NORMATIVE ORDERS

Cluster of Excellence at Goethe University Frankfurt/Main

Normative Orders Working Paper

01/2019

Die normative Ordnung der Cyber-Sicherheit: Zum Potenzial von Cyber-Sicherheitsnormen

Von Matthias C. Kettemann

Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI)
Hamburg

Exzellenzcluster „Die Herausbildung normativer Ordnungen"
Goethe-Universität Frankfurt am Main
www.normativeorders.net

matthias.kettemann@normativeorders.net

Inhaltsverzeichnis

Die normative Ordnung der Cyber-Sicherheit: Zum Potenzial von Cyber-Sicherheitsnormen

Von Matthias C. Kettemann

(Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI), Hamburg und Exzellenzcluster „Die Herausbildung normativer Ordnungen“, Goethe-Universität Frankfurt am Main)

Abstract: Dieses Working Paper zeigt Wege auf, wie völkerrechtlich verbindliche Regeln im Bereich der Cyber-Sicherheit entwickelt werden können. Wichtige Wegmarken können dabei nichtbindende Normen darstellen; auch aus Völkergewohnheitsrecht – besonders dem Kooperationsgebot – lassen sich präventive Schutzpflichten für Staaten (‚due diligence') ableiten. Diesen präventiven Schutzpflichten müssen Staaten mit gemeinsamem Handeln zur Hebung von Cyber-Sicherheit gerecht werden. Um langfristig Rechtssicherheit zu schaffen und Cyber-Sicherheit ganzheitlich zu fördern, führt aber kein Weg am Abschluss eines verbindlichen Übereinkommens über Cyber-Sicherheit vorbei.

1. EINFÜHRUNG

Zentraler Gehalt dieses Working Paper ist es aufzeigen, wie Völkerrecht Cyber-Sicherheit schützt und wie das Schutzniveau gehoben werden kann.[1] Neben der Ableitung von Pflichten mit Bezug auf Cyber-Sicherheit aus Völkergewohnheitsrecht wird die Verabschiedung eines Übereinkommens über Cyber-Sicherheit vorgeschlagen, um die Rechtssicherheit zu erhöhen und Cyber-Sicherheit langfristig zu schützen.

Zunächst wird Cyber-Sicherheit konzeptuell analysiert und eine holistische Definition vorgeschlagen (2.). Sodann wird der völkerrechtliche Rahmen von Cyber-Sicherheit geklärt (3.), wobei insbesondere auf Völkervertragsrecht, Völkergewohnheitsrecht und Allgemeine Prinzipien des Völkerrechts eingegangen wird. Schließlich arbeitet das Working Paper drei Ansätze aus, Cyber-Sicherheit im Völkerrecht stärker zu verankern und zu institutionalisieren (4). An ein Fazit (5) reiht sich ein Vorschlag für Cyber-Sicherheitsnormen.

[1] Dieses Working Paper beruht auf einer Studie des Autors für die Deutsche Telekom. Teile der Studie sind in englischer, aktualisierter Form eingeflossen in die Beiträge: Kettemann, “This is Not a Drill”: International Law and Protection of Cybersecurity, in Wagner/Kettemann/Vieth (Hrsg.), Research Handbook of Human Rights and Digital Technology (Cheltenham: E. Elgar, 2019), 113-128 und Kettemann, Ensuring Cybersecurity Through International Law’ (2017), Revista Española de Derecho Internacional (2017), 281-90.

2. CYBER-SICHERHEIT

Ein umfassendes Konzept der Cyber-Sicherheit

Cyber-Sicherheit ist zentrales Schlagwort der Internetpolitik[2] und eng verknüpft mit der Stabilität, Robustheit, Resilienz und Funktionalität des Internets.[3] Cyber-Sicherheit kann bedroht werden durch Cyber-Kriminalität und Cyber-Terrorismus, aber auch durch mangelnde rechtliche und technische Kooperation zwischen Staaten und fehlende präventive Maßnahmen, wie die Entwicklung von Kriseninterventionszentren und -teams sowie transnationaler Krisenkommunikationsstrukturen für Cyber-Vorfälle.

Ein Drittel der Weltbevölkerung verfügt über Internetzugang; mit dem Internet der Dinge werden sich der Cyberraum und die vernetzten Geräte exponentiell vergrößern. Die Debatte über die Gewährleistung von Cyber-Sicherheit ist daher gerade jetzt mit großem Nachdruck zu führen. Cyber-Sicherheit wird von Staaten teils sehr weit verstanden und umfasst Risiken und Bedrohung wie Cyber-Kriegsführung, Cyber-Konflikte, Cyber-Terrorismus, Cyber-Kriminalität und Cyber-Spionage.[4] Zweifellos ist Cyber-Sicherheit zu einem wichtigen Teil nationaler Innen-, Sicherheits-, Außen- und Verteidigungspolitik geworden.

Die Förderung und die Gewährleistung von Cyber-Sicherheit sind Voraussetzung für den ruhigen Lauf nationaler volkswirtschaftlicher Prozesse und des internationalen Wirtschafts- und Finanzsystems, transnationaler Kommunikationsflüsse, für das Funktionieren von Energienetzen, die Realisierung von Menschenrechten, die Leistungsfähigkeit nationaler, regionaler und internationaler Verteidigungsinfrastrukturen und schließlich Voraussetzung für die volle Realisierung aller Menschenrechte.[5]

---

[2] Adam Segal, The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (New York: Public Affairs, 2016).
[3] Eneken Tikk-Ringas (ed.), Evolution of the Cyber Domain: The Implications for National and Global Security, (London: Routledge, 2015).
[4] Hannes Ebert, Tim Maurer, Cyber Security, Oxford Bibliographies, 11.1.2017.
[5] Am Beispiel der Meinungsäußerungsfreiheit wird dies illustriert in Kettemann/Benedek, Freedom of Expression Online, in Suusi (Hrsg.), Human Rights, the Digital Society and Law: A Research Companion (London: Routledge, 2019) (i.E.)

Zu oft wird (Cyber)Sicherheit als Gegenstück von (Internet)Freiheit konzipiert. Dieser Ansatz ist verfehlt. Wie die Cyber-Sicherheitsstrategie für Deutschland 2016 betont, zählt gerade die Gewährleistung von Freiheit *und* Sicherheit zu den Kernaufgaben des Staates – offline wie online: „Aufgabe des Staates ist es daher, die Bürgerinnen und Bürger und Unternehmen in Deutschland gegen Bedrohungen aus dem Cyber-Raum zu schützen sowie Straftaten im Cyber-Raum zu verhindern und zu verfolgen.“ [6]

Die Cyber-Sicherheitsstrategie für Deutschland definiert Cyber-Sicherheit als „IT-Sicherheit der im Cyber-Raum auf Datenebene vernetzten bzw. vernetzbaren informationstechnischen Systeme“, wobei IT-Sicherheit als „Unversehrtheit der Authentizität, Vertraulichkeit, Integrität und Verfügbarkeit eines informationstechnischen Systems und der darin verarbeiteten und gespeicherten Daten“[7] verstanden wird. Diese Definition ist sehr technikorientiert und greift zu kurz im Lichte des täglich von Wirtschaft und Gesellschaft gelebten Verständnisses von Cyber-Sicherheit. Die Sicherheit im Internet und des Internets kann nicht mit einer Sicherheit von Systemen und Daten gleichgesetzt werden. Richtigerweise muss Cyber-Sicherheit holistisch verstanden werden. Der hier vertretene Ansatz steht Bedrohungsszenarien präventiv statt reaktiv gegenüber, sucht nach umfassenden statt sektoralen Antworten auf Bedrohungen und strebt nach möglichst umfassender Partizipation der verantwortlichen Akteure. Jedes sinnvolle Konzept der Cyber-Sicherheit sollte ein umfassendes und wertebasiertes sein: ein Bemühen um ein stabiles, sicheres, resilientes, funktionsfähiges, offenes und freies Internet und dessen Schutz vor staatlichen wie privaten Angriffen aller Art.[8]

Der Staat kann seiner Aufgabe zu den Bedingungen der Informationsgesellschaft nur gerecht werden, wenn er für alle Akteure auch im Cyberraum „Schutz und Freiheit zur Entwicklung bietet und hierfür seine eigenen Systeme ausreichend sichert.“[9] Dies gilt für jeden Staat. Daher haben alle Staaten ein Interesse an der Erhöhung von Cyber-Sicherheit.

