Martin-Luther-Universität Halle-Wittenberg
Naturwissenschaftliche Fakultät III
Institut für Informatik

Seminar

Informatik und Gesellschaft

Sommersemester 2021

geleitet durch Prof. Dr. Paul Molitor

Einsatz digitaler Technologien durch staatliche Akteure in Demokratien und autokratischen Staaten

Moritz Campino Wolf und Daniel Wurst

Inhaltsverzeichnis

1 Einleitung **3**

2 Begriffserklärung und Einordnung **4**
2.1 Definitionen und Begriffe 4
2.2 Demokratiemessung: Demokratie oder Autokratie? 6

3 Einsatz digitaler Technologien in Demokratien **10**
3.1 Estlands „i-Voting“ 10
3.1.1 E-Government 10
3.1.2 i-Voting 11
3.2 Deutschlands „Vorratsdatenspeicherung“ 15
3.2.1 Vorratsdatenspeicherung 1.0 15
3.2.2 Vorratsdatenspeicherung 2.0 18
3.2.3 Vorratsdatenspeicherung aktuell und Ausblick 19

4 Einsatz digitaler Technologien in Autokratien **21**
4.1 Chinas „Große Firewall“ 21
4.1.1 Hintergrundgeschichte und Ziele 21
4.1.2 Technische Hintergründe und Methoden zum Umgehen der Zensurmaßnahmen 23
4.1.3 Soziale Auswirkungen 28
4.1.4 Wirtschaftliche Auswirkungen 30
4.2 Chinas „Social Credit System“ 31
4.2.1 Ursprüngliche Planungen und Ziele 31
4.2.2 Testphasen und -systeme 33
4.2.3 Öffentliche Diskussion und Wahrnehmung in- und außerhalb Chinas 38
4.3 Russlands Weg in die Internet-Zensur 40
4.3.1 Freie Entwicklung des russischen Internets in den 1990er und 2000er Jahren 40
4.3.2 Erster Angriff auf die Freiheit des russischen Internets 41
4.3.3 Entwicklungen seit dem Arabischen Frühling und der 2011/12er-Protestbewegung 42

5 Fazit **46**

Gender-Hinweis: Wir verwenden in dieser Arbeit den Doppelpunkt als Gender-Gap (Student:innen), um einen digitalen Glottalverschluss durch Screenreader-Programme auch akustisch zu ermöglichen.

1 Einleitung

Die immer weiter voranschreitende Digitalisierung und die damit verbundene stetige Entwicklung neuer Technologien haben das menschliche Leben wohl verändert wie nur wenige Ereignisse zuvor. Nicht umsonst wird in Deutschland im Bezug darauf (v.a. im wirtschaftlichen Kontext) auch von der vierten industriellen Revolution, „Industrie 4.0“, gesprochen [1].

Diese Entwicklungen haben auch vor staatlichen Stellen nicht Halt gemacht. In demokratischen sowie in autokratischen Staaten haben Regierungen und Verwaltungen die Möglichkeiten der neuen Technologien erkannt und setzen diese ein. So hat sich beispielsweise die deutsche Bundesregierung das Ziel gesetzt, bis zum Jahr 2022 sämtliche Verwaltungsdienstleistungen für Bürger:innen und Unternehmen digital über Online-Portale zugänglich zu machen. Wirtschaftsminister Peter Altmaier ist sogar eine Wette eingegangen, dass Deutschland bis dahin die „bürgerfreundlichste Verwaltung Europas“ haben werde [2].

Die Digitalisierung hat aber nicht nur positive Aspekte. In den letzten Jahren sind aber auch die Schattenseiten dieser Entwicklung zu Tage getreten. Die von Edward Snowden öffentlich gemachte, massive Überwachung der weltweiten Internetkommunikation durch den US-amerikanischen Geheimdienst NSA[1], ist nur ein Beispiel von vielen dafür, wie Regierungen auf der ganzen Welt die neuen Technologien einsetzen, um Bürger:innen, Aktivist:innen, Journalist:innen und Oppositionelle auszuspähen und die freie Presse und Meinungsäußerung unterdrücken. Wie der Unternehmensberater Markus Baumanns in seinem Buch „Kick-Off!“ schrieb: „*Die Digitalisierung aller Lebens- und Arbeitsbereiche fordert ihren Tribut und verschafft zugleich ungeahnte Möglichkeiten*“ [3]. Sie hat ihre Vor- und Nachteile.

In dieser Arbeit wird daher an einigen ausgewählten Beispielen aufgezeigt, wie staatliche Akteure in demokratischen und autokratischen Staaten digitale Technologien einsetzen. Dabei ist es in diesem Rahmen auf keinen Fall möglich, einen umfassenden Einblick in die gesamte Thematik zu geben oder gar einen Anspruch auf Vollständigkeit zu erheben. Die von uns gewählten Beispiele sollen lediglich beispielhafte Anwendungen digitaler Technologien durch staatliche Akteure aufzeigen.

[1] kurz für: National Security Agency

2 Begriffserklärung und Einordnung

In diesem Abschnitt sollen zum einen die grundlegenden Begriffe dieser Arbeit definiert und erklärt werden und zum anderen auch die im folgenden betrachteten Staaten hinsichtlich ihrer Regierungsform eingeordnet werden.

2.1 Definitionen und Begriffe

Begonnen wird mit dem Begriff der digitalen Technologie. Dieser Begriff ist im Allgemein schwer zu fassen. In dieser Arbeit werden daher digitale Technologien als eine Kombination aus Computerhardware, Software und die Vernetzung von (Computer-)Systemen verstanden. Um den Rahmen dieser Arbeit nicht zu überspannen wird sich in den Abschnitten 3 und 4 vorrangig mit der Vernetzung von Computersystemen beschäftigt.
Nachdem der erste Hauptbegriff eingegrenzt wurde, wird nun ein zweiter wichtiger Begriff charakterisiert. Dieser Begriff ist in der heutigen Politikwissenschaft ein vergleichsweise unbeliebter, da er beispielsweise zu doppeldeutig ist.[2] Trotz alledem wird in dieser Arbeit der Begriff des Staates gebraucht, da eine Ausführung der Alternativen, welche die politische Systemtheorie darstellt, den Rahmen dieser Arbeit überspannen würde. Um nun den Begriff des Staates greifbarer zu machen, wird die Definition von Schubert und Klein betrachtet. Dies unterscheiden eine weite beziehungsweise enge Begriffsfassung. Hier wird nur die engere Definition betrachtet; in diesem Zusammenhang wird ein Staat verstanden:

> *„(...) als politische Einrichtung (Institutionen und Personen), die mit der Ausübung allgemein verbindlicher Steuerungs-, Regulierungs- und Koordinierungsfunktionen betraut ist, sich (als moderner Verfassungs-S.) dabei demokratischer Willensbildungs- und Entscheidungsprozesse bedient und zur Durchsetzung dieser Entscheidungen mit Sanktionsmitteln ausgestattet ist.“* [4]

Was bei genauer Betrachtung dieser Definition auffällt, ist, dass dem Staat grundsätzlich eine demokratische Grundordnung zugesprochen wird. Dies ist allerdings nicht in allen modernen Staaten, wie später noch gezeigt wird, der Fall.

[2] Als Beispiel könnte dienen: Meint Staat die Regierung der Bundesrepublik Deutschland oder doch die Bundesrepublik Deutschland als Ganzes?

Innerhalb eines Staates handeln zusätzlich auch Akteure, ohne die ein Zusammenleben nicht möglich wäre. Jarren und Donges beschreiben Akteure als diejenigen Personen oder Gruppen,

> „*die bestimmte Handlungsziele und Interessen verfolgen; über Handlungsressourcen und normative Orientierungen verfügen; die Fähigkeit besitzen, strategisch zu handeln; die sich sowohl selbst als Akteur verstehen als auch von anderen als solcher anerkannt werden.*“ [6]

Staatliche Akteure sind in diesem Sinne staatliche Einrichtungen beziehungsweise Behörden, wie das deutsche Bundesamt für Sicherheit in der Informationstechnik oder auch das chinesische Ministerium für Industrie und Informationstechnologie. Weiterhin können auch einzelne Personen, wie der Bundeskanzler der Bundesrepublik Deutschland, ein staatlicher Akteur sein.
Im Grundgesetz für die Bundesrepublik Deutschland steht, dass Deutschland ein „*demokratischer und sozialer Bundesstaat*“ [GG Art. 20, Abs. 1] ist. Dabei ist der Begriff der Demokratie nicht so leicht zufassen und wird gelegentlich auch falsch beziehungsweise nicht weit genug gefasst verwendet. Jan von Deth meinte hierzu „*Wer Demokratie sagt, meint Partizipation.*“ [9] und genau dies ist ein Fehler. Da es in der Literatur zahlreiche Versuche gibt den Begriff der Demokratie zu fassen, wird in dieser Arbeit mit dem Verständnis von Hans-Joachim Lauth gearbeitet:

> „*Demokratie ist eine rechtsstaatliche Herrschaftsform, die eine Selbstbestimmung für alle Staatsbürger:innen im Sinne der Volkssouveränität ermöglicht, indem sie die maßgebliche Beteiligung von jenen an der Besetzung der politischen Entscheidungspositionen (und/oder an der Entscheidung selbst) in freien, kompetitiven und fairen Verfahren (z.B. Wahlen) und die Chancen einer kontinuierlichen Einflussnahme auf den politischen Prozess sichert und generell eine Kontrolle der politischen Herrschaft garantiert.*“ [5]

Dabei wird also klar, dass Demokratie weit mehr ist als nur bloße Beteiligung an Wahlen. Demokratie ist auch sein Leben frei zu bestimmen oder gut recherchierte, freie Medien zu konsumieren ohne dabei von staatlichen Akteuren beeinflusst zu werden.
Eine solche Beeinflussung oder gar Zensur findet man oft in Staaten die eine gegenteilige Staatsordnung haben: Die Autokratie. In diesen Staaten leidet das Volk durch Repressionen durch staatliche Akteure. Schubert und Klein definieren daher die Autokratie wie folgt:

> „*A. bezeichnet Regierungsformen, bei denen alle Staatsgewalt unkontrolliert in den Händen eines Herrschers (oder: Autokraten) liegt und von diesem selbstherrlich ausgeübt wird.*“ [4]

Dabei kann auch eine Gruppe, beispielsweise eine Partei, als Autokrat fungieren.
In der Realität treffen diese Definition nicht immer exakt auf einen Staat zu, so gibt es beispielsweise Mischformen oder auch Staaten, die sich gerade in einer Systemtransformation befinden und dadurch noch nicht eindeutig als demokratischer Staat gelten können. Beispielsweise ist unvollständige Demokratie, eine Demokratie, in der es zwar freie und faire Wahlen gibt und Bürgerrechte akzeptiert sind; allerdings gibt es andere Probleme wie unzureichende Pressefreiheit. Um diese Feinheiten zu erforschen, wird in der Politikwissenschaft probiert, den Grad der Demokratisierung eines Landes zu bestimmen. [5] [7]

2.2 Demokratiemessung: Demokratie oder Autokratie?

In diesem Abschnitt soll erläutert werden, wie in der Politikwissenschaft, der Grad der Demokratisierung untersucht wird und daraus die Einteilungen, der in dieser Arbeit betrachteten Länder, abgeleitet werden.
Das allgemeine Ziel der Demokratiemessung ist es, zu entscheiden, ob eine Demokratie vorliegt und darüber hinaus auch in welcher Qualität. Hierzu wird sich sowohl qualitativer als auch quantitativer Indikatoren bedient. Diese können zum Beispiel sein, welchen Anteil die Wähler:innen an der Gesamtbevölkerung haben oder auch der Grad der politischen Rechte und bürgerlichen Freiheiten. Dabei entstehen allerdings auch Probleme, wie fehlende Transparenz oder auch die Frage nach der Validität des Messverfahrens, wie später noch genauer erläutert wird. [5]
Man findet in der Literatur verschiedene Studien zu diesem Thema, beispielsweise das Polity-Projekt, die Freedom House-Studie oder auch den Democracy Index. Alle drei Studien untersuchen ähnliche Gegenstände. Das Polity-Projekt, aus den 1990er Jahren, und der Democracy Index, in der aktuellen Fassung für das Jahr 2020, untersuchen im wesentlichen wie demokratisch ein Staat ist [5] [7]. Währenddessen Freedom House, auch für das Jahr 2020, vor allem bürgerliche Rechte und politische Freiheiten der Bürger:innen untersucht [8]. Da das Polity-Projekt eher mit älteren Daten arbeitet und Freedom House nur eine Demokratie-äquivalente Untersuchung ist, wird im Folgenden mit den Zahlen des Democracy Indexes gearbeitet und dieser auch genauer vorgestellt.

Democracy Index

Der Democracy Index ist eine Studie des Londoner Beratungsunternehmens The Economist Intelligence Unit[3]. Diese ist ein Tochterunternehmen der The Economist Group, zu der auch die Zeitung The Economist gehört. Das Beratungsunternehmen – The EIU – bietet verschiedene Dienstleistungen, wie Country Analysis, Risk Analysis oder auch Industry Analysis an. [7]
Die Studie untersucht die Staaten in fünf Kategorien:

1. *Wahlprozess und Pluralismus,*
2. *Bürgerrechte,*
3. *Funktionsweise der Regierung,*
4. *politische Teilhabe und*
5. *politische Kultur* [7]

Dabei können in jeder Kategorie null bis zehn Punkte erreicht werden. Hierzu werden 60 Fragen ausgewertet; mit jeweils zwei beziehungsweise drei Antwortmöglichkeiten. Im besten Fall erhält das Land für die Frage einen Punkt; im schlechtesten null Punkte. Zusätzlich gibt es auch noch die Möglichkeit 0,5 Punkte zu erreichen. Eine Frage aus dem Bereich Wahlprozess und Pluralismus lautet beispielsweise:

> *Are municipal elections both free and fair?*
> *1: Are free and fair.*
> *0.5: Are free, but not fair.*
> *0: Are neither free nor fair.* [7]

Die Fragen werden durch Expertenurteile beantwortet, dabei wird allerdings nicht erwähnt, wer diese Experten sind. Weiterhin werden auch Fragen durch Umfrageergebnisse evaluiert. Bei Ländern in denen derartige Umfragen, auf Grund der politischen Lage schwierig sind, werden sie durch Vergleiche mit ähnlichen Ländern, wiederum durch Expertenurteile, bewertet.

[3] kurz: The EIU

Um den Indexwert der einzelnen Staaten zu bestimmen wird der Durchschnitt der fünf Kategorien, siehe oben, bestimmt. Anschließend werden die Länder in vier Regimetypen[4] eingeteilt:

volle Demokratie: bei einem Indexwert größer als acht.

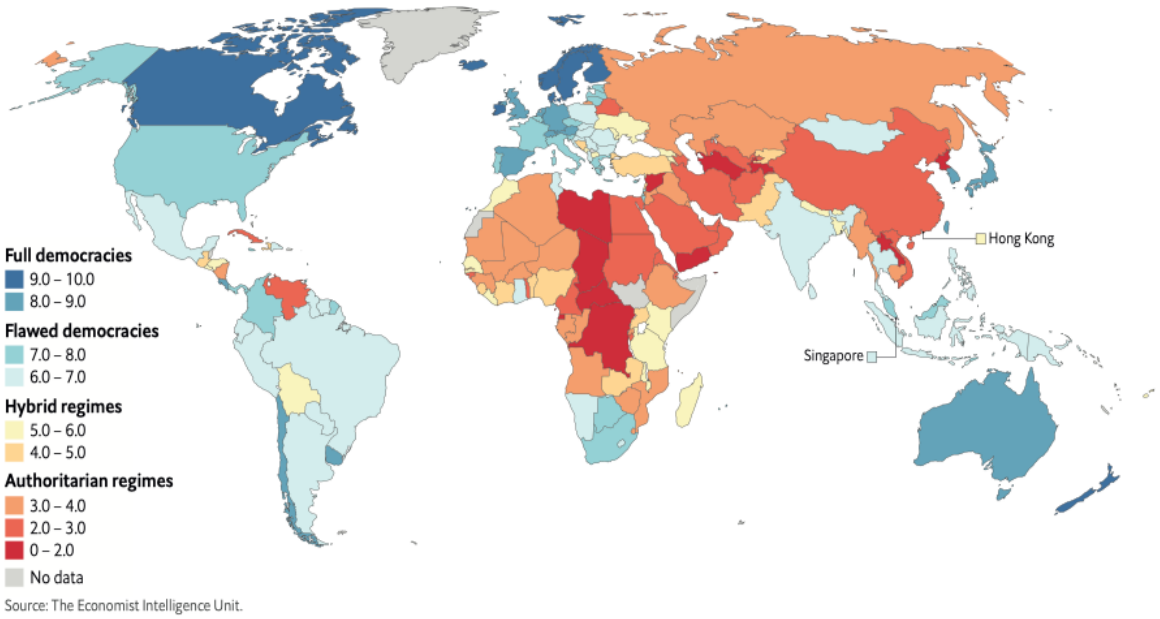
unvollständige Demokratie: bei einem Indexwert zwischen sechs und acht.

Hybridregime: bei einem Indexwert zwischen vier und sechs.

Autokratie: bei einem Indexwert kleiner oder gleich vier.

An dieser Stelle sei noch erwähnt werden, dass eine volle Demokratie keinesfalls als „perfekt“ bezeichnet werden kann. Es kann allerdings davon ausgegangen werden, dass die Gewaltenteilung – Exekutive, Judikative und Legislative – intakt ist und vor allem die Judikative-Gewalt unabhängig von anderen staatlichen Akteuren agiert und Entscheidungen fällen kann. [7]

Abbildung 1: Weltkarte der Regimetypen [7]



[4]In der Politikwissenschaft wird der Begriff des Regimes im Allgemeinen nicht negativ konnotiert verwendet: „*Regime bezeichnen die formelle und informelle Organisation des politischen Herrschaftszentrums einerseits und dessen jeweils besonders ausgeformte Beziehungen zur Gesamtgesellschaft andererseits.*“ [10]

Wie in Abbildung 1 zu sehen ist, gelten Europa, Nord- und Südamerika sowie Ozeanien und Australien überwiegend als Demokratie, auch wenn vor allem in Südamerika und Ozeanien die Mehrzahl der Staaten eine unvollständige Demokratie haben. In Afrika, Asien und dem Nahen Osten überwiegen die Autokratien und Hybridregime.
Nach einzelnen Staaten betrachtet ist Norwegen das demokratischste Land mit dem Democracy Index von 9.81. Platz zwei und drei belegen Island und Schweden. Deutschland ist mit einem Indexwert von 8.67 auf Platz 14 kurz hinter Luxemburg mit 8.68. All diese Staaten zählen damit als volle Demokratie. Frankreich hat mit einem Index von 7.99 nur knapp das Prädikat der vollen Demokratie verpasst und ist somit nur eine unvollständige Demokratie; ebenso wie Estland mit 7.84. Zu Hybridregimen gehören Staaten wie die Ukraine, Hongkong oder Nigeria. Eindeutig autokratische Staaten sind beispielsweise Russland mit einem Indexwert von 3.31, China mit 2.27. Den 167. Platz, welcher in der Untersuchung den Letzten darstellt, bildet Nordkorea mit einem Democracy Index von 1.08. [7]
In den nun folgenden Abschnitten 3 und 4 werden ausgewählte Beispiele aus den Staaten Deutschland und Estland sowie Russland und China diskutiert.

