Was ist Plattformpolitik? Grundzüge einer neuen Form der politischen Macht

von Michael Seemann[1]

Anfang des Jahres, kurz nach der Inauguration Donald Trumps, verbreitete sich das Gerücht, der Facebook-Gründer Mark Zuckerberg plane seinerseits, 2020 als Präsidentschaftskandidat ins Rennen zu gehen. Nun ist es nachvollziehbar, dass man nach Trumps Sieg alles für möglich halten kann, jedoch beruhte die Spekulation lediglich auf der sogenannten „listening tour", Zuckerbergs Reise durch die USA, bei der er „Facebook-User" persönlich treffen wollte.[2] Das Gerücht ist nur Anzeichen des allgemeinen Nichtverstehens unserer Zeit. Denn Zuckerberg ist längst ein Politiker. Er hat enormen Einfluss auf das tägliche Leben von zwei Milliarden Menschen. Er trifft Entscheidungen, die beeinflussen, wie diese Menschen sich zusammenschließen, wie sie miteinander umgehen, sogar wie sie die Welt sehen. Zuckerberg ist der vielleicht mächtigste Politiker der Welt. Jeder Job in der klassischen Politik – inklusive dem des US-Präsidenten – wäre eine Degradierung.

In diesem Text möchte ich versuchen zu benennen und zu analysieren, wie Plattformen Politik machen, wie sie ihre Machtbasis organisieren und in welchen Feldern ihre Politik heute bereits die Welt verändert. Doch zunächst müssen wir drei Missverständnisse über Plattformpolitik ausräumen.

Drei Missverständnisse zur Plattformpolitik

1. Plattformen sind nicht (nur) Objekte der Politik, sondern auch mächtige politische Subjekte.

Wenn wir von "Plattformpolitik" oder Plattformregulierung sprechen, dann denken wir uns Plattformen meist als Gegenstand von Regulierung und von Politik. Das ist soweit auch nicht falsch, aber es verdeckt den viel wesentlicheren Punkt, dass Plattformen heute selber mächtige Regulierer und politische Akteure sind.

Plattformen sind die Infrastrukturen unseres digitalen Zusammenlebens – wobei die Betonung auf „Struktur" liegt. Denn diese Struktur ist weder beliebig noch neutral. Die Struktur von Kommunikation vorzugeben ist bereits eine politische Tat, sie ermöglicht bestimmte Interaktionen und verringert die Wahrscheinlichkeit von anderen Arten der Kommunikation; sie ist bereits ein tiefer Eingriff ins Zusammenleben und damit politisch.

Es macht also Sinn, über Plattformen nicht nur als Firmen nachzudenken, die im Internet Services anbieten, sondern sie als politische Entitäten, gar Institutionen zu betrachten.[3] Ihr Einfluss auf die politische Debatte, auf unser Zusammenleben und somit auf politische Entscheidungen steht dem der klassischen Medien in nichts nach. Plattformen können als die 5. Gewalt verstanden werden. Allerdings sind sie im Gegensatz zu den anderen vier Gewalten nicht national organisiert, sondern denken und agieren per se global. Und im Gegensatz zu den anderen Institutionen versuchen sie ihre gesellschaftspolitische Rolle nicht überzubetonen, im Gegenteil; politische Verantwortung zu haben ist schließlich schlecht fürs Geschäft. Vielmehr neigen Plattformen dazu, ihre eigene politische Macht herunterzuspielen und die Verantwortung nicht anzunehmen zu wollen. Sie sind politische Akteure wider Willen.

2. Plattform üben eine andere Form von Macht aus.

Einer der Gründe, warum Plattformen als politische Akteure immer noch nicht ernst genom-

1 Michael Seemann ist Kulturwissenschaftler und Publizist und beschäftigt sich mit Themen rund um Internet und Gesellschaft. Seine Thesen hat er 2014 als Buch veröffentlicht: Das Neue Spiel, Strategien für die Welt nach dem digitalen Kontrollverlust. Weitere Texte von ihm findet man auf ctrl-verlust.net und michaelseemann.de.

