Autoritäre Modelle der Internetregulierung: Chinas Vorstoß in den digitalen Raum und Implikationen für liberale Demokratien

Julia Gurol

Einleitung: Chinas Digitaloffensive

Chinas digitale Offensive im In- sowie im Ausland stelle eine wachsende Herausforderung für westliche, liberale Demokratien dar. Das betrifft nicht mehr nur die repressive Regulierung des Internets innerhalb der Volksrepublik oder den chinesischen Export digitaler Technologien, Überwachungssoftware und Künstlicher Intelligenz, sondern zunehmend auch den Versuch, dem offenen und freien Internet ein autoritäres Gegenmodell entgegenzusetzen und dieses international zu exportieren. Damit ist die Volksrepublik China zwar bei weitem nicht alleine – auch Russland, Iran und andere autoritäre Staaten bemühen sich um eigene Modelle der Internet- und Datenregulierung sowie deren bilateralen und multilateralen Export – doch mit Abstand der aktivste und organisierteste Akteur. Schon längst gilt die chinesische „Great Firewall" als das umfassendste und dadurch auch restriktivste System der Onlinezensur weltweit.[1]

Während diese Prozesse nicht zuletzt seit dem Beginn der Implementierung der digitalen Seidenstraße (Digital Silk Road, 数字丝绸之路 *shuzi sichou zhi lu*) an Fahrt aufgenommen haben, stellte insbesondere die Corona-Pandemie ein weiteres Möglichkeitsfenster für die Volksrepublik dar, mit dem Argument der Nachverfolgung von Infektionsketten sowie der Pandemiebekämpfung, sowohl innerhalb des eigenen Landes im großen Stil Daten zu sammeln, und gleichzeitig eigene Technologien an andere Staaten zu exportieren. Dies wird an späterer Stelle in diesem Kapitel anhand der Verflechtungen zwischen China und den Vereinigten Arabischen Emiraten (VAE) im digitalen Sektor veranschaulicht. Die Gesundheitsseidenstraße (Health Silk Road, 健康丝绸之路 *jiankang sichou zhi lu*), die auf dem Höhepunkt der ersten globalen Infektionswelle im Frühjahr 2020 offiziell verabschiedet wurde, beispielsweise, soll eng mit der digitalen

1 Griffiths, 2019.

Seidenstraße verflochten sein. Dies trug zu einer Verbreitung chinesischer digitaler Technologien bei – die Volksrepublik China entwickelte sich damit zu einer zentralen Lieferantin von Überwachungstechnologien, CCTV Equipment, sowie Künstlicher Intelligenz.[2] Kurz: der chinesische Techno-Autoritarismus stellt eine wachsende Herausforderung für liberale Demokratien dar – nicht nur im Bereich der Technologiediffusion sondern zunehmend auch im Internet. Der folgende Beitrag skizziert den chinesischen Vorstoß in den digitalen Raum im Bereich Technologieexport sowie Internetregulierung und stellt die Herausforderung für liberale Demokratien dar, diesen Tendenzen stärkere, eigene Modelle entgegenzusetzen.

Das folgende Kapitel widmet sich dem Thema der Internetregulierung sowie dem Export eines autoritären Gegenmodells zum freien, offenen und weitgehend unregulierten Internet als Mechanismus zur Wahrung autoritärer Stabilität. Der Fokus der Betrachtung liegt dabei auf der Volksrepublik China als „Pionier" der Internetregulierung. Zunächst erfolgt eine kurze Darstellung, welche Rolle die Regulierung des Internets für innenpolitische Stabilität autoritärer Regime bedeutet. Darauf aufbauend folgt eine Diskussion des Exports autoritärer Regulierungsmodelle, die anhand des Beispiels chinesisch-emiratischer Verflechtungen im digitalen Sektor veranschaulicht werden soll. Abschließend nimmt das Kapitel die daraus entstehenden Herausforderungen für liberale, westliche Demokratien in den Blick und skizziert Herausforderungen und Handlungsmöglichkeiten.

