

REDLINE | VERLAG

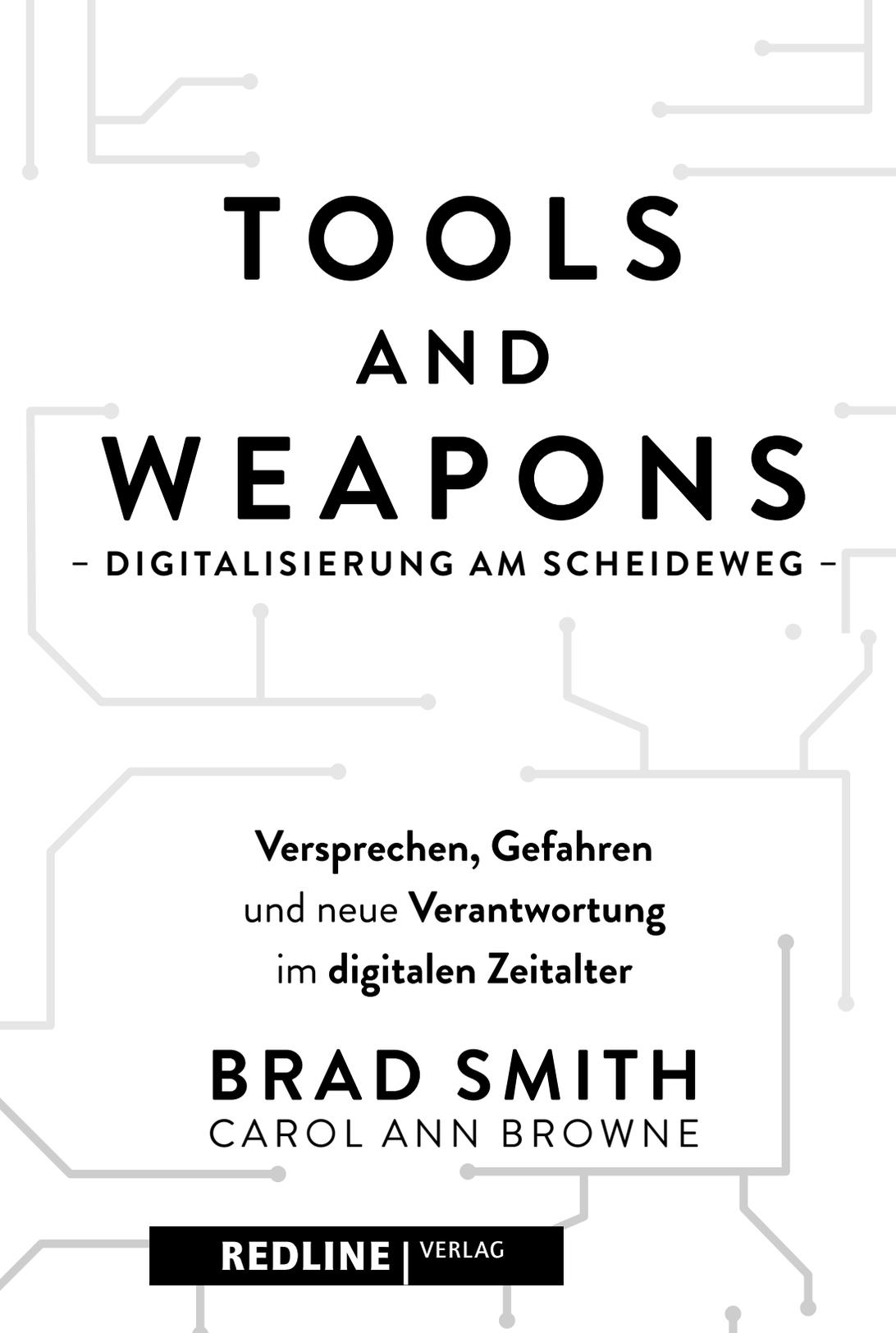
TOOLS AND WEAPONS

- DIGITALISIERUNG AM SCHEIDEWEG -

Versprechen, Gefahren
und neue Verantwortung
im **digitalen Zeitalter**

BRAD SMITH
CAROL ANN BROWNE

MIT EINEM VORWORT VON **BILL GATES**



TOOLS AND WEAPONS

- DIGITALISIERUNG AM SCHEIDEWEG -

**Versprechen, Gefahren
und neue Verantwortung
im digitalen Zeitalter**

BRAD SMITH
CAROL ANN BROWNE

REDLINE | VERLAG

Bibliografische Information der Deutschen Nationalbibliothek:

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://d-nb.de> abrufbar.

Für Fragen und Anregungen:

info@redline-verlag.de

1. Auflage 2020

© 2020 by Redline Verlag, ein Imprint der Münchner Verlagsgruppe GmbH,
Nymphenburger Straße 86
D-80636 München
Tel.: 089 651285-0
Fax: 089 652096

© der Originalausgabe 2019 by Bradorf L. Smith
Die englische Originalausgabe erschien 2019 bei Penguin Press, einem Imprint der Penguin Random House LLC unter dem Titel *Tools and Weapons*.

Alle Rechte, insbesondere das Recht der Vervielfältigung und Verbreitung sowie der Übersetzung, vorbehalten. Kein Teil des Werkes darf in irgendeiner Form (durch Fotokopie, Mikrofilm oder ein anderes Verfahren) ohne schriftliche Genehmigung des Verlages reproduziert oder unter Verwendung elektronischer Systeme gespeichert, verarbeitet, vervielfältigt oder verbreitet werden.

Übersetzung: Norbert Juraschitz, Anja Lerz
Redaktion: Britta Fietzke, Frankfurt a. Main
Umschlaggestaltung: Marc Fischer, München
Umschlagabbildung: Amanda Dewey
Satz: Daniel Förster, Belgern
Druck: GGP Media GmbH, Pößneck
Printed in Germany

ISBN Print 978-3-86881-783-6
ISBN E-Book (PDF) 978-3-96267-197-6
ISBN E-Book (EPUB, Mobi) 978-3-96267-198-3

Weitere Informationen zum Verlag finden Sie unter

www.redline-verlag.de

Beachten Sie auch unsere weiteren Verlage unter www.m-vg.de

INHALT

VORWORT	7
<i>EINLEITUNG</i>	
DIE CLOUD:	
Der Aktenschrank der Welt	11
<i>KAPITEL 1</i>	
ÜBERWACHUNG:	
Eine kurze Lunte	21
<i>KAPITEL 2</i>	
TECHNOLOGIE UND ÖFFENTLICHE SICHERHEIT:	
»Ich wäre lieber ein Verlierer als ein Lügner«	41
<i>KAPITEL 3</i>	
PRIVATSPHÄRE UND DATENSCHUTZ:	
Ein grundlegendes Menschenrecht	59
<i>KAPITEL 4</i>	
CYBERSICHERHEIT:	
Ein Weckruf für die Welt	81
<i>KAPITEL 5</i>	
DEMOKRATIE SCHÜTZEN:	
»Eine Republik, wenn ihr sie bewahren könnt«	97
<i>KAPITEL 6</i>	
SOZIALE MEDIEN:	
Die Freiheit, die uns auseinanderbringt	109
<i>KAPITEL 7</i>	
DIGITALE DIPLOMATIE:	
Die Geopolitik der Technologie	129
<i>KAPITEL 8</i>	
SCHUTZ DER VERBRAUCHERDATEN:	
»Der Spieß wird umgedreht«	151

