Edgar Einemann Februar 2014

Besprechung des Buches

Schmidt, E. & Cohen, J. (2013).

Die Vernetzung der Welt. Ein Blick in unsere Zukunft. Reinbek: Rowohlt.

Eric Schmidt und Jared Cohen aus der Spitze des Google-Konzerns leisten einen Beitrag zur Diskussion über Internet, Informationstechnologie und Gesellschaft: Welche Entwicklungen des Internets sind heute erkennbar, welche Zukunft zeichnet sich für die Menschen, aber insbesondere für die Staaten und die Politik ab? Nicht die ja durchaus interessanten und von Google wesentlich geprägten Strukturveränderungen der Ökonomie stehen im Zentrum, sondern die Veränderungen des menschliche Lebens und des "Überbaus" der Weltgesellschaft.

Das Buch sollte eine Pflichtlektüre für alle Politiker sein, die glauben, auf ihrer jeweiligen (begrenzten) Ebene die Welt zu gestalten. Schmidt Cohen verweisen eindringlich auf Erkenntnisse, die nicht unbedingt neu sind, aber aus ihrem Mund eine besondere Bedeutung bekommen. Sie halten das Internet für das "größte Anarchismusexperiment aller Zeiten" (S. 13), das Internet ist für sie "der größte unregulierte Raum der Welt" (S. 14). Sie sehen die Welt erst am Anfang einer Entwicklung, die "nicht nur eine technische, sondern auch eine kulturelle Revolution bedeuten" (S. 16) wird und machen "Vorboten der anstehenden gesellschaftlichen Revolution" (S. 17) aus. Die Vernetzung durch das Internet wird "ein neues Zeitalter der Globalisierung einläuten - und zwar einer Globalisierung von Produkten und Vorstellungen", wobei "sich das Terrain so schnell ändert, dass kein Gesetz mehr mithalten kann" (S. 23). Prägend für die neue Zeit ist die zunehmende Gestaltungsmacht der global agierenden Internet-Konzerne: "Wir sind überzeugt, dass Portale wie Google, Facebook, Amazon oder Apple weitaus mächtiger sind, als die meisten Menschen ahnen... Diese Plattformen stellen einen echten Paradigmenwechsel dar... Mit Ausnahme von biologischen Viren gibt es nichts, was

sich mit derartiger Geschwindigkeit, Effizienz und Aggressivität ausbreitet wie diese Technologieplattformen, und dies verleiht auch ihren Machern, Eigentümern und Nutzern neue Macht." S. 22).

Der in dem Buch formulierte Anspruch, eine Beitrag zur Gestaltung von Gesellschaft und Politik für die Zukunft zu leisten, ist mehr als löblich: "Die neuen digitalen Plattformen, Netzwerke und Produkte haben schon heute gigantische globale Auswirkungen. Um die Zukunft der Politik, Wirtschaft, Diplomatie und anderer wichtiger Sektoren gestalten zu können, müssen wir daher die Revolution verstehen, die die Technologie auf diesen Gebieten bewirkt." (S. 23).

Ein Buch von fast 400 Seiten mit diesem Anspruch und vielen Details kann nicht kurz zusammengefasst werden. Das wird schon deutlich bei einem Blick auf die Hauptüberschriften der Buchkapitel, die auf die angesprochenen Problemkomplexe verweisen: Die Zukunft des Menschen (1.), von Identität, Zivilgesellschaft und Journalismus (2.), der Staaten (3.), der Revolution(4.), des Terrorismus (5.), der Konflikte und Kriege (6.) sowie des Wiederaufbaus (7.). Wichtig ist noch der Hinweis auf den Zeitpunkt der Publikation: im Frühjahr 2013 waren die Aktivitäten der NSA der Öffentlichkeit unbekannt, Edward Snowden hatte noch nicht ausgepackt.

