www.jusletter-it.eu

Rolf H. Weber

Cybergovernance revisited

Regulierungserwartungen für die Zukunft

Die Cybergovernance ist den Kinderschuhen entwachsen. Internet-Regulierungen haben zwar in den letzten Jahren teilweise nationale Ausrichtungen eingeschlagen, doch sind die Chancen, eine verbesserte globale digitale Kooperation zu erreichen, intakt. Weitere Anstrengungen, die bis 2025 zu einem gestärkten IGF+ führen können, erscheinen deshalb als lohnenswert.

Beitragsart: Beiträge

Zitiervorschlag: Rolf H. Weber, Cybergovernance revisited, in: Jusletter IT 30. September 2021

ISSN 1664-848X, jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77

Inhaltsübersicht

1. Einleitung

[1] Cybergovernance[1] hat fast einen magischen Klang; Erinnerungen an die – nun 25 Jahre alte – emphatische Erklärung vom Februar 1996 zur «Independence of Cyberspace» des vor drei Jahren verstorbenen John Perry Barlow werden wach:[2] «I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear. Cyberspace does not lie within your borders.» In der Zwischenzeit hat sich aber die Erkenntnis durchgesetzt, dass auch das Internet stark reguliert ist und dass die Staaten insbesondere die faktische Möglichkeit haben, ihre Regulierungen in weitem Ausmasse durchzusetzen. Die frühen Technologie-Experten haben die heutigen technologischen Eingriffsmittel somit in keiner Weise vorausgesehen.

[2] Internet Governance ist ein Begriff, der im Wesentlichen vor gut 15 Jahren seine hauptsächliche Konkretisierung erfahren hat, insbesondere im Kontext der beiden Weltinformations-Gipfel von 2003 und 2005. Governance geht etymologisch zurück auf Kybernetes und Gubernator, den Steuermann. In Frage steht das Ringen um gemeinsame Regeln und um Fragen der Grundordnung des Zusammenlebens im Cyberspace.[3] «*Revisited*» muss mit einschliessen, einen Blick in die Vergangenheit zu werfen und eine Bewertung eingetretener Entwicklungen vorzunehmen; nur wer das historisch Geschehene richtig versteht, ist in der Lage, einen ungetrübten Blick in die Zukunft zu werfen.

---

1 Generalthema des (online bzw. hybrid durchgeführten) 24. Internationalen Rechtsinformatik Symposiums IRIS 2021 war die «Cybergovernance». Nach dem Einführungsvortrag (Januar 2021) und dem eigentlichen Tagungsbeitrag zur «Duty of Co-operation» (Jusletter IT vom 25. Februar 2021) durfte der Autor des vorliegenden Aufsatzes am 17. Juni 2021 den Schlussvortrag zum Thema «Cybergovernance revisited» im Rahmen einer zu seinen Ehren von Prof. Dr. Erich Schweighofer (Wien und Brüssel) grosszügig organisierten Schlussveranstaltung in der Klimtvilla (Wien), umrahmt von einem musikalischen Programm, halten. Der Text gelangt hiermit – auch als Dank an Erich Schweighofer – im Vortragsstil, indessen ergänzt durch Fussnoten, zur Publikation.

2 Vgl. https://projects.eff.org/de/cyberspace-independence; die Deklaration konnte kürzlich ihren 25. Geburtstag feiern; vgl. dazu auch Wolfgang Kleinwächter, 25 Years of John Perry Barlow's Declaration of Independence in Cyberspace: When Visions Meet Realities, CircleID of February 6, 2021, [open access, 25 Years of John Barlow's Declaration of Independence in Cyberspace: When Visions Meet Realities (circleid.com)] bzw. https://www.circleid.com/posts/20210206-25-years-of-john-barlows-declaration-of-independence-in-cyberspace/.

3 Rolf H. Weber, Internet Governance at the Point of No Return, EIZ Publishing, Zürich 2021, S. 79 [open access, Internet Governance at the Point of No Return (eizpublishing.ch)].

