinesische Regierung gezielt nicht-staatliche Akteure beauftragen, befähigen oder duldend deren schädigendes Verhalten gegenüber anderen Staaten und nicht-staatlichen Akteuren hinnehmen. Eine plausible Erklärung aus Sicht der politikwissenschaftlichen Normforschung ist, dass diese Regierungen zwar die konstitutive Wirkung der Norm – als legitimes Mitglied der Staatengemeinschaft anerkannt zu werden – schätzen, ihre regulative Wirkung aber mit Hilfe der Delegation von schädigendem Verhalten an Hackergruppen umgehen wollen. Aus unserer Sicht zeigt das Beispiel der amerikanisch-chinesischen Vereinbarung zur Begrenzung der kommerziellen Cyberspionage jedoch, dass Transparenz, öffentlicher Druck und die Spezifizierung der jeweiligen Norm potenziell die klaffende Lücke zwischen der Statuierung einer Norm und deren Umsetzung zumindest partiell zu schließen vermögen.

Gleichwohl gibt es auch eine Reihe alternativer Erklärungen für Verhalten, das nur scheinbar der Befolgung der Norm der Sorgfaltsverantwortung dient. Die Selbstbeschränkung beim offensiven Einsatz schädigender Cyberinstrumente kann auch so erklärt werden, dass (1) Cyberwaffen, anders als konventionelle, replizierbar sind (und zu einem potenziellen Bumerangeffekt führen können); dass (2) besonders schadhafte Cyberwaffen sehr schwer zu produzieren und manche (Zero-Day-Exploits) sogar nur einmal anwendbar sind; dass (3) Cyberwaffen sehr leicht auch Drittakteure beeinträchtigen und dadurch zur Konfliktpartei werden lassen

können; dass (4) Cyberwaffen besonders gegen technisch-fortgeschrittene Gesellschaften eingesetzt werden können, weil deren Verwundbarkeit besonders groß ist.

Kurz: Bestimmte technische und soziale Charakteristika von Cyberwaffen können zu einem Selbstabschreckungseffekt führen.[110] Dieser Selbstabschreckungseffekt kann, so unsere Vermutung, besonders in der Anfangsphase der Normgenese entsprechendes Verhalten konditionieren. Aus Sicht der Normforschung ergibt sich daraus die Frage, wann sich das normkonforme Verhalten von den materiellen Anreizen (Sanktionen durch den Gegner) löst und internalisiert wird.

Aus unserer politikwissenschaftlichen Perspektive spricht daher einiges dafür, dass in diesem frühen Stadium der Normemergenz der Sorgfaltsverantwortung im Cyberraum die eingeschränkte Wirkung der Norm auf die Wirkungsweise eines „untertheoretisierten Übereinkommens“ zurückgeht. Staaten und zum Teil auch nicht-staatliche Akteure verhalten sich derzeit aus unterschiedlichen Gründen normkonform. Zum Teil, weil sie sich mit der Norm und ihrer konstitutiven Wirkung für die Staatengemeinschaft identifizieren. Andere Staaten antizipieren eher die Kosten eines normwidrigen Verhaltens für sich selbst oder für die soziale Dynamik eines „Tabubruchs“ innerhalb der Staatengemeinschaft. Wie das Beispiel der Normentwicklung in der Shanghaier Organisation für Zusammenarbeit sowie entsprechende Regelungen des „Privacy Shield Übereinkommens“ zwischen der Europäischen Union und den USA zeigen, kann Normentwicklung dabei regional sehr unterschiedlich verlaufen und zwischen einer prospektiven und einer retrospektiven Auslegung changieren. Die weitere Forschung sollte daher regionalen Entwicklungsdynamiken besondere Aufmerksamkeit schenken.

Literatur

Constantine Antonopoulos, State Responsibility in Cyberspace, in: Nicholas Tsagourias/Russell Buchan (Hrsg.), Research Handbook on International Law and Cyberspace, 2015, S. 55.

Greg Austin, International Legal Norms in Cyberspace: Evolution of China’s National Security Motivations, in: Anna-Maria Osula/Henry Rõigas (Hrsg.), International Cyber Norms: Legal, Policy & Industry Perspectives, Tallinn: NATO CCD COE Publications, 2016, S. 171.

Greg Austin, Cyber Policy in China, 1. Auflage, 2017.