3 Einsatz digitaler Technologien in Demokratien

In diesem Abschnitt sollen der Einsatz digitaler Technologien durch demokratische Staaten betrachtet werden. Hierbei wird der Fokus auf die Speicherung von Daten zur Terrorabwehr gelegt und auch auf die Digitalisierung der politischen Partizipation. Dabei wird dies exemplarisch an den Staaten Deutschland und Estland verdeutlicht.

3.1 Estlands „i-Voting“

In den letzten Jahrzehnten wird der Ruf nach mehr Digitalisierung in vielen westlichen Ländern immer stärker. In Europa, wenn nicht sogar weltweit, gibt es ein Vorreiterland, welches seit seiner Unabhängigkeit von der UdSSR im Jahr 1991, stetig den Grad der Digitalisierung voran brachte und heute als das „*Silicon Valley Europas*“ bezeichnet wird: dieses Land ist Estland. [19] [4]

3.1.1 E-Government

Estland bezeichnet sich selbst als „E-Estonia“, das „E“ ist dabei vom Begriff E-Government abgleitet, denn die Esten können 99% ihrer Behördengänge über das Internet erledigen [14]. Nach Schubert und Klein bedeutet E-Government:

> „*den verstärkten Einsatz digitaler Technologien und elektronischer Medien, um die Information und Kommunikation sowie den Austausch innerhalb und zwischen staatlichen Einrichtungen auf allen Ebenen zu erleichtern, zu beschleunigen und generell zu verbessern.*“ [4]

Es werden dabei drei Dimensionen des E-Government unterschieden: Die E-Administration, die E-Democracy und das organisatorische Reengineering.
Die E-Administration, oder zu Deutsch Teleadministration, stellt dabei eine Schnittstelle zur computergestützten Abwicklung von Prozessen dar. Somit müssen die Bürger:innen oder auch Unternehmen nicht mehr Behörden aufsuchen, um beispielsweise einen Bauantrag zu stellen oder an einer Ausschreibung teilzunehmen. E-Democracy, oder zu Deutsch Telepartizipation, ist die politische Teilhabe der Bürger:innen beispielsweise bei Wahlen oder Petitionen. Dabei werden diese über das Internet vollzogen. In Estland ist dies schon sehr weit fortgeschritten, wie im Abschnitt 3.1.2 genauer beschrieben wird. Das organisatorische Reengineering, oder auch das Reorganisieren von Strukturen und Prozessen, ist die wichtige Kombination aus E-Administration

und E-Democracy, denn ohne eine möglichst einfache und leichte Handhabe der Bürgerportale ist eine vollständige Digitalisierung der Verwaltung nicht möglich. Dabei steht im Allgemeinen eine Effizienzverbesserung im Vordergrund. Damit einher geht auch ein verbesserter Bürgerservice, denn durch einen zu jeder Tages- und Nachtzeit ermöglichten Zugriff auf alle Angelegenheiten der öffentlichen Verwaltung, entsteht ein sogenanntes „Non-Stop-Government“, welches wiederum auch eine höhere Transparenz gegenüber den Bürger:innen zulässt und sich gleichzeitig an die Bedürfnisse jeder einzelnen Person oder eines Unternehmens anpassen kann. Weiterhin kann durch eine vollständig digitalisierte Verwaltung auch die Sicherheit und Rechtmäßigkeit verbessert werden, da beispielsweise die Veränderungen von Dateien mitgeloggt werden können. Damit sinkt das Risiko von Datenmanipulationen und es könnte effektiv Korruption vorbeugen. [11]
Die Vorstellung einer vollkommen digitalisierten Gesellschaft mag utopisch klingen, doch in Estland ist dies bereits an der Tagesordnung. 99% der Verwaltung sind hier digitalisiert; es gibt lediglich drei Fälle, für die man das Amt persönlich aufsuchen muss: „*E-services are only impossible for marriages and divorces*“ [14] und Immobiliengeschäfte. Um nun eine der vielen anderen möglichen Amtsanliegen, wie eine Vereinsgründung oder die Steuererklärung durchzuführen, müssen sich die Bürger:innen nur mit ihrem Personalausweis auf der Internetseite `www.eesti.ee` anmelden. Mit dieser Praxis konnten bereits 844 Jahre an Arbeit eingespart werden. Doch dies ist dem Vorreiterland noch nicht digital genug. Mit der „*Estonian Government Cloud*“ [14] soll die bestehende digitale Infrastruktur erweitert und verbessert werden. „*The solution will help to integrate the existing siloed IT infrastructure of the Estonian public sector into shared pool of resources.*“ [14] Dabei wird besonders großer Wert auf die Datensicherheit der Systeme gelegt. Hierzu werden die Daten an zwei unterschiedlichen Standorten in Estland gespeichert. Darüber hinaus werden die Daten durch Blockchains signiert. Weiterhin hat nicht jede Behörde Zugriff auf alle Daten eines:einer Bürger:in, trotzdem ist der Datenaustausch zwischen den Behörden möglich. Dabei ist das Hauptziel, dass nicht alle Daten an einem Punkt gespeichert werden. Außerdem ist es jedem:jeder Bürger:in jeder Zeit möglich die Benutzung seiner:ihrer Daten zu kontrollieren, um Missbrauch vorzubeugen. [14] [13] [15]

3.1.2 i-Voting

Wie bereits im letzten Abschnitt 3.1.1 erwähnt, ist ein Teil des E-Government auch die E-Democracy. Somit beschäftigt sich dieser Abschnitt mit den Onlinewahlen in

Estland.
Bereits 2001 wurde in Estland der Ruf nach digitalen Wahlen immer lauter. 2002 wurde dann vom Riigikogu, dem estnischen Parlament, die rechtliche Grundlage für i-Voting geschaffen. Damit einher ging die Einführung eines neuen Personalausweises, welcher gleichzeitig als virtuelle Identität fungiert. Zu den Kommunalwahlen 2005 konnten die Wähler:innen erstmals ihre Stimme über das Internet abgeben. Die Beteiligung bei dieser Internetwahl, war allerdings sehr gering – rund ein Prozent. Dies war unter anderem besonderes der Sorge um den Datenschutz geschuldet, welche auch nicht unbegründet war. 2007 wurde Estland Opfer eines gezielten Cyberangriffs. „*Hacker legten damals mit einer Flut automatisierter Aufrufe gezielt die Webseiten wichtiger Staatsorgane, Banken und Medien lahm, kaperten die Seiten und luden dort politische Parolen und Propagandabilder hoch*“ [12]. Bei der strafrechtlichen Aufarbeitung der Vorfalls konnte ermittelt werden, dass sowohl der Hacker als auch der Drahtzieher einen russischen Hintergrund haben. Seitdem hat die Sicherheit im Internet einen sehr hohen Stellenwert in Estland. Hierzu wurde eigens eine neue Behörde für Informationssysteme gegründet. Mit Hilfe von, sogenannten, White-Hat-Hackern werden die selbstgesetzten Sicherheitsstandards immer wieder überprüft und weiterentwickelt. Daraufhin wird i-Voting in Estland immer populärer. Gleichzeitig stieg auch die Wahlbeteiligung von 58% 2003 auf 62% 2007 an. Bei den Parlamentswahlen 2015 gaben 64% der rund 900.000 Wahlberechtigten ihre Stimmen ab, davon waren rund ein Fünftel i-Votes. 2019 lag der Anteil der online abgegebenen Stimmen bereits bei rund 44%. [16] [12] [20]
Dies liegt auch daran, dass Estland mit gerade einmal rund einer Million Einwohner:innen relativ klein ist und somit gleichzeitig lange Wege ins Wahllokal entstehen können. Speziell der Erfolg des i-Votings lässt sich mit der einfachen Handhabung der i-Voting-Software und des Wahlprozesses begründen.

Wahlprozess für die Wähler:innen

Für die Wähler:innen ist das Verfahren denkbar einfach. Sie navigieren zu der Internetseite `www.valimised.ee`, auf dieser können sie sich, ab zehn Tage vor dem Wahltag, die, so genannte, Voter-Application[5] herunterladen. Die Voter-Application steht für alle gängigen Betriebssysteme – Windows, macOS und Linux – zur Verfügung. Somit ist gewährleistet, dass alle Wahlberechtigten das i-Voting nutzen können. Nach dem

[5]Eine Bilderdokumentation des Wahlprogrammes und -prozesses kann hier berachtet werden: `https://www.valimised.ee/en/internet-voting/guidelines/stages-i-voting-voter-application` (abgerufen am: 17.08.2021)

Download der App identifiziert sich der:die Wähler:in sowohl mit seinem:ihrem Personalausweis als auch mit einem, beispielsweise per SMS erhaltenen, PIN. Anschließend können die Kandidat:innen gewählt werden. Die Wahl muss mit einem zweiten PIN bestätigt werden – dieser gilt als digitale Unterschrift. Anschließend werden die Stimmen übermittelt. Danach kann mit einem QR-Code und der Verification-Application überprüft werden, ob die Stimme auch korrekt an die digitale Wahlurne gesendet wurde. [12] [16]
Der eigentliche Wahlakt kann beliebig oft wiederholt werden, allerdings nur bis vier Tage vor der eigentlichen Wahl. Falls ein:e Wähler:in mehrfach abgestimmt hat wird die zuletzt abgegebene Stimme gewertet. Wer sich am eigentlichen Wahltag noch einmal umentscheiden sollte, kann auch über die herkömmliche Wahl im Wahllokal nochmal seine:ihre Stimme ändern. Dann wird die Stimme aus dem Wahllokal gezählt. [20]

Technischer Hintergrund und die Auszählung der Stimmen

Das i-Voting-System besteht aus zwei Ebenen: Die Voter-Application und der Collection Service.
Die Voter-Application „IVXV“ ist ein in Java geschriebenes Programm. Die App ist vollständig im Internet verfügbar und kann von jedem:jeder Bürger:in eingesehen werden.[6]
Die Voter-Application arbeitet mit einer RSA-Verschlüsselung und Signaturen. Hierzu wird die abgegebene Stimme von der App mit einer zufälligen Zahl und dem public key verschlüsselt. Anschließend wird die Stimme an die Collection Service mittels HTTPS übermittelt. Diese überprüft wiederum, ob die abgegebene Stimme von einer wahlberechtigten Person stammt und fügt der Stimme eine Gültigkeitsbestätigung an. Die nun verschlüsselte und bestätigte Stimme wird nochmal mit einem separaten Zeitstempel versehen und in der „i-bollot box“ – der digitalen Wahlurne – abgespeichert. [18] [16]
Mit Hilfe der Voter-Application wird ein QR-Code erzeugt, der die zufällige Zahl und den Zeitstempel enthält. Mit diesem kann der:die Wähler:in seine:ihre Stimme überprüfen. Hierzu wird der QR-Code mit einer speziellen Smartphone-App, welche für Android, iOS und Windows Phone zur Verfügung steht, eingescannt. Anschließend wird die Stimme, mit den im QR-Code gespeicherten Daten, aus der i-bollot box heruntergeladen und entschlüsselt und dem:der Wähler:in angezeigt. Die Überprüfung kann in einem gewissen Zeitrahmen wiederholt werden. Dieser wird von der Wahlkommission vor der Wahl festgelegt. Die Funktionalität des Überprüfens wurde erst nach der Wahl 2011 bereitgestellt und soll die Wähler:innen vor Manipulationen ihrer Stimme, durch

[6] Sorce Code von „IVXV“ unter `https://github.com/vvk-ehk/ivxv` (abgerufen am: 17.08.2021)

ihr eigens System und etwaiger Software darauf, schützen. [18] [16]
Eine Studie der Universität Tartu besagt allerdings, dass in den Onlinewahlen 2014 und 2015 nur 4.7% der i-Votes auf richtige Übermittlung hin überprüft wurden. Die Studie selbst stellt darüber hinaus fest, dass das bloße Wissen über diese Funktionalität ausreicht, um das Vertrauen in die Technologie zu steigern. [17]
Am Wahltag um 18 Uhr durchlaufen die Stimmen einen dreistufigen Prozesse der Anonymisierung und Auszählung. Im ersten Schritt werden alle Stimmen noch einmal mittels des Zeitstempels und der digitalen Signatur hin überprüft. Es werden dabei beispielsweise Stimmen gelöscht, bei denn die Person nicht mit ihrer digitalen Unterschrift übereinstimmt. Im zweiten Schritt werden alle doppelten Stimmen eines:einer Wähler:in gelöscht. Im dritten und letzten Schritt werden alle Stimmen dem jeweiligen Wahlbezirk zugeordnet und anonymisiert, so dass am Ende nicht mehr nachvollzogen werden kann, wer wie gewählt hat. Ein optionaler vierter Schritt kann angewendet werden, um die Stimmen zu mischen, um noch einmal die Anonymisierung zu erhöhen. Zu diesem Zeitpunkt sind die Stimmen trotz alledem immer noch verschlüsselt. Zu Entschlüsselung und eigentlichen Auszählung der Stimmen wird der private key benötigt. Teile dieses Schlüssels wurde vor der Wahl an unterschiedliche Akteure verteilt, beispielsweise Parteien oder Wahlbeobachter:innen. Nur wenn alle Akteure ihren Teil zum private key beisteuern, können die Stimmen überhaupt ausgezählt werden. Nach der Entschlüsselung aller Stimmen, wird der private key unbrauchbar. [18] [16]
Nachdem das offizielle Wahlergebnis bekannt gegeben wurde, werden alle private keys vernichtet und die Stimmen damit unbrauchbar. Daraufhin werden alle Stimmen gelöscht, „*da das estnische Wahlrecht die Vernichtung sämtlicher ‚Stimmzettel' verlangt*" [16].

Kritik am i-Voting

Ein Kritikpunkt ist der Umgang mit den ausgezählten Online-Stimmen. Diese werden, wie bereits erwähnt, nach der amtlichen Bekanntgabe des Wahlergebnisses gelöscht. Dieser Punkt verhindert eine spätere, erneute Auszählung der Stimmen. Somit kann etwaige Wahlfälschungen nicht aufgedeckt werden. Dies stellt auch gleichzeitig eine Kritik am estnischen Wahlrecht allgemein dar. [16] [20]
Weiterhin wird kritisiert, dass die Wähler:innen nur schwer nachvollziehen können, ob ihre Daten tatsächlich nicht mit ihrer Stimme in Verbindung gebracht werden können. Infolgedessen, könnte die Geheimhaltung der Wahl verletzt sein. Darüber hinaus ist die Software der Voter-Application zwar frei und öffentlich verfügbar und jede wahl-

berechtigte Person kann diese einsehen, allerdings ist bei der eigentlichen Wahl nicht ersichtlich, welche Version der Voter-Application aktuell auf den Servern läuft. Bisher sind noch keine realen Angriffe auf das estnische i-Voting bekannt. Somit kann im Allgemeinen davon ausgegangen werden, dass die Online-Wahl genauso sicher ist, wie beispielsweise eine Briefwahl. [16] [20]
Der Chef der Kriseneinsatzgruppe in Estlands staatlicher Behörde für Informationssysteme, Tõnu Tammer, bekräftigt die Vorteile des i-Votings. Er meint, dass diese Art zu wählen, sogar sicherer sei, als in ein Wahllokal zu gehen: „*Denn wenn Sie in ein Wahlbüro gehen, fragen die Wahlhelfer(:innen) dort nach Ihrem Ausweis und überprüfen anhand dessen Ihre Identität – obwohl sie nicht dafür ausgebildet sind, Dokumentenfälschungen zu erkennen*“ [12].
Abschließend lässt sich festhalten, dass i-Voting sicher ist und die wichtige Partizipation am politisch demokratischen Prozess nicht einschränkt sondern verbessert. Es ist eine echte Alternative in einer zunehmend digitalisierten Welt.

3.2 Deutschlands „Vorratsdatenspeicherung“

In einem modernen Rechtsstaat, wie es die Bundesrepublik Deutschland ist, sollten Straftaten, Terroranschläge und ähnliches möglichst frühzeitig erkannt werden. Dies ist einer der Gründe warum die Vorratsdatenspeicherung eingeführt werden soll.

> *„Der Begriff ‚Vorratsdatenspeicherung‘ wird synonym für die anlassunabhängige Speicherung von Telekommunikationsdaten für Strafverfolgungs- und Gefahrenabwehrzwecke gebraucht. Dabei werden sämtliche Bestands-, Verkehrsdaten und Standortdaten durch einen Telekommunikationsdiensteanbieter über einen vorher bestimmten Zeitraum für einen eventuellen späteren staatlichen Zugriff auf diese Daten vorgehalten.“* [27]

Dabei meint der Begriff Verkehrsdaten, jene Daten, „*die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden*“ [§ 3 Nr. 30 TKG].
Im Folgenden sollen die Entwicklungen in Deutschland aufgezeigt werden. Hierzu wird sich an die Einteilung der Ereignisse, wie in einem Artikel des Bundesbeauftragen für Datenschutz und Informationsfreiheit [21] geschildert werden.