2. Traditioneller Regulierungsrahmen der Internet Governance

[3] Ursprünglich war die Internet Governance konzipiert als Ausdruck für die Gestaltung (d.h. das Design) und die Verwaltung der Technologien, die das Internet funktionsfähig («*operational*») machten. Mehr und mehr ist die technologische Betrachtungsweise aber durch Politiken («*policies*») überlagert worden. Aus diesem Grunde wird der Internet Governance insbesondere die Erfüllung folgender Funktionen zugeschrieben:[4]

- Verwaltung der kritischen Internet Ressourcen (z.B. Namen und Nummern);
- Festlegung der technischen Internet Standards;
- Koordination des Zugang zum Netz und Interkonnektion von Netzen;
- Governance mit Bezug auf Cybersicherheit und Cyberstabilität;
- Regulierung der Rollen von privaten Internet-Intermediären und von Plattformen;
- Durchsetzung legitimierbarer architektur-basierter Immaterialgüterrechte.

[4] Die Liste dieser Politiken zeigt, dass heute nicht mehr allein Themen der Infrastruktur zur Diskussion stehen, sondern ebenso sehr weitere Lebensbereiche eine Rolle spielen, d.h. die Governance betrifft nicht allein das Internet, sondern den ganzen Cyberspace, was die Schaffung des Begriffs «Cybergovernance» gerechtfertigt hat.[5]

[5] In der Rechtswissenschaft wird traditionell oft zwischen dem sog. Hard Law und Soft Law unterschieden.[6] Das Hard Law umfasst die rechtlich durchsetzbaren Normen, etwa in internationalen Verträgen sowie im regionalen (EU) oder nationalen Recht. Multilaterale Verträge zu Internet-Rechtsfragen gibt es – abgesehen von Verträgen im Bereich der Telekommunikation – nur in beschränktem Ausmass (z.B. im Urheber- oder Handelsrecht). Vielmehr überwiegen die «Regeln» des Soft Law, etwa in der Form von Selbstregulierungen (z.B. ICANN) oder technischen Standardisierungen (z.B. IETF). Die Erfahrungen der letzten Jahre im Wirtschaftsrecht (z.B. auch im Finanzmarktbereich) haben aber gezeigt, dass die Dichotomie von Hard Law und Soft Law überwunden werden muss, die beiden Rechtsquellen überlagern sich in relevanter Weise.[7]

[6] Die gegenseitige Verflechtung von Hard Law und Soft Law hat zum rechtstheoretischen Ansatz des Konzepts der polyzentrischen Regulierung geführt, der zum Ausdruck bringt, dass die anwendbaren «Modelle» ein komplexes Geflecht bzw. Netzwerk von verschiedenartigen Normen bilden.[8] Mit Bezug auf die beteiligten Akteure findet zum Teil der Begriff der Co-Regulierung, der das Zusammenspiel von öffentlichen und privaten Regulatoren zum Ausdruck bringt, Anwendung.[9]

---

4 Vgl. Laura deNardis, Introduction: Internet Governance as an Object of Research Inquiry, in: DeNardis/Cogburn/Levinson/Musiani (eds.), Researching Internet Governance – Methods, Frameworks, Futures, Cambridge MA 2020, S. 1, 4 m.w.V.

5 Vgl. Rolf H. Weber, Duty of Co-operation as a New Cybergovernance Concept, Jusletter IT, 25. Februar 2021, Rz. 1; für eine rechtstheoretische Analyse von fünf Cybergovernance-Bezugsrahmen vgl. Vytautas yras/Friedrich Lachmayer, Frames of Cybergovernance, Jusletter IT, 25. Februar 2021.

6 Rolf H. Weber, Regulatory Models for the Online World, Zürich 2002, S. 85 ff.

7 Rolf H. Weber, Integrity in the «Infinite Space» – New Frontiers for International Law, Heidelberg Journal of International Law 2021, Kap. V (im Erscheinen).

8 Weber (Fn. 3), S. 28 f.

9 Vgl. auch Myriam Senn, Non-State Regulatory Regimes. Undertaking Institutional Transformation, Berlin 2011, S. 43, 139 ff., 230.

3. Akteursorientierte Phasen der Cybergovernance

[7] Historisch gesehen kann man verschiedene akteursorientierte Phasen in der Entwicklung des Internet und damit der Cybergovernance, die es wert sind, kurz angespochen zu werden, unterscheiden:[10]

[8] (i) Die erste Phase war militärisch geprägt (1957–1970); die Entwicklung des sog. DARPA-Net erfolgte schwergewichtig durch US-Militärangehörige.