Internetregulierung als Mechanismus zur Wahrung autoritärer Stabilität

Die politikwissenschaftliche Forschung zur Stabilität autoritärer Regime unterscheidet zwischen drei Säulen der innenpolitischen Stabilität: 1) Legitimation, 2) Ko-optation sowie 3) Repression.[3] Bei letzterer wird zudem zwischen „high intensity repression" und „low intensity repression" unterschieden[4]. High intensity repression beinhaltet sichtbare Maßnahmen gegen Oppositionelle oder politische Organisationen, wie beispielsweise die Zerschlagung von Massendemonstrationen oder politische Attentate. Oft kommt es dabei auch zur Anwendung von Gewalt. Low intensity repression dagegen, zielt auf die Einschränkung bürgerlicher Freiheiten ab und ist damit subtiler und weniger sichtbar – allerdings nicht weni-

2 Demmelhuber et al., 2022.
3 Gerschewski, 2013.
4 Levitsky und Way, 2002.

ger weitreichend. Low intensity repression beinhaltet auch die gezielte und von oben gesteuerte Einschränkung der Informations- und Meinungsfreiheit, da ein freier und unkontrollierter Fluss an Informationen als Bedrohung für das Regime wahrgenommen wird. Überwachung und Propaganda waren daher schon immer ein zentraler Bestandteil autokratischer Regime. Und nicht zuletzt seit dem sogenannten Arabischen Frühling ist klar: das Internet schafft Transparenz und bietet Mobilisierungspotential. Gleichzeitig stellen digital Technologien jedoch auch eine Möglichkeit für autokratische Akteure dar, die Möglichkeit, Unterdrückung und Kontrolle viel durchdringender, effizienter und subtiler zu gestalten. Immer mehr autoritäre Regime vertreten daher die Annahme, dass eine Kontrolle des Internets kritisch für ihren Machterhalt ist.[5]

Dies ist auch ein zentraler Bestandteil von Xi Jinpings Vision einer datengestützten Regierungsführung. Der Versuch, das Internet zu überwachen und Inhalte zu zensieren, hat in China somit innenpolitische Wurzeln und dient nicht zuletzt der Machtmanifestation der Kommunistischen Partei unter dem amtierenden Präsidenten Xi Jinping. Ein freier, unzensierter Informationsfluss sowie der uneingeschränkte Zugang der Bevölkerung zur Informationen im Netz werden dabei als zentrale Bedrohung für die Stabilität der Partei angesehen[6]. Daher hat die Kommunistische Partei eine eigene Version fast aller Internetdienste entwickelt. Statt Twitter gibt es den Mikroblogging-Dienst Sino Weibo, statt Google wird die Suchplattform Baidu benutzt und als Alternative zu Facebook oder WhatsApp gilt der Instant-Messenger WeChat. Alle anderen gängigen Netzwerke werden durch die sogenannte Great Firewall blockiert. Dies hat, aus der Perspektive des Regimes, den Vorteil, Inhalte und Nutzungsverhalten kontrollieren und zudem in großem Stil Daten sammeln zu können.[7]

Im 14. Fünfjahresplan (2021-2025) für die Digitalwirtschaft erklärte die Volksrepublik Daten sogar zu „kritischen Produktionsfaktoren" und unterstellt sie daher einer zentralisierten Planung – ein weiterer Schritt der Volksrepublik in Richtung Pionier der Datenregulierung.[8] Desweiteren nennt der Plan Schlüsselbereiche wie High-End-Chips, Betriebssysteme sowie Schlüsselalgorithmen für künstliche Intelligenz und Sensoren als besonders zentral. Eine wichtige Rolle kommt damit auch Unternehmen

5 Gunitsky, 2015.
6 Interview, geführt am 26. Februar 2019, in Shanghai.
7 Stockmann und Gallagher, 2011.
8 Grünberg und Brussee, 2021.

wie Huawei oder Hikvision, über deren Netze und Server in großem Stil Daten gesammelt und gespeichert werden und deren modernste Technologie die Erstellung und Analyse riesiger Datensätze möglich machen.[9] Doch der chinesische Sicherheitsapparat profitiert nicht nur von den engen Beziehungen zu chinesischen Technologieunternehmen, insbesondere Huawei, SenseTime, Hikvision, iFlytek und Megvii, sondern auch von einem Umfeld, in dem es weder Datenschutzgesetze noch Möglichkeiten gibt, sich bei den Behörden zu beschweren, noch Umfragen, bei denen man seinem Ärger Ausdruck verleihen kann. Da die Beziehungen zwischen der chinesischen Regierung und dem Privatsektor immer komplexer werden, könnte Peking auch den privaten chinesischen Technologiesektor dazu zwingen, Technologien zu entwickeln, die speziell dazu dienen, neue Formen gesellschaftlicher Kontrolle auszuüben.[10]