Karine Bannelier-Christakis, Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?, in: Lauri Mälksoo/Ineta Ziemele/Dainius Žalimas, Baltic Yearbook of International Law, Vol. 14, 2014, S. 23.

Annegret Bendiek, Sorgfaltsverantwortung im Cyberraum: Leitlinien für eine deutsche Cyber-Außen- und Sicherheitspolitik, SWP, 2016.

Bundesministerium des Innern, (BMI), Cybersicherheitsstrategie für Deutschland, 2016, https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf, (letzter Zugriff: 02.09.2019).

BRICS, Full Text of BRICS Leaders Xiamen Declaration, 2017, http://www.bricschn.org/English/2017-09/05/c_136583711_2.htm, (letzter Zugriff: 02.09.2019).

[110] Valeriano u. a., Cyber War versus Cyber Realities: Cyber Conflict in the International System, 2015, S. 50.

Bundesamt für Sicherheit in der Informationstechnik (BSI), Gesetz zur Umsetzung der NIS-Richtlinie, 2017, https://www.bsi.bund.de/DE/DasBSI/NIS-Richtlinie/NIS_Richtlinie_node.html, (letzter Zugriff: 02.09.2019).

Mlada Bukanovsky/Ian Clark/Robyn Eckersley u. a., Special Responsibilities: Global Problems and American Power, 2012.

Cuihong Cai, Cybersecurity in Chinese Context: Changing Concepts, Vital Interests and Cooperative Willingness, 9th Berlin Conference on Asian Security (BCAS) International Dimensions of National (In)Security Concepts, Challenges and Ways Forward, Berlin, 14–16. Juni 2015.

Center for Strategic & International Studies (CSIS), Significant Cyber Incidents, 2017, https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity, (letzter Zugriff: 02.09.2019).

Dean Cheng, Cyber Dragon: Inside China's Information Warfare and Cyber Operations, 2017.

Josh Chin, Inside the Slow Workings of the U.S.-China Cybersecurity Agreement, The Wallstreet Journal, 2016, https://blogs.wsj.com/chinarealtime/2016/06/15/inside-the-slow-workings-of-the-u-s-china-cybersecurity-agreement/, (letzter Zugriff: 02.09.2019).

Council on Foreign Relations (CFR), Cyber Operations Tracker, 2017, https://www.cfr.org/interactive/cyber-operations, (letzter Zugriff 02.09.2019).

Correlates of War Project (COW), Data Sets, 2017, http://www.correlatesofwar.org/data-sets, (letzter Zugriff: 02.09.2019).

Jean D'Aspremont/André Nollkaemper/Ilias Plakokefalos/Cedric Ryngaert, Sharing Responsibility between Non-State Actors and States in International Law: Introduction, Netherland International Law Review, Vol. 62, 2015, S. 49.

Datenschutz Hessen, 2008, https://www.datenschutz.hessen.de/datenschutz.htm, (letzter Zugriff: 02.09.2019).

Ronald Deibert, Tracking the Emerging Arms Race in Cyberspace, Bulletin of the Atomic Scientists, Vol. 67, Issue 1, 2011, S. 1.

Laura De Nardis, The Global War for Internet Governance, 2014.

Department of State (DOS), Department of State International Cyberspace Policy Strategy, 2016, https://www.state.gov/documents/organization/255732.pdf, (letzter Zugriff: 02.09.2019).

Kristen Eichensehr, Public-Private Cybersecurity, Texas Law Review, 95, 2017, S. 467.

Toni Erskine/Madeline Carr, Beyond ‚Quasi-Norms': The Challenges and Potential of Engaging with Norms in Cyberspace, in: Anna-Maria Osula/Henry Rõigas (Hrsg.), International Cyber Norms: Legal, Policy & Industry Perspectives, NATO CCD COE Publications, Tallinn, 2016.

Toni Erskine, Making Sense of Responsibility in International Relations: Key Questions and Concepts, in: Toni Erskine (Hrsg.), Can Institutions Have Responsibilities? Collective Moral Agency and International Relations, 2003, S. 1.

EU-Kommission, European Commssion launches EU-U.S. Privacy Shield: Stronger Protection for Transatlantic Data Flows, 2016, http://europa.eu/rapid/press-release_IP-16-2461_en.htm, (letzter Zugriff: 02.09.2019).