[9] (ii) Die zweite Phase (1970–1990) hat sich überwiegend an den Universitäten abgespielt; Forscher entwickelten die Infrastrukturprotokolle, z.B. das Transport Control Protocol (TCP) und das Internet Protocol (IP). Die Verfügbarkeit einer globalen Infrastruktur war die Voraussetzung für die nachfolgende Verbreitung des Internet in der Geschäftswelt und der Zivilgesellschaft.

[10] (iii) Die dritte Phase (1990–1998) hat mit der Entwicklung des World Wide Web (WWW) durch Tim Berners-Lee am CERN in Genf begonnen; das WWW machte es möglich, das Internet kommerziell zu nutzen; in diese Zeit des Aufbruchs fällt auch die erwähnte Veröffentlichung der «Declaration of Independence of Cyberspace» von John Perry Barlow.

[11] (iv) Die vierte Phase (1998–2010) hat zu einem grösseren Einfluss bzw. zur Mitwirkung der Politik in der Gestaltung des Cyberspace geführt. Der Versuch, ICANN einer politischen Kontrolle zu unterwerfen, die Einigung auf ein E-Commerce Programm in der WTO (1998), die von der UNO und der ITU initiierte Durchführung der beiden Weltinformationsgipfel in Genf und Tunis (2003, 2005) sowie schliesslich die Schaffung des Internet Governance Forum (IGF) zeigen deutlich das Interesse der Politik an der Implementierung von Regeln im Cyberspace.

[12] (v) Die fünfte Phase (2010–2020) ist durch eine massgebliche Stärkung der Zivilgesellschaft geprägt gewesen. Smartphones und Social Networks als technologische Innovationen haben die Möglichkeiten erweitert, dass alle gesellschaftlichen Kreise an den grenzüberschreitenden Informationsflüssen und Tätigkeitsausübungen im Cyberspace mitwirken können. Regulatorisch hat parallel dazu insbesondere über das IGF und die NetMundial Konferenz (Sao Paulo, 2014) das Multistakeholder-Modell einen erheblichen Bedeutungszuwachs erfahren. Das Multistakeholder-Prinzip meint:[11] «Development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures and programs that shape the evolution and the use of the Internet». Zwei Aspekte sind in dieser Umschreibung besonders wichtig, nämlich die erwähnten Beteiligten (Regierungen, der private Sektor und die Zivilgesellschaft) sowie die Breite der Rechtsquellen, die sich nicht auf formelle Gesetze beschränken, sondern das Soft Law miteinschliessen. Wolfgang Kleinwächter hat vor zehn Jahren einen wegweisenden strukturellen Vergleich zwischen den «United Nations» als Regierungs-Modell und den «United Constituencies» als Multistakeholder-Modell entwickelt.[12]

[13] (vi) Die sechste Phase (ab 2020), begleitet von stärkeren Bemühungen der UNO, einen Beitrag zur digitalen Kooperation zu leisten, zeigt – nicht zuletzt auch mit Blick auf die Cybersecurity – deutliche geo-strategische Herausforderungen; der Cyberspace ist zu einem «umkämpften»

10 Vgl. auch Kleinwächter (Fn. 2), S. 1 ff.

11 Report of the Working Group on Internet Governance, Juni 2005, www.wgig.org/docs/WGIGREPORT.pdf.

12 Wolfgang Kleinwächter, A New Generation of Regulatory Frameworks: The Multistakeholder Internet Governance Model, in: Sethe et al. (eds.), Kommunikaton, Festschrift für Rolf H. Weber, Bern 2011, S. 559, 571 f.

Raum der Grossmächte geworden.[13] Mit der anvisierten Realisierung des IGF+ besteht aber auch die Chance der Schaffung einer globalen Regulierungsordnung im Cyberspace.

4. Völkerrechtliche Rahmenbedingungen der Cybergovernance

[14] Die völkerrechtlichen Rahmenbedingungen der Cybergovernance sind recht vielfältig und auch im Fluss. Verschiedene Erscheinungen und Entwicklungen stehen zur Diskussion:[14]

[15] (i) *Digitale Verfassungsordnungen*: Im Rahmen des Internet Governance Forum (IGF) ist bereits vor 10 Jahren eine Internet Bill of Rights durch die entsprechende Dynamic Coalition entwickelt worden. Materiell geht es bei dieser Bill of Rights um die Auslegung der bekannten Menschenrechte im Internet-Kontext. Sogar ein Entwurf für eine Internet-Verfassung, der sich strukturell und inhaltlich an traditionelle Verfassungen anlehnt, liegt vor.[15]

[16] (ii) *Internationale Rechtsprinzipien*: Schon heute finden sich in mehreren UNO-Konventionen und Leitlinien materielle rechtsgestaltende Grundsätze, deren Anwendung auch im Kontext der Cybergovernance als sinnvoll erscheint.

