Gefährliche Symbiose

Was Silicon Valley dem US-Staat verdankt – und was die Firmen dafür tun

Tamsin Shaw | **Die großen US-Technologiefirmen sind eine ungute Partnerschaft mit dem Militär und den Geheimdiensten ihres Landes eingegangen. Der Staat fördert neue Erfindungen massiv; dafür testen die Firmen sie massenhaft. Die nationale Sicherheit, aber auch Datenschutz und Transparenz bleiben auf der Strecke, wie sich auch am Facebook-Skandal zeigt.**

Den meisten Amerikanern gelten die großen Technologiekonzerne des Silicon Valley als atemberaubend erfolgreiche kapitalistische Unternehmen, die von genialen Querdenkern geführt werden. Die größten unter ihnen – Microsoft, Apple, Facebook, Amazon und Google (die Big Five) – wurden von jungen, charismatischen und männlichen Visionären in legerer Garderobe gegründet. Offene blaue Hemden, schwarze Rollkragenpullover, graue Strickshirts und Hoodies sind die Markenzeichen dieser Erfolgsunternehmer. Die Gründer haben enorm viel Vertrauen in die neuen Technologien geschaffen, vom Home Computing über die sozialen Medien bis hin zu den neuen Horizonten der künstlichen Intelligenz. Ihre Unternehmen wirken, als ob sie, angetrieben durch den digitalen Wandel und die neuen Freiheiten des Internets, organisch gewachsen wären.

Die amerikanische Regierung erachtet diese großen Silicon-Valley-Konzerne als unverzichtbar für die nationale Sicherheit. Sowohl staatliche Investitionen als auch Gesetzesänderungen der vergangenen Jahrzehnte belegen, dass den Big Five in Washington enormes Vertrauen entgegengebracht wird. Als Gegenleistung kooperieren sie gelegentlich mit den US-Geheimdiensten und dem Militär. Schon seit Jahren wird öffentlich darüber diskutiert, ob diese Zusammenarbeit die Privatsphäre und den Datenschutz gefährdet. Doch selbst die Enthüllungen von Edward Snowden lösten noch keinen nachhaltigen Sturm der Entrüstung aus. Wirklich aufgeschreckt wurde die Öffentlichkeit erst durch die Berichterstattung über das Unternehmen Cambridge Analytica, das auf Millionen von Facebook-Nutzerdaten illegal zugriff und diese auswertete, um die Wahlkampagne von Donald Trump zu unterstützen. Seit Wochen steht Facebook deswegen massiv unter Druck.

Die Big Five verfügen über unvorstellbare Mengen privater Daten und die ausgefeiltesten Instrumente zur Beeinflussung der öffentlichen Meinung, die

Menschen je erdacht haben; dagegen mangelt es an Verfahren, um die Glaubwürdigkeit der von ihnen verbreiteten Informationen zu überprüfen. Journalisten haben schon länger kritisch über die Nutzung dieser Ressourcen zu politischen Zwecken berichtet, während sich Politiker und Kampagnenmanager lange unbesorgt zeigten. Tatsächlich haben sowohl Republikaner als auch Demokraten in den vergangenen Wahlperioden selbst immer komplexere Datenerhebungsverfahren und Analyse-Tools verwendet, um ihre Wählerinnen und Wähler zu erreichen.

Nicht nur Cambridge Analytica, auch andere private Unternehmen nutzen solche Mittel, um Wahlkämpfe zu beeinflussen: i360, eine Firma der Brüder Charles G. und David H. Koch, die finanziell in etwa so gut ausgestattet ist wie die beiden großen Parteien zusammen, erstellt seit Jahren immer detailliertere Profile von rund 250 Millionen Amerikanern und verfeinert Instrumente zur gezielten Werbeschaltung. So wird etwa Mobile-ID-Matching genutzt, um Einzelpersonen alle von ihnen genutzten Geräte zuzuordnen (mithilfe von Cookies konnten bisher nur einzelne Geräte identifiziert werden). Zudem betreibt i360 mithilfe der sozialen Medien weitreichende demografische Analysen. Die Google-Firma DoubleClick und Facebook zählen zu den so genannten Online-Marketing-Partnern von i360. Bis zu den amerikanischen Zwischenwahlen in diesem Herbst will der Konzern eine umfassende Strategie zur gezielten Beeinflussung von Wählerinnen und Wählern entwickeln.

