



HIIG Discussion Paper Series

Discussion Paper No. 2017-02

Vom Völkerrecht des Netzes zur Verfassung des Internets

Privacy und Digitale Sicherheit im Zeichen
eines schrittweisen Paradigmenwechsels

April 2017

Ingolf Pernice

ingolf.pernice@hiig.de
Alexander von Humboldt Institute
for Internet and Society
Humboldt-Universität zu Berlin

ABSTRACT

The 2007 (probably) Russian cyber-attack on Estonia, and even more so the NSA mass surveillance and spy activities revealed by Edward Snowden in 2013 had a great impact on internet politics worldwide, in the EU and in Germany. The first event triggered NATO to look closer on cyber war, with the result that the *Tallinn Manual* was elaborated and published establishing a number of definitions and rules regarding the application of international law, including humanitarian law, on cyber war. A second edition of the Manual, extending it to attacks in peace was published in 2017. As a consequence of the Snowden revelations, Brazil and Germany initiated a process at the UN for establishing the protection of human rights and, in particular, privacy worldwide through clearer provisions under international law (*Pillay Report*). And in its »Digital Agenda« and in the Coalition Agreement for the new government 2013, with a special focus on the digitisation of the society, particular emphasis was given to the »Völkerrecht des Netzes« (the international law of the internet). What is this law, what are the structural shifts cognisable in the international law of the internet, and how can new legal developments at the global level best be conceptualised to respond to the challenges of digitisation? The present contribution uses the *Tallinn Manual*, the *Pillay Report* and the discussion on an international law of the internet as examples and starting points for elaborating some principles of a constitution of the internet, based upon experience from multi-stakeholder settings tested since the *Rio Process* and developed within the diverse fora of internet governance.

KEYWORDS

Privatheit, Verfassung, Internet, Völkerrecht, digitale Sicherheit, Rio-Prozess, Internet Governance

CONTENTS

I.	EINLEITUNG	1
II.	DIGITALE ÜBERWACHUNG UND PRIVATHEIT IM VÖLKERRECHT	5
1.	Der »Pillay-Bericht« zum Recht auf Privatheit	6
2.	Umfang der Menschenrechtsverantwortung der Staaten	10
3.	Kontrolle der Dienste und Rechtsschutz der Betroffenen	12
4.	Erweiterte Menschenrechtliche Schutzpflichten	12
III.	DIGITALE SICHERHEIT UND VÖLKERRECHT	14
1.	Gewaltverbot und Selbstverteidigung bei Cyber-Angriffen: Das Tallinn Manual	15
2.	Neue Aufgaben und Instrumente für den Weltsicherheitsrat	18
3.	Kriegsvölkerrecht und die Entwicklung eines globalen humanitären Rechts	19
IV.	INTERNETGOVERNANCE UND DIE »VERFASSUNG DES INTERNETS«	21

I. Einleitung

Daniel Thürer gehört zu denjenigen Rechtsgelehrten, die sich nicht scheuen, den Blick über den Tellerrand zu werfen und Zusammenhänge des Rechts und der Verfassung jenseits des Staates, in Europa und auf der globalen Ebene zu erkunden, einzuordnen und die Erkenntnisse in ein offenes Verständnis von Staatlichkeit und Völkerrecht münden zu lassen. Keines der großen Themen auf der politischen Tagesordnung unserer Zeit entgeht seiner kritischen verfassungs- und völkerrechtlichen Analyse, stets sind seine Schriften dazu von der Offenheit für Neues, für den Wandel von Staat und Recht in einer globalen Ordnung geprägt. Dies mag es erlauben, in den folgenden Zeilen einige vielleicht etwas gewagte Überlegungen zu einem aktuellen, die Entwicklung des Völkerrechts im Zeitalter des Internets betreffenden Thema zur Diskussion zu stellen. Ein neues Thema zieht die Aufmerksamkeit von Politikern, aber auch einiger Juristen auf sich: »Das Völkerrecht des Netzes«.¹

Der Koalitionsvertrag vom 27. November 2013, der die gegenwärtige Bundesregierung in Deutschland trägt, enthält dazu folgenden zukunftsweisenden Satz:

»Um die Grund- und Freiheitsrechte der Bürgerinnen und der Bürger auch in der digitalen Welt zu wahren und die Chancen für die demokratischen [sic] Teilhabe der Bevölkerung am weltweiten Kommunikationsnetz zu fördern, setzen wir uns für ein Völkerrecht des Netzes ein, damit

¹ Die hier entwickelten Gedanken bauen auf einem Workshop auf, der am 8. September 2014 vom HIIG in Kooperation mit dem Auswärtigen Amt unter diesem Titel durchgeführt wurde, vgl. dazu den Bericht von Emma Peters, Workshop-Eindrücke: Das Völkerrecht des Netzes, den »Gastbeitrag« dazu von Helmut Aust, »Völkerrecht des Netzes«: welche Rolle für die Menschenrechte?, sowie das Protokoll des Workshops, alles abrufbar unter: <http://www.hiig.de/events/das-völkerrecht-des-netzes/>. S. auch die Videodokumentation zum Panel 4 (»Völkerrecht des Netzes«) der Konferenz vom 3. Dezember 2014 über: »Schutz von Privatsphäre und Daten in Zeiten von Big Data, staatlicher Überwachung und digitaler Grenzenlosigkeit« an der Humboldt-Universität zu Berlin, abrufbar unter: <http://www.hiig.de/events/schutz-von-privatsphäre-und-daten/>, mit einem Blogbeitrag von Emma Peters, abrufbar unter: <http://www.hiig.de/eindrücke-der-konferenz-schutz-von-privatsphäre-und-daten-in-zeiten-von-big-data-staatlicher-überwachung-und-digitaler-grenzenlosigkeit/>. Zum Internet-Völkerrecht s. schon die Beiträge von Franz C. Mayer, Das Internet, das Völkerrecht und die Internationalisierung des Rechts, in 23 Zeitschrift für Rechtssoziologie, 2002, S. 93; Robert Uerpman, Internetvölkerrecht, 47 AVR 2009, S. 261; ders., Principles of International Internet Law, 11 German Law Journal, 2010, S. 1245 ff.; für die wirtschaftsrechtliche Seite, die hier nicht behandelt wird, s. Christian Tiedje/Karsten Nowrot, Das Internet im Fokus des transnationalen Wirtschaftsrechts: Normative Ordnungsstrukturen für den E-Commerce 47 AVR 2009, S. 328. Neuestens: Karine BANNELIER and Théodore CHRISTAKIS, Cyber-Attacks – Prevention-Reactions: The Role of States and Private Actors, Les Cahiers de la Revue Défense Nationale, Paris, 2017, abrufbar unter: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988. Der Verf. dankt seinem HIIG-Team, Osvaldo Saldías, Jörg Pohle, Ulrike Höppner, Emma Peters, Rike Meier, Benjamin Lück, Rüdiger Schwarz und Theresa Züger sehr herzlich für Kommentare und Anregungen bei der Anfertigung des Manuskripts. Eine gekürzte Fassung dieses Beitrags ist veröffentlicht in: Giovanni Biaggini / Oliver Diggelmann / Christine Kaufmann (eds.), Polis und Kosmopolis, Festschrift für Daniel Thürer, DIKE/Nomos (2015), S. 575-588.

die Grundrechte auch in der digitalen Welt gelten. Das Recht auf Privatsphäre, das im Internationalen Pakt für bürgerliche und politische Rechte garantiert ist, ist an die Bedürfnisse des digitalen Zeitalters anzupassen».²

Dieser Satz kann als Reaktion auf die Enthüllungen von Edward Snowden verstanden werden und auf die damit offenbarten Praktiken der Massenüberwachung durch amerikanische und britische, aber auch französische und deutsche Geheimdienste. Er verspricht ein Programm, dessen Konturen, Ziele und Stufen noch nicht definiert sind. Erste Ansätze finden sich allerdings in der von der deutschen Bundesregierung am 20. August 2014 beschlossenen Digitalen Agenda 2014–2017. Im vorletzten Punkt unter dem Titel »Weiterentwicklung ‚Völkerrecht des Netzes‘ und Menschenrechtsschutz« wird hier als Ziel die »Erstellung einer Handreichung zu Elementen eines ›Völkerrecht des Netzes« bezeichnet. Zur Erläuterung verweist die Digitale Agenda u.a. auf den »Pillay-Bericht«, der auf eine deutsch-brasilianische Initiative in der UN-Generalversammlung hin vom Menschenrechtsrat der Vereinten Nationen erstellt wurde.³ Der damit begonnene Diskussionsprozess soll der Digitalen Agenda zufolge aktiv begleitet werden. Zudem sollen die deutsche Beteiligung in der »Freedom Online Coalition«⁴ sowie der »Runde Tisch Internet und Menschenrechte« gestärkt werden. All dies dient dem wie folgt formulierten Anliegen:

»Wir wollen Klarheit über das anwendbare ‚Völkerrecht des Netzes‘ herstellen, um die geltenden Grund- und Freiheitsrechte auch in der digitalen Welt wirksam zu schützen und die Chancen für eine demokratische Teilhabe am weltweiten Kommunikationsnetz zu verstärken. Das Recht auf Privatsphäre und die Informations- und Meinungsfreiheit müssen auch im digitalen Zeitalter durchgesetzt werden«.⁵

Anders als der Begriff »Völkerrecht des Netzes« zunächst erwarten lässt, steht damit der Schutz der Grund- und Freiheitsrechte im Zeitalter des

² Koalitionsvertrag vom 27. November 2013, S. 149, abrufbar unter: https://www.bundesregierung.de/Content/DE/_Anlagen/_2013/_2013-12-17-koalitionsvertrag.pdf?__blob=publicationFile.

³ Human Rights Council, 27th session, The right to privacy in the digital age, 30. Juni 2014 (A/HRC/27/37), s. unter: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf.

⁴ S. unter: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf.

⁵ Vgl. Bundesregierung: Digitale Agenda 2014-2017, August 2014, Kapitel VII Ziff. 4, abrufbar unter: <https://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/digitale-agenda-2014-2017,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf>.

Internets im Vordergrund, wenn auch die Stärkung der »Chancen für eine demokratische Teilhabe am weltweiten Kommunikationsnetz« gleich danach als weiteres Ziel genannt und damit zum Gegenstand des Begriffs gemacht wird. Der Kontext dieses Punktes in der Digitalen Agenda zeigt, dass über das Thema Menschenrechte hinaus weit mehr auf der Agenda steht: Um »ein offenes, freies, sicheres globales Internet als Raum der Meinungsvielfalt, Teilhabe, Innovation und als Motor für Wirtschaftswachstum und Arbeit« zu schützen und auszubauen, fordert die Agenda auch die »Schaffung von Regeln und Rahmenbedingungen für das globale Netz«, die ein Handeln auf nationaler, europäischer und internationaler Ebene erfordert.⁶ Zu »Themen wie Netzausbau, Netzneutralität, Vollendung des digitalen Binnenmarktes, Datenschutz, Schutz des geistigen Eigentums im Internet, IT-Sicherheit und die Forschungsförderung« wird ein stärkeres Engagement auf der europäischen Ebene angekündigt,⁷ während im Blick auf die internationale Handlungsebene das Interesse auf den »Multi-Stakeholder-Ansatz«, auf bilaterale Regierungskonsultationen wie etwa den bereits begonnenen »Cyber-Dialog« sowie auf die aktive Mitgestaltung der internetbezogenen Diskussionen in der Internationalen Fernmeldeorganisation ITU und in der OECD gerichtet ist.⁸ Die diversen Foren für das »Management des Internets (Internet Governance)«, in denen sich der »Multi-Stakeholder-Ansatz« gegenwärtig besonders manifestiert, werden eigens angesprochen, verbunden mit dem Vorsatz, dass Deutschland sich hier aktiv beteiligt.⁹

Angesichts dieser Vielfalt von eng miteinander zusammenhängenden Themen liegt es nahe, den Begriff eines Völkerrechts des Netzes inhaltlich weit zu fassen. Er umfasst Fragen des Schutzes der Grund- und Freiheitsrechte, insbesondere den Schutz von Daten und Privatsphäre¹⁰ und den Schutz des geistigen Eigentums im Internet, es geht um die Ermöglichung und Sicherheit von Information und Kommunikation und damit auch um IT-Sicherheit und weitere Problemfelder wie Cyber-Kriminalität und -Spionage¹¹ sowie um den *cyber war* (»Cyber-Sicherheitspolitik«),¹² Fragen, die weder national noch auf europäischer Ebene effektiv zu lösen sind; hierüber ist eine Verständigung auf globaler Ebene

⁶ Ebd., Kap. VII, Vorspann.