<i>KAPITEL 9</i>	
BREITBAND IM GANZEN LAND:	
Der elektrische Strom des 21. Jahrhunderts	171
<i>KAPITEL 10</i>	
DIE TALENTLÜCKE:	
Die Menschen hinter der Technologie	189
<i>KAPITEL 11</i>	
KI UND ETHIK:	
Frag nicht, was Computer tun können, sondern was sie tun sollen	211
<i>KAPITEL 12</i>	
KI UND GESICHTSERKENNUNG:	
Verdienen unsere Gesichter den gleichen Schutz wie unsere Telefone?	231
<i>KAPITEL 13</i>	
KI UND ARBEITSKRÄFTE:	
Der Tag, an dem das Pferd arbeitslos wurde	251
<i>KAPITEL 14</i>	
DIE VEREINIGTEN STAATEN UND CHINA:	
Zwei gegensätzliche Tech-Welten	269
<i>KAPITEL 15</i>	
DIE DEMOKRATISIERUNG DER ZUKUNFT:	
Warum wir eine Open-Data-Revolution brauchen	289
<i>KAPITEL 16</i>	
DIGITALE SOUVERÄNITÄT IN EINER VERNETZTEN WELT:	
Eindrücke aus Deutschland	309
<i>KAPITEL 17</i>	
FAZIT:	
Vom Umgang mit einer Technologie, die größer ist als wir ...	327
DANK	345
ANMERKUNGEN	351
STICHWORTVERZEICHNIS	391



VORWORT

Als ich mich zum ersten Mal wegen eines Ratschlags an Brad Smith wandte, machte ich gerade die schwerste Zeit meines Berufslebens durch. Auch zwei Jahrzehnte später wende ich mich, wenn ich Rat benötige, immer noch an ihn.

Brad fing 1993 in der Rechtsabteilung von Microsoft an, richtig kennengelernt haben wir uns jedoch erst in den späten 1990ern, als die Regierung der USA ein Kartellverfahren gegen die Firma führte. Zahllose Stunden arbeiteten wir da Seite an Seite. Mir war gleich klar, was für ein großer Denker er war. Ich lernte ihn mehr und mehr zu schätzen und seinem Urteilvermögen als Profi zu vertrauen.

Während des Kartellverfahrens prägte Brad unsere juristische Strategie ganz maßgeblich. Außerdem tat er etwas, was mindestens genauso wichtig war: Er leitete einen enormen kulturellen und strategischen Wandel im Unternehmen ein, der auch das Kernthema seines Buches ist.

In Microsofts Anfangszeiten brüstete ich mich damit, wie wenig wir mit den Leuten in der Regierung redeten. Damals sagte ich gerne: »Ist es nicht toll, dass wir auch ohne ein Hauptstadtbüro Erfolg haben?« Während des Kartellverfahrens musste ich auf die harte Tour lernen, dass das keine kluge Sichtweise war.

Nachdem der Prozess beendet war, überzeugte Brad mich und viele andere bei Microsoft von der Notwendigkeit einer anderen Herangehensweise und zeigte uns eine mögliche Vorgehensweise. Brad ist Rechtsanwalt, nicht Programmierer, und obwohl er viel von Technologie versteht, tickt und denkt er anders als wir anderen. (Das meine ich als Kompliment.) Er hatte erkannt, dass wir mehr Zeit und Kraft in die Kommunikation mit verschiedenen Stakeholdern investieren mussten, zu denen auch die Regierung, unsere Geschäftspartner und manchmal sogar unsere Wettbewerber gehörten. Brad hätte einen großartigen Diplomaten abgegeben, was angesichts seines frühen Interesses an internationalen Beziehungen nicht ver-

wunderlich ist. Es sagt viel über Brad aus, dass sein Denken sich nicht allein auf Microsofts ureigene Interessen beschränkte. Er erkannte die zentrale Relevanz der Technologie an sich sowie der sich darauf auswirkenden politischen Strategien und Richtlinien. Er schlussfolgerte, dass es nicht nur für unsere Firma, sondern für die gesamte Branche problematisch wäre, wenn wir uns auf ein Agieren an der Außenlinie beschränken würden. Manchmal müssten wir zwar gewiss allein handeln, doch würde es auch häufig Phasen geben (beispielsweise bei den Themen der Künstlichen Intelligenz, Gesichtserkennung und Cyber-Sicherheit), in denen alle Beteiligten viel mehr von einer Zusammenarbeit profitieren würden.

Wie er in diesem Buch erörtert, liegt es gelegentlich auch im Interesse aller, wenn die Regierung stärker regulierend eingreift. (Brad ist reflektiert genug, um die Ironie darin zu sehen, dass einer der führenden Wirtschaftsköpfe nach mehr statt nach weniger staatlicher Regulierung verlangt.) Er wusste, dass Microsoft und andere Technologieunternehmen sich zu diesem Zweck mehr mit Politikern und Entscheidern in den USA, Europa und anderen Ländern zusammensetzen mussten. Die Zeiten, in denen ich mich mit einem nichtexistenten Hauptstadtbüro brüstete, waren vorbei.

Brads Vision war noch nie so relevant. Regierungen weltweit betrachten viele Technologieunternehmen und die Branche an sich überaus kritisch. Wie wird die entwickelte Technologie eingesetzt? Welche Auswirkungen hat sie? Welche Verantwortung tragen Technologieunternehmen? Welche Gedanken sollten sich Regierungen und die allgemeine Öffentlichkeit zu diesen Themen machen?

Obwohl dies nicht dieselben Fragen wie vor zwanzig Jahren sind, so sind Brads Erkenntnisse von damals doch heute noch genauso wertvoll.

Beispielsweise wären da die Fragestellungen, die im Zusammenhang mit der Gesichtserkennungstechnologie aufkommen. In der öffentlichen Debatte ist das noch kein großes Thema, wird es aber zukünftig werden. Mit welcherlei Einschränkungen sollten Software-Firmen ihre Gesichtserkennungstechnologien versehen? Wie sollte die Branche darüber denken und welche staatlichen Regulierungen wären sinnvoll?

