Staat gegen Netz

Wer kontrolliert die zentralen Zukunftstechnologien des 21. Jahrhunderts?

Stefan Heumann | **Nationalstaat und Globalisierung befinden sich von Natur aus in einem Spannungsverhältnis. Und das Internet steht im Zentrum dieser Spannungen. Drei Konfliktlinien sind dabei besonders interessant: Wer kontrolliert die Informationen, wer behindert den freien Fluss von Daten, und wohin führt die Militarisierung des Cyberraums?**

1996 veröffentlichte John Perry Barlow seine berühmte „Unabhängigkeitserklärung des Cyberspace"; 20 Jahre später teilen nur noch wenige seine utopischen Ideen. Die Vorstellung, dass globale Vernetzung eine freie, bessere Welt schafft, ist einem neuen Realismus gewichen. Der aus der globalen Vernetzung von Computern entstandene Cyberraum hat nicht das Ende der Nationalstaaten eingeläutet. Genauso wenig ist zu bestreiten, dass die globale Vernetzung Staatlichkeit auf vielen Ebenen immer wieder neu herausfordert. Deshalb sind im Spannungsverhältnis zwischen globalem Netzwerk und nationalstaatlichem Machtanspruch Konflikte absehbar, die die internationale Politik in den nächsten Jahren prägen werden. Zugang zu Information, ihre Kontrolle und die Technologien für ihre Auswertung und Verarbeitung sind die zentralen geostrategischen Ressourcen des 21. Jahrhunderts.

Staatliche Informationshoheit in einem globalen Netzwerk

Viel ist über die Rolle sozialer Medien im Arabischen Frühling geschrieben worden. Aber eigentlich begann alles schon zwei Jahre zuvor im Iran. Im Juni 2009 gingen Tausende, vor allem junge Iraner auf die Straße. Sie protestierten gegen die Fälschung der Präsidentschaftswahlen. Die großen Medien des Landes berichteten kaum über die Proteste, aber die Studenten fanden Wege, die staatliche Zensur zu umgehen. Sie tauschten Informationen über soziale Medien und Blogs aus und nutzten das Internet, um ihre Demonstrationen zu organisieren. Über diese Kanäle trug die Protestbewegung ihre Botschaften auch über die Landesgrenzen hinaus und bestimmte für einige Wochen die internationale Berichterstattung, bis es dem Regime gelang, führende Köpfe festzunehmen und die Bewegung zu zerschlagen.

Die Rolle des Internets und sozialer Medien in der Grünen Revolution im Iran 2009 sorgte bereits für internationale Aufmerksamkeit. Mit dem

Arabischen Frühling schien dann wirklich eine neue Ära angebrochen zu sein. Facebook, Twitter & Co waren zwar nicht die Auslöser der Proteste in Tunesien, Ägypten und anderen Staaten, aber sie schienen die Machtverhältnisse auf den Kopf zu stellen. Zeitungen und Verlage wurden von dem jeweiligen Regime kontrolliert, doch da die Regierungskritiker auch per Internet kommunizierten, fehlte den Machthabern jegliche Handhabe. Auf dem Höhepunkt der Proteste im Januar 2011 fiel der ägyptischen Regierung nicht viel mehr ein, als die Verbindung des gesamten Landes zum Internet zu kappen. Diese drastische Maßnahme zeigt, wie bedroht sich die Regierung von der neuen globalen Kommunikationsinfrastruktur fühlte. Man war bereit, Ägypten vom Rest der Welt abzukapseln, um Demonstranten auf dem Tahir-Platz die Möglichkeit zur freien Kommunikation zu nehmen.

Der Enthusiasmus über den Arabischen Frühling währte jedoch nicht lange. Zum einen, weil die politischen Versprechungen – die Hoffnung auf Liberalisierung und Demokratisierung – in den meisten Ländern Nordafrikas und des Nahen Ostens nicht eingelöst wurden. Zum anderen, weil sich der Sieg über repressive Regime mithilfe von sozialen Medien als sehr kurzlebig erwies. Gerade über amerikanische Internetdienste wie Facebook, Twitter und Google ließen sich an Zensurbehörden vorbei Informationen austauschen und Proteste organisieren. Aber die Nutzung digitaler Technologien erzeugt auch ganz neue Verwundbarkeiten. Mit entsprechenden Überwachungsinstrumenten lassen sich sehr schnell Netzwerke und Meinungsführer in der Opposition identifizieren. Repressive Regime haben gelernt, soziale Medien für ihre eigenen Strategien, zur Verbreitung von Propaganda oder zur Desinformation zu nutzen. Der Iran und China zeigen, dass man das Internet nicht gleich „abschalten“ muss, um den meisten Bürgern den Zugang zu unliebsamen ausländischen Internetdiensten zu verwehren.

