



FRIEDRICH NAUMANN
STIFTUNG Für die Freiheit.

DIGITALPOLITIK IM GLOBALEN SYSTEM- WETTBEWERB

Herausforderungen für
liberale Demokratien

Ann Cathrin Riedel

ANALYSE

Impressum

Herausgeberin

Friedrich-Naumann-Stiftung für die Freiheit
Truman Haus
Karl-Marx-Straße 2
14482 Potsdam-Babelsberg

🌐/freiheit.org

📘/FriedrichNaumannStiftungFreiheit

📺/FNFreiheit

📷/stiftungfuerdiefreiheit

Autorin

Ann Cathrin Riedel
Referentin Globale Digitalisierung & Innovation
Abteilung Globale Themen

Kontakt

Telefon +49 30 220126-34
Telefax +49 30 690881-02
E-Mail service@freiheit.org

Stand

März 2023

Hinweis zur Nutzung dieser Publikation

Diese Publikation ist ein Informationsangebot der Friedrich-Naumann-Stiftung für die Freiheit. Die Publikation ist kostenlos erhältlich und nicht zum Verkauf bestimmt. Sie darf nicht von Parteien oder von Wahlhelfern während eines Wahlkampfes zum Zwecke der Wahlwerbung verwendet werden (Bundtags-, Landtags- und Kommunalwahlen sowie Wahlen zum Europäischen Parlament).

Lizenz

Creative Commons (CC BY-NC-ND 4.0)

Inhaltsverzeichnis

EXECUTIVE SUMMARY	4
1. EINLEITUNG	6
2. INTERNATIONALE DIGITALPOLITIK: EIN NEUES SPIELFELD?	7
2.1. Internationale Digitalpolitik vs. Internet Governance	7
3. DIGITALPOLITIK IM SYSTEMWETTBEWERB: WANDEL DURCH ANNÄHERUNG?	9
4. GRUNDLAGE LIBERALER DEMOKRATIEN: INTERNETFREIHEIT	10
5. DER PUDDING IST AN DER WAND: AUTOKRATIEN UND DAS INTERNET	12
6. KRITISCHE INFRASTRUKTUREN: WO GEFÄHRLICHE ABHÄNGIGKEITEN BESTEHEN	13
6.1. Daten aus dem Meer: Unterseekabel	13
6.2. Politisiert: Normen und Standards	14
6.3. Die kritischste Technologie der Welt: Chips	15
7. NEUE POLITISCHE AKTEURE: PRIVATE UNTERNEHMEN IN DER INTERNATIONALEN DIGITALPOLITIK	17
7.1. Internet aus dem Weltall: Elon Musks Starlink	17
7.2. Der Hauptausstatter der chinesischen digitalen Seidenstraße: Huawei	18
7.3. Was darf aufs Smartphone? Google und Apple als Gatekeeper	19
8. POLICY EMPFEHLUNGEN	21
LITERATURVERZEICHNIS	24
AUTORIN	30

Executive Summary

Der deutsche Bundeskanzler Olaf Scholz hat am 27. Februar 2022, drei Tage nach dem völkerrechtswidrigen Angriff Russlands auf die Ukraine, eine Zeitenwende der deutschen Außen- und Sicherheitspolitik ausgerufen. Die Zeitenwende betrifft auch die digitalen und technologischen Abhängigkeiten in Deutschland und Europa. Als Akteur setzt die Europäische Union hier längst internationale Standards für Deutschland und die EU-Mitgliedstaaten und schafft Voraussetzungen für eine handlungsfähige Politik gegenüber den außen- und sicherheitspolitischen Herausforderungen.

Geopolitik gewinnt zunehmend an Bedeutung in der deutschen und europäischen Politik. Bis dato spielte der digitale Raum darin jedoch nur eine untergeordnete Rolle. Die Souveränität Europas und liberaler Demokratien im Allgemeinen hängt im digitalen Zeitalter von einem freien, offenen und globalen Internet ab, aber auch dem Zugang zu Technologien und sicheren, diversifizierten Lieferketten. Die legislative Macht, die Europa in großen Teilen hat – Stichwort *Brussels Effect* – reicht nicht aus, um die Souveränität zu sichern und ein starker, selbstbewusster Akteur in der digitalen Geopolitik zu sein. Das vorliegende Papier führt in die Internet Governance ein und zeigt, warum Internetfreiheit grundlegend für die Freiheit von Gesellschaften im 21. Jahrhundert ist.

Anhand von jeweils drei Beispielen wird exemplarisch analysiert, in welchen Bereichen Abhängigkeiten bestehen (bei Unterseekabeln, in Bezug auf Normen und Standards, oder in der Chips-Industrie) und welche Rolle private Akteure in der internationalen Digitalpolitik einnehmen. Sowohl der privatwirtschaftliche Einfluss beispielsweise beim Zugang zum Internet aus dem Weltall durch Elon Musks Starlink, Huawei und Chinas digitaler Seidenstraße, oder Google und Apple als Gatekeeper für Apps auf Smartphones wird bisher nur im Einzelfall betrachtet, birgt jedoch Risiken für die Souveränität liberaler Demokratien. Die vorliegende Analyse betrachtet die Zusammenhänge der unterschiedlichen Abhängigkeiten.

Die digitale Geopolitik verbindet zwei gegensätzliche Trends in der internationalen Politik: die Machtpolitik territorialer Einheiten (Nationalstaaten und regionale Akteure wie die EU) und dezentralisierte transnationale Netzwerke nichtstaatlicher Akteure und multinationaler Unternehmen. Die Bedeutung der internationalen Digitalpolitik hat in Deutschland zugenommen, wie bereits der Koalitionsvertrag zwischen SPD, Grünen und FDP von 2021 zeigt. Deutschland beteiligt sich seit Jahrzehnten aktiv an der Internet Governance und wirkt in Organisationen wie der Internet Corporation for Assigned Names and Numbers (ICANN), dem Internet Governance Forum (IGF) und der International Telecommunication Union (ITU) mit. Die internationalen Organisationen selbst, ihre Relevanz und die deutsche Rolle in der multilateralen Zusammenarbeit werden in der Öffentlichkeit jedoch kaum wahrgenommen. Doch gerade internationale Institutionen und Normen sind fundamental für die liberale Weltordnung.

Ein offenes und freies Internet ist dafür unerlässlich. Die Grundsätze der Demokratie, des freien Handels und der Rechtsstaatlichkeit können nur aufrechterhalten werden, wenn die freie Meinungsäußerung, der Austausch von Ideen und der Zugang zu Informationen auch in der digitalen Welt gewährleistet sind. Autokratische Staaten verwehren ihren Bürgerinnen und Bürgern diese grundlegenden Rechte. Chinas sogenannte „Große Firewall“ ist zu einem Modell für Autokratien geworden. Die Abnahme der Internetfreiheit in den vergangenen zwölf Jahren demonstriert, dass immer mehr Staaten den Zugang ihrer Bevölkerung zu Informationen einschränken und die freie Meinungsäußerung kontrollieren.

Die Analyse der Digitalpolitik im internationalen Systemwettbewerb ergibt, dass die Dimension der Geopolitik dringend stärker in den Blick genommen werden muss. Der digitale Raum hat eine enorme Bedeutung für Gesellschaften im Alltag und die liberale Weltordnung. Antworten auf den Systemwettbewerb können nur **Allianzen für Demokratie** liefern. Auf nationaler Ebene ist eine stärkere und strategischere Zusammenarbeit einzelner Ressorts, sowie der Wirtschaft und der Zivilgesellschaft erforderlich.

Libérale Demokratien müssen sich auch in Zukunft konsequent für Internetfreiheit, Demokratie und Menschenrechte einsetzen. **Deutschland und die Europäische Union gelten als Vorbild.** Sie sollten es daher unbedingt unterlassen, selber Gesetzesinitiativen vorzulegen, die beispielsweise das Menschenrecht auf Privatsphäre einschränken.

Neben Gas, wurde auch die Abhängigkeit von Chips im Zuge des Krieges Russlands gegen die Ukraine und der Covid-Pandemie deutlich. Ein umfassender und **regelmäßiger Stress- test für digitale und technologische Abhängigkeiten** kann Risiken minimieren und die Souveränität Deutschlands und Europas stärken.

Unterseekabel, die Daten von Kontinent zu Kontinent leiten, sind derzeit nicht nur ungenügend geschützt, sondern auch immer stärker in der Hand von chinesischen und amerikanischen Big Tech-Konzernen. **Internet aus dem Weltraum** kann vornehmlich nur von privaten Unternehmen bereitgestellt werden. Um die Gefahr vor Sabotage und Abhängigkeit zu reduzieren, müssen strategische Maßnahmen ergriffen und Kapazitäten aufgebaut werden. Politisches Engagement im Weltall ist keine Spielerei, sondern eine geopolitische Notwendigkeit. Nur so kann die erforderliche Infrastruktur zur Kommunikation im Fall von bewaffneten Konflikten oder Umweltkatastrophen, wie der Flut im Ahrtal 2021, zur Verfügung zu gestellt werden.

Mit **einer Strategie für internationale Digitalpolitik** sollte Deutschland untermauern, dass es die Bedeutung dieses Themas erkannt hat und in Zukunft ein wichtiger Akteur sein möchte. Dazu sollte die Bundesregierung eine ehrgeizige Stra-

ategie ressortübergreifend und gemeinsam mit der Zivilgesellschaft entwickeln. Parallel sollten **globale Partnerschaften** ausgebaut und neue eingegangen werden. Das betrifft neben natürlichen Verbündeten wie den USA mit dem Trade and Technology Council auch Partner wie Indien und Brasilien. Die „Partnerschaft auf Augenhöhe“ darf insbesondere in Afrika und anderen Ländern des Globalen Südens keine Floskel sein. Für Abstimmungen in internationalen Gremien wie der ITU ist ein starkes demokratisches Lager notwendig.

Offene Standards müssen gefördert und eingesetzt werden. Dies ist für die Herausforderungen des globalen Systemwettbewerbs ebenso von Bedeutung wie für die **Digitalisierung von kommunalen Verwaltungen**.

Menschenrechtliche Sorgfaltspflichten erstrecken sich auch auf den digitalen Raum. Insbesondere dann, wenn Unternehmen eine Gatekeeper-Funktion einnehmen. Das Wettbewerbsrecht und Möglichkeiten, die sich aus der europäischen Gesetzgebung zu Lieferketten ergeben werden, müssen stärker genutzt werden, um **rechtsstaatliche Standards** und menschenrechtliche Normen auch im Digitalen durchzusetzen.

Deutschland und die Europäische Union setzen **regulative Standards** – beispielsweise mit der Datenschutzgrundverordnung oder dem Digital Services Act. Gesetze, Normen und Standards können aber immer nur ein Baustein in der von der EU ausgerufenen wertebasierten Digitalisierung sein. Um diese umzusetzen und Partner für diesen Weg zu überzeugen, sind auch Produkte und Technologien gefragt, die diese Werte by design implementiert haben und erworben werden können. Europäische Unternehmen müssen in der Lage sein, den Transfer zu **marktreifen und international wettbewerbsfähigen digitalen Produkten und Technologien** zu leisten, die das „Made in Germany“ oder „Made in Europe“ des 21. Jahrhunderts werden können.

1. Einleitung

Drei Tage nach dem völkerrechtswidrigen Angriffskrieg Russlands gegen die Ukraine rief Bundeskanzler Olaf Scholz vor dem Deutschen Bundestag eine Zeitenwende aus. Er adressierte neben notwendigen sicherheitspolitischen Maßnahmen und dem 100 Milliarden Euro starken Sondervermögen für die Deutsche Bundeswehr auch die Importabhängigkeiten Deutschlands im Bereich der Energie (Scholz 2022). Neben dem Krieg in Europa waren die Abhängigkeiten, denen Deutschland ausgesetzt ist, politisches Thema des Jahres 2022. Dazu kamen neben denen vom russischen Gas auch die wirtschaftlichen Abhängigkeiten gegenüber China hinzu, die nun nicht mehr nur von einzelnen Expertinnen und Experten kritisch benannt wurden. Die Losung, China sei Partner, Wettbewerber und systemischer Rivale, die zwar schon vom ehemaligen Außenminister Heiko Maas (SPD) 2020 in einem Interview genutzt wurde (Auswärtiges Amt 2020) und auch von der Europäischen Kommission und dem Europäischen Auswärtigen Dienst so verwendet wird (Heinrich 2020), und die Problematik der Beziehung zu China wiedergibt, wird auch daher immer häufiger deutlich genutzt.

In eben jener Rede zur Zeitenwende vom 27. Februar 2022 stellte Olaf Scholz folgende Frage: „Welche Fähigkeiten besitzt Putins Russland, und welche Fähigkeiten brauchen wir, um dieser Bedrohung zu begegnen, heute und in der Zukunft?“ Er erklärte: „Europa ist unser Handlungsrahmen. Nur wenn wir das begreifen, werden wir vor den Herausforderungen unserer Zeit bestehen.“ Dies stellt sich auch im Bereich der digitalen Abhängigkeiten. Zu wenig wird über die digitalen und die technologischen Abhängigkeiten Deutschlands und Europas öffentlich diskutiert (Riedel/Widlok 2022). Eine Ausnahme besteht beim Thema Chips. Die Abhängigkeiten in diesem Bereich bekamen insbesondere während der Corona-Pandemie zahlreiche Unternehmen zu spüren, darunter deutsche Automobilhersteller. In einer weiteren Rede des Bundeskanzlers zur Zeitenwende, am 29. August 2022 in Prag, Tschechien, adressierte er auch diese Abhängigkeit und äußerte den Wunsch, dass Europa Vorreiter bei wichtigen Schlüsseltechnologien werde. Ebenso adressierte er Europas Souveränität, die im Digitalzeitalter auch von Fähigkeiten im Weltraum abhängt. Ein unabhängiger Zugang zum All, moderne Satelliten und Megakonstellationen seien nicht nur für unsere Sicherheit entscheidend, sondern auch für den Umweltschutz, die Landwirtschaft und für den Zugang zum Internet (Scholz 2022).

Geopolitik ist zunehmend wieder Thema in der deutschen und europäischen Politik. Der digitale Raum spielt aber bislang nur eine untergeordnete Rolle. Dabei ist die „digitale Geopolitik [...] auf dem Vormarsch“ (Bendiek et al. 2019). Digitale Geopolitik verdient mehr Beachtung. Schließlich sind die Gesellschaften des 21. Jahrhunderts auf dem Internet aufgebaut. Ein Großteil der Weltbevölkerung ist wirtschaftlich und gesellschaftlich von ihm abhängig. Wie sehr, merken Menschen in liberalen Demokratien häufig erst, wenn das Internet durch technische Fehler oder Naturkatastrophen ausfällt. In autoritär regierten Ländern sind Eingriffe wie Zensur, Internetschuttdowns oder Überwachungsmaßnahmen hingegen an der Tagesordnung.

Das folgende Papier analysiert, was internationale Digitalpolitik umfasst und warum sie im Systemwettbewerb immer bedeutsamer wird, um liberale Demokratien zu schützen und zu stärken. Es soll zudem exemplarisch untersuchen, welche technologischen Abhängigkeiten bestehen und welche Rolle privatwirtschaftliche Akteure im Bereich der digitalen Geopolitik spielen. Dabei geht es nicht darum, die Existenz privatwirtschaftlicher Akteure per se zu kritisieren – Private nehmen schon lange aktive Rollen in der internationalen Politik ein. Es soll aufzeigen, dass im Digital- und Tech-Bereich kritische Machtkonzentrationen liegen, die es zu diskutieren gilt, um digitale Souveränität zu gewährleisten und liberale Demokratien zu stärken. Unter digitaler Souveränität wird in diesem Papier die Umsetzung von drei strategischen Zielen verstanden: die Möglichkeit des Wechsels (eines Anbieters), die Fähigkeit zu gestalten und Einfluss auf Anbieter ausüben zu können. Dafür bedarf es eine Vielfalt von Anbietern, eine notwendige Gestaltungsmacht und gute Beziehungen zu gleichgesinnten Partnern (Riedel/Widlok 2022).

2. Internationale Digitalpolitik: Ein neues Spielfeld?

Insbesondere die Auseinandersetzung zwischen den USA und China um Huawei, das der ehemalige US-Präsident Donald Trump im Mai 2019 auf die Sanktionsliste des US-Handelsministeriums setzen ließ, habe eine zutiefst geopolitische Dimension erreicht, die sinnbildlich für einen fundamentalen Bruch mit der marktwirtschaftlichen Logik steht, schreiben Annegret Bendiek, Nadine Godehardt und David Schulze 2019 in einem Beitrag für das Journal für Internationale Politik und Gesellschaft. Die Autorinnen und Autoren zeigen auf, dass die Fragen der digitalen *Geopolitik* unsere besondere Aufmerksamkeit benötigen. Digitale Geopolitik verbinde zwei gegenläufige Trends der internationalen Politik, die zwar nicht neu seien, aber häufig voneinander getrennt diskutiert werden würden: „Einerseits beruht *digitale* Geopolitik auf der Machtpolitik territorialer Einheiten, beispielsweise von Nationalstaaten wie den USA und China oder regionalen Akteuren wie der Europäischen Union. Andererseits beinhaltet digitale Geopolitik dezentrale transnationale Netzwerke, bestehend aus Konnektivitäten zwischen nicht-staatlichen Akteuren und multinationalen Unternehmen, Plattformen, Knotenpunkten, Inhalten und Infrastrukturen jenseits der politisch fixierten territorialen Einheiten.“ (Bendiek et al. 2019 Hervorhebungen im Original).