EU-Kommission, Gemeinsame Mitteilung an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Cybersicherheitsstrategie der Europäischen Union – ein offener, sicherer und geschützter Cyberraum, 2013, http://www.eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_de.pdf, (letzter Zugriff: 02.09.2019).

David P. Fidler, The U.S. Election Hacks, Cybersecurity, and International Law, Articles by Maurer Faculty, Vol. 2607, 2017.

David P. Fidler/Russell Buchan/Emily Crawford u. a., ILA Study Group Report on Cybersecurity, Terrorism and International Law, 2016.

Martha Finnemore, Cybersecurity and the Concept of Norms, Carnegie Endowment for International Peace, 2017.

Martha Finnemore/Duncan B. Hollis, Constructing Norms for Global Cybersecurity, The American Journal of International Law, Vol. 110, Issue 3, 2016, S. 425.

Mervyn Frost, Ethics in International relations: A Constitutive Theory, Cambridge: Cambridge University Press, 1. Auflage, 1996.

Mei Gechlik, Appropriate Norms of State Behavior in Cyberspace: Governance in China and Opportunities for US Businesses, Hoover Working Group on National Security, Technology and Law, Aegis Series Paper No. 1706, 2017.
Oren Gross, Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-Incidents, Cornell International Law Journal, Vol. 48, 2015, S. 481.
Feike Hacquebord, Zwei Jahre Pawn Storm: Analyse einer mehr in den Mittelpunkt rückenden Bedrohung, 2017, https://www.trendmicro.de/media/wp/operation-pawn-storm-whitepaper-de.pdf, (letzter Zugriff: 02.09.2019).
Ludger Heidbrink, Definitionen und Voraussetzungen der Verantwortung, in: Ludger Heidbrink/Claus Langbehn/Janina Loh (Hrsg.), Handbuch Verantwortung, 2016.
HIIK, Konfliktbarometer, 2016, http://hiik.de/de/konfliktbarometer/pdf/ConflictBarometer_2016.pdf, (letzter Zugriff: 02.09.2019).
Geoffrey Hoffman, A Clash of Cyber Civilisations, ChinaFile, 2018, http://www.chinafile.com/reporting-opinion/viewpoint/clash-of-cyber-civilizations, (letzter Zugriff: 02.09.2019).
Mirko Hohmann, Deutschland 4.0? Germany's Digital Strategy Over the Next Four Years, Council on Foreign Relations, 2018, https://www.cfr.org/blog/deutschland-40-germanys-digital-strategy-over-next-four-years, (letzter Zugriff: 02.09.2019).
Martin Holland, Zero Days: Bundesregierung prüft das Zurückhalten von Sicherheitslücken, heise online, 2017, https://www.heise.de/newsticker/meldung/Zero-Days-Bundesregierung-prueft-das-Zurueckhalten-von-Sicherheitsluecken-3852523.html, (letzter Zugriff: 02.09.2019)
David Ignatius, Russia is pushing to control cyberspace. We should all be worried., The Washington Post, 2017, https://www.washingtonpost.com/opinions/global-opinions/russia-is-pushing-to-control-cyberspace-we-should-all-be-worried/2017/10/24/7014bcc6-b8f1-11e7-be94-fabb0f1e9ffb_story.html?noredirect=on&utm_term=.126d80609652, ((letzter Zugriff: 02.09.2019).
ILA Study Group, ILA Study Group on Due Diligence, Second Report, Duncan French (Chair) and Tim Stephens (Rapporteur), 2016.
ILA Study Group, 2014, https://olympereseauinternational.files.wordpress.com/2015/07/due_diligence_-_first_report_2014.pdf, (letzter Zugriff 02.09.2019).
UN General Assembly (2015), International Code of Conduct for Information Security, UN Doc. A/69/723.
International Court of Justice, Military and Paramilitary Activities in and against Nicaragua (Nicaragua vs. United States of America), ICJ Reports 1986, http://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf, (letzter Zugriff 02.09.2019).
International Law Commission (ILC), Responsibility of States for Internationally Wrongful Acts, Yearbook of the International Law Commission, Vol. II, Part Two, 2001, S. 26.
Eric T. Jensen/Sean Watts, A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer? Texas Law Review, Vol. 95, 2017, S. 1555.
Ronald L. Jepperson/Alexander Wendt/Peter J. Katzenstein, Norms, Identity and Culture in National Security, in: Peter J. Katzenstein (Hrsg.). The culture of national security: Norms and identity in world politics, 1996, S. 33.
Jing De Jong-Chen, China's Evolving Cybersecurity andCyber Development Strategy, The International Bureau of Asian Research, 2017, http://nbr.org/downloads/pdfs/eta/Jong-Chen_commentary_032917.pdf, (letzter Zugriff: 02.09.2019).
Marina Kaljurand, United Nations Group of Governmental Experts: The Estonian Perspective, in: Anna-Maria Osula/Henry Rõigas (Hrsg.), International Cyber Norms: Legal, Policy & Industry Perspectives, NATO CCD COE Publications, 2016, S. 111.
Peter J. Katzenstein (Hrsg.), The Culture of National Security: Norms and Identity in World Politics, 1996.
Matthias Kaufmann, Welches Eigentum gehört zum Menschenrecht auf Freiheit? in: Joachim Renzikowski (Hrsg.), Freiheit als Rechtsbegriff, 2016, S. 115.
Lucas Kello, The Virtual Weapon and International Order, 2017.
John Kerry, Text of John Kerry's Remarks in Seoul on Open and Secure Internet, 2015, https://www.voanews.com/a/text-of-john-kerrys-remarks-in-seoul-on-open-and-secure-internet/2776139.html, (letzter Zugriff: 02.09.2019).