2 Alex Heath: Speculation is mounting that Mark Zuckerberg wants to serve in government, http://www.businessinsider.de/speculation-mounting-that-mark-zuckerberg-wants-work-government-2017-1?r=US&IR=T, 05.01.2017.

3 Vgl. Michael Seemann: Das Neue Spiel - Strategien für die Welt nach dem digitalen Kontrollverlust, 2014, S. 204 ff.

men werden, ist das allgemeine Unverständnis für die Mechanik ihrer Macht.

Wenn Politiker gegenüber Plattformen auftreten, legen sie gern das Gewicht ihrer politischen Legitimation in die Waagschale. Sie sprechen dann vom „Primat der Politik", als wollten sie sich und anderen ihrer Handlungsmacht versichern. Dieses Primat wird daraus abgeleitet, dass der Politiker durch eine souveräne, kollektive Entscheidung in sein Amt kam. Doch auch Plattformen generieren eine Form von Legitimation durch kollektive Entscheidungen, die allerdings leicht anders funktioniert.

David Singh Grewal zeigt in seinem Buch Network Power, wie die Adaption von Standards als kollektive Entscheidung verstanden werden kann.[4] Standards sind Möglichkeitsbedingungen von Interaktion, weswegen jede Entscheidung für oder gegen einen Standard immer schon eine gesellschaftliche Tragweite hat. Und nur weil diese Entscheidungen nicht gleichzeitig getroffen werden wie bei einer Wahl, sondern zeitlich versetzt („aggregiert"), mindert das nicht ihre gesellschaftliche Macht.

Die Macht dieser aggregierten kollektiven Entscheidungen ist nichts Neues. Sie gilt für die Sprache, die wir sprechen, für die Umgangsformen, die wir pflegen oder akzeptieren und natürlich auch für die Entscheidung, über welche Netzwerkdienste wir erreichbar sein wollen. Wir sind schließlich nicht auf Facebook wegen seiner tollen Produktqualität, sondern weil alle unsere Freunde auf Facebook sind.

In der Ökonomie nennt man das Phänomen „Netzwerkeffekt", aber Grewal hat völlig recht, es als politischen Machtfaktor zu verstehen. Ab einer bestimmten Ausbreitung eines Standards sind die Kräfte auf das Individuum so groß, dass ihm kaum etwas anderes übrigbleibt, als den Standard ebenfalls zu adaptieren. Die Alternative ist häufig sozialer Ausschluss. Wir akzeptieren diese „Netzwerkmacht", die Standards ausüben, denn sie kann schließlich nicht von Einzelnen in Stellung gebracht werden. Das gilt zumindest für offene Standards. Niemand kann mich davon abhalten, Russisch zu lernen, oder einen Server mittels offener Protokolle wie TCP/IP im Internet bereit zu stellen. Der soziale Druck geht immer von der ganzen Gemeinschaft aus und kann nicht von Einzelnen gerichtet werden.

Zur "Plattformmacht" wird die Netzwerkmacht aber, wenn der adaptierte Standard zentrale Mechanismen des Ausschlusses kennt. Facebook kann mir den Zugang zu meinen Freunden jederzeit wieder nehmen, oder auch nur temporär oder lokal einschränken. Die Kontrolle über den Zugang zu dem Standard ist einerseits der Schlüssel zum Geschäftsmodell der Plattformen, andererseits auch die Grundlage ihrer politischen Macht.

Kurz: Plattformmacht = Netzwerkmacht + Kontrolle des Zugangs.

3. Plattformregulierung erhöht die Macht der Plattformen

Natürlich ist in der klassischen Politik bereits angekommen, dass Plattformen über eine unheimliche Macht verfügen, aber weil Politiker diese Macht nicht verstehen, verschlimmern sie diesen Zustand noch. Sie glauben, es bei Google, Facebook, Apple und Co. schlicht mit der typischen Konzernmacht zu tun zu haben, die sie von Siemens und der Deutschen Bank kennen. Entsprechend greifen sie zum Rezeptbuch der politischen Regulierung, um dieser Macht entgegenzutreten.