Es kann hier nur darum gehen, einige (quer zu den Einzelfragen liegende) zentrale Gedanken der Autoren zu skizzieren, einzuordnen und sie für die weitere Diskussion aufzubereiten. Wobei, wie schon erwähnt, der für die Frage nach dem Zusammenhang von Internet, Informationstechnologie und Gesellschaft ebenfalls zentrale Themenbereiche "Wirtschaft und Arbeit" bei Schmidt/Cohen bestenfalls eine Nebenrolle spielt und deshalb hier nicht weiter behandelt wird. Und: immer, wenn bei Schmidt/Cohen von Internet-Folgen die Rede ist, geht es um die Entwicklung von Informationstechnologie und Internet insgesamt; so hat es z. B. Forschung, Entwicklung und Produkte im Zusammenhang mit Robotik und Künstlicher Intelligenz schon lange Zeit vor der Herausbildung des Internets gegeben, aber das Internet eröffnet Anwendungsmöglichkeiten in neuer Dimension.

(1) Der Doppelcharakter des Fortschritts

Mit ihrer Kernthese gleich zu Beginn des Buches stehen Schmidt/Cohen in der Tradition einer Vielzahl von Analysen des „technischen Fortschritts“, die oft unter Zuhilfenahme von Begriffspaaren wie „Chance und/oder Risiko“ oder „Fluch und/oder Segen“ vorgestellt wurden. Schmidt/Cohen meinen die Verbindung von Internet und weiterentwickelter Informationstechnologie, wenn sie in Bezug auf das Internet formulieren: „Es hat das Potential, gewaltigen Fortschritt zu bewirken und furchtbaren Schaden anzurichten, und dabei ist das, womit wir uns heute beschäftigen, gerade erst der Anfang.“ (S. 13).

Die Beschreibung der beiden Seiten der Medaille durchzieht das ganze Buch – insbesondere die Beschreibung der Gefahren erfolgt in (unerwartet) schonungsloser Offenheit unter Inkaufnahme der Gefahr, keine beruhigenden Lösungen anbieten zu können. Hier nur ein kleines Beispiel: Unter der Überschrift „Polizeistaat 2.0“ wird darauf hingewiesen, dass „alles, was ein Regime zum Aufbau einer schlagkräftigen Digitalpolizei benötigt, … heute auf dem Markt erhältlich“ (S. 114) ist. Dabei sind „die wichtigsten Datenquellen eines autokratischen Regimes … biometrische Informationen, die die Identifizierung von Menschen anhand ihrer körperlichen und biologischen Merkmale ermöglichen. Dazu gehören unter anderem Fingerabdrücke, Fotografien und DNA-Proben.“(S. 115). Mit Hilfe z. B. von Gesichtserkennung (S. 94, 115, 209, 367) und Cloud Computing (S. 56, 85, 115, 291) sind Personen dann blitzschnell überall identifizierbar. Auf der anderen Seite sollen das Unique Identification Program (UID) und die Kampagne Aadhaar in Indien 1,2 Milliarden Menschen biometrisch erfassen und sie mit einem entsprechenden Ausweis ausstatten: mit vielen Vorteilen und angeblich auch, um Menschen ohne Ausweisdokumente neue Chancen (z. B. auf staatliche Unterstützung) zu ermöglichen. Hier kann man auch eine andere Sicht entwickeln und die Maßnahmen als zu hohen Preis für anders organisierbare soziale Segnungen betrachten – der absehbare Trend zur zukünftigen globalen biometrischen Totalerfassung der Weltbevölkerung ist aber wohl richtig beschrieben.

(2) Viele Vorteile für die Mehrheit und digitale Klassengesellschaft

Schmidt und Cohan vermuten, dass im Jahr 2025 „die meisten der bis dahin vermutlich 8 Milliarden Menschen online sein“ (S. 15) werden. Sie sind davon überzeugt, „dass die überwältigende Mehrheit unterm Strich von der Vernetzung profitieren und in den Genuss höherer Effizienz, neuer Möglichkeiten und größerer Lebensqualität kommen wird.“ (S. 364). Das ist die eine Seite der Medaille. Diese Vorteile sind aber nicht ungetrübt, und sie gelten nicht für alle in gleicher Weise. „Die Vernetzung wird das Problem der sozialen Kluft nicht lösen. (S. 27)“. Vor allem mit Blick auf weniger entwickelte Länder sehen die Autoren die Gefahr, „dass die Unternehmer eine neue digitale Oligarchie bilden“ (S. 322) und sind sich sicher, dass „nicht alle Menschen … in gleicher Weise teilhaben. Die digitale Klassengesellschaft wird uns noch lange erhalten bleiben.“ (S. 364).

