

Rost Likholat

Das Internet existiert nicht

Eine dystopische Perspektive des Cyber-Isolationismus

Das weltweite Netzwerk, welches umgangssprachlich als Internet bezeichnet wird, ist kein alleinstehendes homogenes Ding. Vielmehr wird es auf konsensueller Basis aus der Gesamtheit aller teilnehmenden Subnetze gebildet.

Die Grundlage fürs funktionieren des Informationsaustauschs eines jeden Subnetzes sind Identifikatoren, die allen Netzabonenten wie PCs, Handys, Druckern, etc individuell zugewiesen werden. Der Zusammenschluss mehrerer Netzwerke setzt die Eindeutigkeit dieser IDs, welche über das ganze Gesamtnetzwerk hinweg für jeder einzelne Gerät koordiniert werden muss voraus.¹ Im Internet sowie in allen anderen auf TCP Protokoll basierenden Netzen übernehmen die IP-Adressen die Funktion dieser eindeutigen IDs. Vergeben und verwaltet werden diese von der Internet Corporation for Assigned Names and Numbers (ICANN).

ICANN ist eine nichtstaatliche non-profit organisation aus USA, die auf der Grundlage eines freiwilligen internationalen Konsens operiert.² Wenn eine IP-Adresse von der ICANN zugewiesen wird, stimmen freiwillige Teilnehmer dieser Entscheidung zu, woraufhin die Adresse über das DNS im Internet propagiert wird. Solch eine Körperschaft zur Koordinierung der globalen IP-Adressen ist die Voraussetzung für die Existenz des vereinten Internets.³ Obwohl die Struktur von ICANN für alle Beteiligten vorteilhaft ist, gibt es keine Kraft, welche die Länder dazu zwingt an der zentralen Vergabe der IP-Adressen teilzunehmen.

Das einzige was die einzelnen Staaten daran hindert lokale Behörden einzurichten, die eine inländische Vergabe von IPs übernehmen würden, ist die Tatsache, dass solche nationale Netzwerke keinerlei Konnektivität zur Außenwelt besitzen würden. Die Nutzer*Innen solcher Netze würden lediglich auf die Adressen zugreifen können, die der entsprechenden nationalen Behörde unterliegen. Das ICANN lässt das Internet als ein einheitliches globales Netzwerk funktionieren, jedoch würde die Abwesenheit eines solchen internationalen Mechanismus der Konsensbildung ein Multiversum parallel existierender "Internets" schaffen, in dem das Konzept, jeden auf der ganzen Welt zu erreichen, völlig fremd wäre.⁴

Einige Forscher*innen schlagen bereits Alarm, dass der Tod des einheitlichen und globalen Internets bereits im gange ist. Immer mehr Regierungen finden gefallen an der Idee der Cyber-Isolationismus und schaffen Voraussetzungen zur Durchsetzung ihrer "digitalen Souveränität".

¹ <https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-computer-networking.html>

² <https://www.icann.org/resources/pages/effect-2012-02-25-en>

³ <https://www.icann.org/resources/pages/what-2012-02-25-en>

⁴ <https://teconomy.com/welcome-to-the-splinternet>

In Fachkreisen wächst die Befürchtung, dass diese staatlich geschaffene und von Großunternehmen ermöglichte Netzzersplitterung multiple "nationale Internets" und "Gärten hinter hohen Mauern" zufolge haben wird. Mittlerweile hat sich für dieses Phänomen die Bezeichnung "Splinternet" etabliert. Versteht man das Internet als ein weltweites Netzwerk aller Netzwerke, so ist das Splinternet ein Gegenteil davon.⁵ Zum jetzigen Zeitpunkt hören bereits die ersten Staaten auf, sich am ICANN-Konsens zu beteiligen, und beginnen damit, ihre IP-Adressen auf eigene Faust lokal zuzuweisen.