Doch Plattformanbieter sind nicht einfach nur große Firmen und ihre Macht beruht auf weit mehr als nur Geld und weltweite Ausdehnung. Plattformen stehen Staaten vielmehr als Systemkonkurrenten gegenüber – obwohl das beide nicht wahrhaben wollen.

Anstrengungen der klassischen Politik, Plattformen zu regulieren, enden deswegen in einem Paradox. Während die Politiker ihre Fäuste gen Google und Facebook recken, schanzen sie den Plattformen immer neue hoheitliche Kompetenzen zu. Jede Auflage, die sich die Politik ausdenkt, stärkt die politische Handlungsmacht und Legitimation von Plattformen. Als Beispiel kann das Urteil des EuGH zum Recht auf Vergessen-

4 Grewal, David Singh: Network Power – The Social Dynamics of Globalization, S. 9.

werden gelten, das Google dazu anhält, Suchergebnisse zu Personen nach einem sehr schwammigen Katalog von Kriterien zu bereinigen.[5] Ein anderes Beispiel ist das neuere Netzwerkdurchsetzungsgesetz des Justizministers Heiko Maas, das Facebook und andere Plattformen dazu anhält „offensichtlich rechtswidrige Inhalte" zu löschen.[6] In beiden Fällen gibt der Staat Rechtssprechungs- sowie Rechtsdurchsetzungskompetenzen an die Plattformen ab. Das ist einerseits durchaus sinnvoll, weil Plattformen durch ihre Plattformmacht und tiefe, datenreiche Einsichten die logischen Ansprechpartner zur Regulierung des Digitalen sind. Es ist aber auch fatal, weil der Staat damit das Regime der Plattformen stärkt. Er macht sich abhängig von seinem eigenen Systemkonkurrenten.

Drei Ressorts der Plattformpolitik

Der politische Einfluss von Plattformen ist vielfältig. Ohne Anspruch auf Vollständigkeit möchte ich an dieser Stelle drei Politikbereiche voneinander abgrenzen, in denen Plattformen heute schon sehr einflussreich sind und in Zukunft noch an Einfluss gewinnen werden: Netzinnenpolitik, Netzaußenpolitik und Netzsicherheitspolitik.

Netzinnenpolitik

Der Begriff „Netzpolitik" hat sich vor allem in Deutschland – ausgehend vom gleichnamigen Blog für politische Fragen – rund um das Netz etabliert.[7] Er versammelt Fragen des Datenschutzes, der Netzneutralität, der Zensurfreiheit und andere netzrelevante Politikbereiche. Wesentlich ist, dass das Netz immer als Gegenstand der Netzpolitik gesehen wird.

Der Begriff „Netzinnenpolitik" soll nun zunächst das Eingeständnis signalisieren, dass es dieses innen/außen und Objekt/Subjekt-Verhältnis so nicht mehr gibt und dass die politischen Fragen des Netzes zunehmend aus dem inneren des Netzes selbst erwachsen. Und dass sie auch nur im inneren des Netzes zu lösen sind. Zu nennen wären die vielzitierten Probleme mit Hate Speech, Trolling und Fake News, aber auch ältere Probleme wie Identitätsdiebstahl oder Doxxing (das Veröffentlichen von persönlichen Informationen gegen den Willen der Betroffenen) fallen in die Kategorie.