(3) Die Verletzlichkeit der Gesellschaft

Im Zusammenhang mit langen Abhandlungen über die neuen Möglichkeiten und Gefahren von Cyberkrieg und Cyberterrorismus arbeiten Schmidt/Cohen (mehr oder weniger bewusst) die weitgehende Schutzlosigkeit von Gesellschaft und Einzelpersonen heraus. Sie sehen eine staatliche Aufstockung von Cyberarsenalen – als „die logische Folge“ ergibt sich „ein dauerhafter, niedrigschwelliger Cyberkrieg“ (S. 166), der in Anspielung auf den Kalten Krieg auch als Code War bezeichnet wird und aufgrund von Fehlern auch einmal versehentlich eskalieren kann. Die Tatsache, dass sich die Herkunft von Attacken oft nicht feststellen lässt, erhöht das Sicherheitsproblem (S. 176) insbesondere dann, wenn Terroristen aktiv werden. „Für die Öffentlichkeit wie auch für Staaten, die schon mit dem Schutz ihres physischen Territoriums überfordert sind, und für Unternehmen, die immer verwundbarer werden, sind das schlechte Nachrichten.“ (S. 223). Schmidt/Cohen stellen einige heute denkbare Angriffsszenarien vor und behaupten, dass auch von entlegenen Orten der Welt aus Attacken mit erheblichen Folgen möglich sind: „Mit einem Angriff auf das Transportwesen, die Polizeidatenbanken, den Aktienmarkt oder das Stromnetz einer Großstadt könnten Terroristen die gesamte Stadt lahmlegen. “ (S. 227). Oder: “Ein Anschlag auf die Vereinigten Staaten könnte beispielsweise mit einem virtuellen Ablenkungsmanöver beginnen, einem großangelegten Hackerangriff auf das

Flugleitsystem etwa, mit dem eine große Anzahl von Flugzeugen auf eine falsche Höhe geleitet und auf Kollisionskurs gelenkt wird. Mitten in der einsetzenden Panik könnte ein weiterer Cyberanschlag die Tower vom Netz nehmen… Inzwischen beginnt am Boden der eigentliche Anschlag mit drei Bomben… eine weitere Welle von Anschlägen blockiert die Polizei, Feuerwehr und Notrufzentralen… Während die Rettungsmaßnahmen … nur mühsam vorankommen, legt ein raffinierter Virus die Kontrollsysteme der Wasser- und Stromversorgung sowie der Öl- und Gaspipelines lahm. Wenn Terroristen in diese Systeme eindringen, könne sie zum Beispiel die Stromversorgung abschalten, Kläranlagen umkehren und die Temperaturüberwachung in Atomkraftwerken abschalten. Natürlich ist die Durchführung des eben beschriebenen Szenarios nahezu unmöglich…. Doch die Koordination von physischen und virtuellen Anschlägen ist absehbar.“ (S. 229). Neue Möglichkeiten gibt es nicht nur z. B. durch die Fernzündung von Bomben mit Hilfe der Vibrations-Funktion von Handys (S. 225), sondern auch durch „kleine“ Drohnen (S. 298) und Roboter (S. 293, 307): „Unterhalb der staatlichen Ebene werden auch Zivilisten und andere nichtstaatliche Akteure einen Rüstungswettlauf um Drohnen und Roboter aufnehmen.“ (S. 300).

Es liegt der Gedanke nahe, dass für den ohnehin kaum zu garantierenden Schutz von Staat, Unternehmen und Bürgern auf den Aufbau von (möglichst umfassenden) Kontroll- und Überwachungssystemen gesetzt wird.

(4) Überwachung, Freiheit und Datenschutz

Das Buch von Schmidt und Cohen wurde vor den Enthüllungen Edward Snowdens über die Aktivitäten der NSA geschrieben. Allerdings haben Schmidt/Cohen schon auf das „Problem“ der zersplitterten Erfassung und Lagerung von Bürger-Daten z. B. bei FBI, CIA und anderen Institutionen hingewiesen (S. 253) und angesichts der neuen Möglichkeiten von „Big Data“ (S. 249, 253) vermutet, dass „in Zukunft umfassende und integrierte Informationssysteme zum Standard werden“ (S. 254); sie hielten (wohl in Unkenntnis der Aktivitäten der NSA) die mexikanische Verbrecherkartei noch für „das beste Vorbild“ (S. 254). Es wäre wohl naiv, zu glauben, dass andere Potentaten dieser Welt nicht über zumindest ähnliche Fähigkeiten zur Überwachung kleinerer oder größerer Teile der Weltgesellschaft verfügen. Schmidt/Cohen beschreiben die

Praktiken und die Möglichkeiten der Kontrolle sehr gründlich – das ist interessant, auch wenn vieles inzwischen durch die Realität eingeholt oder überholt wurde.

