Recht der Digitalisierung III

Herausgegeben von
ARNO KAHL und
WERNER SCHROEDER

Internet und Gesellschaft
45

Mohr Siebeck

Internet und Gesellschaft

Schriften des Alexander von Humboldt Institut
für Internet und Gesellschaft

Herausgegeben von

Jeanette Hofmann, Matthias C. Kettemann,
Björn Scheuermann, Thomas Schildhauer
und Wolfgang Schulz

45

Recht der Digitalisierung III

Perspektiven der Internationalisierung und Digitalisierung

Herausgegeben von
Arno Kahl und Werner Schroeder

Mohr Siebeck

Arno Kahl, geboren 1970; Universitätsprofessor am Institut für Öffentliches Recht, Staats- und Verwaltungslehre der Universität Innsbruck.
orcid.org/0000-0002-0014-7825

Werner Schroeder, geboren 1962; Universitätsprofessor am Institut für Völkerrecht, Europarecht und Internationale Beziehungen der Universität Innsbruck.
orcid.org/0000-0001-7039-7187

Die Drucklegung dieses Werks wurde unterstützt durch Mittel der Rechtswissenschaftlichen Fakultät der Universität Innsbruck.

ISBN 978-3-16-162591-6 / eISBN 978-3-16-162592-3
DOI 10.1628/978-3-16-162592-3

ISSN 2199-0344 / eISSN 2569-4081 (Internet und Gesellschaft)

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind über *https://dnb.dnb.de* abrufbar.

Publiziert von Mohr Siebeck Tübingen 2026.

Gedruckt auf alterungsbeständiges Papier. Satz: Laupp & Göbel, Gomaringen.

Mohr Siebeck GmbH & Co. KG, Wilhelmstraße 18, 72074 Tübingen, Deutschland
www.mohrsiebeck.com, info@mohrsiebeck.com

Vorwort

Mit dem vorliegenden dritten Band „Recht der Digitalisierung“ wird die gleichnamige Ringvorlesung an der Rechtswissenschaftlichen Fakultät der Universität Innsbruck vorerst abgeschlossen.

Begonnen wurde die Ringvorlesung im März 2023 mit dem ersten Österreichischen Digitalrechtstag. Dieser ging der Frage nach, ob und wie den zentralen Herausforderungen der Digitalisierung mit dem Recht begegnet werden kann. Die einzelnen Beiträge des ersten Bandes beleuchten Politik und Recht in der Gestaltung der technischen Zukunft, die globale Internet-Governance zwischen Recht und Politik (UNO, EU und Österreich) sowie das neue Recht der Datenmärkte (Zugang, Gemeinwohlpflicht und Interoperabilität).

Im zweiten Band werden aktuelle Herausforderungen der Digitalisierung im justiziellen Bereich behandelt. Expertinnen und Experten unterschiedlicher juristischer Fachrichtungen geben praxisnahe Einblicke in künftige Entwicklungen betreffend Datenschutz, Strafrecht, Zivilprozessrecht und Bankenaufsichtsrecht.

Der gegenständliche dritte Band beinhaltet Beiträge aus dem öffentlichen sowie dem europäischen und dem internationalen Recht. Die Themen reichen von der Digitalisierung der Landesverwaltung und des Bauverfahrens über die Digitalisierung als Motor der Mobilitätswende bis zum AI-Act der EU und der Regulierung des „Cyberspace“ auf UNO-Ebene.

Alle drei Bände zusammen geben einen umfassenden Einblick in die rasch voranschreitende Digitalisierung, die damit verbundenen Herausforderungen und mögliche rechtliche Lösungsansätze. Enthalten ist jeweils auch ein Ausblick auf die Zukunft des Digitalrechts.

Darauf aufbauend wird die Rechtswissenschaftliche Fakultät der Universität Innsbruck die Ringvorlesung in den nächsten drei Jahren weiterführen. Dabei werden weitere Aspekte und neue Entwicklungen der Digitalisierung im Vordergrund stehen. Die Ringvorlesung „Recht und Digitalisierung“ soll sowohl die Forscherinnen und Forscher als auch die Studierenden stets auf dem neuesten Stand halten.

Ein besonderer Dank gilt allen Mitgliedern der Rechtswissenschaftlichen Fakultät und allen externen Expertinnen und Experten, die an der zu Ende gehenden Ringvorlesung mitgewirkt haben. Beim Verlag Mohr Siebeck bedanke ich mich im Namen

der Fakultät für die Verlegung der drei Tagungsbände und für die professionelle Zusammenarbeit.

Innsbruck, im September 2025

Univ.-Prof. Dr. Walter Obwexer
Dekan der Rechtswissenschaftlichen Fakultät
der Universität Innsbruck

Inhaltsverzeichnis

Abkürzungsverzeichnis

a. A.	anderer Ansicht
a. a. O.	am angeführten Ort
a. M.	anderer Meinung
ABl.	Amtsblatt der Europäischen Union
ABoR	Administrative Board of Review
Abs.	Absatz
ACM	Autoriteit Consument en Markt
AGCM	Autorità garante della Concorrenza e del Mercato
AI	artificial intelligence
AIDP	Association Internationale de Droit Pénal
al.	alter
AMLA	Anti Money Laundering Authority
Anm.	Anmerkung
AnwBl	Anwaltsblatt
API	Application Programming Interface
arg.	argumentum
ARHG	Auslieferungs- und Rechtshilfegesetz
ARHV	Auslieferungs- und Rechtshilfeverordnung
Art.	Artikel/Article
Aufl.	Auflage
ausf.	ausführlich
AußStrG	Außerstreitgesetz
Az.	Aktenzeichen
BCBS	Basel Committee on Banking Supervision
BegrRegE	Begründung Regierungsentwurf
Beschl.	Beschluss
betrDEStA	Betrauter Delegierter Europäischer Staatsanwalt
BGBl.	Bundesgesetzblatt
BGH	(deutscher) Bundesgerichtshof
BGHSt	Entscheidungen des Bundesgerichtshofes in Strafsachen
BiBuG	Bilanzbuchhaltungsgesetz
BIS	Bank for International Settlements
BKA	Bundeskanzleramt der Republik Österreich
BKartA	(deutsches) Bundeskartellamt
BlgNR	Beilagen zu den stenographischen Protokollen des Nationalrats
BMJ	Bundesministerium für Justiz
Bsp.	Beispiel
bspw.	beispielsweise
BT-Drs.	Drucksache Deutscher Bundestag

