



Quelle: © Cathal McNaughton, Reuters.

Der Blick nach Westen

Zwischen Innovation und Regulierung

Zur Notwendigkeit transatlantischer
Kooperation im digitalen Raum

Sebastian Weise

Bereits heute durchdringt die Digitalisierung zunehmend die Wirtschafts- und Lebenswelt und treibt einen sich beschleunigenden Transformationsprozess westlicher Gesellschaften an. Angesichts der erheblichen Innovationswucht der Digitalisierung sehen nicht wenige in der Gestaltung der Digitalisierung eine drängende, wenn nicht gar *die* Aufgabe unserer Zeit. Da die Digitalisierung als globaler Prozess nicht an nationalen Grenzen stoppt, bedarf die Gestaltung der digitalen Transformation grenzüberschreitender Antworten. Welche Rolle hierbei das transatlantische Bündnis spielen sollte und spielen kann, nimmt der vorliegende Beitrag in den Blick.

Warum die wirtschaftlich erfolgreiche Gestaltung der Digitalisierung transatlantischer Antworten bedarf

Betrachtet man Kennzahlen des transatlantischen Handels, der digitalen Wirtschaft und des Datenstroms, wird deutlich: Die USA und Europa sind als Märkte wie als Datenräume eng miteinander verwoben und stellen füreinander Treiber des wirtschaftlichen Wachstums dar. Als die zwei größten Wirtschaftsräume der Welt sind Europa und die USA die gegenseitig wichtigsten Handelspartner und zugleich jene Datenräume, zwischen denen heutzutage der Großteil des weltweiten Datenaustauschs stattfindet.¹ Gerade der freie Fluss von Daten ermöglicht erst den heutigen Umfang transatlantischer Waren- und Dienstleistungsströme und fördert zugleich per se wirtschaftliches Wachstum.² Im Bereich der Digitalwirtschaft ist der transatlantische Handel besonders ausgeprägt und stellt die Handelsbeziehungen mit anderen Kontinenten in den Schatten.³ Dies ist insofern bedeutsam, da die Digitalwirtschaft ein entscheidender wirtschaftlicher Wachstumsfaktor und Innovationstreiber ist, der für die Zukunft der wirtschaftlichen Stärke Europas eine wichtige Rolle spielt.⁴ Zugleich ist die Digitalwirtschaft ein Bereich, in dem die USA gegenüber Europa einen Außenhandelsüberschuss aufweisen.⁵ Blickt man auf die entscheidenden digitalen Innovationstreiber in Europa, sind insbesondere US-amerikanische Technologieunternehmen in den zurückliegenden Jahren

tonangebend gewesen. In dieser Rolle haben Unternehmen wie Google (Alphabet), Apple, Facebook und Amazon (kurz: GAFA) die Digitalisierung in Europa erheblich geprägt⁶ und schicken sich an, diese Rolle weiterhin einzunehmen.⁷ Damit sind die USA für Europa als Wirtschaftsmacht und digitaler Innovationstreiber nicht nur per se eine wichtige Bezugsgröße. Als „Heimatland“ digitaler Champions sind die USA ein wichtiger Partner – stehen doch diese Digitalunternehmen bei der Gestaltung der Wirtschaft von morgen (digitale Plattformökonomie) im besonderen Fokus. Gerade für die angesprochenen US-Unternehmen, die zugleich für die USA als Innovationstreiber von zentraler Bedeutung sind, ist Europa wiederum sowohl als Absatzmarkt wie auch als Datenpool von hoher Bedeutung.

Warum eine gesellschaftlich erfolgreiche Gestaltung der Digitalisierung transatlantischer Antworten bedarf

Während nach dem Ende des Kalten Krieges teils das Ende der Geschichte ausgerufen wurde, ist das freiheitlich-liberale Ordnungsmodell heute wieder unter Druck. Herausgefordert wird das westliche Ordnungsmodell durch einen internationalen Autoritarismus, in dem China und Russland eine Führungsrolle einnehmen. Im Lichte dieser Systemkonkurrenz ist die Digitalisierung von besonderer Bedeutung, zielen autoritäre Staaten doch darauf ab, die digitale

Transformation im Sinne eigener Werte- und Ordnungsvorstellungen zu gestalten und Veränderungsdynamiken für den eigenen machtpolitischen Aufstieg zu nutzen.

Betrachtet man die letzten zwei Jahrzehnte, ist die Entwicklung Chinas und der damit einhergehende Zuwachs an wirtschaftlicher Macht beachtlich.⁸ Nachdem China in der jüngeren Vergangenheit Deutschland als Exportweltmeister sowie die USA als Handelsweltmeister bereits abgelöst hat, könnte China manchen Schätzungen folgend bereits Mitte der 2020er Jahre zur quantitativ größten Volkswirtschaft der Welt aufsteigen.⁹ Jenseits dessen strebt China in einer Vielzahl wichtiger Zukunftstechnologien an,¹⁰ zum Westen aufzuschließen und langfristig die Position der globalen Innovationsführerschaft zu erlangen.¹¹ Hierfür investiert das Land nicht nur immense Summen in Forschung und Entwicklung. China nutzt zugleich eine Reihe illegitimer Handelspraktiken,¹² um den Innovationswettbewerb der Systeme zu seinen Gunsten zu entscheiden und den Zuwachs an wirtschaftlicher Macht zu verstetigen.