[6] Bundeministerium des Innern, Cyber-Sicherheitsstrategie für Deutschland 2016, https://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cybersicherheitsstrategie-2016.pdf, 8.
[7] Cyber-Sicherheitsstrategie für Deutschland 2016, 24.
[8] Vgl. Marietje Schaake und Mathias Vermeulen, Towards a values-based European foreign policy to cybersecurity, Journal of Cyber Policy 1 (2016) 1, 75-84.
[9] Cyber-Sicherheitsstrategie für Deutschland 2016, 8.

Cyber-Sicherheit liegt im Gemeinschaftsinteresse aller Staaten

Auch wenn die Definitionen von Cyber-Sicherheit auseinander driften, liegt Cyber-Sicherheit im Gemeinschaftsinteresse aller Staaten. Dieses Gemeinschaftsinteresse ist mehr als die simple Summe aller Einzelinteressen; sie ist vielmehr ihre Querschnittmenge. Liegt ein Schutzgut im Gemeinschaftsinteresse, ergeben sich daraus völkerrechtlich relevante Rechtsfolgen. Daher sind Staaten nach Maßgabe ihrer Jurisdiktionsgewalt über für Cyber-Sicherheit relevante kritische Infrastrukturen hinsichtlich dieser der internationalen Gemeinschaft gegenüber verantwortlich. Dies lässt sich nicht zuletzt aus den Berichten der einflussreichen Group of Governmental Experts (GGE) der Vereinten Nationen für Entwicklungen im Feld der Information und Telekommunikation im Kontext von Informationssicherheit ableiten, die sich kooperativen regelbasierten Maßnahmen zur Bekämpfung von Online-Gefahren auf internationaler Ebene widmet und an der sich Deutschland intensiv beteiligt.[10]

Schon 2013 hielt die GGE fest, dass die Anwendung von Normen, die aus dem bestehenden Völkerrecht abgeleitet werden, „essenziell" ist, um Risiken für den Weltfrieden und die internationale Sicherheit und Stabilität zu minimieren.[11] Cyber-Sicherheit ist im Lichte der informationstechnologischen Herausforderungen inzwischen ein Aspekt des „Weltfriedens".[12] Für die Analyse des völkerrechtlichen Schutzes von Cyber-Sicherheit von besonderer Bedeutung ist der Bericht der GGE von 2015,[13] der im Konsens von einer repräsentativen Gruppe von staatlichen Experten angenommen wurde, die unter anderem China, Deutschland, Russland und die USA umfasste.[14] Zu den für die Cyber-Sicherheit essenzielle Aussagen des Berichts, der im Wesentlichen geltendes Völkerrecht wiedergibt, können gezählt werden, dass Staaten die Jurisdiktion über die informations- und kommunikationstechnologische (IKT)-Infrastruktur in ihrem Territorium verbleibt; dass Staaten in der Nutzung von Information- und Kommunikationstechnologien

[10] Für eine Dokumentation der Berichte einzelner Staaten siehe Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, http://www.un.org/disarmament/topics/informationsecurity.
[11] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98 vom 24.6.2013, Abs. 16.
[12] Ibid.
[13] Developments in the field of information and telecommunications in the context of international security, Report of the Secretary-General, A/70/174 vom 22.7.2015, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174 (im Folgenden: „GGE-Bericht (2015)").
[14] Mitglieder: Belarus, Brasilien, China, Kolumbien, Ägypten, Estland, Frankreich, Deutschland, Ghana, Israel, Japan, Kenia, Malaysia, Mexiko, Pakistan, Russische Föderation, Spanien, Vereinigtes Königreich und USA.

neben anderen Prinzipien des Völkerrechts jene der staatlichen Souveränität, souveränen Gleichheit, friedlichen Streitbeilegung und das Interventionsverbot respektieren müssen; dass das Internet bestehende völkerrechtliche Verpflichtungen, insbesondere hinsichtlich des Schutzes von Menschenrechten und Grundfreiheiten, unberührt lässt; und dass die internationale Gemeinschaft danach strebt, das Internet auf friedliche Weise „for the common good of mankind" zu regulieren. Daraus ergibt sich, dass Aspekte von Cyber-Sicherheit durch Völkerrecht geschützt werden (siehe 3.); das Schutzniveau kann aber noch bedeutend gehoben werden (siehe 4.).

3. CYBER-SICHERHEIT UND VÖLKERRECHT

Völkerrecht und Internet

Technologischer Fortschritt zieht rechtliche Innovationen mit sich. Nur zwölf Jahre nachdem Samuel Morse 1838 den Telegraphen vorgestellt hatte, gründeten Österreich, Preußen, Bayern und Sachsen mittels eines völkerrechtlichen Vertrags den Deutsch-Österreichischen Telegraphenverein.[15] Die Regulierung internationaler Informations- und Kommunikationsflüsse durch das Völkerrecht hat also eine lange Tradition. In der Tat ist auch das Völkerrecht das einzige Rechtsgebiet, mit dem globale (öffentliche) Güter verwaltet werden, das globale öffentliche Interesse geschützt wird und über Verteilungsfragen entschieden werden kann.[16]

Die Ubiquität und grenzenlose Natur der Technologie, auf der das Internet beruht, macht eine nur *einzelstaatliche* Regulierung wirkungsarm; außerdem läuft ein Vertrauen auf nur nationale Regelungen auf die Gefährdung der Integrität des Internets als Grundvoraussetzung für die Cyber-Sicherheit hinaus. Völkerrecht ist nötig, um Cyber-Sicherheit, die im Gemeinschaftsinteresse aller Staaten liegt, legitim und effektiv zu sichern. Das ist keine neue Erkenntnis.[17] Der Konsens der Staaten der Welt hinsichtlich

[15] Staatsvertrag zwischen Oesterreich, Preußen, Baiern und Sachsen vom 25. Juli 1850 über die Bildung des deutsch-österreichischen Telegraphenvereins, Allgemeines Reichs-Gesetz und Regierungsblatt für das Kaiserthum Österreich, No. CXXVII of 30 September 1850, 266 et seq.

[16] Vergleiche ausführlicher: Matthias C. Kettemann, Völkerrecht in Zeiten des Netzes: Perspektiven auf den effektiven Schutz von Grund- und Menschenrechten in der Informationsgesellschaft zwischen Völkerrecht, Europarecht und Staatsrecht (Bonn: Friedrich-Ebert-Stiftung, 2015), http://library.fes.de/pdf-files/akademie/12068.pdf.