BudgetbegleitG	Budgetbegleitgesetz
BWG	Bankwesengesetz
bzw.	beziehungsweise
ca.	circa
CAC	Cyberspace Administration of China
CAs	conversational agents
CEBS	Committee of European Banking Supervisors
cf.	confer
COM	European Commission
COREPER	Ausschuss der Ständigen Vertreter
CRD	Capital Requirements Directive
CRR	Capital Requirements Regulation
d. m.	decreto ministrale
DA	Data Act
DGA	Data Governance Act
Dir.	Directive
DMA	Digital Markets Act
DRiZ	Deutsche Richterzeitung
DRM	Digital Rights Management
DSA	Digital Services Act
DSG	Datenschutzgesetz
DS-GVO	Datenschutz-Grundverordnung
dZPO	deutsche Zivilprozessordnung
e. g.	exempli gratia
EBA	European Banking Authority
ebd.	ebenda
ECJ	European Court of Justice
ecolex	Zeitschrift für Wirtschaftsrecht
Ed(s).	Editor(s)
ed.	edition
EDIS	European Deposit Insurance Scheme
Edit.	Edition
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EEA	Europäische Ermittlungsanordnung
EG	Europäische Gemeinschaft
EGMR	Europäischer Gerichtshof für Menschenrechte
EHDS	European health data space
Einl.	Einleitung
EIOPA	European Insurance and Occupational Pensions Authority
eJABl	Elektronisches Amtsblatt der österreichischen Justizverwaltung
EKHG	Eisenbahn- und Kraftfahrzeughaftpflichtgesetz
ELI	European Law Institute
EMRK	Europäische Menschenrechtskonvention
endg.	endgültig
Entsch.	Entscheidung(en)
Entw.	Entwurf
EO	Exekutionsordnung

ERA	Europäische Rechtsakademie
Erläut.	Erläuterungen
ErläutRV	Erläuterungen zur Regierungsvorlage
ErwGr.	Erwägungsgrund
ESFS	European System of Financial Supervision
ESMA	European Securities and Markets Authority
ESRB	European System Risk Board
EStG	Einkommensteuergesetz
et al.	et alter
etc.	et cetera
et seq.	et sequens
et seqq.	et sequentes
EU	Europäische Union
EuBagatellVO	Europäische Verordnung zur Einführung eines europäischen Verfahrens für geringfügige Forderungen
EuBVO	Europäische Beweisaufnahmeverordnung
EuDigiJustVO	Europäische Verordnung über die Digitalisierung der justiziellen Zusammenarbeit
EU-FinAnpG	EU-Finanz-Anpassungsgesetz
EuG	Europäisches Gericht
EuGH	Europäischer Gerichtshof
EU-JZG	Bundesgesetz über die justizielle Zusammenarbeit in Strafsachen mit den Mitgliedstaaten der Europäischen Union
eur.	europäisch
EU-RhÜbk	Übereinkommen über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union
EUStA	Europäische Staatsanwaltschaft
EUStA-DG	Bundesgesetz zur Durchführung der Europäischen Staatsanwaltschaft
EUStA-VO	Verordnung (EU) 2017/1939 des Rates vom 12.10.2017 zur Durchführung einer verstärkten Zusammenarbeit zur Errichtung der Europäischen Staatsanwaltschaft
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
EvBl	Evidenzblatt der Rechtsmittelentscheidungen der ÖJZ
EZB	Europäische Zentralbank
f.	und folgende
Fallnr.	Fallnummer
ff.	fortfolgende
FM-GwG	Finanzmarkt-Geldwäschegesetz
Fn.	Fußnote
fn.	footnote
FRIA	Fundamental Rights Impact Assessment
FSE	Fascicolo Sanitario Elettronico
FTC	(US-amerikanische) Federal Trade Commission
G7	Group of seven
GAFAM	Google, Apple, Facebook, Amazon und Microsoft
GD GROW	Generaldirektion Binnenmarkt, Industrie, Unternehmertum und KMU

GD JUST	Generaldirektion Justiz und Verbraucher
GDPR	General Data Protection Regulation
gem.	gemäß
ggf.	gegebenenfalls
GOG	Gerichtsorganisationsgesetz
GP	Gesetzgebungsperiode
GRUR Int.	Gewerblicher Rechtsschutz und Urheberrecht Internationaler Teil
GWB	(deutsches) Gesetz gegen Wettbewerbsbeschränkungen
h.A.	herrschende Ansicht
h. M.	herrschende Meinung
HBÜ	Haager Beweisaufnahme-Übereinkommen
HDAB	Health data access bodies
HER	Electronic Health Records
HMI	human-machine interaction
i. d. F.	in der Fassung
i. d. R.	in der Regel
i. e.	id es
i. e. S.	im engeren Sinn
i. S.	im Sinne von
i. S. d.	im Sinne de- s, -r
i. V. m.	in Verbindung mit
i. w. S.	im weiteren Sinn
IBOA	institutions, bodies, offices and agencies of the EU
iFamZ	Interdisziplinäre Zeitschrift für Familienrecht
IO	Insolvenzordnung
IoT	Internet of Things
IRP	Internal Rules of Procedure
Iss.	Issue
ITS	Implementing Technical Standards
JBl	Juristische Blätter
JCA	Journal of Consumer Affairs
JETL	Journal of European Tort Law
öJGG	österreichisches Jugendgerichtsgesetz
JN	Jurisdiktionsnorm
JSt	Journal für Strafrecht
JST	Joint Supervisory Teams
JuBG	Justiz-Begleitgesetz
JusIT	Zeitschrift für IT-Recht, Rechtsinformation und Datenschutz
Kap.	Kapitel
KI	Künstliche Intelligenz
KMU	kleine und mittlere Unternehmen
KOM	Europäische Kommission
KVR	Rechtsbeschwerdeverfahren in Kartell-Verwaltungssachen
leg. cit.	legis citatæ
Lfg.	Lieferung
lit.	littera
LK-StPO	Linzer Kommentar zur Strafprozessordnung
LLM	Large Language Model