Indem er diese Fragen vorhergesehen und Kooperationen angestoßen hat, in denen sie diskutiert werden, hat Brad eine Vorreiterrolle eingenommen. Die Technologiebranche wird sich zusammentun und sowohl

mit Kunden als auch Regierungen weltweit zusammenarbeiten müssen. Mag sein, dass es unmöglich ist, alle an Bord zu bekommen, aber wenn wir eine Fragmentierung zulassen, wenn wir zulassen, dass sich Vorschriften und Regelungen von Land zu Land massiv unterscheiden, wird das weder für die Kunden noch für die Branche noch für die Gesellschaft gut sein.

In *Tools and Weapons – Digitalisierung am Scheideweg* analysiert und diskutiert Brad 15 Themen – ein beeindruckendes Spektrum. Unter anderem geht es um Cyber-Sicherheit, die Diversität der Arbeitskräfte in der IT-Branche und das Verhältnis zwischen den USA und China. Sollte ich das wichtigste Kapitel benennen müssen, würde ich mich wohl für das über Privatsphäre entscheiden. Riesige Datenmengen sammeln zu können, ist ein zweischneidiges Schwert. Einerseits ermöglicht es Regierungen, Firmen und Einzelpersonen, bessere Entscheidungen zu treffen. Andererseits stellen sich dadurch aber auch wichtige Grundsatzfragen, wie zum Beispiel die, wie wir diese Daten nutzen und gleichzeitig das Recht auf Privatsphäre schützen können.

Brad zeigt jedoch auf, dass die Technologie zwar relativ jung sein mag, die Fragen an sich aber bereits alt sind. Mit der einen oder anderen Variante dieses Problems müht sich die Menschheit seit Jahrhunderten ab. Während man vielleicht nicht überrascht darüber ist, dass sich ein Kapitel über Daten und Privatsphäre auch mit der Informationensammlung über das Volk während der Zeit des Nationalsozialismus befasst, kommen die Erwähnung des Krieges von 1812 oder ein kurzer Überblick über die Geschichte der internationalen Rechtshilfe doch eher unerwartet.

Dies zeigt Brads weitreichende Interessen und seine Fähigkeit, sich in beinahe jedes Feld gründlich einzuarbeiten zu können. Dennoch wirkt keins der Kapitel wie ein langweiliger juristischer Schriftsatz. Brad und seine Mitverfasserin Carol Ann Browne sind großartige Geschichtenerzähler, die aus ihrer Insiderperspektive heraus zeigen, wie es ist, diese Fragestellungen in Echtzeit anzugehen, in Konferenzräumen und Gerichtssälen auf der ganzen Welt. Brad lehnt sich nicht zurück und analysiert solche Probleme, stattdessen bringt er Menschen für die Lösungsfindung an einen Tisch zusammen.

Aufgrund eben dieser Themen stehen Brad und ich immer in Kontakt zueinander – persönlich und per E-Mail. Ich verlasse mich auch heute noch

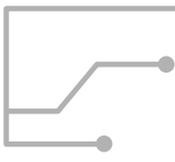
auf seine Weisheit und sein Urteilsvermögen. Angesichts seiner Erfahrung und Intelligenz könnte man sich keinen besseren Lotsen durch das Fragenlabyrinth vorstellen, mit denen sich die Technologiebranche heute konfrontiert sieht.

Und diese Fragestellungen werden sogar noch weiter an Bedeutung gewinnen. *Tools and Weapons – Digitalisierung am Scheideweg* bietet eine klare Sicht auf diese Fragen, die durch die neuen Technologien aufkommen, und zeigt einen möglichen, gangbaren Weg für Technologieunternehmen und Gesellschaft auf. Brad hat für einige der aktuell drängendsten Debatten in Sachen Technologie einen klaren, überzeugenden Wegweiser geschrieben.

Bill Gates

April 2019

EINLEITUNG



DIE CLOUD: Der Aktenschrank der Welt

Seit jeher sind Daten der Stoff, der die Zivilisation am Laufen hält. Die Geschichte der Menschheit begann, als die Menschen die Sprachfähigkeit entwickelten. Durch die Erfindung der Sprache konnten Ideen, Erfahrungen, Wünsche und Bedürfnisse anderen mitgeteilt werden.

Mit der Entwicklung der Schrift beschleunigte sich der Fortschritt. Gedanken verbreiteten sich leichter und präziser, nicht nur von einer Person zur nächsten, sondern auch von Ort zu Ort.

Dann entstand der Funke, der die Flamme des Wissens entfachte: die Fähigkeit, das Geschriebene zu lagern, wiederzufinden und zu teilen. Der Bau von Bibliotheken wurde zu einem Kennzeichen der Antike.¹ Dank dieser Archive voller Dokumente und Bücher konnten Menschen nicht nur über räumliche, sondern auch über zeitliche Distanzen hinweg kommunizieren und Informationen von einer Generation zur nächsten weitergeben. Als Johannes Gutenberg Jahrhunderte später die Druckerpresse erfand, wurde aus der Flamme ein Feuer, das gleichermaßen Schreibenden wie Lesenden mehr Macht verlieh.

Dieses Feuer sollte sich weltweit verbreiten. In den darauffolgenden Jahrhunderten kam es zu einem sprunghaften Anstieg des Welthandels, der einerseits erst durch ein erhöhtes Kommunikationsaufkommen ermöglicht wurde, andererseits auch weiteren Kommunikationsbedarf und somit noch größere Datenmengen nach sich zog. Als schließlich das 20. Jahrhundert anbrach, brauchte jedes Büro einen Lagerraum für seine Dokumente. Aktenschränke füllten ganze Räume.² Obwohl Daten für die Gesellschaft schon immer wichtig waren, spielten sie noch nie eine größere Rolle. Selbst wenn

die Wirtschaft stagniert oder gar einbricht, wächst der Datenfluss unaufhörlich weiter. Manche sagen, Daten seien das Öl des 21. Jahrhunderts. Aber das ist nur eine unzulängliche Beschreibung der Wirklichkeit. Noch vor einem Jahrhundert funktionierten Automobile, Flugzeuge und viele Züge mit Öl oder einem Derivat dessen. Heutzutage wird jeder Aspekt menschlichen Lebens von Daten am Laufen gehalten. In Hinblick auf unsere moderne Zivilisation entsprechen Daten eher der Luft, die wir atmen, als dem Öl, das wir verbrennen.

Anders als Öl haben sich Daten zu einer erneuerbaren Ressource entwickelt, die wir Menschen selbst erschaffen können. Am Ende dieses Jahrzehnts wird es nahezu 25-mal so viele digitale Daten geben als an seinem Anfang.³ Aufgrund der Künstlichen Intelligenz (oder auch: KI) arbeiten wir mehr mit Daten als je zuvor.

Die dies unterstützende digitale Infrastruktur nennen wir die Cloud. Während der Name an eine weiche und flockige Wolke erinnert, ist die Cloud in Wirklichkeit eine Festung. Jedes Mal, wenn Sie etwas in Ihrem Smartphone nachschauen, beziehen Sie Daten aus einem gigantischen Rechenzentrum – einem modernen Weltwunder, das kaum jemand betreten darf.

