FRIEDRICH NAUMANN FOUNDATION For Freedom.

Stanford | Global Digital Policy Incubator
Cyber Policy Center

The Great Firewall: Chinas Totale Internetzensur

Chinas Internetpolitik basiert auf digitaler Unterdrückung, und das Land exportiert sein Modell über nationale Grenzen hinaus. Deshalb muss die freie Welt demokratische Werte auch im Internet beschützen.

Charles Mok

ANALYSE

Impressum

Herausgeberin

Global Innovation Hub
Friedrich Naumann Stiftung für die Freiheit
15F.-6, No. 171, Songde Road,
Xinyi District, Taipei City 110030
Taiwan

/freiheit.org/taiwan
/FNFGIHUB
/FNFGIHUB
/FNFGIHUB

Author

Charles Mok

Redaktion

Global Innovation Hub der Friedrich Naumann Stiftung für die Freiheit

Kontakt

E-Mail: globalinnovation@freiheit.org

Stand

Juli 2023

Inhaltsverzeichnis

Glossary

Terminologie	Erklärung
ARPANET	“Advanced Research Projects Agency Network”. Das erste weiträumige Computernetzwerk mit Paketvermittlung, das die TCP/IP-Protokollfamilie implementierte, die den Grundstein für das heutige Internet bildet.
Augmented Reality (Erweiterte Realität)	Ein interaktives Erlebnis, das die reale Welt und computergenerierte Inhalte kombiniert und eine Echtzeit-Interaktion zwischen virtuellen und realen Objekten ermöglicht.
Blockchain	Eine Form von DLT, die aus Datenblöcken besteht, welche kontinuierlich generiert und mittels kryptographischer Technologien fest verknüpft werden.
Business-to-Business (B2B)	Eine geschäftliche oder elektronische Transaktion zwischen Unternehmen.
Business-to-Consumer (B2C)	Eine geschäftliche oder elektronische Transaktion zwischen einem Unternehmen und einer Verbraucherin oder einem Verbraucher.
Cloud-Computing	Computersystem-Speicher und Computerressourcen, die Nutzerinnen und Nutzern auf Abruf zur Verfügung gestellt werden, aber nicht direkt im Besitz der Nutzerinnen und Nutzer sind oder von ihnen gepflegt werden.
Consumer-to-Consumer (C2C)	Eine geschäftliche oder elektronische Transaktion zwischen mehreren Verbraucherinnen und Verbrauchern oder Privatpersonen.
Deep Packet Inspection (DPI)	Eine Datenverarbeitungstechnik, bei der die über ein Computernetzwerk gesendeten Daten im Detail untersucht werden und die sowohl für positive Zwecke verwendet werden kann, z. B. zur Sicherstellung der Datenintegrität oder zur Überprüfung auf schädliche Codes, als auch für repressive Zwecke, z. B. für Lauschangriffe und Zensur.

Terminologie	Erklärung
Distributed-Ledger-Technologie (DLT)	Eine Technik, die auf konsensbasierten digitalen Daten basiert, die repliziert, weitergegeben, synchronisiert und über viele Server oder Standorte verteilt werden, und welche die Grundlage für die Blockchain bildet.
Domain Name System (DNS)	Die hierarchischen und verteilten Namenssysteme für Computer- und Serverressourcen im Internet, die durch die Zuweisung und Übersetzung von numerischen IP-Adressen in sprachbasierte Domänennamen generiert werden.
Douyin (抖音)	Eine Social-Media-Plattform in China, die kurze Videos anbietet, ähnlich wie TikTok, das außerhalb Chinas genutzt wird. Beide sind Eigentum des chinesischen Unternehmens ByteDance (字节跳动)
Electronic Data Interchange (EDI)	Das Konzept für die digitale Übermittlung von Informationen zu Transaktionszwecken, das auf bestimmten, allgemein anerkannten Standards basiert.
Free Trade Zone (FTZ)	Ein Gebiet innerhalb eines Landes, in dem Waren ohne das Eingreifen der Zollbehörden dieses Landes abgeladen, abgefertigt und wiederausgeführt werden können.
Great Firewall (GFW, 防火长城)	Eine Kombination aus Rechtsvorschriften und Technologien, die von der chinesischen Regierung eingesetzt werden, um das Internet in China zu regulieren.
Information Warfare Monitor (IWM)	Eine Forschungspartnerschaft zwischen der in Ottawa ansässigen Denkfabrik SecDev Group und dem Citizen Lab an der Munk School of Global Affairs der Universität Toronto, die zwischen 2003 und 2012 existierte.
International Telecommunication Union (ITU)	Eine Spezialorganisation der Vereinten Nationen, die sich mit Fragen im Bereich der Informations- und Kommunikationstechnologien beschäftigt.

Terminologie	Erklärung
Internet of Things (IoT)	Physische Objekte mit Sensoren oder anderen Technologien, die mit einem Netzwerk verbunden sind, um Daten mit anderen Geräten und Systemen über das Internet oder über andere Kommunikationsnetze auszutauschen, in der Regel über Wi-Fi, 5G oder spezielle drahtlose Netzwerke.
Internet Society (ISOC)	Eine im Jahr 1992 gegründete, gemeinnützige Organisation, die sich für Technik und Zivilgesellschaft einsetzt und weltweit Zweigstellen besitzt, „um die offene Entwicklung, den Ausbau und die Nutzung des Internets zum Nutzen aller Menschen auf der ganzen Welt zu fördern“.
IP (Internet Protocol)	Das Kommunikationsprotokoll der Vermittlungsschicht für die Übermittlung von Datenpaketen, um die Verbindung von Computernetzen zu ermöglichen. Das IP stellt die technische Grundlage des Internets dar.
IPv6 (Internet Protocol Version 6)	Die neueste Version des IP-Protokolls, die von der Internet Engineering Task Force IETF entwickelt wurde, um das seit langem prognostizierte Problem der Erschöpfung der IPv4-Adressen (die aktuelle und am weitesten verbreitete Version) zu lösen.
IPv6+	Ein von Huawei entwickeltes „intelligentes IP-Netzwerk“ für flexiblere Netzwerkverbindungen, schnellere Servicebereitstellung, individuell anpassbare On-Demand-Dienste und eine gezielte Dienstleistungsgarantie.
ISO/IEC 8802-11	Die Norm für Telekommunikationen und den Austausch zwischen Informationstechnologiesystemen – Anforderungen für lokale und großstädtische Netzwerke –die den Teil 11 umfassen: WLAN-Spezifikationen für die Medienzugriffskontrolle (MAC - Medium Access Control) und die physikalische Schicht (PHY).

Terminologie	Erklärung
ITU-T (ITU Telecommunication Standardization Sector)	Ein Komitee, in dem Expertinnen und Experten aus der ganzen Welt zusammenkommen, um internationale Normen zu entwickeln, die als ITU-T-Empfehlungen bekannt sind und als definierende Elemente der globalen Infrastruktur der Informations- und Kommunikationstechnologien fungieren.
KOL (Key Opinion Leader)	Eine aktiv nutzende Person sozialer Medien, die Ereignisse interpretiert bzw. Meinungen äußert, die andere Nutzerinnen und Nutzer beeinflussen.
New IP	Von Huawei getragene Ansätze für ein künftiges Internetprotokoll (华为), die dem ITU-T, der Internet Engineering Task Force (IETF) und diversen Konferenzen des Institute of Electrical and Electronic Engineers (IEEE) vorgestellt wurden.
The Golden Shield project (金盾工程)	Chinas nationales Infrastrukturprojekt für Netzwerksicherheit, das erstmals Ende der 1990er Jahre gestartet wurde und anschließend ein Teilprojekt einleitete, das als „Great Firewall of China“ bekannt wurde.
Tor-Browser	Der Browser, der Tor („The Onion Router“) integriert, eine freie Open-Source-Software, die den Datenverkehr im Internet über ein globales, ehrenamtlich betriebenes Netzwerk leitet, um Inhalte und Standorte seiner Nutzerinnen und Nutzer geheim zu halten.
URL (Uniform Resource Locator)	Eine Adresse, die dazu dient, eine Web-Ressource zu identifizieren und zu lokalisieren, meist eine Website. Daher auch häufig als „Internetadresse“.

Terminologie	Erklärung
Virtual Reality (- Virtuelle Realität)	Ein simuliertes Erlebnis, das anwendenden Personen das Gefühl vermittelt, in eine virtuelle Welt einzutauchen. Dies geschieht im Allgemeinen durch die Erfassung von Körperhaltungen und den Einsatz von 3D-Displays.
Web 2.0	Ein Begriff, der in den frühen 2020er Jahren populär wurde und Webtechnologien und -konstrukte mit einer interaktiven und interoperablen Kultur bezeichnet, die den Schwerpunkt au anwendergenerierte Inhalte legen, wie z. B. Blogging.
WeChat	Oder Weixin (微　信) auf Chinesisch genannt, eine von Tencent (腾　讯) entwickelte chinesische „Super-App“ mit Funktionen wie Instant Messaging, Social Media, Zahlungen über Mobilgeräte usw.
Weibo	Ein allgemeiner Begriff für Mikroblogging-Plattformen in China, der sich aber auch auf die führende Mikroblogging-Plattform Sina Weibo (新浪微博) beziehen kann.
WPS Office (Writer, Presentation and Spreadsheets)	Früher bekannt als „Kingsoft Office“, ist eine Office-Suite, die vom chinesischen Softwareentwickler Kingsoft entwickelt wurde.
Zero-Day-Fehler	Eine Software-Schwachstelle, die in der Öffentlichkeit entdeckt wird, bevor sie der Händlerin bzw. Herstellerin der betroffenen Software selbst bekannt ist.

Zusammenfassung

Das Internet steht vor seiner bislang größten Krise. Die Zeiten, in denen es allgemein als eine Kraft des Guten, der Gleichberechtigung und der Selbstbestimmung angesehen wurde, sind vorbei. Heute steht das Netz vor zahlreichen Bedrohungen aus verschiedenen Richtungen. Dabei besteht die größte Bedrohung darin, dass es „in separate Netzwerke zerstückelt wird, welche von Regierungen und Konzernen beherrscht werden, die kontrollieren, was die Menschen sehen und welche Dienste sie nutzen".[1] Gleichzeitig ist die Welt mehr und mehr vom Internet abhängig. Menschen, Unternehmen und sogar Regierungen stellen zunehmend fest, dass sie ohne World Wide Web nicht mehr funktionieren können.

Was diese Internetuser vielleicht nicht wissen, ist, dass sie auch in Zukunft ein Internet in seiner ursprünglichen Konzeption und Umsetzung brauchen: Ein offenes, gemeinschaftliches, sicheres und widerstandsfähiges Internet. User müssen auch in Zukunft sichergehen können, dass ihre Informationen und Kommunikationen privat bleiben, dass sie diesem Medium vertrauen können um sich frei auszutauschen, zu handeln und Informationen miteinander zu teilen.

Ein wesentlicher Grund, warum das Internet heute so existenziell bedroht ist, liegt darin, dass es Kräfte gibt, die von mächtigen Staaten unterstützt werden, um es in ein Überwachungssystem zu verwandeln, das die totale Kontrolle über Einzelpersonen und auch über ganze Gesellschaften ermöglichen soll. Heute leben in China,[2] dem Land mit der größten Internetbevölkerung der Welt, mehr als eine Milliarde Internetnutzerinnen und -nutzer hinter der sogenannten Great Firewall (GFW).[3] Dies entspricht fast einem Fünftel aller digitalen Nutzerinnen und Nutzer weltweit. Leider wird ihnen nur eine zensierte und überwachte Version des Internets mit eigenen, staatlich kontrollierten und observierten Plattformen und Anwendungen geboten, die vom Rest des globalen Internets abgespalten und fragmentiert ist.

Diese wissenschaftliche Arbeit erläutert im ersten Teil, wie das chinesische Modell der staatlichen Internetkontrolle entstanden ist. Zunächst wurde es als Möglichkeit entwickelt, „schlechte Inhalte fernzuhalten", indem der Staat in die Kerninfrastruktur in China erst Contentfilter einbaute, sie dann gänzlich kontrollierte und sich schließlich zu eigen machte. Allmählich entwickelte es sich jedoch zu einem ausgefeilten System rechtlicher, technischer und operationeller Apparate, die von der totalitären Regierung genutzt werden. Ziel dieses Systems ist es, einen nahezu in Echtzeit funktionierenden Zensur-Apparat zu perfektionieren, der alle Plattformen und Kanäle durchdringt, um Propaganda- und Falschinformationen zu verbreiten, und riesige Datenmengen zu sammeln.

China betreibt mehr als nur Zensur, aber von Anfang an basierte die chinesische Internetkontrolle darauf. Es geht darum, durch umfassende und zunehmend aggressive und immer schärfere Gesetze zu regulieren und zu regieren, und wirtschaftliche sowie politische Kontrolle über alle großen inländischen kommerziellen Akteure sowie über die globalen Giganten aus dem Ausland auszuüben, bis diese es nicht mehr aushalten. Wenn die ausländischen Unternehmen dann wieder abreisen, braucht China sie nicht mehr.

Unterdessen wird China versuchen, seine Vision für das Internet mittels Überwachung, Zensur, Propaganda, Datenhoheit usw. auszubauen, und damit ein Netz des digitalen Autoritarismus schaffen, wie es die Welt noch nie gesehen hat. Autoritäre Regime können heute über das Internet die internetbasierten Ressourcen ihrer Feinde direkt angreifen. Einst von autoritären Herrschern als potenzielles trojanisches Pferd der Regimekritiker gefürchtet, erweist sich das Internet heute als exzeptionelles Medium zur politischen Unterdrückung und für geopolitische Manöver.

Oder nicht?

Da China bemüht ist, sein digitales Unterdrückungsregime zu transnationalisieren, muss die demokratische, freie Welt strategisch und entschlossen reagieren, um die Technik und die Struktur des Internets und alle damit verbundenen Technologien, Plattformen, Standards und Rahmenbedingungen zu schützen.

Die demokratischen Staaten müssen sich gegen jene Modelle aussprechen, die China in diversen internationalen Foren, Technik- und Standardisierungsorganisationen geschickt propagiert, um das westlich geprägte Internet dem chinesischen anzupassen. Der Umgang mit dem Netz muss offen und partizipativ für alle Beteiligten bleiben, nicht nur für Regierungen. Die Forschung und Entwicklung von Technologien zum Schutz der Privatsphäre und zur Bekämpfung der Zensur muss verstärkt werden. Eine Vision für ein freies und offenes, globales Internet muss in die zukünftige Außenpolitik integriert werden. Nicht nur, weil es angebracht ist, sondern auch, weil China bereits damit begonnen hat, seine eigene konträre Vision zu exportieren.

1 „Internet Society Action Plan 2023." https://www.internetsociety.org/action-plan/2023/
2 „Länder mit der größten digitalen Bevölkerung der Welt, Stand: Januar 2022." Statista. https://www.statista.com/statistics/262966/number-of-internet-users-in-selected-countries/
3 „Anzahl der Internet- und Social Media-Nutzer weltweit, Stand: Juli 2022." Statista. https://www.statista.com/statistics/617136/digital-population-worldwide/

Globale Internetunternehmen können aus ihren Fehlern lernen, auch wenn Expertinnen und Experten immer wieder überrascht sind, wie anfällig sie sind, dieselben Fehler zu wiederholen. Außerdem müssen sie lernen, die Konsequenzen ihres Handelns – und damit ihre Verantwortung – für die nationale Sicherheit und die weltweite Stabilität in ihren Entscheidungen mitzudenken.

In dieser wissenschaftlichen Arbeit soll untersucht werden, wie sich Chinas Regime der Internetkontrolle und -zensur entwickelt hat und welche Lehren daraus gezogen werden können, damit demokratische Staaten neue Wege finden bzw. ihre bestehenden Strategien optimieren können, um ihre Werte zu verteidigen und das Internet in seiner jetzigen Form zu bewahren.

1. Einleitung

Im Jahr 2000 sprach US-Präsident Bill Clinton über die Handelsbeziehungen mit China, welches im darauffolgenden Jahr der Welthandelsorganisation (WTO) beitrat. Er sagte mit Blick auf die immer „billiger, besser und zuverlässiger" werdenden Kommunikationsmittel: „Wir wissen, wie sehr das Internet Amerika verändert hat, und wir sind bereits eine offene Gesellschaft. Nun stellen Sie sich vor, wie sehr es China verändern wird." Und er fuhr fort: „China hat zweifellos versucht, gegen das Internet vorzugehen. Viel Glück. Das ist ungefähr so, als würde man versuchen, Gelee an die Wand zu nageln."[4]

Das Zitat war zwar berüchtigt, weil es Chinas Internet-Kontrolle so lächerlich falsch darstellte, aber eine solche Haltung wurde damals nicht nur von Präsident Clinton vertreten. Zu dieser Zeit herrschte unter Politikerinnen und Politikern, der Wirtschaft und Usern die Meinung vor, dass das Internet eine unaufhaltsame Kraft für das Gute, für Gleichberechtigung und Freiheit sei.

Als vor zehn Jahren die als Arabischer Frühling bezeichneten Proteste im Nahen Osten nachließen, wurden dem Internet und dem damals neuen Phänomen der sozialen Medien allgemein zugetraut, Aktivistinnen und Aktivisten erfolgreich zu organisieren, sowie Meinungsfreiheit, zivilgesellschaftliches Engagement und globale Kommunikation zu fördern.[5]

Wenn wir heute zurückblicken, wird deutlich, wie weit wir in so kurzer Zeit gekommen sind. Die Internetüberwachung in China lebt und ist weiter auf dem Vormarsch – in Form von verschärfter Zensur, weitreichender Überwachung und sogar gezielten Cyberangriffen. Die globale Sicht auf das Internet selbst hat sich zum Schlechten gewendet, mit zügellosen Falschinformationen, Datenschutzverletzungen, Internetsucht und allen anderen sozialen Problemen, für die oft die großen Big-Tech-Firmen sowie mangelhafte staatliche Regulierungen, sogar in demokratischen Ländern, verantwortlich gemacht werden.

4 https://www.c-span.org/video/?c4893404/user-clip-clinton-firewall-jello
5 Heather Brown, Emily Guskin und Amy Mitchell. „The Role of Social Media in the Arab Uprisings." Pew Research Center. November 2012. https://www.pewresearch.org/journalism/2012/11/28/role-social-media-arab-uprisings/

Im Jahr 2022 bekannte sich der Kolumnist und Autor der New York Times, Thomas Friedman, „schuldig“ für seinen „vorschnellen Optimismus“ von 1995 als er Kolumnist wurde. Damals hob er hervor, dass China ein offeneres Informations-Ökosystem entwickeln würde, insbesondere um einen freieren Fluss von unzensierten Nachrichten zu ermöglichen.[6] In jenen frühen Tagen der „Öffnung“ Chinas zur Welt stand die Zahl der neu zugelassenen Nachrichtenquellen in starkem Kontrast zu der Zeit kurz davor, und es war daher für alle Menschen leicht, sich von diesen Entwicklungen blenden zu lassen.

Friedman hat Recht: Wir haben uns getäuscht. Wir haben uns nicht nur in Sachen Internetzensur geirrt, sondern auch in Bezug auf die grundlegenden und weit verbreiteten Annahmen dieser Zeit über Globalisierung, Handel, Diplomatie, Geopolitik und den Wettbewerb mit einer aufstrebenden Macht, sowie darüber, in welche Richtung sich China bewegen und wie es sich entwickeln würde.

Dabei haben wir übersehen, dass unser früher Optimismus im Hinblick auf das Internet und seine positiven Kräfte in Wirklichkeit von Autokraten von Anfang an als existenzielle Bedrohung gesehen wurde. Und durch geschicktes, langfristiges Vorgehen konnten sie den Weg zur absoluten Kontrolle einschlagen, indem sie das Internet für ihre eigenen Regime einsetzten. In diesem Sinne ist die chinesische Internet-Strategie besonders konsequent, hochgradig anpassungsfähig, modern und wird stetig weiterentwickelt.

Im Laufe der Jahre haben sich Chinas Ziele von der Isolation auf den Wettbewerb verlagert. Die Taktik ist von der Defensive auf die Offensive umgeschwenkt und Chinas Fokus hat sich von der Technik auf die staatliche Kontrolle ausgeweitet. Seine Reichweite hat sich von innen nach außen, von lokal auf global oder von national auf transnational gewandelt. Diese Arbeit untersucht die Entwicklung der Kontrolle und der Regulierung des Internets in China, ebenso wie die wachsende Zahl von Instrumenten, Komponenten und Akteuren für die Zensur und die allgemeine Internetpolitik. Zu diesem Zweck behandelt die Arbeit auch die technischen, operativen, industriellen, rechtlichen, regulatorischen und diplomatischen Aspekte dieser Themen.

Auch wenn die Prognosen vor zwei Jahrzehnten falsch waren, soll dies nicht heißen, dass es keine Hoffnung für die Zukunft gibt. Wenn wir, wie Thomas Friedman einräumte, nur „verfrüht optimistisch“ waren, was sollten wir dann jetzt im Sinne der Freiheit besser machen, um die Internetfreiheit für die Bevölkerung in China zu sichern und zu verhindern, dass die „freie Welt“ „immer mehr wie China“ wird? In der Tat ist es zu einer zunehmend akuten Bedrohung geworden, „wie China zu werden“, mit der sich sogar demokratische Staaten auf der ganzen Welt konfrontiert sehen. Populistische Forderungen nach einer stärkeren Kontrolle des Internets werden oftmals von Bürgerinnen und Bürgern sowie den Gesetzgebern gleichermaßen unterstützt: Mehr Überwachung aufgrund von Falschinformationen, Wahlbeeinflussung und der Sicherheit für Kinder im Internet; mehr Überwachung im Zusammenhang mit Verbrechen und Terrorismus usw.

Die Politikerinnen und Politiker in der „freien Welt“ müssen realisieren, dass es um viel mehr geht, als nur darum, ihre Bevölkerung und deren Lebensweise vor den „Gefahren des Internets“ zu schützen. Stattdessen können unsere Handlungen die Entwicklungsrichtung des Internets bestimmen. Das wird deutlich, wenn man sich anschaut, wie verschiedene Akteure um die Infrastruktur des Internets und dessen Zukunft ringen, d. h. ob es autoritärer und fragmentierter wird oder ob es unsere ursprünglichen Hoffnungen auf eine Wende zum Besseren erfüllt. Um mitzuhalten, müssen die Industrie, die Zivilgesellschaft, die Technologieexpertinnen und -experten sowie Internetuser Chinas Strategie besser verstehen.

6 Thomas Friedman. „I Was Wrong About Chinese Censorship.“ 21. Juli 2022 https://www.nytimes.com/2022/07/21/opinion/thomas-friedman-china.html

2. Chinas staatliche Internetpolitik — Zensur und Repressionen

Bei Chinas Internetkontrolle und -regulierung geht es – wie diese Arbeit deutlich machen wird – um mehr als nur um Zensur oder die Great Firewall GFW. Dennoch war das Ziel der Zensur von zentraler Bedeutung für die ursprüngliche Einführung der GFW. Das Konzept der Zensur hat sich seitdem weiterentwickelt und umfasst weit mehr, als nur bestimmte Websites oder Inhalte für Internetnutzende in China unzugänglich zu machen oder Nachrichten auf Chinas Internetplattformen zu löschen.

Wenn es nur eine der Taktiken war, bestimmte Informationen aus China fernzuhalten, dann muss das große Ziel der Zensur etwas viel Fundamentaleres sein. Aus Sicht der chinesischen Regierung trifft der Begriff „Zensur“ nicht zu. Es handelt sich vielmehr um „Management“. In einem Land mit sehr vielen Internetnutzenden scheint ein besseres Management ein berechtigter Grund zu sein, um entsprechende Regelungen und Beschränkungen einzuführen. Letztendlich würde kein Land das Internet vollständig regulieren oder es ganz unkontrolliert lassen, und so können Chinas Machthaber behaupten, dass sie sich nicht vom Rest der Welt unterscheiden: Es gibt Regeln, und wenn jemand gegen diese Regeln verstößt, sollte es Konsequenzen geben, wie im jeweiligen Gesetz festgelegt.[7]

2.1. Wie viele Internetnutzende in China umgehen die Great Firewall?

Der Begriff „Great Firewall“ mag den Eindruck erwecken, dass sie undurchdringbar ist – aber das ist sie nicht und das war wahrscheinlich auch nie beabsichtigt. Die Wissenschaft bezeichnet dies als „durchlässige Zensur“. Das bedeutet, dass die Zensoren nicht auf unplausible, hermetische Verbote aller unerwünschten Inhalte setzen, sondern den Zugang zu bestimmten Inhalten erschweren oder mit hohen Kosten belegen, anstatt ein absolutes Verbot zu erteilen.[8] Durch routinemäßiges Erschweren des

7 外媒质疑中国网络审查制度日趋严格 鲁炜：用词不当 http://news.sina.com.cn/c/2015-12-09/doc-ifxmifzc0923447.shtml

8 Margaret E. Roberts. „Censored: Distraction and Diversion Inside China's Great Firewall.“ 2018. Kapitel 1, 1.1.

Zugangs zu bestimmten Inhalten, z. B. mittels Löschen aus der Liste der Suchmaschinen, durch Anzeigen der Fehlermeldung „404 Nicht gefunden“ oder durch Verlangsamung der Zugriffsgeschwindigkeit, werden die meisten, wenn nicht alle Internetnutzende in ausreichendem Maße vom Zugang abgehalten. Die User wählen dann andere, leichter zugängliche Alternativen, die von den Zensoren und Behörden freigegeben sind. Wenn nur ein kleiner Prozentsatz der User die Ausdauer hat, Umgehungstools oder ein virtuelles privates Netzwerk (VPN) zu nutzen, können die Zensoren mit ihrer Arbeit zufrieden sein.

Obwohl es keine offiziellen Statistiken oder genauen Berechnungen darüber gibt, wie viele Internetnutzende in China regelmäßig die GFW umgehen, können Untersuchungen der letzten Jahrzehnte einen gewissen Aufschluss darüber geben. Im Jahr 2000 führte die Chinese Academy of Social Sciences (CASS) eine Umfrage unter Internetusern in fünf chinesischen Städten dazu durch. Diese Umfrage ergab, dass zehn Prozent der Umfrageteilnehmenden zugaben, „regelmäßig“ Proxyserver zu benutzen, um die Zensur zu umgehen, und dass 25 Prozent dies nur „gelegentlich“ machten.[9] Eine weit umfassendere Harvard-Studie aus dem Jahr 2010 untersuchte die Nutzung von Proxys, VPNs und anderen Umgehungstechnologien. Die Studie ergab, dass nicht mehr als drei Prozent der Internetnutzenden aus Ländern, die in erheblichem Umfang Filter einsetzen (einschließlich China) Umgehungstools nutzen, und dass „die tatsächliche Zahl wahrscheinlich deutlich geringer“ sei.[10] Zudem ergab eine weitere Umfrage aus dem Jahr 2015, dass nur fünf Prozent der chinesisch Stadtbevölkerung jemals versucht hatte, die GFW zu umgehen.[11]

Es ist gewiss bemerkenswert – und ein Beweis für die relative Offenheit Chinas vor zwanzig Jahren – dass mit CASS ein offizielles Forschungsinstitut in China eine Umfrage durchführte, in der offene Fragen zur Umgehung der staatlichen Zensurmaßnahmen gestellt wurden. Das die Prozentwerte und die Zahlen, die in späteren Studien westlicher Wissenschaftlerinnen und Wissenschaftler ermittelt wurden, viel kleiner zu sein scheinen als die der CASS Studie, dann liegt das vermutlich daran, dass im Jahr 2000 die ersten Internetnutzenden in China eher urban lebten, technisch versiert, gut ausgerüstet und gebildet waren. Viele der befragten User späterer Studien kamen im Vergleich dazu aus ländlichen Regionen. Die rasante Zunahme von Internet- und Mobilfunknutzenden in China ab dem Jahr 2000 dürfte diese Ergebnisse zudem beeinflusst haben. Außerdem haben Studien bestätigt, dass Bürgerinnen und Bürger, welche die GFW umgehen, tendenziell jünger, besser ausgebildet und technisch ausgestattet sind, mehr über Politik wissen, weniger Vertrauen in die Regierung haben und schon früher mit Ausländerinnen und Ausländern Kontakt hatten.[12]

2.2. Hin zu noch drakonischeren Regeln und propagandistischen Falschinformationen

Bei der Internetzensur geht es um mehr als nur um das Blocken bzw. Verbieten von bestimmten Inhalten. Vielmehr wird sie als „Einschränkung der öffentlichen Äußerung von oder des öffentlichen Zugangs zu Informationen durch eine Autorität“ definiert.[13] Eine berühmte Harvard-Studie kam zu dem Schluss, dass Zensur „darauf abzielt, kollektives Handeln einzuschränken, indem sie Kommentare unterbindet, die eine soziale Mobilisierung zeigen, verstärken oder anstoßen, unabhängig von ihrem Inhalt“, und versucht, „kollektive Aktivitäten zu verhindern, die gegenwärtig stattfinden oder in Zukunft stattfinden könnten“.[14]

Prof. Margaret Roberts hebt drei Methoden der Internetzensur hervor: Zensur basierend auf Furcht, Frustration und Überflutung.[15] Die auf Furcht basierende Zensur wird durch Gesetze, Vorschriften und potenzielle Strafen umgesetzt. Sie fungiert als rechtliche Abschreckung und Form der Einschüchterung, um die Verbreitung unerwünschter Informationen durch die Medien und einflussreiche Personen einzuschränken und zu unterdrücken. Die auf Frustration basierende Zensur trifft eine breite Masse von Nutzenden, indem sie diesen erschwert, auf bestimmte Inhalte zuzugreifen bzw. nach diesen zu suchen. Und die Zensur durch Überflutung schließlich dient dazu, die Aufmerksamkeit der Nutzenden von unerwünschten Inhalten auf eher profane und manchmal sogar propagandistische Informationen zu lenken. Eine Harvard-Studie aus dem Jahr 2017 ergab, dass ein Heer von chinesischen Staatsbediensteten innerhalb eines Jahres 488 Millionen gefälschte Posts verfasst haben soll und allgemein als „50-Cent-Armee“ bekannt war, da jeder veröffentlichte Post angeblich mit einer Prämie von umgerechnet 50 Cent vergütet wurde.[16] Bei den jüngsten Protestwellen gegen Corona-Lockdowns in China überfluteten Bots, die angeblich aus China stammten, Twitter mit explizit pornografischen Inhalten, indem sie Schlüsselwörter und Tags manipulierten, wenn User nach Nachrichten im Zusammenhang mit den Demonstrationen oder sogar nur nach Namen zahlreicher chinesischer Städte suchten.[17]

9 „II. How Censorship Works in China: A Brief Overview“ in „Race to the Bottom: Corporate Complicity in Chinese Internet Censorship.“ Human Rights Watch. 2006. https://www.hrw.org/reports/2006/china0806/3.htm

10 Hal Roberts, Ethan Zuckerman, Rob Faris und John Palfrey. „2010 Circumvention Tool Usage Report.“ The Berkman Center for Internet & Society. Oktober 2010. https://cyber.harvard.edu/sites/cyber.harvard.edu/files/2010_Circumvention_Tool_Usage_Report.pdf

11 Margaret E. Roberts. “Censored: Distraction and Diversion Insider China’s Great Firewall.” 2018. Kapitel 5, 5.2.1.

12 Ibid. Kapitel 5, 5.2.2.

13 Ibid. Kapitel 2, 2.5.

14 Gary King, Jennifer Pan, und Margaret E. Roberts. „How Censorship in China Allows Government Criticism but Silences Collective Expression.“ 2013. https://gking.harvard.edu/files/censored.pdf

15 Margaret E. Roberts. “Censored: Distraction and Diversion Inside China’s Great Firewall.” 2018. Kapitel 2, 2.7-2.9.

16 Gary King, Jennifer Pan und Margaret E Roberts. „How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, not Engaged Argument.“ Harvard University. 09. April 2017. https://gking.harvard.edu/files/gking/files/50c.pdf?m=1463587807

17 Ryan Fahey. „Chinese bots flood Twitter with explicit porn to drown out news of lockdown protests.“ The Mirror. 28. November 2022. https://www.mirror.co.uk/news/world-news/chinese-bots-flood-twitter-explicit-28604491

Als chinesische Internetnutzende während der COVID-19-Pandemie versuchten, an Gesundheitsinformationen zu gelangen, setzten sie vermehrt Umgehungsmethoden ein, um verbotene Plattformen wie Twitter und Wikipedia aufzurufen.[18] Obwohl Studien zeigen, dass „die Kenntnis der Zensur die Verbraucherinnen und Verbraucher eher zu den Informationen hin- als von ihnen wegführen kann“[19], gaben die chinesischen Zensoren nicht nach und verstärkten ihren Einsatz in dieser Zeit. DYX, das führende digitale Gesundheitsportal des Landes, wurde 2022 verboten und seine Social-Media-Konten auf Weibo, WeChat und Douyin wegen Verstößen gegen „einschlägige Gesetze und Vorschriften“ gesperrt. Der Grund war, dass das Portal die chinesische Zero-COVID-Politik indirekt kritisierte, indem es die traditionelle chinesische Medizin nicht erwähnte und das chinesische Gesundheitssystem anprangerte.[20]

Eine andere Art von Zensur fand nach dem Besuch der Sprecherin des US-Kongresses, Nancy Pelosi, in Taiwan Anfang August 2022 statt. Das Beispiel zeigt, wie komplex und sensibel die Zensur häufig sein kann. Eine Sturmflut negativer Kommentare gegen die vermeintliche Untätigkeit des chinesischen Militärs, die hinter der offiziellen Rhetorik von „starken Vergeltungsmaßnahmen“ vor dem Besuch zurückblieb, brach in den sozialen Medien los. Bestimmte Kommentarbereiche von WeChat-Diskussionen wurden gesperrt, aber die Zensoren konnten die meisten kritischen Kommentare nicht komplett unterbinden[21] da die Emotionen der chinesischen Internetuser behutsam behandelt und nicht noch stärker provoziert werden sollten.