Die absehbaren Möglichkeiten der Überwachung werden häufig mit dem Hinweis darauf verbunden, dass „einige Staaten“ (z. B. S. 57) oder „autoritäre Regimes“ (z. B. S. 92) das eine oder andere verfügbare Instrument nutzen könnten – der Leser kann natürlich auf den Gedanken kommen, dass viele Staaten viele dieser Chancen strategisch kombiniert nutzen. Einige Staaten (?) „werden wissen wollen, wer hinter jedem Nutzerkonto steckt“ (S. 57), und die „Überwachungsregimes werden sich einen langgehegten Traum erfüllen, Handys zu Wanzen umzufunktionieren und ihre Bürger zuhause abzuhören. Technische Lösungen bieten nur einer kleinen, technisch versierten Minderheit Schutz, und auch das nur für kurze Zeit. Diese Regimes werden die Geräte bereits vor dem Verkauf mit der entsprechenden Software ausstatten und sich Zugang zu allem verschaffen, was ihre Bürger öffentlich oder privat sagen, schreiben und veröffentlichen.“ (S. 92).

Resultat: „Der Konflikt zwischen dem Schutz der Privatsphäre einerseits und der inneren Sicherheit andererseits wird sich in den kommenden Jahren weiter verschärfen“. (S. 253). Dabei werden die Sicherheitsbehörden und ihre Systeme „unweigerlich gewaltige Datenmengen über normale Bürger speichern – die Frage ist nur, welche und wo.“ (S. 253). Und ein Hinweis an die Bürger: „Die Vorstellung, Sie könnten ihre persönlichen Daten einfach wieder aus dem Netz entfernen, ist eine Illusion.“ (S. 84). „Wir sind die erste Generation von Menschen mit einer unauslöschbaren Akte.“ (S. 85). Dennoch gibt es das Recht der Bürger auf Datenschutz, es wird Aktivitäten zum Schutz der Privatsphäre geben (S. 90, 92) und Unternehmen (S. 98) sowie Staaten (S. 120) müssen darauf Rücksicht nehmen.

(5) Diktatur, Zensur und Demokratisierung

Schmidt und Cohen gehen davon aus, dass Diktaturen die vorhandenen technischen Möglichkeiten der Überwachung voll ausnutzen werden und auch versuchen, das Internet zu zensieren und/oder mit Hilfe der schon geschilderten Methoden optimal zu überwachen. „Jeder Staat wird versuchen, das Internet zu regulieren und nach seinen eigenen Vorstellungen zu formen. Unabhängig vom politischen System haben alle

Staaten das Bedürfnis, die Gesetze der physischen Welt auf das Internet zu übertragen… Die Mehrheit aller weltweiten Internetnutzer ist einer Form der Zensur ausgesetzt, die auch beschönigend als ‚Filter' bezeichnet wird. Wie diese Zensur aussieht, hängt von der Politik und den technischen Möglichkeiten des jeweiligen Landes ab." (S. 127/28). Bei der näheren Analyse unterscheiden die Autoren „grob zwischen drei Methoden: der unverhohlenen, der feigen und der politisch und kulturell vertretbaren Zensur." (S. 130). Als Beispiel für die unverhohlene Zensur wird China beschrieben, die Türkei steht für die feige Zensur und in Bezug auf Südkorea, Deutschland und Malaysia wird die Zensur als vertretbar bezeichnet (S. 130-135).

Die Autoren schildern für den Fall der Gefahr eines Aufstands das ganze Arsenal von elektronisch gestützten Unterdrückungsmöglichkeiten (z. B. S. 208) am Beispiel des Irans, wie das chinesische Unternehmen Huawei schnell die westlichen Technologie-Lieferanten ersetzte, um dem Regime „zensurfreundliche mobile Nachrichtendienste" (S. 146) zur Verfügung zu stellen.