Heute schalten Autokratien das Internet nicht mehr einfach ab

In den vergangenen Jahren verlief die Konfliktlinie hinsichtlich des Schutzes von Menschenrechten im Internet zwischen westlich geprägten Demokratien und autokratischen Regimen. Vor allem die USA, die EU und weitere demokratische Länder setzen sich für die Position ein, dass Menschenrechte wie freie Meinungsäußerung und Versammlungsfreiheit auch im Internet zu gelten haben. Staaten wie China, Russland oder der Iran sehen dagegen ihre Sicherheit von freier Meinungsäußerung im Internet bedroht und wollen auch dort die Kontrolle über Medien und Informationsaustausch behalten.

Die einfache Aufteilung zwischen Autokratien und Demokratien in Bezug auf den Umgang mit Meinungsäußerung und politischer Mobilisierung bricht allerdings auf, seit der so genannte Islamische Staat (IS) begonnen hat, das Internet zur Verbreitung seiner Botschaften und zur Mobilisierung seiner Anhänger im Westen zu nutzen. Auch in Europa und den USA wird nun diskutiert, wie man Anhänger und Sympathisanten des IS im Netz besser überwachen und ihre Rekrutierungsbemühungen unterbinden kann. Die EU hat ein Forum unter Beteiligung der großen Internetunternehmen initiiert, in dem diskutiert werden soll, wie terroristische Inhalte auf Internetplattformen schnell identifiziert und entfernt werden können und welche Möglich-

keiten es gibt, terroristische Propaganda mit Gegenstimmen aus der Zivilgesellschaft zu bekämpfen.

In den vergangenen Jahren haben vor allem autokratische Staaten versucht, Antworten auf den Verlust der Informationshoheit und die neuen Möglichkeiten für Oppositionelle, sich über das Internet auszutauschen und zu organisieren, zu finden. Aktivisten reagieren darauf mit dem verstärkten Einsatz von Verschlüsselungs- und Anonymisierungstechnologien, um staatlicher Überwachung zu entgehen. Es lässt sich pauschal nicht sagen, wer hier die Oberhand behält. Bei diesem technologischen Wettrüsten sind aber staatliche Akteure allein aufgrund ihrer Ressourcen im Vorteil. Wie dieser Wettlauf ausgeht, lässt sich nicht vorhersagen. Die Bedeutung des Internets und digitaler Technologien wird in diesen Konflikten weiter steigen. Die Bedrohung des islamistischen Terrorismus trägt diese Problematik nun auch in die USA und nach Europa. Angesichts der jüngsten Anschläge wird auch im Westen über Verschlüsselung und Mobilisierung im Internet heftig diskutiert. Politiker in Deutschland fordern leichteren Zugang zu Daten von US-Internetunternehmen wie Facebook. Die Spannungen zwischen Informationsfreiheit und Informationskontrolle werden sich damit ausweiten, und zwar global – in westlichen Demokratien genauso wie in autoritär regierten Staaten.

Terrorismus führt zu verstärkter Kontrolle im Internet

Technologische Souveränität versus Freihandel

Die Internetwirtschaft war jahrelang Inbegriff wirtschaftlicher Verflechtungen über Ländergrenzen hinweg. Als in den neunziger Jahren die ersten Webseiten kommerzielle Dienste anboten, hatten diese, zumindest potenziell, einen globalen Markt. Natürlich gab es auch große Hürden wie Sprachbarrieren oder die Entwicklung und der Einsatz internationaler Bezahlsysteme. Aber die internetbasierte Technologie selbst kannte keinen Unterschied zwischen Landesgrenzen. E-Mail-Anbieter, soziale Medien oder Suchmaschinen wuchsen schnell; schließlich war die potenzielle Nutzerbasis grenzenlos. Die USA verfügten bereits in den neunziger Jahren über eine starke IT-Industrie, und hier gab es auch den ersten großen Markt an Internetnutzern. Es verwundert daher nicht, dass bahnbrechende Innovationen vor allem von amerikanischen Unternehmen entwickelt und auf den Markt gebracht wurden. So erfreuten sich die von Yahoo, eBay, Amazon und Google angebotenen Dienste schnell einer großen internationalen Nutzergemeinde.

Nach der Jahrtausendwende kamen weitere US-Unternehmen wie Facebook und Twitter dazu. Andere, wie IBM, Microsoft, Cisco und Apple, nutzten die neuen Entwicklungspotenziale der rasch wachsenden Internetökonomie. Die meisten Märkte standen diesen Unternehmen offen. Wenn man von Hardware wie PCs oder Netzinfrastruktur absieht, braucht die Digitalwirtschaft, wenn überhaupt, nur eine sehr geringe physische Präsenz in ihren Märkten. Allein der kontinuierliche Ausbau des Internets vergrößerte den Kundenkreis für neue Softwareangebote und digitale Dienstleistungen.