[17] Developments in the field of information and telecommunications in the context of international security,

der Bedeutung von Völkerrecht für die Gestaltung des Internets wird schon in den Schlusserklärungen der Weltgipfel zur Informationsgesellschaft 2003 (Genf) und 2005 (Tunis) sichtbar. In der *Geneva Declaration of Principles* von 2003 (bestätigt im *Tunis Commitment* von 2005[18]) drücken Staaten ihren Wunsch aus,

> to build a people-centred, inclusive and development-oriented Information Society, […] enabling individuals, communities and peoples to achieve their full potential in promoting their sustainable development and improving their quality of life, *premised on the purposes and principles of the Charter of the United Nations and respecting fully and upholding the Universal Declaration of Human Rights*.[19]

Ohne einen legitimen und effektiven völkerrechtlichen Schutz der Cyber-Sicherheit können Individuen und Gesellschaften nicht ihr volles Potenzial entwickeln. Eine ähnliche Selbstverpflichtung auf eine völkerrechtlich gegründete Internetpolitik legte 2014 die Europäische Kommission vor.[20] Völkerrecht ist das zentrale Medium des Interessensausgleichs in den internationalen Beziehungen. Das Prinzip der Völkerrechtsfreundlichkeit des Grundgesetzes ist auch von diesem Gedanken getragen.[21]

Cyber-Sicherheit im Völkervertragsrecht

Das Völkerrecht ist in seiner Gänze auf das Internet anzuwenden.[22] Die Gesamtheit der Normen, die anwendbar sind, können wir als Völkerrecht des Netzes oder Internetvölkerrecht bezeichnen. Einzelnormen aus der Satzung der Vereinten Nationen (wie das Gewalt- und Interventionsverbot) sind für das Völkerrecht der Cyber-Sicherheit

---

A/RES/53/70 vom 4.1.1999, Abs. 2 lit. c, http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70.
[18] WSIS, Tunis Commitment, WSIS-05/TUNIS/DOC/7-E, 18 November 2005, Abs. 2.
[19] WSIS, Geneva Declaration of Principles (2003), Abs. 1 (Hervorhebung des Verfassers).
[20] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Internet-Politik und Internet-Governance. Europas Rolle bei der Mitgestaltung der Zukunft der Internet-Governance, COM/2014/072 final.
[21] Christian Tomuschat, Staatsrechtliche Entscheidung für die internationale Offenheit, in Isensee/Kirchof (Hrsg.), HStR XI^3 (2013), § 226 Rz 4.
[22] Der Rahmen dieser Studie erlaubt nicht, im Detail auf alle anwendbaren völkerrechtlichen Rechtssätze einzugehen. Vgl Michael N. Schmitt und Liis Vihul, The Nature of International Law Cyber Norms, Tallinn Paper No. 5 (NATO CCD COE), 2014, 16, https://ccdcoe.org/sites/default/files/multimedia/pdf/Tallinn%20Paper%20No%20%205%20Schmitt%20and%20Vihul.pdf; Katharina Ziolkowski, General Principles of International Law as Applicable in Cyberspace, in Katharina Ziolkowski (Hrsg.), Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy (Tallinn: NATO CCD COE Publications, 2013), 135-184 (151-152).

relevant.[23] Allerdings besteht kein einzelner Vertrag, der sich zentral mit der Regulierung des Internets und dem Signum der Cyber-Security beschäftigt. Zwar schaffen (zumal in den Augen mächtiger bzw. traditionellen Souveränitätskonzepten verbundener Staaten) Verträge (Rechts)Sicherheit,[24] doch sind bilaterale Cyber-Sicherheitsverträge angesichts der Universalität des Internets regelmäßig unterkomplex[25] und multilaterale Verträge nur in langwierigen Verhandlungsprozessen mit unsicherem Ausgang zu erarbeiten. Dennoch wird ein solcher hier empfohlen.[26] Der Erfolg des Europarats-Übereinkommens gegen Cyberkriminalität (Budapest Convention)[27] zeigt einen gangbaren Weg auf.[28]

Anerkennend, dass „die Staaten und die Privatwirtschaft bei der Bekämpfung der Computerkriminalität zusammenarbeiten [...] müssen“, einigten sich die Staaten in dem 2001 abgeschlossenen Übereinkommen auf innerstaatlich zu treffende Maßnahmen (in staatliches Recht zu übersetzende Straftatbestände), Verfahrensregeln und Regeln zur internationalen Zusammenarbeit. Mit 53 Ratifizierungen, darunter 10 von Nichtmitgliedstaaten des Europarates (Kanada, USA, Japan, Australien, Senegal, Israel ...), ist das Übereinkommen auch über den europäischen Rechtsraum hinaus normativ einflussreich geworden. Strafrechtspflege gehört zu den zentralen Kompetenzen jedes Staates; sie kann nur behutsam völkerrechtlich geregelt werden. Auch stellten sich bei der Ausarbeitung der Konvention komplexe Fragen der Abwägung von Menschenrechten und der internationalen Zusammenarbeit. Der Erfolg der Konvention kann als Indiz dafür verbucht werden, dass völkerrechtliche Verträge zu komplexen Themen mit Internetbezug weiterhin einen sinnvollen normativen Ansatz darstellen.

---

[23] Siehe dazu gleich 3.3. Gewaltverbot und Interventionsverbot haben eine völkervertragsrechtliche Basis, stellen aber auch Völkergewohnheitsrecht dar.

[24] Heise.de, USA und China wollen Vertrag zur Begrenzung von Cyberangriffen, 20.9.2015, http://www.heise.de/ newsticker/meldung/USA-und-China-wollen-Vertrag-zur-Begrenzung-von-Cyberangriffen-2822083.html#mobile_detect_force_desktop.

[25] Vgl. Jack Goldsmith, Cybersecurity Treaties. A Skeptical View, Hoover Institution Future Challenges Essays (2011), http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf und Robert S. Litwak und Meg King, Arms Control in Cyberspace, Wilson Center Digital Futures Project (2015), https://www.wilsoncenter.org/publication/arms-control-cyberspace.

[26] Siehe unten 4.2.

[27] Budapest Convention (2001) des Europarates, Übereinkommen über Computerkriminalität (schweizerische Sprachfassung: Übereinkommen über die Cyberkriminalität), http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

[28] Dies besondes in einem Jahr, in dem Europa ein zentraler Internet Governance-Akteur geworden ist: Internet Governance, Matthias C. Kettemann, Wolfgang Kleinwächter, Max Senges, The time is right for Europe to take the lead in global internet governance: background report for the UN Secretary General's High-level Panel on Digital Cooperation, Normative Orders Working Paper 02/2018, http://publikationen.ub.uni-frankfurt.de/files/48008/Governance_Kettemann_Kleinwaechter_Senges.pdf.

Noch besteht kein Vertrag zu Cyber-Sicherheit. Verbindliche völkerrechtliche Konturierungen können daher nur aus Völkergewohnheitsrecht und Prinzipien des Völkerrechts abgeleitet werden.

Kristallisierung völkergewohnheitsrechtlicher Pflichten mit Relevanz für Cyber-Sicherheit

In der im Rahmen des UN-Weltgipfels zur Informationsgesellschaft (WSIS) verabschiedeten Tunis Agenda und der Verpflichtungserklärung von Tunis (2005) (aufbauend auf den Genfer Dokumenten von 2003) verpflichteten sich die Staaten der Welt zum Aufbau einer

> „den Menschen in den Mittelpunkt stellende[n], inklusive[n] und entwicklungsorientierte[n] Informationsgesellschaft […], gestützt auf die Ziele und Grundsätze der Charta der Vereinten Nationen, das Völkerrecht und den Multilateralismus sowie unter voller Achtung und Einhaltung der Allgemeinen Erklärung der Menschenrechte […],“[29]

wobei bekräftigt wird, dass „Menschenrechte und Grundfreiheiten, einschließlich des in der Erklärung von Wien verankerten Rechts auf Entwicklung, allgemein gültig und unteilbar sind, einander bedingen und miteinander verknüpft sind“;[30] zu einem stabilen und sicheren Internet als weltweite Einrichtung;[31] und zum Multistakeholderansatz. Für den Schutz von Cyber-Sicherheit durch Völkerrecht von besonderer Bedeutung sind das Bekenntnis zu Völkerrecht und die Bedeutung des Internets – stabil und sicher – als weltweite Einrichtung; ohne Cyber-Sicherheit ist dieses Ziel nicht zu erreichen. Die Erklärungen sind zwar formal nicht bindend, haben aber inzwischen eine wichtige Rolle eingenommen als erstes ausdrückliches Bekenntnis von Staaten zu zentralen Werten der Informationsgesellschaft.