Doch wenn Sie das Glück haben, einmal ein Rechenzentrum besuchen zu dürfen, werden Sie die heutige Welt besser verstehen können.

Einer der besten Orte für die Betrachtung dieser Funktionsweisen der Cloud ist die Welthauptstadt der Äpfel. Die kleine Stadt Quincy liegt grob 250 Kilometer östlich von Seattle an der Interstate 90 im Staat Washington. Die Lage der Stadt ist kein Zufall. Quincy befindet sich im Zentrum einer landwirtschaftlich intensiv genutzten Senke, ganz in der Nähe einer tiefen Schlucht, die sich der Columbia River, die größte Wasserstraße im Westen der USA, im Lauf der Jahrtausende gegraben hat. Die Stadt bezieht ihre Elektrizität aus einem Netz aus Wasserkraftwerken, zu dem auch der Grand Coulee Dam gehört, der Staudamm mit dem größten Kraftwerk der Vereinigten Staaten. Dies alles bildet die perfekte Umgebung für das, was zum größten Energieverbraucher der Welt geworden ist: das moderne Rechenzentrum.⁴

Wenige Häuserblöcke von der Hauptstraße entfernt findet man hinter hohen Zäunen und Mauern eine Reihe unauffälliger Gebäude. Manche

von ihnen tragen die Logos von Technologieunternehmen unserer Zeit, andere weisen sich durch gar nichts aus. Die größte dieser Einrichtungen heißt »Columbia Data Center« und gehört Microsoft.

Es ist aufregend – und ein bisschen unheimlich –, die schiere Größe eines Rechenzentrums so vor sich zu sehen. Unsere Anlagen in Quincy bestehen nicht mehr nur aus einem einzigen Gebäude. Sie füllen zwei Areale mit Rechenzentren in über zwanzig Gebäuden, insgesamt sind das etwa 186 000 Quadratmeter. Jedes Gebäude ist so groß wie zwei Fußballfelder und theoretisch groß genug für zwei große Verkehrsflugzeuge. Diese Gebäudeansammlung beherbergt Hunderttausende Servercomputer und Millionen Festplatten, die alle im Drei-Jahres-Zyklus durch schnellere und effizientere Modelle ersetzt werden.

Um sich ein Bild von der Größe eines Rechenzentrums zu machen, geht man am besten zu Fuß vom äußersten Rand bis in die Zentrumsmitte. Vor den Mauern eines jeden Gebäudes befinden sich einige der größten Stromgeneratoren der Welt, die auf Abruf binnen Sekunden hochfahren können, damit das Rechenzentrum keinen Herzschlag lang ohne Strom ist, falls das Elektrizitätsnetz der Region ausfallen sollte. Jeder Generator ist über sechs Meter hoch und könnte genug Energie für 2000 Haushalte produzieren. Die Generatoren sind mit Dieseltanks verbunden, die das Rechenzentrum 48 Stunden lang autark versorgen könnten. Zusätzlich gibt es einen Reserveplan, damit der Betrieb falls nötig auch über diesen Zeitraum hinaus aufrechterhalten werden kann. In unseren neueren Anlagen (wie in Cheyenne, Wyoming) werden die Generatoren mit saubererem Erdgas betrieben und bilden ein Backup für das regionale Stromnetz. Dutzende dieser gigantischen Generatoren stehen neben den Gebäuden der Rechenzentren, allzeit bereit, falls die vom Grand Coulee Dam gelieferte Energie aus Wasserkraft ausfallen sollte.

In jedem Gebäude befinden sich Umspannwerke, die in einer Reihe großer Sicherheitsräume untergebracht sind. In der Regel entnehmen sie Energie in Form von 230 000 Volt aus dem Stromnetz, die sie auf 240 Volt drosseln, um so die Computer des Rechenzentrums zu versorgen. Die Räume mit diesen Umspannanlagen sind durchzogen von zwei Meter hohen IT-Racks, Gestellen mit einem Montageraster. Diese verbinden jeweils 500 oder mehr Batterien miteinander, die im Einzelnen so aussehen

wie die Batterien, die man unter der Motorhaube eines jeden Autos finden kann. Jede Tür zu diesen Räumen ist schussicher, jede Wand feuerfest, um die Ausbreitung eines Brandes von einem Raum zum nächsten zu verhindern. Ein typisches Rechenzentrum verfügt über vier oder mehr solcher Räume. Je nach Konfiguration können in einem solchen Gebäude an die 5000 Batterien untergebracht sein. Sie haben zwei Funktionen: Zum einen fließt Strom aus dem Elektrizitätsnetz durch die IT-Racks, wodurch die Batterien geladen bleiben und potenzielle Energiespitzen abfedern können, sodass der Energiezufluss zu den Computern gleichmäßig und konstant bleibt. Zum anderen halten die Batterien im Falle eines Stromausfalls das Rechenzentrum am Laufen, bis die Generatoren bereit sind.

In einer weiteren Schleuse mit schussicheren Türen und feuerfesten Wänden steht ein Metalldetektor, wie man ihn an Flughäfen findet, besetzt mit zwei uniformierten Wachen. Dieser ist die letzte Bastion zwischen Ihnen und dem Allerheiligsten des Komplexes. Hier dürfen nur in Vollzeit angestellte Mitarbeiter durch, deren Namen auf einer im Voraus bewilligten Liste stehen. Nachdem Sie einen kleinen Empfangsraum betreten haben, schließt sich eine Stahltür hinter Ihnen. Eingeschlossen warten Sie, während die Sicherheitsleute Sie mithilfe einer Kamera mustern, ehe sie die nächste schussichere Tür öffnen.

Endlich betreten Sie einen höhlenartigen Raum. Ein gedämpftes Summen heißt Sie im Zentrum willkommen. Hier gibt es deckenhohe Regale voller Computer – weiter als das Auge reicht. Diese enorme Bibliothek aus Stahl und Schaltkreisen beherbergt die Server, die in ihrem Aufbau alle identisch sind, aber ihre ganz individuellen Datensätze in sich tragen. Dies ist der Aktenschrank der Welt.

Irgendwo in einem dieser Gebäude befinden sich die zu Ihnen gehörenden Daten. Sie enthalten die E-Mail, die Sie heute Morgen geschrieben haben, das Dokument, an dem Sie gestern Abend noch gearbeitet haben, und das Foto, das Sie gestern Nachmittag geschossen haben. Wahrscheinlich finden sich in ihnen auch persönliche Informationen, die Ihre Bank, Ihr Arzt und Ihr Arbeitgeber über Sie angelegt haben. Diese Dateien belegen nur einen Bruchteil des Speicherplatzes auf einer Festplatte in einem dieser Tausende und Abertausende Computer. Jede Datei ist chiffriert, die

Informationen sind also so verschlüsselt, dass nur autorisierte Nutzer diese Daten lesen können.