Darüber hinaus gestalten autoritäre Staaten, allen voran China und Russland, die Digitalisierung im Sinne autoritärer Werte- und Ordnungsvorstellungen.¹³ Abschaltungen des Internets, eine millionenfache Zensur von Internetseiten, die Verfolgung/Identifikation oppositioneller Kräfte über soziale Medien, die Nutzung neuester Technologien für staatliche Überwachungsmaßnahmen (Gesichtserkennung) bis hin zur Einführung eines *Social Scoring System* – all dies sind Beispiele, wie autoritäre Staaten technologische Innovationen zu Lasten der Freiheitsrechte ihrer Bürger nutzen und dabei zu vergleichbar geringen Kosten autoritäre Strukturen stabilisieren.¹⁴

China setzt neue technologische Mittel für autoritäre Zwecke nicht nur im eigenen Land ein, sondern exportiert den digitalen Autoritarismus auch in andere Länder. Deutlich wird dies unter anderem beim Export von Überwachungstechnologien entlang des „One Road One Belt“-Projekts nach Ecuador oder nach Venezuela.¹⁵ Jenseits des Technologieexports

forcieren Russland und China auf internationaler Ebene die Etablierung einer alternativen Ordnung des virtuellen Raums, die den digitalen Autoritarismus zusätzlich stärkt. Statt der liberalen Idee eines freien und offenen Internets, verwaltet durch einen *multi stakeholder*-Ansatz, treten autoritäre Staaten für eine durch nationale Souveränitätsrechte geprägte Ordnung des Internets ein. Im Zuge dieser Ordnungsidee sind Staaten nicht nur die zentralen Akteure. Es wird ihnen, mit Verweis auf die Idee der Informationssicherheit, die Möglichkeit eingeräumt, innerhalb eigener nationaler Grenzen das World Wide Web zu zensieren, Nutzer ohne rechtsstaatliche Kontrolle zu überwachen und die Fragmentierung des heute globalen World Wide Web in nationale virtuelle Räume voranzutreiben.¹⁶ Eine Vielzahl an Fällen von E-Spionage, Cyberangriffen, Fake News-Kampagnen und gezielter Wahlbeeinflussung in sozialen Medien, gepaart mit der Veröffentlichung kompromittierender Daten, zeigen außerdem, dass autoritäre Regime im Kontext der neuen Systemkonkurrenz neue digitale Mittel einsetzen, um die Sicherheit westlicher Staaten zu attackieren bzw. den gesellschaftlichen Zusammenhalt zu schwächen.

Autoritäre Regime setzen neue digitale Mittel ein, um die Sicherheit westlicher Staaten zu attackieren und den gesellschaftlichen Zusammenhalt zu schwächen.

Damit freiheitlich-liberale Systeme angesichts dieser Herausforderung weiterhin gedeihen, sollten Europa und die USA nicht nur im Inneren die Digitalisierung erfolgreich gestalten und die Überlegenheit freiheitlicher Ordnungsmodelle im Innovationswettbewerb der Systeme nachweisen. Gerade auf internationaler Ebene sollten beide Seiten des Atlantiks ihre Gestaltungsmacht nutzen, um im Sinne gemeinsamer Werte und Interessen einen freiheitlich liberalen



Filterbrille: US-Unternehmen wie Google bestimmen den digitalen Raum auch in Europa erheblich.

Quelle: © Peter Power, Reuters.

Ordnungsrahmen für die Digitalisierung weiterentwickeln und den digitalen Autoritarismus einzudämmen.

Ein kurzer Blick in die Vergangenheit: Die Entstehung der Idee der technologischen / digitalen Souveränität Europas

Blickt man in die Vergangenheit, verfolgten Europa und die USA im Bereich der Digitalpolitik sehr ähnliche Interessen und Wertevorstellungen. Getragen von einem eher optimistischen „Internet-Zeitgeist“ zielten Europa und die USA im Rahmen einer *Internet Freedom Agenda* darauf ab, die neuen Möglichkeiten des World Wide Web nach innen wie nach außen zu nutzen. Hierbei war man überzeugt, dass ein freies und offenes Internet sowohl wirtschaftliches Wachstum und

Innovationen fördert, die Resilienz freiheitlicher Gesellschaften ebenso stärkt wie die Demokratie selbst und darüber hinaus weltweit Entwicklung fördert wie auch die Ausbreitung der Menschenrechte und der Demokratie.¹⁷ Insbesondere der sogenannte Arabische Frühling galt nicht wenigen Technologieoptimisten als wichtiges Zeichen für das emanzipatorische und disruptive Potenzial der Digitalisierung und der Notwendigkeit, dieses im Sinne liberaler Werte zu fördern. Die Enthüllungen Edward Snowdens im Jahr 2013 waren hierbei allerdings ein Wendepunkt. Infolge der Enthüllungen breitete sich eine neue Sensibilität der Öffentlichkeit für die Ambivalenz der Digitalisierung aus, im Zuge derer der positive „Internet-Zeitgeist“ an Strahlkraft verlor. Gleichzeitig offenbarten die in Folge der Enthüllungen zu Tage getretenen Praktiken von Geheimdiensten,

dass im transatlantischen Verhältnis ernsthafte Differenzen bestehen. Als Reaktion hierauf wurde diesseits des Atlantiks nun vermehrt eine stärkere digitale Souveränität Europas gefordert¹⁸ und eine eigenständigere Gestaltung der Digitalisierung durch Europa.¹⁹ Dieser Pfad des Strebens nach einer stärkeren digitalen Souveränität hat sich in den letzten Jahren weiter verfestigt und gilt heutzutage als Handlungsimperativ für Europa.²⁰ Steht Europa gegenwärtig doch vor der doppelten Herausforderung, seine wirtschaftliche Prosperität, seine Werte und damit seine Rolle als bedeutende Gestaltungsmacht gegen die Dominanz der USA und Chinas im Bereich der Digitalisierung zu verteidigen.²¹

Was sind die heute zentralen Konfliktfelder?