Das gleiche Effekt wird auch dadurch erreicht, wenn Regierungen landesweite Firewalls einrichten, um den freien Informationsfluss in das und aus dem Land einzuschränken. Beide Tendenzen sind bereits gegenwärtig und auf dem besten Weg, das weltweit erste Splinternet zu schaffen.⁶

Kürzlich nach der Invasion Russlands stellte Ukraine eine Anfrage an ICANN, die einen Ausschluss aller russischen IP-Adressen aus dem Internet forderte. Dies würde die Mehrheit aller .ru-Websites, sowie alle russische Endgeräte wie Computer und Smartphones aus dem globalen Internet verschwinden lassen.⁷ ICANN lehnte die Forderung der Ukraine ab, mit der Begründung, dass es der Corporation weder technisch möglich wäre, noch ihre Aufgabe sei, Sanktionen in Form der Entfernung von IP-Adressen aus dem Internet zu erlassen.

Der Konsens aller Internetbetreiber besteht darin, den Entscheidungen von ICANN folge zu leisten. Dadurch wird garantiert, dass kein Operator über den anderen hinweg entscheiden kann. Der einzige Akteur, der Internet in Russland effektiv lahmlegen kann, ist der Kreml selbst.⁸ In der Tat bereitet sich die Regierung Russlands darauf vor, den Russischen segment des Internets vom Rest der Welt eigenständig abzutrennen, genau wie das von der Ukraine gewünscht wurde. Das Russian National Domain Name System wurde 2021 als konkurrierende Organisation zu ICANN von Kreml ins Leben gerufen. Deren Ziel ist es die Vergabe von IP-Adressen auch dann zu gewährleisten, wenn das Subnetz Russlands vom globalen Internet abgetrennt wird.⁹ Am 15.6.2021 und 15.7.2021 wurden die lokalen Telekommunikationsanbieter und Internet Service Provider Russlands vom Rest des Internets abgetrennt, um zu sehen, ob russische Websites immer noch aufgerufen werden können. Nach offiziellen Angaben verliefen diese Tests erfolgreich.¹⁰ In Zukunft sollen diese Tests jährlich abgehalten und als Teil einer breiter angelegten

⁵ <https://www.economist.com/briefing/2010/09/02/a-virtual-counter-revolution>

⁶ <https://techonomy.com/welcome-to-the-splinternet>

⁷ <https://www.technologyreview.com/2022/03/17/1047352/russia-splinternet-risk>

⁸ <https://edition.cnn.com/2022/03/03/tech/ukraine-russia-internet-icann/index.html>

⁹ <https://www.bloomberg.com/news/articles/2022-03-10/russia-internet-isolation-accelerates-after-ukraine-invasion>

¹⁰ <https://fortune.com/2022/03/22/russia-war-ukraine-great-firewall-splinternet-internet>

Initiative zum Aufbau des eigenen Splinternets namens Runet verstanden werden.¹¹ Vorerst sollte dieser Schritt das russische Internet widerstandsfähiger machen, doch gleichzeitig dient es dazu ein souveränes Netzwerk, das unabhängig vom globalen Konsens funktionieren kann, aufzubauen. Wenn weitere Länder oder Blöcke diesem Beispiel folgen, könnte dies den Anfang eines kalten Informationskrieg einläuten.¹² Dieser würde in Form eines Internet-Wettrüstens stattfinden, bei dem die Nationen sich ermutigt fühlen könnten, Cyberangriffe auf einander zu starten, um das Splinternetz der Gegenseite lahmzulegen, da die nicht vorhandene globale Vernetzung der Opferseite die Gefahr von Fehlschlägen und Kollateralschäden massiv reduzieren würde.¹³

Die Gefahr der Entstehung des Splinternets geht aber nicht allein von nationalen Behörden aus, welche den globalen Internet-Konsens aufheben könnten. Die sogenannten Edge Provider, zu denen die größten sozialen Netzwerke und Suchmaschinen zählen, sind längst zu den zentralen Gatekeepern für den Großteil der Inhalte geworden, welche von den meisten Nutzer*innen konsumiert werden. Einige dieser Dienste werden von Unternehmen mit Quasi-Infrastrukturstatus betrieben.¹⁴ Mit einem monopolähnlichen Marktanteil bietet Amazon Web Services Cloud-Dienstleistungen für viele wichtige Apps und Dienste an. Im Bereich der Suchmaschinen kontrolliert Google 80% des Marktes.¹⁵ Gleichzeitig besitzt Meta die größten sozialen Netzwerke, für die es derzeit keine Alternative gibt.¹⁶ Apple Corporation hat das iPhone-Ökosystem im Würgegriff und übt einseitige Kontrolle darüber aus, welche Apps oder Geräte innerhalb der Plattform zugelassen sind.¹⁷ Jede Entscheidung derartiger Unternehmen birgt in sich ein enormes Schadenspotential für seine NutzerInnen.