LoseBl	Loseblattsammlung
LSI	less significant institutions
LUISS	Libera Università Internazionale degli Studi Sociali
m. a. W.	mit anderen Worten
m. E.	meines Erachtens
m. n.	marginal number
m. w. N.	mit weiteren Nachweisen
ME	Ministerialentwurf
MiCA	Markets in Crypto-assets
Mio.	Millionen
MR	Medien und Recht
Mrd.	Milliarden
MR-Int	Medien und Recht International
NCA	national competent authorities
NJW	Neue Juristische Wochenschrift
NJW-Beil.	Neue Juristische Wochenschrift – Beilage
NLG	Natural Language Generation
no.	number
NPHRL	Entwurf einer neuen Produkthaftungsrichtlinie
Nr.	Nummer
NSCAI	National Security Commission on Artificial Intelligence
NTF	New Technologies Formation
NZKart	Neue Zeitschrift für Kartellrecht
ÖBl	Österreichische Blätter für Gewerblichen Rechtsschutz und Urheberrecht
ÖBl-LS	ÖBl-Leitsätze
ODR	Online Dispute Resolution
OECD	Organisation for Economic Co-operation and Development
OGH	Oberster Gerichtshof
ÖJA	Österreichisches Juristisches Archiv
OJEU	Official Journal of the European Union
ÖJZ	Österreichische Juristenzeitung
ÖJZ-MRK	Entscheidungen zur MRK in der ÖJZ
OLAF	Europäisches Amt für Betrugsbekämpfung
OLG	Oberlandesgericht
österr.	österreichisch
OTF	organised trading facility
para.	paragraph
PHRL	Produkthaftungsrichtlinie
PIF-Richtlinie	Richtlinie (EU) 2017/1371 des Europäischen Parlaments und des Rates vom 5.7.2017 über die strafrechtliche Bekämpfung von gegen die finanziellen Interessen der Union gerichtetem Betrug
PIMS	personal information management systems
PLF	Product Liability Formation
PSA	Payment Services Austria
RDi	Recht Digital
Rec.	Recital
RegE	Regierungsentwurf

RL	Richtlinie
Rn.	Randnummer
Rs.	Rechtssache
RtDP	right to data portability outlined by the GDPR
RTS	Regulatory Technical Standards
RZ	Österreichische Richterzeitung
S.	Satz
s.	siehe
s. o.	siehe oben
SARs	socially assistive robots
Sec.	Section
sent.	sentence
SI	significant institutions
SME	small and medium enterprises
SRM	Single Resolution Mechanism
SSM	Single Supervisory Mechanism
SSRN	Social Science Research Network
SSt	Entscheidungen des Obersten Gerichtshofes in Strafsachen und Disziplinarangelegenheiten
StA	Staatsanwaltschaft
öStGB	österreichisches Strafgesetzbuch
öStPO	österreichische Strafprozessordnung
StPRÄG	Strafprozessrechtsänderungsgesetz
StrEU-AG	Strafrechtliches EU-Anpassungsgesetz
u. a.	unter andere -m, -n
US	United States
u. U.	unter Umständen
UAbs.	Unterabsatz
UK	United Kingdom
UNESCO	United Nations Educational, Scientific and Cultural Organization
untDEStA	unterstützender Delegierter Europäischer Staatsanwalt
öUrhG	österreichisches Urheberrechtsgesetz
Urt.	Urteil
usw.	und so weiter
v.	von, -m
v. a.	vor allem
Vers.	Version
vers.	version
VfGH	Verfassungsgerichtshof
VG	Verwaltungsgericht
vgl.	vergleiche
VLP	very large platforms
VO	Verordnung
Vol.	Volume
VPN	Virtual Private Network
vs.	versus
WK-StPO	Wiener Kommentar zur Strafprozessordnung
WP29	Article 29 Working Group on Data Protection

WTBG	Wirtschaftstreuhandberufsgesetz
Z.	Ziffer
z.B.	zum Beispiel
Zak	Zivilrecht aktuell
ZEuP	Zeitschrift für Europäisches Privatrecht
ZFR	Zeitschrift für Finanzmarktrecht
ZfRV	Zeitschrift für Europarecht, internationales Privatrecht und Rechtsvergleichung
ZIK	Zeitschrift für Insolvenzrecht und Kreditschutz
ZPD	zentraler Plattformdienst
öZPO	österreichische Zivilprozessordnung
ZUM	Zeitschrift für Urheber- und Medienrecht
zust.	zustimmend
ZVN	Zivilverfahrens-Novelle
ZWF	Zeitschrift für Wirtschafts- und Finanzstrafrecht

Die Regulierung des „Cyberspace“ auf UNO-Ebene: Völkerrecht und Cyber Diplomatie[1]

Isabella E. Brunner

I. Einführung

Der Begriff „Cyberspace“ hat sich als wirkungsvolles Schlagwort etabliert und das tägliche Leben der heutigen Generation in vielerlei Hinsicht verändert. Die Menschheit ist globaler und vernetzter geworden, und alltägliche Aufgaben lassen sich dank der stetigen Interkonnektivität schneller erledigen. Diese plötzliche globale Vernetzung führte zu vielen neuen rechtlichen Fragestellungen. Auch im Völkerrecht sind seit der Entstehung des Internets – und damit auch des „Cyberspace“ – neue Herausforderungen entstanden. Dazu zählt insbesondere die grundlegende Überlegung, ob das existierende, traditionelle Völkerrecht überhaupt auf ein neues Phänomen wie den Cyberspace anwendbar ist und, falls ja, wie die geltenden Regeln zu interpretieren sind, um sie für die Herausforderungen, die neue Technologien stellen, brauchbar

[1] Die Autorin bedankt sich bei Dr. Valentin Weber für die hilfreichen Kommentare zu einer früheren Version dieses Beitrags.

zu machen, sowie die Frage, ob potenzielle Lücken bestehen, die womöglich mit neuen Regeln zu schließen wären.