Nimmt man heutige transatlantische Konfliktfelder in den Blick, sind diese zum einen auf eine teils unterschiedliche Gestaltung der Digitalisierung beidseits des Atlantiks zurückzuführen, zum anderen aber auch auf eine Reihe von Skandalen rund um global agierende US-Technologiekonzerne, welche das politische und öffentliche Bewusstsein für die Ambivalenzen der Digitalisierung weiter geschärft haben. Jenseits der seit Edward Snowden per se umstrittenen geheimdienstlichen Praktiken der USA standen hierbei Datenschutzfragen, Haftungsfragen für veröffentlichte Inhalte auf sozialen Medien, Besteuerungsfragen oder auch Fake News-Kampagnen und Wahlbeeinflussungen im Fokus. Anlass für besonders skeptische Aufmerksamkeit der USA gegenüber der europäischen Digitalpolitik waren der Erlass der europäischen Datenschutzgrundverordnung, das durch den europäischen Gerichtshof aufgehobene *Safe Harbor*-Abkommen, das Netzwerkdurchsetzungsgesetz, die Debatte einer Digitalsteuer bis hin zu Vorschlägen zur Zerschlagung von digitalen Plattformen, hohe Sanktionsstrafen gegenüber US-Digitalfirmen sowie die Einbindung des chinesischen Unternehmens *Huawei* beim Ausbau des 5G-Netzes in Deutschland.²² Fasst man all die angesprochenen Differenzen zusammen und abstrahiert diese, lassen sich gegenwärtig vier digitalpolitische Felder benennen, bei denen Differenzen auftreten. Diese sind

- die Wahrung der Bürgerrechte vor staatlicher Überwachung,
- der Schutz persönlicher Daten der Nutzer von digitalen Plattformen,
- die Besteuerung neuer digitaler und allen voran datenbasierter Geschäftsmodelle sowie
- die Wahrung eines fairen wirtschaftlichen Wettbewerbs in Zeiten der Plattformökonomie.

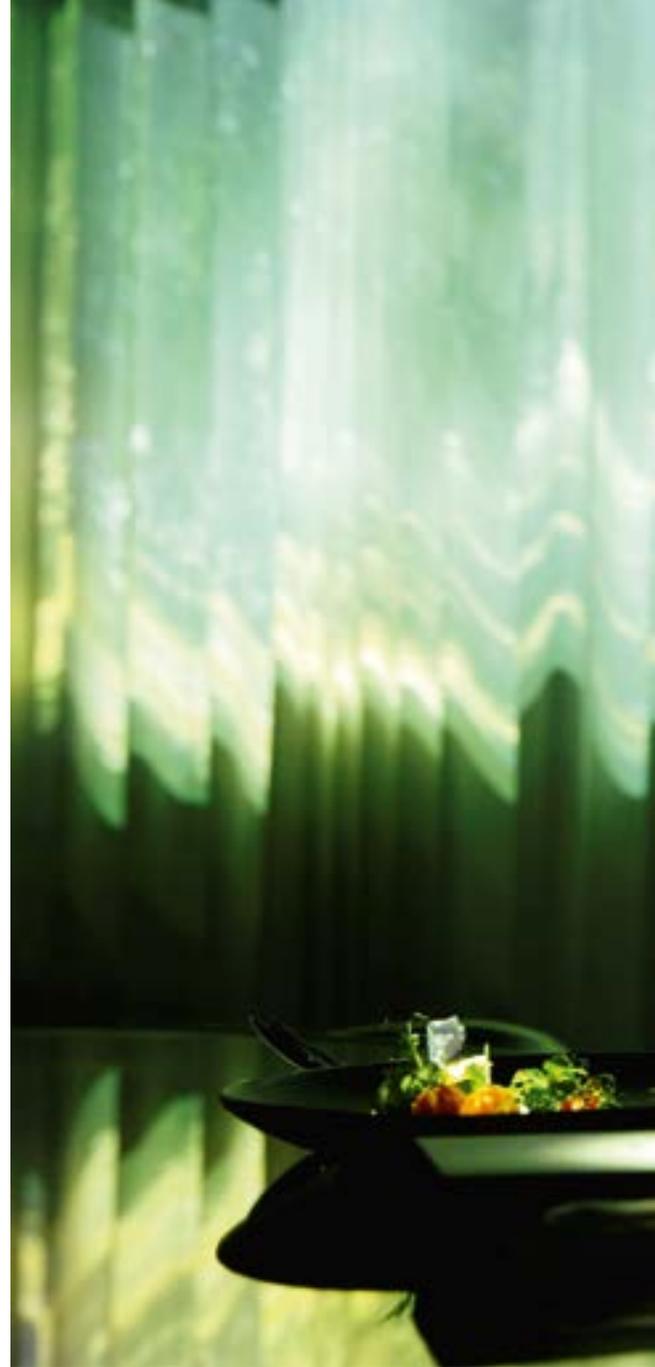
Im Feld der Cybersicherheit existieren zwar durchaus Unterschiede zwischen der europäischen Cybersicherheitspolitik und der US-amerikanischen. Hierbei handelt es sich jedoch weniger um tiefgreifende Differenzen als um unterschiedliche Herangehensweisen und Schwerpunktsetzungen.²³

Internationale Kooperation und die Weiterentwicklung eines internationalen normativen Rahmens sind von hoher Bedeutung im Feld der Cybersicherheit.