3.2.1 Vorratsdatenspeicherung 1.0

In Folge einer Reihe von Anschlägen, beispielsweise der vom 11. September 2001 in New York, wurde der Ruf nach der Speicherung der Verkehrsdaten immer lauter. Im Jahr 2006 verabschiedete das Europäische Parlament und der Europäische Rat eine Richtlinie „*über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden*“ [2006/24/EG]. Mit dieser Richtlinie werden alle Mitgliedsstaat der Europäischen Union dazu aufgefordert, ein entsprechendes Gesetz auf den Weg zu bringen. Daraufhin hat der Deutsche Bundestag, im Jahr 2007, ein „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ auf den Weg gebracht. Dieses trat am 1. Januar 2008 in Kraft und ergänzt das Telekommunikationsgesetz um die Paragraphen 113a und 113b. In §113a werden speziell die „*Speicherungspflichten für Daten*“ [§113a TKG i.d.F.v. 1.01.2008] eingeführt und in §113b die „*Verwendung der nach §113a gespeicherten Daten*“ [§113b TKG i.d.F.v. 1.01.2008]. Darin wird festgelegt, dass die Provider und Telekommunikationsdienste, die Verkehrsdaten ihrer Nutzer:innen für sechs Monate speichern müssen, um diese Daten im Bedarfsfall den Strafverfolgungsbehörden und Nachrichtendiensten zugänglich zu machen. [21] [22]

Bei einem Telefonat werden hierzu die Telefonnummern, der Zeitpunkt des Gesprächsbeginns, die Dauer des Gesprächs, die Seriennummer der Telefone sowie der SIM-Karten und die Funkzellen, in der sich jeweils beide Anrufenden befanden, gespeichert. Bei SMS- und MMS-Nachrichten mussten auf Grund von technischen Grenzen bei der Trennung von Inhalt und Verkehrsdaten auch die Inhalte dieser Nachrichten mit gespeichert werden. Auch der E-Mail-Verkehr samt IP-Adresse ist von der Speicherung betroffen. [21] [26]

Schon bei der Einführung dieses Gesetzte gab es Kritik von allen Seiten, beispielsweise, sagt der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit in einer Stellungnahme, dass die Speicherung unverhältnismäßig und verfassungswidrig sei. Weiter heißt es: „*Durch die anlasslose Speicherung aller Telefon-, E-Mail- und Internet-Verkehrsdaten für ein halbes Jahr wurde das gesamte Telekommunikationsverhalten aller Bundesbürgerinnen und Bundesbürger erfasst*“ [21]. Weiterhin gab es auch Bedenken der Machbarkeit in der Praxis und auch des allgemeinen Nutzens. Einer Studie des Bundeskriminalamtes zu Folge brächte die Vorratsdatenspeicherung nur eine 0,006 prozentige Steigerung der Aufklärungsquote. [21] [28]

Daraufhin kam es zu zahlreichen Verfassungsbeschwerden beim Bundesverfassungs-

gericht in Karlsruhe. 2010 erkläre das Gericht, das Gesetz von 2008 und die damit einhergehenden Änderungen im Telekommunikationsgesetzes für verfassungswidrig. Im Urteil[7], vom 2. März 2010, heißt es, das Gesetz verstößt gegen das, in Artikel 10 Absatz 1 des Grundgesetzes festgeschriebene, Brief-, Post- und Fernmeldegeheimnis. „*Das Gericht führte in diesem Zusammenhang allerdings aus, dass eine anlasslose Speicherung von personenbezogenen Daten über einen Zeitraum von sechs Monaten auf Vorrat lediglich dann strikt verboten sei, wenn sie zu unbestimmten und noch nicht bestimmbaren Zwecken erfolgte*“ [21]. An dieser Stelle ist festzuhalten, dass das Gericht ausschließlich die verdachtsunabhängige Speicherung der Verkehrsdaten für verfassungswidrig hält. Eine Speicherung von Daten, beispielsweise in einem Ermittlungsverfahren ist demnach immer noch möglich – natürlich unter der Voraussetzung gesetzlicher Regelungen. Dabei muss ein hohes Maß an Datensicherheit geschaffen werden. Weiterhin muss die Speicherung transparent für die Bürger:innen sein und gleichzeitig ein effektiver Rechtsschutz gewährleistet werden. Darüber hinaus muss auch eine entsprechende Regelung zum Umfang der Datenverwendung geschaffen werden. Somit darf es nach Ansicht des Gerichtes, nicht möglich sein, ein exaktes Bewegungsprofil der Bürger:innen zu erstellen. [21] [27] [26]

Nach dem Scheitern des Gesetzes vor dem Bundesverfassungsgericht, wurde 2014 das Inkrafttreten der maßgeblichen europäischen Richtlinie 2006/24/EG rückwirkend, durch den Europäischen Gerichtshof, für nichtig erklärt. Auch die Richter:innen des Europäischen Gerichtshof, sehen den Eingriff in das Privatleben der Bürger:innen als unverhältnismäßig an. In der Urteilsbegründung werden vier wesentliche Punkte aufgemacht: Erstens die Speicherung von allen Verkehrsdaten kann nicht im Zusammenhang mit der Bekämpfung einzelner Straftaten stehen. Somit kann es dadurch zur unbegrenzten Speicherung, auch zur Sicherung von Betriebs- oder gar Staatsgeheimnissen, kommen. Zweitens fehle die Begutachtung der Herausgabe der Daten durch ein Gericht oder andere staatlich unabhängige Stellen. Einer gewissenhaften Nutzung der Daten kann somit nicht gerecht werden. Drittens wird bemängelt, dass in der Richtlinie nicht unter verschiedenen Speicherdauern differenziert wird – jegliche Daten werden in einem festen Rahmen gespeichert. Als vierten und letzte Punkt bemerkten die Richter:innen, dass die Datensicherheit kaum eine Rolle spiele. Darüber hinaus gibt es keine Regelung zum Speicherort der Daten. Diese könnten weltweit gespeichert werden und so könnten die Datenschutzbestimmungen der Europäischen Union nicht mehr eingehalten wer-

[7] zu finden unter: `https://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html` (abgerufen am: 18.08.2021)

den. [21] [27]
Nach gut sieben Jahren endet damit der erste Versuch der Einführung einer Vorratsdatenspeicherung. Die Europäische Kommission hat, auf Grund der Entscheidung des Europäischen Gerichtshof, den Versuch einer Einführung fürs Erste auf Eis gelegt.

3.2.2 Vorratsdatenspeicherung 2.0

Entgegen der Einstellung des Vorhabens zur Einführung einer Vorratsdatenspeicherung auf Europäischer Ebene, wagt die Bundesregierung im Jahr 2015 einen neuen Versuch und bringt das „Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten“ auf den Weg. Auch dieses Gesetz erlaubt das anlasslose Speichern von Verkehrsdaten. Im Zuge der Einführung dieses Gesetzes wurden die Paragraphen 113a und 113b des Telekommunikationsgesetzes aus dem Jahr 2008 wieder entfernt und durch eine Reihe neuer beziehungsweise überarbeiteter Normen ersetzt. Beispielsweise wird in §113c die „Verwendung der Daten“ und in §113g das „Sicherheitskonzept“ geregelt. Im Vergleich zu der Novellierung 2008, ist die wesentlichste Änderung die, dass die Verkehrsdaten nicht mehr pauschal sechs Monate gespeichert werden müssen. Standortdaten müssen jetzt vier Wochen gespeichert werden und die übrigen Verkehrsdaten zehn Wochen. Weiterhin wurde die Speicherungspflicht von E-Mail-Daten wieder aufgehoben. [21] [26]
Eine weitere nicht unwesentliche Änderung betrifft die Verwendung der Vorratsdatenspeicherung bei Ermittlungsverfahren. Hierzu wurde §100g „Erhebung von Verkehrsdaten“ in die Strafprozessordnung mit aufgenommen. Diese erlaubt es bei bestimmten Straftaten, wie Mord oder Sportwettenbetrug, mit richterlichem Beschluss, auf die Verkehrsdaten der Verdächtigen zuzugreifen. [§100g StPO] [26]
Auch dieses Gesetz steht wieder in der Kritik, vor allem Datenschützer:innen sehen darin einen erheblichen Eingriff in die Privatsphäre. Weiterhin steht auch die Diskussion über die Vereinbarkeit mit dem Grundgesetz im Raum und der Schutz von Berufs- und Betriebsgeheimnissen, auch wenn diese Daten durch Ermittlungsbehörden nicht genutzt werden können beziehungsweise dürfen. [21] [27] [26]
2016 beschäftigte sich der europäische Gerichtshof erneut mit der Vorratsdatenspeicherung. Geklagt wurde gegen die Umsetzung in Schweden und Großbritannien, da diese, der bereits für unzulässig erklärten Richtlinie 2006/24/EG, entsprachen. In seinem Urteil bekräftigt das Gericht, seine Entscheidung aus dem Jahr 2014. Die anlasslose Speicherung von Verkehrs- und Standortdaten ist nicht mit Grundrechten der Europäischen Union vereinbar, da sie beispielsweise die Achtung des Privatlebens oder auch

die freie Meinungsäußerung verletzt. [22] [21]
Bei einem Treffen der Europäischen Innen- und Justizminister in Estland 2017, wurde der Entschluss gefasst, die Vorratsdatenspeicherung noch einmal zu prüfen und eine für Europa einheitliche Regelung auf den Weg zu bringen. [23]
2017 entschied das Oberverwaltungsgericht in Münster zu Gunsten eines Telekommunikationsunternehmens. Dieses hatte auf Rechtsschutz geklagt, wenn es die Vorratsdatenspeicherung nicht durchführen sollte. Daraufhin setzte die Bundesnetzagentur die Vorratsdatenspeicherung, die am 1. Juli 2017 in Kraft treten sollte, aus. Damit müssen die Telekommunikationsunternehmen und -anbieter in Deutschland keine Daten ihrer Kundinnen und Kunden speichern. In einem weiteren Urteil vom Verwaltungsgericht in Köln, wird unter Bekräftigung des Urteils aus Münster, auf die europäische Rechtsprechung verwiesen. [22]

3.2.3 Vorratsdatenspeicherung aktuell und Ausblick

Auch 2020 beschäftigt das Thema Vorratsdatenspeicherung die Politik und die Gerichte noch immer. Die aktuellen Gesetzesvorlage der Bundesregierung sehen eine Speicherung dennoch vor. Im Juli 2020 wirbt der amtierende Innenminister, Horst Seehofer, für eine sofortige Anpassung der Gesetze. Er sieht dabei vor allem ein effektives Mittel in der Verfolgung von Kindesmissbrauch. Hierzu plädiert er für eine längere Speicherung von IP-Adressen. Dabei ist die Abwehr von potentiellen Terrorangriffen kein Thema mehr. Im Oktober 2020 urteilt der Europäische Gerichtshof abermals, dass eine „*anlasslose und pauschale Vorratsdatenspeicherung von Verkehrs- und Standortdaten, die dokumentieren, wer mit wem, wann, wie lange und von wo aus telefoniert hat*“ [22] nicht zulässig sei. Allerdings stellt das Gericht klar, dass dies ein adäquates Mittel zur Straftatenbekämpfung wäre. Weiterhin dürfen die europäischen Staaten jetzt anlasslos IP-Adressen speichern. [24] [22]
Trotz der großen Kritik und jahrelangen Debatte um das Thema Vorratsdatenspeicherung ist kein Ende in Sicht und das, obwohl eine Studie[8] des Max-Planck-Instituts für ausländisches und internationales Strafrecht, bereits 2011 zu dem Schluss kam, dass die Speicherung auf Vorrat keinen Mehrwert zur Verbrechensaufklärung beiträgt. Damit ist die Forderung der Politik nach einem solchen Verfahren unbegründet. [25]
Auch in den kommenden Jahren wird die Vorratsdatenspeicherung weiter die Politik

[8] „Schutzlücken durch Wegfall der Vorratsdatenspeicherung?“ ist abrufbar unter: `https://csl.mpg.de/de/forschung/projekte/schutzluecken-durch-wegfall-der-vorratsdatenspeicherung` (abgerufen am: 20.08.2021)

und Gerichte beschäftigen. Allerdings wird voraussichtlich auch in Deutschland eine anlasslose Speicherung der Verkehrsdaten gerichtlich nie standhalten.

4 Einsatz digitaler Technologien in Autokratien

Hier soll nun an einigen Beispielen der Einsatz der in Abschnitt 4 beschriebenen digitalen Technologien in autokratischen Staaten aufgezeigt werden.

4.1 Chinas „Große Firewall“

Das Projekt „Goldener Schild“, oft auch „Große Firewall von China“ genannt, ist ein Projekt aus legislativen und technologischen Maßnahmen, das hauptsächlich von der CAC[9], der zentralen Behörde Chinas für alle das Internet und Computernetzwerke betreffenden Angelegenheiten, betrieben wird. Seine grundsätzliche Aufgabe besteht darin, den Internetverkehr in China zu regulieren und zu überwachen, sowie den Zugriff auf ausgewählte ausländische Internetdienste zu behindern. Ein nicht geringer Teil der Zensurmaßnahmen wird von Unternehmen, v.a. in vorauseilender Selbstzensur, umgesetzt. Im Folgenden soll jedoch der Fokus auf die von staatlichen Stellen umgesetzten Maßnahmen gelegt werden [29] [30] [31] [32].

4.1.1 Hintergrundgeschichte und Ziele

In einem Artikel im Magazin Public Choice aus dem Jahr 2008 beschreibt Rebecca MacKinnon, Journalistin und Aktivistin für Internetfreiheit, das Internet als ein weiteres Feld der zentralen Herausforderung für Chinas Regierung, Öffnung mit Kontrolle auszubalancieren, welche mit Deng Xiaopings[10] Reform- und Öffnungspolitik im Jahr 1979 begann. So wurde China für den Handel mit dem Ausland, v.a. dem Westen, geöffnet, und Chines:innen durften dort auch studieren, allerdings sollte dieser Prozess stets kontrolliert ablaufen, u.a. durch wirtschaftliche Anreize sowie polizeilichen Zwang. Dies sollte verhindern, dass durch den kommerziellen auch ein politischer Wandel ausgelöst wird. Ein Lieblingssprichtwort Xiaopings in den frühen 1980er Jahren war: „*Öffnet man das Fenster, um frische Luft hereinzulassen, ist zu erwarten, dass einige Fliegen hereingeweht werden*“ [33] [32].
1994 erreichte das Internet China, und die Regierung hatte keine andere Wahl, als auch dieses „Fenster“ zu öffnen, womit es zu einer weiteren Ebene des ideologischen Kampfes gegen Gegner der Regierung wurde. In einem Leitartikel der Redaktion des People’s Daily[11] von 2005 wird diese Sichtweise sehr gut auf den Punkt gebracht. Darin wird

[9] kurz für: Cyberspace Administration of China
[10] machtvollster Politiker der chinesischen Regierung von 1978 bis 1997
[11] Parteiorgan der KPCh (Kommunistischen Partei Chinas), eine der größten chinesischen Zeitungen

beschrieben, dass, solange nur das Gute des Internets genutzt werde und das Schlechte vermieden werde, dieses gegen den Westen genutzt werden könne. Es wird ein Vergleich zum Koreakrieg[12] gezogen und prophezeit, dass China in einem „großen Internet-Krieg“ nicht besiegt werden würde [32] [34].
Legislative Regulierungen des Internets begannen mit dem freien Verfügbarwerden des Internets in China im Jahr 1994. Am 18. Februar 1994 erließ der chinesische Staatsrat[13] die „Verordnung über den Schutz von Computerinformationssystemen“, in der „gesetzliche Haftung“ für fünf verschiedene Tatbestände vorgeschrieben wurde. Dies waren: Die Verletzung von Schutzsystemen von Computerinformationssystemen und deren Bedrohung; die Verletzung des Registrierungssystems für Computerinformationssysteme in internationalen Netzwerken; das Nichtmelden von Vorfällen in Computerinformationssystemen im vorgeschriebenen Zeitraum; Verweigerung der Verbesserung von Sicherheitsvorkehrungen nach einer Benachrichtigung durch die Behörde für öffentliche Sicherheit, in der solche eine Verbesserung vorgeschrieben wird; und schließlich andere Computerinformationssysteme bedrohende Handlungen. Das chinesische Strafrecht dagegen hatte seine letzte größere Aktualisierung 1979 erfahren und umfasste damit zu diesem Zeitpunkt noch keine Bestimmungen für Verbrechen im Zusammenhang mit Computersystemen oder dem Internet. Dies änderte sich erst 1997, als der Nationale Volkskongress[14] das Gesetz CL97[15], eine Aktualisierung des chinesischen Strafrechts, verabschiedete, die die Artikel 285, 286 und 287 einführte. Damit wurden u.a. das unrechtmäßige Eindringen in Computerinformationssysteme (Art. 285), die Beschädigung oder Zerstörung von Computerinformationssystemen (Art. 286) und das Ausüben von Verbrechen mittels Computern (Art. 287) unter Strafe gestellt [35] [36] [37].
Nach der Verabschiedung von CL97 war es Aufgabe des chinesischen Staatsrats, zu entscheiden, welche Handlungen unter die im Gesetz beschriebenen Tatbestände fallen. Er legte fest, dass die in CL97 festgelegten Tatbestände auch Handlungen wie die Verbreitung von Informationen, die als „schädlich für die nationale Sicherheit“ eingestuft werden, umfassen, sowie die Verbreitung von Informationen, die „*schädlich für die öffentliche Ordnung, soziale Stabilität, und chinesische Moralvorstellungen*“ sind. Der letzte Tatbestand aus Artikel 287 von CL97 (Verbrechen, die mittels Computern verübt werden), diente der Regierung dann auch als Rechtfertigung für das Projekt der „Großen Firewall“ [37].