Die Big Five verfügen über die ausgefeiltesten Instrumente

Ob die Empörung über den Datenmissbrauch für Trumps Wahlkampagne die öffentliche Einstellung auf Dauer verändert, ist offen. Immerhin stellen sich die Amerikaner inzwischen die Frage, ob die Konzerne, die früher vor allem für Informations- und Kommunikationsfreiheit standen, nicht mittlerweile eher als Manipulationsinstrumente dienen. Die Tatsache, dass Unternehmen wie Google, Facebook und Twitter von russischen Trollen und Bots (Fake-Accounts, die sich als echte Nutzer ausgeben) infiltriert und instrumentalisiert wurden, um Falschinformationen zu verbreiten und die Präsidentschaftswahlen zu beeinflussen, nährt die Vermutung, dass gerade diese Unternehmen die nationale Sicherheit gefährden.

Der Informationskrieg

Ein Cyberkrieg lässt sich auf verschiedene Art und Weise führen. Bei DDoS-Angriffen (distributed denial of service) werden Betriebssysteme mit Informationen überschwemmt, um ihre Funktionstüchtigkeit einzuschränken. Eine der größten DDoS-Attacken ging im Oktober 2016 vom so genannten Mirai-Botnetz aus (ein Botnetz entsteht, wenn sich Hacker Zugriff auf vernetzte Geräte verschaffen). Sie legte ein Unternehmen namens Dyn lahm, das für die Verwaltung der Internet-Infrastruktur mitverantwortlich ist. Zeitweise waren weite Teile des Internets in den USA gestört. Andere Hackerangriffe zielen darauf ab, vertrauliche Informationen zu entwenden und weiterzuverbreiten – so wie in den Fällen des Sony-Hacks, der Nordkorea zugeschrieben wird, und dem Hackerangriff auf die E-Mail-Server der US-Demokraten während des Wahlkampfs 2016. Es kann auch darum gehen, mit dem Internet vernetzte,

strategisch wichtige Knotenpunkte lahmzulegen. Dazu zählen Anwendungen, die Transport-, Telekommunikations- und Energieversorgungssysteme steuern. Speziell diese Art von Cyberattacken werden mittlerweile als existenzielle Gefahr für die nationale Sicherheit wahrgenommen.

Im Militärjargon bezeichnete man mit dem Wort „Informationskrieg" einst sowohl Cyberangriffe als auch Militäroperationen, die sich gegen die Informations- oder Telekommunikations-Infrastruktur eines Landes richteten. Heutzutage ist dieser Begriff enger definiert: Als Informationskrieg gilt jeder Angriff, bei dem Informationstechnologie für die Zwecke der Propaganda, der Fehlinformation und der psychologischen Kriegsführung benutzt wird. Die USA haben gerade erst damit begonnen, sich für derartige Angriffe, die verheerende Folgen haben könnten, zu rüsten.

Obamas Erzählung vom demokratischen und freien Internet

Darum geht es in dem wichtigen Buch „The Darkening Web: The War for Cyberspace" von Alexander Klimburg, das zum größten Teil vor den Enthüllungen über die russische Einmischung in die amerikanischen Präsidentschaftswahlen 2016 verfasst wurde, aber weiterhin hochaktuell ist. Klimburg stellt die These auf, dass sich das Risiko für den Ausbruch neuer Informationskriege mit der Entwicklung des Internets deutlich verschärft hat. Algorithmen, die von einigen großen Konzernen programmiert werden, legen fest, welche Ergebnisse unsere Suchmaschinen ausspucken, welche Posts und Nachrichtenmeldungen in unserem Feed erscheinen und welche Werbung auf den von uns besuchten Websites geschaltet wird. Wird dieses komplexe System mit falschen oder irreführenden Informationen gefüttert, kann das weitreichende und unvorhersehbare Folgen haben.