Als Apple sich entschied, Nachrichten-Apps wie Quartz oder The New York Times aus dem chinesischen App Store zu verbannen, bedeutete dies, dass keine iPhone-BenutzerInnen mehr in der Lage waren diese Apps verwenden zu können und es keine Möglichkeit gab, diese Restriktion effektiv zu umgehen.¹⁸ Da Nutzer*Innen von Android ihre Apps nicht nur aus dem Play Store, sondern auch beliebigen Quellen installieren können, hat Apple mit seiner Entscheidung das Splinternetz lediglich die fürs iPhone Ökosystem in China herbeigeführt. Als Amazon beschloss, den Betrieb in

¹¹ <https://www.reuters.com/technology/russia-disconnected-global-internet-tests-rbc-daily-2021-07-22>

¹² <https://www.bloomberg.com/news/articles/2022-03-10/russia-internet-isolation-accelerates-after-ukraine-invasion>

¹³ <https://fortune.com/2022/03/22/russia-war-ukraine-great-firewall-splinternet-internet>

¹⁴ <https://www.reuters.com/article/amazon-cloud-idUSN1E7A727Q20111109> und <https://www.statista.com/topics/4418/amazon-web-services>

¹⁵ <https://www.statista.com/topics/4418/amazon-web-services> und <https://www.statista.com/statistics/216573/worldwide-market-share-of-search-engines>

¹⁶ <https://about.facebook.com/meta>

¹⁷ <https://www.nytimes.com/2019/04/27/technology/apple-screen-time-trackers.html>

¹⁸

<https://www.theverge.com/2019/10/9/20907228/apple-quartz-app-store-china-removal-hong-kong-protests-censorship>
<https://www.nytimes.com/2017/01/04/business/media/new-york-times-apps-apple-china.html>

Russland einzuschränken, bedeutete dies für seine russische Nutzer*Innen, dass sie den Zugang zu Amazons Marktplatz-, Cloud- und Streaming-Service verlieren würden.

Der Rückzug anderer Unternehmen wie Oracle, Dell, Visa oder Microsoft ergab ein Vakuum von Diensten, die nun ausbleiben oder lokal bereitgestellt werden müssen, abgesplittert vom globalen Internet.¹⁹ Die Europäische Union begann bereits damit, Technologieunternehmen unter Druck zu setzen um den Zugang zu den russischen Medien wie RT und Sputnik nicht nur zu verbieten, sondern auch all die Inhalte in Suchmaschinen und Social-Media Apps zu verbannen, die ihre Publikationen wiederholen.

Während die Argumentation, dass staatspropagandistische Medien schädlich sind, auf der Oberfläche liegt, schafft ein derartiges Vorgehen der Europäischen Regierungen gegen Fehlinformationen potentiell gefährliche Präzedenzfälle, die Europäer*Innen einen Schritt weiter weg vom uneingeschränkten Zugang zum Internet positionieren. Es ist erschreckend einfach, die Forderungen nach Zensur in sozialen Medien und Suchmaschinen durchzusetzen.²⁰

Google und Facebook verbrachten Jahre damit, ihre Algorithmen zu trainieren, um Inhalte in Social-Media-Feeds und Suchergebnissen zu personalisieren. Berichte zeigten, dass die meisten Inhalte, die Benutzer abonnieren, niemals in ihrem Feed landen werden. Stattdessen bestimmen eine Reihe von Merkmalen wie das Verhalten der User und ihre Webseiteninteraktionen, was im Feed zu sehen ist.²¹