[17] Art. 38 des Statuts des Internationalen Gerichtshofs nennt neben den multilateralen Staatsverträgen insbesondere auch die allgemeinen Rechtsprinzipien als wesentliche Rechtsquellen der internationalen Normenordnung. Materiell geht es um Grundsätze, die rund um den Globus zur Geltung gebracht werden sollen.[16] Im Kontext der Cybergovernance vermögen insbesondere die Prinzipien von Treu und Glauben sowie des Vertrauensschutzes eine Rolle zu spielen.

[18] Ein wichtiges rechtsrelevantes Konzept ist die Pflicht zur Zusammenarbeit («Duty of Co-operation»).[17] Diese Leitlinie ist in einer Vielzahl von UNO-Dokumenten erwähnt. Bereits die UNO-Charta verweist darauf, dass internationale Probleme ökonomischer, sozialer, kultureller oder humanitärer Natur mittels gegenseitiger Zusammenarbeit zu lösen seien. Kap. 4 der UNO-Charta ist der ökonomischen und sozialen Kooperation gewidmet. Weitere UNO-Dokumente verweisen auf diesen Grundsatz in ähnlicher Weise. Auf regionaler Ebene betonen die Helsinki Akte von 1975 als Dokument zur Gründung der Organisation für Sicherheit und Zusammenarbeit in Europa den Kooperationsgedanken. Auch die internationale Gerichtsbarkeit bezieht sich auf den Zusammenarbeits-Grundsatz (Gulf of Maine-Urteil des Internationalen Gerichtshofs).[18]

[19] Zur gemeinsamen Werteordnung gehört eine ganze Reihe weiterer Prinzipien, die grenzüberschreitende Geltung beanspruchen:[19]

- Globale öffentliche Güter sollen allen Menschen rund um die Weltkugel zur Verfügung stehen; Beispiele sind etwa Natur und Klima. Die einseitige Beanspruchung durch Staaten, Unternehmen oder Private widerspricht der Idee des angemessenen Zugangs für alle.

---

13 Vgl. auch Wolfgang Kleinwächter, Herrscht im Internet schon Krieg?, Frankfurter Allgemeine Zeitung, 18. Februar 2021, S. 13.

14 Vgl. dazu Weber (Fn. 3), S. 36 ff.

15 Eva Thelisson, Un Etat Mondial via Internet?, Puteaux 2012, S. 89 ff.

16 Eingehender dazu Weber (Fn. 3), S. 90.

17 Weber (Fn. 5), Rz. 10.

18 Für weitergehende Ausführungen vgl. Weber (Fn. 5), Rz. 11 ff.

19 Weber (Fn. 3), S. 92 ff. und Weber (Fn. 7), Kap. IV.

- Gemeinsam benutzte Räume (sog. «*international spaces*») als zentrale Cyberspace-Erscheinungen dürfen nicht von einzelnen Staaten exklusiv belegt werden; Beispiele sind etwa die Meere und das Weltall. Faktisch geht es meist um die Ausnutzung von Ressourcen. So legt der Weltraum-Vertrag von 1967 fest, dass ein «*equitable use*» die protektionistische Ausnutzung der Ressourcen durch einzelne Staaten verhindern soll.[20]
- Der Grundsatz der *due diligence* findet sich in verschiedenen internationalen Instrumenten, die sich mit Handelsströmen und Lieferketten beschäftigen (z.B. OECD-Leitlinien für multinationale Unternehmen); wer Ressourcen beansprucht, hat dies mit der angemessenen Sorgfalt zu tun. Auch in den laufenden Bemühungen der WTO, regulatorische Grundlagen für den Handel mit digitalen Gütern und Dienstleistungen zu schaffen, spielt die *due diligence* eine wichtige Rolle.