[12] 1950 bis 1953, chinesische Truppen kamen Nordkorea zu Hilfe gegen US-geführte UNO-Truppen
[13] höchstes Verwaltungsorgan der Volksrepublik China
[14] Legislative der Regierung der Volksrepublik China
[15] kurz für: Criminal Law 1997

Die Nachrichtenagentur Xinhua[16] veröffentliche am 20. September 2000 ein Dokument des chinesischen Staatsrates mit dem Titel: „Maßnahmen zur Verwaltung von Internet-Informationsdiensten“. Darin ist u.a. eine Lizenzierungspflicht für kommerzielle und eine Registrierungspflicht für nicht-kommerzielle „Internet-Informationsanbieter“ vorgeschrieben (Art. 4). Auch enthalten ist die Bestimmung, dass Anbieter von „Internet-Informationsdiensten“ und ISPs[17] Nutzerdaten erheben und speichern müssen. Auch sind sie verpflichtet, diese Informationen Regierungsbehörden gemäß gesetzlichen Bestimmungen zugänglich zu machen (Art. 14) [38].
Der wichtigste Teil des Dokuments, Artikel 15, umfasst neun Arten von Informationen, deren Verbreitung im Internet nicht erlaubt ist. Dazu zählen u.a.: Informationen, die Verfassungsgrundsätzen gegenüberstehen (Art. 15 i); solche, die die nationale Sicherheit gefährden, Staatsgeheimnisse verbreiten, die Macht des Staates untergraben, oder „die Integrität der nationalen Einheit“ gefährden (Art. 15 ii); solche, die Gerüchte verbreiten, die soziale Ordnung oder die soziale Stabilität stören (Art. 15 vi) [38].
Dieses Dokument, v.a. Artikel 15, gilt als Blaupause für die Ziele der chinesischen Internet-Zensur. Damit zielt das Projekt v.a. darauf ab, die von Rebecca MacKinnon benannte Kontrolle zu wahren, über den öffentlichen Diskurs in China, und damit die Wahrung sozialer Stabilität (wie von der Regierung interpretiert). Und wohl auch darauf, zu erreichen, dass die Chines:innen bevorzugt chinesische Internetdienste nutzen, die direkt von den chinesischen Behörden reguliert werden [40] [45].
Daneben wird aber auch vermutet, es gehe bei den Zensurmaßnahmen, v.a. bei solchen wie der Überwachung von VPNs[18], auch darum, Daten ausländischer Firmen, die in China aktiv sind, abzugreifen, also um Wirtschaftsspionage, wobei es dafür keine handfesten Beweise gibt [39].

4.1.2 Technische Hintergründe und Methoden zum Umgehen der Zensurmaßnahmen

In der Anfangszeit waren westliche, v.a. nordamerikanische Firmen wie bspw. Cisco Systems[19] in die Entwicklung der unter dem Schirm der „Großen Firewall“ entwickelten Projekte und Zensurmethoden involviert. Mit zunehmender Entwicklung der einheimischen chinesischen Internetwirtschaft wurden ausländische Unternehmen mehr und

[16] Nachrichtenagentur der Regierung der Volksrepublik China
[17] kurz für: Internet Service Providers, Anbieter von Internetzugängen
[18] kurz für: Virtual Private Networks, geschützte Netzwerkverbindung unter Nutzung öffentlicher Netzwerke
[19] US-amerikanisches Unternehmen, spezialisiert auf Netzwerkinfrastruktur

mehr aus den Projekten entfernt. Mittlerweile stellen inländische Firmen, darunter v.a. Huawei, den Großteil der Hardware (bspw. Router) bereit [50] [51].
Technisch besteht der Hauptzweck der Großen Firewall darin, Inhalte selektiv zu filtern, v.a. beim Zugriff auf im Ausland befindliche Internetdienste. Dazu werden mehrere technische Methoden eingesetzt. Diese Filterung wird dabei durch den Umstand vereinfacht, dass sämtlicher Internetverkehr zwischen China und dem Rest der Welt über Glasfaserkabel läuft, die das Land an einem vor nur zehn existenten Zugangspunkten erreichen. Auch müssen sich alle ISPs im Land beim Ministerium für Industrie und Informationstechnologie registrieren und erhalten von diesem ihre Betriebslizenz. Dies macht es den chinesischen Behörden wesentlich leichter, den Internetverkehr zu analysieren und, wenn gewünscht, auch zu manipulieren [46].

TCP-Reset-Angriffe mit DPI

Eine der Methoden ist das Einsetzen sogenannter TCP[20]-Reset-Angriffe in Verbindung mit Deep Packet Inspection (DPI)[21], bei denen TCP-Reset-Pakete[22] an beide Kommunikationsendpunkte (i.d.R. Client und Webserver) verschickt werden. Wie Young Xu in einem Artikel bei Thousand Eyes[23] darlegt, nutzt diese Methode Komponenten eines Intrusion Detection System (IDS)[24], um zu erkennen, ob verschickte Datenpakete die Filterungsregeln der Regierung verletzen. Dabei werden durch filternde Router (hauptsächlich die Router, die den Datenverkehr zwischen China und dem Rest der Welt bearbeiten) Kopien durchlaufender Datenpakete an von der Verbindung abgekoppelte Geräte geliefert, die auf der benannten IDS-Technologie basieren. Die verschickten Datenpakete können ihren Weg zunächst ungehindert fortsetzen, während ihre Kopien analysiert werden, um ihren Inhalt, inkl. Quell-URL, auf zu blockierende Schlüsselworte zu prüfen. Die Firewall ist auch in der Lage, IP-Fragmente und TCP-Segmente[25] für HTTP[26]-Verbindungen für die Prüfung wieder zusammenzusetzen, was durch das Aufrechterhalten des Verbindungszustandes erreicht wird. Dies ist eine mächtige Funktionalität, über die viele Zensursysteme nicht verfügen [47] [48] [46].
Stellen die IDS-basierten Prüfungsgeräte fest, dass die Datenpakete unerwünschte Inhalte enthalten und damit die Verbindung zwischen Client und Webserver zu blockieren

[20] kurz für: Transmission Control Protocl
[21] Untersuchung des Inhalts verschickter Datenpakete
[22] TCP-Pakete mit dem Zweck, eine Verbindung abzubrechen
[23] Network-Intelligence Unternehmen, das auf Tools zur Netzwerkanalyse spezialisiert ist
[24] System zur Erkennung von Angriffen auf Computernetzwerke
[25] Datenpakete im Rahmen von IP bzw. TCP
[26] kurz für: Hypertext Transfer Protocol

ist, werden durch einen der vorhin benannten Router gefälschte TCP-Pakete, die TCP-Reset-Pakete, in die Verbindung zwischen den Kommunikationsendpunkten eingefügt, sodass sie beide Endpunkte erreichen und die Verbindung damit abbrechen. In einer Forschungsarbeit haben drei Forscher der Universität Cambridge aufgezeigt, dass auch nach Abbruch dieser Verbindung alle weiteren Verbindungsversuche zwischen den gleichen Kommunikationsendpunkten automatisch blockiert werden, was durch das Einfügen weiterer TCP-Reset-Pakete in die Verbindung zwischen ihnen geschieht. Dazu werden die IP-Adressen der Endpunkte, Port-Nummern (wobei dies auf ähnliche Port-Nummern beschränkt ist) sowie die verwendeten Protokolle gesperrter Anfragen zur Erkennung weiterer Verbindungsversuche genutzt [47] [46].
In ihrer Arbeit haben sie auch dargelegt, wie es möglich ist, diese Methode der Zensur zu umgehen, indem die von der Firewall verschickten TCP-Reset-Pakete ignoriert werden. Dies liegt daran, dass diese von der Firewall implementierte Methode sich auf eine dem Standard entsprechende TCP-Implementierung an den Kommunikationsendpunkten verlässt, diese also beim Erhalt eines Reset-Pakets die TCP-Verbindung abbrechen. Werden nun beide Endpunkte so eingestellt, dass sie TCP-Reset-Pakete ignorieren, ist es möglich, auch Inhalte zu empfangen, die von der Firewall normalerweise mittels TCP-Reset-Angriffen blockiert werden, wobei die Firewall aufgrund des nicht erfolgenden Verbindungsabbruchs viele gefälschte Reset-Pakete versendet. Auch ist es möglich, durch eine Verschlüsselung der versendeten Daten die Prüfung und damit den Verbindungsabbruch durch gefälschte Reset-Pakete zu umgehen. Beide Varianten haben den Nachteil, dass häufig die Installation spezieller Software o.ä. erforderlich ist. Wenn chinesische Behörden nun derartigen Datenverkehr feststellen, könnten sie einen der Kommunikationsendpunkte aufspüren (anhand bspw. der IP-Adresse) und besuchen, wobei das Vorhandensein spezieller Software schwerwiegende Konsequenzen haben könnte [47].

IP-Sperren

Das Sperren bestimmter IP-Adressen oder Adressbereiche ist eine kostengünstige und einfach umzusetzende Zensurmaßnahme. Dazu wird lediglich eine Liste zu sperrender IP-Adressen oder Adressbereiche angelegt. Router, die den Datenverkehr weiterleiten, werden dann dazu veranlasst, sämtliche für diese gesperrten IP-Adressen bestimmten Datenpakete zu verwerfen. In der Implementierung der Großen Firewall wird eine Blacklist mittels Null Routing in die Router aller chinesischen ISPs, die für Datenver-

kehr mit dem Rest der Welt zuständig sind, eingebaut. Dies erfolgt mittels BGP[27]. Sogenannte „Null-Routen“ werden für alle gesperrten IP-Adressen ins Netzwerk eingefügt, was Router zwingt, für diese IPs bestimmte Datenpakete zu verwerfen. Obwohl dieses Null Routing nur aus China ausgehenden Datenverkehr blockiert, ist dies meist ausreichend, um Websites zu sperren, da die meiste Kommunikation über das Internet Interaktionen beider Kommunikationsteilnehmern erfordert [46] [52].
Diese Methode ist kostengünstig und leicht einzusetzen, und erfordert kaum Beteiligung der ISPs oder zusätzliche Ressourcen. Allerdings hat diese Methode einige Probleme. So muss die Liste von IP-Adressen aktuell gehalten werden, was aufgrund der Üblichkeit des Wechsels von IP-Adressen durch Diensteanbieter, die diese Sperren umgehen wollen, aufwändig ist. Auch können sich die „Null-Routen“ auf benachbarte Länder auswirken. Und auch ein „Zu-viel-Sperren“ ist möglich, aufgrund der Teilung von IP-Adressen und -Adressbereichen können auch nicht zu sperrende Seiten von Sperren betroffen sein [46].

DNS-Manipulationen

Häufig in Kombination mit dem eben beschriebenen Sperren von IP-Adressen werden auch verschiedene DNS-Manipulationen eingesetzt, wie DNS-Poisoning, -Tampering, -Injection. Diese Begriffe beschreiben grundsätzlich alle eine ähnliche Methode. Es geht darum, gefälschte Antworten auf DNS-Anfragen von Nutzern zurückzuliefern. DNS-Tampering beinhaltet die Fälschung der vom DNS-Server gelieferten Antwort auf eine DNS-Anfrage. Dies kann auf mehreren Wegen geschehen: Der Server kann eine falsche IP-Adresse zurückliefern, durch gewollte Fehlkonfiguration oder DNS-Poisoning (Einfügen fehlerhafter DNS-Einträge im Cache des DNS-Servers). Auch kann er falsche Auskünfte geben über mit dem Domainnamen assoziierte CNAMEs (Zuordnung eines primären Namens zu weiteren Domainnamen), über die weiteren anzusteuernden Server für die Auflösung der DNS-Anfrage, und über die Existenz des Domainnamen selbst. Dadurch erhalten Nutzer falsche DNS-Antworten zu zensierten Seiten. Durch diese Taktik, verbunden mit IP-Sperren, können Websites und Webserver auf Level der Domainnamen und IP-Adressen gesperrt werden [49] [46].
Eine weitere Methode ist die DNS-Injection. Dabei werden, enthält eine DNS-Anfrage ein gesperrtes Schlüsselwort, gefälschte DNS-Antworten in die Verbindung injiziert und zu den Nutzer:innen zurückgeschickt, wobei diese vor der korrekten DNS-Antwort eintreffen und der Zugriff auf die gesperrte Website verhindert wird. Dies betrifft nicht

[27] kurz für: Border Gateway Protocol, Protokoll für Routing über Autonome Systeme hinweg

nur Anfrage an chinesische DNS-Server, sondern auch Anfragen an solche außerhalb Chinas. Diese DNS-basierte Zensur findet nach Forschungsergebnissen fast ausschließlich in den Internetknotenpunkten an Chinas Grenze statt. Die ersten Berichte des Einsatzes dieser speziellen Methoden datieren auf das Jahr 2002. Während der chinesischen Zensurapparat aktiv nach neuen zu sperrenden Domains suchen, findet ein Entsperren blockierter Domains kaum statt. Eine Forschungsarbeit aus dem Jahr 2014 fand heraus, dass (Stand damals) zwei Drittel der gesperrten Domainnamen abgelaufene Registrierungen aufwiesen [49] [46].
Diese DNS-Manipulationen haben aber auch unerwünschte Nebeneffekte. Da die DNS-Injection der Großen Firewall nicht zwischen in das Land ein- und aus dem Land ausgehendem Verkehr unterscheidet, werden auch nicht-zensierte Netzwerke betroffen, wenn DNS-Verkehr durch das chinesische Internet läuft. Dies tritt u.a. dann auf, wenn Server, die DNS-Anfragen auflösen, Nameserver von TLDs[28] anfragen und der Datenverkehr durch China verläuft. Ein Beispiel dafür ist eine Anfrage eines US-amerikanischen Nutzers an eine in China gesperrte deutsche .de-Domain. Dabei löst dann ein DNS-Server in den USA diese DNS-Anfrage auf und kontaktiert den Nameserver für die TLD .de. Wenn der Weg zu diesem Nameserver China passiert, injiziert die Große Firewall eine gefälschte DNS-Antwort, die vom US-amerikanischen Server aufgenommen, gecacht und an den Nutzer zurückgegeben wird, womit der Zugriff auf die .de-Seite verhindert wird. Die TLD .de ist einer der am meisten davon betroffenen TLDs [46] [53].
Um diese DNS-Manipulationen zu umgehen, gibt es mehrere mögliche Methoden. Eine nutzt aus, dass bei der DNS-Injection zwar gefälschte DNS-Antworten injiziert werden, die korrekten DNS-Antworten aber nicht abgefangen werden. Dabei sollte nicht die erste ankommende DNS-Antwort genutzt werden, sondern erst eine sinnvolle Zeit abgewartet werden. Dann sollten die Antworten ausgefiltert werden, die von IP-Adressen kommen, die als solche identifiziert wurden, die von der Großen Firewall zum Verschicken gefälschter DNS-Antworten genutzt werden (bspw. IPv6-Subnetz 2001::/32). Dabei ist aber zu beachten, dass bekannte öffentliche DNS-Server wie Google Public DNS nicht vollständig vor DNS-Poisoning geschützt sind, für diese Umgehungsmethode also nicht geeignet sind. Genutzt werden sollten stattdessen die Authorative Name Servers[29]. Eine andere Methode zum Umgehen der DNS-Manipulationen ist die Nutzung von DNSSEC[30]. Dies ist eine Erweiterung für DNS, die es erlaubt, die Gültigkeit und

[28] kurz für: Top-Level-Domains, letzter Abschnitt eines Domainnamens und höchste Ebene der Domainnamen-Auflösung, bspw. .de, .com
[29] für eine sogenannte Zone (bspw. eine TLD) verantwortliche Nameserver
[30] kurz für: Domain Name System Security Extensions

Korrektheit von DNS-Antworten zu verifizieren. DNSSEC sichert den Pfad zwischen Clients und DNS-Servern ab, sodass keine gefälschten DNS-Antworten eingeschleust werden können. Technische Komplikationen und Kompatibilitätsprobleme haben eine verbreitete Implementation von DNSSEC bisher verhindert [55] [56] [57].

Weitere Methoden zum Umgehen der Großen Firewall

Die am weitesten etablierten Werkzeuge zum Umgehen von Zensurmaßnahmen, VPNs und SSH[31]-Tunnel, sind auch zum Umgehen der Großen Firewall im Einsatz und sind die mächtigsten und stabilsten zu diesem Zweck genutzten Tools. Kommerzielle und öffentliche VPN-Anbieter werden jedoch auf Ebene der Domainnamen und/oder IP-Adressen blockiert, sofern sie bekannt genug sind, so sind bspw. alle *vpn.*-Domainnamen gesperrt. Tor war einige Zeit lang auch ein viel genutztes Mittel, v.a. aufgrund seiner komplexen Verschlüsselung und Vielzahl von Proxys. Allerdings war der zentrale Server, von dem Nutzer:innen eine Liste der Proxyknoten erhielten, die große Schwachstelle. Nachdem die IP-Adresse von Tor in China direkt blockiert wurde, verlor es die meisten seiner Nutzer:innen in China. Kleinere Gruppen verwenden noch unveröffentlichte Tor-Bridges (bspw. Obfs4). Weitere Werkzeuge nutzen Proxyknoten und verschlüsseln dann den Datenverkehr, was die zwei Hauptebenen der Zensur (Inspektion der verschickten Daten und Sperrung von IP-Adressen/Domainnamen) umgeht. Es werden auch spezielle Programme dafür entwickelt (u.a. FreeGate, Ultrasurf), die nach diesem Muster vorgehen und außerhalb Chinas befindliche Proxys nutzen. Sie sind nicht OpenSource, Anpassungen sind dennoch von Zeit zu Zeit nötig, da durch Analyse mittels Reverse Engineering die Proxyknoten ermittelt und blockiert werden können [52].