⁷ Ebd., Kap. VII.1.

⁸ Ebd., Kap. VII.2.

⁹ Ebd., Kap. VII.3.

¹⁰ Ebd., Kap. VI.2.

¹¹ Ebd., A (Grundsätze), S. 5, Kap. II.3 (S. 15), VI.5.

¹² Ebd., Kap. VII.2.

unerlässlich, wenn der globale Charakter des Internets erhalten bleiben soll. In der Folge des Cyber-Angriffs auf Estland 2007 hat Duncan B. Hollis bereits ein »international law for information operations« (ILIO) gefordert, wobei er derartige Angriffe zwischen *cyber crime* und *cyber war* ansiedelt und mit dem Vorschlag eines neuen Abkommens den Unsicherheiten, der Komplexität und den – u. a. auf der neuen Bedeutung nicht-staatlicher Angriffe beruhenden – Unzulänglichkeiten des geltenden Rechts begegnen will.¹³

Dabei stellt sich die Frage, ob die Kategorie »Völkerrecht« im klassischen Sinne nicht zu kurz greift, wenn es doch viel allgemeiner, wie es in der Digitalen Agenda heißt, um »Regeln und Rahmenbedingungen für das globale Netz« geht.¹⁴ Die Frage, ob das Internet das Völkerrecht ändert,¹⁵ scheint eine positive Antwort zu erhalten.¹⁶ Zu Recht werden Entwicklungen im Bereich der Internet-governance angesprochen, wie etwa die Entstehung und wachsende Bedeutung der ICANN,¹⁷ die eine wesentliche Säule des globalen Regelungssystems für das Internet geworden ist. Das Völkerrecht mutiert vom Recht zwischen Staaten zum Recht zwischen Menschen, die durch ihre Staaten handelnd oder auch im Wege eines *private ordering* Rechte und Pflichten für sich selbst begründen. Dann aber liegt es nahe, überhaupt den Begriff »Völker«-recht zu überdenken und jedenfalls für die Regeln und Rahmenbedingungen des globalen Internets einen Begriff zu finden, der die Beschränkung auf das Zwischenstaatliche, das Internationale überwindet und der wachsenden Bedeutung privater Akteure im »Multi-Stakeholder-Modell« der *global governance* Rechnung trägt.

Ein solcher Begriff nimmt das klassische Völkerrecht als wichtiges Element in sich auf, er muss dabei aber die legitimierende Rolle des Individuums auch bei Verträgen zwischen Staaten in den Blick nehmen und andersartig generierte und durchsetzbare global geltende Normen mitumfassen, deren Legitimität ggf. auf neuen Wegen zu konstruieren wäre. Wenn solche Normen unmittelbar für den Einzelnen Rechte und Pflichten begründen, geht es um Konstitutionalisierung. Dann geht es um die »Verfassung« des Systems der Herausbildung globaler Prinzipien und Normen allgemein und es eröffnet sich eine neue

¹³ Duncan B Hollis, Why States Need an International Law for Information Operations, in: 11 Lewis & Clark Law Review (2007), S. 1023, 1026 ff., 1039 ff.

¹⁴ Digitale Agenda (Fn. 5), Kap. VII, Vorspann.

¹⁵ Vgl. dazu schon Henry H. Perritt, The Internet is Changing International Law, 73 Chicago-Kent Law Review (1998), S 997: »The Internet is changing international law because it is eroding the dominance of traditional sovereign states at the same time that it facilitates new institutional mechanisms for making, applying, and enforcing law«.

¹⁶ Krit. noch Franz C. Mayer, Review Essay. The Internet and Public International Law – Worlds Apart?, 12 EJI (2001), S. 617, 621.

¹⁷ Ebd., Kap. VII.3.

Perspektive in der Debatte über den globalen Konstitutionalismus, die dem *multi-stakeholderism* eine wichtige Rolle zuweist.¹⁸

Thema und Begriff »Völkerrecht des Netzes« sind damit Anstoß für eine umfassendere Reflektion mit entwicklungsoffener Perspektive. Der auf die Einzelnen fokussierte konstitutionelle Ansatz stützt ein Verständnis der Garantien von Menschenrechten, insbesondere des Schutzes von Daten und Persönlichkeitsrechten, das auf dem Gedanken eines gegenseitigen Versprechens der Menschenwürde zwischen den Individuen beruht¹⁹ und den Staat vollumfänglich in die Verantwortung nimmt (dazu II.). Er eröffnet aber auch hinsichtlich der Sicherheit einen neuen Blick auf schwierige Abgrenzungsfragen vor allem zur rechtlichen Einordnung und Behandlung von Cyber-Angriffen im Kriegs- und humanitären Völkerrecht, seit nicht nur Staaten, sondern auch vielleicht sogar primär Individuen oder nicht-staatliche Organisationen die relevanten Akteure sind (dazu III.). Die Einzelnen sind damit neben den Staaten zugleich Akteure und Betroffene, wo die Entwicklung neuer Formen der *governance* eine »Verfassung des Internets« befördert, die, nur teilweise im klassischen Völkerrecht verankert, Ausdruck ist für einen vielleicht grundlegenden Wandel des Völkerrechts selbst (dazu IV.).

II. Digitale Überwachung und Privatheit im Völkerrecht

In Reaktion auf die Snowden-Enthüllungen unternahm die entrüstete Bundesregierung zwei Schritte: Zum einen wurde sie bei der US-Regierung vorstellig, um »unter Freunden« eine »no-spy« Vereinbarung mit den USA abzuschließen. Entgegen anfänglichen Hoffnungen²⁰ zeigte Obama Deutschland die kalte

¹⁸ Zum hier zugrunde gelegten gewandelten Verfassungsbegriff s. Ingolf Pernice, Die Verfassung der Internetgesellschaft. Zur Rolle von Staat und Verfassung im Zuge der digitalen Revolution, in: Alexander Blankenagel (Hrsg.), Den Verfassungsstaat nachdenken. Eine Geburtstagsgabe, 2014, S. 171. Die Literatur zum Thema Global Constitutionalism ist inzwischen kaum übersehbar, eine eigene Zeitschrift ist ihm gewidmet: Global Constitutionalism. Human Rights, Democracy and the Rule of Law, <http://journals.cambridge.org/action/displayJournal?jid=GCN>.

¹⁹ Zum Gedanken, freilich bezogen auf den Staat: Hasso Hofmann, Die versprochene Menschenwürde, AöR 118 (1993), 353, 367, für den das in der Verfassung gegebene Versprechen der Achtung der Menschenwürde als »wechselseitige Gleichachtung eines jeden einzelnen Rechtsgenossen« mehr als nur die Anerkennung eines Prinzips oder die »Artikulation eines kollektiven Wertbewusstseins« ist, sondern eine »Gemeinschaftsaktion«: »es ist Staatsgründung«. Zur Übertragung auf die EU s. Ingolf Pernice, Solidarität in Europa. Eine Ortsbestimmung im Verhältnis zwischen Bürger, Staat und Europäischer Union, in: Christian Calliess (Hrsg.), Europäische Solidarität und nationale Identität. Überlegungen im Kontext der Krise im Euroraum, 2013, S. 25, 55 f.

²⁰ S. etwa Peter Carstens, Geheimdienste »No-Spy-Abkommen« nimmt Form an, FAZ e-paper v. 13.8.2013, abrufbar unter: <http://www.faz.net/aktuell/politik/geheimdienste-no-spy-abkommen-nimmt-form-an-12530395.html>.

Schulter; die Vereinigten Staaten sahen keinen Bedarf und fanden die Idee auch nicht gut.²¹ Auf diese Abfuhr folgte ein zweiter Anlauf, eine Resolutionsinitiative bei der UN-Generalversammlung, jetzt gemeinsam mit Brasilien, zu der Außenminister Westerwelle erklärte:

*»Digitale Kommunikation ist heute ein globales Geschäft, deshalb muss der Schutz der Privatsphäre auch auf globaler Ebene gefestigt werden. Wir streben mit der Initiative mit unseren brasilianischen Partnern ein breites internationales Bündnis für einen zeitgemäßen Schutz der Privatsphäre an«.*²²

Ein Interessenausgleich durch völkerrechtlichen Vertrag wäre der direkteste Weg gewesen, das Ziel eines wirksamen Schutzes der Privatsphäre zu erreichen, doch offenbar fehlte das Interesse der anderen Seite. Der mühsamere Weg über die Vereinten Nationen aber erweist sich potentiell als erfolgreicher. Mit dem »Pillay-Bericht« ist ein erster Schritt getan, um die Bedeutung der Menschenrechte bei Überwachungsmaßnahmen zu unterstreichen (dazu 1.). Wie weit die staatliche Verantwortung etwa gemäß dem Internationalen Pakt für Bürgerliche und Politische Rechte (IBPR) reicht, ist allerdings nicht eindeutig (dazu 2.). Dennoch formuliert der Bericht beachtliche Pflichten der Staaten in Bezug auf Kontrolle und Rechtsschutz bei den Tätigkeiten ihrer Dienste (dazu 3.). Nach allem treffen die Staaten erweiterte menschenrechtliche Schutzpflichten (dazu 4.).

1. Der »Pillay-Bericht« zum Recht auf Privatheit

Die UN-Generalversammlung nahm am 18. Dezember 2013 die Resolution Nr. 68/167 über »The right to privacy in the digital age« an, in der auf Art. 12 der Menschenrechtserklärung von 1948 und Art. 17 des Paktes über die Bürgerlichen und Politischen Rechte hingewiesen wird, die Staaten zum effektiven Schutz der Privatheit²³ in der digitalen Kommunikation aufgefordert werden

²¹ Vgl. Torsten Denkler, Bundesregierung beerdigt No-Spy-Abkommen, Süddeutsche.de v. 29. April 2014: Vor Merkels USA-Reise - Regierung beerdigt No-Spy-Abkommen, abrufbar unter: <http://www.sueddeutsche.de/politik/vor-merkels-usa-reise-bundesregierung-beerdigt-no-spy-abkommen-1.1946679>.

²² Pressemitteilung des Auswärtigen Amtes vom 1.11.2013: Außenminister Westerwelle zur UN-Resolution »The Right to Privacy in the Digital Age«, abrufbar unter: <http://www.auswaertiges-amt.de/DE/Infoservice/Presse/Meldungen/2013/131101-Brasilien-VN.html>.