Trotz anfänglicher Skepsis, dass das Recht überhaupt eine Rolle im Cyberspace spielen soll, hat es sich heutzutage weitgehend durchgesetzt, dass Regeln und Normen auch in diesem virtuellen Raum eine Rolle spielen. Dies hat sich seit 2013 auch für das Völkerrecht so etabliert. Die Frage ist nur oft, wie diese herkömmlichen Regeln und Normen zu interpretieren sind und ob die existierenden Rahmenbedingungen ausreichend sind. Manche Staaten (wie z.B. Russland) sind der Ansicht, dass die derzeitigen völkerrechtlichen Regeln nicht genug sind, und ein Vertrag zur internationalen Informationssicherheit ausgehandelt werden sollte.

Dieser Beitrag bietet einen Überblick über die Entwicklungen der vergangenen Jahre und Jahrzehnte – insbesondere innerhalb der Vereinten Nationen –, die maßgeblich zur Regulierung des Cyberspace beigetragen haben. Er argumentiert, dass wir uns derzeit an einem Wendepunkt befinden, an dem sich bestimmte Normen und Regeln zunehmend institutionalisieren. Abschnitt II gibt einen groben Überblick über die anfänglichen Entwicklungen des freien Internets zum regulierten Cyber Raum. Abschnitt III befasst sich im Detail mit den internationalen Regulierungstendenzen in den Vereinten Nationen zum Thema internationale Cybersicherheit. Er behandelt insbesondere die Entwicklungen in den sogenannten GGEs und OEWGs und wie diese die Institutionalisierung des Themas vorangetrieben haben. Abschnitt IV befasst sich mit der kürzlich von der VNGV angenommenen Cyberkriminalitätskonvention der Vereinten Nationen, und Abschnitt V erläutert, wie nationale Positionspapiere, die die Meinungen unterschiedlicher Staaten reflektieren, wie das Völkerrecht auf den Cyberspace anzuwenden ist, zur steten Regulierung der Debatte beitragen. Abschnitt VI fasst zusammen.

Bevor die Regulierung des Cyberspace genauer untersucht wird, ist allerdings klarzustellen, worum es sich bei dem Begriff „Cyberspace" handelt. Die internationale Expert*innengruppe, die für die Entstehung des Tallinn Manual verantwortlich war,[2] definiert „Cyberspace" wie folgt:

> „Die aus physischen und nicht-physischen Komponenten bestehende Umgebung zum Speichern, Ändern und Austauschen von Daten über Computernetzwerke."[3]

Da das Austauschen von Daten über Computernetzwerke oft über das Internet erfolgt, wird der „Cyberspace" oft mit dem „Internet" gleichgestellt. Das Internet kann als „weltweiter Verbund von Computern und Computernetzwerken" definiert wer-

---

[2] Das Tallinn Manual ist eine Art Handbuch, welches darlegt, wie das Völkerrecht auf den Cyberspace angewendet werden kann. Es wurde nach den schwerwiegenden Cyber-Angriffen auf estnische Regierungsserver in 2007 ins Leben gerufen, unter NATOs Schirmherrschaft. Für mehr Informationen zum Tallinn Manual Prozess (die dritte Iteration ist derzeit im Gange) sh. https://ccdcoe.org/news/2020/ccdcoe-to-host-the-tallinn-manual-3-0-process/ (22.9.2025).

[3] Übersetzung aus dem Englischen: „The environment formed by physical and non-physical components to store, modify, and exchange data using computer networks", in *Schmitt/Vihul* (Hrsg.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2017, 564.

den, welches oft genutzt wird, um spezielle Dienstleistungen anzubieten.[4] Auch in diesem Beitrag wird das Internet als Synonym für den Cyberspace verwendet, aufgrund seiner thematischen Überschneidungen. Dennoch ist anzumerken, dass es sich nicht um Wortidentitäten handelt, da der Cyberspace über das Internet hinausgeht.

Wie bereits erwähnt, ist der Begriff „Cyberspace" heutzutage regelrecht zu einem „Buzz-Wort" geworden. William Gibson, ein Autor diverser Science-Fiction Romane, wird oft als Grund für die Popularität des Wortes „Cyberspace" genannt. Gibson selbst meinte, der Begriff sei „im Grunde bedeutungslos" und „deutete auf etwas hin", ohne „wirklichen semantischen Inhalt".[5] Tatsächlich verleiht der Begriff „Cyberspace" im alltäglichen Gebrauch oft den Eindruck eines virtuellen Raums, der schwer greifbar ist. Die Unnahbarkeit dieses Raumes erweckt somit den Eindruck, als ob man diesen schwer regulieren könne.[6] Zu Beginn der Entstehung des Internets war dies auch eindeutig noch die weit verbreitete Meinung.

Wie bereits weiter oben erwähnt, erläutert der nächste Abschnitt die ersten Entwicklungen in Richtung der Regulierung des Cyberspace in den Anfängen des Internets.

II. Vom Traum des Regelfreien Cyberspace zur Realität der Allumfänglichen Regulierung: Ein Grober Überblick

In den späten 1980er Jahren legte Tim Berners-Lee den Grundstein für eine revolutionäre Form der digitalen Vernetzung. Mit der Entwicklung des „World Wide Web" – das 1991 erstmals öffentlich zugänglich wurde – schuf er eine benutzerfreundliche Möglichkeit, Informationen auszutauschen und miteinander zu kommunizieren. Dadurch konnten erstmals auch technisch weniger vernetzte Menschen mit nur wenigen Klicks über nationale Grenzen hinweg mit anderen Menschen kommunizieren.[7] Der plötzlich ermöglichte internationale Austausch erweckte eine richtige Euphorie unter manchen und den Wunsch, dass dieser Ort frei von Regulierung bleiben soll. So erklärte John Perry Barlow, ein cyber-libertärer Visionär, in seiner weltberühmten „Erklärung über die Unabhängigkeit des Cyberspace",[8] dass die Regierungen der industriellen Welt keine Souveränität im Cyberspace hätten.[9] Die Vision

---

[4] Vgl. Duden, https://www.duden.de/rechtschreibung/Internet (22.9.2025).

[5] William Gibson im Dokumentarfilm „No Maps for these Territories" im Jahr 2000.

[6] Sh. dazu auch schon *Brunner,* Austrian Review of International and European Law 2025, 157 (160 ff.).