Dies passiert jedoch nicht nur in Form einer Einschränkung der Informations- oder Meinungsfreiheit vonseiten der Kommunistischen Partei, sondern auch durch vermeintlich subtilere aber nicht minder wirksamen Anreizsysteme, wie das bereits viel diskutierte Sozialkreditsystem Chinas – der sogenannte „citizen score" – das ebenfalls zur Datensammlung beiträgt, dieser jedoch ein positives Image verpassen soll. Kaufverhalten, soziales Engagement, Chatverläufe, GPS-Daten – durch das Sozialkreditsystem entsteht eine gläserne Bürgerschaft gewissermaßen qua Zuckerbrot und Peitsche. Wer sich beispielsweise in der Nachbarschaft engagiert, bekommt Pluspunkte, wer dagegen eine rote Ampel übersieht oder eine Rechnung zu spät bezahlt, bekommt Punkte abgezogen. Jede Alltagshandlung der Bürgerinnen und Bürger wird somit erfasst und anhand einer Sozialtauglichkeitsskala erfasst und bewertet. Was öffentlich durch die Kommunistische Partei als eine Art freiwillige Erziehung des chinesischen Volkes propagiert wird, dient letztlich der Datenbegehrlichkeit der politischen Führung sowie Xi Jinpings Vision, eine datengestützte Regierungsführung zu etablieren.[11]

9 Benner und Hohmann, 2018.
10 Lamenesch, 2021.
11 Drinhausen und Brussee, 2022.

Export eines autoritären Gegenmodells zum freien und offenen Internet als Mechanismus der Autokratieförderung

Repression (und damit auch die Einschränkung der Meinungsfreiheit) als zentrale innenpolitische Säule autoritärer Stabilität ist weitgehend erforscht[12] – ihre Ausweitung in den digitalen Raum im Kontext der steigenden Bedeutung des Internets somit wenig überraschend. Neu ist jedoch die internationale Verbreitung autoritärer Modelle der Internetregulierung. Zu dieser internationalen Dimension autoritärer Staaten werden in der politikwissenschaftlichen Forschung vier Mechanismen unterschieden, bei denen jeweils entweder das Senderland, das Empfängerland oder beide aktiv agieren. Daraus ergeben sich die in der folgenden Tabelle dargestellten Konstellationen (siehe Tabelle 1).

		Akteur	
		Senderland	Empfängerland
Direkter Einfluss	Autokratieförderung	✓	
	Kooperation	✓	✓
Indirekter Einfluss	Lernen/Nachahmung		✓
	Diffusion		

Tabelle 1: Internationale Dimensionen von Autoritarismus, dargestellt nach Bank und Josua, 2017.[13]

Bei einer *Autokratieförderung* („autocracy promotion")[14] geht es um eine „direkte, gezielte Unterstützung und Stärkung autoritärer Regime durch einflussreiche Groß- und Regionalmächte" [15], wie beispielsweise durch China. Im Sinne einer Autokratieförderung bzw. eines Autokratieexports geht es also darum, ein bestimmtes Modell der Internetregulierung bilateral oder multilateral zu verbreiten. Alternativ arbeitet China, ebenfalls als aktives Senderland, in *Kooperation* mit anderen Autokratien („autocratic collaboration") gemeinsam an autoritären Gegenentwürfen. Nicht selten treten zudem sogenannte *Diffusionseffekten* („autocratic diffusion")[16] auf, also weitgehend nichtintendierte, unkoordinierte und kaum zentral ge-

12 Keremoğlu und Weidmann, 2020.
13 Bank und Josua, 2017
14 Bader und Kästner, 2013.
15 Bank und Josua, 2017
16 Ambrosio, 2010.

steuerte Prozesse. Ein Beispiel dafür wäre die Verbreitung staatlicher Einschränkungen des Internetaktivismus durch Diffusionsprozesse. Nicht selten kommt es darüber hinaus zu sogenannten Nachahmungseffekten beziehungsweise *Lernprozessen* („autocratic learning/emulation"), bei denen es zu einer Übernahme und Implementierung von politischen Strategien und Taktiken anderer Autokratien kommt. Durch die Entwicklung Chinas zu einem Vorreiter in Sachen Digitalisierung und technologischer Innovation, sind diese Nachahmungseffekte in den vergangenen beiden Jahrzehnten deutlich stärker geworden. Dies wird oft auch als Verbreitung eines „digitalen Autoritarismus" (digital authoritarianism) bezeichnet.[17]Der Aufstieg Chinas zur digitalen Großmacht hat somit verheerende Folgen für das globale Internet. Denn die Volksrepublik hat längst damit begonnen, ihre eigenen Modelle der Informationskontrolle international erfolgreich zu vermarkten – ihre Führungsrolle im Technologiesektor spielt ihnen dabei in die Hände. Im Kontext der digitalen Seidenstraße exportiert China seine Digitaltechnik und Software bereits jetzt in die ganze Welt.