Allerdings können propagandistische Überflutungstaktiken auch nach hinten losgehen. Nach dem Angriff Russlands auf die Ukraine im Februar 2022 wurde Propaganda für den Kreml von chinesischen Social-Media-Plattformen aus dem Chinesischen in mehrere Sprachen übersetzt und auf Twitter und anderen Social-Media-Plattformen außerhalb der GFW gepostet. Diese sogenannte „Große Übersetzungsbewegung“ wurde vor allem von Chinesinnen und Chinesen im Ausland initiiert.[22] Diese Nachrichten deckten die pro-russischen Falschinformationen auf, die in China kursierten, und standen im Gegensatz zu den relativ zurückhaltenden offiziellen Stellungnahmen von chinesischen Diplomatinnen und Diplomaten. Als Ergebnis der blamablen Situation beschuldigte Chinas offizielles englisches Sprachrohr, die Global Times, „antichinesische Kräfte aus den USA und Taiwan“, „China zu schmähen“, indem sie „selektiv relativ aggressive Rhetorik in chinesischen sozialen Medien übersetzten“.[23]

Unter Präsident Xi Jinping hat sich die chinesische Zensur von einem eher durchlässigen zu einem eher furchtbasierten Ansatz gewandelt. Einschüchterungen des Systems erstrecken sich nicht nur auf Eliten und die Medien. In der Vergangenheit hielten sich chinesische Behörden mit ihrer Zensur aus Angst vor Gegenreaktionen in Krisenzeiten eher zurück, da die Bevölkerung dann meist motivierter war als sonst, sich zu informieren und die Einschränkungen durch die Zensur zu überwinden. Doch wie im weiteren Verlauf noch näher erläutert wird, sind Chinas Interventionen in Krisenzeiten schneller und repressiver geworden. Das wird etwa bei den Razzien in Xinjiang und Hongkong ersichtlich, oder den „White Paper“ Anti-COVID-Protesten in ganz China Ende 2022. Damals wurden viele Menschen Berichten zu Folge von den staatlichen Behörden mit Hilfe von Telefon- und Social-Media-Datensätzen sowie öffentlichen Überwachungssystemen aufgespürt und festgenommen.[24]

18 „Circumvention of Censorship in China Has Increased During COVID-19 Pandemic.“ UCLA. 19. Januar 2022. https://luskin.ucla.edu/circumvention-of-censorship-in-china-has-increased-during-covid-19-pandemic

19 Margaret E. Roberts. “Censored: Distraction and Diversion Inside China’s Great Firewall.” 2018. Kapitel 7, 7.2.

20 Zeyi Yang. „China has censored a top health information platform.“ MIT Technology Review. 11. August 2022. https://www.technologyreview.com/2022/08/11/1057592/china-censored-health-information-platform/

21 Li Yuan. „Perils of Preaching Nationalism Play Out on Chinese Social Media.“https://www.nytimes.com/2022/08/04/business/new-world-nancy-pelosi-taiwan-social-media.html

22 „Great Translation Movement.“ https://en.wikipedia.org/wiki/Great_Translation_Movement

23 大翻译运动向全球展现中国网民言论 指中国官媒“说谎”
https://www.rfi.fr/cn/%E4%B8%AD%E5%9B%BD/20220328-%E5%A4%A7%E7%BF%BB%E8%AF%91%E8%BF%90%E5%8A%A8%E5%90%91%E5%85%A8%E7%90%83%E5%B1%95%E7%8E%B0%E4%B8%AD%E5%9B%BD%E7%BD%91%E6%B0%91%E8%A8%80%E8%AE%BA-%E6%8C%87%E4%B8%AD%E5%9B%BD%E5%AE%98%E5%AA%92-%E8%AF%B4%E8%B0%8E

24 Paul Mozur, Claire Fu und Amy Chang Chien. „How China’s Police Used Phones and Faces to Track Protesters.“ The New York Times. 02. Dezember 2022. https://www.nytimes.com/2022/12/02/business/china-protests-surveillance.html

3. Immer ausgefeiltere rechtliche und technische Werkzeuge

Betrachten wir nun die chinesische Internetpolitik und -kontrolle sowie den Aufbau der GFW etwas genauer. Auch wenn das Internet eine relativ neue Technologie ist, so ist die Zensur für China mit Blick auf die Geschichte weder neu noch fremd: Die Qin-Dynastie war berüchtigt für die „Bücherverbrennung und das Begraben von Gelehrten bei lebendigem Leibe“[25], die berühmte Chinesische Mauer wurde vor fast 2.200 Jahren gebaut, um Ausländerinnen und Ausländer aus dem Land fernzuhalten[26] und das Zensursystem der heutigen Kommunistischen Partei Chinas (KPCh) wurde bereits in der Amtszeit von Mao Zedong mit großer Sorgfalt aufgebaut.[27]

Die GFW und der gesamte Zensurmechanismus in China haben sich im Laufe der Jahre weiterentwickelt und umfassen technische, operative, kommerzielle, rechtliche, regulatorische und vollziehende Elemente. Wie wir noch sehen werden, gehen diese Elemente zunehmend über die Grenzen Chinas hinaus.

3.1. Der Rechtsstaat

3.1.1. Kontrolle der Infrastruktur

Zuerst einmal werfen wir einen Blick auf die Anfänge des Internets in China. In den späten 1980er Jahren begannen verschiedene akademische Institutionen in China damit, private Verbindungen mit Nordamerika und Europa zu knüpfen, indem sie das Chinese Academic Network und das Chinese Research Network gründeten. Die oberste Länderdomäne .cn wurde 1990 vom Defense Data Network Network Information Center erworben, dem ehemaligen internationalen Internet-Informationszentrum, das im Rahmen des Advanced Research Projects Agency Network (ARPANET) – dem ersten öffentlichen paketvermittelten Computernetzwerk, das der Vorläufer des Internets war – des US-Verteidigungsministeriums betrieben wurde.

25 „Burning of books and burying of scholars (焚書坑儒).“ https://en.wikipedia.org/wiki/Burning_of_books_and_burying_of_scholars
26 „The Great Wall of China.“ https://en.wikipedia.org/wiki/Great_Wall_of_China
27 „Censorship in China.“ https://en.wikipedia.org/wiki/Censorship_in_China

Im Jahr 1994 wurde mit dem China Science and Technology Network die erste formelle Internetverbindung sowohl auf nationaler als auch auf internationaler Ebene geschaffen, und später im gleichen Jahr wurde das China Education and Research Network (CERNET) eingerichtet, um die Forschungseinrichtungen, Hochschulen und Universitäten des Landes miteinander zu verknüpfen. Anfang 1995 schloss Chinas staatlicher Telekommunikationsanbieter China Telecom einen Vertrag mit der US-Regierung über die Anmietung von zwei Standleitungen mit 64 kbit/s, um von Peking und Shanghai aus eine Verbindung zu den USA herzustellen, die zur Grundlage für das Backbone von Chinas künftigem Internet, ChinaNet, wurde.[28]

CSTNET, CERNET und ChinaNet bildeten zusammen mit dem China Gold Bridge Network (CHINAGBN),[29] einem nationalen Wirtschaftsnetzwerk für den elektronischen Datenaustausch (EDI), das ursprüngliche Backbone des Internets in China. Die chinesische Regierung besitzt und kontrolliert die gesamte Infrastruktur sowie sämtliche Zugangsrouten, was eine wichtige Grundvoraussetzung für die Zensur darstellt. Ursprünglich durften nur die drei staatlichen Telekommunikationsanbieter kommerzielle Internetdienste anbieten: China Telecom, China NetCom, das später mit China Unicom zusammengelegt wurde, und China Mobile. Anfangs existierten nur drei externe Gateways, die Chinas nationales Netz mit der Außenwelt verbanden, und zwar in Peking, Shanghai und Guangzhou, aber im Jahr 2015 wurden diese auf insgesamt sieben weitere Anschlusspunkte ausgebaut.[30]

Da die chinesische Zentralregierung das Internet auf der Infrastrukturebene vollständig in ihrem Besitz hat, kann sie die absolute Kontrolle und Autorität über das chinesische Internet ausüben, von der physischen bis zur Service-Ebene. Vor allem ihre Kontrolle über internationale Konnektivität führt dazu, dass es für die Behörden relativ einfach ist, eingehenden Datenverkehr und Inhalte von vornherein zu filtern.

Dabei waren die Anfänge des Internets in den USA und in China ähnlich verlaufen – beide waren stark von den Regierungen geprägt. Es entwickelte sich jedoch von da an in verschiedene Richtungen. In den USA wurde das Internet privatisiert. Als es zunehmend kommerzialisiert und für alle nutzbar wurde, gab die Regierung die Kontrolle weitgehend ab. In China behielt die Regierung die vollständige und absolute Kontrolle über die Regulierung des Internets.

3.1.2. Setting the Baseline

Die drei frühesten Beispiele für Rechtsvorschriften der Zentralregierung für das Internet in China sind die zeitweilige Verordnung zur Handhabung internationaler Verbindungen von Computer-Informationsnetzen (die erstmals im Januar 1993 vom Staatsrat erlassen und im Februar 1996 geändert wurde), die Verordnung zum Schutz der Sicherheit von Computer-Informationssystemen (die im Februar 1994 vom Staatsrat erlassen wurde) und die Sicherheitsmanagementverfahren für den Internetzugriff (die vom Staatsrat gebilligt und vom Ministerium für öffentliche Sicherheit im Dezember 1997 erlassen wurden).[31]

Die Verordnung von 1993 sichert dem Staat das alleinige und absolute Recht für den Aufbau, die Steuerung und Kontrolle des Internets zu, einschließlich des „Prinzips der gesamten Planung, einheitlicher Standards, der Organisation in Schichten und des Entwicklungsfortschritts“ in Bezug auf internationale Netzwerkverbindungen, und insbesondere die folgenden Punkte:

- Keine Organisationen oder Einzelpersonen dürfen eigenständig eine direkte internationale Verbindung einrichten.
- Jede direkte Verbindung mit dem Internet muss über ChinaNet, CHINAGBN, CERNET oder CSTNET abgewickelt werden.
- Jeder User, der einen Internetzugang zur Verfügung stellen möchte, benötigt eine Lizenz, und muss sich registrieren, um Zugriff zu erhalten.
- Schadhafte Informationen, die entweder subversiv oder obszön sind, dürfen nicht veröffentlicht werden.

In der Verordnung wird betont, dass die Verantwortung für den Schutz der Sicherheit des Internets beim Ministerium für öffentliche Sicherheit liegt, das „die Sicherheitsmaßnahmen überwacht, überprüft und begleitet“, „illegale Straftaten untersucht und ahndet“ und „andere Überwachungsaufgaben wahrnimmt“. Die Verordnung wurde später weiterentwickelt, um ein Verfahren zu bilden, welches die Art der „schadhaften Aktivitäten“ genauer spezifiziert. Sie umfasst Eindringen, Missbrauch sowie Hacking von Programmen bzw. Daten ohne Befugnis, sowie vorsätzliches Erzeugen oder Verbreiten von Viren und andere schädigende Handlungen im Computernetzwerk.

Anfänglich wurden die Inhalte größtenteils durch die entsprechenden Backbone-Netze kontrolliert. Ihre Bestimmungen legten also fest, was erlaubt war und was nicht. Die Regeln waren nicht überall dieselben. Beispielsweise erlaubten die Richtlinien des CHINAGBN den Nutzenden nicht, „schadhafte Informationen, die die soziale Sicherheit gefährden und die obszöne Inhalte enthalten, zu produzieren, anzusehen, zu verbreiten und zu kommunizieren“ und legten fest, dass „die nationalen Sicherheitsvorschriften strikt eingehalten werden müssen“. Die Vorschriften von CERNET besagten, dass „Artikel mit politischen Problemen konsequent gelöscht werden müssen“.

28 „Die Entwicklung des Internets in China.“ 01. Januar 2001. https://web.archive.org/web/20120527120608/http://www.edu.cn/introduction_1378/20060323/t20060323_4285.shtml

29 CHINAGBN. https://baike.baidu.com/item/CHINAGBN/3438473

30 Chengdu (成都), Xian (西安), Wuhan (武汉), Shenyang (沈阳), Nanjing (南京), Chongqing (重庆), Zhengzhou (郑州) – 新增7个国家级互联网骨干直联点建设全面竣工. 2015.1.12. https://web.archive.org/web/20150121025150/http://www.miit.gov.cn/n11293472/n11293832/n11293907/n11368223/16402896.html and “The Chinese Internet Gets A Stronger Backbone.” 2015. https://www.forbes.com/sites/lisachanson/2015/02/24/the-chinese-internet-gets-a-stronger-backbone/?sh=1ea5a16e1ff4

31 Jack Linchuan Qiu. „Virtual Censorship in China: Keeping the Gate Between the Cyberspaces.“ 1999/2000 https://ciaotest.cc.columbia.edu/olj/ijclp/ijclp_4/ijclp_4a.pdf

Im Dezember 1997 wurden in Artikel 5 der vom Ministerium für öffentliche Sicherheit erlassenen Vorschriften für Sicherheit, den Schutz und die Betreuung von Informationsnetzen und des Internets die Kategorien der verbotenen Inhalte festgelegt:[32]

"Keine Organisation oder Einzelperson darf das Internet nutzen, um die folgenden Arten von Informationen zu erzeugen, zu vervielfältigen, abzurufen oder weiterzugeben:

(1) Aufruf zum Widerstand oder zum Verstoß gegen die Verfassung oder gegen Gesetze oder die Umsetzung von Verordnungen;
(2) Aufruf zum Stürzen der Regierung oder des sozialistischen Systems;
(3) Aufruf zur Aufsplitterung des Landes, wodurch die nationale Einheit geschädigt wird;
(4) Anstiftung zu Fremdenhass oder Diskriminierung zwischen Nationalitäten oder Gefährdung der nationalen Einheit;
(5) Verbreitung von Unwahrheiten bzw. Verdrehung der Wahrheit, Verbreitung von Gerüchten, Zerstörung der gesellschaftlichen Ordnung;
(6) Förderung von feudalem Aberglauben, sexuell anzüglichem Material, Glücksspiel, Gewalt oder Mord;
(7) Terroristische Aktivitäten oder Anstiftung zu kriminellen Handlungen; Beleidigen anderer Personen oder Verfälschen der Wahrheit, um Personen zu diffamieren;
(8) Rufschädigung von Staatsorganen;

Sonstige Aktivitäten, die gegen die Verfassung, Gesetze bzw. behördliche Vorschriften verstoßen."

Ferner wurden dem Staatssicherheitsdienst in Artikel 8 dieser Verordnung weitreichende Befugnisse verliehen, Informationen von Einzelpersonen und Organisationen in China zu überprüfen und sicherzustellen:

„Im Internetgeschäft tätige Organisationen und Einzelpersonen müssen die Sicherheitsüberwachung, Inspektionen und die Weisungen des Staatssicherheitsdienstes respektieren. Dazu gehört auch, dass Informationen, Materialien sowie digitale Dokumente an den Staatssicherheitsdienst weitergegeben werden und dass der Staatssicherheitsdienst bei der Ermittlung und ordnungsgemäßen Abwicklung von Vorfällen im Zusammenhang mit Gesetzesverstößen und kriminellen Aktivitäten, die sich auf Computerinformationsnetze beziehen, unterstützt wird."[33]

3.1.3. Der Umgang mit dem kommerziellen Internet

Als das kommerzielle Internet in China um die Jahrtausendwende aufblühte, wurden weitere Vorschriften erlassen, um die Kontrolle über bestimmte Internetbetreiber bzw. Geschäftsmodelle zu verstärken.

Eine der ersten einschlägigen Verordnungen, die für Internetdienste eingeführt wurden, war das Klarnamen-System. Aus Sicht der Regierung müssen die Behörden vor allem in der Lage sein, Regelverstoßende zu identifizieren. Darüber hinaus sollte sichergestellt werden, dass Nutzende eine reale Furcht verspüren, da sie genau wissen, dass jede ihrer Online-Aktionen bis zu ihrer wahren Identität zurückverfolgt werden kann, sie somit zur Rechenschaft gezogen werden und mit Konsequenzen rechnen müssen. Auf Verlangen diverser Regierungsstellen und Aufsichtsbehörden sowie durch die Selbstregulierung der Branche setzten viele Anbieter von Internet-Diensten, wie z. B. Internet-Cafés, bereits 2003 die Verpflichtung zur Registrierung unter echtem Namen für User durch.[34]

Im Dezember 2012 verabschiedete der Ständige Ausschuss des Nationalen Volkskongresses den „Beschluss über den verstärkten Schutz von Netzinformationen", der die Erfassung persönlicher Identifikationsdaten bei der Registrierung von Nutzenden für Dienste wie Website-Zugang, Festnetz- und Mobiltelefondienste oder andere Online-Informationsdienste vorschreibt. Bevor das Gesetz aber im März 2012 in Kraft trat, hatten alle vier großen Microblogging-Plattformen (Weibo), die von Sina, Sohu, Netease und Tencent betrieben wurden, bereits freiwillig das Real-Name-System vollständig umgesetzt.[36]

Als immer mehr Nutzende auf VPNs auswichen, um die Beschränkungen zu umgehen, erließ das Handelsministerium 1996 die „Interim Regulations of the PRC on the Management of International Networking of Computer Information"[37], um Verbindungen zu „internationalen Netzwerken" über Kanäle außerhalb der von der Regierung zugelassenen Anbieter zu verbieten.[38]

Zudem wurden später Verordnungen für Anbieter von Informationsdiensten erlassen, um Betreibende, die Dienste über Telekommunikationsnetzbetreiber anbieten, direkt zu regulieren. In Artikel 57 der Telekommunikationsverordnung der Volksrepublik China, die im September 2000 vom Staatsrat erlassen wurde, heißt es beispielsweise:

32 „Freedom of Expression and the Internet in China: A Human Rights Watch Backgrounder." Human Rights Watch. https://www.hrw.org/legacy/backgrounder/asia/china-bck-0701.htm
33 „Freedom of Expression and the Internet in China: A Human Rights Watch Backgrounder." Human Rights Watch. https://www.hrw.org/legacy/backgrounder/asia/china-bck-0701.htm
34 „沈阳网吧今起实名上网." July 10, 2003. https://web.archive.org/web/20180221100747/http://hnfy.chinacourt.org/article/detail/2003/07/id/679048.shtml
35 „授权发布：全国人民代表大会常务委员会关于加强网络信息保护的决定." https://web.archive.org/web/20130203205216/http://www.npc.gov.cn/npc/xinwen/2012-12/29/content_1749526.htm
36 „中国官方继续清网 全面推行实名制." https://www.dw.com/zh/%E4%B8%AD%E5%9B%BD%E5%AE%98%E6%96%B9%E7%BB%A7%E7%BB%AD%E6%B8%85%E7%BD%91-%E5%85%A8%E9%9D%A2%E6%8E%A8%E8%A1%8C%E5%AE%9E%E5%90%8D%E5%88%B6/a-18187414
37 Interim-Bestimmungen der VR China über die Kontrolle der internationalen Vernetzung von Computerinformationen
38 „Interim Regulations on the Management of International Networking of Computer Information." http://www.asianlii.org/cn/legis/cen/laws/irotmoinoci880/

„Keine Organisation bzw. Einzelperson darf Telekommunikationsnetze nutzen, um Informationen mit den folgenden Inhalten zu erzeugen, zu vervielfältigen, herauszugeben oder zu verbreiten:

(1) Material, das den Grundsätzen der Verfassung zuwiderläuft;
(2) Material, das die nationale Sicherheit gefährdet, Staatsgeheimnisse offenbart, die Staatsmacht untergräbt oder die nationale Einheit gefährdet;
(3) Material, das dem Wohl und den Interessen des Staates schadet;
(4) Material, das ethnische Spannungen und Diskriminierung verursacht oder die ethnische Solidarität gefährdet;
(5) Material, das die staatlichen religiösen Grundsätze gefährdet oder Sekten und feudalen Aberglauben unterstützt;
(6) Material, das Gerüchte verbreitet, die soziale Ordnung stört oder die soziale Stabilität gefährdet;
(7) Material, das Obszönitäten, Pornografie, Glücksspiel, Gewalt, Mord, Terror oder Anstiftung zu Verbrechen beinhaltet;
(8) Material, das andere beleidigt, diffamiert oder die gesetzlichen Rechte und Interessen anderer verletzt;
(9) Material, das andere durch Gesetze bzw. behördliche Verordnungen verbotene Inhalte umfasst."[39]

In den frühen 2000er Jahren wurde dann zur Regulierung der gängigen Internet-Nachrichtenportale die Verordnung Nr. 292 des Staatsrats erlassen, die eine Lizenz für Websites vorschreibt, damit sie legal als „Internet-Informationsdienste in den Bereichen Nachrichten, Publikationen, Bildung, medizinische Versorgung, Medikamente und medizinische Geräte usw." operieren konnten. Nicht lizenzierte Websites konnten nur noch Nachrichten von anderen lizenzierten Nachrichtenmedien übernehmen und veröffentlichen. Danach durften Websites ohne eine spezielle Zusatzgenehmigung keine ausländischen Nachrichten-Websites mehr verlinken – unabhängig davon, ob die ausländischen Seiten durch die GFW geblockt wurden. Zudem wurde ein Genehmigungssystem für die Nachrichtenpublikation eingeführt, das verhinderte, dass immer mehr private Websites in China Nachrichten veröffentlichten. Beispielsweise wurde berichtet, dass bis Ende 2008 nur acht von 430.000 Websites in der Provinz Guangdong eine Lizenz für die Nachrichtenpublikation erhalten hatten, um ihre Tätigkeit fortzusetzen.[40]

Es handelt sich hierbei nur um eine Momentaufnahme der Gesetze aus der Anfangsphase, als in China die Verordnungen entstanden, die das Internet regelten. Charakteristisch für diese Phase der Regulierung war, dass sich diese Gesetze häufig überschnitten und von mehreren Regulierungsstellen auf verschiedenen Regierungsebenen verwaltet wurden. Dies war zum Teil auf den Wettbewerb zwischen den Verwaltungsstellen zurückzuführen, zum Teil war es aber auch bewusst, weil man sicherstellen wollte, dass eine gewisse Vollständigkeit und Flexibilität bestand, um das für die jeweilige Situation „am besten geeignete" Gesetz anzuwenden. Generell lag die Zuständigkeit immer noch in den Händen der Sicherheits- und Propagandaorgane der Regierung.

Doch 2014 änderte sich dies mit der Machtübernahme von Xi Jinping als Generalsekretär der KPCh und chinesischem Staatspräsidenten. Die Abgrenzung zwischen Staat und Partei verwischte noch stärker, vor allem im Hinblick auf die Regulierung des Internets.

Zuvor wurde die chinesische Internetpolitik von der staatlichen Internet-Informationsbehörde verwaltet, die der Informationsbehörde des Staatsrats unterstellt war. Die Behörde wurde jedoch in das Parteiamt der neuen „Central Cybersecurity and Informatization Leading Small Group" umgewandelt und später zur „Central Cyberspace Affairs Commission" erweitert. Den Vorsitz dieser Kommission übernahm Xi Jinping persönlich als Direktor. Im Jahr 2018 hatte die neue Internet-Informationsbehörde Cyberspace Administration of China (CAC) ihren Platz als operativer Arm der Kommission mit einer klaren Befehlslinie zur Führung der KPCh und des Staates sowie mit vollständiger Autorität und Gesamtverantwortung für das gesamte Cyberpolitik-System eingenommen.[41]

Die allgemein als Chinas „Internetzensoren" oder „Internetregulierer" bezeichnete CAC konsolidierte in den Folgejahren Chinas Internetgesetze mit einer Reihe noch weitreichenderer Gesetze, beginnend mit dem Cybersicherheitsgesetz (CSL) von 2017, dem neueren Datensicherheitsgesetz (DSL) und dem Gesetz zum Schutz persönlicher Daten (Personal Information Protection Law — PIPL). Mit diesen Gesetzen wurde eine stärkere Kontrolle über die Erhebung, Nutzung und Weitergabe von Daten durch die Einführung des Konzepts der „Datensouveränität" initiiert. Außerdem wurde dadurch der Staat gestärkt, indem ihm nach dem chinesischen Recht eine größere extraterritoriale Autorität verliehen wurde.

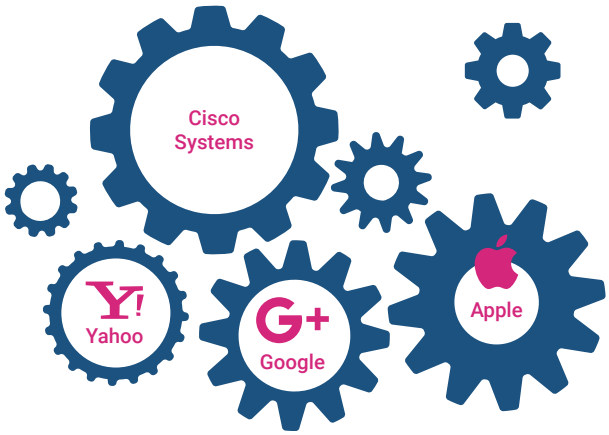
Im November 2017 verabschiedete der Ausschuss des Nationalen Volkskongresses das Cybersicherheitsgesetz. Dieses Gesetz stellt eine Kombination aus früheren Internet- und Zensurgesetzen dar. Damit wurde der rechtliche und administrative Rahmen zur Kontrolle vereinheitlicht und institutionalisiert. Danach wurden Netzbetreiber verpflichtet, Daten lokal in China zu speichern und auf Verlangen der staatlichen Sicherheitsbehörden auszuliefern. Die so genannte „kritische Informationsinfrastruktur" wurde Gegenstand einer nationalen Sicherheitsüberprüfung mit entsprechenden Auflagen in Bezug auf u.a. Datensicherheit, Beschaffung und grenzüberschreitende Datenströme. Personen bzw. Organisationen, welche die Netze nutzten, „durften nicht aufrufen zur Gefährdung der nationalen

39 „Freedom of Expression and the Internet in China." Human Rights News. https://www.hrw.org/legacy/backgrounder/asia/china-bck-0701.htm
40 Bei Feng. „China's Internet Censorship System." Human Rights in China. 14. Juli 2010. https://www.hrichina.org/en/content/3244
41 Nathan Attrill und Audrey Fritz. „China's Cyber Vision: How the Cyberspace Administration of China is building a new consensus on global Internet governance." ASPI. 2021. https://www.aspi.org.au/report/chinas-cyber-vision-how-cyberspace-administration-china-building-new-consensus-global

Souveränität, zum Umsturz des sozialistischen Systems, zum Separatismus, zum Bruch der nationalen Einheit, zu Terrorismus oder Extremismus, zu Völkerhass und zu ethnischer Diskriminierung, zur Verbreitung gewalttätiger, obszöner oder sexueller Inhalte oder zur Erzeugung bzw. Verbreitung von Falschinformationen, durch welche die Wirtschafts- oder Gesellschaftsordnung gestört werden könnte".[42]

Die Definitionen waren jedoch relativ vage, was zu zahlreichen Problemen führte. Zum einen waren einheimische als auch ausländische Unternehmen in China oft unsicher, was genau unter „kritische Informationsinfrastruktur" fällt und ob bzw. wie sie das Cybersicherheitsgesetz einzuhalten hatten. Aus diesem Grund wurden mit der Veröffentlichung der „Sicherheitsverordnung für kritische Informationsinfrastrukturen" durch den Staatsrat, die im September 2021 in Kraft trat, einige Erläuterungen hinzugefügt. In dieser Verordnung wurde beispielsweise erklärt, dass Unternehmen, die Daten verarbeiteten und an ausländischen Börsen notiert waren, als „kritische Informationsinfrastrukturen" betrachtet würden. Aufgrund dieser Bestimmung wurde 2021 gegen Didi Chuxing, Chinas führendes Fahrdienst-Unternehmen, vorgegangen, als es in den USA an die Börse ging.[43]

3.2. Die Zensur-Werkzeuge



3.2.1. Filterung

Obwohl das chinesische Zensursystem heute generell als „Great Firewall" bezeichnet wird, nannte sich das eigentliche offizielle Projekt das Projekt „Golden Shield", das als landesweites Sicherheitsmanagement-Informationssystem entwickelt wurde. Die GFW war ein Teilprojekt zur Zensur und Überwachung, das ab 1998 vom Ministerium für öffentliche Sicherheit betrieben wurde und 2003 vollständig in Betrieb genommen wurde.

Die GFW war ursprünglich auf die aktive Filterung des Internetdatenverkehrs ausgerichtet, um sensible Inhalte herauszufiltern, einschließlich IP-Adressbereiche, DNS, URL sowie DPI, basierend auf dem Erkennen von Mustern der Datenverkehrseinheiten im Internet, den sogenannten Paketen.[44] Für die Filterung wurde eine umfangreiche und dynamische Liste von Schlüsselwörtern entwickelt und geführt. Als immer mehr Nutzende damit begannen, Proxys wie den Tor-Browser oder VPNs zu verwenden, um die Filter zu umgehen, gingen die Zensoren der GFW dazu über, auch diesen Datenverkehr durch aktive Sondierung zu identifizieren und zu blockieren.[45]

Schon sehr bald nach dem Beginn des Projekts „Golden Shield" traten Blogging und später Micro-Blogging sowie soziale Medien in Erscheinung und wurden bei Nutzenden auf der ganzen Welt populär – auch in China. Mit dem sogenannten nutzergenerierten Inhalt, der im Zuge des Web 2.0-Phänomens in den Mittelpunkt rückte, überholten diese Inhalte schnell das Produktionsvolumen der klassischen Medien und anderer Internet-Nachrichten- und Informationsquellen. Die Zensoren mussten nicht mehr nur eingehende Inhalte aus dem Ausland blockieren, sondern auch die rasant zunehmenden Inhalte, die innerhalb der chinesischen Grenzen erzeugt wurden, insbesondere von den Usern. Neben der Filterung auf der Backbone-Ebene musste das GFW-System nun auch den großen Internet-Diensten und Social-Media-Plattformen in China die Aufgabe übertragen, die auf ihren Plattformen generierten Inhalte zu filtern.

Die Plattformen richten häufig Listen mit Schlüsselwörtern für die Filterung ein, die auf Listen der Regierungsbehörden basieren. Die Abwicklung wurde immer dynamischer und musste schnell auf neue Veränderungen reagieren. Chinesische Internetnutzende sind dafür bekannt, dass sie Homonyme bzw. Homofone (Schriftzeichen mit gleicher Aussprache, aber unterschiedlicher Bedeutung), bewusst falsch geschriebene oder Varianten von Schriftzeichen und sogar Tippfehler als Ersatz für gesperrte sensible Schriftzeichen, Schlüsselwörter oder Phrasen verwenden, um die GFW-Zensur zu umgehen.[46] So rekrutierte Weibo (ehemals Sina Weibo), Chinas führende Twitter-ähnliche Mikroblogging-Plattform, im Jahr 2017 öffentlich 1.000 User als "Weibo-Überwacher", die helfen sollten, „pornografische, illegale oder schadhafte" Nachrichten zu überwachen und diese zu melden.[47] Im Zuge der jüngsten Welle von Maßnahmen gegen diese Umgehungstaktiken kündigte Weibo an, seinen „Phrasen-Managementmechanismus" zu verbessern und sein „Schlüsselwortidentifikationsmodell" zu perfektionieren, um ein positives Anreizsystem zu etablieren, das „die Nutzenden dazu bringt, die chinesischen Schriftzeichen auf seiner

42 Rogier Creemers, Paul Triolo und Graham Webster. „Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)." 2018. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/

43 Paul Triolo, Samm Sacks, Graham Webster und Rogier Creemers. „After 5 Years, China's Cybersecurity Rules for Critical Infrastructure Come Into Focus." 08. August 2021. https://digichina.stanford.edu/work/after-5-years-chinas-cybersecurity-rules-for-critical-infrastructure-come-into-focus/

44 Charles Arthur. „China tightens 'Great Firewall' internet control with new technology." The Guardian. 14. Dezember 2012. https://www.theguardian.com/technology/2012/dec/14/china-tightens-great-firewall-internet-control

45 „Learning more about the GFW's active probing system." 14. September 2015. https://blog.torproject.org/learning-more-about-gfws-active-probing-system/

46 Victor Mair. „Typos as a means for circumventing censorship." https://languagelog.ldc.upenn.edu/nll/?p=55382

47 https://m.weibo.cn/status/4156562153528739

Plattform korrekt zu gebrauchen".[48] Doch angesichts der Komplexität der chinesischen Sprache und der Kreativität der Nutzenden – wenn zum Beispiel das chinesische Wort für Holland („Helan") für die Provinz Henan verwendet wird, um über die dortige Bankenkrise im Jahr 2022 zu diskutieren – dürfte das Blocken von Zeichen, Wörtern und Phrasen einen großen Kollateralschaden verursachen, und die Nutzererfahrung in hohem Maße beeinträchtigen.

Im Jahr 2022 wurden diverse Dokumente von Xiaohongshu, einer chinesischen Instagram-ähnlichen Plattform, an die Öffentlichkeit gebracht, aus denen hervorging, dass die moderierenden Personen der Seite über einen Zeitraum von zwei Monaten hinweg 546 Spitznamen für Xi Jinping ermittelt hatten.[49] Diese Enthüllung zeigt, dass die Betreibenden bei großen politischen Ereignissen, politischen Aufruhren bzw. deren Jahrestagen sowie bei Naturkatastrophen oder Unfällen in Echtzeit reagieren, um den Auflagen der Cyberspace Administration of China, der obersten nationalen Stelle für die Internetzensur, nachzukommen.[50]

Es ist offensichtlich, dass die Zensurmaßnahmen im Laufe der Jahre systematischer und automatisierter, zugleich aber zunehmend weniger transparent geworden sind. Im Jahr 2016 berichtete das Citizen Lab, dass Nutzende von WeChat – der „Messaging-Super-App" von Tencent – im Gegensatz zu früher nicht mehr darüber informiert wurden, wenn ihre Nachrichten blockiert wurden. Außerdem werden in Gruppenchats mehr Schlüsselwörter blockiert als in Einzelchats, was darauf hindeutet, dass die Zensur stärker auf Nachrichten ausgerichtet ist, die ein größeres Publikum erreichen und zu organisierten Gruppenaktionen führen könnten. Außerdem bietet die App registrierten Nutzenden außerhalb Chinas mehr Flexibilität als im Inland, obwohl User außerhalb Chinas trotzdem auch von der Zensur betroffen sind.[51]

Und so hat die GFW damit begonnen, sich zusammen mit diesen chinesischen Apps und Diensten über Chinas Grenzen hinaus zu erstrecken. Im Jahr 2020 deckte das Citizen Lab auf, dass WeChat außerhalb Chinas registrierte Konten überwachte und diese Nachrichten nutzte, um seinen Zensur-Algorithmus zu optimieren, der auf in China registrierte Konten angewendet wird. Für User gab es keine Transparenz oder Offenlegung in den entsprechenden Nutzungsbedingungen.[52]

Im Juli 2022 beklagte eine chinesische Schriftstellerin auf Weibo, dass ihr der Zugriff auf ihre eigene unveröffentlichte Arbeit mit 1,3 Millionen Schriftzeichen entzogen worden sei, die online in der WPS Office-Cloud-Textverarbeitungsplattform des chinesischen Softwareentwicklers Kingsoft gespeichert war. Die Begründung dafür lautete, dass „die Datei möglicherweise sensible Inhalte enthalte und der Zugriff entzogen wurde". Dies bestätigt, dass die GFW-Überwachung und -Zensur auch auf Cloud-basierte Anwendungen und Service-Anbieter ausgeweitet wurde. Der Weibo-Post der Schriftstellerin veranlasste zahlreiche weitere chinesische User, ähnliche Erfahrungen zu teilen, die sie selbst zu demselben Thema gemacht hatten. Einige Nutzende behaupteten sogar, dass WPS Office nicht nur Online-, sondern auch Offline-Dateien löschen kann. Kingsoft reagierte auf die Anschuldigungen mit der Aussage, dass der betroffene User im Verdacht stand, gegen die „Richtlinien der Plattform" verstoßen zu haben.[54]

Fang Binxing, der oft als „Gründervater" der GFW bezeichnet wird, erklärte 2011 in einem Interview, dass das Jahr 1998 einen Wendepunkt in der Entwicklung des chinesischen Internets markierte, als die Internetportale Sina und Sohu ins Leben gerufen wurden und die Zahl der Internetuser in China die Marke von einer Million erreichte. Er erklärte, dass die Regierung damals anfangen musste, aufzupassen, und meinte, dass „der Bau der Great Firewall eine natürliche Reaktion auf etwas Neuartiges und Unbekanntes war". Außerdem rechtfertigte er die GFW als ein „weltweit verbreitetes Phänomen" und behauptete, dass „rund 180 Länder, darunter Südkorea und die USA, ebenfalls das Internet überwachten". Diese Aussage ist jedoch insofern irreführend, weil sie die Internetbestimmungen in demokratischen Ländern mit der drakonischen Zensur in autokratischen Ländern gleichsetzt. Fang scheute sich nicht, die politische Natur seiner Position zuzugeben und sagte, dass „China sich gegen die Einmischung anderer Länder in die inneren Angelegenheiten Chinas unter dem Banner der Internetfreiheit verwehre".[55] Bis zum heutigen Tag repräsentiert diese Aussage die chinesische Mentalität in Bezug auf die Rechtfertigung der Entscheidung, den Bürgerinnen und Bürgern ihre Freiheit im Internet zu beschneiden.