[7] *CERN*, A short history of the Web, https://home.cern/science/computing/birth-web/short-history-web (22.9.2025); *Goldsmith/Wu*, Who Controls the Internet? Illusions of a Borderless World, 2008, 52 ff.

[8] Auf Englisch „A Declaration of the Independence of Cyberspace".

[9] *Barlow*, A Declaration of the Independence of Cyberspace, 8. Februar 1996, https://www.eff.org/cyberspace-independence (22.9.2025).

des regelfreien Cyberspace blieb jedoch eine Utopie, denn bereits zur Zeit Barlows hatte sich eine immer stärker werdende Tendenz der Regulierung etabliert.[10]

Im Jahr 2000 verglich der damalige US-Präsident Bill Clinton Chinas Bemühungen, die freie Meinungsäußerung im Internet zu regulieren, mit dem Versuch, Pudding an die Wand zu nageln.[11] Er versuchte damit aufzuzeigen, dass das Internet, aufgrund seiner Grenzenlosigkeit und weltweiten Verbundenheit, sowie Ermöglichung weitgehender Anonymität, nicht durch einen einzigen Staat zensuriert werden könne. Dass sich Bill Clinton geirrt haben muss, scheint heute klar zu sein. Nicht nur China,[12] sondern auch Nordkorea,[13] Russland,[14] Iran,[15] und andere Staaten haben in den letzten Jahren wesentliche Schritte gesetzt, um den Datenfluss, der in ihr Land strömt, einzudämmen, und Informationen, die innerhalb des Landes im Wege des Internets geteilt werden, größtenteils zu regulieren. Beurteilt man die Trends von heute, so ist davon auszugehen, dass die weltweite Regulierung des Internets weiter zunehmen wird. Andere Entwicklungsländer scheinen auch vermehrt Interesse zu haben, Kontrolle über die Datenströme, die in ihr Land fließen, zu erlangen, und tun dies auch bereits.[16] In gewissen Fällen spricht man bereits auch von der „Fragmentierung der liberalen Cyber Ordnung".[17]

Aber auch der Westen folgt nicht gänzlich den cyber-libertären Wunschvorstellungen von John Perry Barlow und anderen Gleichgesinnten. Obgleich Länder wie die Vereinigten Staaten von Amerika seit den Anfängen des Internets starke Verfechter der „Internet Freiheit" Agenda waren.[18] Was sich bald herausstellte war, dass der Cyberspace zwar die noch nie zuvor dagewesene Vielfalt an Kreativität und Austausch weltweit ermöglichte; aber auch im Internet tummelten sich schwarze Schafe, die dieses System der Offenheit und Vertrautheit auszunutzen versuchten. Insbesondere als die ersten e-commerce-Plattformen entstanden, häuften sich die Fragen über die Strafverfolgung im Internet[19] – so z.B. wenn jemand einen Betrugsfall melden

---

[10] Sh. dazu insbesondere *Lessig*, Code: And Other Laws of Cyberspace, Version 2.0, 2. Auflage, 2006, 302–305; sh. auch *Goldsmith/Wu* (Fn. 7), 65 ff.

[11] Auf Englisch: „That's sort of like trying to nail Jello to the wall", sh. *Allen*, The Man Who Nailed Jello to the Wall, Foreign Policy, 29. Juni 2016, https://foreignpolicy.com/2016/06/29/the-man-who-nailed-jello-to-the-wall-lu-wei-china-internet-czar-learns-how-to-tame-the-web/ (22.9.2025).

[12] Sh. z.B. *Roberts*, Censored: Distraction and Diversion Inside China's Great Firewall, 2018.

[13] Sh. z.B. *Gerschewski/Dukalskis*, Georgetown Journal of International Affairs 2018, 12.

[14] Sh. *Sukumar/Basu*, Journal of Cyber Policy 2024, 1 (6).

[15] *Deibert et al* (Hrsg.), Access Denied: The Practice and Policy of Global Internet Filtering, 2008, 292 ff.

[16] So gibt es z.B. Hinweise, dass Indien weitreichende Web Zensur betreibt, sh. *Singh/Grover/Bansal*, WebSci 2020, 21.

[17] *Sukumar/Basu* (Fn. 14), 7.

[18] *Goldsmith*, The Failure of Internet Freedom, Knight First Amendment Institute auf der Columbia Universität, 13. Juni 2018, https://knightcolumbia.org/content/failure-internet-freedom (22.9.2025).

[19] *Goldsmith/Wu* (Fn. 7), insbesondere Kapitel 5, 65 ff.

wollte – oder Fragen über Schadenersatzansprüche – wenn etwa jemand in Frankreich ein Produkt an jemanden in Amerika verkaufte.

Diese Phänomene bedurften einer Regulierung des Staates, damit seine Bürger*innen die Bürger*innen anderer Staaten zur Rechenschaft ziehen konnten bzw. selbst zur Rechenschaft gezogen werden konnten.

Auch vor allem die USA, die – wie bereits erwähnt – seit den 1990er Jahren die sogenannte „Internet Freiheit" Agenda propagierten, welche die Förderung eines freien, offenen und sicheren Internets beinhaltete, gerieten nach den Enthüllungen von Edward Snowden unter heftige Kritik. Unter anderem enthüllte Snowden, dass die USA ihre eigene Bevölkerung, als auch Bürger*innen weltweit ausspionierte.[20] Wo die „Internet Freiheit" Agenda somit den weltweiten freien Austausch von Informationen förderte, nutzten die USA genau diesen freien Datenaustausch aus, um die Menschheit weltweit auszuspionieren.

Obgleich der Cyberspace – durch seine Grenzenlosigkeit – weiterhin gewisse Herausforderungen, insbesondere für die Regulierung gewisser Aktivitäten, an Staaten stellt, würde heute somit niemand mehr bezweifeln, dass rechtliche Rahmenbedingungen auch für den Cyberspace gelten, und dieser keine „rechtsfreie Domäne" darstellt, wie dies von den cyber-libertären Visionären gewollt war. Kurz gesagt: Der grenzenlose rechtsfreie Cyber-Raum ist ein Mythos, der in Realität nicht existiert.