²³ Der Begriff der Privatheit wird hier als Inbegriff der auf der Achtung der Menschenwürde und damit freien (informationellen) Selbstbestimmung des Individuums beruhenden Persönlichkeitsrechte, Schutz von Daten und Privatsphäre des Individuums verstanden, wie er in den Art. 8 EMRK und 17 IPBPR sowie Art. 7 und 8 GRCh verankert ist.

und die Hohe Kommissarin für Menschenrechte ersucht wurde, einen Bericht über den Schutz und die Förderung der Privatheit im Kontext der inländischen und extraterritorialen Massenüberwachung und Abhörpraktiken zu erstellen.²⁴ Trotz diplomatischer Sprache stellt der daraufhin am 30. Juni 2014 vorgelegte »Pillay-Report« mit erstaunlicher Klarheit das Vorliegen sehr problematischer Praktiken fest: »governmental mass surveillance emerging as a dangerous habit rather than an exceptional measure«.²⁵ Der Bericht erläutert ausführlich die völkerrechtlichen Normen, an denen diese Praktiken zu messen sind, stellt ihre grobe Verletzung fest und fordert die Staaten dringlich auf, Abhilfe zu schaffen:

*»Bearing the above observations in mind, there is a clear and pressing need for vigilance in ensuring the compliance of any surveillance policy or practice with international human rights law, including the right to privacy, through the development of effective safeguards against abuses. As an immediate measure, States should review their own national laws, policies and practices to ensure full conformity with international human rights law. Where there are shortcomings, States should take steps to address them, including through the adoption of a clear, precise, accessible, comprehensive and non-discriminatory legislative framework. Steps should be taken to ensure that effective and independent oversight regimes and practices are in place, with attention to the right of victims to an effective remedy«.*²⁶

Jedenfalls implizit offenbart der Bericht, dass wohl kaum ein Staat seinen Pflichten aus den Menschenrechtsverträgen nachkommt. Dabei fordert Art. 17 (1) IPBPR für jeden Menschen den Schutz vor »willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr«; nach Absatz 2 der Vorschrift hat »jedermann« sogar »Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen«, ob sie aus dem Inland oder aus dem Ausland kommen.²⁷ Die massenhafte Sammlung von Daten, auch die Vorratsdatenspeicherung und das Abhören der Kommunikation, werden selbst bei nicht-personenbezogenen Daten schon wegen der Möglichkeiten der Re-Identifikation und der *chilling effects* für Meinungs- und

²⁴ Resolution adopted by the General Assembly on 18 December 2013 (ARES/68/167), abrufbar unter: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167.

²⁵ Human Rights Council (Fn. 3), Ziff. 3.

²⁶ Ibid., Ziff. 50.

²⁷ Ibid., Ziff. 28 ff., 30.

Versammlungsfreiheit als Eingriffe bewertet, wobei die Rechtfertigungslast beim Staat liege.²⁸ Zur Rechtfertigung wird eine spezielle gesetzliche Grundlage gefordert, verbunden mit strengen Kriterien der Verhältnismäßigkeit, bis hin zur Wesensgehaltsgarantie.²⁹ Massenüberwachung und unbeschränkte Datensammlung »für den Fall, dass...«, verkehrten gegenwärtig das Verhältnis von Recht und Schranke, von Grundsatz und Ausnahme ins Gegenteil und erfüllten diese Kriterien nicht.³⁰ Die am 18. Dezember 2014 von der Generalversammlung der UN angenommene Resolution »The right to privacy in the digital age«³¹ bekräftigt, dass die Staaten den Schutz der Privatheit durch die Menschenrechte zu beachten haben, wenn sie die digitalen Kommunikationswege anzapfen oder von privaten Unternehmen die Vorlage personenbezogener Daten Dritter verlangen,³² dass sie Verstöße gegen diese Verpflichtung abstellen, entsprechende Regelungen ändern und effektive Kontrollinstanzen zur Sicherstellung der Erfüllung dieser Pflichten und Rechtsschutz für die Betroffenen einführen müssen.³³ Dazu wird die »responsibility to respect human rights« hervorgehoben, die auch die Wirtschaftsunternehmen trifft.³⁴ Unter Bezugnahme auf die NETmundial vom April 2014 verweist die Generalversammlung ausdrücklich auf die Notwendigkeit des privaten Engagements im Sinne des »Multi-Stakeholder-Ansatzes«:

*»...recognizing that effectively addressing the challenges relating to the right to privacy in the context of modern communications technology will require an ongoing, concerted multi-stakeholder engagement«.*³⁵

Bei geheimdienstlichen Tätigkeiten gibt es die Unterscheidung zwischen drei Kategorien von Fällen: Rein innerstaatliche Überwachung, rein ausländische Tätigkeiten (z.B. Abhören von Telefongesprächen zwischen zwei im Ausland befindlichen Endgeräten) und die Überwachung der grenzüberschreitenden

²⁸ Ibid., Ziff. 17-20, unter Verweis auf die Rechtsprechung des EuGH zur Vorratsdatenspeicherung in Rs. C-293/12 und C-594/12 – Digital Rights Ireland, Rn. 26 f., 37. Bemerkenswert auch: Executive Office of the President, Report to the President. Big Data and Privacy. A Technological Perspective (Mai 2014), S. 19: There is no reason to believe that metadata raise fewer privacy concerns than the data they describe« (abrufbar unter: http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf).

²⁹ Human Rights Council (Fn. 3), Ziff. 21 ff., 25.

³⁰ Ibid., Ziff. 25.

³¹ Dokument A/RES/69/166 v. 18. 12. 2014, <http://research.un.org/en/docs/ga/quick/regular/69>.

³² Ebd., Präambel Abs. 17.

³³ Ebd., Ziff. 4 lit. b-d.

³⁴ Ebd., Präambel Abs. 18, mit Verweis auf die »Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework«, A/HRC/17/31, annex.

³⁵ Ebd., Präambel Abs. 10.

Kommunikation zwischen in- und ausländischen Teilnehmern. Innerstaatliche Handlungsermächtigungen und -grenzen, so auch in Deutschland, betreffen nur die rein inländischen sowie – unter Einschränkung – die grenzüberschreitenden Tätigkeiten.³⁶ Sie erstrecken sich regelmäßig nicht auf Tätigkeiten im Ausland. Dem liegt wohl die Annahme zugrunde, dass ein staatliches Gesetz nicht zu Eingriffen im anderen Staat ermächtigen kann,³⁷ umgekehrt aber die Grundrechte nicht oder nicht in vollem Umfang binden, wenn es um Tätigkeiten der Dienste im Ausland geht.³⁸ Auch der »Pillay-Bericht« erwähnt die unterschiedliche Behandlung von Staatsangehörigen und Ausländern, letzteren werde oft weniger, z. T. gar kein Schutz gewährt.³⁹ Ein legitimer Grund für die Differenzierung ist aus der Perspektive der Menschenrechte nicht ersichtlich.⁴⁰

2. Umfang der Menschenrechtsverantwortung der Staaten

Das völkerrechtliche Problem ist die Bestimmung des Geltungsumfangs der Menschenrechte nach Art. 2 (1) IPBPR, der die Verpflichtung jedes Vertragsstaates zur Achtung der Rechte auf alle »in seinem Gebiet befindlichen und seiner Herrschaftsgewalt unterstehenden Personen« erstreckt, aber auch begrenzt. Auch nach Art. 1 EMRK sichern die Vertragsparteien die in der Konvention bestimmten Rechte nur »allen ihrer Hoheitsgewalt unterstehenden Personen« zu. Ausländern im Inland kommt dieser Schutz zu, auch die Kommunikation von In- und Ausländern über die Außengrenzen eines Staates

³⁶ Vgl. dazu Bertold Huber, Die strategische Rasterfahndung des Bundesnachrichtendienstes - Eingriffsbefugnisse und Regelungsdefizite, NJW 2013, 2572, 2575 f.

³⁷ Dies ist offenbar für das britische Recht kein Problem, vgl. dazu Krieger (Fn. 38), S. 9 f.

³⁸ So die Auffassung der Bundesregierung in BVerfGE 100, 313 – Telekommunikationsüberwachung, S. 362, nach der die räumliche Anwendbarkeit des Art. 10 GG nur »bei hinreichendem territorialen Bezug zur Bundesrepublik Deutschland« gegeben sein sollte. Das Gericht lässt einen »Gebietskontakt« genügen, der etwa gegeben ist, wenn die Erfassung oder Auswertung der Daten auf deutschem Boden erfolgt (ebd., S. 363 f.). Krit. und zur Unanwendbarkeit des Territorialitätskriteriums Florian Becker, § 240 Grenzüberschreitende Reichweite deutscher Grundrechte, in: Josef Isensee/Paul Kirchhof, Handbuch des Staatsrechts der Bundesrepublik Deutschland, 3. Aufl., Bd. XI - Internationale Bezüge, 2013, S. 515, 547 f. (Rn. 87 ff.). Für eine »Geltungserstreckung« votiert auch Heike Krieger, Die Reichweite der Grundrechtsbindung bei nachrichtendienstlichem Handeln, Berliner Online-Beiträge zum Völker- und Verfassungsrecht, Beitrag Nr. 1/08, 2008, S. 2 ff. Ähnl. Christoph Gröpl, Das Fernmeldegeheimnis des Art. 10 GG vor dem Hintergrund des internationalen Aufklärungsauftrages des Bundesnachrichtendienstes, ZRP 1995, 13, 17 f., in Auseinandersetzung mit restriktiveren Auffassungen. Enger wohl Martin Nettesheim, Verfassungsbindung der auswärtigen Gewalt, in: Isensee/Kirchhof (aaO.), § 241, S. 559, 582 (Rn. 57) im Blick auf die »Territorialhoheit anderer Staaten«.

³⁹ Human Rights Council (Fn. 3), Ziff. 35, wobei in Ziff. 36 die Geltung des Diskriminierungsverbots des Art. 26 IPBPR auch insoweit hervorgehoben wird.

⁴⁰ Die Frage wurde offen gelassen in BVerfGE 100, 313 – Telekommunikationsüberwachung, S. 362 ff., weil eine ausreichende Verknüpfung mit dem deutschen Territorium (»Gebietskontakt«) gegeben war.

hinweg. Ob zum geschützten Personenkreis aber auch zwei Kommunikationspartner im Ausland gehören, die von inländischen Diensten abgehört werden, ist nicht entschieden. Noch schwieriger erscheint die Frage des Schutzes von Kommunikation und Datenaustausch zwischen Ausländern, die über einen zentralen Knoten des Internets im Inland laufen und hier erfasst werden. Ursprung und Adressaten sind nicht ohne weiteres erkennbar. Erst die Datenanalyse kann hierüber möglicherweise Aufschluss geben. Schon damit ist aber auch die Privatheit verletzt. Können die ausländischen Kommunikationspartner sich wie die Inländer auf den menschenrechtlichen Schutz ihrer Persönlichkeit berufen?