Die internationale und geopolitische Dimension der Digitalpolitik ist in der deutschen Politik eigentlich nicht neu. Bereits 2013 berief der damalige Außenminister Guido Westerwelle den ersten Beauftragten für Cyber-Außenpolitik (Hebel 2013). Deutschland beteiligt sich bereits seit Jahrzehnten aktiv in internationalen Gremien zur Digitalpolitik, genauer: zur Internet Governance. Darunter fallen zu Beispiel die Internet Corporation for Assigned Names and Numbers (ICANN), das Internet Governance Forum (IGF), die Internet Society (ISOC) oder die Internationale Fernmeldeunion (ITU). Bislang, so kann man sicherlich postulieren, haben sowohl das Engagement dort, als auch die Institutionen an sich wenig breite öffentliche Aufmerksamkeit erlangt. Selbst nicht, als 2019 das IGF in Berlin tagte. Mit dem – wenn auch unverbindlichen – „Jimmy Schulz Call“ bekannten sich dort die unterzeichnenden und überhaupt erstmals in einem Parlamentarier-Track zusammengekommenen internationalen Abgeordneten zu mehr Engagement in den nationalen Parlamenten für ein freies, offenes, stabiles, nicht fragmentiertes und innovatives Internet (Ermert 2019; IGF 2019). Dass die internationale Digitalpolitik an Bedeutung in Deutschland gewonnen hat, zeigt sich an dem Koalitionsvertrag der Regierung zwischen SPD, Grünen und FDP aus dem Jahr 2021 (SPD, Bündnis90/Die Grünen, FDP 2021: 144). Nicht nur findet sich hier – ebenso in der 2022 beschlossenen Digitalstrategie (Die Bundesregierung 2022a: 50ff) – ein Bekenntnis für ein stärkeres Engagement in unter anderem oben genannten Organisationen. Etwas, das sich in den zwei Koalitionsverträgen der Großen Koalitionen zwischen SPD und CDU/CSU von 2013 und 2017 nicht fand. Hier zeigt sich

zudem indirekt, dass die Ampel-Koalition die geopolitische Dimension des Digitalen verstanden hat und Partner, zusammen mit der EU, im Rahmen der Entwicklungspolitik beim Aufbau einer „*unabhängigen* [Hervorhebung der Autorin] digitalen Infrastruktur zur Stärkung ihrer digitalen Souveränität“ (SPD, Bündnis90/Die Grünen, FDP 2021: 144) unterstützen will.

2.1 Internationale Digitalpolitik vs. Internet Governance

Ob *e-*, *cyber*, *virtuell*, oder *digital* – laut dem Standardwerk zu Internet Governance von Jovan Kurbalija könnten diese Präfixe beliebig ausgetauscht werden, denn alle bezeichneten das „Internet-Phänomen“. Das Voranstellen eines Präfixes habe im Laufe der Zeit mehr und mehr an Bedeutung gewonnen. Bestimmte Präfixe bezeichnen dabei häufig einen bestimmten Teilbereich der Policies für das Internet. So wird *e-* häufig für Handelsbezüge (*e-commerce*) verwendet, *cyber* für Kriminalität und Sicherheitsaspekte, *digital* für Entwicklungsunterschiede, später auch eine breitere Nutzung, insbesondere durch Regierungen, und *virtuell* für Währungen, wie zum Beispiel Bitcoin (Kurbalija 2016: 14f).

Die deutsche Bundesregierung definiert „Internet Governance“ eher eng: „Unter dem Begriff der Internet Governance werden Maßnahmen zusammengefasst, die den Zugang, die Stabilität und die Offenheit des Internets sicherstellen sollen.“ (Bundesministerium für Wirtschaft und Klimaschutz o. J.). Darunter versteht sie die Verwaltung wesentlicher Internetfunktionen und die effiziente Verteilung von Internetressourcen, wie die weltweite Vergabe von IP-Adressen und die Registrierung von Domainnamen. Allerdings fasst die Bundesregierung auch andere Themen von „grundsätzlicher Bedeutung“ unter Internet Governance, darunter Datensicherheit, Künstliche Intelligenz oder Netzneutralität (Bundesministerium für Wirtschaft und Klimaschutz o. J.).

Digitalpolitik ist für die Bundesregierung vor allem eine „Querschnittsaufgabe“ aller Ressorts. Darunter fallen auch rein nationale Aufgaben, wie die Digitalisierung der Verwaltung und der Justiz. Diese Themenkomplexe beschäftigen sich zudem eher weniger mit den Strukturen, Normen und Standards des Digitalen an sich, sondern sind eher eine Modernisierung von Soft- und Hardware, sowie eine Transformation von Prozessen (obgleich auch ein Teil der Digitalisierung in diesen Bereichen die gemeinsame Definition von Standards für z. B. Schnittstellen ist). Ebenso ist ein Teil der Digitalpolitik der Bundesregierung die IT-Steuerung, die Förderung der Digitalwirtschaft und der Infrastrukturausbau für ein flächendeckendes Glasfasernetz (Die Bundesregierung 2022b).

Digitalpolitik, wie sie in diesem Policy Paper verstanden werden soll, ist deckungsgleich mit der Definition von Internet Governance von Jovan Kurbalija, dem ehemaligen Vorsitzenden des UN Internet Governance Forums. Diese Definition wurde auch von der UN Commission on Science and Technology for Development übernommen, welche im „Mapping of international Internet public policy issues“ (Commission on Science and Technology for Development 2015) veröffentlicht wurde. Die Begriffe internationale Digitalpolitik und Internet Governance sollen in diesem Papier auch daher synonym verwendet werden, da sich die digitalpolitischen Themen hier auf internationale Aspekte der Digitalpolitik fokussieren, das heißt Politiken, die vornehmlich multilateral behandelt werden können und sollten.

Jovan Kurbalija stellte in seinem Einführungswerk zur Internet Governance, das erstmalig 1997 erschien, auch eine Taxonomie der Policy-Bereiche der Internet Governance vor. Sie besteht aus 53 Policy Feldern in sieben „Baskets“, die hier wiedergegeben werden sollen, um einen Eindruck über die Weite und Komplexität der Internet Governance zu verschaffen.

Internet Governance Taxonomie¹

Infrastructure Basket
The telecommunications infrastructure
Internet access providers
Transmission Control Protocol/Internet Protocol
The Domain Name System
Root zone and root servers
Network neutrality
Technical and web standards
Cloud computing
Internet of Things
Convergence

Security Basket
Cybersecurity
Cybercrime
Critical Infrastructure
Cyberterrorism
Cyberconflict and warfare
Encryption
Spam
Digital signatures
Child safety online

Legal Basket
Legal instruments
Jurisdiction
Alternative dispute resolution
Copyright
Trademarks
Patents
Labour law
Intermediaries

Economic Basket
E-commerce
Internet DATA economy
Internet ACCESS economy
Emerging trends: Internet of Things, artificial intelligence, sharing economy
E-banking, e-money, and virtual currencies
Consumer protection
Taxation

Development Basket
Digital technologies and development: policy framing
How does ICT affect the development of society?
The digital divide
Capacity development

Sociocultural Basket
Content policy
Online education
Cultural diversity
Multilingualism
Global public goods

Human Rights Basket
Online vs offline human rights
Technology and human rights
'New' human rights enabled by the internet
The internet and existing human rights
Freedom of expression and the right to seek, receive, and impart information
Privacy and data protection
Children's rights in a digital world
Rights of persons with disabilities
Gender and human rights online

¹ Zur vertiefenden Lektüre der einzelnen Taxonomien wird das Einführungswerk von Jovan Kurbalija empfohlen, dem diese Taxonomie entnommen ist und das als Open Access frei verfügbar online abrufbar ist: https://www.diplomacy.edu/wp-content/uploads/2021/12/AnIntroductiontoIG_7th-edition.pdf

3. Digitalpolitik im Systemwettbewerb: Wandel durch Annäherung?

Wie kommt es, dass es trotz der immer stärker werdenden Vernetzung zu größeren geopolitischen Spannungen kommt? Ist das politische Konzept „Wandel durch Handel“ beziehungsweise „Wandel durch Annäherung“, wie es eigentlich in der Rede von Egon Bahr vom 15. Juli 1963 auf einer Tagung der Evangelischen Akademie Tutzing eingeführt wurde und den Kern der sozialliberalen Ost- und Entspannungspolitik der Ära Brandt/Scheel bildete (Bahr 1963; Lau 2021; Stenke 2013), auch im digitalen Raum gescheitert, wo doch der Grundgedanke des Internets ist, die Welt zu einem globalen Dorf zu machen?

Der Erfolg der sozialliberalen Ostpolitik konnte zeigen, dass (wirtschaftliche) Verflechtung zu Wandel führen *kann*. Dieses Konzept ist nicht ins Gegenteil verkehrt, doch kann es so unqualifiziert nicht stehen gelassen werden. Die immer stärkere Vernetzung und Verflechtung von Wirtschaft, Lieferketten und Kommunikation habe, so der Politologe Mark Leonard in seinem Buch „The Age of Unpeace“ nicht die Hoffnung erfüllt, Kriege unmöglich zu machen. Vielmehr, so seine These, tragen Staaten Konflikte aus, indem sie genau die Dinge missbrauchen, die sie miteinander verbinden. Diese These sei nicht neu, räumt Leonard selbst ein. Sie gehe bereits auf Jean-Jacques Rousseau zurück und wurde in den 1970ern von Karl Polanyi, Robert Keohane und Joseph Nye diskutiert. Leonard stellt sich in seinem Werk aber die folgenden Fragen: „What if the process that brings us together is actually what *causes* segregation and conflict? What if the growing divisions in the globalized world are not a bug in the system but one of its intrinsic features?“ (Leonard 2021: 9 Hervorhebungen im Original).

Wohl auch durch die stärkere Vernetzung durch Lieferketten, Finanz- und Informationsströme fand ein Wandel in der Betrachtung der internationalen Beziehungen statt. Ab den 1990er Jahren entwickelte sich – zuerst in der Soziologie – ein Fokus auf Netzwerke. Anne-Marie Slaughter verbildlicht dies anhand eines Bildes des Globus aus dem All. Dort sieht man in der Dunkelheit durch die Lichter der Zivilisation die Verbindungen – das Netz – durch die moderne Gesellschaften miteinander verbunden sind. Die Realität, so Slaughter, sei eben keine klassische Karte mit Grenzen, die die Herrschaftsbereiche durch starre Linien eingrenzen, so wie es die klassische „Schachbrett“-Betrachtung der internationalen Beziehungen annimmt (Slaughter 2018: 7–8): „Foreign policy experts have long been taught to see the world as a chessboard, analyzing the decisions of great powers and anticipating rival states’ reactions in a continual game of strategic advantage.“ (Slaughter 2016). Dies sei nun nicht mehr der Fall.

In dieser vernetzten Welt ist die Anzahl an Akteuren, die sich effektiv mit globalen Sachverhalten beschäftigen, dramatisch angestiegen. So würden sich nicht nur diverse Ministerien und



Quelle: Slaughter, Anne Marie (2018)

Behörden in der Außenpolitik einbringen, sondern auch – hier im Falle der USA – Gouverneure der einzelnen Bundesstaaten. Aber auch Vertreterinnen und Vertreter von einzelnen Städten beschäftigen sich mittels Städtepartnerschaften über nationale Grenzen hinweg mit der Lösung von internationalen Problemen. Die thematische Spanne reicht dabei, so Slaughter, von der Umweltpolitik bis hin zur Terrorismusbekämpfung. Dass sich Städte in den internationalen Beziehungen einbringen, begrüßten und befürworteten auch die deutsche Außenministerin Annalena Baerbock und ihr US-amerikanischer Amtskollege Antony Blinken im Rahmen einer Veranstaltung zum Treffen der G7-Außenminister in Münster (US State Department 2022).

Auch außerhalb der Exekutiven finden sich immer mehr Akteure der internationalen Beziehungen. So gestalten Stiftungen, Universitäten und zivilgesellschaftliche Organisationen immer stärker die Lösungsfindung globaler Probleme mit. Besonders die Bekämpfung des Klimawandels und der Einsatz für weltweite Gesundheit sind hier zwei bekannte Politikfelder. Neben diesen NGOs gestalten auch Unternehmen, insbesondere global operierende, die internationale Politik mit. Dass Unternehmen Akteure in diesem Feld sind, ist ebenfalls nicht neu (Slaughter 2018: 20–22). Schon die East India Company hatte eine große Rolle in der Geopolitik (Bremmer 2022). Teilweise sind CEOs solcher Unternehmen sogar mächtigere globale Akteure als Regierungschefs und Außenministerinnen. Zumindest dort, wo keine Stimme bei den Vereinten Nationen oder anderen internationalen und regionalen Organisationen notwendig ist. Haben diese Unternehmen doch mitunter eine größere Marktkapitalisierung, als das Bruttoinlandsprodukt einiger kleinerer Staaten. Bereits 2014 waren unter den 175 weltweit größten Wirtschaftssubjekten 112 Unternehmen und nur 63 Staaten (Malik 2014; Slaughter 2018: 22).

4. Grundlage liberaler Demokratien: Internetfreiheit

Ein offenes und freies Internet ist die Grundlage für eine liberale Weltordnung im 21. Jahrhundert. Die sich auf ihr beruhenden Grundsätze von Demokratie, Freihandel und Rechtsstaatlichkeit können nur gewahrt werden, wenn unter anderem die freie Meinungsäußerung, der Austausch von Ideen und der Zugang zu Informationen auch im digitalen Raum gewährleistet wird. Ebenso gehören internationale Institutionen und Normen zur Grundlage einer liberalen Weltordnung. Sie spielen auch beim Erhalt der Internetfreiheit eine große Rolle. Hervorzuheben sind hier die Internationale Fernmeldeunion (ITU), eine Sonderorganisation der Vereinten Nationen, und das Internet Governance Forum (IGF), ein von den Vereinten Nationen mandatiertes Multi-Stakeholder Format, bei dem sich neben Regierungsvertretern auch Expertinnen aus Wirtschaft, Zivilgesellschaft und Wissenschaft miteinander austauschen – allerdings lediglich mit unverbindlichen Empfehlungen.

Für die Freiheit des Internets können sich Staaten jedoch nicht allein einsetzen. Zu dieser Erkenntnis gelangte man bereits 2005 beim UN-Weltgipfel zu Informationsgesellschaft in Tunis (WSIS II). Vielmehr seien für das Internet relevante Probleme nur mit allen Beteiligten zu lösen. Aus dem WSIS II resultiert daher auch das Mandat für das bereits erwähnte Multi-Stakeholder-Forum, das IGF, bei dem Wirtschaftsvertreterinnen, Wissenschaftlerinnen und NGOs zusammenkommen. Zu anderen, beziehungsweise weiteren Deklarationen kamen nicht nur Staaten, sondern auch Staaten mit nicht-staatlichen Akteuren zusammen. Ein Beispiel dafür ist der 2018 verabschiedete Paris Call for Trust and Security in Cyberspace. Dieser baut auf den Vorarbeiten der Global Commission on the Stability of Cyberspace (GCSC) auf, die 2017 vorschlug, eine universell geltende Norm zum Schutz des öffentlichen Internets zu schaffen. Nach dieser wäre es verboten, die technischen Kernbestandteile des globalen Internets, also Domainnamen, IP-Adressen, Internetprotokolle, Router, Server, Kabel und Satelliten, anzugreifen. Diese Norm fand Eingang in den Paris Call, die 64 Regierungen, darunter die USA, die Europäische Union und ihre einzelnen Mitgliedsstaaten, aber auch Chile, Kambodscha, der Kongo, Südkorea, die Vereinigten Arabischen Emirate, Guinea, Japan, Mauretanien, Usbekistan, Katar, die Zentralafrikanische Republik, Singapur und Tunesien unterzeichneten. Was auffällt, ist, dass Indien und Brasilien fehlen. Außerdem unterzeichneten 672 nicht-staatliche Akteure den Paris Call, darunter die meisten Silicon-Valley-Konzerne (Kleinwächter 2019; Paris Call 2018).

Auch früher gab es bereits Initiativen von Staaten – unabhängig von den oben genannten Institutionen – die sich für die Stärkung des freien und offenen Internets einsetzten. 2011 bildete sich eine Gruppe von 34 Staaten zur Freedom Online Coalition (FOC), die die Internetfreiheit durch die Gestaltung von globalen Menschenrechtsnormen und gemeinsamen Erklärungen, sowie durch diplomatische Koordination und Netzwerke erhalten möchte. Zu den Mitgliedsstaaten gehören neben den USA, Deutschland und Frankreich weitere EU-Mitglieder, aber auch Staaten wie Ghana, Kenia, die Mongolei, die Malediven und Chile (Freedom Online Coalition o. J.). Neben Erklärungen, die sich gegen Zensur im Internet, staatlich veranlasste Störungen des Internets und Beschränkungen des Zugangs zu sozialen Medien ausgesprochen haben, verabschiedete die FOC auch Erklärungen zum Gebrauch und Export von Überwachungstechnologie (Auswärtiges Amt 2018).

2022 versuchte die Biden-Administration mehrere Staaten unter der Deklaration zur Zukunft des Internets zu versammeln. Was als Statement gegen Russland und China angesehen werden kann, sei vielmehr eine Warnung an schwankende Demokratien zu Fehlverhalten im digitalen Raum, so der Brookings-Fellow Alex Engler (Engler 2022). Das nicht-bindende, dreiseitige Dokument wurde von 61 Staaten unterzeichnet. Darunter auch hier die USA, Deutschland und Frankreich sowie weitere EU-Mitglieder und die Europäische Kommission. Aber auch der Kosovo, die Marshall-Inseln und Mikronesien, sowie Niger, Korea, Israel, Taiwan und die Ukraine. Auffällig ist auch hier, dass Indien und Brasilien nicht unterzeichnet haben. Chile hat sich an dieser Deklaration nicht mehr beteiligt. Südostasiatische Staaten wie Indonesien, das 2022 den G20-Vorsitz innehatte, oder Malaysia fehlen ebenso wie beispielsweise Südafrika, Nigeria und Mexiko (Declaration for the Future of the Internet 2022; United States Department of State 2022). Die Deklaration kann als eine Art Verhaltenskodex gewertet werden. Sie will den universellen Internetzugang fördern, die Menschenrechte schützen, einen fairen wirtschaftlichen Wettbewerb gewährleisten, eine sichere digitale Infrastruktur schaffen, Pluralismus und Meinungsfreiheit fördern und einen Multi-Stakeholder-Ansatz für die Internet Governance garantieren (Engler 2022). Selbst wenn das Dokument nicht bindend ist, kann die Vereinigung von 61 Staaten unter diesem Dokument als Erfolg gewertet werden. Gleichwohl müssen sich alle Unterzeichner fragen – auch die EU-Mitglieder und die Europäische Kommission –, ob all ihre (legislativen) Initiativen immer diesen unterzeichneten Ansprüchen Rechnung tragen.