Zum einen schützt der internationale Rechtsbestand Cyber-Sicherheit durch menschenrechtliche Schranken. Was Informations- und Kommunikationsverhalten im

[29] World Summit on the Information Society (WSIS), Tunis Commitment, WSIS-05/TUNIS/DOC/7-E vom 18.11.2005, Ziff. 2.
[30] Ebd. Ziff. 3.
[31] WSIS, Tunis Agenda für die Informationsgesellschaft, WSIS-05/TUNIS/DOC/6(Rev. 1)-G vom 18.11.2005, Ziff. 31.

Internet betrifft, sind Kommunikator, Rezipient und Kommunikationsinhalt durch die in Teilen gewohnheitsrechtlich abgesicherte Norm des Art. 19 des Zivilpakts abgesichert. Neben diesen großteils negativ konzipierten einzelmenschenrechtlich fundierten Pflichten des Staates sind aus den staatlichen Schutz- und Gewährleistungspflichten hinsichtlich der informations- und kommunikationsbezogenen Rechte auch positive Internet-Infrastrukturbezogene Pflichten ableitbar. Staaten müssen also für das Bestehen und die Sicherheit der Netze Sorge tragen.

Für die Gewährleistung und Förderung der Cyber-Sicherheit besonders relevant sind folgende völkerrechtliche Grundsätze,[32] die teils in der Charta in Form von Vertragsrecht gegossen wurden, teils völkergewohnheitsrechtlich geschützt sind und teils als Allgemeine Prinzipien des Völkerrechts auftreten: souveräne Gleichheit, Gewaltverbot, Interventions-verbot, friedliche Streitbeilegung, Menschenrechtsschutz, Kooperationsprinzip (das sich speist aus dem Grundsatz der guten Nachbarschaft (‚no harm') und dem Präventionsprinzip (‚due diligence').

Das Prinzip der souveränen Gleichheit (Art. 2 (1) UN Charta) ist ein zentraler Grundsatz des Völkerrechts. Als „pivotal principle"[33] ist es auch für die Cyber-Sicherheit von besonderer Bedeutung. Jeder Staat hat die Jurisdiktion und Gewalt über sein Territorium und über die IKT-Infrastruktur, die sich dort befindet; dies bedeutet aber auch, dass ein Staat Verantwortung dafür trägt, dass von seinem Territorium aus nicht Völkerrecht verletzende Attacken gegen andere Staaten oder Einrichtungen organisiert oder durchgeführt werden.

Darüber hinaus kann das Nichteingriffsprinzip (Artikel 2 (7) UN Charta) fruchtbar gemacht werden: eine intensive Beeinträchtigung des Funktionieren des Internets in einem anderen Staat (etwa durch Cyberangriffe) könnte eine Intervention darstellen, wobei sich hier regelmäßig Attributionsprobleme ergeben.[34] Nur wenige vom Territorium eines Staates ausgehende Attacken stellen eine ‚Intervention' im Sinne des Völkerrechts dar, weil sie regelmäßig von nichtstaatlichen Akteuren bzw. von Akteuren, die dem Staat nicht nachweislich zugerechnet werden können, ausgeführt werden. [35]

[32] GGE-Bericht (2015), Abs. 26.
[33] Samantha Besson, Sovereignty, in Rüdiger Wolfrum (ed.), MPEPIL (2008) (2011), para. 1.
[34] Sven-Hendrik Schulze, Cyber-"War", Testfall der Staatenverantwortlichkeit (Tübingen: Mohr, 2015).
[35] Der GGE-Bericht (2015) beschreibt klar die Probleme: "the indication that an ICT activity was launched or otherwise originates from the territory or the ICT infrastructure of a State may be insufficient in itself to

Das Gewaltverbot (Art. 2 (4) UN Charta) untersagt Staaten, über einfache ‚Eingriffe' hinausgehende Maßnahmen der Gewalt einzusetzen (erstere sind vom Nichteingriffs-prinzip erfasst); im Kontext des Internets wären nur besonders schwerwiegende Fälle von Cyberattacken mit substanziellen kinetischen Folgen angesprochen.

Das Prinzip der friedlichen Streitbeilegung ist für die Cyber-Sicherheit insofern relevant, als dass Staaten bei Vorfällen jedenfalls die Pflicht haben, zunächst den Sachstand zu ermitteln und Beweise für die Zurechnung eines Völkerrechtsverstoßes zu einem Staat zu sammeln. Selbst wenn dies gelingt, sind zunächst friedliche Mittel der Streitbeilegung anzustreben.

Das Prinzip des Menschenrechtsschutzes ist ein zentraler Grundsatz des Völkerrechts, der auch für Cyber-Sicherheit relevant ist. Völkerrechtlich problematisch sind etwa staatliche Versuche, Cyber-Sicherheit durch eine überschießende Kontrolle des Internets (etwa Aufbau und Einsatz von Überwachungskapazitäten oder staatliche Filterung aller Internetkommunikation) zu heben.

Das Prinzip der guten Nachbarschaft (Art. 74 UN Charta) (auch: ‚no harm'-Prinzip) kann im Internetzeitalter global verstanden werden. Ursprünglich nur für das Verhältnis von aneinander angrenzenden Staaten relevant, wurde das Prinzip graduell erweitert.[36] Im *Corfu Channel Case* beschrieb der Internationale Gerichtshof das Prinzip als „ […] every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States."[37] Das *no harm*-Prinzip hat seine Wurzeln in den *Trail Smelter*[38] und *Lac Lanoux*[39]-Fällen. Ausformuliert wurde es im Prinzip 21 der Stockholm Declaration (1972)[40] und Prinzip 2 der Rio Declaration (1992):[41] Staaten sind verpflichtet "to ensure

attribute the activity to that State. The Group noted that the accusations of organizing and implementing wrongful acts brought against States should be substantiated." (GGE-Bericht (2015), Abs. 28 (f)).

[36] Cf. UN GA Resolution 46/62, Developing and strengthening of good-neighbourliness between States, A/RES/46/62 of 9 December 1991, para. 2 (gute Nachbarschaft sei Pflicht, "whether or not they [die Staaten] are contiguous").

[37] IGH, Corfu Channel Case (UK v. Albania) 1949 ICJ Reports 4, 22.

[38] Trail Smelter Case, United States v Canada, First decision, (1949) III RIAA 1905, (1941) 35 AJIL 684, 16th April 1938, Arbitration.

[39] Lake Lanoux Arbitration, France v Spain, (1963) XII RIAA 281, (1961) 24 ILR 101, 16th November 1957, Arbitration.

[40] Stockholm Declaration of the United Nations Conference on the Human Environment (United Nations [UN]) UN Doc A/CONF.48/14/Rev.1, 3, UN Doc A/CONF.48/PC/6, Principle 21.

[41] Rio Declaration on Environment and Development (United Nations Environment Programme [UNEP]) UN Doc A/CONF.151/5/Rev.1, UN Doc A/CONF.151/26/Rev.1 Vol.1, Annex 1, Principle 2.

that activities within their jurisdiction or control do not cause damage to the environment of other States or of areas beyond the limits of national jurisdiction." Dies lässt sich unschwer von der Umwelt auf andere Regime übertragen.

Die Verpflichtung, grenzenüberschreitenden Schaden zu vermeiden, hat sich zu Gewohnheitsrecht kristallisiert. Vertragliche Bestätigung findet es in Art. 194 (2) der UN-Seerechtskonvention[42] und Art. 20 (1) des ASEAN Agreement on the Conservation of Nature and Natural Resources (1985). Zuletzt bestätigte der IGH im *Nuklearwafffen*-Fall,[43] die Bedrohung der Umwelt sei "no abstraction but represents the living space, the quality of life and the very health of human beings, including generations unborn." Kein Staat darf, dem *no harm*-Prinzip folgend, sein Territorium auf eine Weise nutzen, die anderen Staaten Schaden zufügt. In der präventiven Dimension des *no harm*-Prinzips muss ein Staat Maßnahmen setzen, um diese Gefährdungen zu verhindern. Daraus lässt sich unter anderem eine Verpflichtung zu einer entsprechenden Infrastruktur, zur Entwicklung von Notfallplänen und zum Aufbau einer internationalen Krisenkooperationsstruktur (und -kultur) ableiten.