In jedem Gebäude des Rechenzentrums befinden sich mehrere solcher Räume, die aus Brandschutzgründen voneinander abgeschirmt sind. Jeder Satz Computer ist innerhalb des Gebäudes mit drei Energiequellen verbunden. Und jede Computerreihe ist so angelegt, dass die abgestrahlte Wärme zirkulieren kann, um den Heizbedarf und somit den Energiebedarf im Winter zu senken.

Beim Verlassen des Serverraums müssen Sie die Sicherheitsprozedur erneut über sich ergehen lassen. Schuhe und Gürtel werden ausgezogen. Während Sie noch darüber nachdenken, dass Sie das beim Verlassen eines Flughafens noch nie tun mussten, erinnert Ihr Gastgeber Sie daran, dass die Sicherheitsvorkehrungen aus gutem Grund für beide Richtungen gelten. Microsoft will sicherstellen, dass niemand Daten auf einen USB-Stick kopiert oder gar eine Festplatte mit persönlichen Daten stiehlt. Selbst die Festplatten selbst verlassen das Gebäude durch einen speziellen Ausgang. Wenn sie ersetzt werden müssen, werden die Daten auf einen neuen Computer kopiert und sämtliche Dateien gelöscht. Dann wandert die ausgemusterte Festplatte in eine übergroße Metallvariante eines Reißwolfs.

Das Beeindruckendste wartet gewissermaßen am Schluss der Führung. Man erfährt, dass es in jeder Region, in der sich Rechenzentren befinden, einen zweiten Gebäudekomplex wie diesen hier gibt, sodass die Daten von Unternehmen, Regierungen oder gemeinnützigen Organisationen dauerhaft mittels eines Backups an einem anderen Ort gesichert werden. So kann das zweite Rechenzentrum einspringen, um den Clouddienst problemlos aufrechtzuerhalten, falls es ein Erdbeben, einen Hurrikan oder eine andere Katastrophe – sei sie natürlicher oder menschengemachter Natur – geben sollte. Wir haben es erlebt: Als ein Erdbeben den Norden Japans erschütterte, garantierte unser Rechenzentrum im Süden Japans eine ununterbrochene Sicherstellung des Services.

Heute besitzt, betreibt und least Microsoft Rechenzentren aller Größen an über 100 Standorten in über 20 Ländern (eine kontinuierlich steigende Zahl), bietet 200 Onlinedienste an und bedient über eine Milliarde Kunden in über 140 Märkten.

Als ich 1993 bei Microsoft anfang, brauchte man für die Gründung einer Softwarefirma nicht viel Kapital. Bill Gates und Paul Allen, unsere beiden Gründer, waren die letzten einer ganzen Reihe Entwickler, die ihre Firmen in einer Garage oder einem Wohnzimmer am College gründeten. Für die Softwareentwicklung war nicht viel Geld nötig – das war der springende Punkt. Ein guter Computer, ein wenig Ersparnes und die Bereitschaft, Unmengen Pizza zu vertilgen, reichten für den Anfang.

Während Microsoft sich vom winzigen Start-up zu dem heutigen internationalen Konzern mauserte, erlebten wir das immer wieder. 2004 wollten wir eine Antispy-Softwarefirma namens Giant Company Software aufkaufen. Zur ersten Kontaktaufnahme rief unser Team die Telefonnummer an, die für den technischen Support angegeben war. Als der Anrufer von Microsoft darum bat, zum Geschäftsführer durchgestellt zu werden, wurde das Telefon einfach an den einzigen anderen Mitarbeiter weitergereicht, der einfach auf der anderen Schreibtischseite saß. Es wird daher wohl kaum überraschen, dass die Verhandlungen zügig vonstattengingen.⁵

Bei jedem meiner Besuche eines unserer Rechenzentren denke ich an Giant Company Software. Man kann auch heute noch ein neues Programm oder eine neue App entwickeln, so wie Bill und Paul in ihren Anfangszeiten damals. Open-Source-Entwickler machen das die ganze Zeit. Aber Plattformen bieten, die in unserer globalisierten Gesellschaft von heute für Cloudcomputing benötigt werden? Das ist eine ganz andere Geschichte. Wenn ich zwischen Tausenden blinkenden Computern, Batteriereihen und riesenhaften Generatoren umhergehe, fühlt sich das wie eine andere Ära an. Wie ein anderer Planet. Der Bau von Rechenzentren kostet Hunderte Millionen Dollar. Und sobald der Bau beendet ist, fängt die Arbeit, also die Instandhaltung und das Upgrade der Einrichtung, erst an. Areale werden vergrößert und Server, Festplatten und Batterien auf den neuesten Stand gebracht oder gegen neue und effizientere Geräte ausgetauscht. Ein Rechenzentrum ist niemals fertig.

In vielerlei Hinsicht bildet das moderne Rechenzentrum den Mittelpunkt der neuen digitalen Ära, in die die Welt eingetreten ist. Mit der Ansammlung enormer Datenmengen, Lagerkapazität und Rechenleistung wurde in allen Wirtschaftssystemen weltweit eine noch nie dagewesene Basis für Fortschritt geschaffen. Doch dadurch sind auch neue Probleme

entstanden, die uns vor große Herausforderungen stellen. Wie finden wir in dieser neuen Ära die richtige Balance zwischen öffentlicher Sicherheit, persönlichen Annehmlichkeiten und Privatsphäre? Wie schützen wir uns vor Cyberangriffen, die mithilfe dieser Technologie in unseren Ländern, Unternehmen und Privatleben für Unruhe sorgen? Wie gehen wir mit den ökonomischen Folgen um, die sich nun in unserer Gesellschaft bemerkbar machen? Wird es in Zukunft noch Arbeit für unsere Kinder geben? Werden wir die Welt, die wir erschaffen, überhaupt noch kontrollieren können?

Um Antworten auf all diese Fragen zu finden, müssen wir die Veränderungen der Technologie besser verstehen. Das geht am besten, wenn wir zunächst einmal nachvollziehen, wie sie sich in der Vergangenheit verändert hat.

Seit Anbeginn der Zeit kann jedes Werkzeug zum Guten oder Bösen verwendet werden. Selbst ein Besen kann dazu benutzt werden, den Boden zu kehren oder jemandem zu schlagen. Je mächtiger das Werkzeug ist, desto größeren Nutzen oder Schaden kann es verursachen. Weitreichende digitale Veränderungen bieten vielversprechende Möglichkeiten, doch die Welt setzt die Informationstechnik nicht nur als nützliches Werkzeug ein, sondern auch als mächtige Waffe.