Die Anfälligkeit der liberalen Demokratien

Facebook schätzt, dass 11,4 Millionen Amerikaner Werbemeldungen gesehen haben, die von russischer Seite gekauft wurden, um die Präsidentschaftswahlen 2016 im Sinne Donald Trumps zu entscheiden. Google entdeckte ähnliche Spots auf seinen eigenen Plattformen, auch auf YouTube und Gmail. Weitere 126 Millionen Menschen sahen laut Facebook Posts, die in von Russland unterstützten Facebook-Gruppen veröffentlicht wurden. Rund 1,4 Millionen Twitter-Nutzer wurden benachrichtigt, dass sie möglicherweise russischer Propaganda ausgesetzt wurden. Der Verdacht, dass diese Zahl untertrieben ist, liegt nahe, zumal allein ein einziger von der russischen „Troll-Fabrik" gesteuerter Account @Jenn_Abrams (eine fiktive Amerikanerin Mitte 30) von allen großen Nachrichtenmedien zitiert wurde. All diese Entwicklungen – zusammen mit der immer öfteren Verbreitung von falschen Nachrichtenmeldungen in der Folge der Präsidentschaftswahlen 2016, Berichten über das schwindende Vertrauen der Amerikaner in die traditionellen Medien und einem Präsidenten, der regelmäßig Tweets mit haltlosen Fake-News-Vorwürfen absetzt – bestätigen Klimburgs Ängste.

Klimburg argumentiert, dass liberale Demokratien, die auf das Vertrauen der Bürgerinnen und Bürger untereinander und in die Regierung angewiesen sind, besonders anfällig für die Methoden der Informationskriegsführung

Bild nur in Printausgabe verfügbar

sind. Er stellt fest, dass dieses Vertrauen gerade in den USA brüchig geworden ist. Dazu zitiert er Meinungsumfragen aus der Zeit vor der Wahl von Donald Trump, die belegen, dass schon damals nur 36 Prozent der Befragten Vertrauen in das Amt des Präsidenten und nur 6 Prozent Vertrauen in den Kongress setzten. Und es gibt keinen Grund zu der Annahme, dass sich diese Zahlen seither zum Positiven verändert haben. Das Vertrauen der Bürgerinnen und Bürger in die republikanisch geführten Institutionen ist fragil.

Klimburg beschreibt, wie es zu dieser Situation gekommen ist: Seit 20 Jahren schon entwickelten sich die Realität des Internets und seine Wahrnehmung immer weiter auseinander. In der Amtszeit von Barack Obama war dieser Spagat wohl am größten. Die Technologiekonzerne aus dem Silicon Valley gewannen Einfluss in der Welt und zugleich großes Vertrauen der Bürger, indem sie das Internet als Medium der Informationsfreiheit und der Innovation vermarkteten, das sich dem Einfluss einzelner Nationalstaaten entziehe. Da mittlerweile fast alle US-Ein- und Ausfuhren mithilfe von Informationssystemen der Silicon-Valley-Unternehmen abgewickelt werden, ist es für diese auch von größter wirtschaftlicher Bedeutung, als unabhängig wahrgenommen zu werden. Die größte Handelspartnerschaft der USA – die mit der EU – unterliegt dem EU-US Privacy Shield-Abkommen. Dieses „Datenschutzschild“ soll europäischen Unternehmen garantieren, dass ihre Datentransfers gegen Überwachung und Eingriffe von außen geschützt sind.

In Obamas „International Strategy for Cyberspace“, die am 16. Mai 2011 veröffentlicht wurde, beschreibt der damalige Präsident das Internet als eine demokratische, sich selbst organisierende Gemeinschaft, in der „die Normen verantwortungsvollen, gerechten und friedlichen Umgangs langsam begonnen haben, Einzug zu halten“. Als Edward Snowdens Enthüllungen der Überwachungs-

methoden der NSA und des Sammelns von Metadaten diese Einschätzung zu widerlegen drohten, verabschiedete Obama die „Direktive 28“, die Prinzipien für die Geheimdienstarbeit festlegte, die fortan mit „dem Engagement für ein offenes, dialogfähiges und sicheres globales Internet“ vereinbar sein sollte.