Entscheidend ist, was Begriffe wie Herrschaftsgewalt oder jurisdiction bedeuten.⁴¹ Im »Pillay-Bericht« wird »jurisdiction« mit »within the power or effective control« bzw. »persons within their ‚authority‘« erläutert. Der Bericht votiert für eine extensive Auslegung: Wo die Überwachung in Ausübung staatlicher Macht (»power«) oder effektiver Kontrolle hinsichtlich des Anzapfens etwa der Kommunikations-Infrastruktur erfolgt, direkt oder auch mittelbar über Privatunternehmen, ist eine Bindung an die Menschenrechte gegeben.⁴² Anne Peters greift auf die Rechtsprechung des EGMR zurück, um Klarheit über den Begriff der Kontrolle, die als Ausübung von Herrschaftsgewalt verstanden werden kann, zu erhalten. In Anlehnung an das Urteil *Al-Skeini v. UK* (2011) sieht sie die Maßnahmen der Massenüberwachung als »virtual control« an, womit die Anwendbarkeit der Konvention gegeben wäre.⁴³ Der EGMR formuliert seine Schlussfolgerung sehr allgemein, so dass es nicht darauf ankommen kann, ob das Handeln vom Territorium eines Staates ausgeht und sich im anderen auswirkt oder sein Agent sich physisch im Ausland befindet und handelt:

»It is clear that, whenever the State through its agents exercises control and authority over an individual, and thus jurisdiction, the State is under an obligation under Article 1 to secure to that individual the rights and freedoms under Section 1 of the Convention that are relevant to the situation of that individual«⁴⁴.

⁴¹ Zu vier Möglichkeiten des Verständnisses s. Aust (Fn. 1).

⁴² Ibid., Ziff. 32, 34.

⁴³ Anne Peters, *Surveillance without Borders: The Unlawfulness of the NSA, Panopticon, Part II*, abrufbar unter: <http://www.ejiltalk.org/surveillance-without-borders-the-unlawfulness-of-the-nsa-panopticon-part-ii/>, mit Verweis auf ECHR [GC], 7. Juli 2011, *Al-Skeini v. UK*, No. 55721/07, Rn. 133-135 (abrufbar unter: <http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-105606#%7B%22itemid%22:%5B%22001-105606%22%5D%7D>).

⁴⁴ ECHR [GC], 7. Juli 2011, *Al-Skeini v. UK*, No. 55721/07, Rn. 137.

Auch wenn die Voraussetzungen hierzu eher eng ausgelegt und dann als gegeben anerkannt werden, wenn eine effektive Kontrolle über das Territorium ausgeübt wird,⁴⁵ entspricht eine weite Auslegung eher dem konstitutionellen Sinn der Grund- und Menschenrechte als Grenze und Schutzauftrag jedes staatlichen Handelns, zumal ihrer überstaatlichen Gewährleistung: Wo ein Staat durch seine Bediensteten offiziell handelt, also Herrschaftsgewalt ausübt, ob legal oder völkerrechtswidrig durch Eingriff in fremde Souveränitätssphären, binden ihn die Menschenrechte, gleichsam im Huckepack: Das Handeln der öffentlichen Gewalt ist rechtlich gebundenes Handeln, gebunden letztlich durch die universellen Menschenrechte.⁴⁶ Das gilt für das Handeln im eigenen Territorium, auch wenn dort nur der Knoten der Internetverbindungen zwischen Drittstaaten liegt, der überwacht wird. Aber auch für staatliches Handeln im Ausland. Der Staat kann sich nicht aus der Bindung an die Menschenrechte herausmogeln, weder durch Beauftragung Privater, noch durch ein Agieren im Ausland. Denn auf der demokratisch verfassten rechtlichen Bindung gründet sich seine Legitimation.

Für Hasso Hofmann ist »die versprochene Menschenwürde« konstitutiv für die Staatsgründung;⁴⁷ der Begriff weist weit über den Staat hinaus: Ob Würde mit Kant den Menschen als »Subjekt sittlicher Autonomie« bezeichnet oder ob mit Luhmann »der Mensch Würde aus eigenem selbstbestimmten Verhalten durch gelungene Identitätsbildung« gewinnt,⁴⁸ der Anspruch auf Achtung der Menschenwürde erhält mit der wachsenden Dichte der Beziehungen zwischen Menschen mittlerweile eine globale Dimension.⁴⁹ Die Erklärung der Menschenrechte von 1948 ebenso wie die Pakte von 1966 spiegeln das rudimentär wider; staatliche und zivilgesellschaftliche Initiativen zum Schutz der Privatheit im digitalen Zeitalter sind ein neuer Anlauf zum globalen Schutz der Persönlichkeit und der individuellen Selbstbestimmung gegenüber dem weltumspannenden Datenhunger staatlicher und privater Institutionen.

⁴⁵ Vgl. die Übersicht der Rechtsprechung des EGMR im (Press Unit) Factsheet – Extra-territorial jurisdiction of States Parties, Nov. 2014, abrufbar unter: http://www.echr.coe.int/Documents/FS_Extra-territorial_jurisdiction_ENG.pdf.

⁴⁶ Vgl. auch Krieger (Fn. 38), S. 6: »Die Grundrechtsgeltung ist an die Ausübung von Hoheitsgewalt und nicht an das Staatsgebiet der Bundesrepublik geknüpft«.

⁴⁷ Hofmann (Fn. 19), S. 374 f.

⁴⁸ Immanuel Kant, *Metaphysik der Sitten*, Ed. Vorländer, 1959, S. 285, und Niklas Luhmann, *Grundrechte als Institution*, 1965, S. 35 ff., zit. mit den Worten von Hofmann (Fn. 19), S. 358.

⁴⁹ Vgl. näher Ingolf Pernice, *Global Constitutionalism and the Internet*, Vortrag zum 100-jährigen Bestehen der juristischen Fakultät der Johann Wolfgang Goethe-Universität Frankfurt a.M. am 11.6.2014, Veröffentlichung vorgesehen durch Stefan Kadelbach und Rainer Hofmann (Hrsg.), 2015.

3. Kontrolle der Dienste und Rechtsschutz der Betroffenen

Der Bericht gibt zu Kontrolle und Grenzen der Spionage einige Handreichungen. Dazu gehören Vorschläge zu Rechtsschutz und Kontrolle der Dienste, wie etwa durch »public interest advocacy' positions within surveillance authorization processes« oder ganz unabhängigen – nicht nur parlamentarischen – Kontrollgremien.⁵⁰ Voraussetzung für einen Schutz der Betroffenen ist die (jedenfalls nachträgliche) Information der Betroffenen; die Verpflichtung dazu wird dem Bericht zufolge allerdings in der Praxis regelmäßig ignoriert.⁵¹

Wenn es um Überwachungsmaßnahmen im Ausland geht, kann nichts anderes gelten. Hier sind neue Wege zu suchen. Dazu gehört zunächst die Verbreitung der Einsicht, dass mit neuen Instrumenten, die dem Staat mit dem Internet zur Erfüllung seiner Aufgaben gegeben sind und die seine Wirkungsmöglichkeiten im bislang unbekannten Umfang territorial entgrenzen, auch die Verantwortlichkeit gegenüber den jeweils von ihrem Handeln betroffenen Menschen, ggf. weltweit, in anderem Licht erscheint. Die parlamentarische Kontrolle kann auch insofern zwar sichergestellt werden, die nachträgliche Information und ein angemessener Rechtsschutz bereiten bei Aktionen im Ausland allerdings besondere Schwierigkeiten, die auch mit dem Eingriff in die Souveränitätssphäre des anderen Landes verbunden sein können.⁵² Jedenfalls die Resolution A/RES/69/166 der UN-Generalversammlung vom 18. Dezember 2014⁵³ unterscheidet nicht zwischen In- und Ausland, wenn es um den Schutz der Privatheit der Menschen geht.

4. Erweiterte Menschenrechtliche Schutzpflichten

Die Folgerungen aus dem Bericht konfrontieren die Staaten mit Anforderungen, über die man sich vor Snowden wenig bewusst war. Spionage, so heißt es, hat es immer gegeben und wird es immer geben. Das Völkerrecht schwieg dazu. Ziel war Information über den anderen Staat, die Regierung, ihre Politik, Waffenarsenale, Strategien, eventuelle Angriffs- oder Kriegspläne. Privatpersonen gerieten selten in den Fokus, außer bei der Wirtschaftsspionage. Der Schutz der

⁵⁰ Human Rights Council (Fn. 3), Ziff. 37 f.

⁵¹ Ibid., Ziff. 40, mit der Empfehlung der Untersuchung durch unabhängige Stellen sowie strafrechtlicher Sanktionen (ebd., Ziff. 41).

⁵² Ob deswegen der Schutzzumfang der Grundrechte »reduziert« sein muss, wie Krieger (Fn. 38), S. 8, feststellt, kann nur im Einzelfall entschieden werden.

⁵³ S. oben Fn. 31.

Menschenrechte, insbesondere der Persönlichkeit und der Privatheit, war insoweit kein Thema.

Das hat sich geändert mit dem internationalen Terrorismus und vor allem mit den neuen Überwachungsmöglichkeiten, die das Internet bietet. Zu der Veränderung der Bedrohungen und ihrer Autoren kommt die Veränderung des Instrumentariums der Aufklärung. Potentieller Feind sind heute nicht nur fremde Staaten, sondern auch einzelne Menschen – im In- und im Ausland – und ihre sozialen Netzwerke. Sie operieren über das Internet, und die Staaten reagieren mit der Überwachung des Internets, in Wahrnehmung ihrer Schutzpflicht für das Leben der Menschen, für das Netz als Infrastruktur und für die Informations- und Kommunikationsfreiheit, die das Internet gewährt. Die Unterscheidung von innerer und äußerer Sicherheit verschwimmt, so wie mit der Interdependenz der Staaten und mit den globalen Herausforderungen das völkerrechtliche Innen-/Außenschema überhaupt an Kontur verliert.⁵⁴

Wenn aber nicht Staaten, sondern einzelne Menschen oder nicht-staatliche Gruppen das Sicherheitsrisiko sind, versagen die für Staat-Staat-Konfrontationen entwickelten völkerrechtlichen Instrumente. Wo nicht nur staatliche Macht über die Staatsgrenzen hinaus wirksam wird, sondern vielleicht gerade auch das Versagen der Staatsmacht eines Staates Privaten die Möglichkeit autonomer Angriffe im anderen Staat eröffnet, verlieren nicht nur die Beschränkung der staatlichen Menschenrechtsverantwortlichkeit auf das eigene Territorium und die *jurisdiction* im ursprünglichen Sinne ihre Legitimation. Menschenrechte machen als Grenze des staatlichen Eingriffs, aber auch als Grundlage einer Schutzpflicht an staatlichen Grenzen nicht Halt. Sie zwingen dazu, das Handeln Privater jenseits der Grenzen, auch im Ausland ins Auge zu fassen, soweit es Wirkungen im Inland erzeugt, also selbst Grenzen überschreitet. Nicht nur die innere Sicherheit erhält damit eine externe Dimension, sondern parallel dazu die Bindung an die Menschenrechte. Sie binden das notwendige, wenn auch nicht immer nach den Maßstäben des Zielstaates legale staatliche Handeln im fremden Raum, einschließlich nachrichtendienstlicher Tätigkeiten, das spätestens seit dem Internet und dem internationalen Terrorismus auch die einzelnen Menschen im Fokus hat. Unterschiedliche Menschenrechtsstandards der betreffenden Länder mögen dabei aufeinanderstoßen; nur eine Angleichung

⁵⁴ S. schon Ingolf Pernice in: Horst Dreier (Hrsg.), Grundgesetz Kommentar, 2. Aufl. Bd. II (2006), Art. 32 Rn. 1, 11, entsprechend zur Fragwürdigkeit des Begriffs der auswärtigen Gewalt, ebd., Rn. 18, jeweils mwN. S. auch Krieger (Fn. 38), S. 3 f.

auf der Basis der internationalen Menschenrechtserklärung und Pakte kann etwaigen daraus resultierenden Konflikten vorbeugen.