Das Vorsorgeprinzip/Präventionsprinzip (‚due diligence') ist für die Cyber-Sicherheit von besonderer Bedeutung. Zunächst sind der *due diligence* Verpflichtungen zur Information und Konsultation zu entnehmen.[44] In der Wissenschaft ist es umstritten, inwiefern das Präventionsprinzip eine ‚due diligence'-Dimension hat oder ob die präventiven Verpflichtungen von Staaten durch das *no harm*-Prinzip operationalisiert werden. Es wurde vorgeschlagen, das Prinzip der guten Nachbarschaft ins Zentrum zu stellen und aus diesem Verfahrenspflichten zur Notifizierung und Konsultation hinsichtlich grenzenüberschreitender Schadensfälle abzuleiten. Das Prinzip findet völkervertragsrechtlich verschiedentlich eine Ausprägung. Art. 7 (1) des Übereinkommens über das Recht der nichtschifffahrtlichen Nutzung internationaler Wasserläufe[45] enthält eine Pflicht zur Setzung von "*all appropriate measures* to prevent the causing of significant harm to other watercourse States". Ähnlich bestimmt Art. 194 (2) des UNO-

[42] Seerechtskonvention der Vereinten Nationen, 10.12.1982, Art. 194 (2): "States shall take all measures necessary to ensure that activities under their jurisdiction or control are so conducted as not to cause damage by pollution to other States and their environment, and that pollution arising from incidents or activities under their jurisdiction or control does not spread beyond the areas where they exercise sovereign rights in accordance with this Convention."

[43] IGH, *Legality of the Threat or Use of Nuclear Weapons Advisory Opinion, ICJ Reports 1996,* p. 226, para. 29.

[44] Timo Koivurova, Due Diligence, in Wolfrum (ed.), MPEPIL (2008) (2010) [online], para. 3.

[45] Übereinkommen über das Recht der nichtschifffahrtlichen Nutzung internationaler Wasserläufe, 21.5. 1997.

Seerechtsübereinkommens:[46] Staaten haben zu setzen "*all measures necessary* to ensure that activities under their jurisdiction or control are so conducted as not to cause damage by pollution to other States and their environment". Auch für den Bereich des Kampfs gegen Terrorismus und Terrorismusfinanzierung wurde das *due diligence*-Prinzip fruchtbar gemacht.[47]

Mit einiger Berechtigung können dem *due diligence*-Prinzip daher entsprechende normative Leitlinien für die Regulierung der Cyber-Sicherheit entnommen werden. So obliegt Staaten eine auch durch dieses Prinzip gestützte Verpflichtung, Cyberattacken zu verhindern, die vom eigenen Territorium ausgehen und (präventiv) ein Rechtssystem aufzubauen, das Cyber-Sicherheit gewährleistet und fördert.[48] Diese können sie erfüllen etwa durch „passing stringent criminal laws, conducting vigorous investigations, prosecuting attackers, and, during the investigation and prosecution, cooperating with the victim-states of cyberattacks that originated from within their borders."[49]

Das *due diligence*-Prinzip in seiner präventiven Dimension hilft die Verpflichtungen von Staaten in Hinblick auf Cyber-Sicherheit herauszuarbeiten; dies insbesondere hinsichtlich Cyberkriminalitätsbekämpfung, globaler Kooperation und Kapazitätenaufbau. Cyber security due diligence wurde als Teil des Völkergewohnheitsrechts beschrieben, wobei sich wohl insbesondere die folgenden präventiven Verpflichtungen als völkerrechtliche Verpflichtungen stabilisiert haben:

- dass Regierungen und andere Akteure die Cyber-Sicherheit erhöhen und Cyber-Sicherheitsstrategien entwickeln, die kritische Infrastrukturen schützen;[50]

[46] UN Seerechtsübereinkommen von 1982 (1833 UNTS 397).
[47] Cf. Vincent-Joel Proulx, Babysitting Terrorists: Should States Be Strictly Liable for Failing to Prevent Transborder Attacks?, 23 Berkeley J. Int'l L. 615, 629 (2005).
[48] Michael N. Schmitt, In Defense of Due Diligence in Cyberspace, Yale Law Journal Forum 125 (2015), 68-81.
[49] Matthew J. Sklerov, Solving the Dilemma of State Responses to Cyberattacks: A Justification for the use of Active Defenses Against States Who Neglect Their Duty to Prevent, 201 Military Law Review (2009), 1-85 (62).
[50] Cf. UN GA Res 64/221, Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures, UN Doc. A/RES/64/211 of 17 March 2010 (mit Verweisen auf weitere Resolutionen, darunter Resolutions 55/63 of 4 December 2000 and 56/121 of 19 December 2001 on combating the criminal misuse of information technologies, 57/239 of 20 December 2002 on the creation of a global culture of cybersecurity and 58/199 of 23 December 2003 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001, 57/53 of 22 November 2002, 58/32 of 8 December 2003, 59/61 of 3 December 2004, 60/45 of 8 December 2005, 61/54 of 6 December 2006, 62/17 of 5 December 2007 und 63/37 of 2 December 2008 on developments with respect to information technologies in the context of international security.

- dass Staaten (und andere relevante Akteure) enger im Kampf gegen Cyber-Kriminalität und Cyber-Terrorismus zusammenarbeiten[51] und Verträge wie das Übereinkommen gegen Cyber-Kriminalität des Europarates ratifizieren;[52]
- dass Staaten Verträge zur Zusammenarbeit ihrer Polizeibehörden schließen;[53]
- dass Staaten vertrauensbildende Maßnahmen setzen und das Niveau des Informationsaustauschs erhöhen, sowohl generell als auch (und vor allem) im Falle von cyber-sicherheitsrelevanten Vorfällen.[54]

Vertrauensbildende Maßnahmen sind weiter reichend als dem Kooperationsgebot entspringende völkerrechtliche Verpflichtungen.[55] Allerdings sind sie insofern normativ relevant, also sie die Richtung der Entwicklung völkerrechtlicher Pflichten aufzeigen.[56]

No harm und *due diligence*-Prinzip sind wichtige Fundamente des Prinzips der zwischenstaatlichen Zusammenarbeit (Kooperationsprinzip). Letzteres kann nach Artikel 1 (3) UN Charta in seiner gewohnheitsrechtlichen Auslegung dergestalt weiterentwickelt werden, dass Staaten verpflichtet werden, sich in der Ausgestaltung ihrer nationalen Internetpolitik Cyber-Sicherheitsaspekte zu beachten und bei grenzüberschreitenden Implikationen bilaterale oder multilaterale Konsultationen anzustoßen. Vor Eintritt eines Schadensereignisses bestehen nachbarschaftliche Präventionspflichten; nach Eintritt eines Schadensereignisses begründen diese und das Kooperationsprinzip Zusammenarbeits- und Informationspflichten. [57] Als Vorwirkung dieser Pflichten kann die Einrichtung von Kommunikationsinfrastrukturen für Notfälle, von staatlichen Abwehrzentren und von Response Teams für Cyberattacken als völkerrechtlich geboten erscheinen. Schon die Draft Articles der International Law Commission on Prevention of Transboundary Harm von 2001[58] enthalten eine fortdauernde Pflicht zum Informationsaustausch, die für den Schutz der Cyber-Sicherheit – Cyberattacken sind ein