Schmidt und Cohen sind dennoch optimistisch. Sie sind überzeugt: „Langfristig werden die Kommunikationstechnologien die Positionen der Machthaber in den meisten Diktaturen aushöhlen, da sich das Kräfteverhältnis zwischen einem restriktiven, informationsscheuen Regime und seinen mündigen, mit Informationstechnologie ausgerüsteten Bürgern mit jeder peinlichen Enthüllung zugunsten letzterer verschiebt." (S. 112). Denn: „Selbst in den repressivsten Gesellschaften, deren Regime mit Spionagesoftware und virtuellen Schikanen gegen ihre Bevölkerung vorgehen und Handys manipulieren, werden Menschen mit der nötigen Entschlossenheit andere Möglichkeiten finden, ihre Botschaften zu verbreiten." (S. 281).

(6) Strukturelle Unsicherheit des Internets

Die bisherigen Ausführungen bieten viele Hinweise auf die strukturelle Unsicherheit des Internets für jeden Nutzer – egal, ob Staat, Unternehmen oder Privatperson. Computer, Netze und Handys können angegriffen, überwacht und unter fremder Kontrolle umfunktioniert werden – und einen wirksamen Schutz gibt es kaum. Den damit verbundenen Vertrauensverlust und die Gefahren für die weitere Nutzung des Netzes (Jonathan Zittrain) diskutieren Schmidt und Cohen nicht. Aber sie verweisen

auf einen weiteren wunden Punkt: die unkorrigierbar transparente Identität von Menschen im Netz und die Gefahr des Identitätsdiebstahls.

„Die Identität wird in Zukunft das wertvollste Gut der Bürger sein, und sie wird vor allem in virtuellen Medien existieren… Die Vergangenheit des Menschen lässt sich nicht mehr verändern und kann problemlos für alle sichtbar gemacht werden…. Unsere Kommunikationstechnologie ist von Anfang an auf einen Eingriff in unsere Privatsphäre angelegt… Ohne Regulierung sind unsere Daten daher Freiwild für Arbeitgeber, Zulassungsstellen von Universitäten oder Klatschbasen“. (S. 60/61). Das kann alles noch relativ harmlos sein – schlimmer wird es, wenn sich Kriminelle bedienen und mit Hilfe einer gestohlenen Identität agieren. Schmidt/Cohen diskutieren diesen Punkt nur knapp im Zusammenhang mit der in Zukunft notwendigen **Verifizierung von Quellen (und Personen)**, die vor allem aus Sicherheitsgründen identifizierbar sein müssen (S. 283) und **nicht anonym** sein dürfen (S. 252ff). „Auch Strategien wie eine Registrierung aller Nutzer könnten sich als erfolgreich erweisen.“ (S. 177). Ansonsten beschränken sich die Autoren auf die Bemerkung, dass „wir uns besser gegen Identitätsdiebstahl schützen müssen.“ (S. 257).

Auch die lobend erwähnte **Verschlüsselungstechnik** (z. B. S. 79, 81) hat ihre Grenzen, wenn die Zugänge zu den Schlüsseln legal oder illegal Verbreitung finden. Schmidt/Cohen haben schon vor Bekanntwerden der NSA-Aktivitäten darauf hingewiesen, dass in den USA über Gesetze diskutiert wird, die Anbieter zwingen, Lauschangriffe auf Nutzer zuzulassen „oder den Behörden die Codes zur Entschlüsselung der Nachrichten zur Verfügung zu stellen.“ (S. 108). Fazit: „Doch selbst die Verschlüsselung ist keine Garantie…“ (S.108).

(7) Gedankensteuerung

Im Zusammenhang mit positiven Errungenschaften der Medizin weisen Schmidt/Cohen darauf hin, dass es gute Fortschritte auf dem Gebiet der Roboter-Steuerung nicht nur über Gesten, sondern über Vorstellungen im Gehirn gegeben hat. „In jüngster Zeit wurden auf dem Gebiet der Gedankensteuerung eine Reihe faszinierender Durchbrüche erzielt.“ (S. 34). Gut, solange die Maschinen von den

Gedanken gesteuert werden und nicht umgekehrt. Und gut, solange die Maschinen friedlichen Zwecken dienen.