4.1.3 Soziale Auswirkungen

Die China-Wissenschaftlerin Christina Maags führt in einem Blog-Eintrag im Rahmen des BTI[32] aus, dass durch die Zensurmaßnahmen der „Großen Firewall“ neben den Informationsfluss in das Land hinein (durch die Blockade ausländischer Quellen) auch der Informationsfluss unter den Menschen in China selbst eingeschränkt wird. So wird auch die Meinungsfreiheit und die freie Äußerung selbiger erheblich erschwert. Die Einschränkung der Verbreitung von Informationen ermöglicht es der chinesischen

[31] kurz für: Secure Shell, kryptographisches Netzwerkprotokoll für den sicheren Betrieb von Netzwerkdiensten über ungesicherte Netzwerke

[32] kurz für: Bertelsmann-Stiftung Transformation Index, ein Projekt der Bertelsmann-Stiftung zur Untersuchung der Entwicklung von Schwellenländern in Richtung Demokratie und Marktwirtschaft

Regierung, die öffentliche Meinung in China in von ihr gewünschte Bahnen zu lenken und somit auch die Wahrnehmung von und Reaktion auf Informationen, die ihrer Linie widersprechen, zu steuern und einer möglichen (für die Regierung) negativen Wirkung zuvorzukommen. Auch kann sie öffentlich verbreitete Informationen auf eine von ihr gewünschte Sichtweise spezifisch zuschneiden [45].
Einer der wohl interessantesten, aber auch besorgniserregendsten sozialen Effekte der Zensur ist die Sozialisierung jüngerer Chines:innen. Dies hat Yaqiu Wang, ein auf China fokussierter Forscher von Human Rights Watch, in einem Artikel bei Politico im Jahr 2020 dargelegt. Er führt darin aus, wie v.a. seit dem Machtantritt von Xi Jinping im Jahr 2012 ein Wandel speziell unter jungen, internet-affinen und global vernetzten Chines:innen stattgefunden hat. Für lange Zeit war das Internet in China ein Verbreitungsweg für neue Denkmuster oder zumindest ein Hort größerer Offenheit gegenüber von der Regierungsmeinung abweichenden Stimmen. Damals stattfindende Online-Diskussionen beschreibt er als frei und offen, es wurden verschiedenen Ideen über politische Systeme ausgetauscht, und der richtige Weg für das Regieren Chinas debattiert. Seit einigen Jahren jedoch hat sich dies drastisch geändert, vorangetrieben u.a. durch ein schärferes, ausgefeilteres Vorgehen der chinesischen Regierung gegen abweichende Meinungen, sowie eine deutliche Nationalisierung ihres Narrativs. Es wird dargelegt, dass unter Chinas Jugend gewisse nationalistische Tendenzen schon immer vorhanden waren, v.a. in Bezug auf die nationale Souveränität oder Territorialstreitigkeiten, diese sich aber nun auf viele weitere Bereiche ausgedehnt haben, u.a. Kultur, Technologie und Wissenschaft [41] [42].
Angeführt wird dabei das Beispiel von Fang Fang, einer chinesischen Schriftstellerin. Diese hat im Mai 2020 ihren Bericht über den Beginn des Coronavirus-Ausbruchs in Wuhan, Wuhan Diary, auf Englisch veröffentlicht. Darin kritisiert sie das Verhalten lokaler Behörden und deren Vertuschungsversuche, sagt aber nichts über die Reaktion der Zentralregierung in Peking. Auch lobte sie Kader der KPCh[33] und Mitarbeiter:innen des Gesundheitswesens. Dies fiel in eine Zeit, in der es in China einen großen gesellschaftlichen Aufschrei wegen des Todes von Li Wenliag gab, einem jungen Arzt, der für das Verbreiten eines frühen Berichts über das neuartige Virus bestraft wurde und dann an der von diesem Virus ausgelösten Krankheit COVID-19[34] verstarb [41].
Obwohl Fang Fang keine radikale Stimme ist (sie war u.a. Vorsitzende einer regie-

[33] kurz für: Kommunistische Partei Chinas
[34] kurz für: Coronavirus Disease-2019

rungsnahen Schriftstellerorganisation in Hubei[35]), wurde sie für ihr aus Beiträgen aus (chinesischen) sozialen Netzwerken adaptiertes Werk scharf attackiert. Der Vorwurf v.a. junger Chines:innen war, dass Fang nicht auf den Erfolg der chinesischen Regierung bei der Eindämmung des Ausbruchs einging, und dass sie sich zu einem Werkzeug für „anti-chinesische Kräfte“ mache [41].
Wang führt auch weitere Beispiele von Medien an, die lange Zeit sehr populär in China waren, heutzutage aber als „unpatriotisch“ kritisiert und angegriffen werden, so u.a. die Comedy-Show „Big Shot's Funeral“ vom Beginn des 21. Jahrhunderts, die Vertreter von Chinas damals noch im Aufkommen begriffenen Kapitalismus satirisch darstellte. Auch werden bspw. Wissenschaftler:innen, die den wissenschaftlichen Hintergrund und die Effektivität und Sicherheit der traditionellen chinesischen Heilkunde in Frage stellen, attackiert und als „Han-Verräter“[36] beschimpft [41] [43] [44].

4.1.4 Wirtschaftliche Auswirkungen

Die Große Firewall ist ein Teil des chinesischen Wirtschaftsprotektionismus. Ihr wohl deutlichster wirtschaftlicher Effekt ist die massive Entwicklung der chinesischen Internetbranche, die wohl in dieser Form nicht möglich gewesen wäre, hätten chinesische Firmen ohne die durch die Große Firewall entstandenen Beschränkungen gegen US-Konzerne im Wettbewerb bestehen müssen. Dies hat für US-amerikanische Firmen zu massiven Umsatzverlusten geführt. Nach konservativen Schätzungen des ITIF[37] sind bspw. Microsoft und Amazon im Cloudgeschäft zusammen rund 1,6 Milliarden US-Dollar an möglichen Einnahmen in den Jahren 2017 und 2018 entgangen. Durch die speziellen Umstände in China konnten sich jedoch einheimische Internetgiganten entwickeln, bspw. Konzerne wie Tencent, der heute größte chinesische Internetkonzern, der u.a. mit seiner App WeChat, die sich von einem simplen WhatsApp-Ersatz zu einer Rumdum-App für nahezu alle Lebensbereiche entwickelt hat, u.a. mit einem integrierten Onlinebezahldienst, einer Videotelefonie-Funktion und der Möglichkeit, direkt aus der App Online-Bestellungen zu tätigen. Daneben haben sich auch andere einheimische Dienste entwickelt, die als Pendants zu westlichen Internetdiensten gesehen werden können, u.a. Baidu, die populärste chinesische Suchmaschine, und AliPay, ein PayPal-ähnlicher Onlinebezahldienst. Laut einem Ranking von Alexa, einer Amazon-Tochter,

[35] chinesische Provinz, im Zentrum Chinas gelegen
[36] die Han sind die vorherrschende ethnische Volksgruppe in China, und beziehen sich auf die Han-Dynastie, die in China von ca. 206 v. Chr. bis 220 n. Chr. herrschte
[37] kurz für: Information Technology and Innovation Foundation, Think Tank für Wissenschafts- und Technologiepolitik

sind mit Google und Youtube immer noch zwei US-amerikanische Websites die weltweit meistbesuchten Internetseiten, jedoch liegen unter den Top 10 sechs Websites, die von chinesischen Unternehmen betrieben werden [58] [62] [59] [60].
Die Maßnahmen der Internetzensur haben in den letzten Jahren jedoch nicht nur positive Auswirkungen auf die chinesische Wirtschaft gehabt. Sie führen u.a. dazu, dass die Internetgeschwindigkeiten bei Verbindungen zwischen China und dem Rest der Welt für viele Firmen zu langsam für ihre Arbeit sind. Auch kommt es häufig vor, dass VPN-Verbindungen für einige Zeit unterbrochen werden, was zu Produktivitätsverlusten führt. Zudem müssen Firmen, um in China aktiv sein zu können, eventuell die eingesetzten Cloud-Plattformen zum Austausch von Daten zwischen verschiedenen Standorten wechseln, da Dienste wie Google Documents und Dropbox in China blockiert werden. In der jüngeren Vergangenheit wurde auch die Entwicklung neuer Wirtschaftsbereiche im Internet, wie Video- und Livestreaming, behindert. Diese neuen Branchen entwickelten sich in der ersten Hälfte der 2010er Jahre extrem schnell, sodass chinesische Zensoren kaum damit hinterherkamen, diesen Bereich in die Zensur einzubeziehen. Seit Mitte der 2010er Jahre jedoch wurden die Zensurmaßnahmen mehr und mehr auf diesen Bereich angewandt, was dazu geführt hat, dass die Weiterentwicklung dieses Bereichs extrem verlangsamt wurde, da große Unsicherheiten darüber bestehen, was der Zensur unterliegt oder in Zukunft unterliegen wird [61] [63].

4.2 Chinas „Social Credit System“

4.2.1 Ursprüngliche Planungen und Ziele

Der ursprüngliche Plan für den Aufbau eines chinaweiten Sozialkreditsystems[38] ist in einem Dokument des Staatsrats vom 14. Juni 2014 beschrieben, dem „Planungsschema für den Aufbau eines Sozialkreditsystems (2014 - 2020)“. Darin wird das Sozialkreditsystem als ein bedeutender Teil des „sozialistischen Marktwirtschaftssystems“ und Sozialsystems bezeichnet. Es soll auf einem ausgebauten Netzwerk basieren, das Aufzeichnungen zu Krediten aller Mitglieder der Gesellschaft umfassen soll und auch die Infrastruktur des Sozialkreditsystems selbst. Es soll dazu dienen, eine „Aufrichtigkeitskultur“ zu etablieren und Ehrlichkeit und „traditionelle Tugenden“ fördern. Auch soll es die Aufrechterhaltung von Vertrauen in der Gesellschaft fördern und Beschränkungen für Vertrauensbrüche als Inzentive nutzen. Als fundamentales Ziel wird die Steigerung

[38] elektronisches Überwachungs-, Erfassungs- und Bewertungssystem für Bürger:innen, Unternehmen und Organisationen

der „ehrlichen Mentalität“ in der Gesellschaft benannt. Geplant ist ein System mehrerer vernetzter Sozialkreditsysteme in verschiedenen sozialen Ebenen [64] [65] [66].
Der Staatsrat benennt in diesem Dokument den Aufbau solch eines Systems als einen wichtigen Baustein für die wissenschaftliche Entwicklung Chinas, den Aufbau einer „harmonischen sozialistischen Gesellschaft“, die „Stärkung des Aufrichtigkeitsbewusstseins der Mitglieder der Gesellschaft“ und die Perfektionierung des sozialistischen Wirtschaftssystems und damit die Steigerung der internationalen Wettbewerbsfähigkeit Chinas. Als Planungszeitraum werden die Jahre 2014 bis 2020 angegeben, also soll das System bis Ende 2020 einsatzbereit sein [66] [65].
In dem Dokument wird auch auf den 2014 existenten Entwicklungsstand eingegangen. Es wird festgehalten, dass auf dem Weg hin zu einem möglichen nationalen System einige Fortschritte erzielt wurden. So wurde u.a. eine ministerienübergreifende Arbeitsgruppe für die koordinierte Entwicklung solch eines Systems eingerichtet, es wurden für den Aufbau des Systems Regularien eingeführt und Standards entwickelt, und praktische Vorbereitungen für die Einführung eines landesweiten Systems sind erfolgt [66] [65].
Auch werden aber noch bestehende Probleme aufgeführt. So waren die existenten Systeme zu diesem Zeitpunkt noch unkoordiniert und nicht auf den wirtschaftlichen und sozialen Entwicklungsstand abgestimmt. Auch waren die bestehenden Systeme bei Weitem noch nicht allumfassend, wie es der Plan vorsah. Zudem waren die Aufzeichnungen zu den Kreditständen von Mitgliedern der Gesellschaft größtenteils mangelhaft, und Anreize für die Förderung von Vertrauen und Bestrafungen für Verletzungen desselbigen waren nur sehr unvollständig implementiert [66] [65].
Als Gründe für die Einführung eines solchen Systems gibt der Staatsrat an, dass sich China 2014 in einer Phase der bedeutenden wirtschaftlichen und sozialen Weiterentwicklung befand. Die Einführung des Systems wird als ein sinnvoller und hilfreicher Baustein zur Stärkung der innergesellschaftlichen Ehrlichkeit, der Erhöhung des innergesellschaftlichen Vertrauens und der Verringerung sozialer Gegensätze. Der Staatsrat vermerkte zudem, dass zu dieser Zeit die Öffnung der chinesischen Wirtschaft immer weiter voranschritt und der wirtschaftliche und soziale Austausch mit dem Rest der Welt immer enger wurde. Die Entwicklung und Verbesserung des Systems vernetzter landesweiter Sozialkreditsysteme wurde in diesem Kontext als notwendig beschrieben, um internationalen Austausch und Zusammenarbeit auszudehnen, um den weltweiten Einfluss Chinas auszubauen, und für die Anpassung Chinas an die Umstände der Globalisierung und das Bestehen des Landes in den globalisierten Wirtschaftsstrukturen. Im weiteren Verlauf wird noch darauf eingegangen, dass auch die Ehrlichkeit

im wirtschaftlichen Geschehen innerhalb des Landes durch das System gefördert werden soll, um das Vertrauen in auf dem chinesischen Markt aktive Unternehmen zu erhalten [65] [66].

4.2.2 Testphasen und -systeme

Ein einziges, allumfassendes Sozialkreditsystem oder auch nur ein vernetztes Systems mehrerer Sozialkreditsysteme gab es in China bisher nicht. Eine umfassende Analyse der Landschaft der verschiedenen Sozialkreditsysteme in China stammt von Chuncheng Liu, Doktorand am Department für Soziologie der UCSD[39], aus dem Jahr 2019. Er beschreibt, dass seit der Ausgabe des Planungsschemas durch den Staatsrat im Jahr 2014 eine Vielzahl ko-existierender Sozialkreditsysteme in China entstanden ist, die auf verschiedensten Ebenen agieren und häufig kaum bis gar nicht kooperieren [66].
Aktuell gibt es in China vier Kategorien von Sozialkreditsystemen, die zwei verschiedenen Ansätzen entstammen. Der erste Ansatz ist, Sozialkreditsysteme als ein Teil der Wirtschafts- und Finanzinfrastruktur zu betrachten. Führend ist hierbei die PBOC[40]. Unter diesem Ansatz gibt es ein von der PBOC entwickeltes, landesweites Finanzkreditsystem der Regierung, sowie mehrere von privaten Firmen betriebene kommerzielle Rating- und Kreditsysteme, die von der PBOC überwacht werden. Der zweite Ansatz besteht darin, Sozialkreditsysteme als ein Werkzeug der „sozialen Governance“ anzusehen. Dieser Ansatz wird v.a. von Chinas nationaler Entwicklungs- und Reformkommission (NDRC) verfolgt, einer makroökonomischen Verwaltungsbehörde des Staatsrats. Zu den unter diesem Ansatz entwickelten Systemen gehören u.a. landesweite, von der Regierung eingerichtete Black- und Redlists sowie von lokalen Behörden und Regierungsstellen entwickelte Piloten für Sozialkreditsysteme [66] [68].
Im Folgenden sollen die einzelnen Arten von Sozialkreditsystemen ein wenig genauer beleuchtet werden.

Finanzkreditsystem der PBOC

Das von der PBOC entwickelte System legt seinen Fokus darauf, Unsicherheiten und Risiken anzugehen, die mit unterschiedlichen Informationsbeständen verschiedener Akteure im Wirtschafts- und Finanzsektor einhergehen. Als der Begriff „Sozialkredit“ 2002 zum ersten Mal von der chinesischen Regierung diskutiert wurde, ging es noch um ein solches, eng gefasstes Kreditsystem des Finanzsektors. Das von der PBOC entwickelte

[39] kurz für: University of California, San Diego
[40] kurz für: People’s Bank of China, Chinas Zentralbank

Finanzkreditsystem umfasst Bürger:innen und Unternehmen. Das erste, in den 2000er Jahren in Betrieb genommene System erzeugte v.a. Kreditberichte, die für Individualpersonen lediglich einige finanzielle und wirtschaftliche Informationen enthielten, bspw. Zahlungsrückstände und die Anzahl genutzter Kreditkarten [66].
Seit 2014 wurde das System grundlegend überarbeitet und wird seit Mitte 2019 eingesetzt. Es stellt Kredit-Scores bereit, wie bspw. auch Credit Reports in den USA. Beide Generationen bezogen den Großteil ihrer Datenbasis von Finanzinstituten. Genutzt werden die von ihnen bereitgestellten Informationen fast ausschließlich von Kreditgebern im Finanzsektor [66].

Private Rating- und Kreditsysteme

Am 05. Januar 2015 wurde der Markt für Kreditratings von Bürger:innen eröffnet. Im Rahmen dessen erhielten acht Firmen, v.a. aus der Technologiebranche, Lizenzen für Testläufe, mit denen diese eigene Systeme dafür entwickeln durften. Das am häufigsten eingesetzte kommerzielle Kreditratingsystem in China ist der Sesame Credit Score des Unternehmens Ant Financial, ein Tochterunternehmen von Alibaba [66] [68].
Dieses kommerzielle System unterscheidet sich, wie einige andere, von dem der PBOC und anderen von Regierungsstellen entwickelten Systemen in vielen Aspekten. So werden in die Berechnung der Scores auch persönliche Informationen wie das Bildungsniveau und der Besitz von bspw. Autos mit einbezogen. Auch können Bürger:innen Zertifikate und andere Rechtsdokumente hochladen, um ihre Daten zu verifizieren. Und es werden Verbindungsdaten von sozialen Netzwerken mit einbezogen. Allerdings wird von Ant Financial angegeben, dass sie keinen Zugriff auf einzelne Posts haben. Diese Aussage wurde dadurch ausgelöst, dass vielfach angenommen wurde, dass die Kreditscores von Bürger:innen auch durch politische Ansichten, die sie in sozialen Netzwerken äußern, beeinflusst werden. Zudem werden detaillierte Informationen zum Konsumverhalten mit einbezogen, bspw. führt der Kauf von Windeln zu einem höheren Score, da dies auf ein höheres soziales Verantwortungsbewusstsein hindeutet. Und letztlich ist das System wesentlich komplexer als das der PBOC, u.a. nutzt es künstliche Intelligenz und maschinelles Lernen zum Modellieren von Daten, während Regierungssysteme noch größtenteils auf einfachen Punktebewertungen beruhen [66] [68].
Das System des Sesame Score wurde sehr schnell sehr einflussreich und in vielen Bereichen eingesetzt. Dies wurde u.a. durch Alibabas große Nutzerbasis ermöglicht, Alibabas zwei größte Plattformen, Taobao (E-Commerce-Plattform) und Alipay haben zusammen über 800 Millionen Nutzer:innen. Die Scores beeinflussten das wirtschaftliche Le-

ben stark, so konnten Bürger:innen mit hohen Scores in diesem System u.a. kautionsfrei Hotelzimmer oder Fahrräder mieten. Auch im sozialen Bereich kamen diese Scores zum Einsatz, u.a. auf Dating-Plattformen. Dies wurde von der PBOC kritisiert [66].
Nach dem Ablauf des Versuchszeitraums im Jahr 2017 wurde keine der Lizenzen von der PBOC erneuert. Sie übte starke Kritik an den Firmen, u.a. wegen des kaum vorhandenen Datenaustausches zwischen verschiedenen Plattformen und aufgetretenen Interessenkonflikten. Zudem hatten die Firmen aus Sicht der PBOC kaum verstanden, was in diesem Kontext als „Kredit“ zu verstehen ist. In Folge dessen wurde Anfang 2018 ein Unternehmen für Kreditscores und Kreditrating von Bürger:innen gegründet, Baihang Credit, das als einziges Unternehmen eine Lizenz für dieses Geschäftsfeld erhielt. An diesem Unternehmen hielten sowohl die acht Firmen, die Testsysteme betrieben, Anteile, als auch der nationale Internetfinanzverband, eine der PBOC unterstellte Regierungsbehörde. Noch bevor Baihang Credit begann, seine Dienstleistungen anzubieten, hatten die acht Unternehmen ihre Rating- und Scoringsysteme vom Markt zurückgezogen [66] [67].