[51] Vgl. UNODC, Resolution 22/8 Promoting technical assistance and capacity building to strengthen national measures and international cooperation against cybercrime, UNODC/CCPCJ/2013/RES/22/8, para. 4.
[52] Vgl. 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/68/98 of 24 June 2013, para. 22
[53] GGE (2013), para. 22.
[54] GGE (2013), para 26 et seq.
[55] Organization for Security and Co-operation in Europe, Decision No. 1202: OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies, PC.DEC/1202 (10 March 2016).
[56] Cf. Katharina Ziolkowski, Confidence Building Measures for Cyberspace, in Ziolkowski (ed.) (2013), 533-564.
[57] Christian Walter, Cyber Security als Herausforderung für das Völkerrecht, JZ 2015, 685-736.
[58] ILC Draft Articles, Prevention of Transboundary Harm from Hazardous Activities (2001), Official Records of the General Assembly, Fifty-sixth Session, Supplement No. 10 (A/56/10).

klassischer Fall von *transboundary harm* – einschlägig ist. Daraus lässt sich auch eine Verpflichtung zur Errichtung eines global-interoperablen Lagebildes ableiten, damit Staaten untereinander Wissen und Best Practices abgleichen und Gefährdungstendenzen und -herde frühzeitig identifizieren können.[59]

Nichtbindende Nomen im Internetvölkerrecht

Die Normen des Internets bestehen nicht nur aus nationalem, regionalem und internationalem Recht, sondern auch aus nichtrechtlichen Normen. Gerade die Dynamik der Multistakeholderprozesse in der Internetregulierung führt dazu, dass *soft law* und Instrumente der Selbstregulierung im Internet vorherrschen. Sowohl ‚Cyber-Normen' als auch ‚Prinzipien' (nicht zu verwechseln mit den oben diskutierten Grundsätzen des Völkerrechts) sind für die normative Entwicklung des Internets relevant.

Cyber-Normen sind von der Wissenschaft und Nichtregierungsorganisationen[60] und Unternehmen als normativer Ansatz zur einer granulareren Regulierung des Internets in die Debatte eingebracht worden. Prinzipien (oder Grundsätze) der Internet Governance haben sich seit 2011 als wichtiges Instrument der Internetpolitik entwickelt.[61] 2014 wurden die wichtigsten Grundsätze der Internet Governance in der NETmundial Erklärung (Prinzipien von Sao Paolo) zusammengefasst.[62]

Der Hauptvorteil von Prinzipien liegt in der Offenheit ihrer Formulierung und ihrer Anschlussfähigkeit. Negativ zu bewerten sind die Schwierigkeiten bei der Umsetzung bzw. der Entwicklung konkreter normativer Ansätze aus diesen. Hier können „Normen"

[59] Siehe unten 4.3.
[60] Martha Finnemore, Cultivating International Cyber Norms, in Kristin M. Lord und Travis Sharp (Hrsg.), America's Cyber Future: Security and Prosperity in the Information Age (Washington, DC: Center for a New American Security, 2011), 89-101; Roger Hurwitz (Hrsg.), A Call to Cyber Norms: Discussions at the Harvard–MIT–University of Toronto Cyber Norms Workshops (Cambridge, MA: Belfer Center for Science and International Affairs, 2015); Anna-Maria Osula, and Henry Rõigas (Hrsg.), International Cyber Norms: Legal, Policy & Industry Perspectives (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2016); Mika Kerttunen and Saskia Kiisel, Norms for International Peace and Security: The Normative Frameworks of International Cyber Cooperation (ICT4Peace Norms Project, GCCS), 2015.
[61] Siehe Matthias C. Kettemann, Grotius goes Google: Der Einfluss der Internet Governance auf das Völkergewohnheitsrecht, in Christoph Vedder (Hrsg.), Tagungsband 37. Österreichischer Völkerrechtstag 2012, (Wien: Peter Lang Verlag, 2013), 89-104. Einflussreich war die Erklärung des Ministerkomitees des Europarates über die Grundsätze der Internet Governance vom 21.5.2012.
[62] NETmundial, NETmundial Multistakeholder Statement, 24.4.2014, http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf: Sie bestehen aus „gemeinsamen Prinzipien" und „wichtigen Werten", die beitragen zu einem „inclusive, multistakeholder, effective, legitimate, and evolving Internet governance framework".

erheblich mehr Lenkungskraft entwickeln.[63] So brachte die deutsche Regierung 2015 in ihrem Schreiben an die GGE zum Ausdruck, dass die im GGE-Bericht enthaltenen nichtbindenden Normen Erwartungen definieren und formen können.[64] Die von der GGE ausgearbeiteten Normen seien die „minimum baseline that guides responsible state behavior in cyberspace.“[65]

4. Perspektiven der Verstetigung von Cyber-Sicherheitsnormen

Das Legitimation-Plus des Multistakeholder-Modells[66]

Jeder völkerrechtlichen Verankerung von Cyber-Sicherheit voranzustellen ist die Feststellung, dass in der normativen Entwicklung des Völkerrechts des Internets der Multistakeholder-Ansatz bedeutsam ist. Seit dem Bestehen der Weltgipfel zur Informationsgesellschaft bekennen sich die Staaten mit wenigen Ausnahmen zur Integration aller Stakeholder in für die Internetregulierung relevanten normativen Prozessen. Der Multistakeholderansatz findet seine Verwirklichung in der Entwicklung und Anwendung durch Regierungen (Staaten), den Privatsektor (Unternehmen) und die Zivilgesellschaft (Individuen) „in ihren jeweiligen Rollen“ von Instrumenten und Prozessen zur Regelung des Internets. [67]

Durch die derart erzielte Bündelung der legitimationsstiftenden Wirkung der Beteiligung von Staaten, dem Privatsektor und der Zivilgesellschaft (Input-Legitimität) und Verfahren, die eine gleichberechtigte Interaktion in Regelungsprozessen ermöglichen (Throughput-Legitimität), sind auch die Regelungsergebnisse besonders legitim (Output-Legitimität). Die Regelungsergebnisse von Internet Governance-Prozessen sind aufgrund ihrer Legitimität auch im Großen und Ganzen effektiv, was wiederum ihre Legitimität befördert. Während klassische völkerrechtliche Verträge formale Bindungswirkung entfalten können,

[63] Rolf H. Weber, Principles for governing the Internet, A comparative analysis (Paris: UNESCO, 2015), http://unesdoc.unesco.org/images/0023/002344/234435e.pdf.
[64] Germany, Report on Developments in the Field of Information and Telecommunications in the Context of International Security (RES 69/28), https://unoda-web.s3.amazonaws.com/wp-content/uploads/2015/08/GermanyISinfull.pdf.
[65] Ibid., Abs. 13.
[66] Vgl. Matthias C. Kettemann, *Kettemann*, Internet Governance, in Jahnel et al. (Hrsg.), Internetrecht, 4. Auflage (Wien: Springer, 2019) (i.E.)
[67] WSIS, Tunis Agenda für die Informationsgesellschaft, WSIS-05/TUNIS/DOC/6(Rev. 1)-G vom 18.11.2005, Ziff. 31.

sind in Multistakeholderprozessen entstandene Normen in der Regel formal nicht bindend, aber dennoch einflussreich aufgrund der Besonderheiten des Normenproduktions-prozesses. Um verbindliche und dennoch von allen Stakeholdergruppen als legitim angesehene Normen zu entwickeln, sollten Aspekte des Multistakeholderansatzes in jeder Phase der Entwicklung eines Vertrages mitgedacht werden.