Auf nationalstaatlicher Ebene hat sich somit seit der Entstehung des Internets viel in der Regulierung des Cyberspace getan. Dieser Beitrag fokussiert sich jedoch auf die internationale Ebene, insbesondere die Entwicklungen in den Vereinten Nationen, wo das Thema seit Ende der 1990er Jahre immer prominenter wurde, insbesondere mit Bezug auf die internationale Cybersicherheit. So wurde seit 1998 das Thema internationale Cybersicherheit im jährlichen Abstand in den Vereinten Nationen behandelt. Der restliche Teil dieses Beitrags beschäftigt sich mit der schrittweisen Regulierung und Institutionalisierung der internationalen Cybersicherheits-Debatte bei den Vereinten Nationen.

III. Die Vereinten Nationen und die Internationale Regulierung der Cybersicherheit

1. 1998: Der Start der Verhandlungen

Es war die Russische Föderation, die die Behandlung des Themas der internationalen Cybersicherheit 1998 auf die UNO-Ebene brachte. Somit war es Russland, das 1998 die Generalversammlung (GV)-Resolution 53/70 einbrachte – die erste Resolution, die dieses Thema auf UNO-Ebene behandelte.[21] Es folgten jährliche Resolutionen

[20] *Goldsmith* (Fn. 18).

[21] Sh. VNGV-Res 53/70, 4. Dezember 1998, UN Dok A/RES/53/70.

dazu, die im Jahr 2004 in der Einrichtung einer ersten Arbeitsgruppe mündeten.[22] In der Tat ist der Prozess im Ersten Ausschuss der Vereinten Nationen der am längsten andauernde Prozess im Bereich der internationalen Cybersicherheit in den Vereinten Nationen als auch anderswo.[23]

Die sogenannte „UN Group of Governmental Experts" (GGE) sollte sich – mit einer limitierten Anzahl an teilnehmenden Mitgliedstaaten – eingehend zu dem Thema internationale Cybersicherheit befassen.[24] Insgesamt gab es sechs dieser GGEs, die sich ausführlich mit den Bedrohungen aus dem Cyberspace für die internationale Sicherheit auf Ebene der Vereinten Nationen beschäftigten. Das Ende ihres Mandats war jeweils in den Jahren 2004, 2010, 2013, 2015, 2017 und 2021. Die letzte Expert*innengruppe fand parallel mit der sogenannten Open-Ended Working Group (auf Deutsch „Offene Arbeitsgruppe") statt, und duplizierte somit die Gespräche in zwei verschiedenen Gremien innerhalb des Ersten Ausschusses der Vereinten Nationen. Dazu allerdings noch etwas später mehr.

Obwohl es das Ziel sämtlicher GGEs war, einen Konsensbericht am Ende ihres Mandats zu veröffentlichen, gelang dies 2004 und 2017 nicht. Zu groß waren die Meinungsverschiedenheiten der Staaten insbesondere zum Völkerrecht. So bestand weitgehende Uneinigkeit über die Anwendbarkeit des Selbstverteidigungsrechts und des Humanitären Völkerrechts zwischen den „westlichen Staaten" einerseits und der Russischen Föderation, Kuba und China andererseits.[25] Insbesondere die Vereinigten Staaten und gleichgesinnte UNO-Mitgliedstaaten waren nämlich der Ansicht, dass das Selbstverteidigungsrecht sowie das Humanitäre Völkerrecht auch auf den Cyber Kontext angewendet werden sollten. Die Russische Föderation – und gleichgesinnte Staaten – sahen darin andererseits die Gefahr, dass durch die Anwendbarkeit dieser Rechtsgebiete die Militarisierung des Cyberspace gerechtfertigt und gefördert werden könnte.[26]

Obgleich das Scheitern einer Konsensfindung in den Jahren 2004 und 2017 zu bedauern war, schaffte es der Großteil der GGEs jedoch, mit einem Bericht abzuschließen. So gelang es den Gruppen in 2010, 2013, 2015 und 2021 einen derartigen Bericht zu beschließen. Alle dieser Berichte stellen einen mehr oder weniger großen Fortschritt für diese Diskussionen dar, allerdings sind, aus völkerrechtlicher Sicht, insbesondere die Berichte aus 2013 und 2015 hervorzuheben.

---

[22] *Korzak*, Russia's Cyber Policy Efforts in the United Nations, Tallinn Papers, Nr. 11, 2021, 6.
[23] *Ibid*.
[24] Sh. VNGV-Res 58/32, 18. Dezember 2003, UN Dok A/RES/58/32.
[25] Sh. dazu insbesondere im Detail *Henderson*, in: Tsagourias/Buchan (Hrsg.), Research Handbook on International Law and Cyberspace, 2021, 590–591, und 598–601.
[26] *Ibid*.

2. Der 2013 GGE-Bericht und der UNO-weite Konsens über die Anwendbarkeit des Völkerrechts auf Informations- und Kommunikationstechnologie

Der GGE-Bericht aus 2013 ist insbesondere deswegen hervorzuheben, als er zum ersten Mal erwähnt, dass das Völkerrecht, und insbesondere die UNO-Satzung, auf die IKT-Umgebung anwendbar ist, und darüber hinaus essenziell ist um Frieden und Stabilität, sowie die Förderung einer offenen, sicheren, und friedlichen sowie zugänglichen IKT-Umgebung, aufrechtzuerhalten.[27] Diese explizite Hervorhebung des Völkerrechts und seine Anwendbarkeit auf den Cyber Kontext ist insbesondere deswegen bemerkenswert, als bis ins Jahr 2013 eine derartige Einigkeit auf UNO-Ebene nicht hergestellt werden konnte. Wie bereits weiter oben erwähnt, war die Uneinigkeit über die Anwendbarkeit des Völkerrechts auf den Cyber Kontext einer der zentralen Gründe, warum kein Konsens-Bericht in der ersten Expert*innengruppe im Jahr 2004 zustande gebracht werden konnte.