Informationen, die Einzelne oder Gruppen bewusst oder unbewusst zur Verfügung stellen, können zur Erstellung von Zukunftsprognosen auch in Bezug auf das Kaufverhalten oder von politische Reaktionen genutzt werden. „Wie schon heute werden Onlineanbieter ohne Zustimmung Daten über das Verhalten ihrer Nutzer an Unternehmen und Dritte weitergeben. Die Nutzer geben mehr von sich preis, als sie ahnen. Für Behörden und Unternehmen ist dieser Datenstrom ein Geschenk, mit dem sie auf die Bedürfnisse ihrer Bürger und Kunden eingehen, spezifische demographische Gruppen erreichen und mit Hilfe neuer Methoden künftige Entwicklungen prognostizieren können.“ (S. 88). Das ist die neutrale Form der Darstellung.

(8) Staaten-Bündnisse im Wandel

Eine der Diagnosen des Buches ist die faktische Existenz von Cyberkrieg. „Wir sollten festhalten, dass wir bereits im Zeitalter des Cyberkrieges leben, auch wenn wir uns das selten bewusst machen (S. 155). Schmidt/Cohen vermuten das Entstehen neuer Staaten- und Militärbündnisse, das Entstehen virtueller Staaten und die Einführung einer Visumspflicht im Internet. Vorstellen können sie sich z. B. die Herausbildung eines sunnitischen Internets unter Beteiligung von Saudi-Arabien, Jemen, Algerien und Mauretanien, in dem die Scharia gelten könnte (S. 137). Oder die Cyber-Union besonders autoritärer Staaten wie Weißrussland, Eritrea, Simbabwe und Nordkorea, die untereinander Zensur- und Überwachungsstrategien austauschen (S. 144). Staatenbündnisse könnten Sondereinsatztruppen mit dem Aufbau eigener Netzwerke für Rebellengruppen beauftragen (S. 310). Denkbar ist auch der Aufbau einer „Art Internet-Hanse“ (S. 147) zur Verteidigung von Informations- und Meinungsfreiheit im Internet. Staaten werden ihre Regeln und Gesetze auch im Internet durchsetzen wollen. „Irgendwann wird es auch im Internet die Visumspflicht geben.“ (139). Am Ende könnte es „eine Art Schengener Abkommen für das Internet“ geben – dann „wird die Welt irgendwann ihren ersten Internet-Asylanten haben“ (S. 141). Und es werden „in Zukunft auch virtuelle Staaten entstehen und die virtuelle Landschaft der existierenden Staaten erschüttern“ (S. 150).

(9) Globale Regulierung nötig. Handlungschancen und Akteure.

Schmidt und Cohen erkennen, dass die von ihnen beschriebene globale Dimension der Internet-Entwicklung und der mit ihr verbundenen Gefahren einen Regulierungsbedarf produziert, der nicht auf lokaler oder nationaler Ebene bewältigt werden kann. Erforderlich sind globale Regulierungs-Aktivitäten, für die aber die Instanz fehlt und die Konsense voraussetzt, die auf absehbare Zeit kaum zu erreichen sind. Das deuten Schmidt/Cohen an und liefern Beispiele für die Untermauerung dieser These.

So wünschen sie z. B. „internationale Verträge zum Umgang mit Cyberangriffen"; diese „erfordern erhebliche Investitionen und einen ehrlichen Dialog darüber, was kontrollierbar ist und was nicht." (S. 169/170). Weil z. B. von Schadsoftware befallene Rechner eine Gefahr für alle anderen im Netz darstellen, wird der Vorschlag des Microsoft-Mitarbeiters Craig Mundie referiert, der die befallenen Geräte unter virtuelle Quarantäne stellen will (so werden ja auch „reale" Seuchen bekämpft). „Mundie schlägt die Schaffung einer neutralen internationalen Behörde vor, bei der die Provider die IP-Adressen der infizierten Computer melden. Damit könnten Provider und Staaten diesen Adressen in Quarantäne den Zugang verweigern und so die Reichweite des Angriffs begrenzen… Das infizierte Gerät würde erst dann wieder ans Netz gehen, wenn die Schadprogramme nachweislich beseitigt wurden. Die Arbeit einer solchen Behörde müsste durch einen internationalen Vertrag geregelt werden." (S. 174). Das Problem: Wer betreibt und finanziert die Behörde, wer unterwirft sich den Regelungen, wer überprüft die Virenfreiheit eines jeden Computers oder Smartphones? Wer speichert dann die zu diesem Zweck erhobenen Daten?