Da diese Probleme meistens auf Plattformen entstehen, ist es folgerichtig, von ihnen auch die entsprechenden Gegenmaßnahmen zu erwarten. Das geschieht zwar durchaus, allerdings immer noch in allgemein als unzureichend empfundenem Maße. Tatsächlich zeigen Plattformen eine gewisse Regulierungsaversität. Sie scheuen zurück, die politische Macht, die sie faktisch haben, tatsächlich einzusetzen, um zum Beispiel strengere Regeln aufzustellen und durchzusetzen.[8]

Nichtsdestotrotz scheint sich ein gewisses Problembewusstsein durchgesetzt zu haben. Facebooks neues Missionsstatement von Februar deutete bereits darauf hin[9], von Twitter[10] und Google[11] gab es ähnliche Signale. Nach dem eskalierten Nazi-Aufmarsch in Charlottesville haben viele Plattformanbieter gehandelt und rechtsradikale Accounts und Websites von ihren Services verbannt. Twitter und LinkedIn suspendierten etliche Accounts von „White Suprimacists", Facebook, Google und GoDaddy (ein populärer Domainhändler) sperrten Domains und Gruppen, die Hass verbreiten. Vor allem das Naziportal Daily Stormer war betroffen und flog sogar beim Content Delivery Network Cloudflare raus.[12]

Offen bleibt allerdings, ob solche Maßnahmen geeignet sind, die zitierten Probleme in

5 Michael Seemann: Das Neue Spiel - Strategien für die Welt nach dem digitalen Kontrollverlust, 2014, S. 223.

6 Markus Beckedahl: NetzDG: Fake-Law gegen Hate-Speech, https://netzpolitik.org/2017/netzdg-fake-law-gegen-hate-speech/, 30.06.2017.

7 Siehe netzpolitik.org.

8 Das ist einerseits damit zu erklären, dass es sich immer noch um gewinnorientierte Firmen handelt und solche Art Regulierung keinen Umsatz, aber einen ganzen Rattenschwanz an Kosten verursacht. Andererseits kommen die Firmengründer und Angestellten aus der weitgehend von libertären Denkweisen dominierten Startup-Kultur des Silicon Valleys, wo jegliche Eingriffe in Debatten als Eingriffe gegen die Redefreiheit interpretiert werden.

9 Mark Zuckerberg: Building Global Communiy, https://www.facebook.com/notes/mark-zuckerberg/building-global-community/10154544292806634, 16.02.2017.

10 Kerry Flynn: Twitter just took its biggest stance yet on hate speech, http://mashable.com/2017/10/17/twitter-hate-speech-abuse-new-rules-women-boycott/#vfo7gOJrokqD, 17.10.2017.

11 Dan Seitz: Google Is Cracking Down On Fake News In Search Results, http://uproxx.com/technology/google-search-results-fake-news/, 13.03.2017.

12 David Ingram, Joseph Menn: Internet firms shift stance, move to exile white supremacists, https://www.reuters.com/article/us-virginia-protests-tech/internet-firms-shift-stance-move-to-exile-white-supremacists-idUSKCN1AW2L5, 16.08.2016.

den Griff bekommen. Bisherige Ergebnisse geben wenig Anlass zur Hoffnung.[13]

Netzaußenpolitik

Während Facebooks Umgang mit Hate Speech und Fake News der Netzinnenpolitik zugeordnet werden kann, wäre das bereits erwähnte Netzwerkdurchsetzungsgesetz von Heiko Maas Gegenstand der Netzaußenpolitik. In der Netzaußenpolitik treffen vor allem (aber nicht nur) Plattformen und Staaten aufeinander und handeln ihre gegenseitigen Interessen miteinander aus. Der Standardfall ist dabei natürlich der Versuch der Regulierung von Plattformen durch Staaten, wie wir es bereits besprochen haben. So hat die EU gleich mehrere Verfahren gegen Facebook und Google am Laufen, aber auch die Konflikte zwischen US-Regierung und den Plattformen treten immer deutlicher zu Tage.[14]