Die neue Technologieära hat zunehmend ein neues Angstzeitalter eingeläutet. Diese Anspannung zeigt sich vor allem in den Demokratien der Welt. Da die Besorgnis der Bevölkerungen aufgrund von Zuwanderung, Globalisierung und Einkommensunterschieden wächst, sehen sich Staaten immer häufiger mit populistischen und nationalistischen Verwerfungen konfrontiert, die teilweise von gewaltigen technologischen Veränderungen herrühren. Die Vorzüge moderner Technologien sind nicht gleichmäßig verteilt, außerdem verlangen Charakter und Geschwindigkeit der Veränderungen Einzelpersonen, Gemeinschaften und ganzen Ländern einiges ab. Demokratische Gesellschaften sehen sich größeren Herausforderungen gegenüber, als sie in fast einem Jahrhundert bewältigen mussten. Zusätzlich setzen manche Länder die neuen Technologien zur Ausnutzung dieser Schwäche ein.

Tools and Weapons – Digitalisierung am Scheideweg untersucht diese Themen vom Cockpit eines der weltweit größten Technologieunternehmen

aus. Es erzählt davon, wie der Technologiesektor mit Kräften umzugehen versucht, die größer sind als eine Firma oder sogar die gesamte Branche. Damit erzählt es nicht nur eine Geschichte der Trends und Ideen, sondern der Menschen, Entscheidungen und Handlungen, mit denen man einer sich rapide verändernden Welt begegnet.

Es ist eine fortlaufende Geschichte, die wir bei Microsoft manchmal von einem anderen Standpunkt aus betrachten. Vor zwei Jahrzehnten wurden wir ins Epizentrum einer Entwicklung hineingestoßen, die man als das erste Aufeinandertreffen moderner Informationstechnik und der Welt verstehen könnte. In den USA wollten das Justizministerium und zwanzig Bundesstaaten in einem Kartellverfahren gegen Microsoft das Unternehmen zerschlagen. Regierungen anderer Länder folgten mit eigenen Gerichtsverfahren. Kartellbehörden waren zu dem Schluss gekommen, das Betriebssystem »Windows« sei zu wichtig, um es nicht zu regulieren.

Auch wenn wir uns erfolgreich gegen diese Zerschlagung wehren konnten, war dies doch eine schwierige, aufreibende und sogar schmerzhafte Erfahrung. Als ich 2002 zum General Counsel der Firma ernannt wurde, musste ich mit Regierungen auf der ganzen Welt und Unternehmen quer durch den Technologiesektor eine Art Friedensvertrag aushandeln. Es dauerte fast ein Jahrzehnt⁶ und wir machten dabei wohl mehr Fehler, als vielleicht nötig gewesen wären. Aufgrund meiner Position war ich letzten Endes für fast alle dieser Fehler mitverantwortlich.

Nachdem wir diese Herausforderungen gemeistert hatten, waren wir nicht nur älter, sondern auch klüger. Wir lernten, dass wir in den Spiegel schauen und überlegen mussten, was andere in uns sahen, und uns nicht nur nach unseren eigenen Wünschen wahrnehmen durften. Es war, als wären wir der erste Abschlussjahrgang einer neu gegründeten Schule. Wir waren nicht unbedingt die Klassenbesten, aber wir hatten den Vorteil, dass wir die Schule vor allen anderen abschlossen.

Die Technologien heute sind viel weitreichender und vielschichtiger als noch vor zwanzig Jahren. Wir haben sowohl technologisch als auch gesellschaftlich einen kritischen Wendepunkt erreicht, denn wir leben in einer Zeit, die einerseits mit einer Vielzahl Möglichkeiten lockt, die aber andererseits auch nach sofortigen Lösungsansätzen bei akuten Problemen verlangt.

Infolgedessen wird sich der Technologiesektor wie Microsoft vor zwanzig Jahren verändern müssen. Es ist an der Zeit, ein ebenso einfaches wie wesentliches Grundprinzip anzuerkennen: Wenn man eine weltverändernde Technologie entwickelt, trägt man auch Verantwortung für den Umgang mit dieser neuen miterschaffenen Welt. Man muss sich der Frage stellen, wie man mit dieser Welt umgehen soll. Das scheint zwar soweit unstrittig, ist es aber in einem Sektor nicht, der sich seit Langem zwanghaft auf schnelles Wachstum und manchmal sogar auf disruptive Innovation als Selbstzweck konzentriert hat. Kurz gesagt: Technologien entwickelnde Unternehmen müssen mehr Verantwortung für die Zukunft übernehmen.

Ebenso wichtig ist allerdings ein weiterer Grundsatz: Der Technologiesektor kann diese Herausforderungen nicht allein meistern. Die Welt braucht eine Mischung aus Selbstregulierung und Regierungsmaßnahmen. Auch hier ergeben sich schwerwiegende Folgen für die Demokratien, unter anderem, weil sie am meisten davon abhängig sind, einen breiten ökonomischen und sozialen Konsens aufrechtzuerhalten, und das in einer Zeit, in der Technologie eine so unruhestiftende Kraft entfaltet. Mehr denn je fällt es vielen demokratischen Regierungen schwer, Handlungsbereitschaft aufzubringen. Aber wir leben in einer Zeit, in der demokratische Regierungen neue politische Linien und Programme entwickeln müssen – jede für sich, aber auch gemeinsam und in einer neuen Form der Zusammenarbeit mit der Technologiebranche. Einfach ausgedrückt müssen die Regierungen schneller vorankommen und endlich anfangen, mit der Geschwindigkeit technologischer Entwicklungen Schritt zu halten.

Für diese Herausforderungen gibt es kein Handbuch. Wir können jedoch wichtige Erkenntnisse aus der Vergangenheit ziehen und auf unsere Gegenwart anwenden. Seit dem Beginn der ersten industriellen Revolution in den englischen Midlands im 18. Jahrhundert hat sich der technologische Wandel in mehreren Wellen auf der Welt ausgebreitet. Für jede uns heute beispieldlos erscheinende Herausforderung gibt es oft ein historisches Gegenstück, das trotz des zeitlichen Abstands mit Erkenntnissen für unsere heutige Zeit aufwarten kann. Dieses Buch schildert die Möglichkeiten und Herausforderungen der Zukunft, indem es sich unter anderem auf die Lektionen der Vergangenheit bezieht – mit Gedanken zu deren möglichen Lehren.

Letztendlich geht es bei diesen Fragen um Technologie und deren Folgen für unsere Arbeitsplätze, unsere Sicherheit und die grundlegenden Menschenrechte. Wir müssen eine Ära rapiden technologischen Wandels mit traditionellen und sogar zeitlosen Werten in Einklang bringen. Um das zu erreichen, müssen wir den Fortschritt der Innovation sicherstellen. Dies jedoch muss so geschehen, dass sich die Technologie und die sie erschaffenden Unternehmen den demokratischen Gesellschaften und unserer kollektiven Fähigkeit, selbst über unser Schicksal zu bestimmen, unterordnen.

KAPITEL 1



ÜBERWACHUNG: Eine kurze Lunte

Als am 6. Juni 2013 die Frühsommersonne in Redmond, Washington, durch die Wolken brach, drehte Dominic Carr die Lamellen des Rollos in seinem Büro in der fünften Etage auf dem Microsoftgelände ein wenig weiter auf. Auch wenn es noch einen ganzen Monat dauern würde, bis der Sommer wirklich im pazifischen Nordwesten ankam, waren die Sonnenstrahlen doch ein willkommener Vorbote wärmerer Tage – und hoffentlich eines etwas gemächlicheren Tempos.