Der Staat also wird zunehmend porös, im Völkerrecht menschenrechtlich verankerte Schutzpflichten ebenso wie die Achtung der Menschenrechte sind Gebote mit globaler Reichweite im Interesse jedes Einzelnen. Das völkerrechtliche Normengeflecht zum Schutz der Menschenrechte erhält insofern einen überstaatlich-konstitutionellen Charakter, als die Staatsangehörigkeit kein Differenzierungsmerkmal mehr ist, die Geltung der Rechte nicht auf staatlicher Ordnung beruht, sondern der globalen Rechtsebene angehören. Sie binden Staaten als subjektive Freiheitsrechte des Einzelnen, aber sie sind zugleich objektive Verpflichtung zur Gewährleistung der Sicherheit in Bezug auf staatliches, aber auch auf privates Handeln.

Freiheit und Sicherheit, und damit auch Grundlagen und Grenzen der Spionage und Überwachung des Netzes sind neu zu vermessen.

III. Digitale Sicherheit und Völkerrecht

Wie angedeutet können Cyber-Angriffe von Staaten ausgehen, ebenso wie von Privaten. Eine sichere Feststellung des Ursprungs ist nach wie vor kaum möglich, und daher auch eine Verteidigung dagegen nach klassischem Muster, Abschreckung oder gar Vergeltungsschläge (»hack-back«). Treffen sie kritische Infrastrukturen, etwa die Funktion eines Atomkraftwerks, die Elektrizitäts- oder Wasserversorgung in einem Land, Verkehrssysteme oder auch Krankenhäuser, Industriebetriebe oder sonstige öffentliche oder private Einrichtungen, so sind verheerende Schäden zu befürchten. Das Völkerrecht muss sich den hiermit verbundenen neuen Fragen stellen. Dabei verfügt es nur über ein sehr begrenztes Arsenal, mit den neuen Herausforderungen umzugehen. In der Folge des (wohl) russischen Cyber-Angriffs auf Estland von 2007⁵⁵ hat das NATO Cooperative Cyber Defence Centre of Excellence hierzu auf vielen Hundert Seiten das *Tallinn Manual on the International Law Applicable to Cyber Warfare* erstellt, das 2013

⁵⁵ Vgl. Patrick Howell O'Neill, The cyberattack that changed the world, in: The Daily Dot 20 May 2016, at: <https://www.dailydot.com/layer8/web-war-cyberattack-russia-estonia/>; Patrik Maldre, The Russian Cyber Threat: View from Estonia, at: <http://cepa.org/The-Russian-Cyber-Threat-Views-from-Estonia>; and from the time: Ian Traynor, Russia accused of unleashing cyberwar to disable Estonia, in: theguardian World news 17 May 2007, at: <https://www.theguardian.com/world/2007/may/17/topstories3.russia> (last access all 15 April 2017).

veröffentlicht wurde.⁵⁶ Für die Expertengruppe, die das Werk verfasst hat, »both the jus ad bellum and the jus in bello apply to cyber operations«. Sie sucht zu erklären, wie das Völkerrecht hier anzuwenden ist und was die »cyber-unique aspects« davon sind.⁵⁷ Es gibt Aufschluss über eine mögliche Interpretation des Völkerrechts in vielen relevanten Problembereichen, die die humanitären Errungenschaften ins digitale Zeitalter zu übertragen sucht und dabei die Rechte und Pflichten des Individuums in den Mittelpunkt rückt.

Zentral erscheinen vor allem drei Fragen zur Reichweite und Fortentwicklung vorhandener völkerrechtlicher Institute:

- Inwieweit ist das Gewaltverbot des Art. 2 Abs. 4 SVN auf Cyber-Angriffe anwendbar und unter welchen Bedingungen gilt das Selbstverteidigungsrecht nach Art. 51 SVN in einem solchen Fall (dazu 1.)?
- In welchem Umfang wachsen den Vereinten Nationen, insbesondere dem Weltsicherheitsrat mit dem Auftrag der Wahrung des Weltfriedens neue Aufgaben nach Kapitel VII SVN zu (dazu 2.)?
- Kann das Kriegsvölkerrecht und insbesondere das humanitäre Völkerrecht, dessen notwendigen Wandel Daniel Thürer angesichts des *war on terror* einen bemerkenswerten Aufsatz gewidmet hat,⁵⁸ im Falle des *cyber war* Anwendung finden (dazu 3.)?

1. Gewaltverbot und Selbstverteidigung bei Cyber-Angriffen: Das Tallinn Manual

Nach Art. 2 Abs. 4 SVN unterlassen alle Mitglieder der Vereinten Nationen in ihren internationalen Beziehungen jede Androhung oder Anwendung von Gewalt. Eine Ausnahme davon gibt es nur nach Art. 51 SVN für die individuelle oder kollektive Selbstverteidigung im Falle eines bewaffneten Angriffs. Was bedeutet das für Cyber-Angriffe? Ansatzweise kann in Anlehnung an das *Tallinn*

⁵⁶ Michael N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Prepared by the International Group of Experts at the Invitation of The NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press 2013, abrufbar unter: <http://www.knowledgecommons.in/wp-content/uploads/2014/03/Tallinn-Manual-on-the-International-Law-Applicable-to-Cyber-Warfare-Draft.pdf>. For a second edition (2017) see: http://assets.cambridge.org/9781107177222/frontmatter/9781107177222_frontmatter.pdf. - According to CUP »it addresses such topics as sovereignty, state responsibility, human rights, and the law of air, space, and the sea. Tallinn Manual 2.0 identifies 154 'black letter' rules governing cyber operations and provides extensive commentary on each rule.«

⁵⁷ Ibid., S. 5.

⁵⁸ Daniel Thürer, *International Humanitarian Law: Essence and Perspectives*, SZIER 2/2007, S. 1, abrufbar unter: <http://www.ivr.uzh.ch/institutsmitglieder/thuerer/forschung/SZIER.pdf>.

Manual zu vier zentralen Fragen in der folgenden Richtung eine Antwort gesucht werden:

- a) Ist ein Hacker-Angriff auf ein Atomkraftwerk, der dieses zum Stillstand oder zur Explosion bringt und vielen Menschen das Leben kostet, Anwendung von Gewalt? Hinsichtlich der Tätigkeit erscheint das fragwürdig, denn nach herrschender Auffassung fällt unter den Gewaltbegriff nur Waffengewalt.⁵⁹ Doch hinsichtlich der Folgen kommt der Akt einem Bombardement oder Raketenbeschuss gleich. Auch wenn weder Personen noch Sachen physisch auf das Objekt wirken, sondern nur über elektronische Signale operiert wird, entsprechen die Ursächlichkeit und Wirkung des fremden, digitalen Handelns doch dem, was das Gewaltverbot verhindern soll. Die Form des Handelns und die Art der Einwirkung sollten hier keinen Unterschied machen. Die Feststellung des IGH im Nuclear Weapons Fall, dass Art. 2 Abs. 4 SVN »any use of force, regardless of the weapons employed« betrifft, wird im *Tallinn Manual* so verstanden, dass dies auch der Gebrauch eines Computers sein kann.⁶⁰ Auch der Cyber-Angriff fällt damit bei entsprechenden Folgen unter den Begriff der Gewalt. Ist die Schwelle der Gewalt nicht erreicht, so kann doch ein Fall der Intervention vorliegen.⁶¹
- b) Wird Art. 2 Abs. 4 SVN auch dann verletzt, wenn der Angriff nicht von der staatlichen Gewalt sondern von Einzelnen oder privaten Gruppen ausgeht? Das *Tallinn Manual* führt eine Mindermeinung an, nach der auch nicht-staatliche *cyber operations* die staatliche Souveränität verletzen können.⁶² In Regel 6 wird festgestellt, dass ein Staat verantwortlich ist für die *cyber operations*, die ihm zurechenbar sind.⁶³ Das ist bei staatlichem Handeln, bei Handeln im staatlichen Auftrag oder auch dann der Fall, wenn der Staat Kontrolle über den Angreifer ausübt.⁶⁴ Ein Konsens über die Kriterien der Zurechnung eines privaten Cyber-Angriffs zum

⁵⁹ S. Albrecht Randelzhofer in: Bruno Simma (Hrsg.), Charta der Vereinten Nationen. Kommentar, 1991, Art. 2 Ziff. 4, Rn. 15, mwN.

⁶⁰ *Tallinn Manual* (Fn. 56), Part I Chapter 2, The use of force, Ziff. 1, mit Verweis auf ICJ Nuclear Weapons Opinion, Ziff. 39; s. auch Rule 10, Ziff. 4.

⁶¹ Ibid., Rule 10, Ziff. 6 ff. S. auch Rule 13, Ziff. 17 ff.

⁶² Ibid., Rule 1, Ziff. 14.

⁶³ Ibid., S. 29.

⁶⁴ Vgl. etwa Rule 1, Ziff. 14, Rule 2, Ziff. 7, Rule 5, Ziff. 9, Rule 6 (vgl. dort in Ziff. 4 den Hinweis auf den Ausschluss der Cyber-Spionage per se, die völkerrechtlich nicht verboten sei). S. insbes. Rule 6, Ziff. 11 hinsichtlich »hacktivists«: »The material scope of applicability of Article 8 is relatively stringent in that it is limited to instructions, direction, or control. The State needs to have issued specific instructions or directed or controlled a particular operation to engage State responsibility.«

Verantwortungsbereich des Staates, von dessen Territorium er ausgeht, wurde aber nicht gefunden.⁶⁵ Die Kriterien, die für andere, etwa terroristische, Akte nicht-staatlicher Gruppen gelten, sollten hier indessen Anwendung finden.⁶⁶ Perspektivisch – und unter dem Gesichtspunkt einer konstitutionellen, aus den Menschenrechtspakten folgenden gemeinsamen Schutzverantwortung aller Staaten – wäre zumindest eine Kooperationspflicht der beteiligten Staaten sowohl bei der Prävention wie bei der Abwehr nicht-staatlicher Angriffe anzunehmen.

- c) Hierbei liegt ein besonderes Problem in der mit der Konstruktion des Internets verbundenen Schwierigkeit, im Einzelfall den oder die Akteure überhaupt zu identifizieren und zu lokalisieren. Auch für die Anstrengung in der Identifizierung bzw. Ortung (*geo-location*) des Angreifers ist die geforderte Zusammenarbeit von fundamentaler Bedeutung für die Sicherheit. Nachrichtendienstliche Ermittlungen und Zusammenarbeit, einschließlich der Speicherung von Verbindungsdaten können hierbei eine Rolle spielen, wobei die von den Grund- und Menschenrechten gesetzten Grenzen beachtlich bleiben. Die Kooperationspflicht erstreckt sich auch auf das Festsetzen und die Bestrafung der Angreifer. Verweigert ein Staat diese Kooperation, so spricht viel dafür, ihm selbst das Handeln zuzurechnen. Dabei kann es freilich nicht jedem einzelnen Land allein überlassen sein, unabhängig zu definieren, was ein Cyber-Angriff ist.⁶⁷ Nur gemeinsam entwickelte Standards können eine tragfähige Basis der geforderten Kooperation sein.
- d) Hinsichtlich möglicher Gegenmaßnahmen stellt sich die weitere Frage, wann ein Cyber-Angriff ein »bewaffneter Angriff« ist, der das Recht auf Selbstverteidigung nach Art. 51 SVN auslöst. Dem Zweck der Vorschrift entsprechend, die Anwendung von Gewalt zwischen Staaten weitestgehend auszuschließen, wird dieser Begriff eng ausgelegt. Er setzt die Anwendung von Gewalt im größeren Umfang voraus, wobei auch hier Gewalt als Waffengewalt verstanden wird. Die Bombardierung fremden

⁶⁵ Ibid., Rule 13, Ziff. 16 f., wonach eine Mehrheit sich für die Annahme eines bewaffneten Angriffs aussprach, freilich nicht bezogen auf den Staat, sondern auf »those cyber terrorists«.