[20] Die Einhaltung der gemeinsamen Werteordnung lässt sich auch rechtlich durchsetzen. Seit 20 Jahren gibt es auf der UNO-Ebene die Grundsätze der Staatenverantwortung, die insbesondere auf dem Prinzip der gegenseitigen Rücksichtnahme beruhen.[21] Diskutieren lässt sich, ob die Staatenverantwortung ebenso auf grosse private Unternehmen als «*keepers of international law*»[22] anwendbar sei. Zwar ist die rechtliche Durchsetzung der Verantwortungs-Grundsätze nicht immer einfach, doch vermögen sie zumindest eine politische und reputationsmässige Breitenwirkung zu entfalten.

[21] (iii) *Transnationalismus*: Dass Rechtsregeln grenzüberschreitend zu harmonisieren sind, ist keine neue Erkenntnis. Bereits im Mittelalter haben die Handelsleute eine sog. *lex mercatoria* entwickelt. Mit der stärkeren Globalisierung ist das Bedürfnis nach transnational vereinheitlichten Standards gewachsen.[23] Ausdruck davon sind z.B. auch die Modellgesetze der UNCITRAL.

[22] (iv) *Kosmopolitanismus*: Seit der Zeit von Aristoteles wird die Erkenntnis vertreten, dass – rechtsphilosophisch betrachtet – gewisse Grundsätze wie die Gerechtigkeit oder die gegenseitige Rücksichtnahme im Rahmen von verantwortungsbewussten globalen Governance-Prinzipien zu verwirklichen sind. Solche Grundsätze, die zum «Public Core» des Internet gehören, haben einen universellen Charakter.[24]

[23] Die Anwendung allgemeiner rechtlicher Konzepte, wie sie knapp erörtert worden sind, könnte dazu beitragen, die Entwicklungen mit Bezug auf das Design angemessener Rahmenbedingungen für eine zukunftsgerichtete Cybergovernance positiv zu beeinflussen.

5. Neue Problembereiche: Cybersicherheit und Fragmentierung

[24] Im Infrastrukturbereich spielen die Cybersicherheit, die Cyberstabilität und die Cyberresilienz eine grosse Rolle; in Frage steht die bisher unterschätzte Bedeutung der Integrität des In-

20 Treaty of the Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and other Celestial Bodies, 1976, 610 UNTS 205.

21 Weber (Fn. 3), S. 95 f. m.w.V.

22 Jay Butler, The Corporate Keepers of International Law, American Journal of International Law 114 (2020), S. 189 (Titel).

23 Weber (Fn. 3), S. 37 m.w.V.

24 Weber (Fn. 3), S. 37 f. m.w.V.

ternets.[25] Die UNO hat diese Tatsache recht früh schon erkannt: Seit über 15 Jahren beschäftigen sich Expertengruppen, insbesondere die UN Group of Governmental Experts (UNGEE), mit Grundfragen der Cybersicherheit, doch haben die fünf publizierten (detaillierten) UNGGE-Berichte, die von den Staaten zwar zur Kenntnis genommen worden sind, bisher noch nicht zur Einigung auf global geltende harmonisierende Regeln geführt.[26] Die von Microsoft im Jahre 2018 vorgeschlagene «Digital Geneva Convention» hat vorläufig kaum politische Akzeptanz erfahren. Immerhin einigten sich die Mitglieder der Open-Ended Working Group (OEWG) im März 2021 auf Cybersicherheits-Leitlinien, doch bleibt abzuwarten, wie deren praktische Befolgung in den nächsten Monaten ausfallen wird.

[25] Das hier nur zu streifende Thema der Cybersicherheit vermag selbstredend gewichtige Auswirkungen auf die Cyberstabilität und die Cyberresilienz zu entfalten. Zu Recht hat deshalb die Global Commission on the Stability of Cyberspace (GCSC) am IGF 2019 in Berlin einen umfangreichen Bericht mit dem Titel «Advancing Cyberstability» veröffentlicht und eine Reihe von Prinzipien und Massnahmen erläutert, deren künftige Beachtung als bedeutungsvoll erscheint.[27] Gleichzeitig ist mit Blick auf die Cybersicherheit stärker zu trennen zwischen der traditionellen Cyberkriminalität, die transnational von der Budapest Konvention des Europarates geregelt wird, und den Phänomenen des «Cyberkrieges», die mehr mit der Stabilität und Resilienz von Infrastrukturen zu tun haben.