Google hat bereits zugegeben, dass sein Algorithmus an sogenannten Filterblasenproblem leidet. Das bedeutet, dass es eine algorithmische Voreingenommenheit den einzelnen Benutzern gegenüber gibt, welche darin resultiert, dass bei gleichen Input-Variablen unterschiedliche Vorschläge gemacht werden. Voreingenommenheit dieser Art entsteht hauptsächlich aus Parametern, deren Relevanz jenseits des Bereichs einer konkreten Suchanfrage liegt.²²

Als negatives Paradebeispiel für ein Land, in dem die Verflechtung der Regierung mit diversen IT-Unternehmen eine größere Abspaltung des Internets hervorgerufen hat, dient China. Seitdem die Regierung Chinas die "Große Firewall" errichtet hat, wird der freie Fluss ausländischer Informationen nach China effektiv unterbunden. Zusätzlich

19

<https://www.reuters.com/business/oracle-says-it-has-suspended-all-operations-russia-2022-03-02>

<https://finance.yahoo.com/news/russian-splinternet-014035581.html>

<https://www.bloomberg.com/news/articles/2022-03-10/russia-internet-isolation-accelerates-after-ukraine-invasion>

²⁰ <https://www.technologyreview.com/2022/03/17/1047352/russia-splinternet-risk>

²¹ <https://www.theguardian.com/technology/2017/may/22/social-media-election-facebook-filter-bubbles>

²² <https://qz.com/1194566/google-is-finally-admitting-it-has-a-filter-bubble-problem>

stellt eine speziell dafür eingerichtete Cyber-Behörde sicher, dass alle Suchanfragen, Kommentare und Posts der Bürger*Innen mit ihrer realen Identität verknüpft werden können. Im Zuge dieses Kreuzzuges gegen die Online-Anonymität, sind Dienste wie TOR und VPN im Land illegal gemacht worden, wobei Unternehmen wie Apple bereitwillig mit dieser Politik gegen Online-Freiheiten kooperierten.²³

Gründer*Innen von privaten Chatgruppen werden für alle Inhalte rechtlich verantwortlich gemacht, während die Internetunternehmen dazu verpflichtet wurden, das Verhalten von NutzerInnen zu überwachen und zu bewerten sowie ihnen gemäß einer Richtlinie der Kommunistischen Partei Chinas Punkte zuweisen. Aktuelle Zensurmechanismen Chinas verbieten und entfernen immer mehr Apps und Inhalte, die frühere Zensurmethoden nicht beseitigen konnten.²⁴

Alle ausländischen Social-Media Apps sind in VRC verboten worden, sodass nur von der Regierung autorisierte chinesische Unternehmen eine Online-Plattformen unterhalten dürfen. Da alle Chinesen nur lokale Dienste nutzen können, gibt es keine direkte Kommunikationslinie zwischen Benutzer*Innen aus China und dem Rest der Welt. Momentan entwickelt die chinesische Regierung mit Hilfe heimischer Unternehmen ein neues Internetprotokoll, welches den Aufbau eines landesweiten Netzwerks mit einer Top-Down Struktur ermöglichen soll. Die Unterschiede zum aktuellen Internetprotokoll sind enorm. Während eine globale IP es allen erlaubt, eine eigene Website zu hosten, solange ein Computer mit Internetzugang zur Verfügung steht, muss in China dafür eine Lizenz beantragt werden.²⁵

Das globale Internet hat eine intrinsische Undichtigkeit – was bedeutet, dass keine landesweiten Firewall-Kontrollen ihre Benutzer vollständig abschotten können. Das neue Internetprotokoll würde Zugriffskontrollen fest in das Verbindungsprotokoll eincodieren, damit die chinesischen Zensoren die Geräte innerhalb ihrer Netzwerke automatisiert einschränken können. Mit Hilfe zentral vergebener IP-Adressen würde jeder Internetzugang einer Zulassung bedürfen und Administrator*Innen hätten die Möglichkeit, das Netzwerk im Whitelist-Modus zu betreiben, in dem nur vertrauenswürdige Geräte, Apps und Websites operieren dürfen.