Internet Governance Forum (IGF)²

Das Internet Governance Forum (IGF) ist eine Multistakeholder-Plattform, die den Dialog über politische Fragen im Zusammenhang mit dem Internet ermöglicht. Es wurde 2006 von den Vereinten Nationen (UN) als Ergebnis des Weltgipfels über die Informationsgesellschaft (WSIS) gegründet, der 2003 und 2005 stattfand. Der WSIS war eine globale Konferenz, die sich mit den Chancen und Herausforderungen des Internets befassen und die Nutzung von Informations- und Kommunikationstechnologien (IKT) für die Entwicklung fördern sollte.

Das IGF ist eine Plattform für Interessenvertreter aus Regierungen, dem Privatsektor, der Zivilgesellschaft und der Wissenschaft, um ein breites Spektrum von Fragen der Internet Governance zu erörtern und Ideen auszutauschen, wie z. B. Cybersicherheit, Datenschutz, Meinungsfreiheit und der Digital Divide. Das IGF verfolgt einen Bottom-up-Ansatz, d. h., es legt keine Strategien fest und trifft keine verbindlichen Entscheidungen, sondern fördert Diskussionen, den Austausch bewährter Best Practices und die Entwicklung freiwilliger Leitlinien.

Das IGF hat seit seiner Gründung jährliche Treffen abgehalten, wobei das erste Treffen 2006 in Athen, Griechenland, stattfand, das jüngste 2022 in Addis Abeba, Äthiopien. Die Treffen finden an verschiedenen Orten auf der ganzen Welt statt und ziehen ein breites Spektrum von Teilnehmern aus allen Regionen an. Zusätzlich zu den jährlichen Treffen unterstützt das IGF auch die Einrichtung nationaler und regionaler IGFs sowie die Organisation von Workshops und anderen Veranstaltungen, um den Dialog über Fragen der Internetverwaltung auf lokaler Ebene zu erleichtern.

Auch wenn die Deklaration kein Angriff auf Russland und China sein mag, so darf doch nicht vergessen werden, dass diese Staaten ihre Bevölkerungen von eben jenem offenen und freien Internet abkoppeln, beziehungsweise es zumindest versuchen. Damit sind sie Vorbild für andere, weniger repressive Regime. Daher gilt es für liberale Demokratien, Staaten, die zwischen dem autoritären und demokratischen Lager schwanken, davon zu überzeugen, dass ein offenes und freies Internet in ihrem besten Interesse wäre. Dazu gehören zum Beispiel Staaten wie Brasilien oder Nigeria, die durch ihren regionalen Einfluss auch erhebliches Potenzial bei der Sicherung des globalen freien und offenen Internets haben. Laut Freedom House sind es im Jahr 2022 demokratische Institutionen gewesen, die in diesen Swing States dafür sorgten, dass Regierungen das Recht auf Privatsphäre schützten und Vorhaben zur Kontrolle von Inhalten im Internet Einhalt geboten wurde (Shahbaz et al. 2022).

² Die Autorin hat sich an dieser Stelle erlaubt, die Fähigkeiten der zum Ende des Jahres 2022 breit diskutierten KI-Anwendung Chat GPT von Open AI auszutesten. Dieser Textabschnitt zum IGF wurde von dieser KI erstellt, mit DeepL übersetzt und mit Informationen ab dem Jahr 2021 von der Autorin ergänzt.

5. Der Pudding ist an der Wand: Autokratien und das Internet

Mit dem Beginn des neuen Jahrtausends wurde eine neue Ära eingeleitet. Das Internet wurde immer mehr zum Massenmedium, digitale Geschäftsmodelle begannen sich zu entwickeln. Für den damaligen US-Präsidenten Bill Clinton war das Internet auch ein Triumph für die Freiheit. Die freie Rede online einzuschränken, wie China es seit dem Ende der 1990er Jahre versuchte, hielt er für ein naives Bestreben. „Viel Glück“, witzelte er daher am 8. März 2000. Das sei, als versuche man Pudding an die Wand zu nageln (Allen-Ebrahimian 2016).

Nur wenige Jahre später ist der Pudding an der Wand. China ist mit seiner „Great Firewall“ Vorbild für autokratische Staaten, die ihre Bevölkerung ebenfalls von dem freien Zugang zu Informationen fernhalten und kontrollieren wollen, wie sich Menschen online äußern (Shahbaz 2018). Im Gegensatz zu anderen autokratischen Staaten wie Russland oder Iran hat China jedoch einen „First Mover Advantage“. Da sie bereits Ende der 90er Jahre mit der Abkopplung vom offenen, freien Internet begannen und ebenso frühzeitig chinesische Alternativplattformen zu den aufkommenden Plattformen des Westens – zum Beispiel Google, eBay, Twitter oder Facebook anboten – und diese auf die Bedürfnisse der riesigen chinesischen potenziellen Nutzerschaft abstimmen, kamen die Chinesinnen und Chinesen gar nicht erst in Versuchung, westliche Plattformen nutzen zu wollen. Denn mit Baidu (Suchmaschine), Sina Weibo (Micro-Blogging) und Alibaba (Shopping) waren frühzeitig chinesische Alternativen verfügbar. Russland hat zwar mit VKontakte frühzeitig eine russische Alternative zu Facebook bieten können, die Facebook selbst unattraktiv machte. Allerdings gab es erst sehr spät Versuche, weitere Alternativen zu etablieren, wie beispielsweise für YouTube, weswegen es dem Kreml bislang nicht gelungen ist, regimekritische Journalistinnen und Journalisten zu zensieren, die diese US-amerikanische Plattform nutzen, um die Menschen in Russland mit qualitativ hochwertigen Nachrichten zu versorgen (Soldatov/Borogan 2022).

Xi Jinping und Wladimir Putin haben in einem gemeinsamen Statement im Zuge der Olympischen Spiele im Februar 2022 erklärt, dass sie ihre Zusammenarbeit im Bereich der Digitalpolitik verstärken wollen. Sie wollen die „Internationalisierung“ der Internet Governance vorantreiben und sagen explizit, dass sie die Bedeutung der ITU stärken wollen – das heißt, weg vom konsensualen Multi-Stakeholder-Ansatz hin zu einer staatlich(eren) beziehungsweise zwischenstaatlichen Kontrolle der logischen Infrastrukturen des Internets.

Das Internet, schon durch seine dezentrale Konzeption darauf angelegt, dass Menschen möglichst ungehindert weltweit miteinander kommunizieren können, wird immer mehr zum Splinternet³ – ein Begriff, erstmals 2001 eingeführt von Clyde Wayne Crews (Crews 2001), vom Cato-Institute. Es sind zwar insbesondere autoritäre Regime, die versuchen, sich eigene, abgeschottete Internete zu bauen, um den Informationsfluss für ihre Bürgerinnen und Bürger zu kontrollieren. Doch auch liberale Demokratien sind nicht immun gegen solche Vorhaben – allerdings greifen hier bislang rechtsstaatliche Verfahren, die dem rechtzeitig entgegenwirken. Beispielhaft sei hier die Europäische Kommission und die Diskussionen zur EU-Copyright-Direktive (Stichwort: Uploadfilter) genannt (Renouard 2019). Das Internet, das aus vielen einzelnen Netzwerken besteht, verliert durch solche Bestrebungen seinen Charakter als globales, offenes und freies Netz der Netze. 2022 sank die Internetfreiheit weltweit das zwölfte Jahr in Folge (Shahbaz et al. 2022).

Zwar kann staatliche Internetzensur regelmäßig mit sogenannten Virtual Private Networks (VPN) umgangen werden, doch gehen Staaten immer mehr zu einem Verbot dieser über. Das iranische Regime setzt beispielsweise ein so ausgeklügeltes Überwachungssystem namens SIAM ein, mit dessen Hilfe bestimmte IP-Adressen mit bestimmten VPNs abgeglichen werden und so auf die Identität und den Standort des Nutzers Rückschlüsse gezogen werden können (Biddle/Hussain 2022). China hat es mit seiner enormen wirtschaftlichen Macht deutlich einfacher: Es hat beispielsweise Apple aufgefordert, die wichtigsten VPN Apps aus dem chinesischen AppStore zu verbannen. Der Tech-Konzern ist dieser Aufforderung gefolgt (Rydlink 2017; Shahbaz 2018).

³ Lesenswerte Kritik an der „Fragmentierung“ des Internets von Dr. Julia Pohle und Dr. Daniel Voelsen: <https://link.springer.com/article/10.1007/s11609-022-00478-6>

6. Kritische Infrastrukturen: Wo gefährliche Abhängigkeiten bestehen

6.1 Daten aus dem Meer: Unterseekabel

1858 verbanden mitten auf dem Atlantischen Ozean zwei Kriegsschiffe ein nur 1,5 cm dickes Kabel. Es sollte das erste Unterseekabel sein, das eine Telegraphenverbindung zwischen dem amerikanischen und dem europäischen Kontinent herstellte (Griffiths 2019). Im Jahr 2022 ist die Anzahl an Unterseekabeln auf 530 aktive oder geplante Kabel⁴ angewachsen (TeleGeography o. J.). Im Verlaufe der über 150 Jahre ist nicht nur die Anzahl dieser Kabel gewachsen, sondern auch die Menge an Informationen, die durch sie fließt. Das Internet wäre ohne sie kaum denkbar – schließlich laufen 95 Prozent des Datenverkehrs über die Unterseekabel (Mozilla 2019). Und doch war die Existenz und die Bedeutung dieser Kabel als Rückgrat für die globalisierte Wirtschaft und Gesellschaft, bisher wohl nur wenigen bewusst. Es mag einige überraschen, dass Daten nicht in Wolken schweben, sondern durch das Meer fließen.

Erst der vermutlich von Russland verübte Anschlag auf die Gas-Pipelines NordStream 1 und 2 in der Ostsee (Schürpf et al. 2022) und die darauf folgende Berichterstattung über Pipelines und Kabel, die über den Meeresboden verlaufen, zeigte der breiten Öffentlichkeit und auch politischen Entscheidungsträgern, welche Bedeutung diese als kritische Infrastruktur (KRITIS) zu bewertenden Kabel haben – und wie unzureichend sie und die Orte, an denen sie auf Land treffen, geschützt sind (McCann 2022).

Europa hängt von diesen Unterseekabeln ab – insbesondere den Transatlantischen. Eine große Menge an für Europa relevanten Daten wird in Datacentern in den USA gespeichert beziehungsweise Daten dort für bestimmte Dienstleistungen prozessiert. Diese Kabel und Datentransfers haben nicht nur eine enorme Bedeutung für den transatlantischen Handel, sondern auch für Regierungen. Sie benötigen sie zum Beispiel zur Regulierungsaufsicht, zur Aufklärung von Verbrechen und zum Schutz der nationalen Sicherheit (Cory/Dick 2021; Wall/Morcos 2021).

Diese KRITIS liegt immer stärker in der Hand der großen Tech-Unternehmen wie Amazon, Meta und Google (Burgees 2018; Mauldin 2017; TeleGeography o. J.). Auch China investiert im Rahmen der „Digitalen Seidenstraße“ (Belt and Road Initiative) in größer werdendem Ausmaß in Unterseekabel (Sherman 2021). Das jüngste Projekt, das sogenannte Peace-Kabel, verbindet auf einer Länge von 15.000 Kilometern Asien, Europa und Afrika miteinander. Umgesetzt wird das Projekt mit einer Investitionssumme von 425 Millionen Dollar; das chinesische Unternehmen Huawei ist unter anderem daran beteiligt (Herbling 2022).

Es ist die damit künftig kürzeste Strecke von Europa nach Asien, mit einer Kapazität von 16 Tbit/s pro Glasfaser (Schieb 2022). Zum Vergleich: die Europäische Kommission kofinanzierte durch das BELLA (Building Europe Link to Latin America) Programm das Unterseekabel „EllaLink“ mit 25 Millionen Euro, das auf einer Länge von 6.000 Kilometern Europa direkt mit Lateinamerika verbindet, ohne einen Umweg über Nordamerika machen zu müssen und damit deutliche schnellere Datenübertragungen ermöglicht (bisherige Kabel sind veraltet und werden nur zur Sprach-Übertragung genutzt) (EMOLCP 2021; Europäische Kommission 2015). Allerdings ist die Datenübertragung bei EllaLink schneller als das Peace Kabel. Daten werden hier mit einer Geschwindigkeit von 25 Tbit/s pro Glasfaser transportiert (EllaLink 2022).



Quelle: <http://www.peacecable.net>, Stand: Februar 2023

Neben den Abhängigkeiten von chinesischen und amerikanischen Unternehmen besteht zudem das Risiko der Datenspionage durch Geheimdienste. Der KRITIS-Experte Manuel Atug weist darauf hin, dass es diese Praxis der Spionage schon seit Jahrzehnten gibt. Dazu werden spezielle Unterwasser-Drohnen, Spionage-U-Boote, Tiefseeroboter und auch Schiffe verwendet. Mit solchen Unterwasserwerkzeugen können Datenkabel gezielt sabotiert werden. Zwar ist das Internet darauf angelegt, dass es sich beim Ausfall einer Datenroute eine neue sucht und so eigentlich unzerstörbar ist. Dies ist aber eben nur solange möglich, wie es alternative Datenrouten gibt. Gegebenenfalls kann es auf den noch bestehenden zu Überlastungen oder Problemen im Hochfrequenzbereich kommen (Schieb 2022).

Es gibt bereits Geräte zur Kontrolle solcher Unterseekabel – auch in diesem Fall zum Beispiel Unterwasser-Drohnen oder Sensoren –, um diese so vor Sabotageakten zu schützen. Ein Bericht, der vom Europäischen Parlament beauftragt und im Juni 2022 veröffentlicht wurde, legt allerdings dar, dass keine der europäischen Agenturen, wie zum Beispiel Frontex, das

⁴ <https://www.submarinecablemap.com/> bietet für Interessierte eine interaktive Karte

Mandat haben, Aktivitäten an den Kabeln zu überwachen. Auch die Reparaturkapazitäten für beschädigte Kabel müssten verbessert werden, so der Bericht (Bueger et al. 2022; Kabelka 2022).

6.2 Politisiert: Normen und Standards⁵

Wer Normen und Standards setzt, beherrscht den Markt. Diese Erkenntnis hatte schon Werner von Siemens im 19. Jahrhundert (Delhaes/Hoppe 2021). Viele Normen und Standards, die sich durchgesetzt haben, kennt man aus dem Alltag: das DIN-A4-Papier, den USB-Anschluss und mittlerweile auch die FFP2-Maske. Standards geben unter anderem bestimmte Qualitätsmerkmale vor. Dass Standards nicht immer international gültig sind, merkt der Reisende häufig dann, wenn er für seine technischen Geräte Adapter benötigt, um die örtlichen Steckdosen benutzen zu können. Für den Welthandel ist das Verständnis auf einen gemeinsamen Standard eine wichtige Voraussetzung. Sie betrifft den Überseecontainer genauso wie die in ihm befindlichen W-LAN-Router, die verschifft werden. Normen und Standards bilden einen Pfeiler der globalen Arbeitsteilung.

In Deutschland entwickelt das Deutsche Institut für Normung (DIN), ein Verein, Normen und Standards. Sie werden dort gemeinsam von Verbraucherinnen und Verbrauchern, Wirtschaft und Wissenschaft entwickelt. In Deutschland sind aber nur noch 20 Prozent geltende Normen nationale Normen. Die restlichen 80 Prozent sind europäische und internationale – festgelegt unter anderem von der Internationalen Organisation für Normung (ISO). Im Bereich dieser internationalen Standardsetzung dominieren die Europäer, obwohl sie eigentlich gar nicht die entsprechende ökonomische Macht haben. Allerdings überzeugt die europäische Art und Weise der Festlegung der Standards: Sie setzt auf Harmonisierung und bindet nationale Interessen und die verschiedensten Stakeholder mit ein. Damit ist sie ein wichtiges Instrument für den einheitlichen Binnenmarkt und hat so auch bei der internationalen Standardsetzung ein hohes Gewicht. Die USA hingegen setzen bei der technischen Standardisierung stärker auf den Wettbewerb, was dazu führen kann, dass für ein und dasselbe Produkt in verschiedenen Bundesstaaten diverse Standards gelten (Dohmen 2022).

Die Fraunhofer-Gesellschaft warnt in einem Positionspapier vor der Instrumentalisierung von Normen und Standards in der Handelspolitik und erwähnt explizit Chinas Versuch, Abhängigkeiten von Technologie in strategisch wichtigen Branchen zu schaffen. Sie verweisen neben chinesischen Bemühungen im Bereich von Standards in der Halbleiterindustrie auch auf Huawei. Das Unternehmen ist weltweit führend bei 5G-relevanten Patenten. Europa drohe der Verlust jeglicher Kontrolle über diese Telekommunikationstechnologie. Aber auch US-amerikanische Unternehmen wie Microsoft und Intel haben sich als de-facto-standardisierende Unternehmen durchgesetzt. Technisch überlegene Lösungen, die von den beiden Unternehmen aber nicht anerkannt werden, hätten keine Möglich-

keit sich dennoch durchzusetzen. Im Bereich der Künstlichen Intelligenz und Internet-Technologien trifft dies, so die Autoren, analog auf Facebook und Google zu (Buhl/Schönhof 2021).