Robert Kolb, Reflections on Due Diligence Duties and Cyberspace, German Yearbook of International Law 58, 2015, S. 113.
Elaine Korzak, UN GEE on Cybersecurity: The End of an Era? – What the apparent GGE failure means for international norms and confidence-building measures in cyberspace, The Diplomat, 31. Juli 2017, https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/, (letzter Zugriff: 02.09.2019).
Stefan Krempl, Cyberschläge: Bundesregierung prüft „Hack-Back-Strategie" mit „digitalem Rettungsschuss", heise online, 2017, https://www.heise.de/newsticker/meldung/Cyberschlaege-Bundesregierung-prueft-Hack-Back-Strategie-mit-digitalem-Rettungsschuss-3689279.html, (letzter Zugriff: 02.09.2019).
Jeffrey W. Legro, Which Norms Matter? Revisiting the „Failure" of Internationalism, International Organization, Vol. 51, Issue 1, 1997, S. 31.
Ian Yuying Liu, State Responsibility and Cyberattacks: Defining Due Diligence Obligations, Indonesian Journal of International & Comparative Law, Vol. 4, 2017, S. 191.
Jon R. Lindsay et al. (Hrsg.), China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain, 2015.
Kubo Mačák, From Cyber Norms to Cyber Rules: Re-engaging States as Lawmakers, Leiden Journal of International Law, Vol. 30, Issue 4, 2017, S. 877.
Ryan C. Maness/Brandon Valeriano, Cyber Spillover Conflicts: Transitions from Cyber Conflict to Conventional Foreign Policy Disputes? In: Karsten Friis/Jens Ringsmose (Hrsg.), Routledge Studies in Conflict, Security and Technology: Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives, 2016, S. 45.
Thilo Marauhn, Customary Rules of International Environmental Law: Can they Provide Guidance for Development a Peacetime Regime for Cyberspace? In: Katharina Ziolkowski (Hrsg.), Peacetime Regime for State Activities in Cyberspace – International Law, Foreign Affairs and Cyber-Diplomacy, Tallinn, 2013, S. 465.
John Markoff/Andrew E. Kramer, In Shift, U.S. Talks to Russia on Internet Security, The New York Times, 2009, http://www.nytimes.com/2009/12/13/science/13cyber.html, (letzter Zugriff: 02.09.2019).
Tim Maurer, Cyber Mercenaries: The State, Hackers, and Power, 2018.
Tim Maurer, Cyber Norm Emergence at the United Nations: An Analysis of the Activities at the UN Regarding Cyber-Security, Belfer Center for Science and International Affairs, Discussion Paper 11, 2011.
Elinor Mills, FBI arrests 16 in Anonymous hacking investigation, cnet, 2011, https://www.cnet.com/news/fbi-arrests-16-in-anonymous-hacking-investigation/, (letzter Zugriff: 02.09.2019).
Ellen Nakashima, Russia's apparent meddling in U.S. election is not an act of war, cyber experts say, The Washington Post, 2017, https://www.washingtonpost.com/news/checkpoint/wp/2017/02/07/russias-apparent-meddling-in-u-s-election-is-not-an-act-of-war-cyber-expert-says/?utm_term=.9a211f0b9a50, (letzter Zugriff: 02.09.2019).
Ellen Nakashima, U.S. government officially accuses Russia of hacking campaign to interfere with elections, The Washington Post, 2016, https://www.washingtonpost.com/world/national-security/us-government-officially-accuses-russia-of-hacking-campaign-to-influence-elections/2016/10/07/4e0b9654-8cbf-11e6-875e-2c1bfe943b66_story.html?utm_term=.2be978a38684, (letzter Zugriff: 02.0.2019).
National Cybersecurity and Communications Integration Center (NCCIC), US-CERT Federal Incident Notification Guidelines, 2016, https://www.us-cert.gov/incident-notification-guidelines, (letzter Zugriff: 02.09.2019).
National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity, 2014, https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf, (letzter Zugriff: 02.09.2019).
Martin Ney/Andreas Zimmermann, Cyber-Security beyond the Military Perspective: International Law, Cyberspace, and the Concept of Due Diligence Focus, German Yearbook of International Law, Vol. 49, 2015, S. 51.