[26] Angesichts der intensivierten Bemühungen von eher autokratisch bzw. hierarchisch organisierten Staaten, das Internet gemäss dem Stichwort der digitalen Souveränität zu kontrollieren, droht eine gewisse Fragmentierung des Internet in verschiedene nationale Netze. Eine solche Fragmentierung, die auch im Rahmen der ITU für Gesprächsstoff sorgt, gefährdet die Interoperabilität der grenzüberschreitenden Informationsflüsse und vermag zu einer Erscheinung zu führen, die derzeit oft als «Splinternet» bezeichnet wird.[28]

[27] Die mangelnde Interoperabilität der Netze ist nicht nur ein technologisches Problem, sondern sie hat auch Einfluss auf die Kommunikationsgrundordnung: insbesondere die Meinungsäusserungs- und die Medienfreiheit werden beschränkt, wenn die grenzüberschreitende freie Kommunikation angesichts einer Zensur an der Grenze nicht mehr möglich ist.[29] Als erforderlich erscheint vielmehr ein neues Konzept der Souveränität, das an den Bedürfnissen der Zivilgesellschaft orientiert ist.[30]

[28] Die Problematik der Fragmentierung des Internet zeigt sich auch bereits innerhalb der Organisation der ICANN: neuerdings wird darüber diskutiert, ob es nicht sinnvoll wäre, eine Differenzierung zwischen der technischen und der sozio-politischen Internet Governance einzuführen. ICANN plädiert selbstredend dafür, auf eine technische Fragmentierung zu verzichten, damit die Verwaltung des Internet auch künftig global bleibt. Hingegen scheint die Bereitschaft zu bestehen, sozio-politische Aspekte aus dem Handlungsbereich der ICANN auszugliedern. Eine solche

25 Weber (Fn. 3), S. 83 ff. m.w.V.

26 Für weitere Einzelheiten vgl. Rolf H. Weber, Cybersecurity Governance – international law as policy driver?, Jusletter IT, 27. Mai 2021, Rz. 67 ff.

27 Global Commission on the Stability of Cyberspace, Advancing Cyberstability, Final Report, Berlin (IGF), November 2019.

28 Weber (Fn. 3), S. 87 f.

29 Vgl. Roxana Radu, Negotiating Internet Governance, Oxford 2019, S. 164, 168 f., 190.

30 Vgl. Milton Mueller, Will the Internet Fragment? Sovereignty, Globalization and Cyberspace, Oxford 2017, S. 131 f.

Entwicklung führt unter Umständen zu einer Trennung von technischer und sozio-politischer Cybergovernance, was aus der Sicht der Zivilgesellschaft als nicht wünschenswert erscheint.[31]

6. Blick in die Kristallkugel

[29] Wie sind nun die Entwicklungen im Cyberspace für die nächsten Jahre einzuschätzen? Muss die Cybergovernance «revisited» werden? Wie immer, wenn versucht wird, Prognosen zu erstellen (d.h. in die berühmte Kristallkugel zu schauen), ist zwischen Risiken und Chancen zu unterscheiden.

6.1. Risiken und Chancen der Cybergovernance

[30] Eine Reihe von Risiken, welche die Herausbildung sachgerechter Rahmenbedingungen für die Cybergovernance gefährden, lässt sich nicht übersehen; die entsprechenden Risiken sind genauer zu evaluieren.[32]

[31] (i) Ein digitales Wettrüsten und damit verbunden eine gewisse Militarisierung des Cyberspace scheint derzeit einzusetzen. Hackerangriffe aus politischen Gründen sowie Drohnen und Killerroboter, die Infrastrukturen bedrohen, kommen immer häufiger vor. Solche Angriffe, die oft unterhalb der «roten Linie» von Art. 2 Abs. 4 der UN Charta liegen, haben das Potential, Kaskadeneffekte und riskante Eskalationen zu verursachen.

[32] (ii) Die bereits erwähnte Fragmentierung der Infrastrukturen könnte sich fortsetzen in einem Verzicht auf bestehende (globale) Standardisierungen (z.B. unterschiedliche Internet-Protokolle in einzelnen Ländern) und in einem Aufbrechen bzw. einer Entkoppelung der globalen digitalen Wirtschaft (z.B. Unterbrechung von Lieferketten). Das eigentliche Bedrohungsszenario wäre der Bau von nationalen digitalen Festungen.