Dominic schnappte sich sein Telefon und fuhr mit dem Aufzug nach unten, um sich in der Firmencafeteria nebenan ein Sandwich zu kaufen. Während er sich durch die vielen Menschen auf den Wegen zwischen den Gebäuden schlängelte, vibrierte plötzlich sein Handy in seiner Hosentasche. Dominic war Leiter des Teams für öffentliche Angelegenheiten und Kommunikation und mir somit direkt unterstellt. In dieser Position musste er unter anderem die Firma in einigen der heikelsten Fragen gegenüber der Presse vertreten. Er war nie ohne Telefon unterwegs – und selten weit von seinem Schreibtisch entfernt.

Auf seinem Display leuchtete eine Meldung auf: Eingang einer E-Mail mit dem Betreff »Microsoft/PRISM«. Damals war »PRISM« unsere Bezeichnung für die jährliche Vertriebsleiterversammlung. Es war also nur eine weitere Meldung über das Alltagsgeschäft bei Microsoft. Routine.

Doch diese E-Mail war alles andere als alltäglich. Ihr Inhalt sollte bald die ganze Welt erschüttern – eine kurze Lunte glomm bereits, es würde nur noch drei Stunden bis zur Explosion dauern.

»Wir möchten Sie hiermit darauf aufmerksam machen, dass der *Guardian* für heute Abend einen Artikel zur Veröffentlichung über PRISM vorgelesen hat, ein freiwilliges, geheimes Kooperationsprogramm mehrerer großer Technologieunternehmen mit der NSA«, begann die E-Mail, die sich auf die National Security Agency der Vereinigten Staaten, kurz »NSA«, bezog.

Die E-Mail kam von einem zweiten Dominic, Dominic Rushe, der als Reporter für die britische Tageszeitung *The Guardian* schrieb. Sie war ursprünglich im Posteingang eines PR-Managers von Microsoft in Boston gelandet, der sie mit einer roten Markierung weitergeleitet hatte – einer Markierung mit einem Ausrufezeichen, die im Grunde bedeutet: »Jetzt, sofort und auf der Stelle lesen.«

Zur Mail gehörte eine Liste mit neun komplexen Punkten, zu denen sich Microsoft äußern sollte, allerdings blieb dafür kaum Zeit. Rushe erklärte: »Als verantwortungsvolle Journalisten möchten wir Ihnen die Möglichkeit geben, mögliche Ungenauigkeiten in den oben genannten Punkten konkret zu kommentieren. ... Wir sind bezüglich dieser Story bereits an das Weiße Haus herangetreten. Aufgrund der Vertraulichkeit des Programms ist dies für uns der frühestmögliche Zeitpunkt, Sie hinsichtlich eines Kommentars zu kontaktieren.« Er wollte eine Antwort – und zwar bis 15 Uhr unserer Zeit am selben Nachmittag. Der *Guardian* war an vertrauliche Geheimdienstinformationen gekommen, in denen detailliert geschildert wurde, wie neun US-amerikanische Technologieunternehmen – Microsoft, Yahoo, Google, Facebook, Paltalk, YouTube, Skype, AOL und Apple – sich angeblich an einem freiwilligen Programm namens PRISM beteiligt hatten, wodurch die NSA unmittelbaren Zugang zu E-Mails, Chats, Videos, Fotos, sozialen Medien und anderen Daten erhalten hatte.

Dominics Pläne für seine Mittagspause – und für den Großteil der darauffolgenden Tage – waren vom Tisch. Er machte auf dem Absatz kehrt und rannte immer zwei Stufen auf einmal nehmend zurück in die fünfte Etage. Er vermutete, die Angelegenheit stünde irgendwie im Zusammenhang mit einem besorgniserregenden Artikel, der bereits am selben Morgen im *Guardian* erschienen war. Die Zeitung hatte einen geheimen Gerichtsbeschluss veröffentlicht, nach dem der amerikanische Telekommunikationsriese Verizon den Behörden »laufend, täglich« Aufzeichnungen von Anrufen zu

übermitteln hatte (und zwar von Inlandsgesprächen ebenso wie von Telefonaten zwischen den USA und dem Ausland).¹ Diese Aufzeichnungen wurden von der NSA analysiert, die in ihrem Hauptquartier in Fort Meade, Maryland, schon seit Langem Nachrichtensignale und Daten auf der ganzen Welt sammelte. Laut Artikel waren von dieser Massenspeicherung auch Millionen Amerikaner betroffen, gleichgültig, ob sie sich etwas hatten zu Schulden kommen lassen oder nicht.

Wenn überhaupt jemand bei Microsoft etwas über PRISM wusste, dann John Frank, der Anwalt, der in der juristischen Abteilung die Teams hinsichtlich nationaler Sicherheitsfragen zu unserer Arbeit leitete. Dominic machte sich also schnurstracks auf den Weg zu Johns Büro.

John reagierte auf die Nachricht des *Guardian* auf Dominics Telefon so gefasst und strukturiert wie üblich und dachte erst einmal gründlich nach. Er nahm seine Brille ab, lehnte sich zurück und sah in den sonnigen Früh Sommertag hinaus. Plötzlich wirkte er müde. »Das ergibt überhaupt keinen Sinn. Nichts davon klingt plausibel.«

John wusste nicht nur, wie die Firma auf Anfragen der Gesetzeshüter reagierte, was sie überprüfte und wie sie dabei verfuhr, er hatte diesen gesamten Ablauf selbst strukturiert. Microsoft gab Kundendaten nur aufgrund gültiger Rechtsbeschlüsse in ordnungsgemäßen Verfahren weiter – und dann nur für konkrete Nutzerkonten oder Einzelpersonen.

Als John und Dominic dann zusammen in meinem Büro standen, konnten sie mir wenig mehr zeigen als die Nachricht des Reporters. »Wenn die das tatsächlich tun, dann tun sie es ohne unser Wissen«, sagte John.

Ja, wir waren dem Gesetz nach dazu verpflichtet, Gesuche um die Herausgabe von Daten unserer Kunden zu prüfen und adäquat darauf zu reagieren. Wir verfügten über ein etabliertes Verfahren zur peniblen Überprüfung solcher Behördengesuche und hatten dezidierte Verhaltensstandards. Aber Microsoft ist ein großes Unternehmen. Hatte hier etwa ein einzelner Mitarbeiter auf eigene Faust gehandelt und sich nicht an die Vorschriften gehalten?

Das war eine Frage, die wir jedoch schnell abtaten. Wir kannten unsere Methodik und den Ablauf, wie Anfragen von Behörden entgegen genommen und geprüft wurden, und wie darauf zu reagieren war. Die Nachricht des *Guardian* ergab einfach keinen Sinn.