In Chinas White Paper vom März 2015 wurde die digitale Konnektivität zur obersten Priorität erklärt – in diesem Kontext investiert China international in Glasfaserkabel, baut Datenzentren, die von Peking als „grundlegende strategische Ressource"[18] bezeichnet werden und errichtet damit nach und nach ein digitales Ökosystem, in welches die Länder, die Teil der digitalen Seidenstraße sind, involviert werden.[19] So werden international bereits chinesische Algorithmen für die Entwicklung von Apps zur Nachverfolgung von Bewegungsprofilen genutzt und kommen chinesische Technologien bereits in Smart-City Projekten weltweit zum Einsatz – auch mitten in Europa. Der Belgrader Platz in Serbien beispielsweise steht unter dauerhafter Kamerüberwachung durch ein in China hergestelltes und von dem chinesischen Technologiekonzern Huawei installiertes Überwachungskamerasystem. Diese Beispiele zeigen: Was China im eigenen Land verfeinert hat, exportiert es nun auch ins Ausland.

2019 schlugen gar Forschende von Huawei, China Unicom und dem Ministerium für Industrie und Informationstechnik der Volksrepublik China bei der Internationalen Fernmeldeunion (ITU) eine weitreichende Reform des Internet-Protokolls vor.[20] Dies birgt Gefahren für Meinungsfreiheit, Datensicherheit und, ganz generell, für das freie, offene und

17 Shahbaz, 2018.
18 National Development and Reform Commission, 2016.
19 Russell und Berger, 2020; Hart, 2019.
20 Holz, 2022.

interoperable Internet weltweit und erfordert somit eine stärkere multilaterale Standardsetzung durch liberale Demokratien in den Bereichen Datenschutz, Netzwerkregulierung sowie Kuratierungsalgorithmen.

„China goes global": Chinesisch-Emiratische Verflechtungen im Bereich der Überwachungstechnologie[21]

Eines der illustrativsten Beispiele an der Schnittstelle zwischen der Diffusion autoritärer Praktiken im digitalen Raum sowie der aktiven Verbreitung von Technologien stellen die Verflechtungen zwischen der Volksrepublik China und den Vereinigten Arabischen Emiraten dar, dies insbesondere seit dem Ausbruch der Corona-Pandemie an Fahrt aufgenommen haben.[22] Dabei stehen drei chinesisch-emiratische Netzwerke im Fokus, deren verbindendes Element das emiratische Firmenkollektiv Group 42 (kurz: G42) darstellt. G42 ist ein führendes Unternehmen für künstliche Intelligenz und Cloud-Computing, das 2018 in Abu Dhabi gegründet wurde und seitdem mehrere Unterauftragnehmer und Tochtergesellschaften gegründet hat. Im Laufe der Zeit hat sich G42 zu einem der wichtigsten Knotenpunkte für die autoritäre Zusammenarbeit zwischen China und den VAE entwickelt und steht exemplarische für transregionale Elitenetzwerke, die ausgeprägte Machtbeziehungen zwischen der politischen und wirtschaftlichen Elite Chinas mit und innerhalb der Al Nahyan, der Herrscherfamilie in Abu Dhabi, umfassen.[23] Während der Corona-Pandemie kam es zu einer Diffusion autoritärer Praktiken und Technologien innerhalb dieses Netzwerks, mit der chinesischen Firma Beijing YeeCall Interactive Network Technology als „Sender" und zwei Tochterfirmen von G42, namens Breej Holding Ltd. und ToTok Technology, als „Empfängern". Breej Holding Ltd. und ToTok Technology waren aktiv an der Entwicklung und Programmierung der emiratischen Voice over IP (VoIP) und Chat App ToTok beteiligt, die während der Pandemie zur weitreichenden Kontrolle und Überwachung ihrer Nutzer und Nutzerinnen diente. ToTok basiert nicht nur auf demselben Algorithmus wie die chinesische Tracing App YeeCall (一块), dieser wurde von den Entwicklern von ToTok sogar ko-

21 Die im folgenden Kapitel dargestellten Informationen sind Teil eines von der Volkswagen-Stiftung geförderten Forschungsprojekts zu „Global autocratic collaboration in times of COVID-19: Game changer of business as usual in Sino-Gulf relations?" (Förderzeitraum 2021-2022).