⁶⁶ In diesem Sinne als Grundregel s. ibid., Rule 5: »A State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States«.

⁶⁷ So könnte es China als Cyber-Angriff betrachten, wenn die chinesische Firewall von Wissenschaftlern dahingehend »getestet« wird, wie mit Hilfe von TOR dem chinesischen Nutzer Wege eröffnet werden können, unbeobachtet auf kritische Webseiten zuzugreifen.

Gebiets ist ein Beispielsfall.⁶⁸ Kann das Internet als Waffe verstanden werden? Aus traditioneller Sicht ist das sicher kaum plausibel. Angesichts des Zerstörungspotentials, ggf. unter Nutzung der Schwachstellen der angegriffenen Infrastruktur Schaden anzurichten, erscheint die Annahme aber nicht ausgeschlossen, dass das Internet als Waffe zu betrachten und damit im Falle der möglichen Zerstörung erheblichen Umfangs der Angriff als »bewaffneter Angriff« iSd. Art. 51 SVN zu qualifizieren ist. Daneben werden »cyber-countermeasures« gegen den verantwortlichen Staat nach Regel 9 des *Tallinn Manual* für zulässig gehalten.⁶⁹ Aber gegen wen?

2. Neue Aufgaben und Instrumente für den Weltsicherheitsrat

Nachdem festgestellt werden kann, dass ein Cyber-Angriff Gewalt iSd. Art. 2 Abs. 4 SVN ist und vor allem auch einen bewaffneten Angriff iSd. Art. 51 SVN darstellen kann, ist auch die Verantwortung des Weltsicherheitsrats für die Wahrung des Weltfriedens nach Kap. VII der Satzung begründet. Liegt eine Bedrohung des Weltfriedens vor, ob durch Cyber-Angriff oder in anderer Weise, so kann der Sicherheitsrat insbesondere »Maßnahmen ohne Gewaltanwendung« nach Art. 41 SVN ergreifen. Zu diesen Maßnahmen gehört nach dem *Tallinn Manual* auch die vollständige oder partielle Unterbrechung der *cyber communication* mit dem betreffenden Staat oder nicht-staatlichen Akteur.⁷⁰ Alle Staaten könnten so durch den Sicherheitsrat verpflichtet werden, entsprechende gesetzliche Regelungen zu erlassen, die etwa gegenüber den Internet-Providern die Durchsetzung des Beschlusses sicherstellen.⁷¹ Und der Sicherheitsrat könne seinerseits *cyber operations* gegen einen Staat anordnen, der entgegen den Forderungen des Sicherheitsrats Atomwaffen entwickelt.⁷²

Hier stellt sich nicht nur die Frage, ob der Weltsicherheitsrat nicht die Grenzen seiner Befugnisse überschreiten würde, wenn er sich als Quasi-

⁶⁸ Vgl. in diesem Sinne Randelzhofer (Fn. 59), Art. 51 Rn. 15 ff., 21; restriktiv auch Ian Brownlie, *Principles of Public International Law*, 7. Aufl. 2008, S. 732. S. auch *Tallinn Manual* (Fn. 56), Rule 13; Ziff. : »...Whether a cyber operation constitutes an armed attack depends on its scale and effects«, und *ibid.*, Ziff. 4, wo auf die Wirkungen abgestellt wird.

⁶⁹ *Ibid.*, Rule 9.

⁷⁰ *Ibid.*, Rule 18, Ziff. 4.

⁷¹ *Ibid.*, Rule 18, Ziff. 5.

⁷² *Ibid.*, Rule 18, Ziff. 6.

Gesetzgeber geriert.⁷³ Wie im Falle der *smart sanctions* und der Kadi-Rechtsprechung des EuGH als Reaktion darauf⁷⁴ stellt sich insbesondere die Frage, welchen Rechtsschutz betroffene Einzelne bei solchen Maßnahmen des Weltsicherheitsrats haben. Soweit das Sanktionssystem zwingend mit Rechtswirkungen gegenüber dem Einzelnen operiert, entsteht eine unmittelbare Rechtsunterworfenheit des Individuums unter eine öffentliche Gewalt, die von einer effektiven Bindung an die Menschenrechte nicht befreit sein kann. Der Vorschlag, einen Internationalen Strafgerichtshof für Cyber-Kriminalität zu errichten,⁷⁵ könnte erweitert werden um einen effektiven Rechtsschutz gegenüber Resolutionen des Sicherheitsrats im Bereich der Cyber-Sicherheit. Grundlage müssten auch insoweit gemeinsame Prinzipien und Regeln sein über das, was Cyber-Kriminalität und -sicherheit bedeuten.

Das hier in der Praxis der Staaten und Institutionen sich schrittweise entwickelnde unmittelbare Rechtsverhältnis zwischen Individuum und den Vereinten Nationen als internationaler öffentlicher Gewalt, ist Ausdruck eines Konstitutionalisierungsprozesses, dessen Eckpunkte noch zu bestimmen sind.

3. Kriegsvölkerrecht und die Entwicklung eines globalen humanitären Rechts

Es drängt sich nicht auf, im Falle von Cyber-Angriffen von *cyber war* zu sprechen.⁷⁶ Die Analogie zum Krieg ist allerdings erforderlich, wenn das für bewaffnete Konflikte entwickelte humanitäre Völkerrecht zur Anwendung kommen soll. Das *Tallinn Manual* geht ohne weiteres von der Anwendbarkeit des humanitären Völkerrechts aus, weil das Kriegsrecht unabhängig von den Mitteln und Methoden der Kriegführung anwendbar sei.⁷⁷ Es dekliniert im Teil

⁷³ Von einer «usurpation of global constituent power» spricht Jean L. Cohen, *Globalization and Sovereignty. Rethinking Legality, Legitimacy, and Constitutionalism* (Cambridge University Press 2012), S. 278, 280, 282 ff.

⁷⁴ Zuletzt: EuGH Rs. C-584/10 – Kadi II. S. auch die Entscheidung des EGMR vom 26.11.2013, Case-no. 5809/08 – Al Dulimi, abrufbar unter <http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-138948>, insbes. Rn. 131 und 134; dazu Sébastien Platon, *The 'Equivalent Protection Test'. From European Union to United Nations, from Solange II to Solange I*, *European Constitutional Law Review* 2014, S. 226 ff.

⁷⁵ S. Stein Schjolberg, *Draft United Nations Treaty on an International Criminal Court or Tribunal for Cyberspace* (9th Edition, June 2014), abrufbar unter: www.cybercrimelaw.net.

⁷⁶ S. die Fragen, die in Hans-Peter Gasser/Nils Melzer, *Humanitäres Völkerrecht. Eine Einführung*, 2. Aufl. 2012, S. 198 f., aufgeworfen werden: »Können Angriffe auf Computernetzwerke, welche ohne jede Gewaltanwendung die gesamte militärische Stromversorgung, Radarüberwachung und Kommunikationssysteme des Feindes ausschalten können, überhaupt als Angriffe oder Kampfhandlungen im Sinne des humanitären Völkerrechts betrachtet werden?... Kann ein Computerkrieg überhaupt als ein bewaffneter Konflikt verstanden werden?«

⁷⁷ *Tallinn Manual* (Fn. 56), Rule 20, Ziff. 2: »As used in this Manual, armed conflict refers to a situation involving hostilities, including those conducted using cyber means«, wobei für internationale und nicht-internationale Konflikte die Beteiligung von mindestens zwei Staaten

II dementsprechend das »law of cyber armed conflict« durch, von der grundsätzlichen Anwendbarkeit auf internationale und nicht-internationale Konflikte (Rule 20), über die Verantwortlichkeit bei Kriegsverbrechen (Rule 24), die Voraussetzungen des Beteiligtenstatus (Rules 25-29), die Definition der *cyber attack* (Rule 30) und des terroristischen Angriffs (Rule 36), den Schutz der Zivilbevölkerung und von zivilen Objekten (Rules 32-40), die Mittel und Methoden der Kriegführung (Rules 41-48) und vieler weiterer den Angriff und die Angemessenheit aller weiteren relevanten Handlungen betreffenden Regeln, einschließlich des Schutzes von Gefangenen, Kindern, Journalisten, des Status besetzter Gebiete und der Achtung der Neutralität.

Die Betrachtung des Internets als Waffe und die Anwendbarkeit des Kriegrechts zeigen, dass es insoweit keine Privilegien gibt. Bemerkenswert ist gleichwohl, welch hohes zerstörerisches Potential dem Internet zuerkannt wird. In dem Sinne, wie Herfried Münkler den Wandel des Gesichts des Krieges im Lauf der Zeit beschreibt,⁷⁸ dürfte mit dem Internet als Waffe ein neuer Entwicklungsschritt eingeleitet sein. Veranlasst durch die missglückte Bezeichnung des Kampfes gegen Al-Kaida als *war on terror* bei gleichzeitiger Missachtung des humanitären Völkerrechts durch die Bush-Administration weist Daniel Thürer treffend darauf hin, dass die Ausgangssituation des Kriegsvölkerrechts heute nur selten noch gegeben ist. Nicht nur, dass militärische Operationen zunehmend elektronisch und auf Distanz ausgeführt würden; statt des Konfliktes zwischen Staaten, so schließt er sich einer Formulierung von Robert Smith an, sei das heutige Paradigma der »war amongst the people«. Die Konflikte seien von Angriffen gegen die Zivilbevölkerung und zunehmender Brutalität gekennzeichnet.⁷⁹

Dies verlangt ein Umdenken, wie es im *Tallinn Manual* nur ansatzweise sichtbar wird. Das humanitäre Völkerrecht wird sich vom Recht zwischen Staaten zum Recht zwischen Menschen entwickeln müssen, spätestens mit dem Internet. Es muss dem Einzelnen nicht nur Rechte gegenüber der staatlichen militärischen Gewalt geben, sondern auch Pflichten auferlegen. Das Budapester

(Rule 22) bzw. eine bestimmte Intensität und ein Grad der Organisation der Beteiligten Gruppen gefordert wird (Rule 23). Zu den Unsicherheiten bei der Qualifizierung des Stuxnet-Angriffs im Iran als internationaler Konflikt s. Rule 22, Ziff. 14 ff., wo das Kriterium des Umfangs des Schadens doch eingeführt wird.

⁷⁸ Herfried Münkler, *Der Wandel des Krieges von der Symmetrie zur Asymmetrie*, 2006.

⁷⁹ Thürer (Fn. 58), S. 8, mit Verweis auf die ähnliche Formulierung bei Robert Smith, *The Utility of Force – The Art of Force in the Modern World*, London 2006, S. XIII. S. auch Daniel Thürer, *Manuskript: International Humanitarian Law*, S. 336, abrufbar unter: http://www.ivr.uzh.ch/institutsmitglieder/thuerer/vorlesungen/haager_manuskript.doc.