Martin Libicki, Referent bei der RAND Corporation, einem einflussreichen politischen Think Tank, spielt eine wichtige Rolle, wenn es um die Freiheit des Internets geht. Er hat viel dazu beigetragen, das US-Verteidigungsministerium von der Entwicklung umfassender Offensiv-Kapazitäten abzuhalten. Libicki hat stets den Standpunkt vertreten, dass Amerika sich auf das beschränken solle, was zur Abwehr von Cyberangriffen notwendig ist. Auch andere wie Klimburg fordern, die USA müssten unbedingt daran festhalten, sich als Verfechter des freien Internets zu verstehen – in Abgrenzung zu Befürwortern von Cybersouveränität wie Russland und China, die volle Kontrolle über das Netz und ihre Bürgerinnen und Bürger ausüben wollen.

Täuschung ist längst Bestandteil der US-Verteidigungspolitik

Klimburg warnt davor, dass die Realität diese Sicht allerdings schon lange überholt hat. Das US-Militär und die Geheimdienste hätten den Cyberraum schon immer als potenziellen Austragungsort für Konflikte betrachtet und folgerichtig versucht, Kontrolle über ihn auszuüben. In den 1990er Jahren wurde innerhalb des Militärs intensiv darüber diskutiert, wie man neue Technologien für die Kriegsführung nutzen könnte. Besonderes Augenmerk lag damals auf der psychologischen Kriegsführung. Von ihr erhoffte man sich, die Moral feindlicher Armeen zu schwächen und ausländische Regierungschefs zu stürzen, indem man ihre Unterstützung in der Bevölkerung untergrub.

Nur ein Jahr vor der Veröffentlichung von Obamas International Strategy for Cyberspace entdeckte das russische Softwareunternehmen Kaspersky Lab den Stuxnet-Virus, einen bösartigen Computerwurm, der ursprünglich in den USA und Israel programmiert worden war. Stuxnet sollte das iranische Atomprogramm stören (es infizierte die Kontrollsysteme für Zentrifugen, um Fehlfunktionen und Explosionen auszulösen), breitete sich jedoch über die ganze Welt aus. Dieser Angriff, zusammen mit der Gründung des US Cyber Command durch Obama im Jahr 2009, signalisierte dem Ausland, dass die USA nun auch im virtuellen Raum eine offensive Strategie verfolgten.

Dominanz im Cyberraum

Mit zu den größten Sorgen gehört, zu welchem Ausmaß die amerikanischen Geheimdienste willens sind, die Bevölkerung über ihre Cyberaktivitäten in die Irre zu führen. Mit der Verbreitung von Falschinformationen schaffen sie genau die Art der Verwirrung, die liberale Demokratien, die anfällig sind für psychologische und informationelle Kriegsführung, unbedingt vermeiden sollten. Doch Täuschung ist längst zu einem festen Bestandteil der amerikanischen Verteidigungspolitik geworden. Klimburg geht davon aus, dass die Informationen über geheime Datenerfassungsprogramme, die Bob Woodward in seinem Buch „Obama’s Wars“ (2010) beschreibt, zu Abschreckungszwecken absichtlich an den Journalistenveteran weitergegeben wurden – Washington wollte dem Rest der Welt zeigen, wie sehr man den Cyberraum bereits dominierte.

Gleichzeitig halten andere Regierungsorgane sowohl in der Innen- als auch in der Außenpolitik an der Sichtweise fest, dass das Internet primär ein Ort der Kooperation und nicht des Konflikts ist. Die Sprache, die in offiziellen Strategiepapieren verwendet wird, ist oft absichtlich unklar gehalten. In einer Erklärung zur Cybersicherheit des Verteidigungsministeriums aus dem Jahr 2015 ist die Rede von „Offensive Cyber Effects Operations", die aber nicht weiter erklärt werden. In seinem Buch „Dark Territory: The Secret History of Cyber War" (2016) behauptet Fred Kaplan, die Unterscheidung zwischen offensiven und defensiven Strategien sei schon in der Anfangszeit der Cyberoperationen bei der NSA unter ihrem Direktor Michael Hayden ganz bewusst aufgehoben worden.