3.2.2. Spyware

Zurückblickend erscheint es paradox, dass China im Jahr 2001, während das Projekt „Golden Shield" auf Hochtouren lief, der WTO beitrat und damit die Öffnung des Landes für die Weltwirtschaft eingeleitet wurde. Die Liste der bis dato nicht eingehaltenen Verpflichtungen Chinas gegenüber der WTO ist lang, insbesondere im Hinblick auf die Öffnung des chinesischen Marktes für ausländische Hersteller von Informations- und Kommunikationstechno-

48 „Weibo vows to regulate homonyms, 'misspelt' words, if they are used to evade China's strict censorship." 14. Juli 2022. https://www.scmp.com/tech/policy/article/3185299/weibo-vows-regulate-homonyms-misspelt-words-if-they-are-used-evade

49 Joseph Brouwer. „List of derogatory nicknames for Xi leaked amid crackdown on 'typos'." 20. Juli 2022. https://chinadigitaltimes.net/2022/07/list-of-derogatory-nicknames-for-xi-leaked-amid-crackdown-on-typos/

50 Joseph Brouwer. „How Xiaohongshu censors 'sudden incidents'." 27. Juli 2022. https://chinadigitaltimes.net/2022/07/how-xiaohongshu-censors-sudden-incidents/

51 Lotus Ruan, Jeffrey Knockel, Jason Ng und Masashi Crete-Nishihata. „One App, Two Systems: How WeChat uses one censorship policy in China and another internationally." The Citizen Lab. 30. November 2016. https://citizenlab.ca/2016/11/wechat-china-censorship-one-app-two-systems/

52 Miles Kenyon. „WeChat Surveillance Explained." The Citizen Lab. 07. Mai 2020. https://citizenlab.ca/2020/05/wechat-surveillance-explained/

53 Coco Feng. „Chinese word processor WPS accused of censorship after author says she was locked out of 1.3 million-character document." 14. Juli 2022. https://www.scmp.com/tech/big-tech/article/3185239/chinese-word-processor-wps-accused-censorship-after-author-says-she

54 „Kingsoft's Office Software WPS Denies Deleting User Local Files." https://pandaily.com/kingsofts-office-software-wps-denies-deleting-user-local-files/

55 „Great Firewall father speaks out." Global Times. 18. Februar 2011. https://web.archive.org/web/20110225205053/http://english.sina.com/china/p/2011/0217/360409.html

logien und im Bereich der Telekommunikation.[56] Im Jahr nach dem WTO-Beitritt Chinas stiegen die Investitionskosten für die Zensur im Rahmen des Projekts „Golden Shield“ auf 770 Millionen USD, und die Zahl der für die Zensur zuständigen Polizei- und Sicherheitsbeamten wurde auf rund 30.000 geschätzt. Trotz der Kritik aus dem Westen verkündeten die Beteiligten des Projekts damals stolz, dass sie davon ausgingen, dass das Zensurprojekt vor den Olympischen Spielen 2008 in Peking abgeschlossen sein würde – einem weiteren Ereignis, das nach Ansicht der westlichen Welt zur Integration Chinas in die internationale Gemeinschaft beitragen würde. Die Hoffnungen erwiesen sich jedoch als reines Wunschdenken.

Mit all diesen Investitionen und Ressourcen ging es bei dem Projekt „Golden Shield“ natürlich nie nur um die Filterung, obwohl diese Funktion seit jeher das Kernstück der chinesischen Zensur bildete. Die chinesischen Zensoren versuchten es auch mit anderen Methoden, allerdings mit sehr unterschiedlichem Erfolg. Bei dem bekanntesten Beispiel handelt es sich um den sogenannten „Green Dam“ aus dem Jahr 2009:

Im Mai 2009 gab das Ministerium für Industrie und Informationstechnologie (MIIT) bekannt, dass auf PCs, die in China verkauft werden, ab dem 1. Juli eine „grüne Online-Filtersoftware“ namens „Green Dam Youth Escort“ vorinstalliert sein müsse.[57] Hersteller wurden verpflichtet, die Anzahl der mit der Software vorinstallierten Computer, die ausgeliefert wurden, an die Regierung zu melden. Die Software war in der Lage, automatisch eine Liste von Websites und Schlüsselwörtern herunterzuladen und zu aktualisieren, den Zugriff auf diese Websites zu sperren und ein Textverarbeitungsprogramm zu schließen, wenn ein zensiertes Schlüsselwort eingegeben wurde. Die Software konnte angeblich sogar pornografische Bilder erkennen, indem sie gezielt nach Hauttönen auf den Bildern suchte. Zu dieser Zeit folgten viele der asiatischen PC-Marken aus Taiwan, Japan und China selbst der Anordnung, wie z. B. Acer, Sony, Lenovo, Asus und BenQ, während viele der US-Marken, wie Hewlett-Packard und Dell, sich widersetzten.[58]

„Green Dam“ war von der ersten Stunde an ein Fiasko. Das US-amerikanische Softwareunternehmen Solid Oak Software machte geltend, dass die Quellcodes seines Produkts CYBERsitter kopiert wurden.[59] Die Software enthielt Bugs, funktionierte nicht besonders gut und war für erfahrene User relativ einfach zu umgehen. Sogar das Passwort zur Freischaltung und Deaktivierung der Software wurde gehackt und im Internet verbreitet.[60] In einer ungewöhnlichen und zugleich peinlichen Wendung der Ereignisse gab das MIIT vor dem geplanten Inkrafttreten des Programms bekannt, dass es auf unbegrenzte Zeit ausgesetzt werde. „Green Dam“ wurde im August eingestellt, als das MIIT erklärte, dass die Vorinstallation von „Green Dam“ für Computer, die im Einzelhandel verkauft wurden, nicht mehr erforderlich war, sondern nur noch für Computer in Schulen, Internetcafés und öffentlichen Einrichtungen. [61]

Obwohl „Green Dam“ fehlschlug, handelte es sich um den ersten großen Versuch, de facto eine Spionagesoftware direkt auf den Computern aller chinesischen Nutzenden zu installieren. Gewiss war das nicht der letzte Versuch, die Zensur bis auf die Geräte-Ebene zu dezentralisieren. Seit dem Jahr 2013 wird berichtet, dass die Regierung von Xinjiang damit begann, in großem Umfang Malware auf Android-Telefonen zu installieren, die von der lokalen uigurischen Bevölkerung genutzt werden. Dies wurde erreicht, indem die Telefone von Bürgerinnen und Bürgern entweder gehackt oder schlicht beschlagnahmt und später mit installierter Malware retourniert wurden. In einigen Fällen wurde Bürgerinnen und Bürgern ein völlig anderes Telefon zurückgegeben. Die installierte Spyware ermöglichte es den Beamten, sämtliche Aktivitäten der Telefonnutzenden in Echtzeit zu überwachen.[62]

In der Tat öffnen mobile Apps auf Smartphones heutzutage die Türen auf die Geräte: Hackern, um ahnungslose User zum Herunterladen von Apps mit Malware oder Spyware zu verleiten. Oder autokratischen Regimen, die ihren Bürgerinnen und Bürgern schlichtweg befehlen, bestimmte Programme herunterzuladen. So hat beispielsweise die Kriminalpolizei des chinesischen Ministeriums für öffentliche Sicherheit eine App mit dem Namen „National Anti-Fraud Center“ entwickelt, deren Zweck es sein soll, dass Nutzende der Polizei Online- oder Telefonbetrugsfälle melden können. Es wird geschätzt, dass sie über 200 Millionen Mal heruntergeladen wurde. Allerdings wurde festgestellt, dass die App zu viele Daten von den Telefonen der Nutzenden sammelt, darunter persönliche Informationen, Browserverlauf, Chat-Inhalte, Standortdaten usw. Einige User der App berichteten sogar, dass sie von der Polizei kontaktiert wurden, nachdem sie bestimmte ausländische Finanzwebseiten aufgerufen hatten.[63]

3.2.3. Virtuelle private Netzwerke

Obwohl die Regulierung internationaler Netzwerke die Basis für das Verbot der Nutzung virtueller privater Netzwerke (VPN) oder anderer Proxy-Dienste wie Tor bildet, um die von der Regierung sanktionierten Netzwerkdienste ohne Genehmigung zu umgehen, ist China dafür bekannt, nur hin und wieder den Druck zu erhöhen, um öffentliche

56 Stephen Ezell. „False Promises II: The Continuing Gap Between China's WTO Commitments and Its Practices.“ Information Technology and Innovation Foundation. 26. Juli 2021. https://itif.org/publications/2021/07/26/false-promises-ii-continuing-gap-between-chinas-wto-commitments-and-its/

57 “关于计算机预装绿色上网过滤软件的通知. 工业和信息化部.” May 19, 2009. https://web.archive.org/web/20090612021926/http://www.miit.gov.cn/n11293472/n11293832/n11293952/12398220.html

58 Joe McDonald. „PC makers voluntarily supply web filter in China.“ The Global and Mail. The Associated Press. 02. Juli 2009. https://web.archive.org/web/20090706135434/http://www.theglobeandmail.com/news/technology/pc-makers-voluntarily-supply-web-filter-in-china/article1203981/

59 Charles Mok. „Green Dam: „Bad Idea.“ Computerworld Hong Kong. Juli 2009. https://charlesmok.blogspot.com/2009/07/green-dam-bad-idea.html

60 “绿坝-花季护航软件遭破解 使用者绕开密码限制.” https://www.163.com/tech/article/5BHDPD8F000915BD.html

61 „Green Dam Youth Escort.“ Wikipedia. https://en.wikipedia.org/wiki/Green_Dam_Youth_Escort#cite_note-6

62 Paul Mozur und Nicole Perlroth. „China's Software Stalked Uyghurs Earlier and More Widely, Researchers Learn.“ The New York Times. 01. Juli 2020. https://www.nytimes.com/2020/07/01/technology/china-uighurs-hackers-malware-hackers-smartphones.html

63 “国家反诈中心. 中國數字空間.” https://chinadigitaltimes.net/space/%E5%9B%BD%E5%AE%B6%E5%8F%8D%E8%AF%88%E4%B8%AD%E5%BF%83

Warnungen oder individuelle offizielle Verwarnungen für Personen auszusprechen, denen die Nutzung von VPNs nachgewiesen wurde. Erstmals wurde jedoch 2019 berichtet, dass gegen einen Nutzer in der Provinz Guangdong eine Geldstrafe von 1.000 Yuan für die Nutzung eines VPNs erhoben wurde.[64]

In der Tat wurde erst 2017, unter der Xi-Administration, vom MIIT ein 14-monatiges „Aufräumen" des Internets angekündigt. Die Regierung setzte drastischere administrative und technische Mittel ein, um die Umgehung der Zensur zu erschweren: Die staatlichen Internetanbieter China Telecom, China Mobile und China Unicom wurden angewiesen, VPN-Protokolle in ihren Netzen zu blocken – mit Ausnahme der staatlich zugelassenen, die in der Regel bestimmten staatlichen Organisationen und Behörden vorbehalten sind.[65] Eine der Methoden, die von den chinesischen Zensoren eingesetzt werden, besteht in der aktiven Sondierung, bei der sie die Instanzen aller zuvor unbekannten ausgehenden VPN-Verbindungen überprüfen, um zu versuchen, ihre Sperrliste für VPNs zu verifizieren.[66] Diese Listen können dynamisch erstellt werden, indem die IP-Verbindungen von Tor- und VPN-Servern über einen längeren Zeitraum analysiert werden. Das veranlasst viele VPN- und Proxy-Anbieter dazu, ihre dynamische IP-Adressierung und andere robustere Umgehungsmethoden weiter zu verbessern.

Das Verbot von VPNs ist für ausländische Unternehmen, die in China tätig sind, besonders unangenehm, da es ihnen den Zugang zu den internationalen Internetdiensten erschwert, die sie für ihre Geschäfte benötigen, z. B. zu allen nicht-chinesischen sozialen Medien, E-Mail- und Nachrichtenplattformen. Teilweise werden SIM-Karten aus dem Ausland verwendet, um Zugang zu diesen Diensten zu erlangen. Im Juli 2017 folgte Apple der Anordnung Chinas, VPN-Apps aus der chinesischen Version des App-Stores zu entfernen. VPN-Apps werden in China nun als „illegale Inhalte" eingestuft. Dadurch wird den chinesischen Usern im Inland der Zugang zu solchen Tools erschwert. Gleichzeitig stellt es einen gefährlichen Präzedenzfall dar, wenn ein so großer Konzern mit einer solchen Marktposition im Auftrag einer autokratischen Regierung die Zensur auf seiner Plattform durchsetzt.[67] Es überrascht leider nicht mehr, dass im Oktober 2022 Apple kurzerhand die AirDrop-Nutzung mittels eines Software-Updates ausschließlich für chinesische User einschränkte, als entdeckt wurde, dass User in China die Apple iPhone-Funktion AirDrop nutzten, um Fotos im Zusammenhang mit dem Protest und dem Slogan eines Demonstranten namens „Bridge Man" mit iPhone-Usern in der Nähe auszutauschen, ohne auf ein Mobilfunk- oder WiFi-Netz zuzugreifen.[68]

3.2.4. Internet-Abschaltungen

Die extremste Form der Zensur ist das Abschalten des Internets, bei dem der Zugang zum Netz vollständig oder in großem Umfang abgeschaltet wird, z.B. für große Kommunikations- oder Informationsdienste. Ein Bericht über Abschaltungen des Internets aus dem Jahr 2022, der vom Büro des Hohen Kommissars der Vereinten Nationen für Menschenrechte veröffentlicht wurde, kam zu dem Schluss, dass „Internet-Abschaltungen zu erheblichen Beeinträchtigungen der Wirtschaft, der demokratischen Prozesse und des Informationsflusses führen, die das Vertrauen in Wahlprozesse gefährden und das Risiko von Feindseligkeiten und Gewalt verstärken können", und forderte die Mitgliedsstaaten auf, „von der Unterbrechung des Internetzugangs, inklusive der Drosselung oder Begrenzung der Bandbreite" abzusehen.[69]

Weltweit gibt es jedoch immer mehr Regierungen, die das Internet abschalten, um die freie Meinungsäußerung oder politische Uneinigkeit zu unterbinden. Für China lässt sich allerdings sagen, dass das Land, möglicherweise aufgrund seines akribischen „Managements" des Internets durch sein ausgefeiltes Zensur- und Überwachungssystem, nur selten zu diesem drastischen „Shortcut", der vollständigen Trennung von Verbindungen, greifen muss.[70] Aber es gibt auch beachtenswerte Ausnahmen.

Seit den Volksunruhen in Urumqi, Xinjiang, am 6. Juli 2009, bei denen nach Angaben der Behörden 200 Menschen ums Leben kamen, hat China seine Maßnahmen und die Kontrolle über die Region und ihre muslimische Bevölkerung sowohl offline als auch online verschärft. Es wurden Verordnungen zur Bekämpfung von „Falschinformationen" und Strafen für Website-Betreibende für das Veröffentlichen von „nicht verifizierten Inhalten" erlassen. Der Zugang zum Internet wurde für die gesamte Bevölkerung Xinjiangs abgeschaltet, so dass sie nur noch auf von der Regierung genehmigte Websites zugreifen konnte. Auf diese Weise wurde das Internet zu einem abgeschotteten „Intranet", das lediglich den Empfang von Informationen zulässt.[71] Mitte Mai 2010 wurde dann plötzlich verkündet, dass die Abschaltung wieder „aufgehoben" werde. Daraufhin strömten die Bürgerinnen und Bürger in die Internetcafés, um die seit Monaten ungelesenen E-Mails abzurufen oder um Online-Games zu spielen. Und während viele Schwierigkeiten hatten, sich an ihre Passwörter zu erinnern, wurde natürlich alles weiterhin streng überwacht.[72]

64 David Spencer. „China's VPN crackdown now targeting individual users." 03. Februar 2020. https://www.vpncompare.co.uk/china-vpn-crackdown-individual-users/
65 Olivia Solon. „China cracks down on VPNs, making it harder to circumvent Great Firewall." 23. Januar 2017. https://www.theguardian.com/technology/2017/jan/23/china-vpn-cleanup-great-firewall-censorship
66 „Learning more about the GFW's active probing system." 14. September 2015. https://blog.torproject.org/learning-more-about-gfws-active-probing-system/
67 Saheli Roy Choudhury. „Apple removes VPN apps in China as Beijing doubles down on censorship." 01. August 2017. https://www.cnbc.com/2017/07/31/apple-removes-vpn-apps-in-china-app-store.html
68 Karen Gilchrist. „Apple limited a crucial AirDrop function in China just weeks before protests." CNBC. 30. November 2022. https://www.cnbc.com/2022/11/30/apple-limited-a-crucial-airdrop-function-in-china-just-weeks-before-protests.html
69 Hanna Kreitem. „The U.N. Calls on States to Stop Shutting Down the Internet." 11. Juli 2022. https://pulse.internetsociety.org/blog/the-u-n-calls-on-states-to-stop-shutting-down-the-internet
70 James Griffiths. „Internet shutdowns used to be rare. They're increasingly becoming the norm in much of the world." 21. Dezember 2019. https://www.cnn.com/2019/12/21/asia/internet-shutdowns-china-india-censorship-intl-hnk
71 Edward Wong. „Xinjiang, Tense Chinese Region, Adopts Strict Internet Controls." 10. Dezember 2016. https://www.nytimes.com/2016/12/10/world/asia/xinjiang-china-uighur-internet-controls.html
72 Edward Wong. „After Long Ban, Western China Is Back Online." 14. Mai 2010. https://www.nytimes.com/2010/05/15/world/asia/15china.html

4. Die Beteiligten

4.1. Die Internet-basierte Zivilgesellschaft, die keine ist

Bürgerbeteiligung war nie ein Konzept, das von den chinesischen Machthabenden akzeptiert wurde. Mit Beginn der Ära von Xi Jinping im Jahr 2013 gesellte sich das Konzept der Zivilgesellschaft zu einer langen Liste liberaler Werte, die als „westliche Ansichten" betrachtet wurden und die das Regime als Konkurrenz in einem „intensiven Kampf" gegen seine Legitimität ansah. In der neunten Verlautbarung aus dem Jahr 2013, dem „Kommuniqué zur aktuellen Lage der ideologischen Sphäre" oder dem so genannten „Dokument Nummer 9", wurde die Zivilgesellschaft als eines der Konzepte aufgeführt, die das Land bedrohen – zusammen mit dem Konstitutionalismus, der Marktwirtschaft, den Universalwerten, der Pressefreiheit im Internet und der Aufarbeitung der Geschichte Chinas.

In dem Dokument wurde die Zivilgesellschaft wie folgt beschrieben: „Die Zivilgesellschaft ist eine aus dem Westen stammende soziale und politische Theorie, die behauptet, dass die Rechte des Einzelnen in der sozialen Sphäre an erster Stelle stehen und dass der Staat nicht in diese Rechte eingreifen darf. In den letzten Jahren wurde das Konzept der Zivilgesellschaft von westlichen, antichinesischen Kräften zu einem politischen Instrument umfunktioniert, und auch in unserem Land wird es von einigen Leuten mit verborgenen Absichten propagiert. Dies manifestiert sich vor allem darin, dass die Zivilgesellschaft dazu benutzt wird, westliche politische Konzepte zu propagieren, und dass die Schaffung einer Zivilgesellschaft in China eine Voraussetzung für die Gewährleistung individueller Rechte und die Grundlage für die Verwirklichung einer konstitutionellen Demokratie ist; die Zivilgesellschaft wird als „Allheilmittel" für den Fortschritt der gesellschaftlichen Entwicklung an der Basis in China erachtet, und es werden alle möglichen sogenannten Bürgeraktivitäten unternommen. Der Kern der Propagierung einer Zivilgesellschaft besteht darin, dass sie darauf abzielt, die Führung der Parteiorganisation und das Regime an der Basis von der Selbstverwaltung durch die Massen auszuschließen und sie sogar gegeneinander auszuspielen, um so politische Oppositionskräfte zu bilden."[73]

73 Roger Creemers (übersetzt). „Communique on the Current State of the Ideological Sphere (Document No. 9)." DigiChina. 23. April 2013. https://digichina.stanford.edu/work/communique-on-the-current-state-of-the-ideological-sphere-document-no-9/

Diese feindselige und politisierte Haltung gegenüber der Zivilgesellschaft ist für die KPCh nicht neu, aber sie ist unter der Leitung von Xi noch extremer geworden. Die KPCh war schon immer paranoid in Bezug auf Bedrohungen der Stabilität ihres Regimes, die von Gruppen ausgehen, die sich für eine Sache einsetzen, egal wie akzeptabel oder harmlos diese für die meisten Menschen erscheinen mag. Ob es um Umweltschutz, Arbeitnehmerrechte, Patientenrechte, sexuelle oder rassische Gleichberechtigung, Armut, LGBTIQ-Rechte oder sogar Fangemeinden geht, die Partei beobachtet das immer mit Skepsis.[74] Daher ist der Raum für die Zivilgesellschaft, sich im Internet zu organisieren, in den letzten zehn Jahren in China immer kleiner geworden.

Auf der anderen Seite wurde das Internet selbst unter der Prämisse aufgebaut, dass es niemandem gehört, insbesondere nicht den Regierungen. Gleichzeitig gehört das Internet aber auch allen: durch die Beteiligung zahlreicher Interessengruppen, insbesondere auf globaler Ebene durch die Zusammenarbeit von Gemeinschaften aus dem technischen Sektor, der Zivilgesellschaft, dem kommerziellen Bereich und Regierungen. Seit mehr als 15 Jahren bringt das Internet Governance Forum (IGF), das unter dem Mandat der Vereinten Nationen eingerichtet wurde, zahlreiche Interessengruppen zusammen, um über politische Fragen zu beraten, und die Zivilgesellschaft wurde stets als wichtiger Teil dieses Prozesses betrachtet.

Wer kann also die internetbasierte Zivilgesellschaft in China repräsentieren? Die Internet Society of China (ISC) ist nach eigenen Angaben eine nichtstaatliche Organisation mit über 1.300 Mitgliederinnen und Mitgliedern, zu denen sowohl Einzelpersonen als auch Organisationen gehören, darunter „renommierte Expertinnen und Experten“, „angesehene Wissenschaftlerinnen und Wissenschaftler“ sowie Industrieunternehmen und Forschungsinstitute. Sie wird von diversen Ministerien unterstützt, und ihr derzeitiger Präsident ist ein ehemaliger Minister des MIIT und ehemaliger Vorstandsvorsitzender von China Mobile.[75] Die bedeutendste Errungenschaft des ISC war die Zusammenarbeit mit der Regierung, als es darum ging, „selbstdisziplinäre Regelungen“ zu erlassen und zu vermitteln, insbesondere die öffentliche Verpflichtung zur Selbstdisziplin für die chinesische Internetindustrie aus dem Jahr 2002,[76] mit weit gefassten und wohlwollenden Zielen wie beispielsweise dem Fördern der Internetnutzung, der Prävention von Internetkriminalität, dem Fördern eines gesunden Wettbewerbs in der Branche und der Vermeidung von Urheberrechtsverletzungen. Zugleich enthielt die Verpflichtung aber auch politisch orientierte Aufforderungen, keine „schadhaften Informationen zu erzeugen, zu veröffentlichen oder zu verbreiten, welche die staatliche Sicherheit gefährden und die soziale Stabilität stören könnten“, einschließlich „illegaler Informationen" oder „Aberglauben und Obszönitäten“; andernfalls würden solche Materialien entfernt werden.[77] Die Verpflichtung wurde besonders umstritten, als sie von verschiedenen US-Internetdienstleistern wie Google, Microsoft und Yahoo! unterzeichnet wurde, um Marktzulassungen in China zu erhalten, was den quasi-staatlichen Status der ISC untermauert.
Als solche kann die Gruppe kaum als wirkliche NGO oder zivilgesellschaftliche Gruppe bezeichnet werden. Sie ist bestenfalls eine quasi-staatliche Organisation. Und dennoch ist die ISC möglicherweise die einzige Organisation, die China bzw. seine User in internationalen Foren vertritt, z. B. als Ausrichter von Sitzungen in Foren zur Internetregulierung und im Rahmen des World Summit on the Information Society, die von diversen UN-Vertretern veranstaltet werden. Eine Rolle, die normalerweise von ernsthaften Akteuren aus Zivilgesellschaften anderer Länder übernommen wird. Man kann also zu dem Schluss kommen, dass es in China keine echte Zivilgesellschaft gibt und dass die Internet-User keine wirkliche Stimme haben, wenn es um Internetregulierung geht.

4.2. Chinese Big Tech: Eine kleine Gruppe Begünstigter

Die Politik der chinesischen Internetindustrie bestand schon immer darin, Gewinnende auszuwählen, indem sie die ausländischen Marktführer verdrängt und stattdessen eine begrenzte Anzahl einheimischer Unternehmen in jedem Bereich an die Spitze bringt, um es den Zensoren einfacher zu machen, diese Unternehmen im Gegenzug für größere Marktanteile gefügig zu halten. Die Regierung hat nach wie vor die ausschließliche Kontrolle über staatliche Unternehmen in den Bereichen Infrastruktur und Basis-Telekommunikationsdienste. Darüber hinaus findet auf den Dienstleistungsebenen eine Konsolidierung statt und es werden Begünstigte ausgewählt.

Die chinesische Suchmaschine Baidu hat gegenwärtig einen geschätzten Marktanteil von über 75 Prozent.[78] Die Situation war jedoch etwas anders, als Google zwischen 2000 und 2010 in China präsent war: Noch 2009, ein Jahr vor dem Ausstieg von Google aus dem chinesischen Suchmaschinenmarkt, hielt das Unternehmen über 30 Prozent Marktanteil.[79]

Der erste chinesische Twitter-ähnliche Microblogging-Dienst, Fanfou, startete im Jahr 2007. Er war der „Publikumsliebling“, der ein relativ offenes Forum bot, in dem liberale Diskussionen erlaubt waren. Doch bekam er schon bald starke Konkurrenz von anderen Nachahmenden aus

74 Lawrence Deane. „Will There Be a Civil Society in the Xi Jinping Era? Advocacy and Non-Profit Organising in the New Regime.“ 15. Juli 2021. https://madeinchinajournal.com/2021/07/15/will-there-be-a-civil-society-in-the-xi-jinping-era-advocacy-and-non-profit-organising-in-the-new-regime/
75 Internet Society of China, https://www.isc.org.cn/en
76 „Public Pledge of Self-Regulation and Professional Ethics for China Internet Industry.“ https://govt.chinadaily.com.cn/s/201812/26/WS5c23261f498eb4f01ff253d2/public-pledge-of-self-regulation-and-professional-ethics-for-china-internet-industry.html
77 „Chinese sites agree to censor content.“ The Guardian. 16. Juli 2002. https://www.theguardian.com/technology/2002/jul/16/onlinesecurity.internetnews
78 „Top 5 Chinese Search Engines in 2022 [With Market Share].“ https://www.adchina.io/top-chinese-search-engines/
79 Joe McDonald. „Google defends shrinking China market share. Google history in China.“ Associated Press. 20. September 2010. http://ig-legacy.ft.com/content/faf86fbc-0009-11df-8626-00144feabdc0

dem Internetportal- und Messaging-Sektor, wie Sina Weibo, Sohu Weibo, Netease Weibo und Tencent Weibo. Als kleinerem, unabhängigem Unternehmen wurde der Dienst von Fanfou in seiner Anfangszeit häufig unterbrochen, und im Jahr 2009 wurde er nach den Unruhen in Urumqi in Xinjiang[80] für ein Jahr ausgesetzt, ehe er wieder freigegeben wurde.[81] Kleinere Unternehmen wie Fanfou konnten nur schwer konkurrieren, weil ihnen die Mittel fehlten, ausreichend moderierendes Personal einzustellen, um den staatlichen Zensuranordnungen gerecht zu werden. Letztendlich konnte Sina Weibo den Markt erobern, während andere große Konkurrenten wie Sohu, Netease und Tencent ihre Dienste einstellten, so dass es für die Regierung einfacher war, sich mit nur einem großen Anbieter auseinanderzusetzen. Derzeit, im ersten Quartal 2022, zählt Sina Weibo rund 582 Millionen monatlich aktive User und 252 Millionen täglich aktive User.[82]

Das bedeutet jedoch nicht, dass chinesische Internet-Dienstleister keine erfolgreichen einheimischen Innovationen hervorbringen können. Tencent's WeChat ist das hervorstechendste Beispiel. Das Unternehmen wurde 1998 als Messaging-Dienstanbieter gegründet, und zwar ursprünglich mit einem Produkt namens QICQ, das später in QQ umbenannt wurde. Das Aushängeschild „WeChat" wird heutzutage oft als „Super-App" bezeichnet, die Instant Messaging, soziale Medien, mobilen Online-Handel und Zahlungen als auch „Miniprogramme" kombiniert, die auf ihrem Plattform-Ökosystem betrieben werden. Im ersten Quartal 2022 hatte WeChat 1,26 Milliarden aktive User zu verzeichnen. Während WeChat knapp 20 Prozent des Gesamtumsatzes des Unternehmens ausmacht,[83] hat sich Tencent zudem zum weltweit größten Anbieter von Online-Games entwickelt.[84] Darüber hinaus hat das Unternehmen erhebliche Investitionen in diverse sensible britische Technologiesektoren getätigt, darunter das führende digitale Bankunternehmen Monzo.[85] Vor kurzem hat Tencent sogar in den britischen Militärsoftware-Entwickler Hadean investiert. Dies ist für ein Unternehmen, das in der chinesischen Überwachung und Zensur sowohl im Inland als auch im Ausland verwurzelt ist, eher untypisch.

Im Jahr darauf, 1999, wurde Alibaba gegründet, um ein B2B-E-Commerce-Portal und Transaktionsdienste anzubieten. Auf diese Weise wurde Chinas zunehmender Status als "die Weltfabrik" genutzt, um sowohl auf nationaler als auch auf internationaler Ebene eine Vormachtstellung zu gewinnen. Seitdem hat sich das Unternehmen mit den Marktplatzplattformen Taobao und Tmall auf Dienstleistungen für die Bereiche C2C und B2C im Online-Handel ausgeweitet, unterstützt durch seine Zahlungsplattformen, wie beispielsweise AliPay. Die Finanztechnologie-Tochter Ant Financial Group bietet zusätzlich Online-Banking und andere Finanzdienstleistungen an, und betreibt lizenzierte virtuelle Banken außerhalb des chinesischen Festlandes in Hongkong und Singapur.

Es ist ein eindeutiger Trend zu erkennen: Diese Marktführer, die jahrzehntelang von einer begünstigenden Politik profitieren und als erstes in einem Dienstleistungsbereich als Gewinner ausgewählt und gefördert wurden, entwickeln sich zu Konglomeraten, die sich dann in andere Online-Sektoren horizontal diversifizieren, wobei sie häufig mit traditionellen Marktteilnehmern, wie den staatlichen Banken, konkurrieren und sich durchsetzen. Diese Big-Tech-Firmen expandieren dann auf internationaler Ebene, einerseits durch Übernahmen, insbesondere in Südostasien, Japan, Indien und Europa, und andererseits indem sie ihre eigenen Dienste für User in Übersee anbieten – wie AliPay, WeChat und Weibo für die chinesische Diaspora oder TikTok für junge User in aller Welt–. Die Machthaber in Peking müssen das Gefühl haben, dass sie die Kontrolle über Tycoons wie Jack Ma von Alibaba oder Pony Ma von Tencent und ihre Unternehmen verlieren.

80 Mark Ward. „China clampdown on tech in Urumqi." BBC. 06. Juli 2009. http://news.bbc.co.uk/2/hi/technology/8136944.stm

81 "王兴确认饭否域名逐步解封 暂无互动功能." https://tech.sina.com.cn/i/2010-11-11/23354855959.shtml

82 „Average number of daily active users of Weibo Corporation from 1st quarter 2018 to 1st quarter 2022." https://www.statista.com/statistics/1058070/china-sina-weibo-dau/

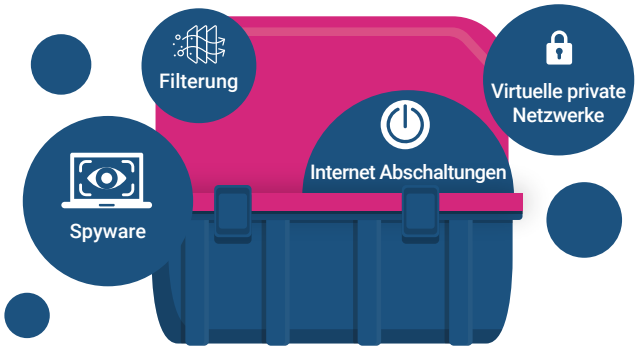
83 Manor Iqbal. „WeChat Revenue and Usage Statistics (2022)." https://www.businessofapps.com/data/wechat-statistics/

84 Lulu Yilun Chen und Yuji Nakamura. „Inside Tencent's Struggle to Bring World's Hottest Game to China." Bloomberg. 23. August 2018. https://www.bloomberg.com/news/articles/2018-08-23/fortnite-tencent-and-the-fate-of-world-s-biggest-game-market#xj4y7vzkg

85 „China's Tencent builds stake in UK digital bank Monzo." Reuters. 31. Dezember 2021. https://www.reuters.com/markets/europe/chinas-tencent-builds-stake-uk-digital-bank-monzo-2021-12-31/

4.3. Big Tech weltweit

Die Journalistin und Internet-Lobbyistin Rebecca McKinnon bezeichnet die globalen Internet-Unternehmen als „die Hüter und Diener, die Helfer und Vollstrecker der inneren Schicht der chinesischen Internetzensur“.[86] Zweifellos wurde einer Reihe ausländischer Unternehmen aus den USA, aus Großbritannien und auch aus Israel von China „angerechnet“, dass sie die Errichtung des Projekts „Golden Shield“ und den Bau der Great Firewall unterstützt haben.[87] In diesem Abschnitt wollen wir uns ansehen, welche Rolle ausländische Unternehmen in den Anfangszeiten der GFW spielten, wie die meisten von ihnen letztlich China verließen und was für diejenigen übrig bleibt, die noch dabei sind.



4.3.1. Cisco Systems

Im Laufe der Jahre wurde Cisco Systems für seine Mitwirkung am Aufbau von Chinas GFW am stärksten kritisiert. Zusammen mit den US-amerikanischen Juniper Networks, damals die beiden führenden Anbieter von Internet-Routern, unterstützte das Unternehmen 2004 Chinas Backbone-Betreiber bei der Aufrüstung ihrer Netze.[88] Cisco soll mehrere Tausend Router an China verkauft haben, und seine technischen Fachkräfte halfen dabei, sie so einzurichten, dass sie „subversive“ Schlüsselwörter in Nachrichten identifizieren.[89] Ein internes Cisco-Dokument aus dem Jahr 2002, das 2008 an die Medien gelangt war, enthüllte zudem, dass das Unternehmen das „rigide Internetzensurprogramm“ der chinesischen Regierung als eine Gelegenheit ansah, „mehr Geld zu verdienen“.[90]

Etwa zur gleichen Zeit befanden sich Cisco und das chinesische Startup-Unternehmen für Netz-Hardware, Huawei Technologies, bereits in einem Rechtsstreit über Urheberrechte, in dem Cisco Huawei beschuldigte, seine Router-Softwarecodes gestohlen zu haben.[91] Zu diesem Zeitpunkt war Huawei offenbar noch nicht in der Lage, die Filteranforderungen der chinesischen Zensoren allein zu erfüllen, und Cisco wurde zu Hilfe genommen. Die US-Firma mag das Gefühl gehabt haben, dass dies der Moment war, den staatlichen Anwendenden in dem Land mit der größten potenziellen Internetbevölkerung der Welt seine technischen Stärken und Alleinstellungsmerkmale zu demonstrieren, ohne sich darüber im Klaren gewesen zu sein, wie entbehrlich es in den Augen der Chinesen war.

Andererseits hätte sich die Entwicklung der GFW höchstwahrscheinlich verzögert oder ihre anfänglichen Funktionen wären reduziert gewesen, wenn Cisco diese Geschäftsmöglichkeit in China nicht ergriffen hätte. Hätte sich die Entwicklung der GFW um ein paar Jahre verzögert, hätte dieses Zeitfenster dann mehr Zeit für die freie Meinungsäußerung unter den chinesischen Usern geboten oder dafür gesorgt, dass andere ausländische Firmen wie Google und Yahoo! zumindest für ein paar Jahre weniger unter dem Druck der staatlichen Zensoren gestanden hätten? Was für einen Unterschied, wenn überhaupt, hätte das anschließend für die Internetfreiheit in China gemacht? Wir werden es niemals erfahren.

4.3.2. Google

Es liegt schon lange zurück, und das Szenario mag unglaublich erscheinen, aber die Suchmaschine von Google war tatsächlich einmal ein bedeutender Wettbewerber mit einem beträchtlichen Marktanteil in China.