Wie tiefgreifend sind die Differenzen eigentlich?

Blickt man eingehender auf die einzelnen Felder, zeigt sich, dass bei den heutigen Differenzen weder fundamental unterschiedliche Weltbilder noch eklatante Interessenkonflikte zum Vorschein kommen. Schließlich lassen sich die Differenzen auf unterschiedliche normative Schwerpunktsetzungen, divergierende Regulierungsansätze und unterschiedliche Ausgangspunkte bei der Digitalisierung zurückführen. Folglich und in Anbetracht der Notwendigkeit transatlantischer Kooperation handelt es sich um Differenzen, die im Rahmen bestehender digitalpolitischer Gesprächsforen ausgeglichen werden können und sollten. Hierbei legen die USA mit einer explorativ-technologiefreundlicheren Disposition die Betonung auf

wirtschaftliches Wachstum sowie nationale Sicherheitsinteressen und verfolgen unter Donald Trump einen stärker wirtschaftsliberalen Ansatz, bei dem Formen der Co- und Selbstregulierung ein Vorzug gegenüber staatlich-legislativer Regelsetzung eingeräumt wird. Da ein Gros der global agierenden digitalen Champions US-Konzerne sind, haben die USA selbstverständlich ein wirtschaftliches und innovationspolitisches Interesse, die wirtschaftliche Freiheit dieser Akteure zu schützen und damit deren Rolle als wichtige Innovationstreiber der Digitalisierung für die USA zu bewahren. Demgegenüber steht ein europäischer Ansatz, der sich zwar intensiver auf den Schutz der Privatsphäre, der Bürgerrechte und die Zukunftsfähigkeit der europäischen Wirtschaft fokussiert und hierzu stärker auf gesetzliche Regulierung von Unternehmen inklusive finanzieller Sanktionsmechanismen setzt. In eine allzu diametrale Gegenüberstellung beider Ansätze sollte man aber dennoch nicht verfallen. Selbstredend wird auch in Europa wirtschaftliches Wachstum und hierfür notwendige unternehmerische Freiheit als Erfolgsfaktor für eine erfolgreiche Gestaltung der Digitalisierung angesehen bzw. ist auch in Europa ein Bewusstsein für die Notwendigkeit der Balance zwischen Regulierung und Innovationsoffenheit vorhanden.²⁴ Dass sich trotz mancher Diskrepanzen bei Sicherheitsfragen im digitalen Raum deutsche, europäische und US-amerikanische Interessen überschneiden, zeigt die Kooperation europäischer Sicherheitsbehörden mit US-Geheimdiensten. Auch die zunehmend intensivere Diskussion der Rolle des chinesischen *Huawei*-Konzerns für den Aufbau des 5G-Netzes zeigt, dass beidseits des Atlantiks ähnliche Sicherheitsrisiken identifiziert werden bzw. sich über geteilte Sicherheitsrisiken eng ausgetauscht wird.²⁵ Blickt man darüber hinaus grundlegend auf die *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* von 2017 und die aktuelle *National Cyber Strategy* der USA, unterstreichen beide Dokumente die hohe Bedeutung internationaler Kooperation im Feld der Cybersicherheit wie auch die Notwendigkeit der Weiterentwicklung eines internationalen normativen Rahmens.²⁶



Was gibt es vor diesem Hintergrund in den nächsten Monaten und Jahren zu beachten?

Gerade mit Bezug auf die Forderung nach einer stärkeren digitalen Souveränität Europas gilt es sich zu vergegenwärtigen, dass die USA trotz vorhandener Differenzen ein notwendiger und



Omnipräsent: Die digitale Durchdringung unserer Lebenswelt wird in Zukunft noch weiter zunehmen.
Quelle: © Kim Kyung-Hoon, Reuters.

wichtiger Partner bleiben, der im Kontrast zu Chinas autoritärem Digitalisierungsmodell mit Europa ein sehr ähnliches Wertefundament teilt. Dies impliziert, dass Deutschland und Europa zusammen mit den USA darauf abzielen sollten, die Gestaltung der Digitalisierung gerade in den Feldern voranzutreiben, wo die Notwendigkeit

nach transatlantischer Kooperation mit geteilten Interessen konvergiert. Gerade mit Blick auf die ordnungspolitische Herausforderung eines digitalen Autoritarismus sollten hierbei jene Risiken gemeinsam adressiert werden, welche die Freiheit, die wirtschaftliche Prosperität und die politische Stabilität des Westens schädigen.²⁷ In den

nächsten Monaten und Jahren gilt aber zu bedenken, dass jenen europäischen Normsetzungen im Feld der Digitalpolitik ein besonderes Maß an Konfliktpotenzial innewohnt, welche explizit auf führende US-Technologiefirmen abzielen und mit dem legitimen Interesse der US-Regierung kollidieren können, diese US-Unternehmen zu schützen. Keineswegs soll jedoch auf Normsetzungen verzichtet werden. Vielmehr leitet sich aus der Erkenntnis des Konfliktpotenzials ein hoher Bedarf nach Dialog und Transparenz ab. Damit einher geht die Forderung nach einem intensiven transatlantischen Austausch bei der Gestaltung der Digitalisierung.