Eine gesunde Demokratie braucht viel mehr Transparenz

Eine gesunde Demokratie braucht in ihrer Cyberpolitik erheblich mehr Transparenz. Die Regierungen sollten die Bürgerinnen und Bürger darüber informieren, nach welchen klaren und unzweideutigen Vorgaben Nachrichtensignale gesammelt werden, was für defensive und offensive Cyberstrategien verfolgt werden, in welchem Verhältnis diese zur konventionellen Militärstrategie stehen und inwiefern sich die Beziehung zwischen Geheimdiensten und Militär verändert. Wenn die amerikanische Regierung zum Beispiel zusagen würde, psychologische Cyberstrategien ausschließlich in Kriegsgebieten anzuwenden – etwa in Form von lokalen und kulturspezifischen Informationskampagnen, wie sie bereits in Afghanistan zum Einsatz kamen – könnte dies das Vertrauen der Menschen in die Politik stärken.

Erfindungen im Auftrag des Militärs

Hinzu kommt die wachsende Macht der Privatkonzerne aus dem Silicon Valley, die jene Plattformen entwickeln und verwalten, über die sich die Regierung Einfluss auf die öffentliche Meinung verschafft. Manche (Klimburg eingeschlossen) halten diese Unternehmen für unabhängig und einzig und allein von wirtschaftlichen Interessen geleitet. Will man sich allerdings wirklich tiefergehend mit dem Thema Cybersicherheit und Einflussnahme beschäftigen, darf man das intransparente Gebaren dieser Konzerne nicht einfach ignorieren. Die Interessen, die bestimmen, welche Technologien im Silicon Valley entwickelt werden, sind eben nicht nur finanzieller Natur. Vielmehr hat der Verteidigungssektor private Unternehmen genutzt, um zur Entwicklung der ungeheuren Cyberfähigkeiten der USA beizutragen. Das hat dazu geführt, dass diese Firmen heute über ein gut gefülltes Cyberwaffenarsenal verfügen, ohne darüber Rechenschaft schuldig zu sein.

Die Ursprünge des Internets gehen bekanntermaßen auf DARPA (die Defense Advanced Research Projects Agency) zurück, eine Agentur, die dafür verantwortlich ist, neue Militärtechnologien zu entwickeln. Schenkt man der Erzählung vom freien Internet Glauben, die Barack Obama, das Silicon Valley und das Verteidigungsministerium pflegen, wurden die von uns genutzten Internettechnologien von der Software bis hin zu den sozialen Medien vom privaten Sektor entwickelt und kontrolliert. Wirft man allerdings einen Blick auf die Liste der Projekte, die DARPA mitfinanziert hat, entdeckt man dort alle erdenklichen

Technologien, von grafischen Benutzeroberflächen über die künstliche Intelligenz und die Spracherkennung bis hin zu so genannten High-Performance-Polymeren und Flüssigkristall-Bildschirmen. Dies sind alles Technologien, ohne die kein Smartphone funktionieren würde. Ohne die Kommerzialisierung von militärischen Erfindungen würde es unser Online-Leben nicht geben.

DARPA ermöglicht auch die Frühfinanzierung von Technologien für Zwecke der nationalen Sicherheit, wobei das Geld an Wissenschaftler und Forscher statt an private Unternehmen geht. Doch die wirtschaftliche Kooperation zwischen dem Silicon Valley und dem Verteidigungssektor reicht noch weiter. In ihrem Buch „America Inc.?: Innovation and Enterprise in the National Security State" (2014) beschreibt Linda Weiss die Entwicklung des Silicon Valley zu einem hybriden öffentlich-privaten Wirtschaftszweig, in dem die Regierung in Privatkonzerne investiert, um die Entwicklung jener Technologien zu beschleunigen, die sie aus sicherheitspolitischem Kalkül benötigt, und die gleichzeitig von jenen Unternehmen kommerzialisiert werden können.

Auf dem iPhone wirkt Gesichtserkennung beinahe harmlos

Regierungsbehörden beteiligen sich an riskanten Investitionen und haben Unternehmen in der Vergangenheit sogar dabei unterstützt, Nachfrage für Produkte zu generieren, von deren Entwicklung sie selbst profitieren. Selbstfahrende Autos dienen dazu, Technologien einzusetzen, zu testen und weiterzuentwickeln, die für die Lenksysteme von Raketen und Drohnen entwickelt wurden. Gesichtserkennungssoftware, die von Geheimdiensten und der Armee zu Zwecken der Überwachung und Identifizierung entwickelt wurde (beispielsweise für Drohnenangriffe), wirkt beinahe harmlos, wenn sie von Millionen von iPhone-Nutzern ausprobiert wird.