Kurze Zeit nach der Gründung von Google im Jahr 1999 war bereits eine chinesische Version des Suchdienstes verfügbar, auch wenn dieser in China mitunter nicht nutzbar war und der Dienst aufgrund von Beeinträchtigungen durch die GFW langsam und unzuverlässig war. Das Unternehmen errichtete seine chinesische Tochtergesellschaft im Januar 2006 und startete einen lokalisierten Dienst, Google.cn, für den Google mit den chinesischen Behörden vereinbarte, bestimmte Websites zu sperren – im Gegenzug für die Genehmigung, seinen Dienst bereitzustellen. Im gleichen Jahr unterzeichnete Google die öffentliche Selbstverpflichtung der Internet Society of China in Bezug auf die Selbstdisziplin für die chinesische Internetindustrie (neben Microsoft und Yahoo! war es der letzte der drei großen US- Internetanbieter, der dies tat).[92] Allerdings versprach Google seinen Usern, dass sie informiert würden, wenn Suchergebnisse gefiltert oder zensiert werden, und dass Dienste wie Gmail und Blogger, die Userinhalte bzw. -daten involvieren, nicht auf dem chinesischen Festland angeboten würden.[93]

Da das Unternehmen der chinesischen Zensur auf diese Weise entsprach, wurde es in den USA vielfach dafür kritisiert, dass es seinem vermeintlichen Firmenmotto „Don't be evil“ nicht treu blieb. In der Zwischenzeit erhielt Google

86 Rebecca McKinnon. „Consent of the Networked: the world-wide struggle for Internet freedom.“ 2012. S. 36
87 “金盾工程.” https://web.archive.org/web/20150416093636/http://www.gdhongan.com:80/industroy.asp?ChannelID=7#
88 Robert McMahon and Isabella Bennett. „U.S. Internet Providers and the ‘Great Firewall of China’.“ Council for Foreign Relations. 23. Februar 2011. https://www.cfr.org/backgrounder/us-internet-providers-and-great-firewall-china
89 Jonathan Mirsky. „China's tyranny has the best hi-tech help.“ International Herald Tribune. 15. Januar 2006. https://www2.kenyon.edu/Depts/Religion/Fac/Adler/Reln270/Internet%20censorship.htm
90 „Cisco Leak: ‘Great Firewall’ of China Was a Chance to Sell More Routers.“ Wired. 20. Mai 2008. https://www.wired.com/2008/05/leaked-cisco-do/
91 Scott Thurm. „Huawei Admits Copying Code From Cisco in Router Software.“ The Wall Street Journal. 24. März 2003. https://www.wsj.com/articles/SB10485560675556000
92 „Public Pledge on Self-Discipline for the Chinese Internet Industry.“ https://en.wikipedia.org/wiki/Public_Pledge_on_Self-Discipline_for_the_Chinese_Internet_Industry
93 More Dickie. „Google to launch censored China service.“ Financial Times. 24. Januar 2006. https://www.ft.com/content/0cf3fc52-8d0b-11da-9daf-0000779e2340

China im September 2007 endlich eine Lizenz für seinen Dienst Google.cn, der vor mehr als eineinhalb Jahren eingerichtet worden war. Allerdings wurde Google in den nachfolgenden Jahren auch von China scharf kritisiert, weil dort Suchergebnisse mit pornografischen Inhalten verlinkt waren. Letztlich wurde Google im Juni 2009 von den Behörden aufgefordert, die Möglichkeit, nach ausländischen Webseiten zu suchen, sowie seine Suchfunktion für assoziierte Wörter einzustellen. Als Google sich der Aufforderung widersetzte, wurde die globale Google-Webseite, Google.com, als auch Gmail zum ersten Mal in China für mehrere Stunden vollständig gesperrt.[94] So unvorstellbar es nun sein mag, aber bis dahin waren diese Google-Seiten tatsächlich weitgehend in China verfügbar.

Unter dem Druck der USA und Chinas veröffentlichte David Drummond, Senior Vice President of Corporate Development und Chief Legal Officer von Google, am 12. Januar 2010 einen Blogbeitrag mit dem Titel „A new approach to China". In diesem Beitrag behauptete er, dass ein „sehr ausgeklügelter und gezielter Angriff" stattgefunden habe, der zum Diebstahl von geistigem Eigentum von Google geführt habe. Außerdem erklärte er, dass auch andere internationale Großunternehmen in verschiedenen Sektoren wie Technologie, Finanzen, Medien und Chemie sowie die Konten von Menschenrechtsaktivisten angegriffen wurden. Das Unternehmen hatte stets erklärt, dass es „die Bedingungen in China sorgfältig beobachten" werde, um zu entscheiden, wie es in Zukunft in dem Land weiter vorgehen wolle. Google gab nun bekannt, dass es die Zensur seiner Suchergebnisse auf Google.cn nicht mehr fortsetzen werde, auch wenn dies möglicherweise das Ende von Google.cn und damit auch der Präsenz von Google in China bedeuten könnte.[95]

Im März 2010 beendete Google schließlich die Zensur seiner Suchergebnisse und leitete alle Suchanfragen für seine chinesische Website auf seine chinesischsprachige Website in Hongkong um, die außerhalb der GFW lag.[96] Letztendlich wurde die Umleitung nach Hongkong jedoch nicht vollends realisiert, und es wurde lediglich eine statische Landing Page für chinesische User mit der Option eingerichtet, über einen Link auf die unzensierte Hongkong-Seite auszuweichen. Das war natürlich mehr symbolisch als alles andere, da die chinesischen Zensoren auch die Website Google.com.hk sperren konnten, und das taten sie auch.

Es gab einen anfänglichen Aufschrei einiger User, die über das Ende von Google in China enttäuscht waren, und etliche Bürgerinnen und Bürger Pekings legten in Scharen Blumen vor dem Google-Büro im Stadtteil Zhongguancun nieder. Die Blumen wurden umgehend vom Sicherheitspersonal wieder entfernt. Da für das Niederlegen von Blumen eine Genehmigung eingeholt werden musste, galt dieser Ort als „illegaler Blumentribut".[97] Selbst Diskussionen über solche illegalen Aktivitäten wurden von anderen Suchmaschinen und Portalen in China zensiert, unter anderem auch von Baidu, dem Hauptkonkurrenten von Google und Hauptnutznießer von Googles Ausstieg.

Aber hat Google daraus gelernt? Unter der Leitung von CEO Sundar Pichai seit 2015 erwog das Unternehmen sogar die Rückkehr auf den chinesischen Markt im Jahr 2018 mit einem internen Projekt namens Dragonfly, das für die Betriebssysteme Android und iOS entwickelt wurde, um mit den chinesischen Zensuranforderungen „kompatibel" zu sein. Ein geleaktes Dokument enthüllte, dass der Suchmaschinen-Prototyp die Bewegungen chinesischer User zusammen mit ihren persönlichen Daten, IP-Adressen und ihrem Suchverlauf nachverfolgen würde und dass alle Informationen an einen chinesischen Partner weitergegeben würden, der „uneingeschränkten Zugriff" auf die Daten haben würde.[98]

Infolgedessen veröffentlichte eine Gruppe von Google-Mitarbeitenden einen offenen Brief, in dem das Unternehmen aufgefordert wurde, Dragonfly zu beenden.[99] Das Unternehmen geriet unter den Druck seiner Mitarbeitenden sowie unter den Widerstand der Regierung von Präsident Donald Trump und des US-Kongresses und änderte seine Position zu dem Projekt mehrfach. Im Dezember 2018 hieß es, das Projekt sei „effektiv beendet",[100] doch gab es immer wieder Gerüchte, dass es nicht vollständig eingestellt wurde. Im Juli 2019 erklärte dann Karan Bhatia, Googles Vice President of Government Affairs and Public Policy, vor dem Justizausschuss des US-Senats, dass Dragonfly eingestellt worden sei.[101]

Warum wollte Google den gleichen Fehler zweimal machen? Selbst wenn die Firma nur auf Gewinne aus war und dachte, dass sie den chinesischen Markt erschließen müsse, war es für die Geschäftsleitung des Unternehmens ausgesprochen naiv zu erwarten, dass ein amerikanisches Unternehmen mit den unersättlichen Auflagen der chinesischen Zensoren fertig werden könnte. Denn diese können selbst die einheimischen chinesischen Big-Tech-Firmen kaum bewältigen, sogar wenn sie Sitze im Vorstand an Mitgliederinnen und Mitglieder der Regierung vergeben. Auch war es von den Verantwortlichen des Unternehmens naiv zu glauben, dass sie mit dem innenpolitischen Druck aus Washington bezüglich des „Kuschelns" mit China fertig werden würden. Dieselben Fehler wurden von amerikanischen Internetfirmen vor weniger als zehn Jahren gemacht, und die Lehren daraus sind bereits wieder vergessen worden.

94 Kathrin Hille und Richard Waters. „China blocks Google websites." Financial Times. 24. Juni 2009. https://www.ft.com/content/8e4ccdce-60cf-11de-aa12-00144feabdc0

95 David Drummond. „A new approach to China." Financial Times. 12. Januar 2010. https://googleblog.blogspot.com/2010/01/new-approach-to-china.html

96 Richard Waters. „Google ends censorship in China." Financial Times. 22. März 2010. https://www.ft.com/content/0081dbd4-35e9-11df-aa43-00144feabdc0

97 Evan Osnos. „China and Google: 'Illegal Flower Tribute'." The New Yorker. 14. Januar 2010. https://www.newyorker.com/news/evan-osnos/china-and-google-illegal-flower-tribute

98 Ryan Gallagher und Lee Fang. „Google Suppresses Memo Revealing Plans to Closely Track User Searches in China." The Intercept. 21. September 2018. https://theintercept.com/2018/09/21/google-suppresses-memo-revealing-plans-to-closely-track-search-users-in-china/

99 Google-Mitarbeiter gegen Dragonfly. „We are Google employees, Google Must Drop Dragonfly." 27. November 2018. https://medium.com/@googlersagainstdragonfly/we-are-google-employees-google-must-drop-dragonfly-4c8a30c5e5eb

100 Jen Copestake. „Google China: Has search firm put Project Dragonfly on hold?" BBC. 18. Dezember 2018. https://www.bbc.com/news/technology-46604085

101 „Google's Project Dragonfly 'terminated' in China." BBC. 17. Juli 2019. https://www.bbc.com/news/technology-49015516

Andererseits ist Eric Schmidt, der von 2001 bis 2011 CEO bei Google war, heute ein großer Kritiker des technologischen Wettbewerbs zwischen China und den USA. Unter seiner Leitung versuchte Google erfolglos, ein Geschäftsmodell in China zu etablieren. Als der Google-Suchdienst in China eingestellt wurde, betonte er weiterhin, dass sich das Unternehmen „nicht aus China zurückzieht" und dass es „viele andere Geschäftsmöglichkeiten in China" habe. Inzwischen warnt er vor einer „nationalen Bedrohungslage" im Hinblick auf den Wettbewerb zwischen den USA und China um künstliche Intelligenz, Forschung und Talententwicklung.[102]

4.3.3. Yahoo!

Yahoo! trat bereits 1999 in den chinesischen Markt ein und eröffnete eine Niederlassung in Peking. Trotz der Proteste von Menschenrechtsgruppen war es 2002 das erste der großen US-Internetunternehmen, das die öffentliche Verpflichtung der Internet Society of China zur Selbstdisziplin für die chinesische Internetindustrie unterzeichnete.[103] Der Suchmaschinendienst von Yahoo! in China wurde aktiv zensiert. Noch problematischer für den Ruf und das Engagement des Unternehmens in China war aber das Bereitstellen von E-Mail-Diensten unter Yahoo.com.cn. Mindestens vier chinesische Bürgerinnen und Bürger wurden aufgrund von E-Mails, die sie über Yahoo! verschickt hatten, in China festgenommen und zu erheblichen Haftstrafen verurteilt.

Der prominenteste dieser Fälle betraf den chinesischen Journalisten Shi Tao. Er erhielt im April 2004 ein Schreiben der KPCh, in dem Reporterinnen und Reporter angewiesen wurden, nicht über den bevorstehenden fünfzehnten Jahrestag des „Tiananmen-Massakers" zu berichten. Er leitete dieses Dokument über eine E-Mail-Adresse von Yahoo! China an eine chinesischsprachige Website in New York weiter.[104] Auf Anfrage der chinesischen Polizei stellte Yahoo! nicht spezifizierte Informationen über Shis E-Mail-Konto und seine E-Mails zur Verfügung, und der Journalist wurde daraufhin festgenommen, angeklagt und wegen der Veröffentlichung von Staatsgeheimnissen verurteilt. Im Juni 2005 wurde er zu einer Haftstrafe von zehn Jahren verurteilt.

Shi war nicht der Einzige. Andere chinesische User von Yahoo.com.cn, die für E-Mails verurteilt wurden, die sie über die Plattform verschickt hatten, waren unter anderem Li Zhi, ein Schriftsteller, der im Dezember 2003 wegen „Anstiftung zum Staatsverrat"[105] zu acht Jahren Gefängnis verurteilt wurde; Jiang Lijun, ein Schriftsteller, der im November 2003 wegen „Staatsverrats"[106] zu vier Jahren Gefängnis verurteilt wurde; und Wang Xiaoning, ein Schriftsteller, der im September 2003 wegen „Anstiftung zum Staatsverrat" zu zehn Jahren Gefängnis verurteilt wurde.[107]

4.3.4. Apple

Apple ist gewiss die US-Big-Tech-Firma, die am stärksten vom chinesischen Markt abhängig ist. Im vierten Quartal 2021 erzielte das iPhone einen Rekordmarktanteil von 23 Prozent in China und eroberte damit zum ersten Mal seit sechs Jahren den Spitzenplatz zurück,[108] wobei es Huawei ablöste. Noch wichtiger ist jedoch, dass sich Apple auf die chinesische Auftragsfertigung verlässt. Analystinnen und Analysten schätzen, dass neunzig Prozent der Apple-Produkte in China hergestellt werden – trotz der jüngsten Bemühungen des Unternehmens, seine Lieferkette zu diversifizieren.[109]

Die chinesischen Behörden verstehen die Bedeutung einer solchen Abhängigkeit eines Unternehmens, das die weltweit beliebtesten Smartphones und Betriebssysteme herstellt. Außerdem ist ihnen klar, wie wichtig die Daten sind, die auf diesen Geräten gespeichert und gesammelt werden. Gemäß den Datenschutzbestimmungen des Landes müssen chinesische iPhone-User, die über die iCloud auf die verschiedenen Apple-Dienste zugreifen, die Daten innerhalb der chinesischen Grenzen speichern. Deshalb investierte Apple eine Milliarde USD in den Bau eines Rechenzentrums in der Provinz Guizhou im Südwesten Chinas, um es von seinem lokalen staatlichen Partner, der Guizhou-Cloud Big Data Industry Co. Ltd. (GCBD), ab Mai 2021 betreiben zu lassen. Obwohl Apple behauptete, dass dieser Schritt „die Erfahrungen der chinesischen User in Sachen Zugriffsgeschwindigkeit und Servicezuverlässigkeit sowie die allgemeine Zuverlässigkeit der Apple-Produkte und -Dienste auf dem chinesischen Festland weiter verbessern würde"[110] , sieht die Realität so aus, dass die GCBD als Vermittler für die ebenfalls staatliche China Telecom fungiert, indem es Userdaten an den bestehenden Internet-Backbone-Betreibenden und damit an einen der wichtigsten Betreibenden des Landes von routinemäßiger Zensur weiterleitet.[111]

102 Ina Fried, Margaret Harding McGill und Ashley Gold. „Eric Schmidt's China alarm." Axios. 01. April 2022. https://www.axios.com/2022/04/01/eric-schmidt-china-alarm-tech-competition

103 Yahoo! Risks Abusing Rights in China." https://www.hrw.org/legacy/press/2002/08/yahoo080902.htm

104 Joseph Kahn. „Yahoo helped Chinese to prosecute journalist." The New York Times. 08. September 2005. https://www.nytimes.com/2005/09/08/business/worldbusiness/yahoo-helped-chinese-to-prosecute-journalist.html

105 Roland Soong. „The case of Li Zhi." http://www.zonaeuropa.com/20060209_2.htm

106 „Yahoo accused of helping jail another Chinese writer." Reuters. 19. Mai 2006. https://www.cnet.com/tech/tech-industry/yahoo-accused-of-helping-jail-another-chinese-writer/

107 „China dissident Wang jailed on Yahoo information freed." BBC. 31. August 2012. https://www.bbc.com/news/world-asia-china-19432800

108 Arjun Kharpal. „Apple reclaims No. 1 spot in China, hits record iPhone market share in the fourth quarter." 27. Januar 2022. CNBC. https://www.cnbc.com/2022/01/27/apple-china-iphone-maker-hits-record-market-share-claims-nopoint1-spot.html

109 Yang Jie. „Apple Looks to Boost Production Outside China." The Wall Street Journal. 21. Mai 2022. https://www.wsj.com/articles/apple-looks-to-boost-production-outside-china-11653142077

110 Antony Savvas. „Apple opens its $1b data center in China." 28. Mai 2021. https://www.capacitymedia.com/article/29otd6mddjpstgh31u1hc/news/apple-opens-its-1bn-data-centre-in-china

111 Nick Statt. „Apple's iCloud partner in China will store user data on servers of state-run telecom." https://www.theverge.com/2018/7/18/17587304/apple-icloud-china-user-data-state-run-telecom-privacy-security

Ein Untersuchungsbericht der New York Times führte verschiedene Kernpunkte zum Thema auf, „wie Apple die Daten seiner chinesischen Kundinnen und Kunden gefährdete und die Zensur der chinesischen Regierung unterstützte“, und fasste diese wie folgt zusammen:[112]

- Apple speichert Kundendaten auf Servern der chinesischen Regierung. Das Rechenzentrum wird von chinesischen Staatsbeamten physisch kontrolliert und betrieben. Apple willigte ein, die digitalen Schlüssel, mit denen die Daten entschlüsselt werden können, in China zu speichern, und konnte auch die Verschlüsselungstechnologie, die es in anderen Rechenzentren verwendet, nicht nutzen, da die chinesische Regierung dies nicht zuließ.

- Apple gibt nun Kundendaten an die chinesische Regierung weiter. Nach US-Recht darf Apple keine Daten an ausländische Behörden weitergeben. Aber Apple kam zu einer rechtlichen Vereinbarung mit seinem chinesischen staatlich kontrollierten Partner, um die US-Beschränkungen zu umgehen. Dadurch, dass die GCBD der rechtmäßige Eigentümer der iCloud-Daten von Kunden in China ist, müssen sich die chinesischen Behörden nur an GCBD wenden, um die Daten zu erhalten. Apple ist aus dem Schneider.

- Apple entfernt proaktiv Apps innerhalb des chinesischen Festlandes, um die chinesischen Funktionäre zu beschwichtigen. Einem Bericht der Times zufolge „schult Apple seine App-Prüfenden und verwendet eine spezielle Software, um Apps daraufhin zu untersuchen, ob darin Themen erwähnt werden, die Apple in China als nicht zulässig einstuft“, anstatt lediglich auf Beschwerden zu reagieren, was einer proaktiven Zensur gleichkommt. Die Times schätzt, dass seit 2017 satte 55.000 aktive Apps aus dem Apple App Store in China gestrichen wurden, obwohl die meisten von ihnen in anderen Ländern weiterhin verfügbar sind. Mehr als 35.000 davon waren Spiele, die in China lizenziert werden müssen. Zu den übrigen 20.000 gehören ausländische Nachrichtenmedien, Dating-Dienste für Homosexuelle, verschlüsselte Messaging-Apps, Tools, die zur Organisation von Protesten gegen die Demokratie genutzt werden können, und auch VPNs. Im Juli 2017 soll Apple sechzig VPNs aus dem chinesischen App Store genommen haben.[113]

- Apple streicht auch proaktiv Apps außerhalb des chinesischen Festlandes, um die chinesischen Funktionäre zu beschwichtigen. Das bedeutet, dass Apple auch außerhalb der chinesischen Gerichtsbarkeit selbst zensiert. Ein Beispiel ist HKmap.live, eine App aus Hongkong, die 2019 während der Proteste gegen das Auslieferungsgesetz in Erscheinung trat. Die App stellte größere Ansammlungen von Polizeikräften dar und half so nach Angaben der Entwickler den Demonstrierenden und Umstehenden, die Polizei zu meiden. Aufgrund eines Aufschreis im Internet gegen Apple teilte der CEO Tim Cook den Mitarbeiterinnen und Mitarbeitern des Unternehmens in einem Schreiben mit, dass die App „böswillig dazu verwendet wurde, einzelne Polizeibeamte mit Gewalt anzugreifen und einzelne Personen und Eigentum zu schädigen, wo keine Polizei präsent war“. Doch der Entwickler der App erwiderte, dass Apple “die Behauptungen der Polizei in Hongkong für bare Münze nahm“ und dass das Streichen der App eine “klare politische Entscheidung war, um die Freiheit und Menschenrechte der Bevölkerung in Hongkong zu unterdrücken.“[114] Zusätzlich ignorierte Apple anscheinend einfach den Entwickler und antwortete weder ihm noch irgendjemand anderem, auch nicht dem Verfasser dieser Veröffentlichung, der damals Parlamentsabgeordneter in Hongkong war.[115]

Die Selbstzensur von Apple ist wohl die stärkste und tiefgreifendste in den USA. In einem Update für sein Betriebssystem iOS 13.1 im Oktober 2019 entfernte Apple das Emoji mit der taiwanischen Flagge von seiner virtuellen Tastatur für User aus Hongkong und Macao.[116] Die Citizen Lab-Forscherinnen und Forscher fanden im August 2021 heraus, dass lange Listen von Apples Gravurdienst für seine AirPod-, AirTag- und iPod-Produkte existieren, die in China 1.045 Schlüsselwörter, in Hongkong 542 und in Taiwan sogar 397 blockieren. Viele dieser Begriffe beziehen sich auf Chinas politisches System, Namen von Dissidentinnen und Dissidenten und Nachrichtenorganisationen sowie Begriffe, die mit Demokratie oder Menschenrechten zu tun haben. Zum Vergleich untersuchten die Forscherinnen und Forscher Schlüsselwörter in Japan, Kanada und in den USA: Die Zahlen sind mit 170-206 Schlüsselwörtern wesentlich geringer und beziehen sich meist auf rassistische und sexistische Äußerungen. Apple rechtfertigt sein Vorgehen damit, dass es um „kulturelle Sensibilität“ gehe. Und noch im August 2022 forderte Apple seine Hersteller und Lieferanten von in Taiwan hergestellten Teilen und Komponenten auf, diese nur noch mit „Taiwan, China“ oder „Chinese Taipei“ zu kennzeichnen.[117]

112 Jack Nicas. „Apple’s Compromises in China: 5 Takeaways.“ The New York Times. 17. Mai 2021. https://www.nytimes.com/2021/05/17/technology/apple-china-privacy-censorship.html

113 „Apple ‘pulls 60 VPNs from China’s App Store’.“ BBC. 31. Juli 2017. https://www.bbc.co.uk/news/technology-40772375

114 Alex Hern. „Tim Cook defends Apple’s removal of Hong Kong mapping app.“ The Guardian. 10. Oktober 2019. https://www.theguardian.com/technology/2019/oct/10/tim-cook-apple-hong-kong-mapping-app-removal

115 https://twitter.com/charlesmok/status/1182336160611201024

116 Matthew De Silva. „Apple bows to China by censoring Taiwan flag emoji.“ Quartz. 07. Oktober 2019. https://qz.com/1723334/apple-removes-taiwan-flag-emoji-in-hong-kong-macau-in-ios-13-1-1/

117 Cheng Ting-Fang und Lauly Li. „Apple warns suppliers to follow China rules on ‘Taiwan’ labeling.“ Nikkei Asia. 05. August 2022. https://asia.nikkei.com/Spotlight/Supply-Chain/Apple-warns-suppliers-to-follow-China-rules-on-Taiwan-labeling

4.3.5. Es wird nur verschärft, nie gelockert

Im Laufe der Jahre hat China immer ausgefeiltere Methoden entwickelt, um globale Technologieunternehmen zu ihren Komplizen in Sachen Zensur zu machen. Der chinesische Markt ist dank seines riesigen Marktpotenzials und der Produktionsmöglichkeiten für Unternehmen sehr attraktiv. Die Formel der Selbstrechtfertigung für die Präsenz in China ist schlicht und einfach: „Wir halten uns an die Gesetze vor Ort" und „Chinas Internetlandschaft ist freier, weil wir dort sind" – zumindest so lange, bis auch diese Unternehmen gezwungen sind, das Land zu verlassen. Die Realität sieht so aus, dass seit Mitte der 2010er Jahre die meisten der großen globalen Suchmaschinen, Social-Media-, Messaging- und anderen Online-Service-Plattformen entweder aus China vertrieben wurden, nachdem sie der Konkurrenz chinesischer Alternativen unterlagen, oder – vielleicht zum Glück – nie die Chance hatten, sich dort zu etablieren, wie es bei Facebook der Fall war. Andere, wie Apple, sind übermäßig von dem Land abhängig geworden, vor allem wegen der Umsätze im Bereich Hardware und der Produktionslieferkette.

Zusätzlich zu den gesetzlichen Bestimmungen, die sicherstellen sollen, dass ausländische Firmen die chinesische Zensur umsetzen, verlangt das Land von ausländischen Firmen für die meisten Dienstleistungen zudem, dass sie mit einem einheimischen chinesischen Partner ein Joint Venture eingehen. Sonst erhält das ausländische Unternehmen nicht die notwendige Lizenz. Diese chinesischen Partner, die sich in der Regel in Staatsbesitz befinden und für die ausländische Firma maßgeschneidert werden, erhalten nicht nur Zugriff auf Technologien, Betriebsabläufe, Finanzinformationen und Daten der Dienstleistungen dieser ausländischen Firmen, sondern auch einen Gewinnanteil.

Trotz der immer härteren Marktbedingungen in China, des Diebstahls von geistigem Eigentum und der strengen Vorschriften gelingt es dem Land nach wie vor, Firmen aus dem Westen auf der Suche nach einem Wachstumsmarkt davon zu überzeugen, dass der chinesische Markt unumgänglich ist. Die Firmen müssen sich bewusst werden, dass die höheren Risiken, die sich aus einem viel drakonischeren und risikoreicheren chinesischen Geschäftsumfeld ergeben, sowie die globalen Spannungen mit China die Geschäftstätigkeit in dem Land zunehmend schwieriger machen.[118]

Roblox ist eine große Online-Game-Plattform. Gemäß internen Dokumenten aus dem Jahr 2022 muss das Unternehmen eine Partnerschaft mit einem chinesischen Unternehmen unterhalten, um in China operieren zu dürfen. Im Fall von Roblox ist dies ein Konkurrent, und zwar die Firma Tencent. Darüber hinaus ist das Unternehmen dazu verpflichtet, seine Userdaten auf lokalen Servern in China zu hosten. Roblox ging sogar davon aus, von seinem Partner gehackt zu werden, dass seine Spiele nachgebaut und jeglicher Code, der sich auf chinesischen Servern befindet, kopiert werden würde.[119] All diese Risiken hätte das Unternehmen in seinem eigenen Land sicherlich nicht in Kauf genommen. Dennoch wagte es den Schritt nach China. In dem internen Dokument von Roblox wurden sogar die geplanten Maßnahmen beschrieben, die das Unternehmen ergreifen würde, um der chinesischen Zensur zu entsprechen: Sie würden die Ansprüche Chinas an Taiwan formell anerkennen, Namen oder Bilder von nationalen Führungspersonen vermeiden und keine Kräfte oder Organisationen zeigen, die in Chinas Hoheitsgebiet eindringen.

Die immer gleichen Fehler werden von vielen Unternehmen wiederholt, auch wenn sich diese Zugeständnisse auf lange Sicht nur selten auszahlen.

118 Charles Mok und Dennis Kwok. „China's Neo-Nationalism Poses Risks for International Businesses." 02. November 2021. https://thediplomat.com/2021/11/chinas-neo-nationalism-poses-risks-for-international-businesses/

© TippaPatt / Shutterstock.com

5. Instrumentalisierung von Daten in China

Die KPCh sieht das Internet und seinen Informationsfluss nicht nur als Bedrohung, sondern auch als Chance an. Seit dem Aufkommen von „Big Data" – extrem große Datensätze, die computergestützt analysiert werden können, um Muster, Trends und Zusammenhänge zu erkennen[120] – hat Chinas Regierung eine führende Rolle eingenommen, wenn es darum geht, die Macht der Daten zu nutzen, von der Datenerfassung über die Analyse bis hin zum Einleiten von Maßnahmen basierend auf deren Ergebnissen. Aus Chinas „vorteilhafter" Perspektive als großer Zensor von Informationen und Daten auf täglicher Basis erkannten Chinas Machthaber schon früh die Bedeutung der gewaltigen Datenmengen, die von den einheimischen Big-Tech-Firmen erfasst werden: Vom Konglomerat der großen Drei – Baidu, Alibaba und Tencent – über andere Branchenführer wie Weibo, JD.com, Didi, Douyin (Besitzer von TikTok), über infrastrukturelle Akteure wie den staatlichen Telekommunikations- und Internet-Backbone-Betreibern (China Telecom, China Unicom und China Mobile) bis hin zu Rechenzentrumsplattformen wie GDS und 21ViaNet.[121]

Sektorübergreifende Dienstleistungen, insbesondere in den Bereichen E-Commerce und Online-Zahlungen, setzten sich in China viel schneller durch als anderorts. Zu verdanken ist dies auch Tencents Super-App-Plattform WeChat. Chinesische Firmen begannen, die Möglichkeiten von Big-Data-Analysen zu nutzen, um Kundinnen und Kunden gezielter und besser anzugehen als irgendwo sonst auf der Welt. Sie verfügten aufgrund der verhältnismäßig geringen Standards beim Datenschutz über mehr Daten für ihre Studien in den Bereichen der künstlichen Intelligenz (KI) und des maschinellen Lernens als Unternehmen im Westen. Die chinesischen Behörden bemerkten dies und begannen damit, schärfere Kontrollen zu entwickeln.

120 Von Oxford Languages. https://languages.oup.com/google-dictionary-en/
121 Herbert Poenisch. „Big Data Management in China." Oxford Business Review. 11. Mai 2021. https://oxfordbusinessreview.org/big-data-management-in-china/

5.1. Smart City or Surveillance City?

Im Laufe der 2010er Jahre wurden in China Investitionen in die Entwicklung von „Smart Cities“ getätigt, um die Stadtverwaltung zu digitalisieren und zu „informatisieren“. Dabei wurden die Bereiche Verkehr, öffentliche Dienstleistungen, öffentliche Sicherheit, Bildung, das Gesundheitswesen und der Umweltschutz als Schwerpunkte für bessere Dienstleistungen und den Schutz der Bevölkerung definiert. Es wurde schnell klar, dass chinesische Stadtbehörden Technologien – insbesondere das Internet of Things (IoT), 5G-Kommunikationen, mobiles Internet, Cloud Computing, Big Data und KI – verstärkt für Überwachungszwecke und -aktivitäten einsetzen. Dies stimmte auch mit dem traditionellen Gedanken der chinesischen KPCh überein: „Massenverteidigung, Massenherrschaft“ bis hin zum „Crowdsourcing“ von Freiwilligen und Bürgerinnen und Bürgern für die Überwachung der breiten Öffentlichkeit.[122]

Allerdings sah die lokale und globale Informationstechnologiebranche in der Diskussion um die „Smart City“ eine riesige Vermarktungsmöglichkeit. Alibaba übernahm die Führung mit der Entwicklung seines City Brain-Systems, das Überwachungstools, Netzinfrastruktur und KI kombiniert, um ein Echtzeitmanagement für Verkehr und öffentliche Verkehrsmittel zu realisieren. Ein erstes Projekt wurde in Kooperation mit der Stadt Hangzhou durchgeführt, bei dem Alibaba nach eigenen Angaben Verkehrsstaus um 15 Prozent reduzieren konnte.[123] City Brain soll bis Ende 2019 in mehr als zwanzig Städten auf dem chinesischen Festland sowie in Macau und Kuala Lumpur, Malaysia, eingeführt worden sein.[124] In ähnlicher Weise ist auch Huawei Partnerschaften mit einigen chinesischen Städten eingegangen, die seine 5G-Technologie nutzen, um modernste Kommunikationslösungen für Flughafen- und Transportkontrollen zu bieten.[125]

Auch hier wollten ausländische Akteure nicht außen vor bleiben. Cisco war besonders aggressiv, als man 2016 eine Vereinbarung mit der Stadt Guangzhou unterzeichnete, um ein Smart City-Projekt im Panyu District zu realisieren. Die Vereinbarung umfasste sieben Kooperationsfelder, einschließlich „Smart Manufacturing“, „Smart Cities“, „Wireless Network“, „Cloud Computing“, „Inkubation von Technologieunternehmen“, „Ausbildung von IT-Talenten“ und „Entwicklung von Innovationsführungskräften“, um „ein hochmodernes System von smarten Industrien zu schaffen und einen Industriepark von Weltniveau mit einem jährlichen Produktionsvolumen von über 100 Milliarden RMB zu errichten“.[126] Nachdem der große Plan für eine ganze Hightech-Region zum Bau von Geschäfts- und Wohngebäuden bereits Jahre alt war, hat Cisco angesichts der wirtschaftlichen Abkühlung in China und weltweit, insbesondere aufgrund der COVID-19-Pandemie, beschlossen, seine globalen Smart-City-Bemühungen zu reduzieren und „den Vertrieb und schließlich auch den Support für seine entsprechende Produktlinie einzustellen“.[127]

Die massive Überwachungsinfrastruktur, die zum Zweck von Verkehrsmanagement bzw. Verbrechensbekämpfung aufgebaut wurde, ist jedoch in vielen chinesischen Städten sehr lebendig und wird weiter ausgebaut. Das Projekt SkyNet zum Aufbau des größten Überwachungssystems der Welt, das Gesichtserkennungstechnologie mit Big Data und künstlicher Intelligenz kombiniert, um so zahlreiche Kameras an öffentlichen Orten wie Bahnhöfen, U-Bahnen und Busstationen sowie Restaurants, Einkaufszentren und Kinos zu verbinden, wurde von Anbietern wie HikVision, SenseTi, Huawei, ZTE, und vielen anderen unterstützt. Im Gegenzug wurden diese Firmen mit lukrativen staatlichen Aufträgen und Subventionen gefördert.[128]

Im Jahr 2017 erhielt der BBC-Reporter John Sudworth „ungewöhnlicherweise Zutritt“ zur Polizeibehörde von Guiyang in der Provinz Guizhou, um das Videoüberwachungssystem der Stadt zu testen. Um das System zu veranschaulichen, wurde er von der Polizei als Verdächtiger ausgewiesen, und er versuchte dann, zu Fuß zum Bahnhof zu gehen. Er wurde binnen sieben Minuten „geschnappt“. China Daily, das staatliche englischsprachige Sprachrohr des Landes, berichtete stolz über die Geschichte, mit einem abschließenden Zitat des Reporters, das den Anschein erweckte, als würde er das System befürworten: „Wenn man nichts Unrechtliches getan hat, hat man auch nichts zu befürchten.“[129] Wenn man sich jedoch den vollständigen Videobericht ansieht,[130] wird deutlich, dass es sich bei diesem „Zitat“ um eine Frage handelte, die der Reporter einem Polizeibeamten während eines Interviews gestellt hatte, und zwar wie folgt: „Wenn man nichts Unrechtliches getan hat, hat man auch nichts zu befürchten?“ Das nennt man dann wohl Falschnachrichten von einem staatlichen Medienunternehmen.