In China werden Normen und Standards nicht wie in liberalen Demokratien entwickelt, sondern werden als Teil der Industriepolitik und nationalen Wirtschaftsentwicklung durch die Kommunistische Partei genutzt. China verbreitet seine technischen Standards über seine Belt and Road-Initiative auch in anderen Teilen der Welt und erzeugt damit unter anderem sogenannte Lock-In-Effekte, die eine Abhängigkeit von entsprechenden Lieferanten bedeuten. In Normen und Standards können gerade im Technologiebereich Wertvorstellungen festgeschrieben werden. Anfang der 2000er Jahre versuchte China beispielsweise WAPI als Alternative zu Wi-Fi-Standard durchzusetzen – unter anderem mit dem Argument der besseren Leistungsfähigkeit. WAPI schützt allerdings die Privatsphäre der Nutzerinnen und Nutzer deutlich schlechter (Dohmen 2022).

In den wichtigsten Standardisierungsgremien verfügt China über erheblichen Einfluss. Dieser verdeutlicht sich unter anderem an den zahlreichen Führungspositionen, die China einnimmt. In den letzten drei Jahren führen oder führten Chinesen die drei größten internationalen Standardisierungsorganisationen: neben der ISO und der ITU auch das Elektrotechnische Komitee. Der Einfluss Chinas in der ITU ist deutlich größer als in den beiden anderen Organisationen. „In der von 2022 bis 2024 währende Studienperiode besetzt China eine von elf Positionen der Vorsitzenden von Studiengruppen. Nur Japan und Südkorea haben mehr Vorsitze erhalten (jeweils zwei). Von den in wesentlich höherer Anzahl vorhandenen stellvertretenden Vorsitzen der Studiengruppen sicherte sich China 8,7 % und liegt damit an erster Stelle vor Südkorea (7,7 %), Argentinien, Japan und Indien (jeweils 5,8 %)“ (Rühlig 2022: 9).

Internationale Fernmeldeunion (ITU)

Die ITU, die Internationale Fernmeldeunion, ist eine Organisation der Vereinten Nationen, die sich mit Informations- und Kommunikationstechnologien beschäftigt. Sie wurde bereits 1865 gegründet. Ihr Sitz ist in Genf, Schweiz. Die ITU agiert im Namen ihrer 191 Mitgliedsstaaten. Alle vier Jahre gibt sie sich in Wahlen ein neues Führungsgremium, darunter einen Generalsekretär und dessen Stellvertretung, sowie drei Direktoren für die drei Sektoren der ITU: ITU-D (Sektor für Telekommunikationsentwicklung), ITU-R (Sektor Funkkommunikation) und ITU-T (Sektor Telekommunikationsnormung) (ITU 2022a, o. J.). Beschlüsse werden in den einzelnen Gremien der ITU per Konsens gefasst. Was Konsens bei der ITU ist, darüber gibt es kein Konsens. Wann Konsens erreicht ist, entscheidet der jeweilige Vorsitz (Scholl 2022). Die Probleme der müßigen Konsensfindung sind bekannt. Künftig sollen Wege eingeschlagen werden, um agiler zu oftmals auch besseren Ergebnissen zu kommen. Dazu könnten die Ergebnisse anderer Standardisierungsorganisationen übernommen werden (Scott 2022). China stellte in der Wahlperiode, die mit dem Jahr 2022 endet, den Generalsekretär der ITU. Im September 2022 wurde ein neues Führungsgremium für die Amtszeit von 2023 bis 2027 gewählt. Bei den Wahlen unterlag der russische Kandidat der US-Amerikanerin, Doreen Bogdan-Martin (Economist 2022; ITU 2022b).

⁵ Zur tiefergehenden Lektüre zu Chinas wachsendem Einfluss bei der Standardsetzung wird die Publikation „Chinas unsichtbare Macht technischer Standards“ von Dr. Tim Rühlig empfohlen: <https://shop.freiheit.org/#/Publikation/1333>

Chinas wachsenden Einfluss in diesem Standardisierungs-gremium sieht man aber auch an den Führungspositionen in nachgeordneten Arbeitsgruppen. Die chinesische Regierung beziehungsweise die Kommunistische Partei Chinas geht strategisch im Bereich der globalen Standardsetzung vor. Diesem parteistaatszentrierten Vorgehen steht das System von öffentlich-privater Partnerschaft aus Europa gegenüber, bei dem der Privatsektor weitgehend freie Hand bei der Entwicklung von Standards gelassen wird. Standardsetzung ist zu selten auf der (strategischen) politischen Agenda, insbesondere von Deutschland (Rühlig 2022). Dies wird auch durch die Stärke der Delegationen bei der Bevollmächtigtenkonferenz der ITU (Plenipotentiary Conference) deutlich, bei der die Delegation Deutschlands zu den kleineren gehört.

Auch bei der Struktur des Internets an sich, also den Protokollen, auf denen das Internet aufbaut, bemüht sich China seine Standards und damit Wertvorstellungen durchzusetzen. China nutzt die UN-Institution ITU, in der Regierungen eine tragende Rolle spielen, um gleichgesinnte und abhängige Staaten auf ihre Seite zu ziehen und ihren Vorschlag eines neuen Internet-Protokolls namens „NewIP“ durchzusetzen. Es wird befürchtet, dass damit die Filterung und Überwachung des Internets nach chinesischen Vorbild möglich wird (Krempf 2022b). Zwar scheint die Debatte um NewIP etwas überhitzt und sie wohl noch weit davon entfernt, eine echte Alternative darzustellen. Dennoch sollte man Chinas Gestaltungsanspruch beim globalen Internet durchaus ernst nehmen (Splett 2020). Die Europäische Kommission hat daher eine Normungsstrategie vorgelegt und beansprucht Europas Führungsrolle in diesem Bereich (Krempf 2022a).

6.3 Die kritischste Technologie der Welt: Chips

„When we think of Silicon Valley today, our minds conjure social networks and software companies rather than the material after which the valley was named. Yet, the internet, the cloud, social media, and the entire digital world only exist because engineers have learned to control the most minute movement of electrons as the race across slabs of silicon. ‘Big Tech’ wouldn’t exist if the cost of processing and remembering 1s and 0s hadn’t fallen by billionfold in the past half century.“ (Miller 2022: xxi). Lediglich drei Nanometer sind die Abstände der Transistoren auf den Chips der jüngsten Generation groß⁶, die der taiwanesischen Chip-Hersteller TSMC seit 2022 produzieren kann. Zum Vergleich: Das Corona-Virus würde mit seiner Größe von 80 bis 140 Nanometer schon lange nicht mehr in diese Zwischenräume passen. Chips sind nicht nur das am meisten produzierte Gut der Welt, es ist auch kaum noch ein Produkt ohne sie denkbar (Miller 2022: xxi). Vom Auto, über den Kühlschrank, das Smartphone, der Reisepass oder die neusten Waffengattungen: alles braucht heutzutage Chips.

Die Wertschöpfungskette von Chips ist eine der am stärksten globalisierten aller Branchen (Lee/Kleinhaus 2021). Im ersten Jahr der globalen Corona-Pandemie sind die Abhängigkeiten von Chips jedem bewusst geworden, der Nachrichten konsumiert, oder ein Produkt kaufen wollte, das wegen der gestörten Lieferketten nicht mehr erhältlich war. Dazu gehörten nicht nur Autos, sondern auch Spielekonsolen – die allerdings nicht wegen fehlender Chips ausgeliefert werden konnten, sondern wegen fehlender Isolierfolien für die Trägerplatten der Chips. Diese Folien werden von nur einem Hersteller auf der ganzen Welt hergestellt. Er sitzt in Japan. Der Chip-Mangel entstand vor allem dadurch, dass Autohersteller ihre Bestellungen stornierten, da sie durch die Pandemie davon ausgingen, dass die Anzahl der Autoverkäufe drastisch zurückgehen würde. Die Chip-Hersteller disponierten daher auch wegen der erhöhten Nachfrage nach Unterhaltungselektronik um. Deren Nachfrage stieg zu Beginn der Pandemie – ebenso wie die nach Laptops – drastisch an. Auch, um diese Bedarfe decken zu können, kauften die Hersteller dieser Produkte die globalen Chip-Vorräte auf. Nicht zu unterschätzen war zusätzlich der Einfluss von Naturkatastrophen oder Bränden auf Fabriken, die einzelne Komponenten in der Produktionskette herstellen, die dadurch nicht mehr produzieren konnten. Verschärft wurde die Chip-Krise außerdem durch Sanktionen, die der damalige US-Präsident Donald Trump gegenüber China verhängte, um den Einfluss chinesischer Tech-Konzerne einzuschränken. Chinesische Unternehmen kauften daraufhin im großen Stil noch verfügbare Chips und Herstellungsanlagen ein (Wirtschaftswoche 2022).

Die Sanktionen wiederum wurden von Trumps Nachfolger Joe Biden nochmals verschärft. Kurz vor dem 20. Parteitag der Kommunistischen Partei Chinas im Herbst 2022 verhängten die USA Exportbeschränkungen für Halbleiterfertigungstechnik und erließen Maßnahmen gegen chinesische Chip-Hersteller. Von den Sanktionen sind nicht nur amerikanische Firmen betroffen, sondern auch europäische und asiatische Zulieferer. Diese müssen sicherstellen, dass ihre Produkte nicht doch in China landen. Die Sanktionen zielen vor allem darauf ab, dass China nicht die Fähigkeit erlangt, die modernsten und damit leistungsfähigsten Chips selber zu bauen, die vor allem für anspruchsvolle KI-Leistungen, Supercomputer, aber auch die Entwicklung von Waffen benötigt werden. Langfristig werden die Sanktionen wohl dafür sorgen, dass selbst ältere Fertigungstechniken nicht mehr reibungsfrei in China eingesetzt werden können – auch, wenn es die Möglichkeit für Ausnahmeregelungen für diesen Bereich gibt. Die Sanktionen gehen sogar so weit, dass es US-Staatsbürgerinnen und -bürgern, oder Menschen mit einer Arbeitsgenehmigung für die USA untersagt ist, für chinesische Firmen zu arbeiten, die unter das Sanktionsregime fallen (Windeck 2022).

Die starke Globalisierung der Wertschöpfungskette der Chips hat auch mit dem enormen wirtschaftlichen Druck und dem Druck zur Innovation zu tun. Verschiedene Regionen der Welt haben sich auf bestimmte Produktionsschritte spezialisiert. So sind zahlreiche zwischenstaatliche Abhängigkeiten ent-

⁶ Je kleiner der Abstand, desto schneller sowie effizienter können Informationen in Form von Elektronen ausgetauscht werden. Je kleiner also die nm-Zahl, desto mehr Transistoren pro Fläche und weniger Ressourcenverbrauch pro Rechenaufwand sind möglich.

standen. Das Design der Chips wird häufig in den USA entwickelt. Die Chips selbst dann in Taiwan, mit Chemikalien aus Japan und Deutschland und Instrumenten aus den Niederlanden produziert und in China montiert und verpackt. Teilweise werden diese Produktionsschritte von wenigen Unternehmen kontrolliert. Bestimmte Vorleistungen in der Chip-Produktion sind gar monopolisiert – können also, wie oben bereits am Beispiel bestimmter Folien erwähnt, nur von einem einzigen Unternehmen getätigt werden. Keine Region oder Nation der Welt ist in der Lage, alle notwendigen Produktionsschritte selbst durchzuführen (Kleinhans/Hess 2021; Lee/Kleinhans 2021).

Durch diese Abhängigkeiten erhält der taiwanische Chip-Hersteller TSMC regelmäßig besondere Aufmerksamkeit. Er ist das technologisch fortschrittlichste Unternehmen und wird diesen Vorsprung wahrscheinlich bis 2027 halten. Die einzigen echten Konkurrenten sind Samsung und Intel. Auch der Marktanteil von TSMC übertrifft die Konkurrenz: mit 55 Prozent ist er dreimal so groß wie Samsung, das auf Platz zwei liegt. Selbst die chinesische Produktion hängt von dem Unternehmen aus Taiwan ab. TSMC gilt daher als „Siliziumschild“ Taiwans, da die Gefahr einer Zerstörung der Produktionsanlagen auch für China enorme wirtschaftliche Folgen hätte. Man vermutet, dass China aus diesem Grund bislang darauf verzichtet hat, Taiwan anzugreifen. China plant bis 2025 70 Prozent des eigenen Chipbedarfs selbst bedienen zu können. Experten hielten dies allerdings bereits 2021 für unwahrscheinlich. Die verschärften amerikanischen Sanktionen aus dem Jahr 2022 werden das chinesische Ziel vermutlich noch weiter hinauszögern (Rother 2021).

Sowohl die USA als auch die Europäische Union versuchen seit geraumer Zeit eigene Chip-Produktionen aufzubauen. So plant der Hersteller Intel beispielsweise die Errichtung einer Fabrik in der Hauptstadt Sachsen-Anhalts, Magdeburg. 17 Milliarden Euro wird der Bau von zwei Werken kosten (tagesschau.de 2022). Der Bund unterstützt die Ansiedelung mit 6,8 Milliarden Euro aus dem Bundeshaushalt (Sauter 2022a). Die Vereinigten Staaten unterstützen mit einem Chips Act und einer darin enthaltenen Investitionssumme von 52 Milliarden Dollar die Errichtung von Produktionsstätten in den USA (Sauter 2022b). Auch die Europäische Union plant einen eigenen Chips Act, der im Jahr 2023 vom Europäischen Parlament verabschiedet werden soll. Mit dem Gesetz soll dem Mangel an Chips entgegengewirkt werden und der weltweite Marktanteil bis 2030 von 10 Prozent auf mindestens 20 Prozent verdoppelt werden. Dies soll zugleich ein Beitrag für die technologische Souveränität der EU sein. Mit dem Chips Act sollen 43 Milliarden Euro an öffentlichen und privaten Investitionen mobilisiert werden (Mantel 2022; Rat der Europäischen Union 2022). Doch auch wenn es Bemühungen gibt, die Produktion und die Produktionsstätten zu diversifizieren und es zudem gelingen sollte, technologische Defizite in den kommenden Jahren aufzuholen, bestehen weiterhin gefährliche Abhängigkeiten bei den für die Herstellung notwendigen Rohstoffe wie Silizium, Gallium oder Germanium (Röhrlich 2022).

7. Neue politische Akteure: Private Unternehmen in der Internationalen Digitalpolitik

Es ist nicht ungewöhnlich und auch nicht neu, dass Unternehmen in der internationalen Politik beziehungsweise der Geopolitik eine Rolle spielen. Bekanntestes Beispiel ist wohl die East India Company. Seit dem 18. Jahrhundert war sie nicht nur ein monopolistisches Handelsunternehmen, sondern vertrat auch die politischen Belange für das britische Empire (Bremmer 2022; Britannica 2022). Zudem wurde der East India Company die britische Militärmacht übertragen, die sie mittels Privatarmeen auf dem indischen Subkontinent ausübte (National Army Museum o. J.). Doch diese übertragene politische und militärische Macht wären, so der Politikwissenschaftler Ian Bremmer, nicht vergleichbar mit der tiefgreifenden globalen Macht, die heutige Technologieunternehmen haben. Es sei eine Sache, so Bremmer, ob in „verrauchten Zimmern“ politische Macht ausgeübt werde, oder ob durch die Unternehmen und ihre Produkte direkt Lebensgrundlagen, Beziehungen, Sicherheit und sogar Denkmuster von Milliarden an Menschen beeinflusst werden. Auch hatten Unternehmen schon immer eine Rolle in der Bereitstellung von elementaren Gütern für eine Gesellschaft, wie beispielsweise Medikamente oder die Stromversorgung.

Selbst im Bereich der nationalen Sicherheit ist es selbstverständlich, dass Rüstungsgüter von privatwirtschaftlichen Unternehmen eingekauft werden. Der Unterschied ist aber, dass es heute zum Beispiel lediglich vier Konzerne gibt – Alibaba, Amazon, Google und Microsoft –, die den Großteil der weltweit benötigten Cloud-Kapazitäten zur Verfügung stellen, die die Grundlage für Leistungen für Wirtschaft, Staat und Gesellschaft sind (Bremmer 2022). Die Macht und der Einfluss privater Akteure muss daher gerade im Blick auf den digitalen Raum und ihre dortige Rolle kritisch analysiert und ein Umgang mit ihnen gefunden werden. Auch wegen des oben bereits dargestellten veränderten Blicks auf die internationalen Beziehungen – weg von der „Schachbrett“-Betrachtung hin zu einer Analyse von Netzwerken. „In the web world, they [non-state actors] are foreign policy actors, full stop“, resultiert Slaughter. (Slaughter 2018: 23)

7.1 Internet aus dem Weltall: Elon Musks Starlink⁷

„@elonmusk, while you try to colonize Mars – Russia try to occupy Ukraine! While your rockets successfully land from space – Russian rockets attack Ukrainian civil people! We ask you to provide Ukraine with Starlink stations and to address sane Russians to stand.“ twitterte der ukrainische Digitalmi-

nister Mykhailo Fedorov am 26. Februar 2022 (Fedorov 2022). Zehn Stunden später antwortete der Unternehmer Elon Musk dem Minister, dass Starlink in der Ukraine nun aktiviert und entsprechende Terminals in das Land unterwegs seien.