Übereinkommen über Computerkriminalität von 2001⁸⁰ betrifft nicht die hier relevanten Fragen. Ein internationales Strafrecht ist aber zwingend. Staaten haben die Herrschaft über die Mittel der Gewalt verloren, nicht nur im Falle der *failed states*. Was sie rechtlich für sich in Anspruch nehmen, das Monopol physischer Gewalt, muss sich dem privaten Gebrauch des Internets als Waffe faktisch entgegenstellen. Eine neue Ordnung des humanitären Rechts muss daher auch den Einzelnen in die Pflicht nehmen, sie muss den Staat und die Menschen auch gegen private Angriffe schützen. Dies erfordert Instrumente, die über den Grundsatz der staatlichen Souveränität hinausgehen, ein globales Recht also, das, angeleitet von der Pflicht zum effektiven Schutz der Menschenrechte, Staaten wie auch nicht-staatliche Akteure unmittelbar bindet. Der Weg zu solch einem globalen humanitären Recht dürfte lang und steinig sein. Vielleicht ist es aber gerade der Gedanke einer »Verfassung des Internets« selbst, der die Richtung anzeigt, in die gedacht werden sollte.

IV. Internetgovernance und die »Verfassung des Internets«

Was könnte die »Verfassung des Internets« sein,⁸¹ und was hat diese ggf. mit dem Völkerrecht zu tun? Ist eine Verfassung des Internets denkbar, die Regeln für die Festlegung und Durchsetzung humanitärer Normen zumindest bei der Verwendung des Internets als Waffe enthält, vielleicht sogar ihr Verbot, jedenfalls aber auch Normen unmittelbar zum Schutz der Privatheit gegen massenhafte Datensammlung und Überwachung durch staatliche Geheimdienste und private Akteure sowie zur effektiveren Garantie anderer Menschenrechte wie der Meinungs- und Pressefreiheit, der Informationsfreiheit oder auch der Wissenschaftsfreiheit im globalen Maßstab? Können Prinzipien, die von den

⁸⁰ Abrufbar unter: <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=GER>. Vgl. dazu auch Amalie M. Weber, Council of Europe's Convention on Cybercrime, in: 18 Berkeley Technology Law Journal (2003), S. 425 ff.

⁸¹ Der Begriff wird unterschiedlich verwendet, vgl. etwa Annegret Bendiek/Ben Wagner, Die Verfassung des Internets. Die EU muss eine gemeinsame Strategie für Cyber-Sicherheit erarbeiten, in: Internationale Politik 2012, S. 85-92, die freilich eine Definition nicht liefern. Immerhin gehe es bei der zukünftigen Verfassung des Internets ebenfalls um die Förderung von Demokratie und den Schutz von Grundrechten auch außerhalb von Europa« (ebd., S. 89), abrufbar unter: <https://dgap.org/de/ip-die-zeitschrift/archiv/jahrgang-2012/november-dezember/die-verfassung-des-internets>. Zum hier verwendeten Begriff der Verfassung s. auch Ingolf Pernice, Die Verfassung der Internetgesellschaft, in: Alexander Blankenagel (Hrsg.), Den Verfassungsstaat nachdenken. Eine Geburtstagsgabe, Duncker & Humblot, Berlin (2014), S. 171-208.

Nutzern gemeinsam entwickelt und gefordert werden, zu einer »Verfassung« des Internets erwachsen.⁸²

Als »Verfassung des Internets« wird bereits der *Marco Civil da Internet* Brasiliens bezeichnet; es handelt sich um ein Gesetz, in dem Rechte und Pflichten von Bürgern, Unternehmen und auch der staatlichen Stellen hinsichtlich der Nutzung des Internets geregelt werden und dessen Zustandekommen unter reger Einbeziehung der Zivilgesellschaft durch die Snowden-Enthüllungen beflügelt wurde.⁸³ Der Begriff »Verfassung« verleiht dem Gesetz einen besonderen legitimatorischen Anspruch, darf aber nicht rechtstheoretisch als oberste Norm im politischen Gemeinwesen verstanden werden. Es gibt bislang keine Definition, die sich schon durchgesetzt hätte. Wenn im Folgenden von »Verfassung des Internets« die Rede ist, ist an die Grundordnung für ein globales Regelungssystem gedacht, das auf einem völkerrechtlichen Vertrag beruhen könnte, aber nicht muss. Die völkerrechtliche Form kann wegen der geringen Aussichten auf einen ausreichenden Konsens nicht ohne Weiteres als realistische Option betrachtet werden. Erst recht nicht kann es um Verfassungsgebung im klassischen Sinne gehen, etwa durch ein Volk als verfassungsgebende Gewalt. Ein globales Volk, das diese Kapazität hätte, gibt es nicht, auch wenn Begriffe wie Weltbürgerschaft oder *global citizenship*⁸⁴ nicht mehr utopisch erscheinen. »Verfassung des Internets« soll vielmehr die Ordnung der Internetgovernance heißen, in der eine Vielzahl von Akteuren in einer Vielzahl unterschiedlicher, aber durchaus korrespondierender Foren tätig sind und Staaten nur ein Akteur unter anderen sind.⁸⁵ Verfassung ist als Prozess zu

⁸² S. jüngst die Studie von Todd Davies, *Digital Rights and Freedoms: A Framework for Surveying Users and Analyzing Policies* (October 3, 2014), in: Luca Maria Aiello and Daniel McFarland (Eds.), *Proceedings of the 6th International Conference on Social Informatics, SocInfo 2014* (Barcelona, November 10-13), Springer LNCS Series, 2014, abrufbar unter: <http://ssrn.com/abstract=2507608>, S. 1 f., 14: »The current moment is one of revival for the idea of a «bill of rights» or «constitution» for users online.

⁸³ S. dazu Carlo Pilz, *Brasilien: Gesetzentwurf der »Verfassung des Internets« veröffentlicht*, in: De Lege Lata. Datenschutz-Privacy-Web 2.0, v. 14.11.2013, abrufbar unter: <http://www.delegedata.de/2013/11/brasilien-gesetzentwurf-der-verfassung-des-internets-veroeffentlicht/>. S. auch Danilo Fariello, *Modelo do Marco Civil da Internet pode ser exportado, diz especialista*, in: O Globo v. 10.7.2014, abrufbar unter: <http://oglobo.globo.com/sociedade/modelo-do-marco-civil-da-internet-pode-ser-exportado-diz-especialista-13214629>. Das Gesetz wurde im April 2014 vom Senat Brasiliens angenommen, vgl. Andreas Knobloch, *Brasiliens Verfassung fürs Internet*, in: heise-online v. 25.4.2014, abrufbar unter: <http://www.heise.de/tp/artikel/41/41594/1.html>.

⁸⁴ S. etwa: Anne Peters, *Dual Democracy*, in: Jan Klabbers, Anne Peters, Geir Ulfstein (eds.), *The Constitutionalization of International Law* (Oxford University Press, 2009), S. 263, 296 -313, insbes. S. 307-313: »globalization of citizenship«. Jürgen Habermas, *The crisis of the European Union. Response* (Polity Press, Cambridge 2012), S. 58-59, 62, 65: »world citizen». A number of civil society organisations use the term global citizen, e.g. <http://www.globalcitizen.org/>, or <http://www.newglobalcitizens.org/>.

⁸⁵ Zur Internet Governance s. etwa Roxana Radu/Jean-Marie Chenou/Rolf H. Weber (Hrsg.), *The Evolution of Global Internet Governance. Principles and Policies in the Making* (Springer 2013); zum Begriff aufschlussreich: Jeanette Hofmann, *Internet Governance. Zwischen staatlicher Autorität und privater Koordination*, in: ipg 3/2005, aufrufbar unter:

verstehen,⁸⁶ sie ist nicht Setzung, sondern emergent,⁸⁷ Ausdruck eines sich entwickelnden Zusammenhangs verfassender Elemente,⁸⁸ der nicht unbedingt dem klassischen Bild einer Verfassung entsprechen muss, sondern fragmentarisch bleiben mag und ohne schriftliches Dokument.

Die schrittweise Entwicklung von Elementen einer Ordnung der Internet-governance, bzw. der Prozess der Emergenz einer Verfassung des Internets haben sehr unterschiedliche Beteiligte: Basis, Rahmen und zugleich betroffen ist die Öffentlichkeit, die sich in Medien und vor allem über das Internet durch die »Emergenz digitaler Öffentlichkeiten«⁸⁹ artikuliert – im entgrenzten Cyber-Raum, also einer vernetzten Öffentlichkeit die dynamisch, divers, dezentralisiert und effektiv über staatliche Grenzen hinaus existiert. Je nach Thema und Arena spielen die Staaten eine Rolle, die Vereinten Nationen sowie andere internationale Organisationen, wie die ITU; hinzu kommen die Zivilgesellschaft und ihre Vertreter, die bei der Artikulierung der relevanten Interessen unterstützend und kanalisierend wirken; auch die Vertreter der Wirtschaft und insbesondere der global operierenden Unternehmen gehören dazu, wie schließlich die *scientific communities* insbesondere aus den Bereichen der Technik, der Sozialwissenschaften und des Rechts. Es ist ein »Multi-Stakeholder-Prozess«, der auf den vorhandenen, auch – aber nicht nur - völkerrechtlichen Strukturen aufbaut, aus ihnen heraus wächst, sie ihrerseits ändert und dabei zunächst ergebnisoffen bleibt. Beispiel und zugleich einer der Ausgangspunkte der Internetgovernance ist die Entwicklung des Systems der Vergabe der Domain-Namen durch ICANN, die Lars VIELLECHNER als Prozess der Eigenkonstitutionalisierung bezeichnet und

http://www.fes.de/ipg/IPG3_2005/03JHOFMANN.PDF; zuletzt dies./Christian Katzenbach/Kirsten Gollatz, Between Coordination and Regulation: Conceptualizing Governance in Internet Governance, HIIG Discussion Paper Series, Discussion Paper No. 2014-04, abrufbar unter: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2484463: Governance as «reflexive coordination».

⁸⁶ In diesem Sinne auch das Votum von Sascha Schumacher, Die Verfassung des Netzes, in: digital constitution – Verfassungsrecht und –politik im Spiegel der digitalen Welt, 3.5.2012, abrufbar unter: <http://www.uni-muenster.de/Jura.tkr/digitalconstitution/?p=406>.

⁸⁷ Zum Konzept vgl. Hans Vorländer, Die Verfassung vor, nach, über und unter dem Staat. Die Konstitutionalismusdebatte in der Suche nach einem anderen Verfassungsbegriff, in: Helena Lindemann/Mina Malaviya/Alexander Hanebeck/Felix Hanschmann/Raner Nickel/Timo Tohidipur (Hrsg.), Erzählungen vom Konstitutionalismus, 2012, S. 36: »das Problem der Verfassungsgeltung ist zureichend nur als ein komplexer Prozess der Emergenz zu verstehen. Die Verfassung gewinnt ihren spezifischen Verfassungscharakter damit erst in einem offenen und öffentlichen Prozess, die stabilisierende, orientierende und regulative Funktion ist mehr ein Produkt erfolgreicher Praxis über Zeit, denn Faktum historischer Setzung«.

⁸⁸ Zum Begriff und Ansätzen im Rahmen einer »universellen Verfassungslehre« vgl. Peter Häberle, Der kooperative Verfassungsstaat – aus Kultur und als Kultur. Vorstudien zu einer universalen Verfassungslehre, 2013, S. 100 ff.