Verrechtlichung von Cyber-Sicherheitsnormen

Normative Interventionen in politischen Prozessen: Multistakeholderforen sind denkbar schlecht geeignet zur Entwicklung von bindendem Völkerrecht. In ihnen können Staaten (oder andere Akteure) lediglich normativ relevante Vorarbeiten leisten. Die Entwicklung von ‚Cyber-Sicherheitsnormen' und deren Präsentation in einem Forum wie der G20 hat zwar keine formale Bedeutung, kann aber den Anfangspunkt eines völkerrechtlichen Verrechtlichungsprozesses darstellen, an dessen Ende ein Übereinkommen über Cyber-Sicherheit steht. ‚Normen' gemeinsam zu diskutieren, kann sinnvoll sein, da schon in der Diskussion gemeinsame Werte ausgedrückt werden[68] und die von Staaten eingenommenen Positionen als Indizien für ihre Haltung zu einer völkerrechtlichen Juridifizierung von Cyber-Sicherheit darstellen können.

Als erster Schritt könnte daher in dem G20-Prozess normativ interveniert werden, um Cyber-Sicherheitsnormen in der Schlusserklärung der nächsten G20-Konferenz zu thematisieren, Cyber-Sicherheit als permanenten Tagesordnungspunkt zu verankern sowie als Querschnittsmaterie zu beachten bzw. mitzubehandeln.

Entwicklung eines Framework of Commitments: Auch ein multistakeholderbasiertes *Framework of Commitments* könnte die globale Debatte über Cyber-Sicherheit befeuern. Um Cyber-Sicherheitsnormen mittelfristig zu verankern, ist deren Präzisierung angebracht. Dies kann im Rahmen eines Multistakeholderverfahrens erfolgen, an dessen Ende ein *Framework of Commitments* als normatives ‚Vehikel' zur zunehmenden Verrechtlichung von Cyber-Sicherheitsnormen steht. Methodisch läuft die Annahme eines *Framework of Commitments* so ab, dass zunächst eine Arbeitsgruppe aus Vertretern aller Stakeholder unter Beteiligung von Vertretern der Wissenschaft gebildet wird. Diese präzisiert dann in

[68] Vgl. Eneken Tikk-Ringas, International Cyber Norms Dialogue as an Exercise of Normative Power, Georgetown Journal of International Affairs (2017) (i.E.), http://ict4peace.org/wp-content/uploads/2017/02/Tikk-Normative-Power.pdf.

einem offenen Verfahren *Commitments* in Form von Normen, die dann veröffentlicht bzw. angenommen werden. Die Annahme kann im *rough consensus* oder im Rahmen einer Schlusserklärung erfolgen.

Weiterentwicklung des Gewohnheitsrechts: Völkergewohnheitsrecht entwickelt sich nur langsam weiter. Statements von Staaten in internationalen normativen Prozessen sind hier von großer Bedeutung als Indizien für Rechtsüberzeugung. Auch die Staatenpraxis muss beobachtet werden.

Verankerung von Cyber-Sicherheit in einem völkerrechtlichen Vertrag: Langfristig am vielversprechendsten zur Verankerung von völkerrechtlich verbindlichen Normen zur Cyber-Sicherheit ist die Verhandlung und Annahme eines völkerrechtlichen Vertrags. Ein solcher verbleibt der ‚gold standard' des Völkerrechts und die wichtigste Rechtsquelle. Die am 4. November 2016 in Kraft getretene Klimarahmenkonvention der Vereinten Nationen[69] hat bewiesen, dass selbst heute noch zu komplexen Themen völkerrechtliche Verträge zur Regulierung globaler Allgemeingüter (wie es auch die Cyber-Sicherheit als Vorbedingung der Funktionalität des Internets ist) erfolgreich abgeschlossen werden können.

Der Weg zu einem Vertrag ist steinig. Angesichts des großen Erfolgs des Übereinkommens gegen Cyber-Kriminalität scheint dieses ein normatives Vorbild zu sein. In der Tat wirkt der Europarat als vielversprechender Ort zur Etablierung – zunächst – eines Komitees, das Vorarbeiten zur Cyber-Sicherheit leisten würde. Dieses würde dann in ein Konventionskomitee umgewandelt werden, das ein Übereinkommen ausarbeitet. Ein solches würde schließlich den Mitgliedstaaten vorgelegt werden, wobei (wie bei der Budapest Convention) selbstverständlich keine geografische Beschränkung erfolgen würde.

Ein derartiges Übereinkommen über Cyber-Sicherheit (Cybersecurity Convention) hat durchaus Erfolgsaussichten. Alternativ wäre ein Prozess zur Ausarbeitung eines entsprechenden Vertrages auch auf Ebene der Vereinten Nationen möglich. Allerdings ist Cyber-Sicherheit ein höchst umstrittenes Thema; und schon das Mandat für ein entsprechendes Verfahren würde absehbar zu politischen Konflikten führen. Ein 2015 aktualisiert vorgelegter „Code of Conduct for Information Security" von sechs Mitgliedern

[69] UN Framework Convention on Climate Change, http://unfccc.int/2860.php.

der Shanghai Cooperation Organization wurde sehr kritisch aufgenommen.[70] Ein regionaler Ansatz kann normative Konflikte in der Erarbeitungsphase verringern, und die geografische Offenheit des Vertrages ermöglicht nach dessen Finalisierung den Anschluss auch anderer Staaten. Diese müssten allerdings – zumindest als Observer – neben anderen Akteuren der Multistakeholderstruktur an passenden Stellen an der Entwicklung des Vertrages teilhaben können, um die Ratifizierungschancen zu erhöhen.

Institutionalisierung von Cyber-Sicherheitsnormen

Zunächst bzw. unabhängig von normativen Ansätzen lässt sich aus dem Kooperationsprinzip in dessen präventiver Dimension die Verpflichtung zur Entwicklung eines global-interoperablen Lagebildes gewinnen. Dieses könnte, wie auch ein Cyber-Sicherheitszentrum, in einem ersten Schritt bei der OECD angesiedelt werden, um den sinnvollerweise im Rahmen des Europarates durchzuführenden normativen Prozess nicht zu überfrachten.

Um für die Umsetzung der Cyber-Sicherheitsnormen langfristig Sorge zu tragen und europaweit Kompetenzen aller Stakeholder im Bereich der Cyber-Sicherheit aufzubauen, erscheint auch die Gründung eines Cyber-Sicherheitszentrums bei der OECD sinnvoll. Dieses würde sich unter anderem der Erhöhung von Cyber-Sicherheit sowie der Bekämpfung von Cyberkriminalität vor dem Hintergrund ihrer schädigenden Dimension für die Wirtschaft widmen. Als Vorbild kann das NATO Cooperative Cyber Defence Centre of Excellence in Tallinn dienen,[71] das Cyber-Sicherheit aus primär militärischer Perspektive erforscht und mit den Tallinn Manuals bahnbrechende Studien zur Anwendbarkeit des Völkerrechts in Kriegs- und Friedenszeiten herausgegeben hat. Entsprechende Studien zur Hebung von Cyber-Sicherheit und zur Verantwortung der Stakeholder könnten im Rahmen eines *OECD Cybersecurity Cooperation Center (OECD C3)* durchgeführt werden. Ein derartiges Zentrum könnte Fortschrittsberichte sammeln und Best Practices und Modellregularien veröffentlichen.

[70] International code of conduct for information security, Annex to Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, UN Doc. A/69/723 vom 13.1.2015, https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf.
[71] NATO Cooperative Cyber Defence Centre of Excellence, https://ccdcoe.org.

5. FAZIT

Im Lichte der Bedeutung des Internets für Staat, Wirtschaft und Gesellschaft ist Cyber-Sicherheit als Vorbedingung eines funktionierenden und sicheren Internets zu einem Schutzgut im globalen Gemeinschaftsinteresse geworden. Cyber-Sicherheit ist umfassend zu verstehen als Bemühen aller Akteure um ein stabiles, sicheres, resilientes, funktionsfähiges, offenes und freies Internet. Cyber-Sicherheit umfasst innen- wie außenpolitische Dimensionen und spricht menschliche Sicherheit, nationale Sicherheit und internationale Sicherheit an.