[33] (iii) Die Gefährdung der Menschenrechte ist ein allgemeines Thema der Digitalisierung, das die Cybergovernance mitbeeinflusst. Beispiele sind die Massenüberwachung durch digitale Gesichtserkennung (in China schon weit fortgeschritten) und die durch künstliche Intelligenz gesteuerte Zensur an der Landesgrenze.

[34] Eine optimistischere, von mir vertretene Einschätzung geht von folgenden Chancen aus, die einen Beitrag dazu leisten können, eine sachgerechte Rahmenordnung für die künftige Cybergovernance zu schaffen:[33]

[35] (i) Die jüngsten Erfahrungen mit der OEWG und der UNGGE haben gezeigt, dass die Bemühungen um den Abschluss eines Cybersicherheits-Abkommens doch nicht als völlig hoffnungslos einzustufen sind.[34] Zwar ist nicht mit einem schnellen Erfolg zu rechnen, aber eine Verdichtung der Leitlinien vom März 2021 scheint nicht ausgeschlossen zu sein. Denkbar ist ebenso eine multilaterale Einigung auf ein Verbot von Killerrobotern und von Angriffen auf kritische

31 Weber (Fn. 3), S. 89.

32 Vgl. Wolfgang Kleinwächter, Regionalisierung und Kontrolle – «Cybersouveränität» in China und Russland, Vortrag vom 7. Juni 2021 in Zürich, Folie 6.

33 Vgl. auch Kleinwächter (Fn. 32), Folie 7.

34 Vgl. vorne Rz. 24. Für einen allgemeinen Überblick vgl. auch Joanna Kulesza, Current Issues in European Cybersecurity: The NIS Directive, Due Diligence And International Law, Jusletter IT, 27. Mai 2021.

Infrastrukturen (Public Core of the Internet, öffentliche Wahlsysteme, Energie- und Wasserversorgung, Krankenhäuser).

[36] (ii) Abgesehen von der weiterhin stattfindenden Harmonisierung von Standards mit Bezug auf das Management kritischer Internet-Ressourcen schreiten die Anstrengungen, ein verbessertes Regelwerk für die globale digitale Wirtschaft zu erarbeiten, voran, insbesondere im Rahmen der WTO (plurilaterales Abkommen zu Electronic Commerce).[35] Die G7 und die OECD sind vorangekommen mit Projekten für eine Digitalsteuer. Die UNO arbeitet intensiv an der noch genauer zu erläuternden Realisierung von nachhaltigen Entwicklungszielen zur Überwindung der digitalen Spaltung (von «digital divide» zu «digital inclusion»).

[37] (iii) Die bereits erwähnte Pflicht zur Zusammenarbeit muss im technischen Bereich zur weiteren Harmonisierung von Standards führen, wie schon das Beispiel der Internationalen Fernmeldeunion zeigt, die im Jahre 1865 als zweite multilaterale Organisation gegründet worden ist. Ein Internet-Protokoll sollte grundsätzlich global sein, um die weltweite Kommunikation sicherstellen zu können; dies gilt auch für den möglichen Ersatz des heute weltumspannenden Transport Control Protocol (TCP) durch eine neue Infrastruktur. Die technologische Architektur hat zudem robust und offen zu sein, um den Zugang für alle zu ermöglichen.

6.2. Digitale Kooperation und Vertrauens-Ethik

[38] In den letzten zwei Jahren hat sich insbesondere die UNO vermehrt dem Thema der digitalen Kooperation zugewendet. Inhaltlich geht es nicht nur um die weltweite Versorgung mit Informationsleistungen, sondern auch darum, das Spannungsfeld, das durch die verstärkte Fragmentierung des Internet aufgetreten ist, zu entschärfen.

[39] Mit Blick auf die digitale Kooperation sticht der von der UNO initiierte Bericht des «UN High Panel on Digital Cooperation» von 2019 hervor, der fünf Gruppen von Aktivitäten mit verschiedenartigen Empfehlungen vorgeschlagen hat.[36] Die entsprechenden Empfehlungen werden in sog. «Roundtables» auf der Basis von «Opinion Papers» diskutiert; Ziel ist die Verabschiedung eines «Global Commitment on Digital Cooperation».[37] Der Themenbereich ist sehr weit und betrifft insbesondere auch das Anliegen der Schaffung eines integrativen («inclusive») Internet, um im Verhältnis zu den weniger entwickelten Ländern ein «digital divide» zu vermeiden. Cybergovernance im eigentlichen Sinn der Steuerung wird gerade mit Blick auf die Zugänglichkeit zu den Informationen immer wichtiger; da Digitalisierung und Technologie das Leben verstärkt umgeben und durchdringen, sind Silos zu durchbrechen und Zugangsrechte zu schaffen.[38]