Der Bericht aus 2013 stellt bis heute die Basis für jegliche weitere Diskussionen über die Anwendbarkeit des Völkerrechts auf UNO-Ebene dar und ist somit ein Grundpfeiler, der nun schwer beseitigt werden kann. Nichtsdestotrotz gibt es vermehrt Versuche gewisser Staaten, die Anwendbarkeit gewisser Teilbereiche des Völkerrechts anzuzweifeln. Wie bereits weiter oben erwähnt, gibt es insbesondere hinsichtlich des Selbstverteidigungsrechts und Humanitären Völkerrechts immer wieder Aussagen von Staaten wie Kuba, China und Russland, dass diese Bereiche des Völkerrechts nicht auf den Cyber Kontext angewendet werden sollten, da dieser nur die Kriegsführung fördere.[28]

Wie gesagt ist jedoch der Konsensbericht aus 2013 über die Anwendbarkeit des Völkerrechts, der seitdem in jeglichen weiteren Berichten, und auch in der OEWG immer wieder zitiert wird, so einflussreich, dass eine Unterminierung dieses Konsenses heutzutage schwer möglich sein wird.

3. Der 2015 GGE-Bericht und die 11 nicht-verbindlichen Normen über verantwortungsvolles Staatenverhalten im Cyberspace

Zwei Jahre nach diesem für das Völkerrecht erfolgreichen Bericht erreichte eine weitere GGE einen erneuten Meilenstein in den UNO-Verhandlungen. Der Bericht aus 2015 erhielt zum ersten Mal Empfehlungen an Staaten für konkrete, allerdings rechtlich nicht verbindliche Normen, die spezifisch auf den Cyber-Kontext anwendbar sein sollten. Der Expert*innenbericht empfiehlt insgesamt elf rechtlich nicht-verbindliche Normen über das verantwortliche Staatenverhalten im Cyberspace (auf English: „voluntary, non-binding rules, norms and principles of responsible state

---

[27] *VNGV*, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 24. Juni 2013, UN Dok A/68/98*, 8, Ziffer 19.

[28] Sh. dazu insbesondere im Detail *Henderson* (Fn. 25), 590–591, und 598–601.

behaviour“).[29] Der Großteil dieser Normen (acht) sind sogenannte positive Normen, welche Staaten dazu anhalten, gewisse Schritte zu setzen, die zur Absicherung der internationalen Cybersicherheit beitragen. Diese Normen geben somit unter anderem vor, dass Staaten in der Stärkung der Cybersicherheit kooperieren sollten (Norm a), bei einem Cyber-Vorfall jegliche zur Verfügung stehenden Informationen beachten sollten (Norm b), die Menschenrechte respektieren sollten (Norm e), Maßnahmen setzen sollten, um die kritische Infrastruktur zu schützen (Norm g), oder auf Unterstützungsanfragen anderer Staaten in einem Cyber-Krisenfall reagieren sollten (Norm h). Drei der Normen sind sogenannte negative Normen und geben vor, welches Verhalten Staaten im Cyber Kontext unterlassen sollten. Norm c besagt somit, dass Staaten ihr Territorium nicht wissentlich für völkerrechtsverletzende Cyber Aktivitäten zur Verfügung stellen sollten. Norm f gibt vor, dass Staaten keine kritischen Infrastrukturen angreifen sollten, und Norm k besagt, dass sogenannte „computer emergency response teams“ (auf Deutsch: „Computersicherheits-Ereignis- und Reaktionsteams“) nicht angegriffen oder für böswillige Cyber Aktivitäten verwendet werden sollten.

Das Spannende an diesen Normen ist, dass diese zwar rechtlich nicht verbindlich sind, dennoch aber einen starken Konnex zu völkerrechtlichen Verpflichtungen aufweisen: So lautet, z.B., Norm c: „Staaten sollten nicht wissentlich zulassen, dass ihr Territorium unter Einsatz von Informations- und Kommunikationstechnologie für *völkerrechtswidrige* Handlungen missbraucht wird.“[30] Diese Norm ist fast eindeutig mit dem Diktum des Internationalen Gerichtshofs im Korfu Kanal-Fall, welches sagt, dass es ein allgemeines und gut anerkanntes Prinzip im Völkerrecht gebe, wonach jeder Staat die Verpflichtung habe, nicht wissentlich zuzulassen, dass sein Territorium für Aktivitäten, die gegen die Rechte anderer Staaten gehen, missbraucht wird.[31] Auf Englisch – in der Originalfassung – ist der Vergleich noch prägnanter.[32] Einerseits stärkt somit die klare Anlehnung an ein völkerrechtliches Diktum die Bedeutung dieser Norm. Durch die explizite Verwendung nicht-bindender Sprache („sollte“ statt „soll“) stellt die Norm allerdings gleichzeitig auch die rechtliche Verbindlichkeit dieses Diktums im Cyber Kontext in Frage. Würde man nämlich der Annahme sein, dass diese Norm – gleich wie im traditionellen Kontext – rechtlich

[29] VNGV, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 22. Juli 2015, UN Dok A/70/174, 7–8, Ziffern 13a–k.

[30] Auf Englisch: „States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs“, VNGV GGE-Bericht (Fn. 29), 7, Ziffer 13c.

[31] *Korfu-Kanal-Fall* (Vereinigtes Königreich/Albanien), IGH, Urteil vom 9. April 1949, ICJ Reports 1949, 4 (22).

[32] Das Diktum des Korfu Kanals lautet wie folgt: „Such obligations are based, … on certain general and well-recognized principles, namely: … every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States“; vergleiche dies mit Norm c, welche (wie bereits weiter oben erwähnt) besagt: „States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs“.

verbindlich ist, dann hätte man einfach das Diktum im Korfu Kanal-Fall Wort für Wort übernehmen können. Die Tatsache, dass dies nicht geschah, deutet darauf hin, dass Staaten keine Übereinstimmung über die rechtliche Verbindlichkeit dieses Diktums im Cyber Kontext finden konnten. Dieser Meinung sind auch die USA, das Vereinigte Königreich, und Israel.[33]

Ein weiteres Beispiel des Konnexes zwischen Völkerrecht und nicht-verbindlicher Norm ist Norm f des 2015 GGE-Berichts. Norm f lautet wie folgt: „Ein Staat sollte *entgegen seinen völkerrechtlichen Verpflichtungen* keine Informations- und Kommunikationstechnologie-Aktivitäten durchführen oder wissentlich unterstützen, die kritische Infrastrukturen vorsätzlich schädigen oder die Nutzung und den Betrieb kritischer Infrastrukturen zur Bereitstellung von Diensten für die Öffentlichkeit anderweitig beeinträchtigen."[34] Demnach wird mit Norm f ein Verhalten als rechtlich unverbindliche Norm empfohlen, welches ohnehin bereits nach dem gängigen Völkerrecht nicht erlaubt wäre. Die explizite Erwähnung der völkerrechtlichen Verpflichtungen stärkt allerdings gleichzeitig die Bedeutung der Norm und stellt klar, dass völkerrechtliche Beschränkungen auch für den Cyber Kontext gelten sollten. Hier stellt sich allerdings die Frage, warum es notwendig erschien, diese Norm explizit auszuführen, wenn es das geltende Völkerrecht doch ohnehin bereits untersagt, kritische Infrastrukturen anzugreifen. Bzw. stellt sich auch gleichzeitig die Frage, was denn konkret diese völkerrechtlichen Verpflichtungen im Zusammenhang mit kritischer Infrastruktur sind, die ein Staat beachten muss.