Das EU-US-Privacy Shield-Abkommen dient der Harmonisierung unterschiedlicher Rechtsräume zugunsten des freien Flusses von Daten.

**Wo gibt es bereits Annäherungen?
Wo ist Kooperation nicht nur
notwendig, sondern auch möglich?**

Dass Annäherung nicht nur notwendig, sondern selbst bei umstrittenen Themen möglich ist, zeigt ein Blick in die jüngere Vergangenheit. Nachdem am 6. November 2015 der Europäische Gerichtshof das bis dato bestehende *Safe Harbour*-Abkommen für ungültig erklärt hatte, gelang es den USA und der EU innerhalb nur weniger Monate, ein neues Abkommen zu entwerfen und zu ratifizieren. Bereits am 1. August 2016 konnte damit das neue *EU-US-Privacy Shield*-Abkommen in Kraft treten. Damit gelang es in relativ kurzer Zeit, nicht nur die unterschiedlichen Vorstellungen zum Datenschutz in Einklang zu bringen. Es wurde ebenso ein Instrumentarium geschaffen, um die unterschiedlichen Rechtsräume zugunsten des freien Flusses von Daten zu harmonisieren, ohne sie gänzlich angleichen zu müssen. Auch wenn beidseits des Atlantiks durchaus unterschiedliche Vorstellungen beim Datenschutz existierten, ermöglichte allen voran

die wirtschaftliche Interessenlage eine schnelle Einigung. Blickt man auf die Gegenwart, lassen sich weitere Zeichen finden, dass selbst bei dem Thema Datenschutz Bewegung möglich ist. So ist festzuhalten, dass trotz aller Kritik an der europäischen DSGVO mittlerweile immer mehr bedeutende US-Unternehmen die Richtlinie für ihren gesamten weltweiten Geschäftsbereich übernehmen (z. B. Microsoft, IBM) bzw. Willensbekundungen hierzu verkündet haben (Facebook, Apple). Auf bundesstaatlicher Ebene hat Kalifornien außerdem bereits eine Gesetzgebung erlassen, welche der DSGVO ähnelt. Darüber hinaus mehren sich in letzter Zeit aber auch die Anzeichen, dass in Folge mehrerer Skandale rund um Facebook und der seitens Europas gesetzten DSGVO die jetzige US-Regierung in Erwägung zieht, den Datenschutz auf nationaler Ebene zu stärken.

Blickt man darüber hinaus auf den Umgang des Westens mit China im Digitalbereich, ist hier ebenso Bewegung zu erkennen, da nicht nur die USA seit dem Amtsantritt Donald Trumps eine wesentlich konfrontativere Linie fahren, im Zuge derer unter anderem der Ansatz der US-chinesischen Cyberdiplomatie aus den Zeiten Barack Obamas grundlegend verändert worden ist.²⁸ Auch auf europäischer Seite zeigt sich zunehmend das Bedürfnis, entschlossener gegen den Abfluss strategisch relevanter Schlüsseltechnologien und Innovationen vorzugehen, wie auch gegen Verstöße des Rechts an geistigem Eigentum.²⁹

Ein weiteres Feld, in dem Kooperation möglich und wünschenswert ist, ist der Bereich *Internet Governance*. In diesem Feld stemmen sich die USA, Europa und weitere freiheitliche Partner bereits seit Jahren gegen autoritäre Bestrebungen nach einer alternativen Ordnung des virtuellen Raums. Gemeinsam steht der Westen mit seinen Partnern dabei in verschiedenen Formaten für die liberale Idee eines freien und offenen Internets ein.³⁰ Während Europa gegenwärtig darauf abzielt, die Normentwicklung im Bereich des Cyberspace voranzutreiben,³¹ erfährt der Bereich der Cyberdiplomatie allgemein und *Internet Governance* im Speziellen in den USA

nur wenig Aufmerksamkeit. Dennoch zeigt ein genauerer Blick, dass innerhalb des *U.S. Department of State* die *Internet Freedom Agenda* weiter verfolgt wird und das Thema auch im Blickfeld des US-Senats liegt.³² Zusätzlich haben sich in den letzten Jahren bedeutende US-Unternehmen in diesem Feld aktiv eingebracht, da diese die Gefahr einer zunehmenden, der Wirtschaft schadenden Fragmentierung durch nicht international koordinierte Normsetzungen sehen.³³ Ein in diesem Feld sinnvoller Anknüpfungspunkt wäre weiterhin eine stärkere Verknüpfung der Thematik mit dem Bereich der Cybersicherheit, insofern unter der jetzigen US-Regierung ein Möglichkeitsfenster für Weiterentwicklungen in diesem Bereich zu bestehen scheint.

Ein mahndendes Wort zum Abschluss

Blickt man auf die Gestaltung der Digitalisierung, sind die USA für Deutschland und Europa ein sicherlich nicht immer einfacher, aber letztlich wichtiger Partner. Gerade wenn in Zukunft mal wieder die Rede von einem Mehr an europäischer Selbstbehauptung in Abgrenzung zu den USA die Rede sein sollte, gilt es, sich die geteilten Ordnungsvorstellungen und Interessen einerseits wie auch die Entschlossenheit autoritärer Herausforderer andererseits ins Gedächtnis zu rufen. Man sollte sich diesseits des Atlantiks weniger an einer regulierungsfixierten Abgrenzung zu den USA abarbeiten. Wichtiger sind die Fragen, wie die USA eine solche Vorreiterrolle bei der Digitalisierung einnehmen konnten und welche Lehren Deutschland sowie Europa hieraus für die eigene erfolgreiche Gestaltung der Digitalisierung ziehen können und ziehen müssen.