Julien Nocetti, Contest and Conquest: Russia and Global Internet Governance, International Affairs, Vol. 91, Issue 1, 2015, S. 111.
Jens David Ohlin, Did Russian Cyber Interference in the 2016 Election Violate International Law?, Texas Law Review, Vol. 95, 2017, S. 1579.
Anna-Maria Osula/Henry Rõigas, Introduction, in: Anna-Maria Osula/Henry Rõigas (Hrsg.), International Cyber Norms: Legal, Policy & Industry Perspectives, NATO CCD COE Publications, Tallinn, 2016, S. 11.
Valentin Rauer, Distribuierte Handlungsträgerschaft: Verantwortungsdiffusion als Problem der Digitalisierung sozialen Handelns, in: Christopher Daase/Julian Junk/Stefan Kroll/Valentin Rauer (Hrsg.), Politik und Verantwortung: Analysen zum Wandel politischer Entscheidungs- und Rechtfertigungspraktiken, PVS-Sonderheft 52/2017, 2017, S. 436.
August Reinisch/Markus Beham, Mitigating Risks: Inter-State Due Diligence Obligations in Case of Harmful Cyber Incidents and Malicious Cyber Activity – Obligations of the Transit State, German Yearbook of International Law, Vol. 54, 2015, S. 101.
Thomas Risse, Konstruktivismus, Rationalismus und Theorien Internationaler Beziehungen – Warum empirisch nichts so heiß gegessen wird, wie es theoretisch gekocht wurde, in: Gunther Hellmann/Klaus Dieter Wolf/Michael Zürn (Hrsg.), Die neuen Internationalen Beziehungen: Forschungsstand und Perspektiven in Deutschland, 2003, S. 99.
Russian Federation, Agreement between the Government of the Russian Federation and the Government of the People's Republic of China on cooperation in ensuring international information security, 2015, https://cyber-peace.org/wp-content/uploads/2013/05/RUS-CHN_CyberSecurityAgreement201504_InofficialTranslation.pdf, (letzter Zugriff: 02.09.2019).
David E. Sanger, White House Confirms Pre-Election Warning to Russia over Hacking, The New York Times, 2016, https://www.nytimes.com/2016/11/17/us/politics/white-house-confirms-pre-election-warning-to-russia-over-hacking.html?_r=0, (letzter Zugriff: 02.09.2019).
Christian Schaller, Internationale Sicherheit und Völkerrecht im Cyberspace: Für klarere Regeln und mehr Verantwortung, SWP-Studie 8/2014, 2014, S. 1.
Hans-Joachim Schmidt/Harald Müller, Zwischen nationaler Selbstbehauptung und Kooperationssignalen: Zur Einschätzung der neuen russischen Militärdoktrin, HSFK-Report, Bd. 1, 2010.
Michael Schmitt (Hrsg.), Tallinn Manual 2.0 on the international law applicable to cyber operations, 2017.
Michael Schmitt, In Defense of Due Diligence in Cyberspace, Yale Law Journal Forum, Vol. 125, 2015, S. 68.
Michael Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare, 2013.
Michael Schmitt/Liis Vihul, The Nature of International Law Cyber Norms, Tallinn Paper No. 5, Special Expanded Issue, CCDCOE, Tallinn, 2014.
Adam Segal, Chinese Cyber Diplomacy in a New Era of Uncertainty, Hoover Working Group on National security, Technology, and Law, Aegis Paper Series No. 1703, 2017.
Anja Seibert-Fohr, Die völkerrechtliche Verantwortung des Staats für das Handeln von Privaten: Bedarf nach Neuorientierung?, in: Zeitschrift für ausländisches öffentliches Recht und Völkerrecht, Bd. 73, 2013, S. 37.
Shanghai Cooperation Organization (SCO), Agreement between the Governments of the Member States of the Shanghai Cooperation Organization in the Field of International Information Security, 2009, http://www.ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreement.pdf, (letzter Zugriff: 02.09.2019).
Scott Shackelford/Scott Russell, Operationalizing Cybersecurity Due Diligence: A Transatlantic Comparative Case Study, University of South Carolina Law Review, Vol. 67, Issue 1, 2016, S. 1.
Scott Shackelford/Scott Russell/Andreas Kuehn, Unpacking International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors, Chicago Journal of International Law, Vol. 17, Issue 1, 2016, S. 1.
Scott Shackelford/Andrew Proia/Brenton Martell/Amanda Craig, Toward a Global Cybersecurity Standard of Care? Exploring the Implications of the 2014 NIST Cybersecurity Framework on