22 Gurol et al., 2022.

23 Demmelhuber et al., 2022.

piert und an den emiratischen Kontext angepasst – klare Evidenz für eine Nachahmung chinesischer Modelle der Repression und Kontrolle im digitalen Raum.[24] Beide Apps greifen auf Geo-Daten, Bewegungsprofile, Fotos und Kontaktdaten der Nutzerinnen und Nutzer zu und sammeln damit weit mehr Daten, als für eine Nachverfolgung im Sinne der Pandemiebekämpfung notwendig wäre.

Dass es sich bei G42 nicht einfach um ein reguläres Unternehmen handelt, das auf der Suche nach Profit und innovativen Ideen international Ausschau hält, zeigt die Gründungsgeschichte des Firmenkollektivs. Vor der offiziellen Gründung von G42, operierten ähnliche Strukturen und Akteure unter einem anderen Namen, DarkMatter. Die sogenannte DarkMatter Group wurde 2015 gegründet, von der emiratischen staatlichen Aktiengesellschaft Mubadala mit Hauptsitz in Abu Dhabi finanziert, und erlangte insbesondere durch die digitalen Angriffe auf Dissidentinnen und Dissidenten sowie Kritikerinnen und Kritikern des emiratischen Regimes an internationaler Bekanntheit. Im Jahr 2019 wurde DarkMatter jedoch endgültig durch den emiratischen Staat aufgelöst, bedingt durch die wachsende öffentliche Kritik. Dennoch operieren zentrale Akteure und Strukturen weiter – nun unter dem Namen der Group42, von der sie nahezu eins zu eins übernommen wurden.[25] Dies zeigt, dass Chinas Modelle der Datensammlung, Kontrolle und Unterdrückung – insbesondere im digitalen Raum – international längst Nachahmende gefunden hat. Desweiteren legt es die Bedeutung digitaler Infrastruktur im Bereich der aktiven Verbreitung aber auch der unintendierten, unkontrollierten Diffusion autoritärer Praktiken dar.[26]

Herausforderungen und Handlungsoptionen für liberale Demokratien

Noch im Jahr 2000 beschrieb der damalige Präsident der Vereinigten Staaten, Bill Clinton, den Versuch das Internet zu regulieren, als vergleichbar schwierig wie „einen Pudding an die Wand zu nageln". Dies zeigt nicht nur Kontinuitäten zur amerikanischen Deregulierungspolitik der 1990er Jahre, die heute weitgehend überholt scheint, sondern wird durch die restriktive Regulierung des Internets durch die Kommunistische Partei in China ganz klar widerlegt – hier wurde der Pudding bereits an die

24 Marczak, 2020.
25 Intelligence Online, 2021.
26 Gurol und Schütze, im Erscheinen.

Wand genagelt. Das Erstarken autoritärer Regime wie China und ihr zunehmender Versuch, dem offenen und freien Internet ein autoritäres Modell entgegenzusetzen, stellt somit eine große Herausforderung für liberale Demokratien dar, ihre eigenen Modelle zu revidieren und über die Notwendigkeit demokratischer Regulierung nachzudenken. Die auf dem libertären Modell der 1990er Jahre beruhende Prämisse, der Staat solle sich aus der Regulierung des Internets so weit wie möglich heraushalten, scheint in seiner Ursprungsform nicht mehr zeitgemäß und dem Wettbewerb mit dem autoritären Gegenmodell nicht gewachsen. Kurz: auch in Demokratien benötigt es Regulierungsmodelle, allerdings solche die demokratisch legitimiert sind und unter Beteiligung einer Vielzahl an Akteuren – staatlichen wie privaten – entwickelt werden. Diese sollten sich auf alle vier Ebenen der Internetregulierung beziehen: 1) Die *infrastrukturelle* Ebene, die Hardware, welche die Grundstruktur des globalen Netzes bildet also Glasfaserkabel, Router oder Server, 2) die *logische* Ebene, die technische Normen und Standards beinhaltet, 3) die *Anwendungsebene* mit Software-Anwendungen, Systemen und Website sowie 4) die *inhaltliche* Ebene, also Text, Bild, Ton, und Video sowie virtuelle Realitätswelten.[27]

Problematisch ist dabei, dass die Internetkommunikation in freien Gesellschaften häufig von privaten Technologieunternehmen kontrolliert wird. Regierungen dagegen fehlt es oft an technischem Fachwissen über die sich schnell entwickelnden Technologien. Der digitale Autoritarismus gedeiht unbestreitbar in einem Umfeld schwacher Regierungsführung und schwacher Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor.[28] Es bedarf demnach einer verstärkten intergouvernementalen, also zwischenstaatlichen, sowie Multistakeholder-Koordinierung, um die digitale Kompetenz zu fördern, böswillige Akteure zu identifizieren und ihre Wirkung einzudämmen. Wenn es um den Schutz von Daten geht, müssen Nutzerinnen und Nutzern zudem die Möglichkeit haben, sich gegen unzulässige Eingriffe in ihr persönliches Leben sowohl durch die Regierung als auch durch Unternehmen zu wehren.