Stabile Kommunikationskanäle, auch über das Internet, sind in Kriegs- und Krisenregionen von besonderer Bedeutung. Nicht nur für Zivilisten, sondern auch für die Regierung und das Militär. Mykhailo Fedorov handelte daher in weiser Voraussicht, als er Elon Musk um Zugang zum Internet über dessen Satellitenkonstellation bat. Der Aggressor Russland sorgte nach seinem völkerrechtswidrigen Überfall auf die Ukraine in besetzten Gebieten, wie zum Beispiel in Cherson, schnell dafür, dass der Internetverkehr über russische Provider läuft und damit die Hoheit und Kontrolle über die Kommunikation erlangt wurde. Zugriffe auf soziale Medien und die freie Presse konnten so unterbunden werden (Satariano 2022; Shahbaz et al. 2022)

Starlink ist ein vom Raumfahrtunternehmen SpaceX betriebenes Satellitennetzwerk mit über 3.000 LEO-Satelliten. CEO ist der Milliardär Elon Musk. Genehmigungen und Pläne, weitere Satelliten in fünfstelliger Höhe in den Orbit zu schicken, liegen dem Unternehmen beziehungsweise den Behörden vor (Foust 2022). LEO-Satelliten sind Satelliten, die sehr nah an der Erde sind (Low Earth Orbit). Sie sind von ihr aus zu sehen. Im Unterschied dazu gibt es GEO-Satelliten (Geostationary Earth Orbit). Diese sind deutlich weiter von der Erde entfernt und eignen sich eher nicht für das Herstellen einer Internetverbindung. Internet aus dem Weltall ist beispielsweise für ländliche Regionen gedacht, die ansonsten keinen Zugang zu schnellem Internet haben – oder für den Krisen- und Katastrophenfall. Um eine Verbindung zum Internet über Satelliten aufzubauen, sind Terminals notwendig, also kleine Empfangsgeräte (Crist 2022; Voelsen 2021).

Dass Kommunikationsinfrastrukturen von privaten Unternehmen betrieben werden, ist weder neu noch ungewöhnlich. Staaten neigen dazu die jeweiligen nationalen Wirtschaftsakteure als Erweiterung beziehungsweise Verlängerung ihrer Macht zu sehen. Problematisch wird es allerdings, wenn erhebliche Machtkonzentrationen, also Oligo- oder Monopole entstehen und Betreiber diese Machtposition ausnutzen. Dass gerade der Unternehmer Musk dazu neigt, sieht man nicht nur anhand seiner Entscheidungen nach der Übernahme des Kurznachrichtendienstes Twitter ab Herbst 2022. Auch bei der zur Verfügungsstellung von Starlink – die Kosten von mehreren Millionen Dollar übernahmen die USA, das Vereinigte Königreich und Polen; die US Agency for International

⁷ Zur tiefergehenden Lektüre wird die Publikation „Internet aus dem Weltall“ von Dr. Daniel Voelsen empfohlen: <https://www.swp-berlin.org/publikation/satelliten-internet#hd-d18627e293>

Development (USAID) kaufte Terminals für 3 Millionen Dollar – zeigte sich Musks erratische und teils problematische Einstellung. Als das Internet über Starlink ausfiel und so zu katastrophalen Kommunikationsverlusten beim ukrainischen Militär führte, fürchteten ukrainische Militärbeamte eine geheime Vereinbarung zwischen Musk und Wladimir Putin. Das lag unter anderem daran, dass Musk zuvor mit Tweets zur Zukunft der Krim auf sich aufmerksam machte, bei denen vermutet wurde, er mache sich zum Sprachrohr Putins (Iyengar 2022; Tett 2022; Trappe 2022).

Das Weltall mag unendlich weit klingen, aber viel Platz ist dort nicht. Insbesondere nicht für Satelliten. Bislang sind es wenige Unternehmen – vor allem amerikanische und chinesische –, die Konstellationen aufbauen und betreiben. Zögerliches Handeln kann hier zum deutlichen Nachteil werden – insbesondere bei der digitalen Souveränität Europas. Das Weltall hat bereits seit 1967 durch das Weltraumrecht als Teil des Völkerrechts einen rechtlichen Rahmen. Der „Weltraumvertrag“ wurde von 107 Staaten ratifiziert (Voelsen 2021). Er bietet allerdings keine Antworten auf Abhängigkeiten oder den Umgang mit privaten Betreibern.

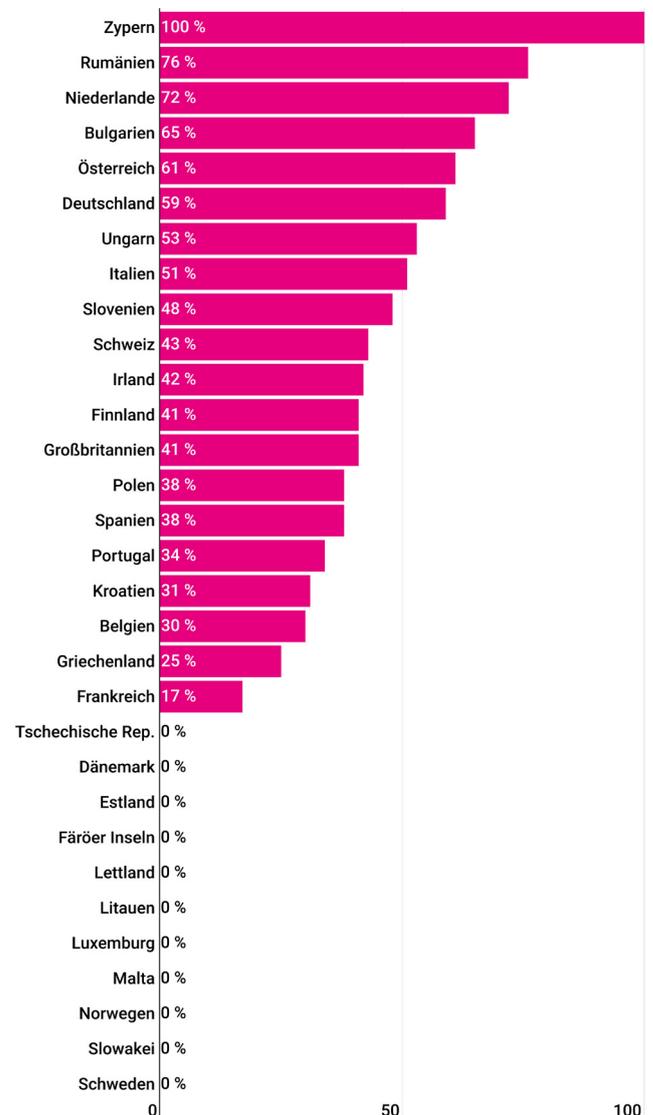
7.2 Der Hauptausstatter der chinesischen digitalen Seidenstraße: Huawei

Am 26. Januar 2018 berichtete die Zeitung Le Monde Afrique, dass das Hauptquartier der Afrikanischen Union (AU) in Addis Abeba, Äthiopien, gehackt wurde. Aus dem Hauptquartier, in dem sich regelmäßig die afrikanischen Staatsoberhäupter und Regierungschefs treffen, sollen fünf Jahre lang Daten direkt nach Peking abgefließen und dort auf Servern gespeichert worden sein. Bemerkte wurde es von einem Informatiker der AU ein Jahr vor der Berichterstattung, da die Datenübertragungen regelmäßig zwischen Mitternacht und zwei Uhr morgens Spitzenwerte erreichten – obwohl die Büros leer waren (Kadiri/Tilouine 2018).

Der Neubau, in dem die AU sitzt, wurde mit 200 Millionen Dollar komplett von China finanziert. Chinesische Staatsunternehmen führten den Bau aus; mit Equipment von Huawei (und in kleinen Teilen vom chinesischen Anbieter ZTE) wurde die gesamte IT-Infrastruktur des Hauptquartiers aufgebaut. Die Telekommunikationsinfrastrukturen in afrikanischen Staaten sind generell vornehmlich mit Technik von Huawei aufgebaut (Aglionby et al. 2018). Doch Huawei wird nicht nur in Afrika verbaut. Auch in vielen westlichen Ländern, insbesondere in Ländern der EU, wird Huawei zum Ausbau des 5G-Netzes eingesetzt. Teilweise ist dies kritische Infrastruktur. Deutschland gilt als ein Hotspot für den Einsatz von Huawei – schließlich geht Chinas Seidenstraße bis nach Duisburg. Dort sollte mithilfe des Unternehmens eine Smart City entstehen. Im November 2022 wurde die 2017 eingegangene Kooperation allerdings auf Eis gelegt, aber nicht beendet (Cerulus 2022; Heide/Verfürden 2022).

In Deutschland kommen sowohl Politik als auch Telekommunikationsanbieter immer mehr zu der Erkenntnis, dass das chinesische Unternehmen kein vertrauenswürdiger Anbieter ist und tauschen teilweise entsprechende technische Komponenten im 5G-Netz aus. Dazu beigetragen hat auch das IT-Sicherheitsgesetz 2.0, das im Jahr 2021 verabschiedet wurde (Alvares de Souza Soares et al. 2022; Beuth 2021). Gegen Huawei gibt es seit 2019 zwar weitreichende Sanktionen der USA, da diese Huawei enge Verbindungen zu chinesischen Behörden, Spionage und Sabotage unterstellen, dem Umsatz des Unternehmens hat dies aber nur kurz geschadet. Nach einem Einbruch ist der chinesische Konzern nach eigenen Angaben wieder auf Normalbetrieb und hat im Jahr 2022 86 Milliarden Euro Umsatz gemacht (Knaack 2022).

Anteil von Huawei in europäischen 5G Netzwerken



Stand: 2022

Quelle: Strand Consult / Erika Di Benedetto (POLITICO)

Huawei ist der weltweit größte Anbieter von Telekommunikationsausrüstung. 2017 überholte das Unternehmen Apple als größten Hersteller von Smartphones. Er ist das chinesische Schlüsselunternehmen, das die Regierung, beziehungsweise die Kommunistische Partei, zur Umsetzung ihrer digitalen Seitenstraße (Belt and Road Initiative) einsetzt. Die China- und Technologieexpertin Elsa Kania sagt daher, dass es schwierig sein könne, das Streben von Huawei nach kommerziellen Vorteilen von Chinas Verfolgung strategischer Ziele zu unterscheiden. In Zukunft könne der entscheidende Marktanteil und die potenzielle weltweite Dominanz von Huawei genutzt werden, um sowohl Unternehmens- als auch nationale Regierungsinteressen voranzutreiben (Kania 2018a). Es sei klar, dass „Huawei's global expansion, in and of itself, can serve as a vector for Beijing's influence.“ (Kania 2018b). Auch die China-Experten Clive Hamilton und Mareike Ohlberg analysieren in ihrem Buch „Die lautlose Eroberung“, wie das Unternehmen nicht nur chinesischen Geheimdiensten nahesteht, sondern auch gezielt versucht, Einfluss in westlichen Regierungen beziehungsweise bei Regierungsvertretern und Spitzenpolitikerinnen zu erlangen. Beide konstatieren, dass „Huawei [...] ein Angelpunkt für Präsident Xis zwei Fusionen [ist]: der Fusion der Partei mit der Unternehmenswelt und der zivil-militärischen Integration. Wir könnten eine dritte hinzufügen, nämlich die Fusion von Einflussnahme und Spionage“ (Hamilton/Ohlberg 2021: 239–240).

7.3 Was darf aufs Smartphone? Google und Apple als Gatekeeper

Wer als App-Entwickler tätig ist, muss Apps so entwickeln, dass sie den Vorgaben von Google und Apple für ihre jeweiligen App-Stores entsprechen. Er hat auch keine Möglichkeiten, mit den beiden Unternehmen zu verhandeln – was zum Beispiel die Marge betrifft, die der jeweilige App-Store beim Verkauf einer App oder eines Abonnements einbehält. Apples AppStore und Googles PlayStore sind proprietäre Märkte. Sie bilden ein Duopol (Staab 2019: 171). Der Spielehersteller Epic Games, bekannt für das Spiel Fortnite, verklagte in den USA Apple wegen dieser marktbeherrschenden Stellung. Epic war nicht mehr bereit, 30 Prozent des Kaufpreises pro verkaufter App über Apples AppStore an das Unternehmen abzutreten und wollte erreichen, dass es auf dem iPhone seinen eigenen App-Store anbieten kann. Dem kam das Gericht zwar nicht nach, verpflichtete Apple aber dazu, die Regeln des AppStores so zu ändern, dass Anbieter in ihren Apps auf günstigere Zahlungsweisen hinweisen dürfen, die den AppStore als Zwischenhändler umgehen.

Politik und Wettbewerbsbehörden – sowohl in den USA als auch in Europa – üben immer mehr Druck auf Apple und Google und ihre marktbeherrschende Stellung aus. Mit dem in der EU 2022 verabschiedeten Digital Markets Act (DMA), der ab Mai 2023 anwendbar ist, liegt für die EU bereits ein Gesetz vor, das mehr Wettbewerb ermöglicht. Im Dezember

2022 wurde bekannt, dass sich Apple darauf vorbereitet, weitere App-Stores für seine Geräte zuzulassen (Europäische Kommission o. J.; Herbig/Wölbart 2021; Krempel 2022c; Muth 2021; Schwan 2022).

Apple und Google üben ihre Gatekeeper-Funktion auch bei den Inhalten der Apps aus, die auf ihren Plattformen angeboten werden können. Durch ihre Regeln entscheiden sie zum Beispiel, welche Inhalte angemessen sind und welche nicht. Wie oben bereits erwähnt, hat sich Apple der chinesischen Regierung gebeugt und VPN-Apps aus dem AppStore für den chinesischen Markt entfernt, sodass Chinesinnen und Chinesen nicht mehr das Netz außerhalb der chinesischen Firewall besuchen konnten. Gleiches gilt für generelle Inhalte, die Apple für nicht angemessen hält. Pornografie gehört zu den unangemessenen Inhalten. Die Blogging-Plattform Tumblr beispielsweise, früher bekannt für ihre erotischen und pornografischen Inhalte, insbesondere aus der LGBTQI-Community, hat Nacktheit nun von ihrer Plattform entfernt. Als Grund wird vermutet, dass man wieder in Apple AppStore verfügbar sein möchte. Aus dem flog die Tumblr-App heraus, da auf der Plattform Darstellungen von Kindesmissbrauch nicht durch die hauseigene Software gefiltert wurden und Apple solche Inhalte (zu Recht) nicht duldet. Um die Chancen auf eine Rückkehr in den AppStore zu erhöhen, soll daher „adult content“ nicht mehr gestattet werden – auch wenn dieser in keiner Weise etwas mit illegalen Darstellungen von Kindesmissbrauch zu tun hat (Beuth 2018).

Erotik und Pornografie mag als Randphänomen gesehen werden, jedoch zeigt sich an diesem Beispiel, wie Plattformanbieter ihre Gatekeeper-Funktion ausüben können und darüber entscheiden, welche Inhalte verfügbar sein dürfen und welche nicht. Wohlgemerkt ist Pornografie in den meisten Staaten nicht illegal. Dass beim Zugriff Regeln des Kinder- und Jugendschutzes eingehalten werden müssen, eine Selbstverständlichkeit (Riedel 2021). Dass auch nicht-erotische Nacktheit gelöscht wird, weil Ansichten oder elektronische Filter anders interpretiert werden, zeigt auch das Spiel „Papers, Please“, das 2014 vom AppStore abgelehnt wurde. In dem Spiel geht es darum, Einreisende an der Grenze zu kontrollieren. Dabei kommt auch ein „Nacktschanner“ zum Einsatz, den die Entwickler wieder entfernen mussten, um im AppStore gelistet werden zu können (derstandard.at 2014). Wie sehr die App-Stores Einfluss auf Inhalte der bei ihnen angebotenen Apps nehmen, beschreibt auch der ehemalige Head of Trust and Safety von Twitter, Yoel Roth, nach seinem Weggang vom Unternehmen in einem Meinungsbeitrag im Herbst 2022 für die New York Times: „There is one more source of power on the web – one that most people don't think much about but may be the most significant check on unrestrained speech on the mainstream internet: the app stores operated by Google and Apple.“ (Roth 2022)

Die Gatekeeper-Funktion hat auch politische Auswirkungen. In Hongkong wurde beispielsweise eine App erst nicht genehmigt, weil sie, so Apple, ein Verhalten ermögliche und

fördere, das illegal sei. Dabei ging es um eine Anwendung, die den Menschen während der Massenproteste 2019 verwenden sollten, um nicht in Polizeikontrollen zu geraten. Dies irritierte vor allem daher, da Nutzerinnen und Nutzer auch in Navigations-Apps Polizeikontrollen melden können und dies von Apple nicht als illegal gewertet wurde. Der Entwickler hoffte auf ein bürokratisches Versagen bei Apple und wollte nicht von Zensur sprechen. Einen Beigeschmack hatte der Vorfall wegen des Verhaltens Apples in China dennoch. Die App wurde nach einem – nicht ungewöhnlichen – Revisionsprozess doch freigegeben (Becker 2019). In Russland haben Apple und Google im Vorfeld der russischen Parlamentswahlen von 2021 die App des Oppositionellen Alexej Nawalny auf Druck der russischen Behörden aus ihre App-Stores gelöscht (Hoppenstedt 2021). Google brachte die App kurz nach den Wahlen zurück in seinen PlayStore, Apple erst im April 2022 (Petereit 2022).