Das Völkerrecht ist vollumfänglich auf das Internet anzuwenden und konturiert daher auch die Cyber-Sicherheit. Besonders das Völkergewohnheitsrecht und die Allgemeinen Rechtsprinzipien des Völkerrechts beschränken (und befähigen) nationale Internetpolitik. Insbesondere bestehen dem Völkergewohnheitsrecht entfließende Schutzpflichten eines die Cyber-Sicherheit beeinträchtigenden Staates gegenüber der internationalen Gemeinschaft, Gefahren für die Stabilität, Integrität und Funktionalität des Internets abzuwenden und den globalen, unbeschränkten, grenzübergreifenden Internetverkehr nicht negativ zu beeinflussen.

Dem Vorsorgeprinzip (*due diligence*-Prinzip) sowie den Grundsätzen der guten Nachbarschaft sind neben Informations- und Kommunikationspflichten nach Vorfällen auch präventive Pflichten zu entnehmen. Doch Völkergewohnheitsrecht entwickelt sich nur langsam. Wichtige Wegmarken können daher nichtbindende Normen darstellen.

Um Cyber-Sicherheit langfristig effektiv im Völkerrecht zu verankern, sind drei Ansätze sinnvoll. Zunächst muss unter Verweis auf Cyber-Sicherheit in politischen Prozessen interveniert und das Profil des Konzepts Cyber-Sicherheit gehoben werden. Gerade angesichts der beherrschenden Bedeutung der Cyber-Sicherheit für Staat, Wirtschaft und Gesellschaft muss Cyber-Sicherheit zu einem zentralen, permanenten Agendapunkt von Organisationen und Institutionen werden, die sich mit Fragen globaler Koordination und Kooperation auseinandersetzen.

Cyber-Sicherheitsnormen können in einen multistakeholderbasierten Prozess zur Erstellung eines Frameworks of Commitment präzisiert werden. Zwar kann ein derartiger Prozess nicht zu bindenden Normen führen, doch ermöglicht er stakeholderüber-

greifenden Meinungsaustausch und führt zu staatlichem Partizipationsdruck. Dieser kann dann auf das eigentliche Ziel gelenkt werden: die Entwicklung und Annahme einer Convention on Cyber-Security. Ein derartiges Übereinkommen über Cyber-Sicherheit würde am besten von einem Expertenkomitee des Europarates ausgearbeitet, das dabei an die Entwicklung der Budapest Convention anknüpfen könnte.

Darüber hinaus muss die Cyber-Sicherheit verstärkt institutionalisiert werden. Aus dem Kooperationsprinzip in dessen präventiver Dimension lässt sich eine zumindest in Konturen belastbare Verpflichtung zur Entwicklung eines global-interoperablen Lagebildes ableiten. Auch bei der OECD könnte ein *Cybersecurity Cooperation Center (OECD C3)* eingerichtet werden, das Best Practices zu Cyber-Sicherheit sammelt und Modellregularien entwirft.

Die Cyber-Sicherheitsstrategie für Deutschland 2016 bestätigt die Bedeutung der engen Zusammenarbeit und Koordinierung für die Prävention und das „Erkennen, Zuordnen, Abwehren und Verfolgen von Cyber-Angriffen“. Im Cyberraum tragen alle Akteure eine gemeinsame, geteilte Verantwortung. Wie in der Studie gezeigt wurde, bestehen klare völkerrechtliche Regeln, auf deren Grundlage Cyber-Sicherheit geschützt wird. Weitere Schritte zur besseren Verankerung von Cyber-Sicherheit im Völkerrecht wurden ebenso aufgezeigt. Die im Folgenden angeführten Cyber-Sicherheitsnormen stellen ein normatives Minimum zur Hebung der Cyber-Sicherheit durch Völkerrecht dar und können als Hintergrund für globale politische Kooperationsprozesse, als Grundlegung zum Framework of Commitment oder als Ideen für eine Erklärung des Europarates verwendet werden, die den Prozess der Ausarbeitung einer Convention on Cyber-Security anstoßen kann.

EIN VORSCHLAG FÜR CYBER-SICHERHEITSNORMEN

1. Das Ziel von Cyber-Sicherheitsnormen ist ein stabiles, sicheres, resilientes, funktionsfähiges, offenes und freies Internet.

2. Cyber-Sicherheit kann nur gewährleistet werden, wenn alle Stakeholder – Staat, Wirtschaft, Gesellschaft – auf allen Ebenen – lokal, regional, global – ihre gemeinsame, geteilte Verantwortung tragen und auf einer gemeinsamen Grundlage aufbauend die nötigen Schritte zur Gewährleistung und zur Förderung von Cyber-Sicherheit setzen.

3. Staaten müssen umfassend die Cyber-Sicherheit im Internet respektieren, schützen, gewährleisten und fördern, weil sie nur so ihrer Pflicht nachkommen können, allen ihrer Jurisdiktion unterstehenden Personen und Unternehmen alle einschlägigen Rechte und Freiheiten zu sichern.

4. Staaten müssen neben anderen Prinzipien des Völkerrechts jene der staatlichen Souveränität, souveränen Gleichheit, der Nichtintervention, der friedlichen Streitbeilegung, der guten Nachbarschaft und der Kooperation respektieren. Alle völkerrechtlichen Verpflichtungen bleiben bestehen, insbesondere hinsichtlich des Schutzes von Menschenrechten.

5. Staaten obliegt die Jurisdiktion über die informations- und kommunikationstechnologische (IKT)-Infrastruktur in ihrem Territorium, wobei sie, um Jurisdiktionskonflikte zu vermeiden, stets mit anderen Staaten kooperieren sollten.

7. Staaten dürfen nicht zulassen, dass ihr Territorium zu Handlungen missbraucht wird, die ihre völkerrechtlichen Verpflichtungen verletzen. Sollte eine derartige Handlung gesetzt werden, müssen sie ihrer völkerrechtlichen Verantwortlichkeit gerecht werden.

8. Zur Gewährleistung von Cyber-Sicherheit müssen Staaten, Wirtschaft und Gesellschaft national, regional und international kooperieren, um Maßnahmen zu setzen, die die Sicherheit und Stabilität der Informations- und Kommunikationsinfrastruktur und der über sie ablaufenden Kommunikationen und den Datenverkehr erhöhen.

9. Staaten verpflichten sich dazu, präventive Maßnahmen zu ergreifen, um Vorfälle im Bereich der Cyber-Sicherheit zu verhindern bzw. effektiv abzuwehren und eine möglichst offene Kommunikation gegenüber anderen Akteuren in Staat und Wirtschaft zu gewährleisten, um innerstaatlich wie international koordinierte Schritte gegen Vorfälle zu setzen.

10. Staaten verpflichten sich dazu, nationale kritische Infrastruktur zu identifizieren und adäquat zu schützen; die Wirtschaft trägt dazu nach Kräften bei.

11. Staaten leisten sich gegenseitige Unterstützung bei der Abwehr von Gefährdungen der Cyber-Sicherheit unter Beachtung der Bedeutung eines freien Internets und unter Gewährleistung des Schutzes der Menschenrechte.

12. Staaten sind sich bewusst, dass Cyber-Sicherheit auch ein Vertrauen der Endnutzer in die Integrität von Dienstleistungen und die Sicherheit von Produkten voraussetzt; dieses muss entlang der Wertschöpfungs- und Lieferkette gewährleistet sein.

14. Im Rahmen ihrer jeweiligen Verantwortlichkeiten tragen Staaten und Wirtschaft zur Bekämpfung von Kriminalität im und durch das Internet bei.

15. Staaten bekennen sich zu der Bedeutung von vertrauensbildenden Maßnahmen, um Cyber-Sicherheit zu stärken. Diese fördern Kooperation zwischen Akteuren auf nationaler, regionaler und internationaler Ebene und führen zu mehr Transparenz und Stabilität.