Dabei ist es ein delikater Balanceakt Regulierung und den Schutz der Freiheitsrechte und der Meinungsvielfalt gleichermaßen zu berücksichtigen und nicht etwa durch redaktionelle Filter die Möglichkeiten demokratischer Beteiligung im Netz zu beschneiden. In den EU-Vorschriften beispielsweise ist der Grundsatz des offenen Internetzugangs tief verankert: Der Internetverkehr ist ohne Diskriminierung, Blockierung, Drosselung

27 Niesyto und Otto, 2016.
28 Yayboke, 2020.

oder Priorisierung zu behandeln.[29] Diese Regulierung (2015/2120) ist Kernbestandteil der Europäischen Digitalstategie, die europaweit einheitliche Reglungen anstrebt. Als europäisches Gremium, in dem alle nationalen Regulierungsbehörden (NRB) vertreten sind, stützt sich der sogenannte Body of European Regulators for Electronic Communications (BEREC) auf das Wissen, die Erfahrung und den technischen Sachverstand der ihm angehörenden NRB vor Ort. Im europäischen Gesetz zur Gründung des BEREC ist festgelegt, dass es sowohl die europäischen Institutionen als auch die NRB im Bereich der elektronischen Kommunikation beraten soll. Um zur einheitlichen Anwendung der Open-Internet-Verordnung beizutragen, verpflichtet Artikel 5 Absatz 3 der Open-Internet-Verordnung das BEREC ausdrücklich, Leitlinien für die Umsetzung der Verpflichtungen der NRB aus der Verordnung herauszugeben.

Ein Vorstoß in Richtung Verankerung klarerer Regeln und stärkerer Regulierung war ein EU-Parlamentsbeschluss im Januar 2022 und damit die Verabschiedung des sogenannten „Digital Services Act" (DSA). Dieser soll den digitalen Raum transparenter und fairer machen und legt klarere Regeln für Plattformen fest, wie sie gegen Hassnachrichten und „fake news" vorgehen sollen. Die Kommission hat bei der Ausarbeitung dieses Legislativpakets ein breites Spektrum von Interessengruppen konsultiert. Dazu gehörten der Privatsektor, Nutzer digitaler Dienste, Organisationen der Zivilgesellschaft, nationale Behörden, die Wissenschaft, die Fachwelt, internationale Organisationen und die breite Öffentlichkeit. Darüber hinaus wurde eine Reihe ergänzender Konsultationsschritte durchgeführt, um die Ansichten der Beteiligten zu Fragen im Zusammenhang mit digitalen Diensten und Plattformen umfassend zu erfassen.[30]

Fazit und Ausblick

Ziel dieses Kapitels war es, die chinesische Offensive im digitalen Raum zu umreißen und die Herausforderungen darzulegen, die sich durch Entwicklung und Export eines autoritären Gegenmodells zum freien und offenen Internet für liberale Demokratien ergeben. Es wurde deutlich, dass sich autoritäre Staaten, wie China, längst nicht mehr damit begnügen ihre Modelle der Daten- und Internetregulierung innerstaatlich anzuwenden, sondern dass es zunehmend auch zu einem Export von Regulierungsmo-

29 Amtsblatt der Europäischen Union, 2015.
30 Europäische Kommission, 2022.

dellen, Technologien sowie autoritären Praktiken der Überwachung und Datensammlung kommt. Dieser Vorstoß in den digitalen Raum kann gleichermaßen als Strategie der Wahrung innerstaatlicher Stabilität und der Machtmanifestation der Kommunistischen Partei unter Xi Jinping, sowie auch als Mechanismus der Außenpolitik der Volksrepublik China im Sinne einer Autokratieförderung interpretiert werden. Gleichzeitig setzt die Entwicklung Chinas zum digitalen Vorreiter und Ausgangspunkt zahlreicher digitaler Technologien und Standards Mechanismen des autoritären Lernens sowie der Diffusion autoritärer Praktiken der Internetregulierung, Datensammlung und flächendeckenden Überwachung in Kraft, die ebenso wie die aktive Verbreitung autoritärer Modelle zu einer Ausbreitung des digitalen Autoritarismus weltweit beitragen.