Sebastian Weise ist Referent für Globale Innovationspolitik der Konrad-Adenauer-Stiftung.

- 1 Vgl. u. a. Damen, Mario / Przetacznik, Jakub 2018: Die Europäische Union und ihre Handelspartner, Europäisches Parlament, 10/2018, in: <https://bit.ly/2AVpHLj> [20.02.2019]; vgl. Hamilton, Daniel S. / Quinlan, Joseph P. 2018: The Transatlantic Economy 2018, Center for Transatlantic Relations, S. VII, in: <https://bit.ly/2T6lNGD> [21.01.2019]; Manyika, James / Lund, Susan / Bughin, Jacques / Woetzel, Jonathan / Stamenov, Kalin / Dhingra, Dhruv 2016: Digital globalization: The new era of global flows, McKinsey Global Institute, 02/2016, in: <https://mck.co/2k8ozxW> [21.01.2019].
- 2 Vgl. u. a. Metzler, Joshua P. 2014: The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment, Brookings Institute, 15.10.2014, in: <https://brook.gs/2FMoFVl> [21.01.2019]; vgl. Mandel, Michael 2017: The Economic Impact of Data: Why Data Is Not Like Oil, Progressive Policy Institute, 12.07.2017, in: <https://bit.ly/2sBwTYy> [21.01.2019].
- 3 Konkret ist die Europäische Union das Ziel von 45 Prozent aller *digitally derivable service exports* der USA und gleichzeitig die Quelle für 46 Prozent der US-Importe in diesem Bereich. Die aus den USA importierten digitalen Güter und Dienstleistungen werden in Europa zu 53 Prozent wiederum für die Produktion von Gütern und Dienstleistungen genutzt, die anschließend wieder exportiert werden. Ein weiteres Beispiel für die digitalwirtschaftliche Vernetzung ist der Onlinehandel. Allein in Deutschland nutzen 48 Prozent aller Onlinekäufer US-amerikanische E-Commerce-Anbieter, während parallel 49 Prozent der Onlinekäufer aus den USA auf europäische Anbieter zurückgreifen. Der Umstand, dass gegenwärtig mehr als 4.000 US-Unternehmen unter dem US-EU-*Privacy Shield* registriert sind – so dass personenbezogene Daten aus der EU relativ einfach in die USA transferiert werden können –, unterstreicht die enge digitale und wirtschaftliche Verflechtung letztlich ebenso. Vgl. u. a. Hamilton / Quinlan 2018, N. 1, S. 24–26; vgl. Suominen, Kati 2017: Where the Money Is: The Transatlantic Digital Market, Center for Strategic & International Studies, 12.10.2017, in: <https://bit.ly/2W9vxd> [21.01.2019]; vgl. U.S. Department of Commerce 2018: Privacy Shield List, Stand 06.12.2018, in: <https://bit.ly/2b0ljdq> [21.01.2019].
- 4 Vgl. Hamilton / Quinlan 2018, N. 1, S. 24.
- 5 Vgl. ebd., S. 24 f.
- 6 Zu nennen wären hier insbesondere die *Big Four* der Digitalisierung Google (Alphabet), Apple, Amazon und Facebook. Für Nutzer- und Umsatzstatistiken der *Big Four* siehe konkret für Facebook: Statista 2018: Soziale Netzwerke, in <https://bit.ly/2MleaJP> [21.01.2019]; für die Zahlen zu Google: Statista 2018: Google, in: <https://bit.ly/2MoIxio> [21.01.2019]; für die Zahlen zu Amazon: Statista 2018: Amazon, in: <https://bit.ly/2HqaKa1> [21.01.2019]; für die Zahlen von Apple: Statista 2018: Apple, in: <https://bit.ly/2FF0FnO> [21.01.2019].