Die Regierung nutzt verschiedene Kanäle, um derartige Projekte zu finanzieren. Das Small Business Innovation Research Program (SBIR) ist laut Weiss mittlerweile die größte Quelle für die Frühfinanzierung von Hochtechnologiefirmen in den USA. Als ihr Buch veröffentlicht wurde, flossen auf diesem Wege jährlich 2,5 Milliarden Dollar an Unternehmen. Dieses Investment – die nationalen Sicherheitsbehörden stellen rund 97 Prozent des SBIR-Budgets – dient nicht nur als eine Art „Regierungszertifizierung", die Risikokapitalgeber anlocken soll, sondern auch als Innovationsanreiz, da SBIR für die Investitionen kein Eigenkapital als Gegenleistung verlangt.

Eine besondere Art von Standort-Politik

Das Silicon Valley ist nachhaltig durch die Risikokapitalfonds geprägt worden, die von Regierungsbehörden gegründet wurden. Die CIA, das Verteidigungsministerium, die Armee, die US-Marine, die Nationale Agentur für Geografische Aufklärung (NGIA), die NASA und das Heimatschutzministerium verfügen allesamt über Risikokapital, mit dem sie sich an privaten Unternehmen beteiligen können. Weiss zitiert einen Bericht des Verteidigungsministeriums an den US-Kongress von 2002, in dem der Sinn derartiger Investitionen erklärt wird. Darin heißt es, das Ziel sei, technisch überlegene und finanzierbare Sicherheitstechnologien zu entwickeln, die in den Privatsektor überführt werden können, um die USA als Technologie- und Industriestandort zu stärken.

In anderen Worten: Die Entwicklung technologischer Innovationen im Privatsektor wird klar durch die Agenda von Regierungsbehörden beeinflusst, ohne dass die breite Öffentlichkeit darüber informiert wird. So lässt sich beispielsweise zurückverfolgen, welch nachhaltigen Einfluss In-Q-Tel ausübt, ein überaus erfolgreicher Risikokapitalfonds der CIA. Früher ist der Fonds gelegentlich als Alleininvestor in Start-ups aufgetreten; heute investiert er vermehrt in Partnerschaften mit den Big Five. In-Q-Tel war auch der einzige Geldgeber für Palantir, ein Softwareunternehmen von Peter Thiel, dem Mitgründer von PayPal, das sich auf die Analyse großer Datenmengen spezialisiert hat. Ein Tochterunternehmen namens Palantir Gotham, das Daten zur Terrorismusbekämpfung auswertet, ist mittlerweile für das FBI, das Heimatschutzministerium, die NSA, das Center for Disease Control and Prevention (CDC), die US-Marine, die Luftwaffe und das US Special Operations Command tätig.

Mit In-Q-Tel hat die CIA ihren eigenen Risikokapitalfonds

In-Q-Tels Engagement nimmt hin und wieder auch vermeintlich alltäglichere Formen an: Google Earth wurde von Keyhole Inc. entwickelt, einem 3D-Mapping-Start-up, das in Teilen der NGIA gehört und von In-Q-Tel finanziert wurde. Die Cloud-Technologie, die immer mehr Menschen nutzen, wird von Unternehmen wie Frame entwickelt, das gemeinsam von In-Q-Tel, Microsoft und Bain Capital Ventures finanziert wird. Dank eines anderen von In-Q-Tel finanzierten Unternehmens namens Infinite Z wird es schon bald möglich sein, mit holografischen 3D-Projektionen zu interagieren. Aquifi wiederum entwickelt Scanner, die farbige 3D-Kopien beliebiger Objekte erstellen können.

Regierungsberater mit Monopolstellung

Da viele der Start-ups, in die Regierungsbehörden investieren, über kurz oder lang von den Big Five aufgekauft werden, wird die Beziehung zwischen diesen Unternehmen und den Geheimdiensten und Sicherheitsbehörden immer enger. Die Big Five beraten die Regierung auch in technologischen Fragen. Eric Schmidt, der ehemalige Chef von Google bzw. Alphabet, sitzt heute dem Defense Innovation Board des Pentagons vor (auch Amazon-Gründer Jeff Bezos gehörte in der Vergangenheit dazu), das Anfang 2018 in einem Bericht forderte, die Gründung von Tech-Start-ups im Militär zu fördern. Das Ziel sei es, wie in der Wirtschaft Inkubatoren einzurichten, die zur Entwicklung von Start-ups mit einer Spezialisierung auf Verteidigungs- und Sicherheitstechnologien – etwa die Analyse von Metadaten – beitragen würden.