Wenngleich die Volksrepublik China nicht der einzige Akteur ist, der dies aktiv betreibt, so stellt insbesondere die Digitale Seidenstraße eine zentrale Herausforderung in dieser Hinsicht dar. Zusammenfassend lässt sich festhalten, dass das chinesische, autoritäre Gegenmodell zum freien und offenen Internet innerstaatlich bereits alle vier Ebenen der Internetregulierung (*infrastrukturelle Ebene*, *logisch Ebene*, *Anwendungsebene*, *inhaltliche Ebene*) abdeckt, außenpolitisch bislang vor allem die infrastrukturelle, sowie die Anwendungsebene und nur in Teilen die logisch und die inhaltliche Ebene exportiert wird. Insbesondere auf diesen Ebenen gibt daher von Seiten liberaler Demokratien Handlungsbedarf. Hier ist es insbesondere notwendig, insbesondere auf europäischer Ebene, Internetregulierung nicht allein als nationale Aufgabe zu verstehen, sondern EU-weite Standards zu entwickeln.

Bibliografie

Bader, Julia, & Kästner, Antje (2013). Externe Autokratieförderung? In: S. Kailitz & P. Köllner (Hrsg.), Autokratien im Vergleich (1. Auflage, S. 564–586). Nomos.

Bank, André, & Josua, Maria (2017). Gemeinsam stabiler: Wie autoritäre Regime zusammenarbeiten. German Institute for Global and Area Studies (GIGA), Focus 2. Online abrufbar unter: https://www.giga-hamburg.de/de/publikationen/giga-focus/gemeinsam-stabiler-wie-autoritaere-regime-zusammenarbeiten (zuletzt besucht: 28.06.2022).

Benner, Thorsten und Hohmann, Mirko (31. August 2018). Wider das autoritäre Modell: Plädoyer für eine neue deutsch-europäische Internet-Außenpolitik. Internationale Politik. Online abrufbar unter: https://internationalepolitik.de/de/wider-das-autoritaere-modell (zuletzt besucht: 18.09.2022).

Demmelhuber, Thomas, Gurol, Julia und Zumbrägel, Tobias (2022). The Corona temptation? Autocratic linkages in times of a global pandemic. In: Jan Völkel, Lena-Marie Möller and Zeina Hobaika (Hrsg.), The MENA Region and COVID-19: Impact, Implications, and Future Prospects (1. Auflage, S. 19-35). Routledge.

Drinhausen, Katja und Brussee, Vincent (9. Mai 2022). Chinas Sozialkreditsystem im Jahr 2021: Von Fragmentierung zu Integration. Mercator Institute for China Studies (MERICS) Online abrufbar unter: https://merics.org/de/studie/chinas-sozialkreditsystem-im-jahr-2021-von-fragmentierung-zu-integration (zuletzt besucht: 18.09.2022).

Europäische Kommission (7. Juni 2022). The Digital Services Act Package. Online abrufbar unter: https://digital-strategy.ec.europa.eu/de/node/27 (zuletzt besucht: 22.06.2022).

Europäisches Parlament (26 November 2015). Verordnung (EU) 2015/2120 des Europäischen Parlaments und des Rates vom 25. November 2015 über Maßnahmen zum Zugang zum offenen Internet und zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten sowie der Verordnung (EU) Nr. 531/2012 über das Roaming in öffentlichen Mobilfunknetzen in der Union. Amtsblatt der Europäischen Union. Online abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32015R2120&from=EN (zuletzt besucht: 25.06.2022).

Gerschewski, Johannes (2013). The three pillars of stability: Legitimation, repression, and co-optation in autocratic regimes. In: Democratization, 20(1), pp. 13–38. https://doi.org/10.1080/13510347.2013.738860.

Griffiths, James (2019). The Great Firewall of China: How to Build and Control an Alternative Version of the Internet. Zed Books.

Grünberg, Nils und Brussee, Vincent (9. April 2021). China's 14th Five-Year-Plan – strengthening the domestic base to become a superpower. Mercator Institute for China Studies (MERICS). Online abrufbar unter: https://merics.org/de/kurzanalyse/chinas-14th-five-year-plan-strengthening-domestic-base-become-superpower (zuletzt besucht: 18.09.2022).

Gunitsky, Seva (2015). Corrupting the Cyber-Commons: Social Media as a Tool of Autocratic Stability. In: Perspectives on Politics, 13(1), pp. 42–54. https://doi.org/10.1017/S1537592714003120.