Während der Corona-Pandemie zeigte sich Googles und Apples Gatekeeper-Funktion auch in Deutschland und der Europäischen Union deutlich. Bei den Diskussionen um eine Corona-App, die die Menschen tracken oder tracen sollte, gab es auch in Deutschland Stimmen, die auf Tracking setzen, also forderten, dass nachvollziehbar ist, wo sich eine Person wie lange aufgehalten hat. Bürgerrechtlerinnen und Bürgerrechtler forderten eine datenschutzfreundlichere Maßnahme, nämlich das Tracing, bei dem mittels Bluetooth über Abstände und Dauer zwischen zwei Smartphones bestimmt werden sollte, wie hoch die Gefahr eine Ansteckung ist. Das Tracing setzte sich auch daher durch, weil Apple und Google mit ihren Betriebssystemen iOS und Android nur hierfür Schnittstellen zur Hardware ermöglichten und ein Tracking so technisch deutlich schlechter funktioniert hätte. Apple und Google ermöglichten außerdem nur ausgewählten Apps von Gesundheitsbehörden den Zugang zu ihren App-Stores. In diesem Falle nutzen sie ihre Gatekeeper-Position, um nicht nur autoritäre Staaten, sondern auch Vorhaben liberaler Demokratien, ihre Bevölkerung in einem nicht-verträglichen Maß zu überwachen, Einhalt zu gebieten. Bei aller Kritik an den Vorhaben einzelner Akteure der damaligen Großen Koalition und darüber hinaus für eine Tracking-App, der sich auch die Autorin anschloss, muss doch angemerkt werden, dass hier Konzerne demokratisch legitimierte Entscheidungen von Staaten übertrumpfen hätten können (Beuth 2020; Dillinger 2020; Riedel 2020).

8. Policy Empfehlungen

Geopolitik findet verstärkt auch im digitalen Raum statt. Diese Erkenntnis muss daher Grundlage für alle Handlungsempfehlungen sein. Digitalpolitiker und -politikerinnen müssen den Systemwettbewerb Ernst nehmen und in ihren Entscheidungen und Strategien berücksichtigen. Generell müssen Allianzen für Demokratie gebildet werden, um eine Antwort auf illiberale und autoritäre Bestrebungen zu geben. Die Friedrich-Naumann-Stiftung für die Freiheit hat daher bereits im Juni 2022 ein interdisziplinäres Grundlagenpapier mit liberalen Ansätzen für den neuen Systemwettbewerb veröffentlicht (Lissowsky et al. 2022).

Die digitale Dimension muss stärker Beachtung in der internationalen Politik bekommen. Dazu gehört auch die strategische Zusammenarbeit einzelner Ressorts, insbesondere der Digital-, Wirtschafts-, Sicherheits-, Außen- und Entwicklungspolitik. Zudem muss – wie bereits eingangs erwähnt – digitale Souveränität angestrebt werden. Dazu müssen drei strategische Ziele erreicht werden können: Wechselseitigkeit, Gestaltungsfähigkeit und Einfluss auf Anbieter, wofür es einer Vielfalt von Anbietern, der notwendigen Gestaltungsmacht und guter Beziehungen zu gleichgesinnten Partnern bedarf.

Konsequenter Einsatz für Internetfreiheit, Demokratie und Menschenrechte

Liberalen Demokratien müssen sich sowohl in ihren Nationalstaaten, als auch auf supra- und internationaler Ebene konsequent für ein globales freies und offenes Internet einsetzen – ebenso für Demokratie und Menschenrechte im digitalen Raum. Deutschland und die Europäische Union sind nicht nur Vorbild, sie setzen auch regulative Standards wie beispielsweise die Datenschutzgrundverordnung. Damit geht eine hohe Verantwortung ein. Gesetzesinitiativen, die beispielsweise die Privatsphäre einschränken, das Internet zensurieren, filtern oder überwachen würden, oder generell Vorhaben zur Einschränkung von Bürger- und Menschenrechten sollten daher strikt unterlassen und gar nicht erst zur Diskussion gestellt werden. Liberale Demokratien können nur so glaubwürdig in ihrem Angebot für eine Alternative zum autoritären Lager sein.

Stresstest für digitale und technologische Abhängigkeiten

Abhängigkeiten bedeuten immer Risiko. Mit einem Stresstest sollte regelmäßig festgestellt werden, wie groß die (sicherheitspolitischen) Risiken für Wirtschaft und Gesellschaft ausfallen, um sie dann möglichst zu verringern. Beachtung finden sollten hier zum Beispiel Lieferketten für Chips und andere wichtige Vorprodukte. Aber auch Rohstoffe und Infrastrukturen für die Kommunikation wie Unterseekabel oder 5G-Netze. Ein kontinuierliches Monitoring geplanter Vorhaben in inter-

nationalen Gremien zur Internet Governance und Standardisierung sollte ebenso dazu gehören, sodass frühzeitig durch diplomatische Bemühungen das demokratische Lager bei Abstimmungen gestärkt werden kann.

Um Abhängigkeiten zu verringern, reicht ein Stresstest an sich selbstverständlich nicht aus. Es müssen neue Bezugsquellen für Rohstoffe gefunden und auch mögliche neue Abbaugelände in Europa genutzt werden. Die Bevölkerung muss dafür frühzeitig eingebunden, aufgeklärt und mitgenommen werden. Ebenso müssen beispielsweise im Bereich der Chip-Produktion die Bereiche, in denen Deutschland und Europa bereits stark oder federführend sind – zum Beispiel Sensorik oder Optoelektronik – weiter ausgebaut werden. Die stark ausdifferenzierte Arbeitsteilung in diesem Bereich überwinden zu wollen, und alle Teile der Lieferkette in Europa anzusiedeln, ist utopisch und nicht sinnvoll. Autarkie sollte auch hier nicht angestrebt werden. Darüberhinaus sollte sich auf die Weiterentwicklung von Chip-Designs fokussiert werden. Das schließt auch die Anwerbung und Ausbildung von entsprechenden Fachkräften ein, die in deutlich höherer Zahl benötigt werden.

Strategie für internationale Digitalpolitik

Die Bundesregierung hat in ihrer verabschiedeten Digitalstrategie vom Sommer 2022 festgelegt, dass sie bis zum Jahr 2025 eine Strategie für die internationale Digitalpolitik vorlegen möchte. Damit wäre Deutschland eines der wenigen Länder weltweit, die eine solche Strategie entwickelt haben. Die thematischen Fokusse solcher Strategien gehen im internationalen Vergleich deutlich auseinander. Da Daniel Voelsen mit seiner jüngsten Arbeit einen guten Vorschlag für eine thematische Ausrichtung der deutschen Strategie vorgelegt hat, soll dieser an dieser Stelle bestärkt und unterstützt werden (Voelsen 2022). Voelsen verweist darauf, dass diverse verabschiedete Strategien bereits wichtige und geopolitisch relevante Teile abdecken. Darunter die Industriestrategie 2030, die gegebenenfalls angepasst werden müsste, die geplanten Zukunfts- und Chinastrategien, sowie die Anfang 2023 erwartete Nationale Sicherheitsstrategie. Themen, die für die deutsche Strategie für internationale Digitalpolitik noch abzudecken sind, sind Handelspolitik im Verbund mit Datenschutz und Nachhaltigkeit (Stichwort: free flow of data with trust), Entwicklungszusammenarbeit, insbesondere bei digitalen Infrastrukturen, sowie Menschenrechte und Demokratie. Voelsen empfiehlt außerdem – auch das soll hier unterstützt werden – dass die Bundesregierung, beziehungsweise das federführende Ministerium für Digitalisierung und Verkehr (BMDV) das Wissen der hiesigen netzpolitischen Community, die über ein enormes Detailwissen verfügt, in den Strategieentwicklungsprozess mit einbinden sollte.

Die Strategie für internationale Digitalpolitik sollte entsprechend Deutschlands bisherigen Engagements in den internationalen Gremien zur Internet Governance, der Bedeutsamkeit des Digitalen und der Geopolitik – nicht nur durch die Zeitwende – und aufgrund der Erwartung, die Partner gegenüber Deutschland haben, durchaus ambitioniert ausfallen. Dazu sollte eng mit dem Auswärtigen Amt (AA) und dem Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung (BMZ) kooperiert werden, um eine umfassende und bei den Koalitionspartnern nachhaltig verankerte Strategie vorzulegen.

Bessere und weitere Partnerschaften: gemeinsam gestalten und entwickeln

„[I]nternational politics has become more and more like a dysfunctional relationship, in which the partners aren't able to split up but can't stand being together either“ (Leonard 2021: 171). In einer vernetzten Welt ist es nahezu utopisch zu glauben, dass alle Probleme umfassend gelöst werden können. Vielmehr kommt es darauf an, zu lernen, mit Problemen umzugehen, sie zu managen. Einfach gesagt: sich auf eine kontinuierliche Paartherapie einzulassen (Leonard 2021). Bestes Beispiel hierfür ist der Datenaustausch zwischen der EU und den USA (Nebel 2022). Das gilt aber auch für Partnerschaften, die aus strategischen Gründen ausgebaut werden sollten. Dazu gehören beispielsweise die Partnerschaften mit Indien, Nigeria und Brasilien als einflussreiche Staaten in ihren jeweiligen Regionen. Mit Indien hat die Europäische Kommission im Jahr 2022 einen Trade and Technology Council (TTC) ins Leben gerufen. Dieser sollte ebenso wie der TTC mit den USA ausgebaut werden. Die gesamte Region des Indopazifiks wird für Deutschland und Europa nicht nur wegen der Chip-Produktion immer relevanter. Auch aus sicherheitspolitischen Überlegungen sollten hier entsprechende Partnerschaften gestärkt und ausgebaut werden (Valenti 2022). Gleiches gilt für den gesamten afrikanischen Kontinent. Die Bundesregierung will laut ihrer Digitalstrategie die bestehenden Digitaldialoge⁸ (unter anderem mit Indien, Indonesien und Mexiko) ausbauen und drei afrikanische Partner etablieren. Bislang finden mit dem afrikanischen Kontinent solche Digital Dialoge noch nicht statt.

Partnerschaften sind immer auf Augenhöhe zu führen. Dies gilt insbesondere für den Globalen Süden. Deutschland und Europa sollten partnerschaftlich und strategisch beim Aufbau von Cyber-Kapazitäten, zum Beispiel in Afrika, unterstützen. Die bei der Friedrich-Naumann-Stiftung für die Freiheit 2022 erschienene Publikation zum Thema gibt hier entsprechende Handlungsempfehlungen (Sahin 2022). Die Global Gateway Initiative der Europäischen Union ist hier als bestehendes, aber noch ausbaufähiges Instrument zu nennen.

Kooperationsprojekte wie GovStack⁹ können als vorbildliches Beispiel angeführt werden. Die offene Multi-Stakeholder-Initiative unter der Leitung BMZ, der Gesellschaft für Internationale Zusammenarbeit (GIZ), das Ministerium für Auswärtige Angelegenheiten Estlands, der ITU und der

Digital Impact Alliance entwickelt Bausteine für eGovernment-Services. Die auf Open-Source basierenden Verwaltungsdienstleistungen können von Regierungen weltweit eingesetzt werden, um die eigene Verwaltung digital zu transformieren und den Bürgerinnen und Bürgern moderne Verwaltungsdienstleistungen anzubieten. Die Förderung dieser Initiative ist ein Teil der Digitalstrategie der Bundesrepublik.

Einsatz in internationalen Gremien stärken und ausbauen

Deutschland ist nicht nur ein langjähriges und verdientes Mitglied in bereits eingangs erwähnten zahlreichen internationalen Gremien. Deutschlands aktives Engagement in diesen Gremien wird auch von der Weltgemeinschaft erwartet. Auch wenn sich das Land gerne in nationalen digitalpolitischen Diskussionen klein macht, so ist die Bedeutung Deutschlands und ebenso der Europäischen Union nicht zu unterschätzen. Neben der Erfahrung ist es vor allem die technische Expertise, die hier zum Tragen kommt. Die Europäische Union hat bereits erkannt, dass sie sich strategischer in Normungsprozesse einbringen muss. Das Gleiche muss für die Mitgliedsstaaten gelten, die in Institutionen wie der ITU jeweils ein Stimmrecht haben.

Deutschland und die EU-Mitglieder sollten auch in ihren diplomatischen Beziehungen für Initiativen in diesen Gremien um Unterstützung werben, die dafür sorgen, dass das Internet ein global offenes und freies bleibt und Menschenrechte schützt. Für Deutschland gilt zudem, dass es die Größe seiner Delegationen, die zu entsprechenden Gremiensitzungen reisen, deutlich ausbaut und damit verdeutlicht, dass man diesem Thema wirklich Bedeutung beimisst.

Der Multi-Stakeholder-Ansatz aus Wissenschaft, Wirtschaft und Zivilgesellschaft bei der Entwicklung von Normen und Standards sollte unbedingt beibehalten werden. Allerdings sollten Möglichkeiten geschaffen werden, gerade Mittelständler und Zivilgesellschaft finanziell zu unterstützen. Denn die Freistellung und die Reisekosten für entsprechende Mitarbeiterinnen und Mitarbeiter mit entsprechender Fachexpertise hat teilweise hohe Opportunitätskosten für Organisationen, die sich für sie nicht lohnen. Solch eine Maßnahme wäre eine Möglichkeit dem staatlichen strategischen Vorgehen Chinas etwas entgegenzusetzen, ohne selbst direkten staatlichen Einfluss auf die Standardsetzung auszuüben.

Das UN-Mandat für das IGF läuft 2025 aus. Die deutsche Bundesregierung sollte sich für eine Verlängerung des Mandats ebenso einsetzen, wie für eine Weiterentwicklung des Multi-Stakeholder-Forums.

Verantwortung von Unternehmen im digitalen Raum

Menschenrechtliche Sorgfaltspflichten erstrecken sich auch auf den digitalen Raum. Das gilt insbesondere dann, wenn Unternehmen eine Gatekeeperfunktion einnehmen. Um Unter-

⁸ <https://digital-dialogues.net/de/>

⁹ <https://www.govstack.global/>

nehmen zur Durchsetzung rechtsstaatlicher Standards und menschenrechtlicher Normen zu bewegen, bieten sich sowohl die Instrumente des Wettbewerbsrechts an, als auch die Möglichkeiten, die sich aus der Gesetzgebung zu Lieferketten ergeben. Grundsätzlich gilt, dass mit einer bestimmten Unternehmensgröße und einer herausgehobenen Stellung im Markt eine besondere Verantwortung einhergeht.

Mit dem bereits verabschiedeten Digital Markets Act (DMA) der Europäischen Union und dem noch zu verhandelnden Lieferkettengesetz stehen die dafür geeigneten Instrumente bereits in den Startlöchern. Der DMA ist seit November 2022 in Kraft, kommt aber erst im Mai 2023 zur Anwendung. Ende 2022 wurde bekannt, dass Apple die Öffnung für alternative App Stores vorbereite – vermutlich wegen der Vorgaben aus dem DMA. Die Öffnung soll allerdings nur für Nutzerinnen und Nutzer der EU sein. Es ist zu hoffen, dass perspektivisch der DMA, ähnlich wie die Datenschutzgrundverordnung (DSGVO) globale Standards setzen wird.

Sicherung und Aufbau von Infrastruktur: Unterwasserseekabel und Satelliten

Die Anschläge auf die Pipelines in der Ostsee haben gezeigt, wie angreifbar kritische Infrastruktur auf dem Meeresboden ist. Unterseekabel und Pipelines müssen geschützt werden. Dafür braucht es im Falle der Europäischen Union ein entsprechendes Mandat zum Beispiel für Frontex. Doch nicht nur der Meeresboden muss überwacht und vor Sabotage und Spionage geschützt werden, sondern auch die Orte, an denen die Kabel an Land kommen. Außerdem müssen Unterseekabel ausgebaut werden. Dabei sollten Betreiberstrukturen gewählt werden, die Abhängigkeiten und Risiken so weit wie möglich minimieren.

Im Herbst 2022 hat das EU-Parlament und die Mitgliedstaaten den Aufbau einer eigenen Satellitenkonstellation, Iris² (Infrastructure for Resilience, Interconnection and Security by Satellites), beschlossen. Das ist ein guter und wichtiger Schritt, um unabhängig von anderen Staaten oder privaten Anbietern zu werden. So können nicht nur Internetverbindungen in abgelegenen Regionen bereitgestellt werden, sondern auch in Kriegs- oder Katastrophenfällen, wie beispielsweise in der Ukraine oder im deutschen Ahrtal, wo die Überschwemmungen auch die Internet- und andere Kommunikationsverbindungen zerstörten. Hier ist vor allem öffentliche Überzeugungsarbeit zu leisten, da Aktivitäten im Weltraum häufig als Spielereien gesehen werden und der politische und gesellschaftliche Rückhalt für die hohen Investitionskosten sonst wegbrechen könnte.

Offene Standards einsetzen und fördern

Wer China zu Recht dafür kritisiert, dass es strategisch andere Staaten durch ihre Standards in einen Lock In-Effekt steuert, darf selber nicht ähnliches tun – selbst wenn diese Standards auf demokratischen und menschenrechtlichen Werten basie-

ren. Für Standards muss das Gleiche gelten wie für das Internet an sich: Sie müssen offen und interoperabel sein. Offene Standards müssen der Standard werden – das ist sowohl für die großen Herausforderungen der Geopolitik sinnvoll, als auch für die der Digitalisierung der kommunalen Verwaltungen und der dort genutzten Fachverfahren. Die Bundesregierung hat nicht umsonst den Einsatz für offene Standards als eines von drei Hebelprojekten benannt. Zur Förderung offener Standards sollten Gesetzgeber diese wo möglich zur Nutzung in der Verwaltung vorschreiben. Dadurch wird auch die eigene digitale Souveränität gestärkt.

Produkte und Technologien als das „Made in Europe“ des 21. Jahrhunderts

Datenschutzgrundverordnung, Digital Services Act, Digital Markets Act, AI Act usw. – Deutschland und die Europäische Union rühmen sich im Verabschieden von Digitalgesetzen, die global den Standard – wenn nicht gar den „Goldstandard“ vorgeben sollen (Stichwort: Brussels Effect). Doch Gesetze, Normen und Standards können nur ein Baustein in dem von der EU ausgerufenen Bestreben sein, eine wertebasierte Digitalisierung und damit den sogenannten „dritten Weg“ neben dem chinesischen und US-amerikanischen Modell anzubieten. Dies gilt insbesondere für das Vorhaben, Partner des Globalen Südens mit überzeugenden Angeboten weg vom autoritären Lager hin zum demokratischen Lager zu bewegen. Europäische Unternehmen müssen in der Lage sein, den Transfer zu markt-reifen und international wettbewerbsfähigen digitalen Produkten und Technologien zu leisten, die das „Made in Germany“ oder „Made in Europe“ des 21. Jahrhunderts werden können.