122 Katherine Atha, Jason Callahan, John Chen, Jessica Drun, Ed Francis, Kieran Green, Brian Lafferty, Joe McReynolds, James Mulvenon, Benjamin Rosen und Emily Walz. „China’s Smart City Development.“ Januar 2020. https://www.uscc.gov/sites/default/files/China_Smart_Cities_Development.pdf

123 Abigail Beall. „In China, Alibaba’s data-hungry AI is controlling (and watching) cities.“ Wired. 30. Mai 2018. https://www.wired.co.uk/article/alibaba-city-brain-artificial-intelligence-china-kuala-lumpur

124 „City Brain Now in 23 Cities in Asia.“ Alibaba Cloud. 28. Oktober 2019. https://www.alibabacloud.com/blog/city-brain-now-in-23-cities-in-asia_595479

125 Alexander Rosas. „What To Know About China’s Smart Cities and How They Use AI, 5G, and IoT.“ The China Guys. 26. August 2021. https://thechinaguys.com/china-smart-cities-development/

126 Hilton Romanski. „Cisco to bring in resources for innovation and digital transformation.“ 25. September 2017. https://www.newsgd.com/node_2ba302884e/2f-6cd5b7bd.shtml

127 Aaron Tilley. „Cisco Systems Pulls back From Smart City Push.“ The Wall Street Journal. 28. Dezember 2020. https://www.wsj.com/articles/cisco-turns-off-lights-on-smart-city-push-11609178895

128 “天网工程.”China Digital Times. https://chinadigitaltimes.net/space/%E5%A4%A9%E7%BD%91%E5%B7%A5%E7%A8%8B

129 „China’s Skynet Project finds people in minutes.“ China Daily. 12. Dezember 2012. http://www.chinadaily.com.cn/a/201712/12/WS5a2fa4f7a3108bc8c6727f5c.html

130 „In Your Face: China’s all-seeing state.“ BBC. 10. Dezember 2017. https://www.bbc.com/news/av/world-asia-china-42248056

5.2. Werden COVID-19-Apps zur Ermittlung von Kontaktpersonen wirklich nicht mehr eingesetzt?

Als die COVID-19-Pandemie Ende 2019 erstmals in China ausbrach, bot sich plötzlich die perfekte Gelegenheit, digitale Technologien, Sozialkreditsysteme und die Erfahrungen jahrzehntelanger Internetüberwachung und -zensur in die Tat einzusetzen. Dabei handelte es sich nicht nur um einen Beta-Test für einen realen Notfall, sondern auch um ein Experiment, um die Fügsamkeit und den Grad der Akzeptanz der Bevölkerung auf die Probe zu stellen: Inwieweit ist das chinesische Volk bereit, Einschränkungen und Einbußen seiner persönlichen Freiheit und Privatsphäre in Kauf zu nehmen, um seine Gesundheit und die öffentliche Sicherheit zu schützen?

Verschiedene Gesundheits-Apps spielten bei der digitalen Reaktion Chinas auf die Pandemie eine zentrale Rolle. Die Apps konnten nicht nur die Kontaktpersonen von Infektionskranken ermitteln, sondern wurden auch dafür eingesetzt, die Bewegungsfreiheit der Bevölkerung während der Pandemie einzuschränken. Durch die starke Verbreitung von Mobiltelefonen in China war der Staat in der Lage, die Nutzung dieser Gesundheits-Apps zur Pflicht zu machen. Was schlichtweg ignoriert wurde, war das Problem der digitalen Kluft sowie die Menschen, die kein Smartphone mit Datenverbindung besaßen oder die älter, körperlich eingeschränkt oder nicht in der Lage waren, digitale Technologie problemlos zu nutzen.

In China bildeten die Popularität und die extrem hohen Verbreitungsraten zweier Apps, nämlich WeChat von Tencent und AliPay von Ant Group, die Basis für die schnelle Einführung und Umsetzung von Apps zur Ermittlung von Kontaktpersonen, Gesundheitscodes und von anderen Gesundheits-Apps in China. So wurde die Registrierung unter echtem Namen mit nationalen Ausweisnummern bereits bei der Anmeldung für diese Apps vorgenommen. Die von lokalen Regierungsstellen, wie z. B. Provinz- oder Stadtverwaltungen, entwickelten Gesundheits-Apps hatten unter Umständen unterschiedliche Namen und Funktionen, und die Richtlinien für Restriktionen variierten teilweise. Im Allgemeinen enthielten jedoch alle Gesundheits-Apps drei Farbmodi: grün, gelb und rot, die jeweils angaben, ob die Person gesund, potenziell mit dem Virus infiziert war oder positiv auf COVID-19 getestet wurde. Für die Registrierung und Nutzung war oftmals auch die Gesichtserkennung erforderlich.[131]

Auch wenn in den einzelnen Provinzen und Städten unterschiedliche Vorschriften galten, war für den Zutritt zu den meisten öffentlichen Einrichtungen ein grüner Code auf der App erforderlich, ein gelber Code konnte eine Isolation von sieben Tagen bedeuten, und ein roter Code erforderte eine strengere Quarantäne, z. B. 14 Tage in einer staatlichen Einrichtung, wie es im Februar 2020 in Hangzhou in der Provinz Zhejiang der Fall war.[132]

Andere Gesundheits-Apps enthielten einen Code zur Erfassung von Reiseverläufen, anhand von Daten, die von den größeren staatlichen Mobilfunk- und Telekommunikationsunternehmen bereitgestellt wurden, sowie anhand von Informationen über Fahrten mit öffentlichen Verkehrsmitteln. Darüber hinaus wurden Daten von Anbietern elektronischer Zahlungsdienste miteinbezogen, um potenzielle Risiken im Zusammenhang mit vermuteten oder diagnostizierten Erkrankungen zu ermitteln. Und als die Impfungen verfügbar wurden, setzte der Staat auch weiter auf ein umfangreiches System mit regelmäßigen Tests und anschließender gründlicher Überwachung der Bürgerinnen und Bürger. Impfungen und PCR-Tests wurden in Gesundheits-Apps erfasst, die Daten von der staatlichen Gesundheitsbehörde erhielten. Diese Apps wurden dann häufig mit der ursprünglichen Gesundheits-App kombiniert, da manche Lokalitäten den Nachweis einer Impfung oder eines negativen Testergebnisses für den Zutritt verlangten.

Obwohl die Entwicklung dieser Apps dezentral und von verschiedenen regionalen Behörden durchgeführt wurde, wurden die Daten auf der Ebene der Nationalen Staatlichen Serviceplattform koordiniert und zentralisiert. Die Bevölkerung konnte ihren Gesundheitszustand auf mindestens vier Kanälen überprüfen bzw. abrufen: Auf einer offiziellen staatlichen Website, in einer App des Staatsrates, in einem Mini-Programm auf WeChat und in einem Mini-Programm auf AliPay. In Bezug auf Datenschutz betonte die CAC von Anfang an, dass die Apps und die damit erhobenen Daten nicht für andere Zwecke als die Pandemiebekämpfung eingesetzt werden würden.[133]

Allerdings gab es unter Wissenschaftlerinnen und Wissenschaftlern, Bürgerinnen und Bürgern und natürlich auch Dissidentinnen und Dissidenten weiterhin Zweifel: Mit zunehmender Nutzung dieser Gesundheits-Apps in China und immer ausgereifteren Tracking-Funktionen – würde die chinesische Regierung diesen Schatz an Daten dann wirklich nicht anrühren? Eine Jura-Professorin der führenden Tsinghua-Universität warf genau diese Frage über Weibo auf, als Peking während einer früheren Welle des Wiederauflebens von COVID-19 durch die Omikron-Variante im Jahr 2022 begann, Daten des öffentlichen Nahverkehrs in den Tracking-Apps zu konsolidieren. Die Professorin kritisierte die Praxis, Daten aus der Gesichtserkennung, Gesundheitscodes und der Nutzung öffentlicher Verkehrsmittel zu kombinieren, als potenziell maßlos und „gefährlich für den Schutz von öffentlichen Informationen durch die Verlinkung unterschiedlicher Datenban-

131 Mia Zhong. „China's COVID Apps: A Primer." DigiChina. 14. Juli 2022. https://digichina.stanford.edu/work/chinas-covid-apps-a-primer/

132 Almond Li. „Explainer: China's Covid-19 health code System." Hong Kong Free Press. 14. Juli 2022. https://hongkongfp.com/2022/07/13/explainer-chinas-covid-19-health-code-system/

133 "Notice on Protecting Personal Information and Using Big Data to Support Joint Prevention and Joint Control Work." Cyberspace-Administration China. 09. Februar 2020. https://digichina.stanford.edu/work/translation-chinese-authorities-emphasize-data-privacy-and-big-data-analysis-in-coronavirus-response/

ken ohne angemessene Gesetze oder Vorschriften“. Es ist nicht überraschend, dass ihr Beitrag innerhalb von weniger als 24 Stunden von Weibo gelöscht wurde.[134]

Es wurde schnell klar, dass die Bedenken in Bezug auf den Missbrauch der Gesundheitscodes und -Apps und der damit verbundenen Daten durchaus berechtigt waren. Ein Rechtsanwalt für Menschenrechte bemängelte, dass auf seiner Gesundheits-App ein roter Code erschien, als er im November 2021 nach Peking reisen wollte, um seine Mutter zu besuchen, nachdem es den Polizeibeamtinnen und -beamten nicht gelungen war, ihn von seiner Reise abzuhalten.[135] Im Jahr 2022, während der Bankenkrise in der Provinz Henan, erhielten Bankkundinnen und -kunden rote Codes in ihren Apps,[136] die sie daran hinderten, öffentliche Verkehrsmittel zu nutzen, öffentliche Einrichtungen zu betreten, an Protesten teilzunehmen, bei der Polizei Anzeige zu erstatten, an Gerichtsverhandlungen teilzunehmen, bei denen es um ihre eingefrorenen Konten bei diversen ländlichen Banken in der Provinz ging,[137] oder einfach ihr eigenes Haus zu verlassen. Dies war der bisher größte Fall von potenziellem Missbrauch der Gesundheitscode-App in China seitens der Regierung.

In Anbetracht der Tatsache, dass Chinas Politik der vollständigen Beseitigung von COVID bis zu ihrer plötzlichen Beendigung nach einer Welle von Protesten Ende 2022 so fest verankert war, schien es offen gesagt undenkbar, dass China dieses weit verbreitete und effektive Tracking-Gerät, das sich bereits in jeder Tasche befand, jemals zurücknehmen würde. Während die Regierung bekannt gab, dass einige Tools zur gesundheitlichen Nachverfolgung und zur Ermittlung von Kontaktpersonen, wie z. B. die „mobile Reisekarte“, deaktiviert wurden, war das Scannen von Gesundheitscodes, um den Nachweis zu erbringen, dass man COVID-frei war, anfangs noch an einigen wenigen Orten in China notwendig.

Die abrupte Kehrtwende in der Zero-Covid-Politik kann entweder als Zugeständnis an die öffentliche Missstimmung oder als unvermeidlicher Schritt zur Rettung von Chinas kollabierender Wirtschaft betrachtet werden. Jedenfalls kann sich die Staatsführung in Peking wohl sicher sein, dass sich dieses Überwachungsinstrument bewährt hat und jederzeit wieder eingesetzt werden kann.

5.3. Vom Datensicherheitsgesetz zur Cyber-Souveränität

Während Chinas Zensurregime heranreift und sich stabilisiert, richten sich die Bemühungen des Regimes, eine Cyber-Supermacht zu werden, nun auf Daten. Neben der Erweiterung der nationalen und globalen Kapazitäten, Daten zu sammeln und zu analysieren, ist die Kontrolle über Daten zu einer der wichtigsten nationalen Prioritäten geworden. Dies unterscheidet sich stark von der vorherrschenden Haltung der USA oder Europas in Bezug auf das Thema Datenkontrolle. Europa hat das Thema bisher als eine Wettbewerbsangelegenheit mit den USA betrachtet und die USA haben bis vor kurzem kaum Interesse an diesem Thema gezeigt. Und wenn sie an dieses Thema denken, geht es vor allem darum, die amerikanischen Spitzentechnologien im Zaum zu halten. Dies sollte China mehr Spielraum geben, um der Welt seine Vision der Datennutzung zu verkaufen, aber China hat sich zur gleichen Zeit auch mit der Cyber- und Datensouveränität beschäftigt. Beides zusammengenommen könnte durchaus einen gewissen Widerspruch mit sich bringen.

Man könnte es auch Datensouveränität nennen, für die China mit dem Cybersicherheitsgesetz von 2017 eine rechtliche Grundlage gelegt hat. Nach diesem Gesetz sind die Eigentümer und Verarbeiter von Daten in China verpflichtet, ihre Daten in China zu halten. Im September 2021 trat das Datensicherheitsgesetz (Data Security Law, DSL) in Kraft, das den Umfang des Cybersicherheitsgesetzes weiter ausweitete. Es führte mehr Kontrollen für globale Firmen ein, die in China tätig sind, und gilt für sämtliche Daten, die irgendetwas mit China zu tun haben oder auch nur durch China durchgeleitet werden.

Im DSL heißt es, dass das Gesetz "formuliert wurde, um die Handhabung von Daten zu standardisieren, die Datensicherheit sicherzustellen, die Entwicklung und Nutzung von Daten zu fördern, die gesetzlichen Rechte und Interessen von Einzelpersonen sowie Organisationen und die nationale Souveränität, Sicherheit und Entwicklungsinteressen zu schützen“.[138] Dies soll dadurch erreicht werden, dass „ein Datenklassifizierungssystem und Verpflichtungen für Organisationen, die mit Daten umgehen, eingeführt werden, einschließlich Sicherheitsbestimmungen und Evaluierungen für den Schutz, die Erhebung, die Nutzung und die Weitergabe von Daten im In- und Ausland“.[139]

Allerdings blieben auch nach der Einführung von DSL Unklarheiten über die Regeln für die Datenübermittlung bestehen: Was muss bleiben, was kann raus, und wie sehen die Verfahren zur Beurteilung aus? Im Juli 2022 wurden die langerwarteten Maßnahmen, um die Sicherheit ausgehender Datenübermittlungen zu untersuchen, schließlich von der CAC verabschiedet.[140] Die Definitionen in den früheren Gesetzen für Betreiber von kritischen Informationsinfrastrukturen und die Zulassungsbedingungen waren ziemlich verwirrend gewesen. Die neuen Maßnahmen sind zwar ausführlicher, doch nicht unbedingt hilfreicher.

134 https://digichina.stanford.edu/wp-content/uploads/2022/07/Screen-Shot-2022-07-14-at-1.52.49-PM.png
135 https://twitter.com/xieyang911/status/1456741388519804933
136 https://twitter.com/wangcongxh/status/1536978429479747585
137 „Das chinesische Covid-Pass-System, das vermeintlich zur Unterbindung von Protesten genutzt wurde, löst im Internet wütende Kritik aus.“ AFP via Hong Kong Free Press. https://hongkongfp.com/2022/06/15/china-covid-pass-system-allegedly-used-to-block-protest-sparking-furious-condemnation-online/
138 „Translation: Data Security Law of the People's Republic of China (Effective Sept. 1, 2021).“ DigiChina. 29. Juni 2021. https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/
139 „China's Evolving Data Governance Regime.“ U.S.-China Economic and Security Review Commission (CECC). 26. Juli 2022. https://www.uscc.gov/sites/default/files/2022-07/Chinas_Evolving_Data_Governance_Regime.pdf
140 „Outbound Data Transfer Security Assessment Measures.“ Cyberspace-Administration China. 07. Juli 2022. https://digichina.stanford.edu/work/translation-outbound-data-transfer-security-assessment-measures-effective-sept-1-2022/

Firmen müssen in den folgenden Fällen Selbstauskünfte erteilen und eine CAC-Bewertung beantragen: Wenn sie beabsichtigen, wichtige Daten im Ausland bereitzustellen, wenn sie Betreiber kritischer Informationsinfrastrukturen sind und personenbezogene Daten ins Ausland exportieren wollen, oder wenn sie personenbezogene Daten von mehr als einer Million Usern verarbeiten und diese Daten ins Ausland übermitteln wollen. Was aber sind „wichtige Daten"? In den Maßnahmen werden sie als Daten definiert, die, „wenn sie manipuliert, zerstört, gestohlen, illegal beschafft oder genutzt werden, die nationale Sicherheit, wirtschaftliche Angelegenheiten, die soziale Stabilität, die öffentliche Gesundheit oder die öffentliche Sicherheit beeinträchtigen können" – das ist zwar schön formuliert, aber nicht sehr hilfreich.

Die Branche wird also weiterhin mit solch unklaren Termini und vagen Definitionen umgehen müssen. Da es nur wenige oder überhaupt keine Vollzugsunterlagen gibt, auf die man sich beziehen kann, können Rechtsbeistände bzw. Analystinnen und Analysten in Bezug auf die Vorschriften nur zur Vorsicht raten, da die CAC und andere chinesische Aufsichtsbehörden sich einfach so viel Ermessensspielraum offenhalten wie möglich. Dadurch erhalten sie die größtmögliche Flexibilität, um Verfahren einzuleiten, wenn sie dies wünschen, und die Politik wird ihre Entscheidungen auch weiterhin prägen.[141]

Während China einerseits seine Datensouveränität festschreibt, um sensible Daten zu kontrollieren, die das Land verlassen, was es zum „datenrestriktivsten Land der Welt"[142] macht, will China andererseits auch die Macht der Daten für sich nutzen. Die KPCh schlug immer wieder vor, Daten zu einem „Produktionsfaktor" zu machen, neben den traditionellen Produktionsfaktoren wie Land, Arbeitskräfte, Kapital und Technologie. In diversen Planungsdokumenten des 14. Fünfjahresplans, wie z. B. jenen zur nationalen Informatisierung[143] und zur digitalen Wirtschaft,[144] wurde darauf hingewiesen, wie wichtig es ist, die Rahmenbedingungen und Standards zu schaffen, um die Zirkulation der „Datenfaktoren" zu optimieren.[145]

Doch trotz dieser Absicht könnte China bei der Umsetzung seiner Vision in die Praxis auf große Hindernisse stoßen. Der Plan für Daten erfordert eine strenge staatliche Lenkung des Datenwirtschaftsmarktes, wobei Daten in erster Linie als nationales Gut behandelt werden, das im Ermessen des Staates liegt. Im Einklang mit der dualen Zirkulationsstrategie des Landes, die sowohl den inländischen als auch den internationalen Markt ankurbeln soll, könnte China der inländischen Zirkulation den Vorrang geben und grenzüberschreitende Ströme und Allianzen auf streng kontrollierte Weise aufbauen.[146]

5.4. Was kommt als Nächstes? e-CNY, Blockchain, Metaverse, Web3 und IoT

Chinas Strategie für Überwachungstechnologien kann auch zukunftsorientiert ausgerichtet sein. Die Behörden verfolgen aufmerksam die neuesten Trends in der Entwicklung digitaler Technologien und werden so früh wie möglich einsteigen, um zu experimentieren und einen Weg zur Vorherrschaft zu finden.

Der digitale Renminbi, oder e-CNY, ist ein leuchtendes Beispiel dafür. Diese von der People's Bank of China (PBoC), der Zentralbank des Landes, ausgegebene Central Bank Digital Currency (CBDC) wird bereits seit mehr als zwei Jahren öffentlich getestet, wobei die Forschung bereits 2014 begonnen hat.[147] Die öffentlich erklärten Ziele der PBoC sind die Bekämpfung von Geldwäsche, Terrorismusfinanzierung und anderen illegalen Aktivitäten sowie die Verbesserung der Effizienz von Transaktionen im Finanzsystem des Landes. Kritikerinnen und Kritiker befürchten, dass das System der Regierung ermöglichen wird, alle Finanztransaktionen von Bürgerinnen und Bürgern sowie Unternehmen bis ins kleinste Detail auszuspionieren.

Das Projekt wurde bei den Olympischen Winterspielen 2022 in Peking getestet, obwohl die Teilnahme an der Veranstaltung durch COVID-19-Beschränkungen behindert wurde. Dennoch wurden dort mit einer Reihe von öffentlichkeitswirksamen Werbekampagnen in mehreren Großstädten über 260 Millionen elektronische Geldbörsen eingerichtet, wobei der Gesamtwert der Transaktionen über 87 Milliarden RMB erreichte.[148] Für ein Land mit mehr als 1,4 Milliarden Einwohnerinnen und Einwohnern ist die Akzeptanz des e-CNY jedoch noch relativ gering. Diejenigen, die die elektronischen Geldbörsen heruntergeladen haben, verfügen nur über ein geringes Guthaben auf ihrem e-CNY-Konto, und die für Transaktionen verwendeten Beträge sind entsprechend niedrig. Das mag daran liegen, dass der Markt für E-Payment-Dienste in China bereits

141 „Global companies need to look out for China's new data transfer rules." MERICS China Essentials. 14. Juli 2022. https://merics.org/en/merics-briefs/data-transfer-rules-g20-exports

142 Nigel Cory und Luke Dascoli. „How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them." Information Technology & Innovation Federation. 19. Juli 2021. https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/

143 Rogier Creemers, Hunter Dorwart, Kevin Neville, Kendra Schaefer, Johanna Costigan, und Graham Webster. „Translation: 14th Five-Year Plan for National Informatization - Dec. 2021." DigiChina. 24. Januar 2022. https://digichina.stanford.edu/work/translation-14th-five-year-plan-for-national-informatization-dec-2021/

144 "十四五"数字经济发展规划. 中国国务院." 21. Dezember 2021. http://www.gov.cn/zhengce/content/2022-01/12/content_5667817.htm

145 Charles Mok. „The Making of China's Future Internet." Friedrich-Naumann-Stiftung für die Freiheit. 18. Februar 2022. https://www.freiheit.org/taiwan/making-chinas-future-internet

146 Rebecca Arcesati. „China activates data in the national interest." MERICS. 04. Juli 2022. https://merics.org/en/short-analysis/china-activates-data-national-interest#msdynttrid=Z24YXo9vA-OMrEblhl1y4nLwz6rKly3Tt88FbVdCZH0

147 Jonathan Cheng. „China Rolls Out Pilot Test of Digital Currency." The Wall Street Journal. 20. April 2020. https://www.wsj.com/articles/china-rolls-out-pilot-test-of-digital-currency-11587385339

148 Ananya Kumar. „A Report Card on China's Central Bank Digital Currency: the e-CNY." Atlantic Council. 01. März 2022. https://www.atlanticcouncil.org/blogs/econographics/a-report-card-on-chinas-central-bank-digital-currency-the-e-cny/

von Plattformen wie AliPay und WeChat Pay beherrscht wird, die zusammen einen Marktanteil von über 80 Prozent halten.[149] Da die PBoC bei AliPay und WeChat Pay jedoch auch die Rolle der Regulierungsbehörde für E-Payment spielt, und angesichts der laufenden „vertieften Untersuchung" von kartellrechtlichen Fragen im E-Payment-Sektor,[150] ist es nicht ausgeschlossen, dass der e-CNY-Dienst schon bald weiter in diese Zahlungsdienste integriert wird. Der Staat könnte auch beschließen, einen oder beide dieser privaten E-Payment-Dienste zu „verstaatlichen", sodass die hohe Marktakzeptanz und die verbesserte Technologie, die für die Transaktionszeiten, den Durchsatz und die Zuverlässigkeit verwendet wird, sofort zum Tragen kommen.

Für viele Menschen mag Blockchain mehr Privatsphäre bedeuten, da die meisten Kryptowährungen wie Bitcoin die Distributed-Ledger-Technologie übernommen haben und auf dezentralen, zulassungsfreien Blockchains laufen, die offen, vertrauensunabhängig und für jeden zugänglich sind. Chinas dominantes, offiziell anerkanntes Blockchain-basiertes Servicenetzwerk (BSN) hingegen ist als genehmigte Blockchain eher zentralisiert. Das Projekt wird von einem Konsortium chinesischer staatlicher oder staatseigener Einrichtungen unterstützt, darunter das State Information Center unter der mächtigen Nationalen Entwicklungs- und Reformkommission, zusammen mit China UnionPay und China Mobile, obwohl es von einem in Hongkong ansässigen Unternehmen, Red Date Technology, geleitet und betrieben wird.[151] Als Backbone-Blockchain-Infrastrukturtechnologie für China zwischen der Regierung, Unternehmen und Einzelpersonen wird BSN auch auf die Digitale Seidenstraße, Chinas internationalem Projekt für die Partnerländer der Belt and Road Initiative (BRI), ausgedehnt, um Anwendungen über die Infrastruktur zu verbinden, ähnlich wie ein Cloud-Service.[152] Es ist unnötig zu erwähnen, dass die zentralisierten und staatlichen Eigenschaften der BSN bedeuten, dass die Infrastruktur wieder vollständig von der Regierung kontrolliert, wahrscheinlich auch überwacht, und daher keine gewöhnliche Blockchain sein wird.

Metaverse ist ein weiteres Schlagwort. Während die Definition des Metaverse schwer zu fassen ist, meint es im Allgemeinen einen virtuellen Raum, der Aspekte der physischen und der digitalen Welt miteinander verbindet, wobei die User sie durch Virtual-Reality- und Augmented-Reality-Anwendungen erfahren. Chinesische Big-Tech-Firmen wie Tencent, Baidu und Alibaba haben beträchtliche Investitionen in Hardware (z. B. VR-Headsets oder -Kameras) und Software (z. B. Spiele, Live-Unterhaltung und Produktivitätsanwendungen) getätigt, die mit dem Metaverse zusammenhängen. Was die staatliche Gesamtplanung für das Metaverse betrifft, so hat China bereits eine rechtliche Konsultation für potenzielle Vorschriften über so genannte „Deep-Synthesis-Aktivitäten in Internet-Informationsdiensten" herausgegeben, die Virtual-Reality-Umgebungen, Gesichts-, Ton- und Musikerzeugung usw. umfassen, um festzulegen, dass sie, wie alle anderen Internetdienste auch, „die zentrale sozialistische Wertvorstellung vorantreiben, die nationale Sicherheit und das öffentliche Interesse der Gesellschaft zu schützen"[153] und auf der Grundlage anderer Gesetze wie dem CSL, DSL, Internet Information Service Management Measures und dem PIPL arbeiten müssen. Mit anderen Worten: Das Metaverse in China wurde bereits vor seiner Geburt als tatsächlicher Dienst reguliert. In gewissem Sinne könnte das Metaverse in China und im Westen von Anfang an einen unterschiedlichen Verlauf nehmen, als „Splinterverse".

Und trotz der derzeitigen Konjunkturabschwächung in China und der anhaltenden Einschränkungen im Tech-Bereich bemühen sich die Regionalregierungen bereits um die Förderung von Unternehmen, die sich mit dem Metaverse beschäftigen. Shanghai hat Pläne für den Aufbau einer „52-Milliarden-Dollar"-Metaverse-Industrie und die Gründung von zehn innovativen Unternehmen durch die Einrichtung einer Reihe von Fonds und Subventionen zur Förderung von Forschung und Entwicklung vorgeschlagen.[154] Der Distrikt Tongzhou in Peking kündigte ein Projekt zur Umgestaltung eines alten Industriegebiets an, um dort eine 32.000 Quadratmeter große Metaverse-Kunstzone einzurichten, die ein „virtuelles Ökosystem im Metaverse-Stil" bilden soll. Ironischerweise werden dort für ein „virtuelles Projekt" Büros, Mitgestaltungsräume, Buchläden, Kinos usw. entstehen.[155] Ob Metaverse oder Web3, die Stadt Peking hat außerdem angekündigt, „ein bis zwei" führende „virtuelle menschliche" Unternehmen mit einem Umsatz von über fünf Milliarden Yuan zu fördern und einen entsprechenden Governance-Mechanismus zu entwickeln. Der Wettlauf um Subventionen und die Auswahl von Gewinnenden scheint eine Wiederholung der alten „Regierungsformel" für die technische Entwicklung zu sein.

149 Iori Kawate und Daisuke Maruyama. „China struggles to launch digital yuan after 8 years of trials." Nikkei Asia. 22. Juli 2022. https://asia.nikkei.com/Business/Markets/Currencies/China-struggles-to-launch-digital-yuan-after-8-years-of-trials

150 Frank Tang. „China to 'deepen' antitrust probe into mobile payment sector despite 'interim progress'." South China Morning Post. 24. September 2021. https://www.scmp.com/economy/china-economy/article/3149985/china-deepen-antitrust-probe-mobile-payment-sector-despite

151 Arjun Kharpal. „China has been quietly building a blockchain platform. Here's what we know." CNBC. 15. Mai 2022. https://www.cnbc.com/2022/05/16/china-blockchain-explainer-what-is-bsn-.html

152 Michael Sung. „China's National Blockchain Will Change the World." CoinDesk. 24. April 2020. https://www.coindesk.com/policy/2020/04/24/chinas-national-blockchain-will-change-the-world/

153 Roger Creemers und Graham Webster. „Translation: Internet Information Service Deep Synthesis Management Provisions (Draft for Comment) - Jan. 2022." DigiChina. 04. Februar 2022. https://digichina.stanford.edu/work/translation-internet-information-service-deep-synthesis-management-provisions-draft-for-comment-jan-2022/

154 Sergio Goschenko. „Shanghai Aims to Grow a $52 Billion Metaverse Cluster by 2025." Bitcoin.com. 15. Juli 2022. https://news.bitcoin.com/shanghai-aims-to-grow-a-52-billion-metaverse-cluster-by-2025/

155 Zijing Fu. „Peking to establish a 32000 square meter metaverse art zone in Tongzhou." Pingwest. https://en.pingwest.com/a/10099

Außerdem wäre da noch das IoT. Da China die „Fabrik der Welt“ ist, werden viele der heute verfügbaren IoT-Geräte und -Module zwangsläufig dort hergestellt, und viele werden in westlichen Produkten von Auto-, Computer-, Elektro- und Elektronikgeräteherstellern verwendet. Die US-Behörde für Cybersicherheit (CISA) hat vor kritischen Schwachstellen in GPS-fähigen IoT-Geräten aus chinesischer Produktion gewarnt, die in Autos und Motorrädern installiert sind, sowie vor dem Risiko von Datenverletzungen, durch die die Kontrolle über die Fahrzeuge potenziell an Hacker gelangen könnte.[156]

China wird weiterhin sein zentralisiertes Politik- und Technologiekontrollmodell nutzen, um mit dem Westen zu konkurrieren. Das ist nicht das Modell, das die freie Welt nachahmen sollte, denn es ist nicht förderlich für freies Denken, Kreativität und Innovation. Die Demokratien sollten sich den Risiken jedoch stets bewusst sein, insbesondere aufgrund ihrer Verflechtung und Abhängigkeit von China, und geeignete Maßnahmen zum Schutz ihrer Infrastrukturen, Investitionen, Institutionen und Menschen ergreifen.

156 Alexi Drew. „Chinese technology in the 'Internet of Things' poses a new threat to the west.“ 10. August 2022. https://www.ft.com/content/cd81e231-a8d3-4bc0-820a-13f525a76117

6. Chinas allgegenwärtige Firewall – Transnationalisierung des digitalen Autoritarismus

6.1. Digitale Seidenstraße

Chinas „Digitale Seidenstraße“ (Digital Silk Road, DSR) wurde 2015 als Teil der BRI ins Leben gerufen, der globalen Strategie des Landes für Infrastrukturinvestitionen, Entwicklung und Diplomatie. Die Initiative ist nicht genau definiert und wird eher als Markenbegriff für chinesische Technologieunternehmen verwendet, die mit Kundinnen und Kunden oder Partnern in BRI-Ländern auf der ganzen Welt Vertriebs- oder Geschäftskooperationen eingehen, die häufig chinesische Investitionen oder Finanzierungen beinhalten.[157]

Bislang sind sich die Expertinnen und Experten uneinig darüber, ob die DSR ein „Masterplan Pekings zur Anwendung seines techno-autoritären Modells“[158] in den BRI-Ländern ist. Einige sind der Meinung, dass Gesichtserkennungstechnologie und in die Privatsphäre eingreifende Cyber-Infrastruktur zwar tatsächlich in BRI-Länder exportiert werden könnten, dass diese jedoch eher von der Nachfrage als von Peking diktiert werden. Chinas Absicht könnte eher darin bestehen, den Export der proprietären Technologien seiner Anbieter zu unterstützen, um die Festlegung globaler Technologiestandards zu beeinflussen.[159] Aber in jedem Fall wird China profitieren.

Für andere Beobachtende stellen viele der an DSR-Projekten beteiligten Unternehmen Güter mit doppeltem Verwendungszweck für militärische und industrielle Zwecke

157 Assessing China's Digital Silk Road Initiative. Council for Foreign Relations. https://www.cfr.org/china-digital-silk-road/
158 Ibid.
159 Robert Greene und Paul Triolo. „Will China Control the Global Internet Via its Digital Silk Road?“ Carnegie Endowment for International Peace. 08. Mai 2020. https://carnegieendowment.org/2020/05/08/will-china-control-global-internet-via-its-digital-silk-road-pub-81857

her. Einige dieser Projekte müssen offensichtlich in die Kategorie der digitalen autoritären Werkzeuge fallen, wie etwa die „nationale Firewall der nächsten Generation". Infrastrukturausbauprojekte für BRI-Länder umfassen häufig Dienste zur aktiven Überwachung und Datenanalyse.[160]

Alle Expertinnen und Experten sind sich jedoch einig, dass Chinas politischer Einfluss und sein politischer Fokus auf die DSR nur zunehmen werden. Peking hat ein großes Interesse daran, seine Unternehmen zu nutzen, um eine bessere Wettbewerbsposition in den BRI-Ländern zu erlangen, insbesondere in Bereichen wie 5G, Mobilfunk, Cloud, Datenanalyse, KI und sogar Satellitenortung und -navigation. Dies wird zum Teil auch als eine Möglichkeit gesehen, den Bemühungen der westlichen Länder um eine technologische Abkopplung von China entgegenzuwirken.

In Afrika sind chinesische Unternehmen beispielsweise stark in die digitalen Technologiemärkte des Kontinents eingedrungen, wobei Regierungen wie Tansania, Kamerun, Kenia, Nigeria, Äthiopien, Guinea, die Elfenbeinküste und Sierra Leone chinesische Staatsfinanzierungen für Netzwerkinfrastrukturprojekte akzeptieren, die hauptsächlich von Huawei und ZTE bedient werden, mit Finanzierungen zwischen 30 und 337 Millionen US-Dollar.[161] Einige afrikanische Staaten sind möglicherweise weniger besorgt über die angeblichen Sicherheitsrisiken und Hintertüren, die von Netzwerkausrüstung aus chinesischer Produktion ausgehen, und einige begrüßen die Überwachungshilfe sogar. Eine Untersuchung des Wall Street Journal aus dem Jahr 2019 ergab, dass technisches Personal von Huawei tatsächlich staatliche Cybersicherheitskräfte in Uganda und Sambia dabei unterstützt, verschlüsselte Kommunikation und Social-Media-Nachrichten abzufangen und Zellstandortdaten zu nutzen, um politische Gegner zu verfolgen.[162]

In Asien haben Länder wie Pakistan, Laos, Brunei und Thailand bereits BeiDou, Chinas globales Satellitenortungssystem, übernommen, und auch in BRI-Regionen wie Zentralasien, dem Nahen Osten und Afrika wird es zunehmend eingesetzt.[163] Kambodschas geplantes „nationales Internet-Gateway", das „Vermittlung und Verwaltung von Internetverbindungen zur Verbesserung der Einnahmeerhebung der Regierung, der nationalen Sicherheit und der Bewahrung von sozialer Ordnung, Kultur und Tradition" ermöglichen soll, ist eine Imitation der GFW, obwohl sich dessen Einführung verzögert hat.[164] Auch Thailands Militärregierung hat 2015 einen gescheiterten Versuch, eine eigene nationale Firewall nach chinesischem Vorbild zu errichten wieder aufgegriffen – im Namen der nationalen Sicherheit und zur Verhinderung von Online-Kriminalität, zur Beschränkung des Zugangs zu externen Online-Inhalten und zur Regulierung von Online-Nachrichten.[165] Auch wenn diese Projekte vielleicht nicht unter der Bezeichnung DSR laufen oder direkt von China finanziert werden, wie es bei einigen afrikanischen Projekten der Fall ist, so gehören sie doch zu einem Trend, bei dem autokratische Regierungen Chinas Zensur mit Bewunderung betrachten und imitieren, wobei sie häufig auf chinesische Technologien zurückgreifen. Es sollte daher nicht überraschen, dass die nationale Cybersicherheitsbehörde Thailands gerade eine Absichtserklärung mit Huawei unterzeichnet hat, um bei der Entwicklung von Cybersicherheitskompetenzen im Land zusammenzuarbeiten.[166]

Einige werden sicherlich argumentieren, dass es nicht nur chinesische Technologieunternehmen sind, die autoritären Staaten Überwachungstechnologien zur Verfügung stellen. Cisco hat es getan, und andere israelische und US-amerikanische Unternehmen folgen diesem Beispiel. Autoritäre Regierungen wollen solche Überwachungssysteme und andere digitale Instrumente. Doch im Gegensatz zu den genannten Unternehmen müssen chinesische Firmen keine Gegenreaktionen im eigenen Land befürchten. Wenn es nach einem perfekten Zusammentreffen von gemeinsamen illiberalen und totalitären Werten aussieht, können die demokratischen Staaten nicht einfach von der Seitenlinie aus zusehen.