Gurol, Julia, Zumbrägel, Tobias, & Demmelhuber, Thomas (2022). Elite Networks and the Transregional Dimension of Authoritarianism: Sino-Emirati Relations in Times of a Global Pandemic. In: Journal of Contemporary China, online first. https://doi.org/10.1080/10670564.2022.2052444.

Gurol, Julia und Schuetze, Benjamin (im Erscheinen). Infrastructuring Authoritarian Power: Arab Gulf–Chinese Transregional Collaboration beyond the State. In: International Quarterly for Asian Studies.

Hart, Melanie (28. Februar 2019)). Mapping China's Global Governance Ambitions. Online abrufbar unter: https://www.americanprogress.org/issues/security/reports/2019/02/28/466768/mapping-chinas-global-governance-ambitions/ (zuletzt besucht: 24.06.2022).

Holz, Sebastian (26. April 2022). Welche Normen regieren das Internet? GTAI – German Trade and Invest. Online abrufbar unter: https://www.gtai.de/de/trade/eu/specials/welche-normen-regieren-das-internet--831930 (zuletzt besucht: 18.09.2022).

Intelligence Online (21. Januar 2021). Digital14 picks up Darkmatter's key activities, including vulnerabilities. Intelligence Online. Online abrufbar unter: https://www.intelligenceonline.com/surveillance--interception/2021/01/21/digital14-picks-up-darkmatter-s-key-activities-including-the-vulnerabilities-researcher-xen1th labs,109636378-gra (zuletzt besucht: 19.06.2022).

Keremoğlu, Eda und Weidmann, Nils B. (2020). How Dictators Control the Internet: A Review Essay. In: Comparative Political Studies, 53(10–11), pp. 1690–1703. https://doi.org/10.1177/0010414020912278.

Lamenesch, Marie (9. Juli 2021). Authoritarianism has been reinvented for the digital age. Center for International Governance Innovation. Online abrufbar unter: https://www.cigionline.org/articles/authoritarianism-has-been-reinvented-for-the-digital-age/ (zuletzt besucht: 22.06.2022).

Levitsky, Steven und Way, Lucan A. (2002). Elections without Democracy: The Rise of Competitive Authoritarianism. In: Journal of Democracy 13, pp. 51-65.

Marczak, Bill (2. Januar 2020). A Breej too far: How Abu Dhabi's Spy Sheikh hid his Chat App in Plain Sight. Medium. Online abrufbar unter: https://medium.com/@billmarczak/how-tahnoon-bin-zayed-hid-totok-in-plain-sight-group-42-breej-4e6c06c93ba6 (zuletzt besucht: 19.06.2022).

National Development and Reform Commission (2016). The 13th Five-Year Plan for Economic and Social Development of the People's Republic of China (2016–2020). Online abrufbar unter: https://en.ndrc.gov.cn/policies/202105/P020210527785800103339.pdf (zuletzt besucht: 24.06.2022).

Niesyto, Johanna und Philipp Otto (2016). Wer regiert das Internet? Akteure und Handlungsfelder. Friedrich-Ebert-Stiftung. Online abrufbar unter: https://library.fes.de/pdf-files/akademie/12736.pdf (zuletzt besucht: 24.06.2022).

Russell, Daniel R. und Berger, Blake H. (2020). Weaponizing the Belt and Road Initiative. Asia Policy Society Institute Report. Online abrufbar unter: https://asiasociety.org/sites/default/files/2020-09/Weaponizing%20the%20Belt%20and%20Road%20Initiative_0.pdf (zuletzt besucht: 24.06.2022)

Shahbaz, Adrian (2018). Freedom on the Net 2018: The Rise of Digital Authoritarianism. Freedomhouse. Online abrufbar unter: https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism (zuletzt besucht: 12.09.2022).

Stockmann, Daniela, & Gallagher, Mary E. (2011). Remote Control: How the Media Sustain Authoritarian Rule in China. In: Comparative Political Studies, 44(4), pp. 436–467. https://doi.org/10.1177/0010414010394773.

Vanderhill, Rachel (2013). Promoting authoritarianism abroad. Lynne Rienner Publishers.

von Soest, Christian (2015). Democracy prevention: The international collaboration of authoritarian regimes. In: European Journal of Political Research, 54(4), pp. 623–638. https://doi.org/10.1111/1475-6765.12100

Yayboke, Erol (2020). Promote and Build: A Strategic Approach to Digital Authoritarianism. Center for Strategic and International Studies (CSIS). Online abrufbar unter: https://www.csis.org/analysis/promote-and-build-strategic-approach-digital-authoritarianism (zuletzt besucht: 22.06.2022).