Shaping Reasonable National and International Cybersecurity Practices, Texas International Law Journal, Vol. 50, 2015, S. 303.
Beth Simmons, Mobilizing for Human Rights, 2009.
Stefan Steiger/Sebastian Harnisch/Kerstin Zettl/Johannes Lohmann, Conceptualising Conflicts in Cyberspace, Journal of Cyber Policy, Vol. 3, Issue 1, 2018, S. 77.
Cass Sunstein, Incompletely Theorized Agreements in Constitutional Law, University of Chicago Public Law & Legal Theory Working Paper No. 147, 2007.
Kevin Townsend, China May Delay Vulnerability Disclosures For Use in Attacs, Securityweek, 2017, https://www.securityweek.com/china-may-delay-vulnerability-disclosures-use-attacks, (letzter Zugriff: 02.09.2019).
Nicholas Tsagourias, Non-State Actors, Ungoverned Spaces and International Responsibility for Cyber Acts, Journal of Conflict and Security Law, Vol. 21, Issue 3, 2016, S. 455.
Uppsala Conflict Data Program (UCDP), 2017, www.ucdp.uu.se/database, (letzter Zugriff: 02.09.2019).
UN GGE, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/70/174, 2015.
Brandon Valeriano/Ryan C. Maness, Cyber War Versus Cyber Realities: Cyber Conflict in the International System, 2015.
Brandon Valeriano/Ryan C. Maness, The Dynamics of Cyber Conflict between Rival Antagonists, 2001–11, Journal of Peace Research, Vol. 51, Issue 3, 2014, S. 347.
Mark Ward, Anti-Sec: Who are the world's most wanted hackers?, bbc, 2012, http://www.bbc.com/news/technology-17548704, (letzter Zugriff: 02.09.2019).
White House, National Security Strategy oft he United States, 2017, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf, (letzter Zugriff: 02.09.2019).
White House, Office of the Press Secretary, Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment, 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity, (letzter Zugriff: 02.09.2019).
White House, Office of the Press Secretary, FACT SHEET: President Xi Jinpings State Visit to the United States, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states, (letzter Zugriff: 02.09.2019).
White House, International Strategy for Cyberspace, 2011, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, (letzter Zugriff: 02.09.2019).
Robert D. Williams, The ‚China, Inc.+' Challenge to Cyberspace Norms, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 1803, 2018.
Samon Yuen, Becoming a Cyber Power: China's Cybersecurity Upgrade and its Consequences, China Perspectives, Vol. 2, 2015, S. 53.
Katharina Ziolkowski, General Principles of International Law as Applicable in Cyberspace, in: Katharina Ziolkowski (Hrsg.), Peacetime Regime for State Activities in Cyberspace – International Law, Foreign Affairs and Cyber-Diplomacy, Tallinn, 2013, S. 135.