- 7 Für amerikanische Unternehmen – die zugleich in dem Innovationsökosystem der USA eine herausragende Rolle spielen – ist Europa sowohl als Absatzmarkt wie auch als Datenpool von hoher Bedeutung.
- 8 Vgl. u. a. Internationaler Währungsfonds 2018: China's Economic Outlook in Six Charts, 26.06.2018, in: <https://bit.ly/2UTuSUu> [21.01.2019].
- 9 Vgl. Layne, Christopher 2018: The US-Chinese Power Shift and the end of the Pax Americana, in: *International Affairs* 94: 1, S.95.
- 10 Wichtige Zukunftstechnologien sind hierbei z. B. Künstliche Intelligenz, Quantencomputing, Autonome Systeme, Big Data, Gen- und Biotechnologie, Erneuerbare Energien. Vgl. u. a. Fischer, Sophie-Charlotte 2018: Artificial Intelligence: China's High-Tech Ambitions, *CSS Analyses in Security Policy* 220, 02/2018, in: <https://bit.ly/2Ho1GCl> [21.01.2019].
- 11 Vgl. u. a. Beckley, Michael 2012: China's Century? Why America's Edge Will Endure, *International Security* 36: 3, S. 42–78.
- 12 Während China seinen eigenen digitalen und technologischen Markt unter anderem mit Verweis auf Sicherheitsinteressen (Informationssicherheit) abschottet, engagiert es sich aktiv in der westlichen Digitalwirtschaft, forciert den Abfluss von digitalen Schlüsseltechnologien sowie Innovationen und schreckt auch vor Industriespionage und der Verletzung geistigen Eigentums keineswegs zurück. Vgl. Segal, Adam/Hoffmann, Samantha/Hanson, Fergus, Uren, Tom 2018: Hacking for ca\$h: Is China still stealing Western IP, *Australian Strategic Policy Institute*; vgl. Shalal, Andrea 2018: Germany risks losing key technology in Chinese takeovers – spy chief, *Reuters*, 11.04.2018, in: <https://reut.rs/2Mni0Ci> [21.01.2019].
- 13 Vgl. u. a. Burgers, Tobias/Robinson, David R. S. 2018: Networked Authoritarianism Is on the Rise, in: *Sicherheit und Frieden* 34: 4, S. 248–252; vgl. Mitchell, Anna/Diamond, Larry 2018: China's Surveillance State Should Scare Everyone, *The Atlantic*, 02.02.2018, in: <https://bit.ly/2DZ0hMy> [21.01.2019]; vgl. *The Economist* 2018: China has turned Xinjiang into a police state like no other, 31.05.2018, in: <https://econ.st/2JkTBy5> [21.01.2019].
- 14 Vgl. u. a. Wright, Nicholas 2018: How Artificial Intelligence Will Reshape the Global Order, *Foreign Affairs*, 10.07.2018, in: <https://fam.ag/2uKfxtD> [21.01.2019]; vgl. Benaim, Daniel/Gilman, Hollie R. 2018: China's Aggressive Surveillance Technology Will Spread Beyond Its Borders, *Slate*, 09.08.2018, in: <https://bit.ly/2Mu4Ouv> [21.01.2019].
- 15 Vgl. u. a. Weber, Valentin 2018: The Rise of China's Security-Industrial Complex, *Blog Post Digital and Cyberspace Policy Program des Council on Foreign Relations*, 17.07.2018, in: <https://on.cfr.org/2FF1Eo0> [21.01.2019]; vgl. Romaniuk, Scott N./Burgers, Tobias 2018: How China's AI Technology Exports Are Seeding Surveillance Societies Globally, *The Diplomat*, 18.10.2018, in: <https://bit.ly/2TYOLIJ> [21.01.2019].
- 16 Vgl. u. a. Hohmann, Mirko/Benner, Thorsten 2018: *Getting Free and Open Right: How European Internet Foreign Policy Can Compete in a Fragmented World*, *Global Public Policy Institute*, S. 10–17. Für eine spezifische Betrachtung Russlands siehe Nocetti, Julien 2015: Contest and conquest: Russia and global internet governance, in: *International Affairs* 91: 1, S. 111–130; für China, siehe Sacks, Samm 2018: China's Emerging Cyber Governance System, *CSIS*, in: <https://bit.ly/2RHwLGO> [21.01.2019]; Sacks, Samm 2018: Beijing Wants to Rewrite the Rules of the Internet, *The Atlantic*, 18.06.2018, in: <https://bit.ly/2REXcxf> [21.01.2019].
- 17 Vgl. u. a. Clinton, Hillary 2010: Remarks on Internet Freedom, 21.01.2010, in: <http://bit.ly/2MkqjXe> [21.01.2019]; vgl. Lynch, Marc 2010: The Internet Freedom Agenda, *Foreign Policy*, 22.01.2010, in: <https://bit.ly/2WfFEFs> [21.01.2019]; vgl. Europäische Kommission 2013: *Internet Freedom*, 08.03.2013, in: <https://europa.eu/!rp48kF> [14.02.2019].
- 18 Der damalige deutsche Verkehrs- und Internetminister Alexander Dobrindt plädierte etwa dafür, dass anlässlich der Enthüllungen Deutsche und Europäer grundlegend ihre digitale Souveränität gegenüber den USA zurückgewinnen müssten. Vgl. Backhaus, Michael/Lambeck, Martin S./Uhlenbroich, Burkhard 2013: Minister Dobrindt gibt die Richtung vor. „Wir brauchen das schnellste Internet der Welt“, *Interview, Bild*, 22.12.2013, in: <https://bild.de/-33955848.html> [14.02.2019]; siehe darüber hinaus hierzu grundlegend Gueham, Farid 2017: *Digital Sovereignty*, *Fonation pour l'innovation politique*, S. 9, 13, in: <https://bit.ly/2R2XiIG> [21.01.2019].
- 19 Vgl. u. a. Bendiek, Annegret/Berlich, Christoph/Metzger, Tobias 2015: Die digitale Selbstbehauptung der EU, *SWP-Aktuell* 71, 08/2015, in: <http://bit.ly/2SwB07R> [14.02.2019]; vgl. Bitkom 2015: *Digitale Souveränität: Positionsbestimmung und erste Handlungsempfehlungen für Deutschland und Europa*, in: <https://bit.ly/2T5yEsN> [21.01.2019]; vgl. Gueham 2017, ebd.; vgl. Hackenbroich, Jonathan 2018: *Reality bytes: Europe's bid for digital sovereignty*, *ECFR*, 17.10.2018 in: <https://bit.ly/2j64nFV> [21.01.2019].
- 20 Zentrale Bausteine hierbei sind unter anderem ein geeinter europäischer digitaler Binnenmarkt, die Schaffung eines europäischen Forschungs-, Entwicklungs- und letztlich auch europäischen Innovationsökosystems auf Spitzenniveau, ein Mehr an technischer Souveränität bis hin zur Infrastruktur im Cyberspace, ein integrierter europäischer Datenraum, eine eigenständige europäische Regulierung sog. digitaler Plattformen und eine faire Besteuerung datenbasierter Geschäftsmodelle.
- 21 Vgl. u. a. *Internet Governance Forum* 2018: *IGF 2018 Speech by French President Emmanuel Macron*, 2018, in: <https://bit.ly/2U8pvzQ> [21.01.2019]; vgl. Hackenbroich 2018, N. 19.