China hat bislang keine Einzelheiten darüber dargelegt, wie das neue IP-Framework aufgebaut werden soll, allerdings wenn das Projekt Erfolg haben sollte, könnten sie damit beginnen, es Entwicklungsländern als Dienstleistung anzubieten und ihre Kontrolle über Chinas Splinternetz hinaus im Ausland auszudehnen.

²³ <https://www.bloomberg.com/news/articles/2022-03-10/russia-internet-isolation-accelerates-after-ukraine-invasion>

²⁴ https://www.washingtonpost.com/world/asia_pacific/the-walls-are-closing-in-china-finds-new-ways-to-tighten-internet-controls/2017/09/26/2e0d3562-9ee6-11e7-b2a7-bc70b6f98089_story.html

²⁵ <https://techcrunch.com/2019/03/13/the-splinternet-is-already-here>

Nicht vielen Menschen ist es bewusst, dass sie auf das Internet zugreifen können, weil ihr Internetdienstanbieter ihnen diese Erlaubnis erteilt hat.²⁶ Die monatliche Internetrechnung, ist eine Zahlung für die Nutzung der Router und Kabel des Netzbetreibers, der Milliarden ausgegeben hat, um diese Infrastruktur anbieten zu können. Allerdings, wenn globale ISPs keine Verbindungen mehr untereinander austauschen können, wird der Wert ihrer Internet Vermittlungsdienstleistung sehr schnell auf Null sinken. Das Vertrauen in die Telekommunikationsanbieter ist der Kern des Problems.

Wir tragen und verwenden Geräte, die eine drahtlose Übertragung mit hoher Bandbreite ermöglichen, ohne jemals an eine Telekommunikationsleitung angeschlossen zu sein. Unsere Geräte können auf Peer-to-Peer-Weise miteinander kommunizieren, selbst wenn eine Regierung das Internet für das ganze Land abschaltet. Darin liegt die Lösung für das Problem des Splinternets. Wenn wir unser eigenes Mesh-Netzwerk aus Peer-to-Peer-Verbindungen mit jedem Telefon, Tablet oder PC in Reichweite aufbauen könnten, müssten wir uns nicht so sehr auf die Erdkabeln verlassen. Die einzige Hürde wäre die interkontinentale Kommunikation sowie verbindungen zu den extrem abgelegenen Gebieten. Aber das könnte gelöst werden, wenn es Privatpersonen erlaubt wäre, das Internet mit Drohnen oder Satelliten vom Himmel herunter zu beamen.

Für Städte und dicht besiedelte Regionen sollte eine derartige Kommunikation jedoch bereits möglich sein. Es gibt zwei Projekte, die ich zu diesem Zweck genau verfolge, obwohl sie noch nicht ganz da sind. Briar²⁷ und Cwtch²⁸ bauen Peer-to-Peer Netzwerke auf, die das Internet überhaupt nicht benötigen. Sie können mithilfe von Bluetooth und WLAN, Tor verwenden und Ende-zu-Ende-Verschlüsselung gewährleisten, um die Privatsphäre und Anonymität der Teilnehmenden zu schützen. Allerdings sind beide keine Mesh-Netzwerke, da sie derzeit keine Weiterleitung des Datenverkehrs ermöglichen. Das erste Peer-to-Peer-Netzwerk, das damit beginnt, Mesh-Routing anzubieten, wäre unsere beste Chance, ein wirklich erlaubnisfreies, neutrales und auf verteilten Konsens basierendes Internet zu schaffen, das von keiner einzelnen Behörde abgeschaltet werden kann.

Während die Regierungen versuchen, das einheitliche globale Internet durch Splinternet zu ersetzen, können wir mit dem Aufbau eines völlig neuen, unkontrollierbaren Internets von Grund auf eigenständig beginnen.

²⁶ <https://www.ft.com/content/ba94c2bc-6e27-11ea-9bca-bf503995cd6f>

²⁷ <https://briarproject.org>

²⁸ <https://cwtch.im>

Referenzen

What is Computer Networking?