Doch die Beziehungen zwischen Plattformen und Staaten waren in der Vergangenheit nicht immer so schlecht. Insbesondere das amerikanische Außenministerium unter Hillary Clinton nutzte Plattformen für außenpolitische Zwecke. In ihrer bedeutenden Rede von 2010 zu Internet und Freiheit bezeichnete sie die Plattformbetreiber als wichtige Partner, wenn es darum geht, Demokratie und Menschenrechte in die Welt zu tragen.[15]

Eine besondere Scharnierfunktion erfüllte dabei Jared Cohen.[16] Er kam noch unter Condoleezza Rice ins Außenministerium, stieg aber vor allem unter Clinton auf. Als 2009 im Iran eine Revolution auszubrechen drohte, rief er bei Twitter an und überzeugte sie, ihre geplante Wartungsdowntime aufzuschieben.[17] Twitter spielte eine wichtige Rolle zur Koordination der Aufstände.

Als dann Anfang 2011 der Arabische Frühling ausbrach, arbeitete Cohen bereits bei Google und half verschiedene Projekte zwischen Plattformen zu koordinieren. Facebook, Twitter und Google versuchten jeweils auf ihre Weise die Aufstände zu unterstützen und teilweise kooperierten sie dazu auch. Wie zum Beispiel beim Dienst speak2tweet, bei dem Google eine Telefonnummer bereitstellte, bei der Menschen aus Ägypten aufs Band sprechen konnten. Das Gesagte wurde dann per Twitter veröffentlicht und so die Internetabschaltung umgangen.[18]

Spätestens seit den Snowden-Enthüllungen von 2013 ist das Verhältnis zwischen Silicon Valley und Washington deutlich abgekühlt. Plattformen versuchen sich seitdem eher stärker gegen Eingriffe des Staates abzugrenzen und zu schützen. Dies geschieht vor allem durch die allgemeine Verbreitung von verschlüsselten Verbindungen und die Erhöhung der technischen wie rechtlichen Sicherheit.[19] Die USA sehen diese Entwicklung ihrerseits mit wachsendem Unbehagen, insbesondere den Trend zu immer besser kryptografisch abgesicherten Systemen.

Im Frühjahr 2016 eskalierte der Streit schließlich anhand des iPhones, das FBI-Ermittler bei dem Attentäter von San Bernardino gefunden hatten. Es war gesperrt und verschlüsselt und die Ermittler verlangten von Apple Kooperation bei der Entschlüsselung. Apple verweigerte. Für das Aufschließen hätte Apple in die Sicherheitssoftware eine Schwachstelle einbauen müssen. Aus Apples Sicht ein gefährliches Unterfangen, das die Sicherheit aller anderen Geräte und damit der Nutzer gemindert hätte. Am Ende musste das FBI mit einer externen Sicherheitsfirma zusammenarbeiten, um das iPhone zu entsperren.[20]

Neben den Kooperationen und Konflikten der Plattformen mit Staaten gibt es natürlich

13 Kerry Flynn: Facebook's ‚Trust Indicators' is apparently a gift to select media partners, http://mashable.com/2017/11/16/facebook-trust-indicators-fake-news-problem/, 16.11.2017.

14 Julia Fioretti: EU increases pressure on Facebook, Google and Twitter over user terms, https://www.reuters.com/article/us-socialmedia-eu-consumers/eu-increases-pressure-on-facebook-google-and-twitter-over-user-terms-idUSKBN1A92D4, 24.07.2017.

15 Hillary Clinton: Statement: Hillary Clinton on internet freedom, https://www.ft.com/content/f0c3bf8c-06bd-11df-b426-00144feabdc0, 21.01.2010.

16 Wikipedia: Jared Cohen, https://en.wikipedia.org/wiki/Jared_Cohen

17 Ewen MacAskill: US confirms it asked Twitter to stay open to help Iran protesters, https://www.theguardian.com/world/2009/jun/17/obama-iran-twitter, 17.06.2017.

18 Charles Arthur: Google and Twitter launch service enabling Egyptians to tweet by phone, https://www.theguardian.com/technology/2011/feb/01/google-twitter-egypt, 01.02.2011.