Die US-Regierung hat die Monopolstellung der Big Five in der jüngeren Vergangenheit auch deshalb unterstützt, weil sie von ihrer Soft Power in der Welt profitieren wollte. In einem RAND-Bericht von 2007 mit dem Titel „Conquest in Cyberspace: National Security and Information Warfare“ spekuliert Libicki, dass den USA die „freundliche Eroberung“ anderer Staaten gelingen könnte, wenn sie diese Länder von US-Technologie abhängig machen: „Je größer und reicher das System, desto stärker seine Anziehungskraft.“ Riesige globale Konzerne wie Microsoft, deren Produkte eng mit der technologischen Infrastruktur anderer Staaten verzahnt sind, tragen am Ende dazu bei, dass der amerikanische Einfluss im Ausland wächst.

Es ist offensichtlich an der Zeit zu fragen, ob sich die Entwicklung einer hybriden Ökonomie im Silicon Valley aus sicherheitspolitischer Sicht rentiert hat. Weiss gibt zu bedenken, dass die Regierung zwar regelmäßig Forschungsprojekte finanziert, die Patente für neue Technologien aber später den Privatkonzernen überlässt, die mit ihnen viel Geld verdienen. Auf den Webseiten von Organisationen wie In-Q-Tel und DIUx lassen sich die Verträge einsehen, die sie anbieten. Die Lizenzen, die sie erwerben, sind für gewöhnlich nicht exklusiv, was bedeutet, dass die Technologien, auf denen die amerikanische Sicherheitsinfrastruktur aufbaut, überall und an jeden weiterverkauft werden können. Die Profite streichen Unternehmen ein, die nicht zwangsläufig nationale Interessen im Sinn haben. So unterrichtete Intel vor Kurzem die chinesische Regierung über eine mögliche Schwachstelle ihrer Computerchips, bevor das Unternehmen Washington davon in Kenntnis setzte.

Die Regierung trägt das Risiko, und Apple kassiert den Gewinn

In „The Entrepreneurial State“ (2013) untersucht Mariana Mazzucato Apple – den Konzern der Big Five, der am wenigsten Geld für Forschung und Entwicklung ausgibt. Apples wirtschaftliches Erfolgsgeheimnis ist es, Technologien, die vom Militär- und Geheimdienstsektor finanziert wurden (etwa Touchscreens und Gesichtserkennung), in modische und attraktive Konsumartikel zu integrieren. Im Endeffekt trägt die US-Regierung das wirtschaftliche Risiko, und Apple streicht die Gewinne ein. Anders gesagt: Konzerne wie Apple sind durch Steuergelder reich geworden. Sie danken dies der Regierung aber nur selten mit guter Steuermoral. Das wissen wir aus den Enthüllungen der Paradise Papers über die Offshore-Steuerparadiese der Reichen. So schaffte es Apple durch die Gründung von Tochtergesellschaften in Irland, Steuerabgaben auf einen Großteil seiner Gewinne in Höhe von 128 Milliarden Dollar zu vermeiden. Der Konzern versprach erst, diese Gelder in die USA zurückzubringen, als die Trump-Regierung die Körperschaftsteuer kräftig senkte.

Konzerne aus dem Silicon Valley haben nicht nur enorm viel Geld, sondern auch unvorstellbare Mengen von Daten. Traditionsunternehmen wie Unilever und die Bank of America verfügen zwar schon aufgrund ihres Alters über noch größere Massen an persönlichen Informationen. Doch die Big Five, Uber und andere Konzerne besitzen extrem hochentwickelte Analysewerkzeuge und verwalten Plattformen, die einzig und allein darauf ausgelegt sind, Daten effektiv zu erfassen und für Werbung und Einflussnahme zu nutzen.