Schmidt und Cohen sehen eine besondere Verantwortung und besondere Chancen für die großen Technologieunternehmen, die bei der Verteidigung demokratischer Werte eine Vorreiterrolle übernehmen können (S. 263). Faktisch gestalten sie Gesellschaft, faktisch machen sie Politik. „Es ist ein schmaler Grat zwischen Zensur und Schutz der Sicherheit, und dementsprechend müssen wir unsere Regeln gestalten." (S. 264). Es bleibt die offene Frage, wer denn die global agierenden Internet-Konzerne wie demokratisch kontrollieren kann und will.

(10) Technologiekritik

Schmidt und Cohen bieten Formulierungen für eine Debatte, die früher zum Thema Atomenergie geführt wurde. Dabei ging es um die Verantwortbarkeit des Einstiegs in eine Technologie, deren Beherrschbarkeit und Rückholbarkeit nicht gesichert erschien.

Im Zusammenhang mit der Analyse möglicher zukünftiger (Cyber-)Kriege und des Einsatzes von ferngesteuerten oder sich selbst steuernden Drohnen fragten die Autoren bei der früheren Direktorin der Forschungs- und Entwicklungsabteilung des amerikanischen Verteidigungsministeriums (DAPRA) danach, „wie die Vereinigten Staaten mit der großen Verantwortung umgehen, die mit der Entwicklung solcher letztlich unkontrollierbaren Technologie einhergeht." (S. 299). Die in die Frage eingeflossene Feststellung der Entwicklung einer **letztlich unkontrollierbaren Technologie** zeigt die Dramatik der Situation.

Das gilt auch für den Aufbau der Überwachungstechnologie, deren bei der NSA erreichte Qualität zum Zeitpunkt der Buchproduktion zumindest öffentlich noch nicht bekannt war. Aber die Ahnungen von Schmidt und Cohen reichten schon für die Benennung eines ernsten Problems im Zusammenhang mit **Überwachungs-Datenbanken, mit denen man gar nicht verantwortungsbewusst umgehen kann, selbst wenn man es will** und die ein zukünftiges Gefahrenpotenzial darstellen. „Verantwortungsbewusste Staaten stehen vor schwierigen Problemen. Das Missbrauchspotenzial dieser Datenbanken ist erschreckend groß, ganz zu schweigen von den Gefahren menschlichen Versagens, der Fehlinterpretation von Daten oder einfach der Neugierde. Ein voll integriertes Informationssystem, das Daten aus allen erdenklichen Quellen bezieht und mit Hilfe von komplizierten Algorithmen Verhaltensweisen interpretiert und prognostiziert, ist möglicherweise derart mächtig, dass man gar nicht verantwortungsbewusst damit umgehen kann, selbst wenn man es wollte. Und wenn ein solches System einmal eingerichtet worden ist, wird es nie mehr verschwinden. Welche Regierung würde schon freiwillig ein derart leistungsstarkes Instrument zur Verbrechensbekämpfung aus der Hand geben, selbst wenn sich die Sicherheitslage wieder entspannte? Aber niemand kann garantieren, dass die nächste Regierung dieselbe Zurückhaltung und Sorgfalt beim Umgang mit den Daten walten lässt. Noch stecken integrierte Informationssysteme wie dieses in den Kinderschuhen

und kranken an verschiedenen Problemen (zum Beispiel der uneinheitlichen Datenerfassung), die ihre Effizienz einschränken. Doch diese Probleme lassen sich beheben, und die Verbreitung dieser Plattformen scheint lediglich noch eine Frage der Zeit. Das einzige Mittel gegen eine digitale Diktatur ist eine Stärkung des Rechtsstaats und die Wachsamkeit der Zivilgesellschaft gegenüber möglichem Machtmissbrauch.“ (S. 256).

Insgesamt bietet das Buch einen hervorragenden Eindruck der möglichen (und wohl auch wahrscheinlichen) Zukunft. Ein Grund zur Beruhigung wird nicht geboten. Und die Diskussion von Gestaltungsmöglichkeiten hat noch nicht einmal ernsthaft angefangen.