Landesweite Black- und Redlist-Systeme der Regierung

Das wohl meistdiskutierte Sozialkreditsystem in China ist ein System bestehend aus Blacklists „diskreditierter Subjekte“ und Redlists, die positiv bewertete Personen und Organisationen beinhalten. Im Jahr 2015 wurde im Rahmen dessen eine komplett neue digitale Infrastruktur eingerichtet, Credit China[41], um Informationen über Personen und Organisationen auf Black- und Redlists öffentlich zugänglich zu machen, und Informationen sowie Nachrichten zu Sozialkreditsystemen in China zu verbreiten [66].
Die Existenz dieser zentralisierten Digitalinfrastruktur bedeutet nicht, dass es ein vereintes System von Red- und Blacklists gibt. Es existiert eine Vielzahl verschiedener Systeme, die von zahlreichen Behörden der Zentralregierung in ihren Aufgabenbereichen eingerichtet wurden und dabei von der NDRC überwacht und koordiniert werden. Jedes System hat seine eigenen spezifischen Kriterien für das Einordnen einer Person oder Organisation in eine Black- oder Redlist. So hat bspw. die CAC vorgeschlagen, Personen, die im Internet Gerüchte verbreiten, auf seine „Blacklist diskreditierter Subjekte bezüglich Internetdiensten“ aufzunehmen. Die CAA[42] setzt Bürger:innen auf ihre Blacklist, die sich auf Zivilflügen unangemessen verhalten [66] [68].
Die Folgen der Aufnahme auf Blacklists sind uneinheitlich. Dies änderte sich auch

[41] Website: https://www.creditchina.gov.cn/
[42] kurz für: Civil Aviation Administration, zivile Luftfahrtbehörde Chinas

nicht, nachdem 44 Behörden der Zentralregierung im Jahr 2016 ein Abkommen schlossen, Daten zwischen ihren Black-/Redlist-Systemen auszutauschen und Personen auf mehreren Blacklists gemeinsam zu bestrafen. Einer der wenigen gemeinsamen Ansätze ist die Veröffentlichung von Personen auf Blacklists, zusammen mit weiteren persönlichen Informationen wie Name, Adresse und Grund der Aufnahme in die Blacklist. Wird eine Person bspw. in die Blacklist der CAC aufgenommen, wird ihre Internetnutzung beschränkt, während eine Aufnahme in die CAA-Blacklist in einer Beschränkung oder dem Verbot des Reisens per Flugzeug resultieren kann [66] [68].
Das am weitesten entwickelte System ist die „Liste diskreditierter Vollstreckungsschuldner“, die am 16. Juli 2013 vom SPC[43] in Betrieb genommen wurde, um das Problem mit der Durchsetzung von Gerichtsurteilen und -vollziehungen anzugehen. Im Normalfall werden Personen oder Unternehmen in die Liste aufgenommen, wenn sie Geld schuldig sind, aber eine Zahlung verweigern, obwohl sie dazu wirtschaftlich in der Lage wären und ein Gericht sie dazu verurteilt hat. Den fortgeschrittenen Entwicklungsstand des Systems kann man an vielen Aspekten erkennen. So ist es das am weitesten verbreitete System. Im Januar 2019 befanden sich von den 215.582 Personen auf den Blacklists aller Systeme 214.141 von ihnen auf der „Liste diskreditierter Vollstreckungsschuldner“. Auch beinhaltet es die mit Abstand erfolgreichste Anwendung gemeinsamer Bestrafungen. Seit Beginn des Systems hat der SPC mit verschiedensten Regierungsstellen zusammengearbeitet, um gegen Schuldner Sanktionen zu erlassen, um deren Kaufverhalten zu beschränken, u.a. bezogen auf Erste-Klasse-Tickets für Züge und Flüge. Im Verlauf der Zeit haben SPC und NDRC die Verbindungen zwischen den Regierungsbehörden und gemeinsame Sanktionen ausgebaut. Nun resultieren aus der Aufnahme in die Blacklist neben Konsumeinschränkungen auch beschränkte Möglichkeiten, für die Regierung zu arbeiten oder in öffentlichen Institutionen befördert zu werden [66].
Diese Systeme zielen auf Individuen als auch auf Institutionen wie NGOs, Unternehmen und Regierungen ab. Bei Institutionen sind auch deren rechtliche Vertreter sowie Verantwortliche für rechtliche und finanzielle Verpflichtungen betroffen. Mit Stand April 2017 waren auch mehr als 480 lokale und nationale Regierungen als diskreditiert eingestuft. Regierungsangehörige erfuhren dann u.a. Reisebeschränkungen, und die Zugänge der Regierungen zu Kredit- und Investitionsmöglichkeiten waren eingeschränkt [66].

Lokale Pilotsysteme

Trotz aller Anstrengungen von Behörden der Zentralregierung sind es meisten Stellen

[43] kurz für: Supreme People's Court, Chinas oberstes Gericht

lokaler Regierungen, die die Richtlinien umsetzen, also Daten sammeln und in die Systeme hochladen sowie Personen einordnen und bestrafen, allerdings sind Bestrafungen nicht immer häufig. Eine Stadt hatte bspw. im Jahr 2018 11.000 Menschen auf ihrer Blacklist, aber nur 50 Bestrafungen verhängt. Andere Städte sind dabei bereits weiter fortgeschritten. So zeigt ein Gericht in Louyuan, einer Kleinstadt in Fujian[44], private Informationen wie Name, Adresse, Bild und geschuldete Geldmenge vor Filmen im lokalen Kino. In einer anderen Stadt arbeitet das lokale Gericht mit Mobilfunkanbietern zusammen, um an „diskreditierten" Bürger:innen spezielle Klingeltöne zu vergeben, damit diese in der Öffentlichkeit als solche erkennbar sind [66].
Anders als auf Ebene der Zentralregierung ist es lokalen Regierung auch deutlich besser gelungen, verschiedene Behörden auf ihrer Ebene zur Zusammenarbeit zu bringen. Dies ist gut daran zu erkennen, dass, anders als in der Zentralregierung, auf lokaler Ebene häufig eine eigene Behörde dafür existiert. Und obwohl lokale Sozialkreditsysteme für Unternehmen nach sozialen Aspekten und den Aufgabenbereichen verschiedener Behörden aufgeteilt sein können, werden Sozialkreditsysteme für Bürger:innen stets in ein lokal vereintes System integriert. Einige dieser Systeme bringen lediglich Kreditberichte heraus, während andere mit quantifizierten Punktezahlen arbeiten [66].
Rongcheng, eine Hafenstadt an der Nordostküste Chinas, war die erste Stadt, die nach der Ausgabe des Planungsschemas durch den Staatsrat im Jahr 2014 ein auf Punktescores basierendes Sozialkreditsystem in Betrieb nahm. Die meisten chinesischen Städte sind seitdem diesem Ansatz gefolgt, bis Mai 2019 hatten 21 von ihnen bereits ähnliche Systeme in Betrieb, 27 weitere befanden sich in Vorbereitungen dafür. Der Großteil dieser Städte befindet sich an Chinas Ostküste und ist wirtschaftlich und/oder politisch von großer Bedeutung. Die meisten lokalen Systeme machen die Berechnungsmethoden für die Punktescores und die Indikatoren für Punkteadditionen und -abzüge öffentlich. Die Anzahl dieser Indikatoren schwankt stark, in manchen Systemen sind es einige Dutzend, in anderen weit über 1.000. Viele lokale Systeme ordnen Bürger:innen anhand ihrer Scores auch in Klassen ein, bspw. gibt es in Rongcheng vier Klassen, je nach Punktescore: A ($\geq$ 960), B (850 - 959), C (600 - 849) und D ($\leq$ 599). Das Erreichen hoher Scores (und damit die Einordnung in höhere Klassen) bringt eine Reihe von Vorteilen mit sich, bspw. Rabatte auf Tickets im öffentlichen Personenverkehr oder bevorzugte Behandlung in Verwaltungsangelegenheiten. In manchen Städten gibt es auch Rabatte auf Kredite. Bestrafungen für niedrige Scores sind weniger und meist kleiner gefasst. In den meisten Städten werden keine genauen Bestrafungen bekannt gegeben, meist

[44]Provinz im Südosten Chinas

geht und um die „Ehre“ der Personen und es werden für Mitarbeiter:innen öffentlicher Insititutionen mit niedrigen Scores Beförderungen ausgesetzt. Manche Systeme führen ebenfalls Reisebeschränkungen für Menschen mit niedrigeren Scores ein, bspw. ist es in Rongcheng nur Personen in Klasse A möglich, Tickets für Erste-Klasse-Flüge oder Fahrten mit Hochgeschwindigkeitszügen zu erwerben [66] [69].
Die Quellen, aus denen die lokalen Systeme ihre Daten beziehen, sind sehr unterschiedlich. Manche basieren größtenteils auf bereits existierenden Richtlinien und Regularien verschiedener Regierungsbehörden. Allerdings ist die Beteiligung von Behörden sehr uneinheitlich. So bezieht das System von Yiwu[45] 41 Regierungsstellen und öffentliche Institutionen mit ein, das in Suqian[46] nur 10. In allen Systemen, die die beteiligten Stellen öffentlich machen, sind Gerichte, Staatsanwält:innen, lokale Polizei, Steuerbehörden und staatliche Versorgungsunternehmen mit involviert. Allerdings sind bspw. Gesundheits- und Bildungsbehörden in einigen lokalen Systeme beteiligt, in anderen wiederum nicht. Auch beziehen einige lokale Systeme Daten aus anderen Quellen mit ein. So wird bspw. in Rongcheng auch das „soziale und moralische Verhalten“ mit einbezogen, bspw. „abergläubische Aktivitäten“. Dort sind auch sogenannte „Informationssammler“ unterwegs, meist Rentner:innen, die das Leben ihrer Mitmenschen im öffentlichen Raum beobachten und Aufzeichnungen machen, die dann in die Berechnung der Punktescores mit einbezogen werden [66] [69].

4.2.3 Öffentliche Diskussion und Wahrnehmung in- und außerhalb Chinas

Die Wahrnehmung der Entwicklung von Sozialkreditsystemen in China war zunächst sehr kritisch. Im Jahr 2010, als die Stadt Suining[47] einen ersten lokalen Piloten für ein System quantifizierter Punktescores für alle Einwohner:innen an den Start brachte, reagierten chinesische Medien mit harscher Kritik. Sie argumentierten, die Regierung solle generell keine Punktescores für Bürger:innen nutzen und äußerten die Sorge, solche Methoden seien ein Fall extremen Machtmissbrauches durch Regierungsstellen. Dies scheint sich aber (nach verfügbaren Informationen) im Laufe der Zeit geändert zu haben. Im August 2018 veröffentlichte Prof. Genia Kostka von der Freien Universität Berlin eine Studie, in der 2.209 Chinesen mit verschiedensten Hintergründen, die ein repräsentatives Abbild chinesischer Internetnutzer:innen zwischen 14 und 65 Jahren darstellten, u.a. zu ihren Ansichten zu Sozialkreditsystemen und ihrer Teilnahmen an

[45] Stadt ca. 250 km südwestlich von Shanghai
[46] Stadt ca. 500 km nordwestlich von Shanghai
[47] in Zentralchina gelegen

diesen befragt wurden. In dieser wird auch auf in den Vorjahren durchgeführte Studien verwiesen, die u.a. ergaben, dass die Einstellung von Chines:innen zu solchen Systemen u.a. davon abhängt, wer sie betreibt, so werden Regierungsstellen diesbezüglich als vertrauenswürdiger angesehen als Unternehmen. Auch Kritik in den einheimischen Medien fokussierte sich v.a. auf Unternehmen, die auf viele persönliche Daten zugreifen, und kaum auf Systeme von Regierungsstellen. Die Studie von Kostka ergab, dass ungefähr 84 % der Befragten an einem Sozialkreditsystem teilnehmen. Von den Befragten gaben ca. 80 % an, an einem kommerziellen System teilnehmen, wobei der Sesame Credit das mit Abstand am häufigsten genannte ist, während nur 7 % an Pilotsystemen lokaler Regierungen teilnehmen. Bezüglich der Ansichten der Befragten zu Sozialkreditsystemen hat sich ergeben, dass wieder ca. 80 % der Befragten Sozialkreditsystemen gegenüber positiv eingestellt sind, während nur ungefähr 1 % diese ablehnt. Dieses Ergebnis ist jedoch unter dem Aspekt zu betrachten, dass diese Umfrage in einem autoritären Umfeld stattfand, wodurch einige der Befragten trotz der anonymisierten Behandlung der Umfragedaten unwahre Antworten gegeben haben könnten, um staatlichen Repressionen zu entgehen. Bei tiefergehender Betrachtung der Umfrageergebnisse zeigt sich auch, dass v.a. Chines:innen mit höheren Einkommen und höheren Bildungsniveaus sowie solche, die in urbanen Regionen leben, Sozialkreditsystemen besonders positiv gegenüberstehen. Dies erscheint zunächst überraschend, da besonders diese Gruppen eher liberale Ansichten haben und Dinge wie Privatsphäre und Datenschutz als wichtig erachten. Aber die Studie zeigt, dass die positive Einstellung v.a. daher stammt, dass Sozialkreditsysteme als nützliche Werkzeuge angesehen werden, um den Mangel an innergesellschaftlichem Vertrauen zu beheben und regulatorische Lücken zu schließen und die Durchsetzung von Regularien in verschiedensten Bereichen von Lebensmittelsicherheit bis Umweltschutz zu verbessern [66] [70] [71] [72].

Außerhalb Chinas ist die Wahrnehmung größtenteils sehr kritisch. In einem Beitrag für die ACLU[48] aus dem Jahr 2015 beschreibt einer ihrer politischen Analysten, Jay Stanley, die Entwicklungen in China als eine deutliche Warnung an die Bürger:innen der USA und anderer westlicher Staaten. Das System wird als eine gamifizierte Version von Autoritarismus bezeichnet, und ein Beispiel dafür, wie autoritäre Regierungen die neuen Möglichkeiten der Digitalisierung nutzen, um anders als die totalitären Regime des 20. Jahrhunderts freie Märkte und größere persönliche Freiheiten zuzulassen, aber trotzdem jedwede Bedrohung oder Herausforderung ihrer Herrschaft zu unterdrücken. Zudem spricht er eine Warnung aus, dass bereits in den USA Tendenzen existieren, u.a.

[48] kurz für: American Civil Liberties Union, größte US-amerikanische Bürgerrechtsorganisation

die private Kreditscoring-Industrie, die eine ähnliche Entwicklung nehmen könnten, wie sie in China stattfindet. Samantha Hoffman vom Australian Strategie Policy Institute kritisierte in einem Beitrag von Wired im Juni 2019 fehlenden Schutz für diejenige, die von den Systemen erfasst werden, vor Fehlern oder auch Missbrauch aufgrund des Mangels an Rechtsstaatlichkeit in China. Das US-Politmagazin The Hill verglich die existenten Systeme im Jahr 2018 mit der totalitären Dystopie des Buches „1984“ von George Orwell und schrieb: „*Das totalitäre 1984 der Zukunft ist das China des Jahres 2018.*“ [73] [74] [75].
Die ausländische Sicht auf diese Entwicklungen ist jedoch mit Missverständnissen verbunden. In einem Wired-Bericht von 2019 wird beschrieben, dass westliche Bedenken zu den Möglichkeiten der chinesischen Systeme sich von der realen Situation immer weiter entfernen. Dies führe auch dazu, dass verstärkte Überwachungsmaßnahmen in anderen Teilen der Welt nur unzureichende Beachtung fänden. Das Logic Magazine beschrieb im selben Jahr, dass durch westliche Medienberichte das Bild einer technologischen Dystopie erschaffen worden sei, das nicht mit der Realität in China übereinstimme. Als Gründe für diese Missverständnisse werden u.a. Übersetzungsfehler sowie unterschiedliche Wortwahl in Chinesisch und in westlichen Sprachen genannt [76] [77].

4.3 Russlands Weg in die Internet-Zensur

Das Internet in Russland war für lange Zeit ein Zufluchtsort für regierungskritische Stimmen. Als die traditionellen Medien schon auf Regierungslinie gebracht worden waren, konnte im russischen Internet noch recht freizügig berichtet und diskutiert werden. Ab Anfang der 2010er-Jahre hat sich dies tiefgreifend geändert [78].

4.3.1 Freie Entwicklung des russischen Internets in den 1990er und 2000er Jahren

Das russische Internetzeitalter begann in den frühen 1990er Jahren, und die Entwicklung war früh eine sehr schnelle. Es entwickelten sich einige große Firmen, die zumindest auf dem russischen Markt bis heute mit der westlichen Konkurrenz, mithalten können, bspw. Mail.ru, das in Russland mindestens so beliebt wie Googles Gmail ist, und soziale Netzwerke wie VKontakte, Marktführer in Russland. Trotz dieser rasanten Entwicklung, die auch eine stark ansteigende Zahl russischer Internetnutzer:innen einschloss, hat die russische Regierung in den 1990er und 2000er Jahren kaum versucht, eine ernsthafte Kontrolle des Internets einzuführen. So fand im Dezember 1999 ein

Treffen zwischen dem damaligen Ministerpräsidenten, Vladimir Putin, und Vertretern der russischen Internet-Community statt. Im Ergebnis dessen sicherte Putin im Austausch für Unterstützung zu, jede Gesetzesinitiative bezüglich des Internets werde im öffentlichen Rahmen diskutiert werden. Nachdem Dmitrij Medvedev 2008 auf Putin im Amt des Präsidenten folgte, warb er um US-Konzerne für sein Projekt eines „russischen Silicon Valley“. Die kritischen Journalist:innen und Oppositionsaktivist:innen, die im Internet sehr aktiv waren, wurden damals nicht als Bedrohung angesehen [78] [79].
Im rechtlichen Rahmen hatten die traditionellen Medien (Print, TV, Radio) in Russland im Rahmen von Glasnost und Perestroika[49] mehr Freiheiten erhalten, was schließlich in der Aufnahme der Medienfreiheit in die Verfassung der Russischen Föderation im Jahr 1993 mündete. Im Verlauf der 1990er-Jahre änderte sich daran nicht viel. In Putins ersten zwei Amtszeiten als Präsident von 2000 bis 2008 fand jedoch eine tiefgreifende Umwälzung der russischen Medienlandschaft statt, viele regierungskritische Medienkonzerne und Redaktionen wurden geschlossen oder unter die direkte oder indirekte Kontrolle des Staates gebracht, viele durch direkten Druck auf die Firmen. Damit wurde das Internet der Hauptort für den Austausch regierungskritischer Ideen [78] [79].