Privatisierung staatlicher Aufgaben

An dieser Stelle überschneiden sich Klimburgs Warnungen vor der Entwicklung offensiver Cyberstrategien durch das Militär und die Geheimdienste auf besorgniserregende Weise mit dem Problem der immer weiter voranschreitenden Privatisierung digitaler Technologien. Die USA haben seit Beginn des „Kriegs gegen den Terror“ immer mehr militärische und geheimdienstliche Aufgaben an Privatunternehmen übertragen, speziell an solche, die Datenanalyse betreiben. Regierungsbehörden haben sowohl ältere Unternehmen wie Booz Allen Hamilton und Boeing AnalytX als auch Palantir, die SCL Group und auch SCLs inzwischen berüchtigtes Partnerunternehmen Cambridge

Analytica mit lukrativen Verträgen ausgestattet. Auf diese Weise haben sie die Unternehmen dazu gebracht, immer ausgeklügeltere Methoden der Einflussnahme und Meinungsmache zu entwickeln. Diese neugewonnenen Instrumente der Informationskriegsführung können sie dann auf ihre eigenen Kunden anwenden.

Auf welche Weise sich im Besitz der Big Five befindliche Daten mittels Partnerschaften zwischen Regierung und Unternehmen ausnutzen lassen, fangen viele von uns gerade erst an zu begreifen. Aber diese enorme Macht lässt sich ungebremst auch für Zwecke nutzen, die die nationale Sicherheit bedrohen. Das Beispiel der Brüder Koch, die ihre Ressourcen einsetzen, um Zweifel am Klimawandel zu schüren, sollte uns eine Warnung sein. Das Problem wird durch die außerordentliche Art der Unternehmensführung verschärft, die den Big Five gestattet wird. Obwohl Facebook und Google an der Börse gehandelt werden, halten ihre Gründer – Mark Zuckerberg bei Facebook, Larry Page und Sergey Brin bei Google – über 50 Prozent der Stimmrechte im jeweiligen Vorstand. Das bedeutet, dass sie effektiv die völlige Kontrolle haben.

Mark Zuckerberg: „Sie vertrauen mir – diese Vollidioten“

Klimburg ist davon überzeugt, dass der Nationale Sicherheitssektor unverantwortlich handelt, weil er seine Offensivkräfte im Cyberraum viel zu stark entwickelt hat. Soweit es um das Streben nach Vorherrschaft bei Kapazitäten von Militär und Geheimdiensten geht, mag das stimmen. Aber zur gleichen Zeit hat die Regierung, indem sie unwiderstehliche Anreize fürs Silicon Valley schuf, militärische Technologien zu entwickeln, den Unternehmen nie dagewesene Macht überlassen. Weltweit tätigen Konzernen, die man nicht zur Rechenschaft ziehen kann und die keinen Nutzen aus der Wahrheit ziehen, wurde die weitgehende Kontrolle über Informationen überlassen. Es ist momentan lächerlich einfach, wie Russlands Präsident Wladimir Putin dreist demonstriert hat, über die von ihnen betriebenen Plattformen ausländische Propaganda zu verbreiten. Aber selbst wenn sie Verfahren entwickeln können, die so etwas verhindert, bleiben wir noch immer auf den guten Willen einer Handvoll Milliardäre angewiesen. Sie sind und bleiben dafür verantwortlich, das Vertrauen der Öffentlichkeit in die Qualität von Informationen zu erhalten. In ihren Händen liegt es, die Glaubwürdigkeit zu bewahren, die wir für das Wohlergehen und den Erfolg unserer liberalen demokratischen Gesellschaften brauchen.

In den Anfangstagen von Facebook wurde Zuckerberg gefragt, warum Menschen ihm überhaupt ihre persönlichen Daten übermitteln sollten. Seine Antwort – die er heute mit Sicherheit bereut – ist bekannt: „Sie vertrauen mir – diese Vollidioten.“ Endlich wird uns klar, wie sehr wir alle beleidigt worden sind. Jetzt müssen wir herausfinden, wie wir die Konzerne, die wir mit unseren Steuern, unseren Daten und unserer ungeteilten Aufmerksamkeit unterstützt haben, davon abhalten, uns auch weiterhin wie Vollidioten zu behandeln.

Dr. Tamsin Shaw
ist Associate Professor of European and Mediterranean Studies and Philosophy an der New York University.

Dieser Beitrag erschien zuerst in der New York Review of Books, 8. April 2018.