<https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-computer-networking.html>

What's the effect of ICANN 's role and work on the Internet?

<https://www.icann.org/resources/pages/effect-2012-02-25-en>

What Does ICANN Do?

<https://www.icann.org/resources/pages/what-2012-02-25-en>

Welcome to the Splinternet

<https://techonomy.com/welcome-to-the-splinternet>

A virtual counter-revolution - The Economist

<https://www.economist.com/briefing/2010/09/02/a-virtual-counter-revolution>

Russia is risking the creation of a "splinternet" and it could be irreversible - MIT Technology Review

<https://www.technologyreview.com/2022/03/17/1047352/russia-splinternet-risk>

ICANN rejects Ukraine's request to cut off Russia from the global internet - CNN

<https://edition.cnn.com/2022/03/03/tech/ukraine-russia-internet-icann/index.html>

Ukraine War Accelerates Russia Isolated From US Internet Companies - Bloomberg

<https://www.bloomberg.com/news/articles/2022-03-10/russia-internet-isolation-accelerates-after-ukraine-invasion>

What is the 'Splinternet'?

Russia's war on Ukraine accelerating breakaway Internet - Fortune

<https://fortune.com/2022/03/22/russia-war-ukraine-great-firewall-splinternet-internet>

Russia disconnects from internet in tests as it bolsters security - RBC daily

<https://www.reuters.com/technology/russia-disconnected-global-internet-tests-rbc-daily-2021-07-22>

Amazon finds startup investments in the 'cloud' - Reuters

<https://www.reuters.com/article/amazon-cloud-idUSN1E7A727020111109>

Amazon Web Services - Statistics & Facts - Statista

<https://www.statista.com/topics/4418/amazon-web-services>

Search engine market share worldwide 2022 - Statista

<https://www.statista.com/statistics/216573/worldwide-market-share-of-search-engines>

Welcome to Meta

<https://about.facebook.com/meta>

Apple Cracks Down on Apps That Fight iPhone Addiction - The New York Times

<https://www.nytimes.com/2019/04/27/technology/apple-screen-time-trackers.html>

Apple's App Store is now also under antitrust scrutiny in the UK | TechCrunch

<https://techcrunch.com/2021/03/04/apples-app-store-is-now-also-under-antitrust-scrutiny-in-the-uk>

Apple reportedly removes Quartz news app in China over Hong Kong coverage - The Verge

<https://www.theverge.com/2019/10/9/20907228/apple-quartz-app-store-china-removal-hong-kong-protests-censorship>

Apple Removes New York Times Apps From Its Store in China

<https://www.nytimes.com/2017/01/04/business/media/new-york-times-apps-apple-china.html>

Oracle suspends operations in Russia, SAP pauses sales

<https://www.reuters.com/business/oracle-says-it-has-suspended-all-operations-russia-2022-03-02>

The Russian 'splinternet' is here - POLITICO

<https://finance.yahoo.com/news/russian-splinternet-014035581.html>

How social media filter bubbles and algorithms influence the election - The Guardian

<https://www.theguardian.com/technology/2017/may/22/social-media-election-facebook-filter-bubbles>

Google is finally admitting it has a filter-bubble problem - Quartz

<https://qz.com/1194566/google-is-finally-admitting-it-has-a-filter-bubble-problem>

The walls are closing in:

China finds new ways to tighten Internet controls - The Washington Post

https://www.washingtonpost.com/world/asia_pacific/the-walls-are-closing-in-chinafinds-new-ways-to-tighten-internet-controls/2017/09/26/2e0d3562-9ee6-11e7-b2a7-bc70b6f98089_story.html

The 'splinternet' is already here - TechCrunch

<https://techcrunch.com/2019/03/13/the-splinternet-is-already-here>

Inside China's controversial mission to reinvent the internet - Financial Times

<https://www.ft.com/content/ba94c2bc-6e27-11ea-9bca-bf503995cd6f>

Briar Project: Secure messaging, anywhere

<https://briarproject.org>

Cwtch: Surveillance Resistant Network Infrastructure

<https://cwtch.im>