Literaturverzeichnis

Aglionby, John/Feng, Emily/Yang, Yuan (2018): African Union accuses China of hacking headquarters. In: Financial Times, 29. Januar 2018.

Allen-Ebrahimian, Bethany (2016): The Man Who Nailed Jello to the Wall. Foreign Policy. Text abrufbar unter: <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/> (Zugriff am 24.10.2022).

Alvares de Souza Soares, Philipp/Heide, Dana/Koch, Moritz (2022): Kritische Infrastruktur: „Müssen Naivität dringend ablegen“: Das China-Risiko im deutschen 5G-Netz. Text abrufbar unter: <https://www.handelsblatt.com/politik/deutschland/kritische-infrastruktur-muessen-naivitaet-dringend-ablegen-das-china-risiko-im-deutschen-5g-netz/28757958.html> (Zugriff am 2.1.2023).

Auswärtiges Amt (2018): Menschenrechte - online wie offline. Auswärtiges Amt. Text abrufbar unter: <https://www.auswaerziges-amt.de/de/aussenpolitik/themen/menschenrechte/freedom-online-coalition/2165464> (Zugriff am 22.12.2022).

Auswärtiges Amt (2020): China ist Partner, Wettbewerber und Rivale. Auswärtiges Amt. Text abrufbar unter: <https://www.auswaertiges-amt.de/de/newsroom/maas-rnd/2367282> (Zugriff am 4.1.2023).

Bahr, Egon (1963): Wandel durch Annäherung. Tutzing, 15. Juli 1963. Text abrufbar unter: https://www.1000dokumente.de/index.html?c=dokument_de&dokument=0091_bah&object=translation&st=&l=de (Zugriff am 28.10.2022).

Becker, Leo (2019): Hongkong-Proteste: Apple verweigert App der Demonstranten die Freigabe. Mac & i. Text abrufbar unter: <https://www.heise.de/mac-and-i/meldung/Hongkong-Proteste-Apple-verweigert-App-der-Demonstranten-die-Freigabe-4546094.html> (Zugriff am 9.1.2023).

Bendiek, Annegret/Godehardt, Nadine/Schulze, David (2019): Das Zeitalter der digitalen Geopolitik. Text abrufbar unter: <https://www.ipg-journal.de/rubriken/aussen-und-sicherheitspolitik/artikel/das-zeitalter-der-digitalen-geopolitik-3579/> (Zugriff am 25.10.2022).

Beuth, Patrick (2018): Tumblr verbietet ab dem 17. Dezember Pornografie und Nacktheit. In: Der Spiegel, 4. Dezember 2018. Text abrufbar unter: <https://www.spiegel.de/netzwelt/web/tumblr-verbietet-ab-dem-17-dezember-pornografie-und-nacktheit-a-1241851.html> (Zugriff am 9.1.2023).

Beuth, Patrick (2020): Corona-Apps: Apple und Google veröffentlichen Schnittstelle für Gesundheitsbehörden. Text abrufbar unter: <https://www.spiegel.de/netzwelt/apps/corona-apps-apple-und-google-veroeffentlichen-schnittstelle-fuer-gesundheitsbehoerden-a-a4c05fcc-e010-4c66-a576-e4f346e4019e> (Zugriff am 9.1.2023).

Beuth, Patrick (2021): IT-Sicherheitsgesetz 2.0: Bundestag beschließt Hürden-für-Huawei-Gesetz. In: Der Spiegel, 23. April 2021. Text abrufbar unter: <https://www.spiegel.de/netzwelt/netzpolitik/it-sicherheitsgesetz-2-0-bundestag-beschliesst-huerden-fuer-huawei-gesetz-a-2f50a7dc-e5f5-4b35-ba30-1ecbf1db4eed> (Zugriff am 2.1.2023).

Biddle, Sam/Hussain, Murtaza (2022): Hacked Documents: How Iran Can Track and Control Protesters' Phones. Text abrufbar unter: <https://theintercept.com/2022/10/28/iran-protests-phone-surveillance/> (Zugriff am 20.12.2022).

Bremmer, Ian (2022): The Technopolar Moment. Text abrufbar unter: <https://www.foreignaffairs.com/articles/world/2021-10-19/ian-bremmer-big-tech-global-order> (Zugriff am 3.11.2022).

Britannica (2022): East India Company | Definition, History, & Facts | Britannica. Text abrufbar unter: <https://www.britannica.com/topic/East-India-Company> (Zugriff am 3.11.2022).

Bueger, Christian/Liebetrau, Tobias/Franken, Jonas (2022): Security Threats to Undersea Communications Cables and Infrastructure – Consequences for the EU.

Buhl, Thomas/Schönhof, Raoul (2021): Wer sie gestaltet, beherrscht den Markt: Normen und Standards. Text abrufbar unter: https://www.fraunhofer.de/content/dam/zv/de/ueber-fraunhofer/wissenschaftspolitik/Positionen/Positionspapier%20Normen_und_Standards.pdf (Zugriff am 5.1.2023).

Bundesministerium für Wirtschaft und Klimaschutz (o. J.): Internet Governance. Text abrufbar unter: <https://www.bmwk.de/Redaktion/DE/Artikel/Digitale-Welt/internet-governance.html> (Zugriff am 24.10.2022).

Burgees, Matt (2018): Google and Facebook Are Gobbling up the Internet's Subsea Cables. Wired UK, Text abrufbar unter: <https://www.wired.co.uk/article/subsea-cables-google-facebook> (Zugriff am 27.10.2022).

Cerulus, Laurens (2022): Germany Is (Still) a Huawei Hotspot in Europe. POLITICO, Text abrufbar unter: <https://www.politico.eu/article/germany-is-still-a-huawei-hotspot-in-europe-5g-telecoms-network/> (Zugriff am 2.1.2023).

Commission on Science and Technology for Development (2015): Mapping of International Internet Public Policy Issues. E/CN.16/2015/CRP.2. Text abrufbar unter: https://unctad.org/system/files/official-document/ecn162015crp2_en.pdf.

Cory, Nigel/Dick, Ellysse (2021): How to Build Back Better the Transatlantic Data Relationship | ITIF. Text abrufbar unter: <https://itif.org/publications/2021/03/25/how-build-back-better-transatlantic-data-relationship/> (Zugriff am 27.10.2022).

Crews, Clyde Wayne (2001): One Internet Is Not Enough. Cato Institute. Text abrufbar unter: <https://www.cato.org/techknowledge/one-internet-not-enough> (Zugriff am 24.10.2022).

Crist, Ry (2022): Starlink Internet Explained. CNET. Text abrufbar unter: <https://www.cnet.com/home/internet/starlink-satellite-internet-explained/> (Zugriff am 23.12.2022).

Declaration for the Future of the Internet (2022): Declaration for the Future of the Internet. Text abrufbar unter: <https://www.state.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet.pdf>.

Delhaes, Daniel/Hoppe, Till (2021): Standards und Normen: Fraunhofer-Forscher warnen: Deutschland droht wachsende Abhängigkeit von USA und China bei Standardsetzung. Text abrufbar unter: <https://www.handelsblatt.com/politik/deutschland/standards-und-normen-fraunhofer-forscher-warnen-deutschland-droht-wachsende-abhaengigkeit-von-usa-und-china-bei-standardsetzung/27095900.html> (Zugriff am 5.1.2023).

derstandard.at (2014): „Papers Please“ für iOS zensuriert: Nacktscanner-Grafik für Apple zu pornografisch - GamePolitics - derStandard.at › Web. Text abrufbar unter: <https://www.derstandard.at/story/2000009294597/nacktscanner-pixelgrafik-spiel-war-fuer-apple-zu-pornografisch> (Zugriff am 9.1.2023).

Die Bundesregierung (2022a): Digitalstrategie. Gemeinsam digitale Werte schöpfen. Text abrufbar unter: https://digitalstrategie-deutschland.de/static/1a7bee26afd1570d3f0e-5950b215abac/220830_Digitalstrategie_fin-barrierefrei.pdf.

Die Bundesregierung (2022b): Digitalpolitik: Neuordnung der Zuständigkeiten | Bundesregierung. Webseite der Bundesregierung | Startseite. Text abrufbar unter: <https://www.bundesregierung.de/breg-de/themen/digitaler-aufbruch/digitalpolitik-2072890> (Zugriff am 24.10.2022).

Dillinger, Yannick (2020): Netzexpertin Riedel: Es darf bei Corona-App keinen „Man in the Middle“ geben. Augsburger Allgemeine. Text abrufbar unter: <https://www.augsburger-allgemeine.de/panorama/Corona-App-Netzexpertin-Riedel-Es-darf-bei-Corona-App-keinen-Man-in-the-Middle-geben-id57272371.html> (Zugriff am 9.1.2023).

Dohmen, Caspar (2022): Geopolitische Macht durch technische Normen - Wie China versucht, eigene Standards durchzusetzen. Deutschlandfunk. Text abrufbar unter: <https://www.deutschlandfunk.de/china-technische-standards-geopolitik-100.html> (Zugriff am 5.1.2023).

Economist (2022): An election that could make the global internet safer for autocrats. Text abrufbar unter: <https://www.economist.com/international/2022/09/20/an-election-that-could-make-the-global-internet-safer-for-autocrats> (Zugriff am 20.12.2022).

EllaLink (2022): Sines to Lisbon: The New Submarine Cable by EllaLink. EllaLink. Text abrufbar unter: <https://ellalink.com/2022/05/18/sines-to-lisbon-the-new-submarine-cable-by-ellalink/> (Zugriff am 27.10.2022).

EMOLCP (2021): Submarine Cable Linking Europe to South America Is „of the Utmost Strategic Importance“ – António Costa. EU 2021. Text abrufbar unter: <https://www.2021portugal.eu/en/news/submarine-cable-linking-europe-to-south-america-is-of-the-utmost-strategic-importance-antonio-costa/> (Zugriff am 27.10.2022).

Engler, Alex (2022): The Declaration for the Future of the Internet Is for Wavering Democracies, Not China and Russia. Brookings, Text abrufbar unter: <https://www.brookings.edu/blog/techtank/2022/05/09/the-declaration-for-the-future-of-the-internet-is-for-wavering-democracies-not-china-and-russia/> (Zugriff am 22.12.2022).

Erment, Monika (2019): IGF: Zum Schluss Streit über Cybersicherheit – und ein Denkmal für Jimmy Schulz. heise online. Text abrufbar unter: <https://www.heise.de/newsticker/meldung/IGF-Zum-Schluss-Streit-ueber-Cybersicherheit-und-ein-Denkmal-fuer-Jimmy-Schulz-4600037.html> (Zugriff am 25.10.2022).

Europäische Kommission (2015): The EU-Latin America Submarine Cable: Boosting the Connection between Our Continents | Shaping Europe's Digital Future. Text abrufbar unter: <https://digital-strategy.ec.europa.eu/en/news/eu-latin-america-submarine-cable-boosting-connection-between-our-continents> (Zugriff am 27.10.2022).

Europäische Kommission (o. J.): Das Gesetz über digitale Märkte: für faire und offene digitale Märkte. Text abrufbar unter: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_de (Zugriff am 9.1.2023).

Fedorov, Mykhailo (2022): @elonmusk, While You Try to Colonize Mars – Russia Try to Occupy Ukraine! While Your Rockets Successfully Land from Space – Russian Rockets Attack Ukrainian Civil People! We Ask You to Provide Ukraine with Starlink Stations and to Address Sane Russians to Stand. Twitter, Text abrufbar unter: <https://twitter.com/FedorovMykhailo/status/1497543633293266944> (Zugriff am 23.12.2022).

Foust, Jeff (2022): FCC Grants Partial Approval for Starlink Second-Generation Constellation. SpaceNews. Text abrufbar unter: <https://spacenews.com/fcc-grants-partial-approval-for-starlink-second-generation-constellation/> (Zugriff am 23.12.2022).

Freedom Online Coalition (o. J.): Members. Freedom Online Coalition, Text abrufbar unter: <https://freedomonlinecoalition.com/members/> (Zugriff am 22.12.2022).

Griffiths, James (2019): The Global Internet Is Powered by Vast Undersea Cables. But They're Vulnerable. CNN. Text abrufbar unter: <https://www.cnn.com/2019/07/25/asia/internet-undersea-cables-intl-hnk/index.html> (Zugriff am 27.10.2022).

Hamilton, Clive/Ohlberg, Mareike (2021): Die lautlose Eroberung: wie China westliche Demokratien unterwandert und die Welt neu ordnet. 6. Auflage. München: Pantheon.

Hebel, Christina (2013): NSA-Spähaffäre: Westerwelle beruft Cyber-Beauftragten. Text abrufbar unter: <https://www.spiegel.de/politik/deutschland/nsa-spaehaffaere-westerwelle-beruft-cyber-beauftragten-a-913443.html> (Zugriff am 25.10.2022).

Heide, Dana/Verfürden, Michael (2022): China: Duisburg legt umstrittene Kooperation mit Tech-Konzern Huawei auf Eis. Text abrufbar unter: <https://www.handelsblatt.com/politik/deutschland/china-duisburg-legt-umstrittene-kooperation-mit-tech-konzern-huawei-auf-eis/28801022.html> (Zugriff am 2.1.2023).

Heinrich, Alexander (2020): China als systemischer Rivale. Deutscher Bundestag. Text abrufbar unter: https://www.bundestag.de/webarchiv/presse/hib/2020_06/703540-703540 (Zugriff am 4.1.2023).

Herbig, Daniel/Wölbart, Christian (2021): Entwickler und Behörden setzen App-Store-Betreiber unter Druck. c't Magazin. Text abrufbar unter: <https://www.heise.de/news/Entwickler-und-Behoerden-setzen-App-Store-Betreiber-unter-Druck-6046626.html> (Zugriff am 9.1.2023).

Herbling, David (2022): Huawei-Backed Undersea Cable Linking China, Europe, Africa Lands in Kenya - Bloomberg. Text abrufbar unter: <https://www.bloomberg.com/news/articles/2022-03-29/huawei-backed-cable-linking-china-europe-africa-lands-in-kenya> (Zugriff am 27.10.2022).

Hoppenstedt, Max (2021): Russland: Nawalny-App bei Apple und Google nicht mehr verfügbar. In: Der Spiegel, 17. September 2021. Text abrufbar unter: <https://www.spiegel.de/netzwelt/netzpolitik/russland-nawalny-app-bei-apple-und-google-nicht-mehr-verfuegbar-a-90081c61-2b7b-4a86-abba-913b526b4157> (Zugriff am 9.1.2023).

IGF (2019): Message from the Meeting of Parliamentarians Participating in the 14th UN Internet Governance Forum. Berlin. Text abrufbar unter: https://www.intgovforum.org/en/filedepot_download/7505/1807.

ITU (2022a): ITU's Election Process Explained. ITU. Text abrufbar unter: <https://www.itu.int:443/en/mediacentre/backgrounders/Pages/election-process.aspx> (Zugriff am 20.12.2022).

ITU (2022b): Elections Results. PP-22, Text abrufbar unter: <https://pp22.itu.int/en/elections/elections-results/> (Zugriff am 20.12.2022).

ITU (o. J.): About ITU. ITU. Text abrufbar unter: <https://www.itu.int:443/en/about/Pages/default.aspx> (Zugriff am 20.12.2022).

Iyengar, Rishi (2022): Why Ukraine Is Stuck With Elon (for Now). Foreign Policy. Text abrufbar unter: <https://foreignpolicy.com/2022/11/22/ukraine-internet-starlink-elon-musk-russia-war/> (Zugriff am 23.12.2022).

Kabelka, Laura (2022): EU Aims to Tackle Threats to Submarine Data Cables. www.euractiv.com. Text abrufbar unter: <https://www.euractiv.com/section/digital/news/eu-aims-to-tackle-threats-to-submarine-data-cables/> (Zugriff am 4.1.2023).

Kadiri, Ghalia/Tilouine, Joan (2018): A Addis-Abeba, le siège de l'Union africaine espionné par Pékin. In: Le Monde.fr, 26. Januar 2018. Text abrufbar unter: https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html (Zugriff am 2.1.2023).

Kania, Elsa (2018a): Much Ado about Huawei (Part 1). The Strategist. Text abrufbar unter: <https://www.aspistrategist.org.au/much-ado-huawei-part-1/> (Zugriff am 2.1.2023).

Kania, Elsa (2018b): Much Ado about Huawei (Part 2). The Strategist. Text abrufbar unter: <https://www.aspistrategist.org.au/much-ado-huawei-part-2/> (Zugriff am 2.1.2023).

Kleinhans, Jan-Peter/Hess, Julia (2021): Understanding the Global Chip Shortages. Stiftung Neue Verantwortung.

Kleinwächter, Wolfgang (2019): Gegen Angriffe und Alleingänge: Wie retten wir das globale Internet? In: FAZ.NET, 2. Mai 2019. Text abrufbar unter: <https://www.faz.net/aktuell/feuilleton/debatten/das-globale-internet-retten-kleinwaechter-fordert-grundvertrag-16165952.html> (Zugriff am 15.10.2022).

Knaack, Tobias (2022): Huawei steuert trotz US-Sanktionen von Krisenmodus zu Normalbetrieb. heise online. Text abrufbar unter: <https://www.heise.de/news/Huawei-steuert-trotz-US-Sanktionen-von-Krisenmodus-zu-Normalbetrieb-7444499.html> (Zugriff am 2.1.2023).