⁸⁹ Vgl. Stefan Münker, Emergenz digitaler Öffentlichkeiten. Die sozialen Medien im Web 2.0, 2009. Yochai Benkler, A Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth State, Harvard Civil Rights-Civil Liberties Law Review, Draft (2011) abrufbar unter: http://benkler.org/Benkler_Wikileaks_current.pdf, spricht von einer politischen Öffentlichkeit im Sinne eines »Networked Fourth Estate«.

beschreibt.⁹⁰ Der Staat (die USA) ist hier nur am Rande beteiligt, das auf einem Geflecht privatrechtlicher Verträge beruhende »transnationale Regelungsarrangement«⁹¹ errang globale Bedeutung und ist das Ergebnis des Zusammenwirkens einer Vielzahl diverser Akteure. Die Kritik an der Abhängigkeit der ICANN vom amerikanischen Recht und amerikanischer Aufsicht führte zur Ankündigung, diese Bindung aufzulösen und eine neue Struktur zu finden.⁹² Ihre Unterwerfung unter das Regime der ITU, wie Russland und China das fordern, würde sie zum Völkerrecht zurückführen; die USA und die Mehrzahl der OECD-Staaten ziehen das »Multi-Stakeholder-Modell« vor, doch ist eine konkrete Lösung noch nicht in Sicht.⁹³

Völkerrechtlich radiziert und jedenfalls anfänglich vom Modus des UN-Systems geprägt war dagegen die Entwicklung des Internet Governance Forums (IGF), das im Jahre 2014 zum neunten Mal tagte. An diesem Forum in Istanbul fanden rund 3000 Personen aus allen »Stakeholder-Gruppen« zur öffentlichen und inklusiven Debatte der dringlichsten Probleme zusammen.⁹⁴ Die Einrichtung des IGF geht von der Generalversammlung Vereinten Nationen aus.⁹⁵ Hier werden keine Entscheidungen getroffen. Aber der Austausch von Gedanken und die Diskussion weiterführender Vorschläge gibt den Teilnehmern Einblick in das Interessengeflecht und die wichtigsten Positionen zu Einzelfragen, als Grundlage für entsprechende Schritte in anderen Foren und Gremien, die ggf. mit mehr Entscheidungskompetenz ausgestattet sind.

Das deliberative »Multi-Stakeholder-Verfahren« des IGF, an dem jeder unmittelbar oder, soweit er Zugang zum Internet hat, auch on-line teilnehmen kann und das auf der Webseite des IGF dokumentiert ist, nimmt für sich zwar nicht in Anspruch, repräsentativ zu sein, und sicher nehmen potente Wortführer einzelnen weniger renommierten Stimmen Raum und Aufmerksamkeit;⁹⁶ doch gibt es so lange kein Legitimationsproblem, wie es allein um Meinungs- und

⁹⁰ Lars Viellechner, Transnationalisierung des Rechts, 2013, S. 127-143, 253 ff., 257 ff.

⁹¹ Ibid., S. 147 ff., 262.

⁹² Vgl. NTIA Announces Intent to Transition Key Internet Domain Name Functions, abrufbar unter: <http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions>.

⁹³ Vgl. dazu Bendiek/Wagner (Fn. 81), S. 87 f.

⁹⁴ Vgl. die Begrüßung durch den Vorsitzenden der »Multistakeholder Advisory Group«, Botschafter Janis Karlins, IGF 2014 – the gateway for the future, abrufbar unter: <http://www.intgovforum.org/cms/blog-igf-2014>.

⁹⁵ UN General Assembly Resolution 56/183 (21 December 2001), die der ITU die Verantwortung für die Organisation des World Summit of the Information Society (WSIS) 2003/2005 überträgt; die dort beschlossene »Tunis Agenda« sieht in Ziff. 72 die Einberufung des Internet Governance Forums vor. Weitere Information zum WSIS unter: <http://www.itu.int/wsisis/basic/about.html>.

⁹⁶ Krit. insofern Aust (Fn. 1).

Willensbildung ohne jede verbindlichen Festlegungen geht. Was hier »vorgedacht« und diskutiert wird, kann allerdings Legitimationsfragen aufwerfen, wenn es in die Verhandlungen anderer Foren oder Institutionen einfließt, die – wie die von Brasilien veranstaltete NETmundial von 2014⁹⁷ – darauf gerichtet sind, Prinzipien zu formulieren,⁹⁸ an denen sich die Politik der Staaten und auch internationaler Organisationen orientieren, die aber auch Richtschnur für die Entwicklung von Standards sein können, welche von technischen Normierungsgremien, wie der IETF,⁹⁹ oder als Maßstab unternehmerischen Handelns im Rahmen der *corporate social responsibility* (CSR)¹⁰⁰ entwickelt werden. Je breiter die Konsensbasis, desto mehr Legitimität könnte den so entwickelten Prinzipien zukommen, desto größer ist jedenfalls der Geltungsanspruch solcher rechtlich unverbindlichen Prinzipien oder Standards und desto erheblicher können sie auch als Orientierung für die staatliche Politik oder als Referenz für Verpflichtungen werden, wie sie in der Folge Gegenstand internationaler Konventionen werden könnten.

Das Völkerrecht des Netzes kann auf diese Weise normativ verbindlich Standards und Prinzipien in positives Recht verwandeln, deren Inhalt sich möglicherweise in einem Dreischritt herausbildet:

- Im offenen Diskurs der durch das Internet möglichen, schrittweise sich entfaltenden global vernetzten Öffentlichkeit,
- mit der diskursiven Artikulierung der hier entwickelten Auffassungen und Interessen auf öffentlichen Foren wie dem IGF
- und durch die Verdichtung und Transformation der tragenden Leitgedanken aus dieser Diskussion in Prinzipien und Standards.

⁹⁷ Global Multistakeholder Meeting on the Future of Internet Governance, on the invitation of the government of Brazil, offizielle Website: www.netmundial.org. Zu den Ergebnissen s. das NETmundial Multistakeholder Statement vom 24. April 2014, mit den »Internet Governance Principles« und einer »Roadmap for the future evolution of the Internet Governance Ecosystem«, abrufbar unter: <http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf>.

⁹⁸ Dazu Jeanette Hofmann, Inside NETmundial – Wie in Brasilien über die Zukunft des Internets diskutiert wird, HIIG Blog, 28 April 2014, abrufbar unter: <http://www.hiig.de/inside-netmundial-wie-in-brasilien-uber-die-zukunft-des-internet-diskutiert-wird/>.

⁹⁹ Internet Engineering Task Force (IETF), zu Organisation und Verfahren s. die Website: <https://www.ietf.org/>.

¹⁰⁰ Vgl. etwa Birgit Spießhofer, Unternehmerische Verantwortung, in: Hanno Kube, Rudolf Mellinshoff, Gerd Morgenthaler, Ulrich Palm und Thomas Puhl (Hrsg.), Leitgedanken des Rechts. Paul Kirchhof zum 70. Geburtstag (C.F.Müller, Heidelberg 2013), S. 1235-1245; Birgit Spießhofer/Friedrich Graf von Westphalen, Corporate Social Responsibility und AGB-Recht, in: 70 Betriebsberater (2015), S. 75-85. Zu den Maßnahmen auf EU-Ebene zur CSR s. zuletzt die Richtlinie 2014/95/EU des Europäischen Parlaments und des Rates vom 22. Oktober 2014 zur Änderung der Richtlinie 2013/34/EU im Hinblick auf die Angabe nichtfinanzieller und die Diversität betreffender Informationen durch bestimmte große Unternehmen und Gruppen, ABl. 2014 L 330/1, dazu Thomas Volland, Erweiterung der Berichtspflichten für Unternehmen nach der neuen CSR-Richtlinie, in: 49 Der Betrieb (2014), S. 2815-2818.

Als Modell eines solchen Prozesses vom Gedanken zur Norm bietet sich der Rio-Prozess an, in dem die Prinzipien der Rio-Erklärung und die Agenda 21 als Ergebnis eines langjährigen weltweiten Diskurses über Umwelt und Entwicklung Zwischenschritt und Orientierung für internationale Konventionen und nationale Politiken auf dem Wege zur Nachhaltigkeit wurden. Dem Governance-Ansatz folgend ist die zur weiteren Dynamisierung des Prozesses die 1992 eingesetzte »Commission of Sustainable Development« auf der Rio+20 Konferenz 2012 ersetzt worden durch das »High-Level Political Forum of Sustainable Development«,¹⁰¹ in dessen Arbeit die relevanten nicht-staatlichen Akteure einbezogen werden sollen.¹⁰² Das neue, »hybrid« strukturierte Forum ist am »Multi-Stakeholder-Modell« orientiert, und gerade davon werden Impulse für größere Effizienz erwartet. Bemerkenswert ist dabei die neue Rolle der Vereinten Nationen nach der Zuschreibung der für die Einrichtung des neuen Forums eingesetzten Expertengruppe:

»The UN is a 'norm-setting' institution; how best can the forum and international community help to translate agreed norms into policies at the national level?«¹⁰³

Inwieweit sich diese Funktion aus dem Text der Satzung der Vereinten Nationen herauslesen lässt, bedarf einer genaueren Prüfung. Möglicherweise wird, wie sich u. a. aus Art. 31 Abs. 3 lit. b) der Wiener Vertragsrechtskonvention ergibt, die konsentierende nachfolgende Praxis eine solche neue, auch erweiternde Auslegung der Satzung tragen.¹⁰⁴

Die im Rio-Prozess entwickelten Ansätze lassen sich gewiss nicht Eins zu Eins auf die Internetgovernance übertragen. Sie deuten indessen auf eine Richtung hin, in der zumindest mittelfristig globale Herausforderungen normativ beantwortet werden können, auch im Bereich einer notwendigen globalen Regulierung des Internets. Die Generalversammlung der Vereinten Nationen hat mit dem Anstoß zur Gründung des IGF bereits ein Stück Verantwortung übernommen. Zu den spezifischen Fragen einer Cyber-

¹⁰¹ Näheres auf der Webseite <http://sustainabledevelopment.un.org/csd.html>.

¹⁰² UN Sustainable Development Knowledge Platform, Announcement for the Expert Group Meeting on the role of the high-level political forum on sustainable development in post-2015 development framework, 30 April – 1 May 2014, available at: <http://sustainabledevelopment.un.org/index.php?page=view&nr=667&type=13&menu=1556>.

¹⁰³ S. <http://sustainabledevelopment.un.org/index.php?page=view&nr=998&type=12&menu=1556>.

¹⁰⁴ Zum Grundgedanken vgl. Christopher Peters, Praxis Internationaler Organisationen – Vertragswandel und völkerrechtlicher Ordnungsrahmen, Diss. Berlin, i.E. (2015).

Sicherheitspolitik dürfte dem Weltsicherheitsrat eine wichtige Rolle zukommen, die über die Reaktion auf konkrete Bedrohungen des Friedens hinaus um der Prävention willen auch ein proaktives Wirken einschließt. Dem durch die Resolution Nr. 60/251 ins Leben gerufenen UN-Menschenrechtsrat obliegt es schließlich, u.a. durch Empfehlungen an die Generalversammlung für die vorbehalts- und ausnahmslose Bindung jeder öffentlichen Gewalt an die Menschenrechte insbesondere hinsichtlich des Schutzes von Privatheit, Meinungs- und Informationsfreiheit einzutreten und die effektive Wahrnehmung entsprechender Schutzpflichten gegenüber privaten Eingriffen durch die einzelnen Staaten, aber auch auf globaler Ebene durch die Staatengemeinschaft zu fordern und zu fördern.

Die wenigen hier aufgezeigten Elemente einer Verfassung des Internets, die sich als Ordnung der Aufgaben, Befugnisse und des Zusammenspiels von öffentlichen und auch privaten Akteuren – im Sinne der Internetgovernance – entwickelt, sind damit Ausdruck dessen, was als Völkerrecht des Netzes verstanden werden kann. Sie zeigen zugleich einen Wandel des Völkerrechts hin zu einem globalen Rechtsrahmen an, der die Menschen als Adressaten und auch als Legitimationssubjekte anerkennt und damit einen konstitutionellen Charakter annimmt.