Nur wenige Länder widersetzten sich dem Expansionsdrang amerikanischer Internetkonzerne; China ist sicherlich das prominenteste Beispiel. Auch

Bild nur in Printausgabe verfügbar

aus den genannten politischen Gründen war man in Peking von Anfang an darauf eingestellt, das Vordringen amerikanischer Internetdienstleister abzuwehren. Die Kommunistische Partei war sich bewusst, dass sie US-Firmen schwerlich dazu bringen konnte, sich chinesischen Zensur- und Überwachungsmaßnahmen zu unterwerfen. Aber auch aus wirtschaftlichem Interesse setzte man auf die Förderung einer eigenen Internetindustrie; schließlich verfolgt China schon lange das Ziel, bei Zukunftstechnologien international wettbewerbsfähig zu werden – Alibaba, Tencent und Baidu belegen den Erfolg dieser Strategie. Das rasante Wachstum der chinesischen Internetökonomie wurde durch eine Kombination von politischer Abschottung und wirtschaftlichem Protektionismus ermöglicht.

Angesichts des Bekenntnisses zum freien Welthandel war für Europa eine Politik der Abschottung und des Protektionismus im Bereich der Internetwirtschaft lange Zeit nicht denkbar. Die Snowden-Enthüllungen haben diesen Konsens allerdings aufgebrochen, denn sie zeigten europäischen Ländern, wie abhängig sie von ausländischen IT- und Internetunternehmen sind. Angesichts der rasant wachsenden Bedeutung der Digitalwirtschaft sorgt man sich um den Verlust von technologischer Souveränität. Und man fragt sich, ob die von US-Unternehmen gesetzten Standards auch die eigenen Interessen und Werte widerspiegeln. Das Ringen um die europäische Datenschutzgrundverordnung zeigt die neuen Konfliktlinien auf. Aber es geht nicht nur um Datenschutz; auch die Datensicherheit und der mögliche Zugriff staatlicher Akteure auf die globalen Datenströme werden intensiv diskutiert.

Als der Europäische Gerichtshof im vergangenen Oktober die Safe-Harbor-Regelung zum Transfer persönlicher Daten aus der EU in die USA kippte, drohte zum ersten Mal etwas, das vor wenigen Jahren noch unvorstellbar ge-

wesen war. Denn die Gerichtsentscheidung stellte den freien Datenaustausch, das Fundament des Internets, grundsätzlich infrage. Große US-Firmen wie Facebook und Google empfanden das Urteil als direkten Angriff auf ihre Geschäftsinteressen; in den USA wurde das Urteil daher auch als protektionistisch kritisiert, während man in der EU von der Notwendigkeit sprach, seine eigene Rechtsordnung durchzusetzen. Mit dem Privacy Shield hat man sich zwar auf ein Nachfolgeabkommen geeinigt, doch damit wird das Problem nicht erledigt sein – die Dominanz des Silicon Valley im Technologiesektor ist größer denn je. Aber nicht nur Russen oder Chinesen bereitet dies Kopfzerbrechen, auch in Europa denkt man mittlerweile immer lauter darüber nach, wie man den US-Firmen die Stirn bieten kann. Für die einen geht es um zentrale Grundrechte wie Datenschutz; andere sehen eine neue Tendenz zum Protektionismus. Wo auch immer man in dieser Debatte steht, die Konflikte um den freien Fluss von Daten werden sich international ausweiten. Aber eigentlich geht es um noch viel mehr. Es geht um die Frage, wer die zentralen Zukunftstechnologien des 21. Jahrhunderts kontrolliert.

Wer kontrolliert die Zukunftstechnologien des 21. Jahrhunderts?

Militarisierung des Cyberraums

Das Internet wuchs in den neunziger Jahren rasant, immer mehr Computer verbanden sich mit dem Netzwerk. Auch Regierungsnetzwerke wurden immer größer. So war es nur eine Frage der Zeit, bis das Eindringen in fremde IT-Systeme nicht nur für junge Computerexperten, so genannte Hacker, sondern auch für staatliche Akteure interessant wurde. Militärs und Geheimdienste, die zentralen Akteure nationalstaatlicher Sicherheitspolitik, entdeckten bereits in den neunziger Jahren den Cyberraum als neues Operationsfeld; 1998 bemerkten IT-Experten des Pentagons erstmals Eindringlinge in ihrem System. Unter dem Codenamen „Moonlight Maze“ verfolgten Pentagon und NSA über mehrere Jahre Angriffe auf ihre Informationsnetzwerke. Die Angreifer schienen sich besonders für streng geheime Rüstungsprojekte zu interessieren. Da in einem globalen Netzwerk viele Zugriffswege möglich sind, ist die Zuordnung von Cyberangriffen äußerst komplex und heikel. Amerikanische Regierungsvertreter sahen die Indizien allerdings als so stark an, dass sie Russland öffentlich für die Angriffe verantwortlich machten. „Moonlight Maze“ bot einen Vorgeschmack auf das neue, internationale Konfliktfeld. Heute sind Geheimdienste und Militärs im Internet präsenter als je zuvor.