Krempl, Stefan (2022a): Standardisierung: EU-Kommission beansprucht Führungsrolle Europas bei Normen. heise online. Text abrufbar unter: <https://www.heise.de/news/Standardisierung-EU-Kommission-beansprucht-Fuehrungsrolle-Europas-bei-Normen-6346558.html> (Zugriff am 5.1.2023).

Krempl, Stefan (2022b): Angst vor Zensur: China wirbt im „Protokollkrieg“ auf ITU-Ebene für IPv6+. heise online. Text abrufbar unter: <https://www.heise.de/news/Angst-vor-Zensur-China-wirbt-im-Protokollkrieg-auf-ITU-Ebene-fuer-IPv6-7134187.html> (Zugriff am 5.1.2023).

Krempf, Stefan (2022c): Kartellrecht: EU-Kommission prüft Marktmissbrauch beim Google Play Store. heise online. Text abrufbar unter: <https://www.heise.de/news/Kartellrecht-EU-Kommission-prueft-Marktmissbrauch-beim-Google-Play-Store-7202834.html> (Zugriff am 9.1.2023).

Kurbalija, Jovan (2016): An Introduction to Internet Governance. 7th edition. Msida, Malta Geneva Belgrade: Diplo- Foundation.

Lau, Jörg (2021): Wandel durch Handel. Text abrufbar unter: <https://internationalepolitik.de/de/wandel-durch-handel-0> (Zugriff am 28.10.2022).

Lee, John/Kleinhans, Jan-Peter (2021): Mapping China's Semiconductor Ecosystem in Global Context. Stiftung Neue Verantwortung.

Leonard, Mark (2021): The age of unpeace: how connectivity causes conflict. London: Bantam Press.

Lissowsky, Michaela/Winter, Theresa/Hilgers, Sven/Riedel, Ann Cathrin (2022): Allianzen für Demokratie. Liberale Ansätze für den neuen Systemwettbewerb. Text abrufbar unter: <https://shop.freiheit.org/#!/Publikation/1280> (Zugriff am 23.1.2023).

Malik, Nesrine (2014): Too big and too scary, but the global fat cats can be chopped down to size. Text abrufbar unter: <https://www.theguardian.com/commentisfree/2014/dec/10/big-scary-global-fat-cats-multinationals-tax-dodgers> (Zugriff am 3.11.2022).

Mantel, Mark (2022): EU Chips Act: Alte Fertigungsprozesse können „State of the Art“ sein. heise online. Text abrufbar unter: <https://www.heise.de/news/EU-Chips-Act-Alte-Fertigungsprozesse-koennen-State-of-the-Art-sein-7351852.html> (Zugriff am 22.12.2022).

Mauldin, Alan (2017): A Complete List of Content Providers' Submarine Cable Holdings. Text abrufbar unter: <https://blog.telegeography.com/telegeographys-content-providers-submarine-cable-holdings-list> (Zugriff am 27.10.2022).

Miller, Christopher (2022): Chip War. The Fight for the World's Most Critical Technology. 1. New York: Scribner.

Mozilla (2019): The New Investors in Underwater Sea Cables. The Internet Health Report 2019. Text abrufbar unter: <https://internethealthreport.org/2019/the-new-investors-in-underwater-sea-cables/> (Zugriff am 27.10.2022).

Muth, Max (2021): Apple gewinnt gegen Epic Games: „Erfolg ist nicht strafbar“. Süddeutsche.de. Text abrufbar unter: <https://www.sueddeutsche.de/wirtschaft/apple-epic-game-fortnite-gericht-urteil-1.5409289> (Zugriff am 9.1.2023).

National Army Museum (o. J.): Armies of the East India Company. Text abrufbar unter: <https://www.nam.ac.uk/explore/armies-east-india-company> (Zugriff am 3.11.2022).

Nebel, Jens (2022): Bald „Schrems III“? EU-USA-Datentransfer und EuGH. Legal Tribune Online. Text abrufbar unter: <https://www.lto.de/recht/hintergruende/h/eu-usa-daten-transfer-eugh-schrems-datenschutz-geheimdienste-unternehmen/> (Zugriff am 5.1.2023).

Paris Call (2018): Paris Call for Trust and Security in Cyberspace. Text abrufbar unter: <https://pariscall.international/en/> (Zugriff am 22.12.2022).

Petereit, Dieter (2022): Nawalny-App: Apple bringt Putin-Opposition zurück in den App-Store. t3n Magazin. Text abrufbar unter: <https://t3n.de/news/nawalny-app-apple-zurueck-1464719/> (Zugriff am 9.1.2023).

Rat der Europäischen Union (2022): Chip-Gesetz: Rat legt Standpunkt fest. Text abrufbar unter: <https://www.consilium.europa.eu/de/press/press-releases/2022/12/01/chips-act-council-adopts-position/> (Zugriff am 22.12.2022).

Renouard, Guillaume (2019): Die Balkanisierung des Internets. www.euractiv.de. Text abrufbar unter: <https://www.euractiv.de/section/eu-innenpolitik/news/die-balkanisierung-des-internets/> (Zugriff am 24.10.2022).

Riedel, Ann Cathrin (2020): Corona-Warn-App: Lockdown 2: Am Datenschutz scheitert die Corona-Bekämpfung nicht. Text abrufbar unter: <https://www.freiheit.org/de/corona-warn-app-lockdown-2-am-datenschutz-scheitert-die-corona-bekaempfung-nicht> (Zugriff am 9.1.2023).

Riedel, Ann Cathrin (2021): Liberalismus: Was das Tiananmen-Massaker mit Pornoseiten zu tun hat. In: Die Zeit, Hamburg, 21. Juni 2021. Text abrufbar unter: <https://www.zeit.de/politik/deutschland/2021-06/liberalismus-digitalisierung-datenschutz-freiheit-buergerrechte> (Zugriff am 9.1.2023).

Riedel, Ann Cathrin/Widlok, Teresa (2022): Mehr digitale Souveränität. Liberal. Text abrufbar unter: <https://liberal-magazin.de/2022/04-2022/digitalisierung> (Zugriff am 4.1.2023).

Röhrlich, Dagmar (2022): Silizium, Kobalt, Lithium - Der globale Kampf um Rohstoffe der Zukunft. Deutschlandfunk. Text abrufbar unter: <https://www.deutschlandfunk.de/silizium-kobalt-lithium-rohstoffe-seltene-erden-100.html> (Zugriff am 22.12.2022).

Roth, Yoel (2022): What's Twitter's Future? The Former Head of Trust And Safety Weighs In. Text abrufbar unter: <https://www.nytimes.com/2022/11/18/opinion/twitter-yoel-roth-elon-musk.html> (Zugriff am 23.1.2023).

Rother, Carina (2021): Taiwans Chip-Produzent TSMC - Systemrelevant für die Welt. Deutschlandfunk Kultur. Text abrufbar unter: <https://www.deutschlandfunkkultur.de/taiwans-chip-produzent-tsmc-systemrelevant-fuer-die-welt-100.html> (Zugriff am 22.12.2022).

Rühlig, Tim (2022): Chinas unsichtbare Macht technischer Standards. Friedrich-Naumann-Stiftung für die Freiheit. Text abrufbar unter: <https://shop.freiheit.org/#!/Publikation/1333> (Zugriff am 20.12.2022).

Rydlink, Katherine (2017): China: Apple löscht alle wichtigen VPN-Apps aus App-Store. In: Der Spiegel, 29. Juli 2017. Text abrufbar unter: <https://www.spiegel.de/netzwelt/netzpolitik/china-apple-loescht-alle-wichtigen-vpn-apps-aus-app-store-a-1160451.html> (Zugriff am 20.12.2022).

Sahin, Kaan (2022): Cyber-Kapazitäts-Aufbau und strategisches Engagement in Afrika. Friedrich-Naumann-Stiftung für die Freiheit. Text abrufbar unter: <https://shop.freiheit.org/#!/Publikation/1235> (Zugriff am 5.1.2023).

Satariano, Adam (2022): How Russia Took Over Ukraine's Internet in Occupied Territories. In: The New York Times, 9. August 2022. Text abrufbar unter: <https://www.nytimes.com/interactive/2022/08/09/technology/ukraine-internet-russia-censorship.html> (Zugriff am 23.12.2022).

Sauter, Marc (2022a): Halbleiterfertigung: Intel bekommt 6,8 Mrd. Euro für Magdeburg-Fab. Text abrufbar unter: <https://www.golem.de/news/halbleiterfertigung-intel-bekommt-6-8-mrd-euro-fuer-magdeburg-fab-2206-165882.html> (Zugriff am 22.12.2022).

Sauter, Marc (2022b): Chips Act for America: Milliarden-Investment für US-Industrie ist beschlossen. Text abrufbar unter: <https://www.golem.de/news/chips-act-for-america-milliarden-investment-fuer-us-industrie-ist-beschlossen-2207-167256.html> (Zugriff am 22.12.2022).

Schieb, Jörg (2022): Datenleitungen in Gefahr? Das Internet verläuft durchs Meer. Text abrufbar unter: <https://www1.wdr.de/nachrichten/schieb-seekabel-infrastruktur-internet-meer-sabotage-sicherheit-100.html> (Zugriff am 27.10.2022).

Scholl, Reinhard (2022): The Art of Reaching Consensus. Genf, 10. März 2022. Text abrufbar unter: https://www.itu.int/en/ITU-T/tutorials/202203/Documents/Reinhard%20Scholl_v2_The%20art%20of%20reaching%20consensus.pdf.

Scholz, Olaf (2022): Reden zur Zeitenwende. In: Text abrufbar unter: <https://www.bundesregierung.de/resource/blob/992814/2131062/78d39dda6647d7f835bbe76713d30c31/bundeskanzler-olaf-scholz-reden-zur-zeitenwende-download-bpa-data.pdf?download=1>.

Schürpf, Thomas/Höltschi, René/Gerald, Hosp/Keusch, Nelly (2022): Nord-Stream-Pipelines: die neusten Entwicklungen. Text abrufbar unter: <https://www.nzz.ch/wirtschaft/pipeline-projekt-nord-stream-2-die-neusten-entwicklungen-ld.1483495> (Zugriff am 27.10.2022).

Schwan, Ben (2022): Sideloadung und alternative App Stores: Wie die iPhone-Zukunft aussehen könnte. Mac & i. Text abrufbar unter: <https://www.heise.de/news/Sideloadung-und-alternative-App-Stores-Wie-die-iPhone-Zukunft-aussehen-koennte-7396367.html> (Zugriff am 9.1.2023).

Scott, Mark (2022): Digital Bridge: Stop the Steal 2.0 – ITU's Standards Guru – China and Chips. POLITICO, Text abrufbar unter: <https://www.politico.eu/newsletter/digital-bridge/stop-the-steal-2-0-itus-standards-guru-china-and-chips/> (Zugriff am 20.12.2022).

Shahbaz, Adrian (2018): The Rise of Digital Authoritarianism. Freedom House. Text abrufbar unter: <https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism> (Zugriff am 20.12.2022).

Shahbaz, Adrian/Funk, Allie/Vesteinsson, Kian (2022): Countering an Authoritarian Overhaul of the Internet. Freedom House. Text abrufbar unter: <https://freedomhouse.org/report/freedom-net/2022/countering-authoritarian-overhaul-internet> (Zugriff am 21.10.2022).

Sherman, Justin (2021): Beijing's Growing Influence on the Global Undersea Cable Network. Jamestown. Text abrufbar unter: <https://jamestown.org/program/beijings-growing-influence-on-the-global-undersea-cable-network/> (Zugriff am 27.10.2022).

Slaughter, Anne-Marie (2016): How to Succeed in the Networked World: A Grand Strategy for the Digital Age. In: Foreign Affairs, Council on Foreign Relations, 95 (6), 76–89.

Slaughter, Anne-Marie (2018): The Chessboard and the Web: Strategies of Connection in a Networked World. New Haven: Yale University Press.

Soldatov, Andrei/Borogan, Irina (2022): Russland – YouTube und globale Plattformen. Friedrich-Naumann-Stiftung für die Freiheit. Text abrufbar unter: <https://shop.freiheit.org/#!/Publikation/1261> (Zugriff am 20.12.2022).

SPD, Bündnis90/Die Grünen, FDP (2021): Mehr Fortschritt wagen. Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit. Koalitionsvertrag zwischen SPD, Bündnis 90/Die Grünen und FDP. Text abrufbar unter: https://www.fdp.de/sites/default/files/2021-11/Koalitionsvertrag%202021-2025_0.pdf.

Splett, Candida (2020): NewIP – Grundstein für ein globales Internet nach chinesischen Vorstellungen? Stiftung Wissenschaft und Politik (SWP). Text abrufbar unter: <https://www.swp-berlin.org/publikation/newip-grundstein-fuer-ein-globales-internet-nach-chinesischen-vorstellungen> (Zugriff am 5.1.2023).

Staab, Philipp (2019): Digitaler Kapitalismus: Markt und Herrschaft in der Ökonomie der Unknappheit. 1. Auflage. Berlin: Suhrkamp Verlag; Originalausgabe edition.

Stenke, Wolfgang (2013): Wandel durch Annäherung. Deutschlandfunk. Text abrufbar unter: <https://www.deutschlandfunk.de/wandel-durch-annaeherung-104.html> (Zugriff am 28.10.2022).

tagesschau.de (2022): Milliarden-Investition: US-Konzern Intel baut Chipfabrik in Magdeburg. tagesschau.de. Text abrufbar unter: <https://www.tagesschau.de/wirtschaft/unternehmen/intel-magdeburg-101.html> (Zugriff am 22.12.2022).

TeleGeography (o. J.): Submarine Cable FAQs. Text abrufbar unter: <https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions> (Zugriff am 27.10.2022).

Tett, Gillian (2022): Ukraine's Starlink problems show the dangers of digital dependency. Text abrufbar unter: <https://www.ft.com/content/692a222b-7823-4308-80a1-afa05111351c> (Zugriff am 23.12.2022).

Trappe, Nathalie (2022): Deal zwischen Musk und Putin befürchtet: Ukraine meldet Ausfälle von „Starlink“-Satelliten – SpaceX-Chef weist Kritik zurück. In: Der Tagesspiegel Online, 8. Oktober 2022. Text abrufbar unter: <https://www.tagesspiegel.de/politik/deal-zwischen-musk-und-putin-befurchtet-ukraine-meldet-ausfalle-von-starlink-satelliten-8727622.html> (Zugriff am 23.12.2022).

United States Department of State (2022): Declaration for the Future of the Internet. United States Department of State, Text abrufbar unter: <https://www.state.gov/declaration-for-the-future-of-the-internet/> (Zugriff am 22.12.2022).

US State Department (2022): Remarks at a U.S.-German Futures Forum Moderated Discussion with German Foreign Minister Annalena Baerbock. United States Department of State, Text abrufbar unter: <https://www.state.gov/remarks-at-a-u-s-german-futures-forum-moderated-discussion-with-german-foreign-minister-annalena-baerbock/> (Zugriff am 6.1.2023).

Valenti, Alix (2022): Friedrich-Naumann-Stiftung für die Freiheit - Shop. Friedrich-Naumann-Stiftung für die Freiheit. Text abrufbar unter: <https://shop.freiheit.org/#/Publikation/1330> (Zugriff am 23.1.2023).

Voelsen, Daniel (2021): Internet aus dem Weltraum. Stiftung Wissenschaft und Politik (SWP). Text abrufbar unter: <https://www.swp-berlin.org/publikation/satelliten-internet> (Zugriff am 23.12.2022).

Voelsen, Daniel (2022): Deutschlands erste Strategie zur internationalen Digitalpolitik. Stiftung Wissenschaft und Politik (SWP). Text abrufbar unter: <https://www.swp-berlin.org/publikation/deutschlands-erste-strategie-zur-internationalen-digitalpolitik> (Zugriff am 5.1.2023).

Wall, Colin/Morcos, Pierre (2021): Invisible and Vital: Undersea Cables and Transatlantic Security. Text abrufbar unter: <https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security> (Zugriff am 27.10.2022).

Windeck, Christof (2022): Bit-Rauschen: Chinas Halbleiterbranche im Würgegriff von US-Sanktionen. c't Magazin. Text abrufbar unter: <https://www.heise.de/news/Chinas-Halbleiterbranche-im-Wuergegriff-von-US-Sanktionen-7324568.html> (Zugriff am 22.12.2022).

Wirtschaftswoche (2022): Halbleitermangel: Wie der Chipmangel entstanden ist – und wie er überwunden werden kann. Text abrufbar unter: <https://www.wiwo.de/unternehmen/auto/halbleitermangel-wie-der-chipmangel-entstanden-ist-und-wie-er-ueberwunden-werden-kann/27893766.html> (Zugriff am 20.12.2022).

Autorin



Ann Cathrin Riedel

ist Referentin für Globale Digitalisierung und Innovation bei der Friedrich-Naumann-Stiftung für die Freiheit. Sie ist Vorsitzende von LOAD e.V. – Verein für liberale Netzpolitik. Im Jahr 2022 wurde sie in den Beirat zur Umsetzung der Digitalstrategie der Bundesregierung beim Bundesministerium für Digitalisierung und Verkehr und in den Digitalrat des Landes Sachsen-Anhalt berufen. Desweiteren begleitet sie die Arbeit des Co:Lab – Denklabor & Kollaborationsplattform für Gesellschaft & Digitalisierung e.V., des Digital Autonomy Hub und des Projekts Plattform//Demokratie als Beirätin. Sie war Sachverständige zu digitalpolitischen Themen im Deutschen Bundestag und Berliner Abgeordnetenhaus. Das Capital Magazin zeichnete sie 2020 als Top 40 unter 40 in der Kategorie „Wissenschaft und Gesellschaft“ aus. In ihren Funktionen publiziert und spricht sie regelmäßig über Ethik und Bürgerrechte, Meinungsfreiheit und Kommunikation im digitalen Raum, sowie digitale Souveränität – unter anderem in ihrem prämierten Newsletter „Ann Cathrin's Digital Digest“.