6.2. Die Hacker der nationalistischen öffentlich-privaten Partnerschaft

Der Begriff „Great Firewall" weckt oft das Bild eines defensiven Wächters, der unerwünschte Inhalte fernhält. Aber wie wir gesehen haben, handelt es sich in Wirklichkeit um ein viel aggressiveres Konzept. Viele Menschen haben Warnungen vor potenziellen, staatlich gesponserten Hacking- oder Phishing-Versuchen auf ihren Google-Konten erhalten, wie z. B.: „Von der Regierung unterstützte Angreifende versuchen möglicherweise, Ihr Passwort zu stehlen." Nach Angaben des Unternehmens wurden bis Oktober 2021 etwa 50.000 solcher Warnungen verschickt, was einem Anstieg von fast einem Drittel gegenüber dem gleichen Zeitpunkt vor einem Jahr entspricht.[167] Nicht alle davon kamen aus China: Russische und iranische Hacker teilen sich die „Ehre", die meisten „nennenswerten" Kampagnen durchzuführen, aber auch chinesische Hacker sind nicht zu ignorieren.

160 "数字丝绸之路." https://chinadigitaltimes.net/space/%E6%95%B0%E5%AD%97%E4%B8%9D%E7%BB%B8%E4%B9%8B%E8%B7%AF

161 Motolami Agbebi. „China's Digital Silk Road and Africa's Technological Future." Council for Foreign Relations. https://www.cfr.org/sites/default/files/pdf/Chinas%20Digital%20Silk%20Road%20and%20Africas%20Technological%20Future_FINAL.pdf

162 Joe Parkinson, Nicholas Bariyo, und Josh Chin. „Huawei Technicians Helped African Governments Spy on Political Opponents." The Wall Street Journal. 15. August 2019. https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017

163 Richard Ghiasy und Rajeshwari Krishnamurthy. „China's Digital Silk Road and the Global Digital Order." The Diplomat. 12. April 2021. https://thediplomat.com/2021/04/chinas-digital-silk-road-and-the-global-digital-order/

164 Adrian Wan und Charles Mok. „Internet Impact Brief: Cambodia National Internet Gateway." Internet Society. 18. Februar 2022. https://www.internetsociety.org/resources/2022/internet-impact-brief-cambodia-national-internet-gateway/

165 Joseph O'Connor. „Minister signals a move to resurrect a national internet gateway and stronger online controls." ThaiExaminers.com. 22. Februar 2022. https://www.thaiexaminer.com/thai-news-foreigners/2022/02/22/minister-resurrects-internet-gateway-scheme/

166 „National Cyber Security Agency signs MoU with Huawei." Bangkok Post. 03. August 2022. https://www.bangkokpost.com/thailand/pr/2360342/national-cyber-security-agency-signs-mou-with-huawei

167 Sergio Gatlan. „Google sent 50,000 warnings of state-sponsored attacks in 2021." Bleeping Computer. 14. Oktober 2021. https://www.bleepingcomputer.com/news/security/google-sent-50-000-warnings-of-state-sponsored-attacks-in-2021/

Ein frühes Beispiel für solche Aktivitäten bot GhostNet, eine groß angelegte Cyberspionageoperation, die 2009 von Forschenden des Information Warfare Monitor entdeckt und benannt wurde. Es wurde eingesetzt, um Zielobjekte vom Dalai Lama bis hin zu Botschaften und Regierungsstellen vieler Länder auf der ganzen Welt auszuspionieren, darunter Indien, Südkorea, Indonesien, Rumänien, Zypern, Thailand, Deutschland und Pakistan. Das Hackernetzwerk soll im Jahr 2009 1.295 Computer in 103 Ländern infiltriert haben.[168] Die von GhostNet hauptsächlich eingesetzte Trojaner-Malware war Gh0st RAT, die auf Windows-Computer abzielte, indem sie Programm- und andere Dateien in den Systemordnern anlegte, die Spionageprogramme beim Neustart der Computer startete und ausführte und Hintertüren einrichtete, um mit den Command-and-Control-Servern zu kommunizieren, die sich in der chinesischen Provinz Hainan befanden. Der ferngesteuerte „Geist" konnte jeden Tastendruck beobachten und auf jede Datei zugreifen, die auf den infizierten Computern erstellt wurde.[169]

Es ist schwer, sich über die Art der chinesischen Hacker-Einheiten Klarheit zu verschaffen. Neben den Bemühungen, die direkt von Regierungseinheiten, insbesondere dem Militär, geleitet werden, bestehen auch aktive inoffizielle Einheiten wie die so genannte Cyber-Miliz und die Hacktivisten-Einheiten.[170] Cyber-Milizen sind Gruppen, die sich aus Hackern, Wissenschaftlerinnen und Wissenschaftlern, Netzwerkingenieurinnen und -ingenieuren und Fremdsprachenübersetzerinnen und -übersetzern sowie IT-Unternehmen zusammensetzen. Sie spielen eine wichtige, aber unklare Rolle außerhalb des Militärs.

Hacktivistinnen und Hacktivisten hingegen sind weitaus kämpferischer und aggressiver. Ein Beispiel ist die „Red Hacker Alliance", die seit Anfang der 2000er Jahre mit Hunderttausenden von Hackern aktiv ist. Sie wurde auch als Täter eines geplanten, öffentlichkeitswirksamen DDoS-Angriffs gegen CNN.com im April 2008 angeführt. Die Gruppe schien selbstorganisiert zu sein, wurde aber von der Regierung stillschweigend anerkannt. Sie wurde im April 2005 in einem Artikel der offiziellen chinesischen Nachrichtenagentur Xinhua erwähnt, in dem die Gruppe als „Anti-Hacking-Gruppe" bezeichnet wurde. In dem Artikel hieß es weiter, die Mitglieder der Allianz könnten „in wenigen Minuten einen Computervirus entwerfen", würden dies allerdings unterlassen, da es ihre Aufgabe sei, „die Web sites [sic!] vor Angriffen zu schützen", insbesondere vor solchen aus dem Ausland.[171]

Die Beziehung zwischen Staat und Hacktivistinnen und Hacktivisten ist mitunter kompliziert. Untersuchungen von Daten aus den Jahren 1990 bis Anfang 2012 zeigen, dass die Cyberangriffe chinesischer Hacktivistinnen und Hacktivisten in dem Maße, in dem sie politisch motivierter, öffentlicher und zurechenbarer wurden, auch zunehmend mit den Auseinandersetzungen und Drohungen des chinesischen Staates mit seinen Gegnern zusammenhingen, ähnlich wie bei russischen und iranischen Hackergruppen. Es scheint klar zu sein, dass China diese Angriffe zuließ, um Drohungen und Warnsignale an seine Gegner zu senden. Gleichzeitig könnten die Angreifenden als „nationalistischer als der Staat" angesehen werden und China einen diplomatischen Preis auferlegen, wenn es in einem bestimmten Streit „nachgibt". In diesem Fall bestünde die Gefahr, dass sich die Hacktivistinnen und Hacktivisten gegen ihren eigenen Staat wenden, oder ihre Angriffe im Ausland „außer Kontrolle" geraten und einen unumkehrbaren Konflikt zwischen den Staaten auslösen.[172] Obwohl diese Szenarien noch nicht eingetreten sind, bleiben solche Risiken bestehen, insbesondere bei nationalistischen Themen wie Taiwan, die stetig an Brisanz gewinnen.

Jedoch war es die direkte Rolle des chinesischen Militärs bei chinesischen Angriffen in Übersee, die die Aufmerksamkeit der westlichen Strafverfolgungsbehörden auf sich zog. Im Mai 2014 kündigte das US-Justizministerium eine Anklage an. Sie richtete sich gegen fünf Offiziere der Einheit 61398 der Volksbefreiungsarmee wegen Diebstahls vertraulicher Geschäftsgeheimnisse und geistigen Eigentums von US-amerikanischen Unternehmen, darunter Alcoa, Allegheny Technologies, U.S. Steel, Westinghouse und andere, sowie wegen der Installation von Schadsoftware auf deren Computern.[173] Ihre Hackergruppe erlangte Bekanntheit unter dem Namen APT1.

Im Juni 2015 gab das United States Office of Personnel Management (OPM) eine Datenpanne von etwa 22,1 Millionen Personaldaten und -aufzeichnungen von Regierungsangestellten bekannt, darunter auch solche, die einer Sicherheitsüberprüfung unterzogen worden waren. Der Vorfall war besonders heikel, da die Identitäten zahlreicher Geheimdienstmitarbeitenden preisgegeben wurden. Der Hack war seit Ende 2013 in mindestens zwei Angriffszyklen durchgeführt worden. Die Angreifenden galten weithin als staatlich gesponserte Hacker, die für die chinesische Regierung arbeiteten, und in den folgenden Jahren kam es zu einer Reihe von Verhaftungen oder Anklagen chinesischer Staatsangehöriger in den USA wegen Cyberangriffen im Zusammenhang mit den OPM-Hacks.[174]

168 „Major cyber spy network uncovered." BBC. 29. März 2009. http://news.bbc.co.uk/1/hi/world/americas/7970471.stm

169 James Griffiths. „The Great Firewall of China." Kapitel 13.

170 Mike Raud. „China and Cyber: Attitudes, Strategies, Organization." NATO CCD-COE. August 2016. https://ccdcoe.org/uploads/2018/10/CS_organisation_CHINA_092016_FINAL.pdf

171 „China's anti-hacking alliance regrouped." Xinhua and Shenzhen Daily. 26. April 2005. https://web.archive.org/web/20090622160745/http://news.xinhuanet.com/english/2005-04/26/content_2879866.htm

172 Jeffrey Kwong. „State Use of Nationalist Cyber Attacks as Credible Signals in Crisis Bargaining. China and Cybersecurity. Political, Economic, and Strategic Dimensions." Bericht von Workshops an der UCSD. April 2012. http://www.bdo3c.f-sc.org/archives/921.pdf

173 Jim Finkle, Joseph Menn, und Aruna Viswanatha. „U.S. accuses China of cyber spying on American companies." 20. November 2014. https://www.reuters.com/article/us-cybercrime-usa-china-idUSKCN0J42M520141120

174 Josh Fruhlinger. „The OPM hack explained: Bad security practices meet China's Captain America." CSO. https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html

Unmittelbar nach der Enthüllung der OPM-Hacks verkündete Präsident Barack Obama Ende 2015, als der chinesische Präsident Xi Jinping die USA besuchte, eine „gemeinsame Vereinbarung" mit China über Cyberspionage. Das gemeinsame Verständnis bestand darin, dass die beiden Regierungen zwar nicht auf die „traditionelle Cyberspionage von Regierung zu Regierung" verzichten, es aber vermeiden würden, wissentlich den Cyberdiebstahl von Betriebsgeheimnissen oder Geschäftsinformationen zu unterstützen. Xi wiederholte natürlich, dass China ein Opfer von Hacking sei, dass die chinesische Regierung keine Rolle beim Hacken von US-Zielen spiele und dass das Thema nicht „politisiert" werden dürfe.[175]

In jenen Tagen, als die Beziehungen zwischen den USA und China noch nicht so frostig waren, wurde die Xi-Obama-Vereinbarung zur Cybersicherheit vorsichtig begrüßt, aber die meisten Beobachtenden waren skeptisch, ob China sich an seine losen Versprechen halten würde. Während erste Daten des IT-Sicherheitsunternehmens FireEye zeigten, dass es 2016 einen „spürbaren Rückgang" chinesischer Eindringlinge gegen Unternehmen und 25 andere Länder gab, war es auch möglich, dass die chinesischen Hackergruppen angewiesen wurden, sich vorübergehend anderen Zielen wie Russland zuzuwenden, wie die russische Sicherheitsfirma Kaspersky Lab berichtete.[176]

Fakt ist jedoch, dass seit 2016 die Zahl der als „Advanced Persistent Threat" (APT) bezeichneten Gruppen – Akteure, die in der Regel von einem Staat unterstützt werden – ständig gestiegen ist. Es wird nach wie vor vermutet, dass viele dieser APT-Gruppen in China angesiedelt sind. Im März 2022 wurden sechs US-Bundesstaaten von einer chinesischen Gruppe organisierter ziviler Verbrechersyndikate gehackt, die unter der Bezeichnung APT41,[177] oder „Double Dragon" agiert. Dies geschah über eine Schwachstelle in einer Software zur Erfassung von Viehseuchen, die in diesen Bundesstaaten verwendet wurde.[178] Sieben Personen der Gruppe wurden im September 2020 vom US-Justizministerium angeklagt, wobei zwei von ihnen in Malaysia festgenommen wurden und die anderen fünf in China auf der Flucht sind.[179]

Chinas Fähigkeiten und Reichweite bei Cyberangriffen werden immer größer. Eines der jüngsten Beispiele stellt eine weitere APT-Gruppe mit dem Namen TA418 dar. Ihr Schwerpunkt liegt auf Angriffen auf Ziele in Asien und Osteuropa, einschließlich Russland. Die Gruppe nutzt in erster Linie Schwachstellen in Microsoft Office, die es den Hackern ermöglichen, durch eine Hintertür auf Dateien in den betroffenen Computern zuzugreifen und die gestohlenen Daten an Server in China zu senden, so Kaspersky Lab.[180]

Darüber hinaus finden sich Beispiele für chinesische Hackerangriffe, die eng mit den politischen und militärischen Aktivitäten des Landes verbunden sind. Im Zuge des Besuchs der Sprecherin des US-Repräsentantenhauses Nancy Pelosi in Taiwan wurden Cyberangriffe und Desinformationskampagnen gegen Taiwan offensichtlich verstärkt. Dabei stellten taiwanesische Verteidigungsbehörden fest, dass „Operationen der kognitiven Kriegsführung" bereits vor Chinas Ankündigung von Militärübungen begonnen wurden, was die Entstehung eines Modells der hybriden Kriegsführung gegen Taiwan befürchten lässt. So wurden beispielsweise die digitale Beschilderung in 7-Eleven-Läden im ganzen Land und ein großer Bahnhof in der Stadt Kaohsiung gehackt, um Protestbotschaften gegen Pelosi zu verbreiten, und die offizielle Website des Präsidialamtes der taiwanesischen Staatspräsidentin Tsai Ing-Wen wurde aufgrund eines Cyberangriffs für zwanzig Minuten lahmgelegt.[181] Zwar scheinen solche gezielten Angriffe nicht vom chinesischen Militär durchgeführt zu werden, doch sind sie möglicherweise ein Beispiel für die Art von Cyber-Störungen, zu denen eine große Zahl chinesischer ziviler Hacker in der Lage ist.

6.3. Chinas globale Datenerfassung

Chinas Regierung ist davon überzeugt, dass sie im eigenen Land so viele Kanäle zur Datenerfassung über ihre Bürgerinnen und Bürger, Unternehmen, Organisationen und deren Aktivitäten schaffen und unterhalten sollte. Diese Überzeugung macht nicht an den Landesgrenzen halt. So sind Chinas wachsende Exporte seiner technologischen Produkte und Leistungen zum perfekten Mittel geworden, um weltweit Daten zu sammeln, und zwar sowohl gezielt als auch wahllos.

6.3.1. 5G und Infrastruktur: Huawei et al.

Huawei stand immer wieder im Fokus im Zusammenhang mit Vorwürfen, seine Geräte enthielten verdeckte „Backdoors", um ohne das Wissen der User Informationen und Daten zu sammeln. Das lag zum Teil daran, dass die Geräte des Unternehmens, die an Telekommunikations- und Mobilfunkanbieter in aller Welt verkauft und von diesen genutzt werden, hochkomplex sind, und dass Backdoors von Natur aus schwer zu erkennen und zu beweisen sind.

175 Matt Spetalnick und Michael Martina. „Obama announces 'understanding' with China's Xi on cyber theft but remains wary." 25. September 2015. https://www.reuters.com/article/us-usa-china/obama-announces-understanding-with-chinas-xi-on-cyber-theft-but-remains-wary-idUSKCN0RO2HQ20150926

176 James Griffiths. „The Great Firewall of China." Kapitel 16.

177 APT 41 Group. „FBI Most Wanted." https://www.fbi.gov/wanted/cyber/apt-41-group

178 Garrett O'Brien. „Who is APT41?" The Wire China. 31. Juli 2022. https://www.thewirechina.com/2022/07/31/who-is-apt41/

179 „Seven International Cyber Defendants, Including 'Apt41' Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally." Pressemitteilung des US-Justizministeriums. 16. September 2022. https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer

180 Sergio Gatlan. „Chinese hackers use new Windows malware to backdoor govt, defense orgs." Bleeping Computer. https://www.bleepingcomputer.com/news/security/chinese-hackers-use-new-windows-malware-to-backdoor-govt-defense-orgs/

181 Hsia Hsiao-hwa und Raymond Chung. „China steps up cyberattacks, disinformation campaigns targeting Taiwan." Radio Free Asia. 08. August 2022. https://americanmilitarynews.com/2022/08/china-steps-up-cyberattacks-disinformation-campaigns-targeting-taiwan/

Im Februar 2020 zitierte ein Bericht des Wall Street Journal US-Bedienstete, die behaupteten, Huawei habe heimlich Wege für den Zugang zu Netzwerken offen gehalten. Dies geschah über Schnittstellen, die auf ihren Geräten ohne das Wissen ihrer Kundinnen und Kunden, den Netzbetreibern, betrieben wurden. Die Beamtinnen und Beamten erklärten, dass sie die Situation seit mehr als einem Jahrzehnt beobachtet haben, lehnten es jedoch ab zu erklären, ob die USA das Unternehmen bei der Nutzung dieses Zugangs tatsächlich beobachtet haben. Sie weigerten sich auch, weitere Einzelheiten über diese Backdoors zu nennen.[182]

Diese Zweideutigkeit hat einige zu der Annahme veranlasst, dass diese Anschuldigungen nur spekulativer oder politischer Natur und somit falsch waren. Nichtsdestotrotz haben die USA ein Verbot der Geräte von Huawei in ihren eigenen Netzen sowie in jenen ihrer Verbündeten gefordert. Eine wachsende Zahl von Ländern ist dem Beispiel der USA gefolgt, darunter Großbritannien, Kanada, Australien und Neuseeland. Einige Länder wie die USA und Kanada haben zudem ein Verbot für den wichtigsten chinesischen Konkurrenten von Huawei, ZTE, verhängt.[183] Im November 2022 verbot die Biden-Administration die Genehmigung für den Kauf neuer Telekommunikationsgeräte von Huawei, ZTE und mehreren anderen chinesischen Unternehmen für Überwachungstechnologie, weil sie ein „inakzeptables Risiko" für die nationale Sicherheit der USA darstellen.[184]

Ein Großteil der Bedenken der USA und anderer westlicher Staaten gegenüber Huawei konzentrierte sich zunächst auf die engen Beziehungen des chinesischen Militärs zu dem Unternehmen und dessen Gründer Ren Zhengfei.[185] Und da das Unternehmen privat und nicht börsennotiert ist, sind die Informationen darüber noch undurchsichtiger als bei anderen, börsennotierten chinesischen Technologieunternehmen. Huawei bestreitet diese Vorwürfe natürlich öffentlich und verweist darauf, dass Backdoors zum Zwecke des „rechtmäßigen Abhörens" für Strafverfolgungs- oder Wartungszwecke üblich sind und nur unter strenger Aufsicht eingesetzt werden, und dass das Unternehmen niemals eine Sicherheitslücke in seinem Netzwerk installiert habe.[186]

Es sollte jedoch darauf hingewiesen werden, dass die Schwachstellen eines Netzes, die darauf zurückzuführen sind, dass seine Ausrüstung ohne das Wissen des Betreibers missbraucht wird, nicht nur das Vorhandensein und die Verwendung von Backdoors umfassen. Backbone-Netzausrüstungen für Netzbetreibende sind komplex, und in der Regel spielen Geräte- und Technologieanbieter bei der Gestaltung der Netzarchitektur und der Betriebsdetails mit den Kunden des Netzbetreibers eine Rolle. Sie verkaufen nicht nur standardisierte Hardware, sie erhalten auch eine Vielzahl von Informationen über die Netzgestaltung und den Betrieb der Kundinnen und Kunden. Dieses Wissen kann, wenn es in die falschen Hände gerät, ebenfalls Anlass zur Sorge geben, da Staaten nicht wollen, dass ihren Gegnerinnen und Gegnern der Gesamtentwurf ihrer wichtigsten Infrastrukturelemente oder deren Schwachstellen bekannt werden.

Selbst wenn einige Länder den Kauf von Huawei-Geräten verbieten, ist es keine leichte Aufgabe, die bereits im Einsatz befindlichen Geräte zu ersetzen. Es wird vermutet, dass beispielsweise in den USA viele ländliche Netzwerke mit alter chinesischer Technik ausgestattet sind, deren Austausch sich die lokalen Betreiber nicht leisten können, und dass, selbst wenn sie sie ersetzen wollen, die entsprechenden Subventionen der US-Regierung gekürzt wurden.[187] Die Abhängigkeit der europäischen Länder von Huawei und anderen chinesischen Netztechnologien ist auch für die bestehende 4G-Infrastruktur von Bedeutung, wenn nicht sogar für 5G, ganz zu schweigen von vielen anderen Teilen Asiens und Afrikas, wo der Marktanteil von Huawei möglicherweise sogar steigt.

Neben Huawei und ZTE sind auch viele andere chinesische Technologieunternehmen als Teil von Chinas verdeckter Datenerfassung in den Blick geraten. Sie fallen in mehrere Kategorien: Überwachungsgeräte, digitale Produkte und Dienstleistungsplattformen sowie soziale Medien.

182 Bojan Pancevski. „U.S. Officials Say Huawei Can Covertly Access Telecom Networks." The Wall Street Journal. 12. Februar 2022. https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256

183 „Canada bans China's Huawei Technologies from 5G networks." Associated Press. 20. Mai 2002. https://www.npr.org/2022/05/20/1100324929/canada-bans-chinas-huawei-technologies-from-5g-networks

184 Diane Bartz und Alexandra Alper. „U.S. bans new Huawei, ZTE equipment sales, citing national security risk." Reuters. 30. November 2022. https://www.reuters.com/business/media-telecom/us-fcc-bans-equipment-sales-imports-zte-huawei-over-national-security-risk-2022-11-25/

185 Kate O'Flaherty. „Huawei Security Scandal: Everything You Need to Know." Forbes. 26. Februar 2019. https://www.forbes.com/sites/kateoflahertyuk/2019/02/26/huawei-security-scandal-everything-you-need-to-know/?sh=2814f40473a5

186 „What exactly is a backdoor? Here's a quick tutorial." Huawei. https://www.huawei.com/ie/media-center/transform/01/what-is-a-backdoor

187 Jon Heldel. „Why suspected Chinese spy gear remains in America's telecom networks." Politico. https://www.politico.com/news/2022/07/21/us-telecom-companies-huawei-00047045

6.3.2. Überwachungs-Software: HikVision et al.

Manche bezeichnen HikVision als „das größte Überwachungsunternehmen der Welt, von dem Sie noch nie gehört haben".[188] Ob es nun das größte Unternehmen der Branche ist oder nicht, sein Name wurde zum Synonym für die Verwicklung des IT-Sektors in Chinas Menschenrechtsverletzungen in Xinjiang. Die Überwachungskameras des Unternehmens werden von der Polizei und anderen Behörden auf der ganzen Welt eingesetzt, um Bürgerinnen und Bürger überall zu überwachen, oft mit Gesichtserkennungsfunktionen. Das Unternehmen hat schnell Bekanntheit erlangt, und die Liste der von den USA und anderen westlichen Ländern gegen das Unternehmen verhängten Sanktionen wird zweifellos kontinuierlich länger.

Im Oktober 2021 verabschiedete das US-Repräsentantenhaus den Secure Equipment Act of 2021, um die Einfuhr und den Verkauf aller neuen Produkte von HikVision und einem anderen chinesischen Unternehmen, Dahua Technology, wirksam zu verbieten. Darüber hinaus wurde die Federal Communications Commission (FCC) förmlich verpflichtet, die vorgeschlagenen Maßnahmen zu übernehmen, die die FCC selbst zuvor für Unternehmen eingeführt hatte, deren Produkte und Technologien als Bedrohung der nationalen Sicherheit eingestuft wurden.[189] Seit März 2021 stehen die Produkte und Leistungen von Unternehmen wie Huawei, ZTE, HikVision, Hytera Communications, Dahua Technology, China Mobile, China Telecom sowie des russischen IT-Sicherheitsunternehmens AO Kaspersky Lab auf der FCC-Liste.[190] Berichten zufolge wird in Washington immer noch über eine Verschärfung dieser Sanktionen diskutiert, einschließlich der Aufnahme von HikVision in die Kategorie der „Most Wanted" auf der SDN-Sanktionsliste der USA.[191]

Wie im Falle von Huawei sind auch bei HikVision die engen Verbindungen zur chinesischen Regierung ein Grund zur Sorge. Das Unternehmen hat 48 Prozent seiner Anteile an den chinesischen IT-Konzern CETC übertragen und ist damit faktisch ein Tochterunternehmen eines staatlichen Unternehmens. Darüber hinaus ist HikVision durch seine tiefe Verstrickung in die chinesische Unterdrückung in Xinjiang, wo das Unternehmen mindestens 275 Millionen Dollar an staatlichen Verträgen zum Aufbau seines Überwachungsnetzes erhalten hat, sicherlich negativ aufgefallen.

Neben den USA haben auch britische Parlamentsabgeordnete auf ein Verbot des Verkaufs und der Verwendung von HikVision- und Duhua-Geräten in ihrem Land gedrängt und den weit verbreiteten Einsatz dieser Überwachungskameras mit dem „dystopischen Überwachungsstaat" wie in Xinjiang in Verbindung gebracht.[192] Untersuchungen der britischen Gruppe Big Brother Watch ergaben, dass 73 Prozent der britischen Kommunen, 57 Prozent der weiterführenden Schulen, sechzig Prozent der National Health Service Trusts sowie Universitäten, die Polizei und andere Regierungsstellen diese chinesischen Geräte verwenden.[193] Der liberale Abgeordnete Lord David Alton warnte ebenfalls vor der Datenerfassung und äußerte seine Sorge, dass Daten von Sicherheitskameras im Vereinigten Königreich an andere Länder weitergegeben werden könnten.[194] Im November 2022 kündigte die britische Regierung ein Verbot der Installation von Sicherheitskameras von HikVision in britischen Regierungsgebäuden und -einrichtungen an.[195] Auch die US-Regierung verbot jegliche Neueinfuhr chinesischer Überwachungsgeräte von HikVision sowie von Dahua Technology und Hytera Communications.[196]

Backdoors in Videokameras von HikVison und anderen Unternehmen, ob absichtlich oder durch Fehler, sind ein weiteres ernsthaftes Problem. IPVM, ein führendes Medienunternehmen für Überwachungstechnologie, berichtet seit 2017 über Backdoor-Exploits von HikVision.[197] Im Jahr 2021 veröffentlichte das Unternehmen selbst einen Sicherheitshinweis über eine „Befehlsinjektionsschwachstelle, die es Bedrohungsakteuren ermöglichen könnte, die vollständige Kontrolle über kompromittierte Geräte zu erlangen", die von einem externen Cybersicherheitsforscher entdeckt wurde.[198] Die Verwendung solcher Geräte birgt mit Sicherheit ein hohes Risiko für die von der Öffentlichkeit gesammelten Daten – sie könnten direkt nach Peking oder an andere Hacker gehen.

6.3.3. Produkte und Leistungen für verbrauchende Personen

Die Kategorie von Produkten und Leistungen, die wohl die größte Menge an Daten sammeln und direkt nach China weiterleiten können, sind Verbraucherprodukte, die sich in den Händen von Millionen von usern weltweit befinden, die damit täglich Transaktionen durchführen: Smartphones von Anbietern wie Xiaomi und natürlich Huawei

188 Zeyi Yang. „The world's biggest surveillance company you've never heard of." MIT Technology Review. 22. Juni 2022. https://www.technologyreview.com/2022/06/22/1054586/HikVision-worlds-biggest-surveillance-company/

189 Joel Griffin. „Congress passes bill banning new FCC equipment authorizations for HikVision, Dahua and others." SecurityInfoWatch.com. 29. Oktober 2021. https://www.securityinfowatch.com/video-surveillance/article/21243600/congress-passes-bill-banning-new-fcc-equipment-authorizations-for-HikVision-dahua-and-others

190 „List of Equipment and Services Covered By Section 2 of The Secure Networks Act." Federal Communications Commission. https://www.fcc.gov/supplychain/coveredlist

191 Demetri Sevastopulo. „US moves towards imposing sanctions on Chinese tech group HikVision." Financial Times. 03. Mai 2022. https://www.ft.com/content/7bc70335-138e-4f56-afe1-ae4383eefb2b

192 Chris Vallance. „MPs call for UK ban on two Chinese CCTV firms." 04. Juli 2022. https://www.bbc.com/news/technology-62003253

193 „Who's Watching You? The dominance of Chinese state-owned CCTVs in the UK." Big Brother Watch. 07. Februar 2022. https://bigbrotherwatch.org.uk/wp-content/uploads/2022/02/Whos-Watching-You_The-dominance-of-Chinese-state-owned-CCTV-in-the-UK-17746.pdf

194 „Eyes everywhere: China's surveillance equipment spreads worldwide." Nikkei Asia. 16. Februar 2022. https://asia.nikkei.com/Spotlight/The-age-of-Great-China/Eyes-everywhere-China-s-surveillance-equipment-spreads-worldwide

195 Ryan Morrison. „UK government ban for Chinese HikVision CCTV cameras." TechMonitor. 25. November 2022. https://techmonitor.ai/government-computing/HikVision-ban-uk-government-oliver-dowden

196 Diane Bartz und Alexandra Alper. „U.S. bans new Huawei, ZTE equipment sales, citing national security risk." Reuters. 30. November 2022.https://www.reuters.com/business/media-telecom/us-fcc-bans-equipment-sales-imports-zte-huawei-over-national-security-risk-2022-11-25/

197 „HikVision Backdoor Exploit." IPVM. 03. September 2017. https://ipvm.com/reports/hik-exploit

198 Benjamin David. „Cybersecurity Vulnerability Could Affected Millions of HikVision Cameras." 24. September 2021. https://www.infosecurity-magazine.com/news/vulnerability-HikVision-cameras

und seiner neuen Marke HONOR sowie Finanz-, Transport- und andere beliebte Plattformen wie AliPay, Didi, und andere, die überall auf der Welt genutzt werden.

Stand Juli 2022 ist Xiaomi mit einem Marktanteil von 12,86 Prozent das drittgrößte Smartphone-Unternehmen der Welt, lediglich hinter Samsung und Apple und vor den anderen chinesischen Rivalen Huawei, Oppo und Vivo. Die vier chinesischen Marken kommen zusammen auf 28,91 Prozent des weltweiten Marktanteils.[199] Viele der chinesischen Smartphones sind aufgrund ihrer günstigen Preise in Entwicklungsländern äußerst beliebt. Doch Xiaomi ist bereits 2014 wegen seiner Datenschutzpraxis in die Kritik geraten. Damals deckte die Informationssicherheitsfirma F-Secure auf, dass das Unternehmen Daten aus den Cloud-Adressbüchern und Messaging-Diensten seiner User außerhalb des chinesischen Festlands sammelte und die Daten ohne Genehmigung an Server in Peking übertrug.[200] F-Secure entschuldigte sich schnell und behauptete, dass es den Austausch und die Speicherung der internationalen Userdaten außerhalb Chinas verlegen würde.[201] Doch die Vorwürfe gegen Xiaomi wegen unzulässiger Datenübertragungen hielten an.

Ein Bericht von Forbes aus dem Jahr 2020 enthüllte, dass Browser auf Xiaomi-Telefonen heimlich Browsing-Daten von Usern sammelten, selbst wenn Nutzende sie auf den privaten oder „Inkognito"-Modus einstellten.[202] Nachdem das Unternehmen dies zunächst als Missverständnis abgetan hatte, stellte es umgehend ein Browser-Update zur Verfügung, das den Usern ermöglichte, die Datenerfassung im Inkognito-Modus zu deaktivieren. Allerdings hätten solche Daten gar nicht erst gesammelt werden dürfen.[203]

Auch globale Dienstleistungsplattformen wie AliPay und Didi haben sich schnell auf dem globalen Markt ausgebreitet, sowohl für chinesische Reisende im Ausland als auch für lokale User in anderen Ländern. Seit 2017 hat Didi seine Dienste auf Brasilien, Mexiko, Australien, Japan, Chile, Kolumbien, Costa Rica, Russland, Neuseeland, Südafrika, Kasachstan und Ägypten ausgeweitet und ist strategische Partnerschaften mit Unternehmen in Afrika und Europa eingegangen. (Im Jahr 2022 zog sich das Unternehmen unter Hinweis auf Marktprobleme aus Kasachstan und Südafrika zurück.)[204] In einigen dieser Länder werden die Dienste von Didi möglicherweise nicht einmal unter der eigenen Marke angeboten, wie dies in Brasilien und anderen lateinamerikanischen Ländern der Fall war, wo Didi unter dem Namen „99" operierte.[205]

Als Chinas Cyberspace-Verwaltung Didi schließlich im Juli 2021 im Rahmen ihrer abschließenden Untersuchung bestrafte, stellte sie fest, dass Didi seit Juni 2015 unter anderem fast zwölf Millionen Screenshots und 107 Millionen Gesichtserkennungsdaten von Passagieren sowie mehr als 167 Millionen Datensätze ihrer Standortdaten illegal gesammelt hatte.[206] Diese Zahlen betrafen wahrscheinlich nur die Vorfälle innerhalb Chinas. Doch wenn solche Verstöße innerhalb Chinas begangen wurden, sollte man erwarten, dass ähnliche Praktiken auch in anderen Ländern, in denen Didi tätig ist, stattfinden, insbesondere in Märkten mit schwächeren Datenschutzregelungen. Während frühere Didi-Führungskräfte betonten, dass das Unternehmen „alle inländischen Userdaten auf Servern in China" speichert und dass es unmöglich ist, Daten in die USA weiterzugeben, gab es nie eine offizielle Stellungnahme dazu, ob Daten in die andere Richtung, nämlich von außen nach China, gesendet würden.[207]

Expertinnen und Experten haben auch auf ähnliche Probleme bei anderen beliebten chinesischen Apps wie AliPay und WeChat Pay hingewiesen, den beiden führenden mobilen Zahlungs-Apps, die von Chinesinnen und Chinesen sowohl im Inland als auch international, und zunehmend auch von ausländischen Usern außerhalb Chinas verwendet werden. Die Forscherinnen und Forscher weisen darauf hin, dass die Eigentümerinnen und Eigentümer dieser Apps, Ant Group und Tencent, von der chinesischen Regierung kontrolliert werden und mit ihr zusammenarbeiten. Sie haben keine andere Wahl – die Unternehmen sind per Gesetz verpflichtet, den Anordnungen der chinesischen Regierung in vollem Umfang Folge zu leisten. Nach Informationen, die über den App Store von Apple bereitgestellt wurden, sammeln AliPay und WeChat Pay in großem Umfang Informationen von ihren Usern, einschließlich Gesundheits- und Fitnessdaten, Standort, Kontakte, Userinhalte, Such- und Browserverläufe und vieles mehr. Obwohl dies nicht nur bei chinesischen Apps der Fall ist und viele westliche Apps dasselbe tun, hindert nichts diese chinesischen Unternehmen daran, der Aufforderung Pekings nachzukommen und die gesammelten Daten zu übergeben. Wie ein Rechtsexperte es ausdrückte: „Chinas Vorgehen vermittelt: 'Wenn eure Systeme chinesische Bürgerinnen und Bürger betreffen, haben wir das Recht, eure Systeme zu überprüfen'."[208]

Darüber hinaus gibt es Berichte, dass China seine Regeln zur Offenlegung von Software-Schwachstellen dazu nutzt, potenziell gefährliche Zero-Day-Schwachstellen für seine

199 „Mobile Vendor Market Share Worldwide - July 2022." Statcounter GlobeStats. https://gs.statcounter.com/vendor-market-share/mobile/worldwide/

200 Gerry Shih. „China smartphone maker Xiaomi apologize for unauthorized data access." Reuters. 11. August 2014. https://www.reuters.com/article/us-china-mobilephone-xiaomi/china-smartphone-maker-xiaomi-apologizes-for-unauthorized-data-access-idUKKBN0GB0WY20140811

201 Liam Tung. „Xiaomi moving international user data and cloud services out of Beijing." ZDNet. 23. Oktober 2014. https://www.zdnet.com/article/xiaomi-moving-international-user-data-and-cloud-services-out-of-beijing/

202 „Xiaomi accused of sending 'private' user data to China; company denies claims." The Indian Express. 03. Mai 2020. https://indianexpress.com/article/technology/mobile-tabs/xiaomi-accused-of-secretly-sending-private-user-data-to-china-6389861/

203 Suzana Dalul. „Is selling your privacy for a cheaper phone really a good idea?" Android Authority. 04. Juni 2022. https://www.androidauthority.com/xiaomi-privacy-cheap-phone-1118444/

204 https://en.wikipedia.org/wiki/DiDi#Globalization

205 Ingrid Lunden. „Didi confirms it has acquired 99 in Brazil to expand to Latin America." TechCrunch. 03. Januar 2018. https://techcrunch.com/2018/01/03/didi-confirms-it-has-acquired-99-in-brazil-to-expand-in-latin-america/

206 Zen Soo. „China's Didi Global fined $1.2 billion for data violations." Associated Press. 21. Juli 2022. https://apnews.com/article/technology-china-data-privacy-cheng-wei-d7c76a253e50d5b5aa8218eb1d3cebbd

207 Scott Murdoch und Yilei Sun. „Didi says it stored all China user and roads data in China." Reuters. 03. Juli 2021. https://www.reuters.com/world/china/riding-hailing-giant-didi-says-it-stores-all-china-user-data-china-2021-07-03/

208 Elisabeth Braw. „JPMorgan's Deal With Alipay Will Put the PLA in Your Pocket." Foreign Policy. 12. Oktober 2021. https://foreignpolicy.com/2021/10/12/china-jpmorgan-barclaycard-wechat-alipay-data-intelligence-national-security-threat/

eigenen nachrichtendienstlichen Zwecke auszutesten. Nach den in China geltenden Vorschriften müssen Unternehmen alle gefundenen Schwachstellen innerhalb von zwei Tagen nach ihrer Entdeckung an die Regierung melden und dürfen sie „bei wichtigen nationalen Ereignissen" nicht öffentlich machen.[209] Im Fall des Log4j-Fehlers[210], der wahrscheinlich schwerwiegendsten Java Sicherheitslücke in der Geschichte der Internets, meldete ein Alibaba-Ingenieur, der die Schwachstelle entdeckt hatte, diese zunächst an Apache, die globale gemeinnützige Stiftung, die das Software-Tool verwaltet. Dafür wurde Alibaba bestraft, indem die Regierung eine Cybersicherheits-Partnerschaft mit dem Unternehmen aussetzte.[211] Dabei handelte es sich bei Apache nicht einmal um eine chinesische oder Alibaba-eigene Software, sondern um eine Sicherheitslücke in einer Open-Source-Software außerhalb Chinas. Nichtsdestotrotz betrachtete die chinesische Regierung selbst diese Information als „Geheimnis" Chinas, aus dem einfachen Grund, dass jemand in China sie entdeckt hat.