- 22 Vgl. u. a. Lewis, Patricia / Parakilas, Jacob / Schneider-Petsinger, Marianne / Smart, Christoph / Rathke, Jeffrey / Ruy, Donatienne 2018: *The Future of the United States and Europe: An Irreplaceable Partnership*, Chatham House, 11.04.2018, S. 11–15.
- 23 Vgl. u. a. U.S. Chamber of Commerce 2018: *Transatlantic Cybersecurity Report: Forging a United Response to Universal Threats*, in: <https://uscham.com/2FNX99U> [21.01.2019]; vgl. Lewis et al., ebd., S. 15–21, 25–26.
- 24 Vgl. u. a. European Political Strategy Centre 2016: *Towards an Innovation Principle Endorsed by Better Regulation*, 30.06.2016, in: <https://bit.ly/2nbBRci> [21.01.2019]; Ausführungen im Rahmen der EU *Single Market Strategy*: Europäische Kommission, Internal Market, Industry, Entrepreneurship and SMEs. Industry. Innovation, in: <https://bit.ly/2fk9a5l> [21.01.2019].
- 25 Vgl. u. a. Heide, Dana / Scheuer, Stephan 2019: *Sorge um Datensicherheit – Berlin erwägt, Huawei beim Netzausbau auszusperrern*, Handelsblatt, 17.01.2019, in: <https://bit.ly/2HhVc88> [21.01.2019]; vgl. Böhm, Markus 2018: *USA warnen vor Chinas Einfluss auf 5G-Netz*, Spiegel Online, 29.11.2018, in: <http://spon.de/afmZV> [14.02.2019].
- 26 Vgl. The White House 2017: *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, 11.05.2017, in: <https://bit.ly/2tg9vmu> [21.01.2019]; vgl. The White House 2018: *National Cybersecurity Strategy*, S. 20.
- 27 Um einen Überblick über mögliche Partner zu gewinnen, ist ein Blick auf die *Freedom Online Coalition* sinnvoll, bei der sich 30 Staaten zugunsten des freien und offenen Internets zusammengeschlossen haben, siehe Freedom Online Coalition, in: <https://freedomonlinecoalition.com> [14.02.2019].
- 28 Vgl. u. a. Miles, Tom 2018: *U.S. and China clash over 'technology transfer' at WTO*, Reuters, 28.05.2018, in: <https://reut.rs/2FGOKaZ> [21.01.2019]; vgl. Fidler, David P. 2018: *U.S. Cyber Diplomacy Requires More than an Office*, Council on Foreign Relations, 26.07.2017, in: <https://on.cfr.org/2FGOSY1> [21.01.2019].
- 29 So hat die EU auch in Absprache mit den USA bei der WTO im Jahr 2018 einen Fall gegen China wegen unfairer Praktiken des Technologieabflusses eröffnet, sich auch 2018 wie in der Vergangenheit immer wieder explizit über chinesische Verstöße gegen das Recht an geistigem Eigentum beschwert und Ende 2018 auf Initiative Frankreichs, Deutschlands und Italiens auch eine Verordnung zur Überprüfung ausländischer Direktinvestitionen auf den Weg gebracht, die in Zukunft gerade den Abfluss wichtiger digitaler Schlüsseltechnologien und Innovationen nach China verhindern soll.
- 30 Für einen ersten Überblick über europäische und US-amerikanische Bekenntnisse zu dem freien und offenen Internet und den dabei zentralen Prinzipien in diversen Strategiedokumenten siehe z. B. Morgus, Robert / Sherman, Justin 2018: *The Idealized Internet vs. Internet Realities (Version 1.0)*, S. 10–13.
- 31 Zugunsten einer Weiterentwicklung des normativen Rahmens im Cyberspace engagiert sich Europa aktiv u. a. innerhalb der G7 / G8, im Rahmen der UN GGE (Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security), sowie auch bei dem „Paris Call for Trust and Stability“, den Emmanuel Macron auf dem diesjährigen Internet Governance Forum vorstellte, und der Unterstützung der aktuell zirkulierenden „Contract for the web“-Initiative.
- 32 Vgl. Segal, Adam 2018: *The Internet Freedom Agenda: Not Dead, but Not Exactly Thriving Either*, Council on Foreign Relations, Digital and Cyberspace Policy Program, 21.05.2018, in: <https://on.cfr.org/2ISw7QR> [14.02.2019].
- 33 Dass gerade auch US-Unternehmen hier aktiv sind, zeigt sich unter anderem an den Initiativen von Microsoft im Bereich Cybersicherheit wie auch an der Unterzeichnung des „Paris Call for Trust and Stability“ durch US-Unternehmen.