19 Google und Twitter zum Beispiel bekämpften seit 2013 etliche Geheimgerichtsbeschlüsse bis zur letzten Instanz. Siehe zum Beispiel: Sam Byford: Google challenges US government's private data demand in court, https://www.theverge.com/2013/4/5/4185732/google-fights-national-security-letter, 05.04.2013.

20 Wikipedia: FBI-Apple encryption dispute, https://en.wikipedia.org/wiki/FBI–Apple_encryption_dispute.

noch die Beziehungen der Plattformen untereinander.[21] Doch politisch greifbarer ist die Entwicklung, dass Facebook zunehmend Nutzer und Nutzerinnen aus dem rechten und rechtsradikalen Milieu an VKontakte verliert.[22] VKontakte ist Facebooks russisches Pendant, hat aber ganz andere Richtlinien. Während man zum Beispiel auf Facebook Probleme bekommt, wenn man homophobe Postings veröffentlicht, bekommt man auf VKontakte Probleme, wenn man die Regenbogenfahne veröffentlicht.

Eine Spaltung der Gesellschaft entlang unterschiedlicher Plattformen und ihrer Policies erscheint durchaus als ein plausibles Szenario und bietet zukünftig viel Stoff für netzaußenpolitische Konflikte.

Netzsicherheitspolitik

Seit einiger Zeit wird in politischen Kreisen vermehrt von „Cyberwar" und „Cybersicherheit" gesprochen. Gemeint ist eine neue Form des Krieges mit digitalen Mitteln. Die USA und Israel hatten 2010 vorgelegt und mittels einer hochgerüsteten „Cyberwaffe" – einem speziell entwickelten Computerwurm – Urananreicherungsanlagen im Iran zerstört.[23] Der Stuxnet-Shock war der Beginn eines allgemeinen Wettrüstens in Sachen Hacking-Kapazitäten weltweit. Cyberangriffe sind seitdem Alltag geworden, seien es die Angriffe von China auf Google[24], Nordkorea auf Sony-Pictures[25] oder Russlands auf die amerikanische Wahl. „Cyber" wird gerne damit erklärt, dass das Militär verschiedene Einsatzgebiete kennt: Boden (Armee), Wasser (Marine) und Luft (Luftwaffe) und nun komme eben mit „Cyber" ein neues Einsatzgebiet hinzu, für das man entsprechende Kapazitäten aufbauen muss.[26]

Doch das wesentliche Missverständnis bei dem Thema ist, davon auszugehen, dass Cyberwars vornehmlich zwischen Staaten stattfinden. Das ist bereits heute nicht der Fall. Zum einen ist fast jeder „Cyber-Angriff" zumindest auch ein Angriff auf eine Plattform. Sei es, auf das Betriebssystem von Microsoft (wie bei Stuxnet und viele anderen Fällen) oder auf Services (der Angriff aus China auf Google richtete sich auf Gmail-Postfächer, der russische Hack des Postfaches von John Podesta betraf ebenfalls Gmail). Fast immer ist eine Software oder ein Dienst betroffen, der von einem Plattformanbieter bereitgestellt wird.

Zum anderen zielen schon heute viele Angriffe konkret auf Plattformanbieter als Primärziel. Am prominentesten ist vielleicht der Angriff Chinas auf die Entwicklerplattform GitHub von 2015. GitHub ist eine Plattform, auf der Softwareentwickler ihren Code versionieren und gleichzeitig mit anderen teilen können. Beinahe alle populären Open Source Projekte sind dort zu finden, unter anderem auch eines mit dem Titel „The Great Fire". Als „Great Firewall" wird für gewöhnlich die mächtige Internetzensurarchitektur Chinas bezeichnet und so war „The Great Fire" ein eigens bereitgestelltes Toolkit zur Umgehung eben dieser. Das gefiel der chinesischen Regierung natürlich nicht.