In den letzten Tagen seiner Amtszeit untersagte Präsident Trump per Erlass chinesischen Dienste wie AliPay, CamScanner, TikTok, QQ Wallet, SHAREit, Tencent QQ, VMate, WeChat, WeChat Pay und WPS Office Geschäfte mit ihren Apps in den USA. Die Verfügung wurde von Präsident Biden bei seinem Amtsantritt widerrufen.[212] Bidens neue Direktive verlangt vermutlich, dass das Handelsministerium prüft, ob Apps, die mit ausländischen Konkurrentinnen und Konkurrenten in Verbindung stehen, ein „inakzeptables Risiko" darstellen. Dieses Risiko wird daran bemessen, ob sie „im Besitz von Personen sind, von diesen kontrolliert werden oder von Personen verwaltet werden, die militärische oder nachrichtendienstliche Aktivitäten ausländischer Gegner unterstützen oder in böswillige Cyber-Aktivitäten verwickelt sind, oder ob es sich um Anwendungen handelt, die sensible personenbezogene Daten erfassen".[213]

Zwar war die Trump-Verfügung in der offenen Internetumgebung der USA eher symbolisch als praktikabel, aber es bedarf mehr als nur der Aufhebung des Erlasses. Journalistinnen und Journalisten berichten immer wieder über Apps, Dienste oder Geräte, die täglich Userdaten sammeln und nach China weiterleiten.

6.3.4. Soziale Medien: TikTok

Zu behaupten, TikTok habe die sozialen Medien verändert, ist sicherlich eine Untertreibung. Die App zum Teilen von Kurzvideos ist die internationale Version der chinesischen App Douyin des Mutterunternehmens ByteDance, die 2016 auf den Markt gebracht wurde. Sie hat in der kurzen Zeit seit ihrer Einführung 2017 insbesondere die jüngere Generation auf der ganzen Welt im Sturm erobert. Allerdings sind zahlreiche Probleme mit TikTok aufgetaucht, wie Abhängigkeit, Zensur, frauenfeindliche Inhalte, Diskriminierung und Desinformation. Und die Liste wächst stets weiter.

Das Problem von TikTok für den Westen ist nicht nur, dass es sich um eine Big-Tech-Plattform handelt, bei der der Profit an erster Stelle steht. Die App ist, genau wie unsere vorherigen Beispiele, ein Tochterunternehmen eines chinesischen Unternehmens, das verpflichtet ist, chinesische Gesetze zu befolgen, obwohl TikTok selbst behauptet, dass es völlig unabhängig von seiner Muttergesellschaft operiert.

Dokumente, die 2019 den Medien zugespielt wurden, legen nahe, dass TikTok seine globalen Moderatoren angewiesen hat, Videos zu zensieren, die politische Themen erwähnen, die Peking als problematisch erachtet. Die sind z. B. die religiöse Gruppe Falun Gong, der Platz des Himmlischen Friedens, Tibet oder Xinjiang, wobei der Großteil der verbotenen Inhalte in eine Kategorie fällt, die intern als „Hassrede und Religion" bezeichnet wird. Verbotenes Material kann von der Seite gelöscht und der Usern vom Dienst ausgeschlossen werden. Bei leichteren Verstößen kann der Inhalt als „nur für sich selbst sichtbar" markiert werden, wobei der Inhalt auf der eigenen Seite verbleibt, aber nicht an andere User weitergeleitet wird.[214] Aber nicht nur das: Die Zensoren von TikTok haben offenbar weltweit die Sensibilität der chinesischen Zensoren für gesellschaftlich umstrittene Themen übernommen. Einige User haben berichtet, dass sogar Phrasen, die sich auf „Black Lives Matter" beziehen, als unangemessen eingestuft wurden.[215]

209 Suzanne Smalley. „China could be reviewing security bugs before tech companies issue patches, DHS official says." Cyberscoop. 10. August 2022. https://www.cyberscoop.com/dhs-official-chinese-rules-exploit/

210 https://www.ingenieur.de/technik/fachbereiche/ittk/log4j-sicherheitsluecke-warum-der-fehler-unvermeidbar-war/

211 Zeyi Yang. „Beijing punishes Alibaba for not reporting Log4j loophole quickly enough." Protokoll. 22. Dezember 2021. https://www.protocol.com/bulletins/alibaba-cloud-log4j

212 Campbell Kwan. „Biden revokes Trump-era executive orders that aimed to ban AliPay, TikTok, WeChat." ZDNet. 09. Juni 2021. https://www.zdnet.com/article/us-president-biden-revokes-trump-era-executive-orders-that-banned-alipay-tiktok-wechat/

213 „Fact Sheet: Executive Order Protecting Americans' Sensitive Data from Foreign Adversaries." Das Weiße Haus. 09. Juni 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/09/fact-sheet-executive-order-protecting-americans-sensitive-data-from-foreign-adversaries/

214 Alex Hern. „Revealed: how TikTok censors videos that do not please Beijing." The Guardian. 25. September 2019. https://www.theguardian.com/technology/2019/sep/25/revealed-how-tiktok-censors-videos-that-do-not-please-beijing

215 Abby Ohlheiser. „Welcome to TikTok's endless cycle of censorship and mistakes." MIT Technology Review. 13. Juli 2021. https://www.technologyreview.com/2021/07/13/1028401/tiktok-censorship-mistakes-glitches-apologies-endless-cycle/

TikTok hat das gleiche Problem wie die zuvor erwähnten chinesischen Apps: Exzessives Sammeln von Daten und unerlaubte Übertragungen. Das australisch-amerikanische Sicherheitsunternehmen Internet 2.0 berichtete im Juli 2022 über die exzessive Datensammlung von TikTok, einschließlich des Zugriffs auf Kontaktlisten, Kalender und Festplatten und einer stündlichen Geolokalisierung. Verweigert ein User seine Zustimmung zur Datenerfassung und -weitergabe, fragt TikTok immer wieder nach, bis der User einwilligt. Vor allem aber haben die Untersuchungen ergeben, dass die Daten durch den Einsatz von Tracking-Bots durchgängig auf nicht identifizierte Server in China geolokalisiert werden.[216]

Nach einem öffentlichen Aufschrei und einer offiziellen Anfrage des Schattenministers für Cybersicherheit, James Paterson, gab TikTok Australien schließlich zu, dass ausgewählte Mitarbeitende in China auf die Daten australischer User zugreifen können, „um ihre Arbeit zu erledigen". Paterson wies darauf hin, dass TikTok Australien seiner eigenen früheren Zusicherung widersprochen hat, dass die Daten in den USA und Singapur gespeichert würden statt in China. Wie auch andere Expertinnen und Experten feststellten, wären alle von TikTok in China gespeicherten Daten nach chinesischem Recht für die chinesische Regierung zugänglich.[217]

Ein Untersuchungsbericht von Forbes aus dem Jahr 2022 stellte bei der Untersuchung von ByteDance-Profilen von Mitarbeitenden auf LinkedIn außerdem fest, dass Hunderte von ihnen zuvor für verschiedene staatliche Medien in China gearbeitet hatten. Sie besetzen nun mittlere bis leitende Positionen bei ByteDance in den Bereichen Inhaltspartnerschaft, Strategie, Politik, Monetarisierung und Medienkooperation, was die Befürchtung weiter schürt, dass die User von TikTok einer direkten Manipulation durch Peking ausgesetzt sind.[218]

Trotz all dieser Probleme gehörte TikTok zu den Apps, deren Verbot Biden 2021 nach Trumps Erlass wieder aufhob. In ähnlicher Weise wurde auch Trumps frühere Anordnung vom August 2020, TikTok an einen US-Eigentümer zu veräußern, von der Biden-Administration ausgesetzt.[219] Scheinbar ist es den US-Gesetzgebern und der Regierung wichtiger, ihren eigenen amerikanischen Social Media- und Big Tech-Firmen das Leben schwer zu machen als chinesischen Plattformbetreibern, die möglicherweise ein größeres Risiko für die nationale Sicherheit darstellen.

6.3.5. Die Antwort der USA: Das Clean Network

Als die Clean-Network-Initiative im August 2020 vom republikanischen US-Außenminister Mike Pompeo angekündigt wurde, beschrieb er sie als eine Maßnahme gegen „langfristige Bedrohungen des Datenschutzes, der Sicherheit, der Menschenrechte und der vertrauensvollen Zusammenarbeit". Da das Programm anfänglich von führenden demokratischen Kongressabgeordneten unterstützt wurde, war es weitgehend überparteilich.[220]

Die meisten Menschen wussten, dass die Initiative Huawei- und ZTE-Geräte aus den Telekommunikationsnetzen demokratischer Länder fernhalten sollte, wobei sich angeblich mehr als sechzig Länder angeschlossen hatten. Aber die Regelung war so konzipiert, dass sie weit mehr als nur 5G-Backbone- und Backend-Telekommunikationsgeräte abdeckte.

In der Tat wurden sechs Arbeitsbereiche definiert:[221]

(1) Clean Carrier – um sicherzustellen, dass kritische chinesische Anbieter nicht mit US-Telekommunikationsnetzen verbunden sind.

(2) Clean Apps – um zu verhindern, dass nicht vertrauenswürdige chinesische Smartphone-Hersteller vertrauenswürdige Apps vorinstallieren oder in ihren App-Stores zum Download bereitstellen. Vertrauenswürdige App-Hersteller aus den USA und anderen Ländern sollten im Gegenzug ihre Apps aus dem Huawei-Store und anderen chinesischen App-Stores entfernen.[222]

(3) Clean Store – Entfernung nicht vertrauenswürdiger Apps aus US-App-Stores. In diesem Zusammenhang erließ Trump zwei Anordnungen gegen TikTok und WeChat, die später von der Biden-Administration aufgehoben wurden.

(4) Clean Cloud – um zu verhindern, dass die sensibelsten personenbezogenen Daten von US-Bürgerinnen und Bürgern und das wertvollste geistige Eigentum von Unternehmen in chinesischen Clouds wie Alibaba, Baidu, China Mobile, China Telecom und Tencent gespeichert und verarbeitet werden.

(5) Clean Cable – um sicherzustellen, dass die Unterseekabel, die die USA mit dem Rest der Welt verbinden, nicht für nachrichtendienstliche Zwecke durch die VR China „im großen Stil" unterwandert werden, und dass neue Unterseekabel, die weltweit mit ausländischen Partnern gebaut werden, nicht vertrauenswürdige Anbieter ausschließen.

216 Rafqa Touma. „TikTok has been accused of 'aggressive' data harvesting. Is your information at risk?" The Guardian. 19. Juli 2022. https://www.theguardian.com/technology/2022/jul/19/tiktok-has-been-accused-of-aggressive-data-harvesting-is-your-information-at-risk

217 Jake Evans. „TikTok admits Australian data can be accessed in China, prompting warnings app may be compromised." ABC News. https://www.abc.net.au/news/2022-07-13/tiktok-admits-australian-data-accessible-in-china/101233320

218 Mia Sato. „Go read this report on ByteDance employees with ties to Chinese state media." The Verge. https://www.theverge.com/2022/8/11/23301724/go-read-this-bytedance-tiktok-employees-chinese-state-media-propaganda-connections

219 Natalie Gagliordi. „Oracle, Walmart deal for TikTok shelved indefinitely, reports WSJ." ZDNet. 10. Februar 2021. https://www.zdnet.com/article/oracle-walmart-deal-for-tiktok-shelved-indefinitely-reports-wsj/

220 Michael Mink. „How the Clean Network Alliance of Democracies Turned the Tide on Huawei in 5G." Life & News. 02. Dezember 2020. https://www.lifeandnews.com/articles/how-the-clean-network-alliance-of-democracies-turned-the-tide-on-huawei-in-5g/

221 „The Clean Network Safeguards America's Assets". US- Außenministerium, Datenblatt. 11. August 2020. https://2017-2021.state.gov/the-clean-network-safeguards-americas-assets/index.html

222 Campbell Kwan. „Biden revokes Trump-era executive orders that aimed to ban AliPay, TikTok, WeChat." ZDNet. 09. Juni 2021. https://www.zdnet.com/article/us-president-biden-revokes-trump-era-executive-orders-that-banned-alipay-tiktok-wechat/

(6) Clean Path – Schutz von Sprache und Daten über 5G-Netzwerke, die in diplomatische Einrichtungen der USA im In- und Ausland gelangen und diese verlassen, indem sichergestellt wird, dass ein durchgängiger Kommunikationspfad zur Verfügung steht, der keine Übertragungs-, Steuerungs-, Rechen- oder Speichergeräte von nicht vertrauenswürdigen IT-Anbietern wie Huawei und ZTE verwendet. Dieser Teil untermauert den ursprünglichen Fokus auf das Verbot von Huawei und ZTE aus den 5G-Netzen der Partnerländer.

Sicherlich sind einige Teile der Clean-Network-Initiative erfolgreicher als andere, wie z. B. das Verbot von unsicherer Netzwerkausrüstung von Unternehmen wie Huawei in Partnerländern. Aber in einigen Fällen wurde dies nicht ohne Debatte und weitere Überlegungen erreicht. In Deutschland zum Beispiel regte sich zunächst Widerstand bei den Telekommunikationsbetreibenden und der Regierung. Dies war auf eine Reihe von Faktoren zurückzuführen, unter anderem auf die Abhängigkeit von Huawei bei den bisherigen 4G-Netzsystemen des Landes und die potenziell hohen Kosten eines Wechsels. Ein weiteres Problem war, dass in Deutschland und Europa keine nennenswerte unabhängige Debatte zu diesem Thema stattfand, was das Vorhaben zu einer fast ausschließlich von den USA gesteuerten Angelegenheit machte. Um seine Abhängigkeit von chinesischen Anbietern zu verringern, sollte Europa gleichgesinnten Partnern zusammenarbeiten und langfristige Anstrengungen unternehmen, die seine eigenen Technologieanbieter stärken und einen früheren Vorsprung bei der Übernahme künftiger offener Technologiestandards erzielen.[223]

Was die anderen Elemente der Clean-Network-Initiative betrifft, so entspricht Clean Cable lediglich der bereits bestehenden Politik der Vereinigten Staaten: Chinesische Partner sind von der Entwicklung von Unterseekabeln, die in die USA führen, ausgeschlossen, und Kabel, die in die USA führen, dürfen nicht in chinesischen Städten wie Hongkong enden.[224] Die US-Behörden können dies durch Lizenzanforderungen der FCC und anderer Behörden kontrollieren. Die Auswirkungen dieser Entscheidungen sind bereits zu spüren: Regionale ostasiatische Telekommunikations- und Rechenzentrumsknotenpunkte verlagern sich von Hongkong an andere Standorte wie die Philippinen, Taiwan, Korea und andere, ganz zu schweigen von den bestehenden Knotenpunkten in Singapur und Japan.[225] Diese Aspekte der Clean Network-Initiative wurden von der Regierung Biden im Wesentlichen beibehalten.

Andererseits waren chinesische Cloud-Dienste in den USA ohnehin noch nie wettbewerbsfähig oder weit verbreitet, sodass die Zielsetzung der Clean Cloud leicht zu erreichen ist. Die Bereiche, die große Telekommunikationsunternehmen oder Cloud-Service-Anbieter betreffen, lassen sich relativ leicht umsetzen, aber die Verwirklichung in Bezug auf Apps und App-Stores erweist sich als schwieriger. Wie bereits erwähnt, waren die Anordnungen von Trump gegen TikTok und WeChat im offenen Marktumfeld der USA schwer zu implementieren. Es besteht zudem das Risiko, dass die Anordnungen vor Gericht angefochten werden könnten. Außerdem hat TikTok bereits fast achtzig Millionen User in den USA[226], und WeChat verzeichnete 2021 in den USA über 1,7 Millionen Downloads.[227] Damit sind die USA nach China der zweitgrößte Markt für die Super-App. Jeder Versuch, diese Apps gewaltsam vom US-Markt zu entfernen, wird zweifellos auf heftige Gegenreaktionen von Usern, Werbetreibenden und Entwicklern stoßen, die von den Apps abhängig sind, um Einnahmen zu erzielen.

Auch wenn ein vollständiges Verbot der genannten Apps für die USA und andere Demokratien vielleicht nicht sofort umzusetzen ist, müssen gezieltere Regelungen zur Kontrolle von Fehlinformationen, Desinformation, ausländischer Einmischung, Wahlbeeinflussung und anderen Schäden auf diesen Plattformen in Betracht gezogen und dringend angegangen werden.

Wie hat China auf das Clean Network reagiert? Im September 2020 schlug China einen eigenen Rahmen für die globale Datensicherheit und den digitalen Handel vor, die „Global Data Security Initiative“. Mit der Betonung auf „Multilateralismus, sichere Entwicklung, Fairness und Gerechtigkeit“ definiert die Initiative im Großen und Ganzen Grundsätze der Zusammenarbeit in Bezug auf Daten- und Cybersicherheit. China nutzt die Initiative, um befreundete Länder wie Russland, Tansania, Pakistan, Ecuador, einige Mitglieder der Arabischen Liga und der ASEAN für die Bildung einer eigenen losen Daten- und Technologie-Allianz zu gewinnen.[228]

223 Thorsten Benner. „Seven Lessons From the German 5G Debate.“ Global Public Policy Institute. 30. Dezember 2021. https://gppi.net/2021/12/30/seven-lessons-from-the-german-5g-debate

224 Shermaine Yung. „Trans-Pacific Cable Chaos, Shifting Asian Hubs.“ TeleGeography BLOG. 20. Mai 2021. https://blog.telegeography.com/trans-pacific-cables-asian-hubs-plcn-status

225 Charles Mok. „Taiwan can be East Asia<2>'s new internet and data hub.“ CommonWealth Magazine. 05. Mai 2022. https://english.cw.com.tw/article/article.action?id=3219

226 “Number of TikTok users in the United States from 2020 to 2023.” Statista. 28. Januar 2022. https://www.statista.com/statistics/1100836/number-of-us-tiktok-users/

227 „Leading markets of Tencent's WeChat in 2021, based on app downloads.“ Statista. 07. Februar 2022. https://www.statista.com/statistics/1287237/tencent-wechat-app-downloads-by-country/

228 Chaeri Park. „Knowledge Base: China's 'Global Data Security Initiative“ (全球数据安全倡议). DigiChina. 31. März 2022. https://digichina.stanford.edu/work/knowledge-base-chinas-global-data-security-initiative/

6.4. Internet-Standards und -Governance treffen auf Außenpolitik

6.4.1. Technische Standardsetzung: Von WAPI zu New IP

China weiß, wie wichtig es ist, Einfluss auf die globale Standardsetzung zu nehmen – erstens, um die heimische Industrie auf dem internationalen Markt voranzubringen, und zweitens, um wissenschaftliche Forschung zu fördern und so den Markt in eine für das Land günstige Richtung zu lenken. Auf diese Weise werden auch Elemente der technisch-autoritären Kontrollphilosophie der KPCh ihren Weg in die globalen Standards finden.

Bereits 2003 versuchten die chinesischen Behörden, den heimischen Markt zu nutzen, um einen „chinesischen nationalen WLAN-Standard" durchzusetzen, der zusätzlich zu den von den globalen Standardisierungsgremien angenommenen WiFi-Standards gelten sollte. Dieser Standard mit der Bezeichnung WAPI (WLAN Authentication and Privacy Infrastructure) sollte ursprünglich bis zum 1. Juni 2003 einseitig und verbindlich in China eingeführt werden. Begründet wurde diese Entscheidung damit, dass damit eine vermeintliche Lücke in der internationalen WLAN-Norm ISO/IEC 8802-11 geschlossen werden sollte. In den ersten Tagen des Beitritts Chinas zur WTO wurde sofort diskutiert, ob dadurch der Marktzugang für ausländische Netzwerkfirmen verwehrt wird. Um WAPI-kompatible Produkte für den chinesischen Markt zu produzieren, wären ausländische Unternehmen höchstwahrscheinlich gezwungen gewesen, mit einem der wenigen chinesischen Unternehmen zusammenzuarbeiten, die Zugang zu dem Standard hatten.

Im April 2003 erzielten die USA und China eine Vereinbarung, in der China sich bereiterklärte, die WAPI-Anforderungen auf unbestimmte Zeit aufzuschieben.[229] Die USA betrachteten dies seinerzeit als Erfolg. In der Zwischenzeit wiesen chinesische Medien bereits darauf hin, dass die Chinesinnen und Chinesen im Gegenzug für den Aufschub der WAPI-Vereinbarung und das Versprechen, die Durchsetzung der Vorschriften zum Schutz des geistigen Eigentums gegen Piraterie zu verbessern, eine Lockerung der strengen Anforderungen für die Erteilung von Ausfuhrgenehmigungen für US-Hightech-Geräte nach China erhielten.[230]

Die Pattsituation um WAPI hielt mehrere Jahre an. Im Jahr 2006 reichte China bei der ISO-Normungsorganisation einen Antrag auf Anerkennung als internationale Norm ein, der jedoch abgelehnt wurde. Im Jahr 2009 wurde der Antrag erneut eingereicht, aber 2011 zog China den WAPI-Antrag endgültig zurück.

Die WAPI-Saga war eine wichtige Lektion für China, dass der Zeitpunkt für die Einführung verfrüht war. Chinas Markt könnte ein enormer Einflussfaktor werden, aber dem Land fehlte damals ein eigener führender Technologieanbieter mit weltweitem Einfluss. Wären die technischen Standards „aufgesplittet" worden, hätte China mehr zu verlieren als zu gewinnen gehabt, indem beispielsweise seine aufstrebenden einheimischen Technologieunternehmen wie Huawei im globalen Wettbewerb benachteiligt worden wären. Die Behörden erkannten auch, dass es sich stärker an den globalen Normungsgremien beteiligen musste, um bei künftigen Entscheidungen mehr Mitspracherecht zu haben. China versprach, sich Zeit zu lassen und es erneut zu versuchen.

Machen wir einen Zeitsprung in die Gegenwart. China schlägt jetzt aktiv zwei neue und verwandte konzeptionelle Standards vor: New IP und IPv6+. In den letzten zehn Jahren hat China viel mehr Erfahrung mit internationalen Normungsprozessen gesammelt, nationale Verbündete gewonnen und mit Huawei nun einen hochdotierten Unternehmensriesen als Unterstützer.

Im September 2019 reichte Huawei eine Reihe von Vorschlägen bei der Beratungsgruppe für Telekommunikationsnormen des ITU Telecommunication Standardization Sector (ITU-T) ein, um seinen mit China Mobile, China Unicom und der China Academy of Information and Communications Technology entwickelten „New-IP"-Beitrag einzuleiten. Im Januar 2020 reichte Huawei einen „New-IP"-Vorschlag bei der Focus Group on Technologies for Network 2030 der ITU-T ein, die die Anforderungen an ein zukünftiges Netzwerk mit höherem Durchsatz, schnellerer Reaktionsgeschwindigkeit und höheren Anforderungen an die Präzision der Kommunikation erarbeitet hatte. New IP sollte die Lösung sein. Im Juli 2020 änderte Huawei seinen Vorschlag dahingehend, dass der Begriff „New IP" in „Future Vertical Communication Network" geändert werden sollte, mit dem Ziel, "eine Vielzahl von vertikalen Netzen miteinander zu verbinden, von denen jedes mit einem eigenen Protokoll arbeitet", während der Inhalt der Vorschläge gleich blieb. Die Studiengruppen der ITU-T haben im Dezember 2020 beschlossen, den New-IP-Vorschlag bis auf weiteres nicht anzunehmen. Jedoch tauchen Elemente des Vorschlags immer wieder in verschiedenen anderen Studiengruppen auf und halten die Bemühungen am Leben.[231]

Die Bedenken gegen New IP betreffen zwei Aspekte: Die Technologie und den Prozess der Standardisierung. Die Internet Society (ISOC) – eine weltweit führende Organisation der Zivil- und Technologiegesellschaft – wies darauf hin, dass Huawei in seinen Vorschlägen für New IP eine Reihe falscher Behauptungen aufgestellt hat, um seine Prämisse zu untermauern, dass das bestehende Internetprotokoll und seine Architektur vollständig überarbeitet werden müssen. So hat Huawei beispielsweise behaup-

229 Richard Shim, Michael Kanellos, und Evan Hansen. „China, U.S. strike trade agreement." 21. April 2004. https://web.archive.org/web/20050407222112/http://news.zdnet.com/2100-9584_22-5197087.html

230 Charles Mok. „WAPI 內地標準暫緩實行中美貿易爭端得以紓緩." Hong Kong Economic Journal. 29. April 2003. https://charlesmok.blogspot.com/2003/04/wapi.html

231 „Huawei's 'New IP' Proposal - Frequently Asked Questions." Internet Society. 22. Februar 2022. https://www.internetsociety.org/resources/doc/2022/huaweis-new-ip-proposal-faq/

tet, dass die derzeitige Netzwerkumgebung nur aus dem Internet besteht, und dabei eine Fülle von Nicht-Internet-Netzwerken ignoriert, die existieren und gut funktionieren. Huawei hat auch behauptet, dass die gegenwärtigen Netzwerktechnologien nicht angemessen mit heterogenen Netzwerken interagieren können, was technisch nicht stimmt. In der Tat erlaubt das Design des Internets genau die Untervernetzung, die nachweislich eine flexible Vernetzung ermöglicht. Indem Huawei den Fokus auf eine bestimmte Variante des Transmission Control Protocol (TCP) lenkt, behauptet das Unternehmen, das Internet könne keinen extrem hohen Übertragungsdurchsatz bewältigen, und ignoriert dabei die effektive und kontinuierliche Weiterentwicklung der TCP- und IP-Leistung. Eine weitere falsche Behauptung betrifft die Notwendigkeit einer extrem niedrigen Latenzzeit für New IP. Von Kritikerinnen und Kritikern wird diese als „unvereinbar mit den Gesetzen der Physik" verspottet wird, da sie zu überzogenen Geschwindigkeitsangaben führt, die bei genauerer Betrachtung der Zahlen tatsächlich die Lichtgeschwindigkeit übersteigen würden.[232]

Neben diesem unhaltbaren technischen Entwurf weisen die Branchenverbände auf das Hauptproblem von New IP hin: seine mangelnde Kompatibilität mit dem bestehenden Internet. New IP zielt unnötigerweise darauf ab, das gesamte Internet umzugestalten, anstatt den bislang üblichen schrittweisen Ansatz zu verfolgen. Befürworter von New IP behaupteten, dass es den derzeitigen Entwürfen an bestimmten Funktionen fehle. Dagegen argumentierten die Telekommunikationsbetreiber, dass dies nur deshalb der Fall sei, weil einige Funktionen aufgrund mangelnder Geschäftsmöglichkeiten nicht eingeführt worden waren. Die Neugestaltung des gesamten Protokolls wurde als unnötig und nachteilig angesehen, da sie zu einer Aufspaltung des „neuen" und des „alten" Internets führen könnte.[233]

Und es deutet noch mehr auf eine versteckte Agenda hinter New IP hin. Die Internet Corporation for Assigned Names and Numbers (ICANN) – die Multi-Stakeholder-Organisation, die globale Internet-Ressourcen wie Domain-Namen verwaltet – warnt, dass New IP „die Idee einer starken regulatorischen Bindung zwischen einer IP-Adresse und einem User vorantreibt". Wenn sie eingeführt wird, könnte eine „allgegenwärtige Kontrolle" – d.h. Überwachung – viel einfacher werden, da jedes Vermittler-Netzwerkelement vollen Zugriff darauf hat, „welcher Benutzer was tut". In ähnlicher Weise werden auch die Anbieter von Inhalten die Identität von jeder Person kennen, die sich mit ihnen verbindet. Kurz gesagt, das New-IP-Internet würde zu einer großen Überwachungsmaschine. Da die New-IP-Infrastrukturen nicht mit den bestehenden IPv4- und IPv6-Infrastrukturen kompatibel sind, muss ihre Einführung separat und parallel erfolgen, und jede nennenswerte Einführung und Vernetzung wird Jahrzehnte dauern.[234]

In der Zwischenzeit gehen Huawei und China auch strategisch vor die ITU, obwohl die Gerichtsbarkeit der ITU derzeit nicht für das Internet gilt. Internettechnologienormen werden traditionell in einem Multi-Stakeholder-Prozess entwickelt, an dem Gruppen wie die Internet Engineering Task Force (IETF), der Internet Architecture Board (IAB), die Internet Research Task Force (IRTF), das World-Wide Web Consortium, der Berufsverband Institute of Electrical and Electronics Engineers (IEEE) und indirekt auch die Internet Society beteiligt sind, die IETF, IAB und IRTF unterstützt, während die Multi-Stakeholder-ICANN die Nummern und Bezeichnungen für Netzwerkprotokolle zuteilt. Autoritäre Regime wollten der ICANN und den zahlreichen Interessengruppen, zu denen die Industrie, die Zivilgesellschaft, die technische Gemeinschaft, die Wissenschaft und die Verbraucher gehören, schon lange die Kontrolle über die Verwaltung des Internets entziehen und die gesamte Macht über die ITU in die Hände der Regierungen legen.[235]

China ist der Ansicht, dass der Multi-Stakeholder-Ansatz „nicht einseitig sein sollte, und jede Tendenz, die Rolle von Unternehmen und Nichtregierungsorganisationen in den Vordergrund zu stellen, während Regierungen an den Rand gedrängt werden, vermieden werden sollte", wie es in seinem Beitrag zur Zehn-Jahres-Überprüfung des Weltgipfels zur Informationsgesellschaft 2015, einem Multi-Stakeholder-Prozess unter der UN und der ITU, hieß. China forderte, dass die ICANN „internationalisiert" werden sollte – eine Anspielung auf die Tatsache, dass die ICANN amerikanischen Ursprungs ist und somit weiterhin „den USA gehört" – und dass den Vereinten Nationen eine vorrangige Rolle in der Internetpolitik und -verwaltung übertragen werden sollte.

Dies wurde von der Internet-Gemeinschaft nicht begrüßt, wie die ISOC betonte: „Internetprotokolle und -architekturen sollten weiterhin in einem offenen, bottom-up, Multi-Stakeholder-Ansatz entwickelt werden – so wie es die IETF und die IEEE machen – und nicht – so wie bei ITU-T – top-down gesteuert sein."[237]

Für China ist der Prozess, die bestehende Internet-Standardisierung umzukrempeln, offensichtlich genauso wichtig wie der Plan des New IP. Wenn das Gesamtpaket nicht angenommen wird, zerlegen sie es in einzelne Teile, um bestimmte alternative Normungsgremien und Untergremien sowie alternative Zielgruppen anzusprechen, die möglicherweise aufgeschlossener sind. Im Mai 2022 fass-

232 Ibid.
233 „ETNO position paper on the New IP proposal." European Telecommunications Network Operators' Association. 05. November 2020. https://www.etno.eu/library/positionpapers/417-new-ip.html
234 Alain Durand. „New IP." ICANN. 27. Oktober 2020. https://www.icann.org/en/system/files/files/octo-017-27oct20-en.pdf
235 Mark Montgomery und Theo Lebryk. „China's Dystopian 'New IP' Plan Shows Need for Renewed US Commitment to Internet Governance." Just Security. 13. April 2021. https://www.justsecurity.org/75741/chinas-dystopian-new-ip-plan-shows-need-for-renewed-us-commitment-to-internet-governance/
236 James Griffiths. „The Great Firewall of China." Kapitel 20.
237 Elizabeth Drolet. „Proposals at ITU-T for Internet Evolution Raise Serious Concerns; According to ISOC." NANOG. 04. August 2022. https://www.nanog.org/stories/new-ip-proposals-are-a-threat-according-to-isoc/

ten China und Huawei einen neu modifizierten Beschluss zur Einführung von IPv6+, einer verbesserten Version der neuesten Version des IP-Protokolls, IPv6. Trotz der Ähnlichkeit der Funktionen und Philosophien von New IP und IPv6+ behauptet Huawei, dass die beiden unterschiedlich sind und dass IPv6+ genau die Art von natürlicher und schrittweiser Erweiterung von IPv6 ist, an die Standardentwickler gewöhnt sind, und nicht eine neue Architektur wie New IP. Strategisch gesehen hat Huawei auf der Weltkonferenz zur Entwicklung der Telekommunikation, der Konferenz der ITU, in letzter Minute einen Beschluss gefasst, um sich der Aufmerksamkeit des Westens zu entziehen und gleichzeitig an die Unterstützung der Länder des globalen Südens zu appellieren, die bei der Einführung von IPv6 im Rückstand sind und sich angesichts der Investitionen und des Engagements von Huawei für Infrastrukturprojekte von IPv6+ angezogen fühlen könnten.[238]

Chinas Bemühungen, das Internet neu zu definieren, werden fortgesetzt. Sollte dieses Ziel nicht erreicht werden, wird China zumindest versuchen, sein eigenes, überwachungsstaatliches Internet mit seinen autokratischen Verbündeten – mit Stellvertretern wie Huawei und nationalstaatlichen Partnern wie Russland, Iran, Kuba und Nordkorea – abzuspalten. Die versteckte Agenda liegt auf der Hand: Nachdem sich China darüber beschwert hat, dass das Internet eine amerikanische Erfindung ist und immer noch von den USA kontrolliert wird, möchten die Behörden der Zivilgesellschaft, der Wissenschaft, der Wirtschaft und den Usern jegliche Rolle bei der Entscheidungsfindung abnehmen.