4.3.2 Erster Angriff auf die Freiheit des russischen Internets

Der erste Versuch der russischen Regierung, die Freiheit des Internets zu beschränken, fand im Jahr 2008 statt, vor dem Hintergrund des Georgienkrieges. Im September 2008 verhinderten russische Behörden die Betriebsaufnahme eines Rechenzentrums der Firma Yandex[50]. Zudem wurde u.a. gegen den Yandex-Chef Arkadij Volož ein Strafverfahren eingeleitet. Ausgelöst wurde dies dadurch, dass der Yandex-Nachrichten-Aggregator yandex.novosti auf georgischen Quellen basierende Schlagzeilen vermeldete. Nachdem zwei hochrangige russischen Regierungsvertreter sich vorführen ließen, dass yandex.novosti Nachrichten anhand eines speziellen Algorithmus auswählt, verlangten diese, dass Beamt:innen der russischen Regierung Zugang zur Schnittstelle des Dienstes erhalten sollen, um unliebsame liberale Nachrichten auszusortieren. Dies war der erste Fall, in dem der Kreml seine in den traditionellen Medien erfolgreich erprobte Taktik, direkten Druck auf Firmen auszuüben, um diese unter staatliche Kontrolle zu bringen oder zur Selbstzensur zu bewegen, im Internet anzuwenden versuchte. Dieser erste Angriff konnte noch abgewehrt werden, doch er war ein Vorbote dessen, was in den 2010er Jahren folgen sollte [78].

[49] Öffnungspolitik von Michail Gorbatschow in der Sowjetunion ab 1985
[50] größter russischer Internetkonzern

4.3.3 Entwicklungen seit dem Arabischen Frühling und der 2011/12er-Protestbewegung

Seit Anfang der 2000er-Jahre glaubte die russische Regierung, die USA würden mittels „Farbrevolutionen“ Regimewechsel herbeiführen, wobei Jugendbewegungen, wie sie u.a. zum Sturz Slobodan Milosevic[51] führten, von ihr als ein neues Mittel Washingtons zu diesem Zweck angesehen wurden. Nach dem Ausbruch des Arabischen Frühlings, dessen Proteste sich zum Großteil über soziale Netzwerke organisierten, war der Kreml erneut alarmiert und sah eine unmittelbare Bedrohungslage für die Regierung. Dazu kam, dass nach den Parlamentswahlen vom Dezember 2011 auch in Russland über soziale Netzwerke organisierte Proteste begannen, die sich gegen Fälschungen seitens der Regierung richteten. Die russische Regierung war zu diesem Zeitpunkt überzeugt, von den USA angegriffen zu werden. Die russischen Geheimdienste, allen voran der Inlandsgeheimdienst FSB, hatte auf diese vermeintliche Bedrohung zunächst keine Antwort. Der stellvertretende Direktor Sergej Smirnov forderte im März 2012, es müssten Werkzeuge und Methoden entwickelt werden, um von staatlicher Seite auf diese neuen Technologien und Möglichkeiten der Vernetzung und Organisation zu reagieren [78] [79].
Nachdem Wladimir Putin im Mai 2012 wieder das Präsidentenamt übernahm, brachten Abgeordnete des russischen Parlaments ein Gesetzespaket ein, das die schärfere Kontrolle des Internets zum Ziel hatte. Vorgeblich ging es um den Jugendschutz, diente aber in der Realität der Einführung eines landesweiten Filtersystems mit einem Zentralregister gesperrter Websites. Es wurde Ende Juli vom Parlament verabschiedet und kurz darauf vom Präsidenten unterzeichnet. Einheimische und ausländische Internet-Konzerne waren besorgt und trafen sich mehrmals mit russischen Regierungsvertreter:innen, so ging es u.a. darum, zu verhindern, dass aufgrund inkriminierter Inhalte auf einer Unterseite eine gesamte Domain gesperrt wird. Solch ein Fall trat im September ein, als ein Film von der russischen Generalstaatsanwaltschaft als extremistisch eingestuft wurde und Roskomnadzor[52] noch vor der Gerichtsentscheidung alle russischen ISPs aufforderte, den Film für Nutzer:innen unzugänglich zu machen. Einige konnten nur YouTube als Ganzes sperren. Um solch ein drastisches Vorgehen in Zukunft vermeiden zu können, wurde nach einer Lösung gesucht. Gefunden wurde sie in der bereits in Abschnitt 4.1.2 beschriebenen Technologie der Deep Packet Inspection (DPI). Sie stand bis 2012 allen russischen ISPs zur Verfügung, und nach schwachem Widerstand waren sie unter Regierungsdruck bereit, sie einzusetzen [78] [79].

[51] einflussreichster Politiker in Serbien und der Bundesrepublik Jugoslawien von 1987 bis 2000
[52] russische Aufsichtsbehörde für Kommunikation, Informationstechnologien und Medien

Im Oktober 2012 wurde die landesweite Internet-Zensur dann endgültig eingeführt, mit einem Erlass über die Einführung eines von Roskomnadzor verwalteten „Verzeichnis verbotener Internetseiten“. Zunächst wurden nur Seiten aufgenommen, die Zwecken wie Kinderpornografie oder Drogenherstellung und -erwerb dienten. Jedoch waren von Beginn an auch Seiten darunter, die per Gerichtsbeschluss verboten wurden, wie „extremistische Materialien“. Einige Monate später kam ein weiteres Gesetz dazu, es erlaubte die Sperrung von Seiten, die zu „*Massenunruhen, extremistischer Tätigkeit oder der Teilnahme an gegen die öffentliche Ordnung verstoßenden öffentlichen Massenveranstaltungen*“ aufrufen, durch Roskomnadzor ohne Gerichtsbeschluss. Nach Inkrafttreten am 01. Februar 2014 gab es schnell erste Sperren, u.a. des Blogs von Alexej Nawalny und mehrerer Nachrichten- und Kommentarseiten. Auch wurde 2012 in Russland das sogenannte „NGO-Gesetz“ verabschiedet. Danach muss jede nicht-kommerzielle Organisation, die in Russland politisch tätig ist und mindestens einen Teil ihrer Finanzierung aus dem Ausland bezieht, sich als „Ausländeragenten“ registrieren lassen, wobei die Definition politischer Tätigkeit sehr unklar ist. Auch Organisationen aus den Bereichen Wissenschaft, Kultur und Soziales wurde diese Designation zugewiesen. Da auf Verweigerung der Registrierung sehr hohe Geldstrafen oder Gefängnis stehen, mussten Dutzende Organisationen ihre Arbeit in Russland einstellen [78] [79].
Mit dem Erlass vom Oktober 2012 und den folgenden Gesetzen war das System der russischen Internet-Zensur installiert und institutionalisert. Die Sperren waren zu Beginn noch ziemlich durchlässig, denn sie griffen nur, wenn der Rechner, von dem der Zugriff auf eine gesperrte Seite erfolgte, eine russische IP-Adresse hatte. Dies war mittels VPNs oder Tor-Netzwerken leicht zu umgehen. Um das zu unterbinden, setzte die russische Regierung u.a. auf Druck auf Unternehmen. So wurde ein Gesetz erlassen, dass das „Propagieren“ von Werkzeugen und Methoden zum Umgehen von Sperren unter Strafe stellt. Auch fanden „informelle Gespräche“ mit Internet-Konzernen statt, in denen auf diese Druck aufgebaut wurde. Dies war nur teilweise erfolgreich. Im Dezember 2014 wurde jedoch ein Gesetz verabschiedet, das alle im russischen Internet tätigen Unternehmen verpflichtete, Daten russischer Bürger:innen auf russischen Servern zu speichern. Einige, v.a. ausländische Unternehmen wie Facebook und Google widersetzten sich der Regelung auch nach dem Inkrafttreten des Gesetzes am 01. September 2015, und tun dies bis heute [78] [79].
Parallel dazu baute der russische Inlandsgeheimdienst FSB seine Möglichkeiten der Internet-Überwachung weiter aus. Im April 2015 wurde die dritte Generation von

SORM[53] in Betrieb genommen, die russische Verfahren mit Technologie aus dem Westen verbindet. SORM-1 wurde in der Sowjetunion zum Zwecke des Abhörens von Telefongesprächen entwickelt und 1996 in Betrieb genommen, SORM-2 konnte auch Internetverkehr abfangen und speichern und war ab 2000 im Einsatz. Diese Systeme waren jedoch auf die gezielte Überwachung von Einzelpersonen ausgelegt, nicht auf Massenüberwachung. SORM-3 stellte in dieser Hinsicht einen Paradigmenwechsel da. Durch Zusammenführung mit der Technologie der Deep Packet Inspection wurde die Massenüberwachung der russischen Internetnutzer:innen möglich [78] [79].
Ende Juli 2016 traten dann weitere Gesetzesänderungen in Kraft, u.a. wurde eine Art Vorratsdatenspeicherung eingeführt. Ab 01. Juni 2018 müssen Mobilfunkanbieter und ISPs sämtliche Verbindungsdaten für drei Jahre und Kommunikationsinhalte für bis zu sechs Monate speichern. Aufgrund fehlender technischer Voraussetzungen seitens russischer Unternehmen hat dies dazu geführt, dass chinesische Unternehmen wie Huawei nun im russischen Internet als Hardware-Lieferanten aktiv sind. Auch hat China mit Russland Technologien seiner Großen Firewall geteilt. Am 01. November 2017 trat in Russland ein Gesetz in Kraft, das es VPN-Anbietern vorschreibt, den Zugang zu Seiten zu sperren, die von Roskomnadzor in das „Verzeichnis verbotener Internetseiten“ aufgenommen wurden. Zudem müssen Unternehmen, die beim Datenaustausch zwischen Standorten VPNs nutzen, definieren, welche Personen diese Tunnel nutzen. Diese Maßnahmen wurden im Allgemeinen als wenig wirksam und durchsetzungsschwach erachtet. Gleichzeitig wurde beschlossen, dass ab Anfang 2018 Messengerdienste wie Facebook Messenger und Telegram alle Daten mit staatlichen Stellen teilen müssen. Auch die Durchsetzung dieser Regelung war bisher relativ wenig erfolgreich [78] [80] [81].
Im November 2019 trat ein Gesetz in Kraft, das zum Ziel hat, das russische Internet in ein „eigenständiges Internet unter kompletter Staatskontrolle“ umzuwandeln. Das Gesetz sieht die totale technische Kontrolle des russischen Staates über das russische Internet vor, und eine Ausweitung der Vorratsdatenspeicherung. Der russische Internetverkehr soll den Plänen nach künftig vollständig über von Roskomnadzor kontrollierte Knotenpunkte in Russland gelenkt werden. Damit würde Roskomnadzor nun auch selbst aktiv werden und Seiten blockieren. Die Regierung verteidigt das Projekt als eine Notwendigkeit für die Gewährleistung der nationalen Sicherheit und verweist auf die zunehmende Gefahr von Cyberangriffen [82] [83].
Im Februar 2021 trat das jüngste russische Zensurgesetz in Kraft. Es besagt, dass Betreiber von in Russland aktiven sozialen Netzwerken, wie Twitter, und VKontak-

[53] System zur elektronischen Überwachung

te, ihre Dienste nach Informationen zu nicht genehmigten Demonstrationen durchsuchen und diese dann blockieren müssen. Twitter weigerte sich, diesem Gesetz nachzukommen, weswegen Roskomnadzor im März 2021 damit begann, Verbindungen aus Russland zu mit Twitter assoziierten Domains auf 128 kbps[54] zu beschränken. Dies betraf u.a. die Domains *twitter.com, *.twing.com und *t.co*, wodurch auch andere Seiten, die diese Domainteile enthielten, verlangsamt wurden, u.a. microsoft.com und reddit.com [84] [85].

[54] 128 Kilobit pro Sekunde = 128.000 bit pro Sekunde

5 Fazit

Wie wir an den Beispielen in dieser Arbeit gezeigt haben, gibt es für digitale Technologien vielfältige Einsatzmöglichkeiten in demokratischen Staaten. Sie werden eingesetzt in Verwaltungsprozessen, zur digitalen Abwicklung von Abstimmungen und Wahlen und zur allgemeinen Effizienzsteigerung der Regierungs- und Verwaltungsarbeit. Aber auch für eher undemokratische Zwecke werden sie eingesetzt, so gibt es auch in Demokratien digitale Massenüberwachungsprogramme, wie die Abhörprogramme der USA oder auch die deutsche Vorratsdatenspeicherung, die bisher jedoch immer an rechtlichen Hürden scheiterte. Die Entscheidung, wie mit diesen digitalen Technologien in Zukunft umzugehen ist, wird eine der größten Herausforderungen für demokratische Staaten auf der ganzen Welt sein.
In autokratischen Staaten haben Machthaber überall das Potenzial digitaler Technologien zur Sicherung ihrer Herrschaft und Unterdrückung jedweder Opposition und Reformbestrebungen erkannt. Sei es in der massenhaften Zensur des Internets zur Unterdrückung regierungskritischer Stimmen, oder zur Erfassung des Verhaltens von Bürger:innen und Organisationen, um damit eventuell einmal abweichende Tendenzen identifizieren zu können. Neben den in der Arbeit betrachteten Beispielen können dazu noch viele andere betrachtet werden, die ebenfalls aufzeigen, wie autokratische Machthaber die neuen Möglichkeiten nutzen. Ein sehr aktuelles Beispiel dafür sind die Taliban, die bei ihrer Eroberung Afghanistans biometrische Erkennungsgeräte des US-Militärs erbeutet haben und diese nun nutzen könnten (und dies in der Vergangenheit bereits getan haben), um afghanische Helfer der westlichen Truppen sowie Aktivist:innen, bspw. für Frauenrechte, aber auch Angehörige der gestürzten afghanischen Regierung und ihrer Sicherheitskräfte aufzuspüren [86]. Diese und andere Beispiele zeigen, dass digitale Technologien den Machthabern neue, mächtige Werkzeuge an die Hand gegeben haben, um oppositionelle Bestrebungen und Demokratisierungsbewegungen zu unterdrücken. Der Umgang damit ist für demokratische Staaten eine Gewissensfrage, zwischen moralischen Bedenken und wirtschaftlichen Erfordernissen.

Literatur

[1] Jann Raveling
Die Geschichte der Digitalisierung – Teil II, 2020,
https://www.wfb-bremen.de/de/page/stories/digitalisierung-industrie40/geschichte-der-digitalisierung-teil-zwei (abgerufen am: 14.08.2021)

[2] Dr. Sebastian Stern et. al.
Digitalisierung 2022 – Was jetzt zu tun ist. *Strategie | Transformation*, Vol. 1-2, McKinsey & Company, 2018

[3] Markus Baumanns
Kick-off! - Auf Entdeckungsreise zur Organisation der Zukunft, Haufe Verlag für Fachbücher, ISBN-13: 978-3-648-12901-2, 2019

[4] Klaus Schubert und Martina Klein
Das Politiklexikon, Sonderausgabe für die Bundeszentrale für politische Bildung, Verlag J. H. W. Dietz Nachf., 2018

[5] Hans-Joachim Lauth
Demokratie und Demokratiemessung, VS Verlag für Sozialwissenschaften, ISBN-13: 978-3-742-50206-3, 2004,
https://doi.org/10.1007/978-3-663-01617-5

[6] Patrick Donges, Otfried Jarren
Politische Kommunikation in der Mediengesellschaft, Springer Fachmedien Wiesbaden, 2017,
https://doi.org/10.1007/978-3-658-16572-7

[7] The Economist Intelligence Unit
Democracy Index 2020, The Economist Intelligence Unit Limited,
https://www.eiu.com/n/campaigns/democracy-index-2020/, 2021

[8] Freedom House
Freedom on the World 2021 - Democracy under Siege, 2021,
https://freedomhouse.org/sites/default/files/2021-02/FIW2021_World_02252021_FINAL-web-upload.pdf

[9] Jan W. van Deth
Politische Partizipation. *In Politische Soziologie*, pp. 141-161, VS Verlag für Sozialwissenschaften, 2009, https://doi.org/10.1007/978-3-531-91422-0_6

[10] Wolfgang Merkel
Systemwandel und -wechsel in der Vergleichenden Politikwissenschaft. In *Handbuch Vergleichende Politikwissenschaft*, pp. 1-15, Springer Fachmedien Wiesbaden, 2015, https://doi.org/10.1007/978-3-658-02993-7_8-1

[11] Olaf Winkel
Zukunftsperspektive Electronic Government. *Aus Politik und Zeitgeschichte*, Vol. B18/2004, pp. 7-15, Bundeszentrale für politische Bildung, Bonn, 2004, https://bpb.de/system/files/pdf/XVUNGN.pdf

[12] Jasper Steinlein
E-Voting ist sicherer als analoge Wahl. *tagesschau.de*, 04.03.2019, https://www.tagesschau.de/ausland/estland-wahl-cyber-101.html (abgerufen am: 14.08.2021)

[13] Fintropolis
Estland: ganz schön smart!. *fintropolis.de*, 10.03.2021, https://www.fintropolis.de/article/estland-ganz-smart (abgerufen am: 16.08.2021)

[14] e-estonia
e-governance. *e-estonia.com*, 2021, https://e-estonia.com/solutions/e-governance/government-cloud/ (abgerufen am: 16.08.2021)

[15] Katharina Goldberg
Estland, der digitale Musterstaat. *juwiss.de*, 24.10.2017, https://www.juwiss.de/112-2017/ (abgerufen am: 16.08.2021)

[16] Johannes Merkert
Wahl in Estland: Ein Fünftel gibt Stimme per I-Voting ab. *heise online*, 27.02.2015, https://www.heise.de/newsticker/meldung/Wahl-in-Estland-Ein-Fuenftel-gibt-Stimme-per-I-Voting-ab-2561003.html (abgerufen am: 16.08.2021)