Sicherheit war schon immer die Kerndomäne des Nationalstaats. Daher mag es nicht verwundern, dass das Internet mittlerweile auch ins Visier nationalstaatlich organisierter „Cyberkrieger“ geraten ist. In den Jahren seit der Jahrtausendwende haben sich staatliche Aktivitäten im Cyberraum und damit auch das Eskalationspotenzial massiv ausgeweitet. Im April 2007 legten in Estland so genannte Denial-of-Service-Attacken die Server von Banken, Regierungseinrichtungen und Medien mit gravierenden Auswirkungen auf das öffentliche Leben lahm. Die Ursprünge des Angriffs wurden in Russland vermutet, auch wenn die russische Regierung jegliche Verantwortung bestritt. 2010 sabotierte der Computerwurm Stuxnet das iranische Atomprogramm, indem er Fehlfunk-

tionen in Uran-Zentrifugen auslöste und diese durch den dadurch provozierten fehlerhaften Betrieb dauerhaft beschädigte. Die Komplexität des Angriffs ließ auf einen staatlichen Ursprung des Computerwurms schließen; weitere Analysen legten eine Beteiligung der USA und Israels nahe. 2016 führte eine Cyberattacke zu Ausfällen im ukrainischen Stromnetz. Und zuletzt machten der Bundestagshack und die Veröffentlichungen der E-Mail-Korrespondenz der Führung der Demokratischen Partei in den USA Schlagzeilen.

Die Entwicklungen der vergangenen Jahre zeigen, dass der Cyberraum sich zu einem immer bedeutenderen Konfliktfeld zwischen Staaten entwickelt. Durch die voranschreitende Vernetzung, die Ausweitung und Weiterentwicklung digitaler Steuersysteme werden wir verwundbarer. Gleichzeitig investieren Staaten immer mehr Ressourcen, um solche Verwundbarkeiten auszunutzen. Die Möglichkeit, Cyberangriffe in einem globalen Netzwerk zu verschleiern, verringert die Hemmschwelle, solche Angriffe auch wirklich auszuführen. Zusätzlich ist die Grenze zwischen Spionage und Cyberangriffen sehr schwammig. So ist für den Verteidiger nur schwer erkennbar, ob ein Eindringling Informationen stehlen oder einen möglichen Angriff vorbereiten will.

Auch die Bundeswehr will mehr offensive Cyberkapazitäten

Fragen von Zuordnung und die unklare Grenze zwischen Spionage und Cyberangriffen erschweren die Entwicklung internationaler Normen. Selbst die Frage, ob Cyberoperationen eher defensiv (zum Schutz der eigenen Infrastruktur) oder offensiv (zum Angriff auf die Infrastruktur Dritter) ausgelegt sind, lässt sich oft nicht klar beantworten. Wenn nun auch ein Land wie Deutschland, das traditionell eher auf Deeskalation und zivile Konfliktlösung setzt, offensive Cyberkapazitäten für die eigenen Streitkräfte anstrebt, wird klar, dass mit der Militarisierung des Cyberraums weitere Konflikte vorprogrammiert sind.

Die Ära des Nationalstaats ist noch lange nicht vorbei

Nationalstaat und Globalisierung befinden sich von Natur aus in einem Spannungsverhältnis. Als Infrastruktur, die globaler Kommunikation und Vernetzung zugrundeliegt, steht das Internet auf ganz besondere Weise im Zentrum dieser Spannungen. Drei zentrale Konfliktlinien sind hier identifiziert worden, sie verdienen mehr Aufmerksamkeit in der internationalen Politik. Denn sie werden mit darüber entscheiden, wohin wir uns in Zukunft entwickeln. Als globale Kommunikationsinfrastruktur steht das Internet für Globalisierung. Aber die hier diskutierten Konflikte in den Bereichen Informationskontrolle, digitale Wirtschaft und Cyberkonflikt zeigen: Die Ära des Nationalstaats ist noch lange nicht vorbei. Vielmehr zeigt die Entwicklung dieser Konfliktfelder, wie Staaten sich in einer global vernetzten Welt geostrategisch in Stellung bringen.

Dr. Stefan Heumann ist Mitglied der Geschäftsleitung des Berliner Think Tanks Stiftung Neue Verantwortung und beschäftigt sich u.a. mit internationaler Daten- und Cyber-Außenpolitik.