Trotz dieses Links zum Völkerrecht schien es allerdings dennoch wichtig, dass diese Normen rechtlich unverbindlich sind. Eine Anekdote besagt, dass Jurist*innen bei den GGE-Verhandlungen manchmal den Raum verlassen mussten, damit überhaupt eine Einigung erreicht werden konnte.[35] Dies lässt auch darauf schließen, dass die Debatte rund um das Völkerrecht noch zu heikel war, um grundlegenden Konsens darüber zu finden, wie es konkret auf den Cyber Kontext anwendbar ist. In der Tat stellt die Debatte um das Völkerrecht auch weiterhin einen der umstrittensten Punkte in den UNO-Verhandlungen dar.

Andererseits erschien es den Verhandler*innen wichtig, unverbindliche Verhaltensnormen aufzustellen, um ein klares Zeichen zu setzen, dass gewisse Aktivitäten

---

[33] *Schöndorf*, International Law Studies 2021, 403–404; VNGV, Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by states submitted by participating governmental experts in the group of governmental experts on advancing responsible state behaviour in cyberspace in the context of international security established pursuant to General Assembly resolution 73/266, 13. Juli 2021, UN Dok A/76/136*, 117, Abs. 12 (Vereinigtes Königreich), 141 (Vereinigte Staaten von Amerika).

[34] Auf Englisch: „A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public", GGE Bericht 2015 (Fn. 29), 7–8, Ziffer 13 f.

[35] *Barrinha*, The Hague Journal of Diplomacy 2024, 13–14.

nicht tolerierbar sind. Eine rechtlich unverbindliche Norm bedeutete eine weniger bedrohliche Einschränkung des Handlungsspielraums der jeweiligen Staaten, aber gleichzeitig eine einzigartige Möglichkeit, der Dringlichkeit der Sache Ausdruck zu verleihen.[36]

Trotz ihrer völkerrechtlichen Unverbindlichkeit tragen diese Normen somit dennoch einen wesentlichen Schritt zur weiteren Regulierung des Cyberspace durch die Staatengemeinschaft dar. Auch wenn sie nicht rechtlich verbindlich sind, wurden sie bereits des Öfteren von Staaten verwendet, um ihre Missgunst gegenüber einem Verhalten eines anderen Staates auszudrücken. So wiesen die Vereinigten Staaten, in einer öffentlichen Mitteilung über die Attribuierung eines Cyber Angriffes auf China, darauf hin, dass sich die internationale Gemeinschaft auf eine Reihe von nicht-verbindlichen Verhaltensnormen im Cyberspace (eben jene elf Normen des 2015 GGE-Berichts) geeinigt habe und China sich nicht wie ein verantwortlicher Akteur und Einhalter dieser Normen verhalte.[37] In einem anderen Vorfall bezichtigte Australien Russland der Nichteinhaltung des „Rahmenwerks des verantwortungsvollen Staatenverhaltens im Cyberspace", unter welches diese Normen zählen.[38]

Im Gegensatz dazu gab es – unter den zahlreichen Attribuierungen in den letzten Jahren – kaum einen Hinweis auf die Verletzung des *Völkerrechts* durch diese Cyber-Angriffe. Als impliziter Vermerk zum Völkerrecht wird manchmal eine Attribuierung von Cyber-Angriffen gegen Georgien durch Russland vom Vereinigten Königreich gesehen. Hier vermerkte das Vereinigte Königreich, dass es weiterhin uneingeschränkt die Souveränität und territoriale Integrität Georgiens unterstütze.[39] Der explizite Hinweis auf die Souveränität und territoriale Integrität Georgiens könnte so gelesen werden, als ob das Vereinigte Königreich den Cyber-Angriff Russlands als Verletzung der Souveränität Georgiens sehe (was allerdings angezweifelt werden kann, da das Vereinigte Königreich nicht an eine Souveränitätsregel im Cyber Kontext glaubt).[40] Nahezu sämtliche politische Attributionen enthalten im Gegensatz dazu allerdings keinen Hinweis auf das Völkerrecht; dieses markante Schweigen zum Völkerrecht in den politischen Attributionen – welche zum Großteil von westlichen Staaten, allen voran den USA, ausgehen – ist durchaus nicht hilfreich

---

[36] Über die Bedeutung von sogenanntem „Soft Law" und seine Auswirkungen auf das Völkerrecht, sh. unter anderem *Thürer*, in: Peters/Wolfrum (Hrsg.), Max Planck Encyclopedia of Public International Law, 2009.

[37] *US Vertretung zur NATO*, Responding to the PRC's Destablizing and Irresponsible Behavior in Cyberspace, 19. Juli 2021, https://nato.usmission.gov/responding-to-the-prcs-destabilizing-and-irresponsible-behavior-in-cyberspace/ (22.9.2025).

[38] *Australien*, Attribution of Malicious Cyber Activity in Georgia by Russian Military Intelligence, Februar 2020, https://parlinfo.aph.gov.au/parlInfo/download/media/pressrel/7197176/upload_binary/7197176.pdf (22.9.2025).

[39] *Vereinigtes Königreich*, UK Condemns Russia's GRU over Georgia Cyber-attacks, 20. Februar 2020, www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks (22.9.2025).

[40] Sh. dazu *Wright*, Cyber and International Law in the 21st Century, 23. Mai 2018, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century (22.9.2025).