[40] Im Juni 2020 hat der UN Generalsekretär António Guterres zudem eine «Roadmap for Digital Cooperation» publiziert und damit den Bemühungen um die Schaffung von Grundsätzen für digitale Kooperationen mehr Nachdruck verliehen.[39] Ziel dieser Roadmap ist ebenso, im Jahre

35 Vgl. Mira Burri, Towards a New Treaty on Digital Trade, Journal of World Trade 2021, S. 77 ff.

36 Vgl. https://digitalcooperation.org und https://www.giplatform.org/resources/hlp-report.

37 Weber (Fn. 3), S. 100.

38 Swiss IGF 2021, Messages from Bern, 21. Juni 2021, S. 2 f.

39 Vgl. Report of the UN Secretary-General's Roadmap for Digital Cooperation, June 2020, https://www.un.org/en/content/digital-coopeartion-roadmap/.

2025, mit Blick auf den Ablauf der nunmehrigen 10-Jahresperiode des Bestands des IGF, ein dynamischeres IGF+ für die Zukunft zu schaffen.

[41] Die UNESCO arbeitet an Projekten, um die «digital literacy» zu verbessern; nur wenn alle Bevölkerungsteile (d.h. alte und junge Menschen) sowie alle Regionen rund um den Globus sich der modernen Technologien bedienen können, vermag die Digitalisierung die ihr innewohnenden Chancen auch zu verwirklichen. Parallel dazu ist es wichtig, den Prinzipien von Ethik und Vertrauen im Cyberspace eine breitere Wirkung zu eröffnen; entsprechende Grundsätze und Leitlinien sind an sich vorhanden,[40] doch bedarf es ihrer konkreten Umsetzung in der politischen Realität.

6.3. Auf dem spannenden und verheissungsvollen Weg zum IGF+

[42] Die Cybergovernance steht vor herausfordernden Zeiten: Bis im Jahr 2025 soll das IGF eine neue, besser gefestigte Form erhalten und dadurch zu einem IGF+ werden. Unbestreitbar hat sich das IGF weiter zu entwickeln, wie schon der Name IGF+ zum Ausdruck bringt. Folgende Eigenschaften sind dabei zu verstärken: Das IGF muss dynamisch, integrativ («inclusive»), strategisch, multidimensional (in Verwirklichung des Multistakeholder-Modells), wirksam («impactful») und nachhaltig («sustainable») werden.[41] Als erwünscht erscheint auch eine besser fokussierte und die Themenvielfalt zusammenführende Agenda, unter gleichzeitiger Verstärkung der Zusammenarbeit von staatlichen Akteuren mit privatwirtschaftlichen Dienstleistern und zivilgesellschaftlichen Organisationen (i.S. einer «Public-Private/Civil Partnership»).

[43] Die Cybergovernance-Entwicklungen sind m.E. am «Point of No Return» angekommen.[42] Insbesondere hat Cybergovernance ein Narrativ für das konzeptionelle Design der Internetpolitiken und für die Anwendung internationaler Rechtsprinzipien gefunden. «*Revisited*» kann deshalb nicht meinen, das bisher Erreichte über Bord zu werfen, sondern muss bedeuten, die Cybergovernance punktuell neuen und zugleich verbesserten Lösungen zuzuführen. Aus juristischer Sicht ist für die Ausgestaltung des IGF+ die Vision beizusteuern, dass alle «Akteure» dazu beitragen mögen, das internationale Recht im Cybergovernance-Kontext sichtbarer («*more visible*») zu machen.[43]

Prof. Dr. Rolf H. Weber, Professor für Wirtschaftsrecht an der Universität Zürich und Rechtsanwalt in Zürich (Bratschi AG).

Alle Internetzitate sind am 7. Juli 2021 besucht worden.

40 Weber (Fn. 3), S. 100.

41 MAG Working Group on IGF Strengthening and Strategy: proposals on strategic improvements to the IGF and operational measures in 2021, Version 3.1, January 22, 2021, S. 2 ff.

42 So der Titel des Buches von Weber (Fn. 3).

43 Weber (Fn. 3), S. 104.