[17] Mihkel Solvak und Kristjan Vassil
E-voting in Estonia: Technological Diffusion and Other Developments Over Ten Years (2005 - 2015). *University of Tartu, Johan Skytte Institute of Political Studies*, 2016, https://skytte.ut.ee/sites/default/files/skytte/e_voting_in_estonia_vassil _solvak_a5_web.pdf (abgerufen am: 17.08.2021)

[18] State Electoral Office of Estonia
General Framework of Electronic Voting and Implementation thereof at National Elec-

tions in Estonia. *State Electoral Office of Estonia*, 20.06.2017, https://www.valimised.ee/sites/default/files/uploads/eng/IVXV-UK-1.0-eng.pdf (abgerufen am: 17.08.2021)

[19] Florian Hartleb
Estland – eine digitale Erfolgsgeschichte. In *Perspektive Smart Country – Wie digitale Transformationen unser Leben verändern*, pp. 38-39, Bertelsmann Stiftung, 2017, https://www.bertelsmann-stiftung.de/fileadmin/files/Projekte/Smart_Country/PerspektiveSmartCountry_2017.pdf

[20] Markus Reiners
E-Voting in Estland: Vorbild für Deutschland?. In *Aus Politik und Zeitgeschichte*, pp. 33-38, Bundeszentrale für politische Bildung, 2017, https://www.bpb.de/shop/zeitschriften/apuz/255952/apuz

[21] Der Beauftragte für den Datenschutz und die Informationsfreiheit
Historie zur Vorratsdatenspeicherung. 2021a, https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Telefon-Internet/Positionen/Historie_zur_Vorratsdatenspeicherung.html (abgerufen am: 18.08.2021)

[22] Der Beauftragte für den Datenschutz und die Informationsfreiheit
Vorratsdatenspeicherung. 2021b, https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Telefon-Internet/Positionen/Vorratsdatenspeicherung.html?nn=252990 (abgerufen am: 18.08.2021)

[23] Stefan Krempl
EU-Staaten wollen neue Regeln zur Vorratsdatenspeicherung. *heise online*, 08.07.2017. https://www.heise.de/newsticker/meldung/EU-Staaten-wollen-neue-Regeln-zur-Vorratsdatenspeicherung-3767450.html (abgerufen am: 20.08.2021)

[24] Seehofer für längere Vorratsdatenspeicherung. *tagesschau*, 26.07.2020. https://www.tagesschau.de/inland/seehofer-vorratsdatenspeicherung-103.html (abgerufen am: 20.08.2021)

[25] Stefan Hügel
Und täglich grüßt das Murmeltier. *netzpolitik.org*, 26.05.2021. https://netzpolitik.org/2021/vorratsdatenspeicherung-und-taeglich-gruesst-das-murmeltier/ (abgerufen am: 20.08.2021)

[26] Datenschutz.org
Vorratsdatenspeicherung – Stehen alle Menschen unter Generalverdacht?. *Daten-*

schutz.org, 24.07.2021,
https://www.datenschutz.org/vorratsdatenspeicherung/ (abgerufen am: 01.06.2021)

[27] Antonie Moser-Knierim
Vorratsdatenspeicherung, Springer Fachmedien Wiesbaden, 2014,
https://doi.org/10.1007/978-3-658-04156-4

[28] Peter Mühlbauer
Vorratsdatenspeicherung für eine 0,006 Prozentpunkte höhere Aufklärungsquote. *heise online*, 16.07.2007,
https://www.heise.de/newsticker/meldung/Vorratsdatenspeicherung-fuer-eine-0-006-Prozentpunkte-hoehere-Aufklaerungsquote-151466.html (abgerufen am: 18.08.2021)

[29] Conrad Chan et. al.
China's Great Firewall - Background Information. *Free speech vs Maintaining Social Cohesion - A Closer look at Different Policies*, 2011,
https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreeExpressionVsSocialCohesion/china_policy.html
(abgerufen am: 01.08.2021)

[30] Jennifer Cheung
China's 'great firewall' just got taller. *openDemocracy - digitaLiberties*, 14.07.2015,
https://www.opendemocracy.net/en/digitaliberties/chinas-great-firewall-just-got-taller/ (abgerufen am: 01.08.2021)

[31] Große Firewall. *GazWiki*,
https://gaz.wiki/wiki/de/Great_Firewall_of_China (abgerufen am: 02.08.2021)

[32] Rebecca MacKinnon
Flatter world and thicker walls? Blogs, censorship and civic discourse in China. *Public Choice*, Vol. 134 (1-2), pp. 31-46, Springer Science and Business Media LLC, 2007,
https://www.jstor.org/stable/27698209

[33] Uli Franz
Porträt: Deng Xiaoping. *Bundeszentrale für politische Bildung*, 2008,
https://www.bpb.de/internationales/asien/china/44262/deng-xiaoping (abgerufen am: 04.08.2021)

[34] Qian Gang
What Ails the People's Daily. *China Media Project*, 24.02.2020,

https://chinamediaproject.org/2020/02/24/what-ails-the-peoples-daily/ (abgerufen am: 04.08.2021)

[35] Xingan Li
Regulation of Cyber Space: An Analysis of Chinese Law on Cyber Crime. *International Journal of Cyber Criminology*, Vol. 9 (2), pp. 185-204, 2015

[36] Cybercrime laws in the People's Republic of China. *Cybercrime Law*,
https://www.cybercrimelaw.net/China.html (abgerufen am: 05.08.2021)

[37] Claudio R.
The Great Firewall Of China – What Is It And How To Bypass It. *Anonymster*, 20.03.2017,
https://anonymster.com/tutorials/great-firewall-china-bypass/
(abgerufen am: 05.08.2021)

[38] Measures for the Administration of Internet Information Services (Chinese Text and CECC Partial Translation). *Congressional-Executive Commission on China*, 2000,
https://www.cecc.gov/resources/legal-provisions/measures-for-the-administration-of-internet-information-services-cecc (abgerufen am: 05.08.2021)

[39] Christoph Giesen
China kappt alle Verbindungen zum freien Internet. *Süddeutsche Zeitung*, 31.03.2018,
https://www.sueddeutsche.de/politik/china-die-neue-grosse-mauer-1.3926957 (abgerufen am: 05.08.2021)

[40] Matt Schmitz
Wie die große Firewall Chinas die Leistung von Websites außerhalb Chinas beeinflusst. *Dotcom-Monitor*, 26.06.2020,
https://www.dotcom-monitor.com/blog/de/2020/06/26/how-the-great-firewall-of-china-affects-performance-of-websites-outside-of-china/
(abgerufen am: 05.08.2021)

[41] Yaqiu Wang
In China, the 'Great Firewall' Is Changing a Generation. *Politico*, 01.09.2020,
https://www.politico.com/news/magazine/2020/09/01/china-great-firewall-generation-405385 (abgerufen am: 02.08.2021),

[42] Prof. Dr. Thomas Heberer
Rolle und Verständnis des chinesischen Staates. *Bundeszentrale für politische Bildung*, 2020,

https://www.bpb.de/internationales/asien/china/322033/rolle-und-verstaendnis-des-chinesischen-staates (abgerufen am: 02.08.2021)

[43] Christoph Giesen
Han, Uiguren und andere Chinesen. *Süddeutsche Zeitung*, 24.11.2019,
https://www.sueddeutsche.de/politik/china-ethnien-han-uiguren-1.4694373 (abgerufen am: 03.08.2021)

[44] Han Dynastie, das erste große Imperium in China. *China Rundreisen*,
https://www.chinarundreisen.com/china-info/han-dynastie.htm
(abgerufen am: 03.08.2021)

[45] Christina Maags
Neue Mauern II: Die Große Firewall Chinas. *BTI Project Blog*,
https://blog.bti-project.de/2019/10/14/neue-mauern-ii-die-grosse-firewall-chinas/ (abgerufen am: 03.08.2021)

[46] Young Xu
Deconstructing the Great Firewall of China. *Thousand Eyes*, 08.03.2016,
https://www.thousandeyes.com/blog/deconstructing-great-firewall-china
(abgerufen am: 07.08.2021)

[47] Richard Clayton, Steven J. Murdoch, Robert N. M. Watson
Ignoring the Great Firewall of China. *I/S: A Journal of Law and Policy for the Information Society*, Vol. 3 (2), Ohio State University, 2007

[48] Nicholas Weaver, Robin Sommer, Vern Paxson
Detecting Forged TCP Reset Packets. *Proceedings of the Network and Distributed System Security Symposium, NDSS 2009*, The Internet Society, 2009

[49] Anonym
Towards a Comprehensive Picture of the Great Firewall's DNS Censorship. *FOCI 2014*, 2014,
https://www.usenix.org/system/files/conference/foci14/foci14-anonymous.pdf (abgerufen am: 09.08.2021)

[50] Wei Chun Chew
How It Works: Great Firewall of China, 01.05.2018,
https://medium.com/@chewweichun/how-it-works-great-firewall-of-china-c0ef16454475
(abgerufen am: 06.08.2021)

[51] Arthur Herman
Huawei's (And China's) Dangerous High-Tech Game. Forbes, 10.12.2018, https://www.forbes.com/sites/arthurherman/2018/12/10/huaweis-and-chinas-dangerous-high-tech-game/ (abgerufen am: 06.08.2021)

[52] Daniel Anderson
Splinternet Behind the Great Firewall of China. *ACM Queue*, Vol. 10 (11), pp. 40-49, ACM, 2021, https://dl.acm.org/doi/abs/10.1145/2390756.2405036

[53] Anonym
The Collateral Damage of Internet Censorship by DNS Injection. *Computer Communication Review*, Vol. 42 (3), pp. 21-27, AGM SIGCOMM, 2012, http://dx.doi.org/10.1145/2317307.2317311

[54] Hilmar Schmundt, Wieland Wagner
Chinesische Mauer 2.0. *Spiegel Online*, 27.04.2008, https://www.spiegel.de/politik/chinesische-mauer-2-0-a-7fa41c78-0002-0001-0000-000056756404 (abgerufen am: 09.08.2021)

[55] Nguyen Phong Hoang et. al.
How Great is the Great Firewall? Measuring China's DNS Censorship, 2021, https://arxiv.org/pdf/2106.02167.pdf (abgerufen am: 09.08.2021)

[56] The Great Firewall of China: A Digital Black Hole. *Catchpoint*, 18.11.2019, https://www.catchpoint.com/blog/great-firewall-of-china (abgerufen am: 09.08.2021)

[57] DNSSEC – Domain Name System Security Extensions. *DENIC*, https://www.denic.de/wissen/dnssec/ (abgerufen am: 09.08.2021)

[58] Anirudh Kannan
Here's why the Great Firewall of China has benefited the country. *Young Post*, South China Morning Post, 12.10.2017 https://www.scmp.com/yp/discover/your-voice/opinion/article/3066603/heres-why-great-firewall-china-has-benefited-country, (abgerufen am: 10.08.2021)

[59] Rebecca Sauber
WeChat: Was ist das? Alle Features im Überblick. *CHIP Praxistipps*, 10.08.2020, https://praxistipps.chip.de/wechat-was-ist-das-alle-features-im-ueberblick_123406 (abgerufen am: 10.08.2021)

[60] The top 500 sites on the web, https://www.alexa.com/topsites (abgerufen am: 12.08.2021)

[61] Christopher Balding
How Badly Is China's Great Firewall Hurting the Country's Economy?. *Foreign Policy*, 18.07.2017,
https://foreignpolicy.com/2017/07/18/how-badly-is-chinas-great-firewall-hurting-the-countrys-economy/, (abgerufen am: 10.08.2021)

[62] Nigel Cory
Testimony Before the Senate Subcommittee on International Trade, Customs, and Global Competitiveness of the Committee on Finance, Hearing on 'Censorship as a Non-Tariff Barrier to Trade', 03.03.2020,
https://www2.itif.org/2020-censorship-non-tariff-barrier-trade.pdf (abgerufen am: 10.08.2021)

[63] Alexander Chipman Koty
China's Great Firewall: Business Implications. *China Briefing*, 01.06.2017,
https://www.china-briefing.com/news/chinas-great-firewall-implications-businesses/ (abgerufen am: 10.08.2021)

[64] Prof. Dr. Oliver Bendel
Sozialkreditsystem. *Gabler Wirtschaftslexikon*, 13.07.2021,
https://wirtschaftslexikon.gabler.de/definition/sozialkreditsystem-100567/version-384523 (abgerufen am: 11.08.2021)

[65] Planning Outline for the Construction of a Social Credit System (2014-2020), 2014,
https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/ (abgerufen am: 12.08.2021)

[66] Chuncheng Liu
Multiple Social Credit Systems in China. *Economic Sociology: The European Electronic Newsletter*, Vol. 21 (1), pp. 22-32, 2019, https://dx.doi.org/10.2139/ssrn.3423057

[67] Christoph Jehle
Digital Vertrauen schaffen. *Telepolis*, Heise Online, 18.09.2020,
https://www.heise.de/tp/features/Digital-Vertrauen-schaffen-4892881.html (abgerufen am: 15.08.2021)

[68] Leonie Ludwig
Wie Chinas Sozialkredit-System wirklich funktioniert. *Krosse.info*, 12.01.2021,

https://krosse.info/wie-chinas-sozialkredit-system-wirklich-funktioniert/ (abgerufen am: 15.08.2021)

[69] VICE News
China's 'Social Credit System' Has Caused More Than Just Public Shaming (HBO), 12.12.2018, https://www.youtube.com/watch?v=Dkw15LkZ_Kw

[70] Genia Kostka
Kostka, Genia, China's Social Credit Systems and Public Opinion: Explaining High Levels of Approval, 23.07.2018, https://dx.doi.org/10.2139/ssrn.3215138

[71] Kommunikations- und Marketingbüro der FU Berlin
Study: More than two thirds of Chinese take a positive view of social credit systems in their country, 23.07.2018,
https://www.fu-berlin.de/en/presse/informationen/fup/2018/fup_18_198-studie-sozialkreditsystem-china/index.html

[72] Zhou Tailai, Matthew Walsh
In Depth: How Chinese Companies Can Get Off Social Credit Blacklists. *Caixin*, 27.05.2020,
https://www.caixinglobal.com/2020-05-27/in-depth-how-chinese-companies-can-get-off-social-credit-blacklists-101559282.html (abgerufen am: 16.08.2021)

[73] Jay Stanley
China's Nightmarish Citizen Scores Are a Warning For Americans. *ACLU*, 05.10.2015, https://www.aclu.org/blog/privacy-technology/consumer-privacy/chinas-nightmarish-citizen-scores-are-warning-americans (abgerufen am: 16.08.2021)

[74] Nicole Kobie
The complicated truth about China's social credit system. *Wired*, 07.06.2019,
https://www.wired.co.uk/article/china-social-credit-system-explained (abgerufen am: 16.08.2021)

[75] Tyler Grant
The West could be closer to China's system of 'social credit scoring' than you think. *The Hill*, 07.05.2018,
https://thehill.com/opinion/technology/386524-the-west-could-be-closer-to-chinas-system-of-social-credit-scoring-than (abgerufen am: 16.08.2021)

[76] Louise Matsakis
How the West Got China's Social Credit System Wrong. *Wired*, 29.07.2019,

https://www.wired.com/story/china-social-credit-score-system/
(abgerufen am: 16.08.2021)

[77] Shazeda Ahmed
The Messy Truth About Social Credit. *logic magazine*, 01.05.2019,
https://logicmag.io/china/the-messy-truth-about-social-credit/
(abgerufen am: 16.08.2021)

[78] Christiane Körner, Andrej Soldatov
Überwachung und Strafen: Die Verschärfung der Internetkontrolle in Russland. *Osteuropa*, Vol. 66 (11/12), pp. 3-14, Berliner Wissenschafts-Verlag, 2016,
https://www.jstor.org/stable/44937771

[79] Irina Kharuk
Internetfreiheit in Russland nach den Wahlen 2011–2012: Änderungen und neue Herausforderungen aus der Sicht von Medienexpert_innen und Journalist_innen, FU Berlin, 31.08.2020,
https://refubium.fu-berlin.de/bitstream/handle/fub188/28389/Kharuk_Irina_Dissertation_2020.pdf

[80] Andrei Soldatov and Irina Borogan
Putin brings China's Great Firewall to Russia in cybersecurity pact. *The Guardian*, 29.11.2016,
https://www.theguardian.com/world/2016/nov/29/putin-china-internet-great-firewall-russia-cybersecurity-pact (abgerufen am: 20.08.2021)

[81] Thielko Grieß
Das Ende des anonymen Surfens im russischen Netz?. *Deutschlandfunk.de*, 02.11.2017,
https://www.deutschlandfunk.de/internetzensur-in-russland-das-ende-des-anonymen-surfens-im.2907.de.html?dram:article_id=399678 (abgerufen am: 20.08.2021)

[82] Silke Bigalke
Russland will sich vom globalen Internet abkoppeln. *Süddeutsche Zeitung*, 11.04.2019,
https://www.sueddeutsche.de/digital/russland-internet-zensur-abschottung-telegram-opposition-ueberwachung-1.4404609 (abgerufen am: 20.08.2021)

[83] Putin koppelt Russland vom Internet ab. *Spiegel Online*, 01.11.2019,
https://www.spiegel.de/politik/ausland/wladimir-putin-koppelt-russland-vom-internet-ab-umstrittenes-gesetz-a-1294331.html (abgerufen am: 20.08.2021)

[84] Diwen Xue et. al.
Throttling of Twitter in Russia. *Censored Planet at the University of Michigan*, 06.04.2021, https://censoredplanet.org/throttling (abgerufen am: 20.08.2021)

[85] dpa
Russland verlangsamt Twitter - und droht mit Blockade. *Zeit Online*, 10.03.2021, https://www.zeit.de/news/2021-03/10/russland-verlangsamt-twitter-und-droht-mit-blockade (abgerufen am: 20.08.2021)

[86] Sonja Peteranderl
Wie die Taliban die Identitätserkennung der Amerikaner nutzen können. *Spiegel Online*, 19.08.2021,
https://www.spiegel.de/ausland/afghanistan-wie-die-taliban-die-identitaetserkennung-der-amerikaner-ausnutzen-koennen-a-c6c5aa4f-29e4-4b34-ba90-a78dbbf5c43d (abgerufen am: 21.08.2021)