Nun ist es für China nichts ungewöhnliches, unliebsame Dienste einfach mittels der Great Firewall auszusperren, doch GitHub bildet hier eine Ausnahme. Den einheimischen Entwicklern den Zugang zu GitHub zu versperren, käme einer Komplettaufgabe der chinesischen Softwarebranche gleich. Etwas, das sich nicht mal China leisten kann. Da aber China in seiner Zensurinfrastruktur Millionen von Anfragen pro Sekunde ins Leere laufen lassen muss, kam es auf die Idee, die geblockten Anfragen stattdessen auf ein Ziel im Internet zu richten. Das ist die Idee hinter "The Great Cannon".[27]

Was auf GitHub einprasselte waren Millionen und Abermillionen Abfragen aus ganz China,

21 Auf die ständigen Konflikte zu Schnittstellen, Standards und Marktanteile will ich gar hier allerdings gar nicht eingehen, obwohl auch diese natürlich politisches Gewicht haben.

22 Katie Zawadski: American Alt-Right Leaves Facebook for Russian Site VKontakte, https://www.thedailybeast.com/american-alt-right-leaves-facebook-for-russian-site-vkontakte, 11.03.2017.

23 Wikipedia: Stuxnet, https://en.wikipedia.org/wiki/Stuxnet.

24 Die Angriffe gingen unter dem Namen "Operation Aurora" in die Geschichte ein. Wikipedia: Operation Aurora: https://en.wikipedia.org/wiki/Operation_Aurora.

25 Axel Kannenberg: USA: Nordkorea steckt hinter Hackerangriff auf Sony Pictures, https://www.heise.de/newsticker/meldung/USA-Nordkorea-steckt-hinter-Hackerangriff-auf-Sony-Pictures-2504888.html, 19.12.2014.

26 Handelsblatt: Zu Land, zu Wasser, in der Luft – und im Internet, http://www.handelsblatt.com/politik/deutschland/bundeswehr-erhaelt-cyber-truppe-zu-land-zu-wasser-in-der-luft-und-im-internet/13505076.html, 24.04.2016.

27 Federführend bei der Untersuchung des Vorfalls war das Citizen Lab, das auch einen ausführlichen Bericht darüber geschrieben hat. Citizen Lab: China's Great Cannon: https://citizenlab.ca/2015/04/chinas-great-cannon/, 10.04.2015.

die den Service bis weit an die Belastungsgrenze führte. In IT-Sicherheitskreisen nennt man das einen DDoS Angriff – einen "Distributed Denial of Service"-Angriff.[28]

Plattformen sind aber nicht nur Ziel von Angriffen, sondern immer öfter auch die letzte Verteidigungslinie für Angegriffene. 2016 traf ein DDoS-Angriff das Blog des Sicherheitsforschers Brian Krebs. Bei einer Analyse des Angriffs stellte sich heraus, dass der Angriff vornehmlich von Internetroutern und Sicherheitskameras ausgegangen war. Der Grund: Ein Fehler im Betriebssystem „Mirai", das in solchen Geräten oft zum Einsatz kommt, hatte es Angreifern erlaubt, viele Millionen von ihnen virtuell in Besitz zu nehmen. Es war die größte Bot-Armee, die die Welt je gesehen hat.

Krebs wusste sich nicht anders zu helfen, als unter Googles eigens für solche Fälle eingerichtete Serverinfrastruktur namens „Project Shield" zu schlüpfen. Dieses wird – nebenbei bemerkt – von Jared Cohens aus Google ausgegründetem Thinktank Jigsaw betrieben.[29]

Die unbequeme Wahrheit hinter „Cyber" ist, dass nicht Staaten im Mittelpunkt des Geschehens stehen, sondern Plattformen. Sie sind es, die die Infrastruktur bereitstellen, die angegriffen wird. Sie sind sehr häufig auch Ziele der Attacken. Vor allem aber sind sie derzeit die Einzigen, die über die technischen Kapazitäten und menschlichen Ressourcen verfügen, Angriffe abzuwehren, ihnen vorzubeugen und am Ende den Tag zu retten.[30] So oder so. Den Staaten wird im Falle des Falles nichts anderes übrigbleiben als, wie Brian Krebs, unter den Schutzschirm der Plattformen zu schlüpfen. Staatliche "Cybersouveränität" bleibt derzeit ein unrealistischer Traum.