Und das gilt nicht nur für das Internet. Zurück im Bereich der Mobilkommunikation, wo die Diskussionen über 6G bereits im Gange sind, hat China „aktuell in vielen Aspekten der drahtlosen 5G-Telekommunikation eine vorteilhafte Position inne, die eine starke Grundlage für weitere Fortschritte bietet". Dies belegen 6G-Entwicklungskennzahlen wie „Patentanmeldungen und reale Implementierungen relevanter Grund- oder Vorläufertechnologien". [239] Die USA und Europa müssen in der Art und Weise, wie sie ihre Ressourcen für 6G priorisieren und ihre Politik darauf ausrichten, aufholen, so wie sie das auch für das zukünftige Internet tun müssen.

Möglicherweise war China vor über zehn Jahren mit der WAPI noch nicht bereit, aber das Land glaubt, dass es jetzt so weit ist. China hat 2018 seine „China Standards 2035" ins Leben gerufen, und seine Normungsverwaltung und die staatliche Verwaltung für Marktregulierung (SAMR) haben 2022 einen Vorschlag zur Stellungnahme veröffentlicht. Dieser wird ein breites Spektrum an vorgeschlagenen Normen abdecken, die sogar für PCs und Server gelten können, was enorme Auswirkungen auf den Markteintritt ausländischer Technologieanbieter haben wird.[240] Der Vorschlag kann auch andere, noch im Entstehen begriffene Technologien abdecken, wie z. B. das Quantencomputing. Die Botschaft, die von den Bemühungen um die nationale und internationale Standardsetzung ausgeht, lautet: „Wir verfügen über unsere Standards, und wir wollen nicht, dass ihr uns eure Produkte verkauft, sondern wir wollen, dass unsere Standards globale Standards werden, damit wir euch unsere Produkte verkaufen können, indem wir die Dinge auf unsere Weise machen."

6.4.2. Internet-Governance und die ITU

Als der russische Präsident Wladimir Putin Peking zur Eröffnungsfeier der Olympischen Winterspiele 2022 besuchte, nur wenige Wochen bevor seine Truppen gewaltsam in die Ukraine einmarschierten, saßen er und der chinesische Präsident Xi Jinping zusammen, um sich gegenseitig grenzenlose Unterstützung anzubieten. Zu den Erklärungen Pekings, in denen die wirtschaftliche, energiepolitische und diplomatische Zusammenarbeit zwischen den beiden Ländern zugesagt wurde, gehörte auch das Versprechen, die „Internationalisierung der Internetverwaltung" und die „Gleichberechtigung der Länder bei der Regulierung des World Wide Web" zu unterstützen. Die beiden Länder versprachen, „die bilaterale Zusammenarbeit im Bereich der internationalen Informationssicherheit zu vertiefen", erklärten ihre Unterstützung für eine „internationale Konvention zur Bekämpfung der Nutzung von Informationstechnologien für kriminelle Zwecke" und sprachen sich für eine stärkere Beteiligung an der ITU aus.[241]

Die beiden Länder teilen gemeinsame Werte in Bezug auf das Internet – Überwachung, Zensur und totale Kontrolle.[242] Bei den Olympischen Winterspielen in Peking konnten Athletinnen und Athleten sowie Journalistinnen und Journalisten nur an bestimmten Punkten oder in bestimmten Hotels auf das „freie" Internet zugreifen. Die mobile App, die für alle Teilnehmenden vorgeschrieben war, um die Dienste der Veranstaltung in Anspruch zu nehmen, enthielt nach den Feststellungen der ermittelnden Personen von Citizen Lab so viele Sicherheitslücken, dass sie als trojanisches Pferd in jedermanns Tasche fungieren konnte, um sich heimlich Daten zunutze zu machen.[243]

Der Weg Russlands zur Internetzensur verlief jedoch etwas anders als der Chinas. Das Land war anfangs wesentlich offener, und Journalistinnen und Journalisten kommentierten sogar, dass „das Internet der freieste Bereich

238 Luca Bertuzzi. „China rebrands proposal on internet governance, targeting developing countries." Euractiv.com. 05. Juni 2022. https://www.euractiv.com/section/digital/news/china-rebrands-proposal-on-internet-governance-targeting-developing-countries/

239 John Lee und Meia Nouwens. „Strategic Settings for 6G: Pathways for China and the US." IISS. 12. August 2022. https://www.iiss.org/blogs/research-paper/2022/08/strategic-settings-for-6g-pathways-for-china-and-the-us

240 Shunsuke Tabeta. „China takes wider target at foreign tech with national standards plan." Nikkei Asia. 06. Juli 2022. https://asia.nikkei.com/Business/Technology/China-takes-wider-aim-at-foreign-tech-with-national-standards-plan

241 „Russia and China call for internationalization of Internet governance - statement." Tass. 04. Februar 2022. https://tass.com/economy/1398177

242 Charles Mok. „China and Russia Want to Rule the Global Internet." The Diplomat. 22. Februar 2022. https://thediplomat.com/2022/02/china-and-russia-want-to-rule-the-global-internet/

243 Liza Lin. „Official Beijing 2022 Olympics Mobile App Is Marred by Security Flaws, Researchers Say." The Wall Street Journal. 19. Januar 2022. https://www.wsj.com/articles/official-beijing-2022-olympics-mobile-app-is-marred-by-security-flaws-researchers-say-11642511957

der Medien in Russland ist, während fast das gesamte Fernsehen und viele Zeitungen unter formeller oder inoffizieller staatlicher Kontrolle stehen."[244] Doch im Zuge der innenpolitischen Unruhen und der Kriege im Ausland haben die russischen Behörden nach und nach mehr Zensurmaßnahmen im Internet ergriffen. Im Jahr 2021 gelang es den russischen Behörden, Apple und Google dazu zu bewegen, eine Wahl-App des führenden Dissidenten Alexej Nawalny aus ihren App-Stores zu entfernen. Außerdem verstärkten sie ihre Bemühungen, die Nutzung von Verschlüsselungsprogrammen wie dem Tor-Browser und VPN-Diensten zu unterbinden. Human Rights Watch bezeichnete daher das Jahr 2021 als „das Jahr der Verschärfung der Internetzensur" in Russland.[245]

Das Zentralkomitee der KPCh und der Staatsrat Chinas veröffentlichten im November 2021 die National Standardization Development Outline, in der sie ihren Plan für „China Standards 2035" darlegten.[246] Dafür brauchte China natürlich die Unterstützung Russlands, um die „chinesischen Standards" weltweit zu verbreiten. Russland wiederum brauchte China im September 2022 zur Unterstützung von Rashid Ismailov,[247] Russlands stellvertretendem Minister für Telekommunikation und Massenkommunikation und Kandidat des Landes bei der Wahl zum Generalsekretär der ITU, der gegen eine Amerikanerin antrat, Doreen Bogdan-Martin, Direktorin des ITU-Büros für Telekommunikationsentwicklung.[248] Die Wahl war ein Kräftemessen um die künftige Verwaltung von Telekommunikations- und Internetstandards. Schließlich wurde[249] Bogdan-Martin mit einem deutlichen Vorsprung von 139 zu 25 Stimmen gewählt.[250]

6.4.3. Two Futures of the Internet?

Am 9. und 10. Dezember 2021 veranstaltete das Weiße Haus das erste Gipfeltreffen für Demokratie, an dem Hunderte von Regierungen, führenden Vertreterinnen und Vertreter der Zivilgesellschaft und der Wirtschaft teilnahmen, „um die Herausforderungen und Chancen zu erörtern, denen sich Demokratien im 21. Jahrhundert zu diskutieren.[251] Aufgrund der anhaltenden COVID-19-Pandemie handelte es sich bei der Veranstaltung eher um ein großes Webinar als um eine physische Zusammenkunft. Als das Außenministerium in den Monaten zuvor das Programm ausarbeitete, sollte einer der Punkte die Bildung einer Koalition von Demokratien sein, die eine Vision für ein freies und offenes Internet verfolgen. Die Allianz für die Zukunft des Internets wurde von Peter Harrell, Senior Director für internationale Wirtschaft und Wettbewerbsfähigkeit im Nationalen Sicherheitsrat, und Tim Wu, Sonderassistent des Präsidenten für Technologie und Wettbewerbspolitik, angeführt.

Der Plan stieß jedoch auf beträchtliche Skepsis und Gegenreaktionen, insbesondere seitens der Zivilgesellschaft und der Verfechter digitaler Rechte. Zum einen sollte die Allianz eine Gruppe „gleichgesinnter Länder" dazu verpflichten, spezifische Verpflichtungen in den Bereichen Cybersicherheit, Datenschutz, Datentransfer und anderen Bereichen einzugehen, die sich mit sensiblen Politikbereichen von der nationalen Sicherheit bis zum Handel überschnitten. Jedoch wurden auch Bedenken geäußert, dass die Bemühungen den Fokus auf demokratische Werte, Internetfreiheit und Menschenrechte in den Hintergrund drängen und zu einem bloßen „Anti-China-Club" reduziert werden könnten.[252] Einige Nichtregierungsgruppen befürchteten, dass die Allianz durch die Konsolidierung der „freien Welt" das Internet weiter zersplittern würde, anstatt es zu schützen, und sich damit von den Internet Usern in autoritären Ländern entfernen würde. In letzter Minute wurde der Start der Allianz verschoben.[253]

Vier Monate später wurde die Allianz schließlich in eine Erklärung umgewandelt. Am 28. April 2022 gab das Weiße Haus eine Erklärung für die Zukunft des Internets bekannt, die von den USA und sechzig globalen Partnern unterzeichnet wurde. Die Unterzeichner wurden als „Partner" und nicht als Länder bezeichnet, wahrscheinlich um die wichtige Einbeziehung Taiwans zu berücksichtigen. Das Weiße Haus bezeichnete die Erklärung als politisches Bekenntnis der Partner, „ein einheitliches globales Internet zu fördern – eines, das wirklich offen ist und den Wettbewerb, den Schutz der Privatsphäre und die Achtung der Menschenrechte gewährleistet". Zu den Grundsätzen gehören der Schutz der Menschenrechte und der Grundfreiheiten für alle, die Förderung des freien Informationsflusses, integrative und erschwingliche Konnektivität für alle, die Förderung des Vertrauens in globale digitale Ökosysteme durch den Schutz der Privatsphäre sowie der Schutz und die Stärkung des „Multi-Stakeholder-Ansatzes für die Verwaltung".

244 „Russian prosecutors eye Internet censorship." Agence France-Presse. 23. April 2008. https://archive.ph/20140727020225/http://newsinfo.inquirer.net/breaking-news/infotech/view/20080423-132253/Russian-prosecutors-eye-Internet-censorship#selection-2971.0-2971.154

245 „Russia: Year of Doubling Down on Internet Censorship." Human Rights Watch. 24. Dezember 2021. https://www.hrw.org/news/2021/12/24/russia-year-doubling-down-internet-censorship

246 Patrick Lazada, Tim Ruhlig und Helen Toner. „Chinese Involvement in International Technical Standards: A DigiChina Forum." 06. Dezember 2021. https://digichina.stanford.edu/work/chinese-involvement-in-international-technical-standards-a-digichina-forum/

247 Rashid Ismailov. „Bio." ITU. https://www.itu.int/en/council/2018/Pages/chairman.aspx

248 Fiona Alexander. „Behind the Race to Run the UN's Internet Agency." CEPA. 14. Juli 2022. https://cepa.org/behind-the-race-to-run-the-uns-internet-agency/

249 „Member states elect Doreen Bogdan-Martin as ITU Secretary General." ITU Press Release. 29. September 2022. https://www.itu.int/en/mediacentre/Pages/PR-2022-09-29-ITU-SG-elected-Doreen-Bogdan-Martin.aspx

250 ITU-Wahlergebnisse. https://pp22.itu.int/en/elections/elections-results/

251 „Summit for Democracy: Year of Action." Informationsblatt, US- Außenministerium. 09. März 2022. https://www.state.gov/summit-for-democracy-year-of-action-factsheet/

252 Issie Lapowsky. „Inside the scramble to fix Biden's plan for the future of the internet." Protokoll. 04. Dezember 2021. https://www.protocol.com/policy/white-house-alliance-future-internet

253 Issie Lapowsky. „White House delays Alliance for the Future of the Internet launch." Protokoll. 06. Dezember 2021. https://www.protocol.com/white-house-delays-alliance

254 „Fact Sheet: United States and 60 Global Partners Launch Declaration for the Future of the Internet." Das Weiße Haus. 28. April 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/28/fact-sheet-united-states-and-60-global-partners-launch-declaration-for-the-future-of-the-internet/

255 „A Declaration for the Future of the Internet." Das Weiße Haus. 28. April 2022. https://www.whitehouse.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet_Launch-Event-Signing-Version_FINAL.pdf

Obwohl China und Russland nicht ausdrücklich erwähnt werden, geht die Erklärung eindeutig auf die zentralen Herausforderungen ein, die sich aus ihrem digitalen, autoritären Internetmodell und ihrer Untergrabung des Multi-Stakeholder-Modells der Internetverwaltung in der Praxis ergeben. Als Reaktion auf frühere Kritik, dass sie die Initiativen der Zivilgesellschaft, zwischenstaatlicher und anderer Multi-Stakeholder-Foren unterminiert,[256] erkennt die Erklärung Werte wie den Multi-Stakeholder-Gedanken an. Sie verspricht zudem, „beizutragen" zu Bemühungen und Organisationen wie der ICANN, dem IGF und der Freedom Online Coalition. Letztere ist ein Zusammenschluss von 34 Regierungen, die „zusammenarbeiten, um die Internetfreiheit zu unterstützen und die grundlegenden Menschenrechte – freie Meinungsäußerung, Vereinigungsfreiheit, Versammlungsfreiheit und Schutz der Privatsphäre online – weltweit zu schützen".[257]

Die anfänglichen Erwartungen an die Erklärung waren jedoch ungewiss. Denn was mit der Hoffnung auf ein enges Bündnis begann, endete, zumindest zunächst, in einem bloßen Papier. Einige Analystinnen und Analysten sind zwar der Meinung, dass dies besser ist als gar nichts, da die US-Regierung Interesse an der Internetverwaltung als Teil der Außenpolitik zeigt, aber der Initiative müssen „harte Gespräche" folgen, um „digitale Übertretungen zurückzudrängen." Das bleibt abzuwarten. Darüber hinaus könnte die Erklärung für einige unterzeichnende Parteien, die auf der demokratischen Skala relativ unbedeutend sein mögen, eine diplomatische Mahnung darstellen, nicht weiter in den digitalen Autoritarismus abzugleiten.[258] Andererseits fehlen unter den unterzeichnenden Parteien der Erklärung auch wichtige asiatische Internet-Volkswirtschaften wie Indien, Singapur und Südkorea, die sich wahrscheinlich aufgrund ihrer eigenen Tendenz zur Kontrolle des Internets sowie geopolitischer Sensibilitäten in Bezug auf China dagegen entschieden haben, zu unterzeichnen.

Für Peking wäre die einzig logische und schnell umzusetzende Antwort vermutlich die Gründung seines eigenen Clubs. Seit 2014 organisiert die chinesische Cyberspace-Verwaltung ihre wichtigste jährliche Internetveranstaltung, die World Internet Conference, in der Stadt Wuzhen im Osten des Landes. Von der ersten Veranstaltung berichteten die Teilnehmenden, dass sie den Entwurf eines Manifests von einer unbekannten Quelle „um Mitternacht unter ihren Hoteltüren hindurchgeschoben bekamen", ein Vorgehen über das sich viele beschwerten. Schließlich wurde die Erklärung am Ende der Konferenz nicht mehr erwähnt.[259] So wie der erste Versuch der USA, ein Bündnis zu schließen, verschoben wurde und es schließlich bei einer Erklärung blieb, scheiterte auch der erste Versuch Chinas, eine Erklärung abzugeben.

Im darauffolgenden Jahr, im Dezember 2015, hielt Xi Jinping auf der zweiten Weltinternetkonferenz (WIC) eine Rede, in der er seine Vision für „Dialog und Zusammenarbeit auf der Grundlage von gegenseitigem Respekt und Vertrauen" und die Förderung der Umgestaltung des globalen Internet-Governance-Systems" darlegte. Eine solche Umgestaltung sollte auf der „Achtung der Cyber-Souveränität"[260] beruhen, und die neue „internationale Cyberspace-Governance" sollte nicht „einseitig" erfolgen oder „eine Partei alle Fäden in der Hand halten".[261] Diese Visionen spiegeln die gescheiterte Erklärung von vor einem Jahr wider.

Was liegt also näher, als die bestehende Plattform der WIC zu nutzen, um eine Allianz zu bilden, die der von den USA angeführten Erklärung entgegenwirkt? Und wenn die USA noch nicht in der Lage waren, eine Allianz mit ihren Partnern zu bilden, warum ihnen dann nicht zuvorkommen? China hat genau das getan. Im Juli 2022 wurde die WIC in eine „internationale Organisation" umgewandelt, die aus „Gründungsmitgliederinnen und -mitgliedern" besteht, darunter „Institutionen, Organisationen, Unternehmen und Einzelpersonen aus fast 20 Ländern".[262] Xi hielt eine Videoansprache auf der Eröffnungskonferenz, in der er die neue Gruppe beglückwünschte, da sie mit „Weisheit und Macht zur Entwicklung der globalen Internet-Governance" beitrage um einen „fairen und vernünftigen, offenen und toleranten, sicheren und stabilen und lebendigen Netzraum" zu schaffen.[263]

Wer sind die Mitgliederinnen und Mitglieder der neuen Organisation „World Internet Conference"? Es soll sich um eine nicht näher bezeichnete Liste „weltbekannter führender Internetunternehmen, maßgeblicher Branchenorganisationen und Internet Hall of Famers" handeln.[264] Unabhängig davon, ob die Nichtveröffentlichung auf Geheimhaltung oder Bluff zurückzuführen ist, könnte China zumindest behaupten, seinen Club vor den USA gegründet zu haben. Auf der Weltinternetkonferenz 2022 selbst, die eher unauffällig im November stattfand, wurden kaum Neuigkeiten über die Organisation der WIC bekannt gegeben. Nichtsdestotrotz müssen die Demokratien wachsam bleiben, was die WIC als Nächstes vorhat.[265]

256 „Empty Promises? Declaration for Future of the Internet is nice on paper." AccessNow. 28. April 2022. https://www.accessnow.org/declaration-for-future-internet/

257 „Aims and Priorities." Freedom Online Coalition. https://freedomonlinecoalition.com/aims-and-priorities/

258 Alex Engler. „The Declaration for the Future of the Internet is for wavering democracies, not China and Russia." 09. Mai 2022. https://www.accessnow.org/declaration-for-future-internet/„China Delivers Midnight Internet Declaration - Offline."

259 The Wall Street Journal. 21. November 2014. https://www.wsj.com/articles/BL-CJB-24963

260 „China internet: Xi Jinping calls for 'cyber sovereignty'." BBC. 16. Dezember 2015. https://www.bbc.com/news/world-asia-china-35109453

261 Veni Markovski und Alexey Trepykhalin. „Country Focus Report: China Internet-Related Policy Initiatives and Laws." ICANN. 31. Januar 2022. https://itp.cdn.icann.org/en/files/government-engagement-ge/ge-010-31jan22-en.pdf

262 Jiaxing Li. „China's World Internet Conference goes 'international' as Beijing seeks to promote its own vision of global cyberspace." South China Morning Post. 13. Juli 3022. https://www.scmp.com/tech/big-tech/article/3185151/chinas-world-internet-conference-goes-international-beijing-seeks

263 "世界互聯網大會成立大會舉行." 人民網. 13. Juli 2022. http://cpc.people.com.cn/BIG5/n1/2022/0713/c64094-32473662.html

264 "世界互联网大会成立." 中国经济周刊. 13. Juli 2022. https://www.163.com/dy/article/HC587ONF0530I1ON.html

265 Justin Sherman. „China's New Organization Could Threaten the Global Internet." Slate. 29. Juli 2022. https://slate.com/technology/2022/07/china-world-internet-conference-organization-standards.html

7. Aufruf zu einer wettbewerbsorientierten Antwort

Zusammenfassend lässt sich feststellen, dass sich Chinas Internetpolitik von einer absoluten internen Kontrolle zu einem Export von digitalem Autoritarismus entwickelt hat. Erreicht wurde dies durch die Perfektionierung seines Rechts- und Verwaltungskonzepts der Zensur und Kontrolle sowie durch technologischen Wettbewerb und eine erneute Konzentration auf sein Modell einer Überwachungsdatenwirtschaft. Auf diese Weise strebt China die globale Vorherrschaft über das westliche Modell der liberalen Demokratie an, aus welchem das Internet ursprünglich hervorgegangen ist.

Was können die Demokratien also tun, um wettbewerbsfähig zu bleiben?

Vor zwanzig Jahren waren die Demokratien übermäßig optimistisch, was das Internet für die Gesellschaft im In- und Ausland bedeuten würde. Inzwischen wissen sie es besser, auch wenn sie ihre Lektionen mitunter auf die harte Tour gelernt haben. Die Demokratien dürfen gegenüber dem Internet und der Technologie nicht übermäßig pessimistisch sein. Sie müssen jedoch lernen, wo sie versagt haben, was sie bewahren und was sie ändern sollten.

Es ist nicht so, dass die Demokratien das techno-autokratische Potenzial des Internets nicht erkannt hätten oder, dass autoritäre Regierungen auf der ganzen Welt das Recht auf freie Meinungsäußerung und den freien Informationsfluss beschnitten hätten. Im Jahr 2006 hat die US- Außenministerin Condoleezza Rice die Global Internet Freedom Task Force (GIFT) einberufen, um eine solide globale Internetstrategie zu entwickeln. Damit sollten Bedrohungen der Internetfreiheit überwacht werden und darauf reagiert werden. Außerdem sollten die Grenzen der Internetfreiheit erweitert werden, indem der Zugang zum Internet durch die Koordinierung mit verschiedenen Regierungsbehörden und der Technologieindustrie ausgebaut wird.[266]

266 „Global Internet Freedom Task Force." US- Außenministerium, Archiv. https://2001-2009.state.gov/g/drl/lbr/c26696.htm#:~:text=Secretary%20of%20State%20Condoleezza%20Rice,of%20information%20on%20the%20Internet.

Am 21. Januar 2010 hielt die damalige US-Außenministerin Hillary Rodham Clinton im Newseum in Washington, D.C., eine Rede über die Freiheit des Internets, und zwar genau zu dem Zeitpunkt, als amerikanische Unternehmen beschuldigt wurden, die Zensur im Ausland, darunter auch in China, zu unterstützen. Als Teil der in ihrer Rede skizzierten Maßnahmen wurde die GIFT der vorherigen Regierung als Forum reaktiviert, das sich mit der Internetfreiheit auf der ganzen Welt befasst. Die Zusammenarbeit mit US-amerikanischen Technologieunternehmen sollte verstärkt werden, auch über nichtstaatliche Branchenorganisationen wie die Global Network Initiative. Auch sollten mehr staatliche Mittel investiert werden, um die Entwicklung von Instrumenten gegen die Umgehung von Gesetzen sowie andere Bemühungen um die Internetfreiheit in der ganzen Welt zu unterstützen.

Nach der Bush- und der Obama-Administration kam das Thema Internetfreiheit erst gegen Ende der Trump-Administration wieder auf die Tagesordnung, nämlich mit der Einführung des Clean Network. Der Unterschied war, dass es bei der Trump-Initiative um Sanktionen ging, denn inzwischen war der technologische Einfluss Chinas in der Welt enorm gewachsen. Im Gegensatz zu den Zeiten, als die Außenministerinnen Rice und Clinton vor allem über Zensur sprachen, die die Meinungsfreiheit der Menschen in autokratischen Ländern einschränkte, exportierten China und seine Technologieunternehmen bis 2020 ihre Technologie zusammen mit ihrer Philosophie und ihrer versteckten Überwachungsagenda an private und öffentliche Kundinnen und Kunden in aller Welt. Viele Unternehmen, auch in Europa und Nordamerika, waren in hohem Maße von ihnen abhängig geworden.

Was in den letzten zwanzig Jahren der globalen Internetpolitik fehlte, war eine kontinuierliche Politik der USA. Ein weiteres Manko dieser Nicht-Politik ist die fehlende Aktion und Koordination mit dem privaten Sektor und anderen Demokratien. Der Vorschlag der Biden-Regierung für eine Allianz für die Zukunft des Internets hätte ein Versuch sein sollen, einige dieser Probleme anzugehen, aber es scheint immer noch schwierig zu sein, die Frage der globalen Internetverwaltung und -führung zu einer diplomatischen Priorität unter den vielen dringenden außenpolitischen Problemen zu erklären, denen sich die Demokratien in der Welt heute gegenübersehen.

In der Zwischenzeit war Europa nicht in der Lage, die Führung im Kampf für die globale Internetfreiheit und gegen die wachsende Techno-Autokratie zu übernehmen: Die führenden Nationen der Europäischen Union haben sich eher darauf konzentriert, die Dominanz der amerikanischen Big Tech zu bekämpfen, und sogar darauf, an Chinas wachsendem Markt zu partizipieren. Europa ist es zu verdanken, dass sich die Lücke in der Daten- und Datenschutzpolitik geschlossen hat, indem es mit der Datenschutz-Grundverordnung (DSGVO) eine Vorreiterrolle übernommen hat. Die DSGVO diente sogar als Modell für die chinesische Regierung. China hat Konzepte und Bestimmungen aus der DSGVO übernommen, wie z. B. die Extraterritorialität, sowie aus US-Gesetzen wie dem Cloud Act, der Unternehmen reguliert, die in den USA elektronische Kommunikations- und Remote-Computerdienste anbieten, und sie auf seine eigene drakonische Weise eingesetzt.

Sicherlich war die Sicht auf das Internet einst allzu rosig und etwas naiv. Aber auch die demokratischen Regierungen und ihre Gesetzgeber sind heute vielleicht zu sehr auf die „dunkle Seite" des Internets fixiert und erliegen daher simplen Lösungen, die ebenso naiv und wenig hilfreich sein könnten, wie z. B. die Regulierung von Tech-Unternehmen „wie Versorgungsunternehmen".[267] Manche mögen sogar auf die Flutwelle chinesischer Tech-Razzien blicken und denken, dass China etwas richtig macht, z. B. ein „Gleichgewicht zwischen staatlicher Kontrolle, Wirtschaftswachstum und Innovation" zu schaffen. Nichts könnte falscher sein.[268]

Gerade weil das Internet global ist, müssen die Demokratien ein gesundes Internet und seine Freiheit als eine globale Angelegenheit betrachten. Das Internet global zu halten, als ein Internet ohne Fragmentierung, ist ein entscheidender Teil des Kampfes für ein besseres Internet der Zukunft. Wenn ein Teil des Internets versagt, besteht die Gefahr, dass andere Teile des Internets weniger frei, weniger offen, weniger sicher und weniger widerstandsfähig werden. Das ist auch der Grund, warum wir uns standhaft gegen Bestrebungen wehren müssen, das Netz von China und anderen Ländern abzuspalten, die seine autoritären Werte teilen.

Gesetze in demokratischen Ländern können sich auch auf andere Länder auswirken. Nehmen Sie das deutsche NetzDG als Beispiel. Der Kampf gegen Fake News, Hassreden, Desinformation und Fehlinformationen im Internet ist richtig. Aber wenn Plattformen verpflichtet werden, Inhalte auf Anfrage der Regierung umgehend zu entfernen, wird ein Präzedenzfall für Zensur geschaffen, dem Autokraten nur zu gerne nachkämen. Man kann zwar argumentieren, dass autokratische Länder dies ohnehin selbst einführen können, aber nun dürfen sie sich stolz damit rechtfertigen, dass „demokratische Länder es zuerst getan haben". Die Demokratien verlieren jeglichen moralischen Vorsprung, wenn sie auf die gleichen Zensur- und Überwachungstaktiken zurückgreifen wie autoritäre Staaten.

267 Lauren Feiner. „Justice Thomas suggests regulating tech platforms like utilities." CNBC. https://www.cnbc.com/2021/04/05/justice-thomas-suggests-regulating-tech-platforms-like-utilities.html

268 Matt Perault. „Internet Freedom 10 Years In." Lawfare. 21. Januar 2020. https://www.lawfareblog.com/internet-freedom-10-years

Dennoch sehen wir dies immer wieder in umstrittenen Gesetzesvorschlägen, die in Australien, der EU, den USA, Großbritannien und Kanada eingebracht werden und Hintertüren für Internetunternehmen und -plattformen fordern, so wie es China vorgemacht hat. Die Überwachungstaktiken, die jetzt in einigen US-Bundesstaaten angewandt werden, um „Abtreibungskriminelle" aufzuspüren, ähneln auffallend denen, die in autoritären Ländern angewandt werden. Tatsächlich kann China nun selbstbewusst darauf verweisen: „Seht ihr, wir hatten doch recht, jetzt müsst auch ihr lernen und es uns gleichtun." Deshalb ist es für Demokratien so wichtig, vor der eigenen Haustür zu kehren.

Der US-Kongress verabschiedete im August 2022 den sogenannten „CHIPS and Science Act"[269], um die wissenschaftliche Forschung und die fortschrittlichen Fertigungskapazitäten der USA zu stärken, damit sie mit China konkurrieren können. Die Politik erkannte, dass der technologische Vorsprung des Landes in Bereichen wie Halbleiter, künstlicher Intelligenz, Quantencomputer und Robotik schrumpfte und die Stabilität der Chip-Lieferkette schwand. Ein ähnlicher politischer Schwerpunkt und eine ähnliche Priorität müssen auf das Internet gelegt werden, wenn die freie Welt mit China und Russland konkurrieren will.

Man kann sich darüber streiten, wie viele Jahre die USA oder Taiwan China in der Halbleiterentwicklung, -herstellung und -produktion noch voraus sind. Aber in der Internet- und Kommunikationstechnologie hat China bereits aufgeholt oder in einigen Bereichen sogar die Führung übernommen. Beim Internet ist die Lage also wohl noch dramatischer. Die Bedrohung durch das Splitter-Internet ist vergleichbar mit den Problemen in der Halbleiterlieferkette – oder sogar noch gravierender: Probleme in der Supply Chain lassen sich manchmal durch Marktveränderungen beheben und umkehren, aber das Internet ist bereits seit Jahrzehnten durch Maßnahmen wie der GFW zersplittert, wobei Informationen und Dienste über lange Zeiträume vollständig abgeschottet sind. Eine solche Unterbrechung der „Supply Chain" des Internets lässt sich möglicherweise viel schwieriger korrigieren. Und irgendwie akzeptieren wir Chinas Zensur als Norm. Dies sollte nicht der Fall sein.

Abschließend Vorschläge für mögliche Komponenten einer wettbewerbsorientierten Antwort gegen digitalen Autoritarismus:

1. Demokratische Regierungen sollten **dem Drang nach Cyber-Souveränität widerstehen**. Vor der Einführung von Cybergesetzen sollte eine globale Folgenabschätzung durchgeführt werden, um alle negativen Nebeneffekte der möglichen Förderung des digitalen Autoritarismus in anderen Ländern zu berücksichtigen, die der globalen Internetfreiheit schaden würden. Wie im Falle des Klimawandels kann eine nicht ausreichend durchdachte lokale Gesetzgebung Auswirkungen auf die ganze Welt haben.
2. Bewahren Sie die Führungsposition in der Datenwirtschaft, indem Sie dringend **globale Datenschutz- und Datenaustauschregeln** und Regulierungsnormen für das Internet in der freien demokratischen Welt einführen. Dies kann z.B. durch die Beschleunigung der Verhandlungen zwischen Europa und den USA, der Asiatisch-Pazifischen Wirtschaftsgemeinschaft APEC usw. in die Wege geleitet werden.
3. **Das Multi-Stakeholder-Modell für die Internetverwaltung sollte unterstützt und angenommen werden**, bei gleichzeitiger Verstärkung der Beteiligung der Zivilgesellschaft weltweit an den bestehenden und neu entstehenden Organisationen und Foren für die politische Diskussion und Gestaltung.
4. **Verstärken Sie die Beteiligung an und die Führung von Organisationen, die Standards setzen und das Internet verwalten,** um die Werte der offenen Technologie und des freien Internets gegen Einflüsse von autokratischen Ländern zu schützen, die versuchen, diese Prozesse und Organisationen zu übernehmen.
5. **Investieren Sie in die Erforschung und Entwicklung von Technologien zur Wahrung der Privatsphäre, zur Bekämpfung von Zensur und Überwachung sowie in den Einsatz solcher Technologien**, während Sie gleichzeitig Informationsdienste der nächsten Generation entwickeln, um Zensur zu überwinden.
6. **Der Privatsektor sollte den Grundsatz eines offenen Internets und eines „eingebauten Datenschutzes"** für alle Produkte und Leistungen übernehmen und sich dazu verpflichten, diese überall auf der Welt zu nutzen. Tech-Unternehmen sollten außerdem darin geschult werden, die Auswirkungen ihrer Produkte und Innovationen auf die nationale Sicherheit und Verteidigung zu verstehen.[270]
7. **Den Bestrebungen autokratischer Länder, ihre digitale Unterdrückung zu transnationalisieren, wirkt man entgegen,** indem man gezielte Sanktionen und Regulierungsmaßnahmen gegen Überwachungsplattformen und -technologien aus autoritären Ländern ausweitet, die tatsächlich in ihrem Namen arbeiten.
8. **Internetuser auf der ganzen Welt** können durch Bildung, Weiterbildung und Entwicklungshilfe gefördert werden, insbesondere in unterentwickelten Ländern und unterprivilegierten Gemeinschaften, indem digitale Rechte und die Redefreiheit im Internet unterstützt werden.

269 „The CHIPS and Science Act." US- Repräsentantenhaus. https://science.house.gov/chipsandscienceact

270 Elisabeth Braw. „Tech experts need defence training for NATO's race against China." Financial Times. 26. Juli 2022. https://www.ft.com/content/4cc97d-cc-d02e-4ae6-a4e7-d2fafffc5d26

Über den Autor

Charles Mok ist derzeit Gastwissenschaftler am Global Digital Policy Incubator des Cyber Policy Center der Stanford University, wo sich seine Forschung auf digitalen Autoritarismus und Cyberpolitik im asiatisch-pazifischen Raum konzentriert. Außerdem ist er Vorstandsmitglied der Internet Society und Gründer von Tech for Good Asia, einer regionalen Initiative, die die positiven Kräfte der digitalen Technologien für die Gesellschaft nutzt. Von 2012 bis 2020 war Charles Mok Mitglied des Legislativrats in Hongkong und vertrat den funktionalen Wahlkreis für Informationstechnologie, wo er sich für Themen wie Informationsfreiheit, Datenschutz, Cybersicherheit und Innovation, sowie Menschenrechte und Demokratie einsetzte.

Vor seiner politischen Laufbahn war Charles Mok 1994 Mitbegründer von HKNet, einem der ersten ISPs in Hongkong, und Mitbegründer und Vorsitzender der Internet Society Hong Kong und der Hong Kong Internet Service Providers Association. Darüber hinaus fungierte er als Präsident der Hong Kong Information Technology Federation. Charles war zudem Vorsitzender der Asian, Australasian, and Pacific Islands Regional At-Large Organization (APRALO) der ICANN.

Er erwarb einen Bachlorabschluss in Computer- und Elektrotechnik und einen Masterabschluss in Elektrotechnik an der Purdue University und wurde 2022 von der Elmore Family School of Electrical and Computer Engineering der Universität als herausragender Elektro- und Computeringenieur ausgezeichnet.