Fazit

Plattformen besetzen bereits heute zentrale Stellen der gesellschaftlichen Ordnung, die selbst zunehmend zur digitalen wird. Sie regulieren für die Gesellschaft kritische Infrastruktur und bieten Schutz und Ordnung im Internet. Sie stehen damit in Konkurrenz zu Staaten und generieren Abhängigkeiten, die für die Staaten bedrohlich werden könnten.

Ob Staaten in dieser Hinsicht auf lange Frist ihre Unabhängigkeit und Souveränität aufrechterhalten werden, wird davon abhängen, ob es ihnen gelingt, eine eigene digitale Infrastruktur ins Werk zu setzen. Der Staat muss auf lange Sicht selbst zum Plattformanbieter werden.[31]

Plattformen dagegen täten gut daran, sich bei den Staaten die gewachsenen, demokratischen Institutionen abzuschauen, um mit ihren netzinnenpolitischen Problemen fertig zu werden. Ein wenigstens rudimentäres Recht statt Terms of Service, einen Ansatz von Gewaltenteilung, Transparenz und Einspruchsmöglichkeiten bei allen Verfahren, würden den Kampf gegen Hate Speech und Fake News glaubhafter, gerechter und mit Sicherheit auch erfolgreicher machen.[32]

Kurz: Plattformen müssen mehr werden wie Staaten und Staaten mehr wie Plattformen.

Beiden, d.h. Staaten und Plattformen bleibt derweil nicht viel anderes übrig, als ein kritisch-kooperatives Verhältnis zueinander zu pflegen und in allen drei Feldern – Netzinnenpolitik, Netzaußenpolitik und Netzsicherheitspolitik – zu kooperieren. Es bleibt noch darauf hinzuweisen, dass das Konkurrenzverhältnis zwischen beiden im Zweifel für den Bürger, bzw. User sogar gewinnbringend sein kann. Während mich der Staat vor dem überbordenden Zugriff der Plattformen zu beschützen sucht, versucht der Plattformanbieter mich vor dem Datenzugriff des Staates zu schützen. ■

28 Wikipedia: DDoS: https://en.wikipedia.org/wiki/Denial-of-service_attack#Distributed_attack

29 Brian Krebs: How Google Took on Mirai, KrebsOnSecurity, https://krebsonsecurity.com/2017/02/how-google-took-on-mirai-krebsonsecurity/, 03.02.2017.

30 Das Hauptproblem von Staaten in diesem Bereich ist tatsächlich das Personal. IT-Sicherheitsexperten gehören zu einer personellen Rarität und werden in der Industrie entsprechend mit astronomischen Honoraren und Karrierechancen bedacht - bei beidem können Staaten – vor allem das Militär – schlecht mithalten.

31 Wie das gehen könnte, habe ich im Rahmen einer Expertenanhörung des Deutschen Bundestags ausgeführt. Siehe Michael Seemann: Stellungnahme: Fragenkatalog für das Fachgespräch zum Thema „Interoperabilität und Neutralität von Plattformen" des Ausschusses Digitale Agenda am 14.12.2016, https://www.bundestag.de/blob/484608/b1dc578c0fdd28b4e53815cda384335b/stellungnahme-seemann-data.pdf, 12.12.2016.

32 Das habe ich 2016 in einem Vortrag auf der re:publica vorgeschlagen. Siehe Michael Seemann: Netzinnenpolitik - Grundzüge einer Politik der Plattformgesellschaft, https://www.youtube.com/watch?v=eQ-a13ZL33g, 11.03.2016.