Niemand bei Microsoft hatte je von PRISM gehört. Der *Guardian* wollte die durchgesickerten Dokumente, aus denen sie die Informationen bezogen hatten, nicht preisgeben. Wir wandten uns an unsere Kontakte im Weißen Haus, doch auch die wollten nicht über vertraulich eingestufte Dokumente reden oder uns gar einen Einblick gewähren. Irgendwann im Laufe des Nachmittags überlegte ich laut vor John und Dominic: »Vielleicht sind wir Teil einer so geheimen Geheimgesellschaft, dass wir nicht einmal wissen, dass wir dazugehören.«

Wir mussten das Erscheinen des Artikels abwarten, bevor wir auch nur den Versuch einer Antwort unternehmen konnten.

Um 15 Uhr Pacific Daylight Time ließ der *Guardian* die Bombe platzen: »PRISM-Programm der NSA greift Nutzerdaten von Apple, Google und anderen ab.«² Nun erfuhren wir, dass PRISM, das Programm für die nationale elektronische Sicherheitsüberwachung, eine Abkürzung für »Planning Tool for Resource Integration, Synchronization, and Management«³ (»Planungswerkzeug für Ressourcenintegration, Synchronisation und Management«) war. Wer hatte sich nur diesen Zungenbrecher ausgedacht? Das klang wie ein schlechter Produktname aus dem Technologiesektor. Laut Medienberichterstattung handelte es sich um ein elektronisches Überwachungsprogramm, mit dem Mobilgeräte, Anrufe, E-Mails, Onlineunterhaltungen, Fotos und Videos nachverfolgt werden konnten.⁴

Binnen Stunden schlugen der Artikel des *Guardian* und ein ähnlicher Bericht der *Washington Post* weltweit hohe Wellen. Unsere Vertriebsleute und unsere Anwälte wurden von Kundenanrufen überschwemmt.

Sie alle stellten dieselbe Frage: Stimmt das?

Anfangs war unklar, woher die Presse ihre Informationen bezogen hatte. Es wurde darüber debattiert, ob diese überhaupt echt sein konnten. Aber drei Tage später ließ die Zeitung eine Bombe platzen, die der ersten Meldung in nichts nachstand. Der *Guardian* gab seinen Informanten preis, nachdem dieser selbst darum gebeten hatte.⁵

Dieser Informant war ein 29 Jahre alter Mitarbeiter des militärischen Dienstleisters Booz Allen Hamilton mit dem Namen Edward Snowden. Er arbeitete als externer Systemadministrator im Threat Operations Center der NSA in Hawaii. Er hatte mehr als eine Million höchst vertraulicher Dokumente heruntergeladen,⁶ bevor er am 20. Mai 2013 ein Flugzeug

nach Hongkong bestieg. Von dort aus setzte er sich mit Journalisten des *Guardian* und der *Washington Post* in Verbindung und begann, der Welt die Geheimnisse der NSA mitzuteilen.⁷

Snowdens Dokumente zogen in jenem Sommer und dem darauf folgenden Herbst eine ganze Reihe Presseberichte nach sich. Das erste öffentlich gemachte Dokument war eine vertrauliche PowerPoint-Präsentation mit 41 Folien, die in der Ausbildung von Geheimdienstmitarbeitern verwendet wurde. Aber das sollte nur der Anfang sein. Reporter melkten Snowdens Beute bis weit ins nächste Jahr hinein und schürten mithilfe einer konstanten Schlagzeilenschwemme die Angst. Eine Flutwelle öffentlichen Misstrauens baute sich auf, während immer mehr Behauptungen aufkamen, die Regierungen der USA und Großbritanniens hätten Zugriff auf Telefonaten und Nutzerdaten, darunter auch Informationen, die ausländischen Staatslenkern und Millionen unschuldiger Amerikaner gehörten.⁸

Die Nachrichten trafen einen Nerv in der Bevölkerung, und das aus gutem Grund. Die Behauptungen stellten den Schutz der Privatsphäre infrage, den demokratische Gesellschaften über zwei Jahrhunderte für selbstverständlich gehalten hatten. Diese Rechte, auf die wir uns heute stützen, wenn wir Ihre Daten in unserem Rechenzentrum in Quincy hüten, erblickten im 18. Jahrhundert während einer hitzigen Kontroverse in Londons Straßen das Licht der Welt. Der Mann, der diesen politischen Feuersturm ausgelöst hatte, war selbst ein Mitglied des Parlaments: John Wilkes.

John Wilkes war wohl der dramatischste – und radikalste – Politiker seiner Zeit. In den Sechzigerjahren des 18. Jahrhunderts forderte er nicht nur den Premierminister, sondern sogar den König mit Worten heraus, die manchem heutigen Politiker die Schamesröte ins Gesicht treiben würden (beinahe jedenfalls). Im April 1763 veröffentlichte Wilkes in einem oppositionellen Journal eine anonyme Kritik. Der Artikel erzürnte den britischen Justizminister Charles Yorke, der Wilkes als Autor im Verdacht hatte. Kurz darauf erließ die Regierung einen Durchsuchungsbefehl, der so breit gefasst war, dass die Ordnungshüter autorisiert wurden, fast jeden Ort zu jeder Zeit zu durchsuchen.

Auf den leisesten Verdacht hin stürmten sie mitten in der Nacht das Haus eines verdächtigen Druckers, »zerrten ihn aus dem Bette von seiner Frau weg, ergriffen all seine persönlichen Unterlagen und nahmen 14 Ge-

sellen und Bedienstete fest.«⁹ Die britischen Behörden durchsuchten kurz darauf vier weitere Häuser und nahmen insgesamt 49 Personen fest, die jedoch allesamt unschuldig waren. Sie traten Türen ein, nahmen Lastkarren auseinander und knackten Hunderte Schlösser.¹⁰ Nach einer Weile hatten sie genug Beweise gesammelt, um den Mann zu schnappen, hinter dem sie eigentlich her waren: John Wilkes wurde in Haft genommen.

Nun war Wilkes nicht der Typ, der sich so etwas einfach gefallen ließ. Innerhalb eines Monats hatte er ein Dutzend Klagen eingereicht und war vor Gericht gezogen, um die Mächtigsten des Landes zur Verantwortung zu ziehen. Das überraschte kaum jemanden, doch der eigentliche Schock für das britische Establishment und vor allem für die Regierung kam erst noch: Die Richter entschieden zu Wilkes Gunsten. Sie verlangten einen schwerwiegenden hinreichenden Verdacht für eine behördliche Untersuchung, die selbst in diesem Fall nur in eingeschränkterem Maße durchzuführen sei. Damit beendeten sie Jahrhunderte willkürlicher Machtausübung des Königs und seiner Gefolgsleute. Die britische Presse begrüßte die Entscheidung und zitierte die berühmte Aussage, dass eines jeden Engländers »Haus sein Schloss sei, das nicht von den boshaft neugierigen Boten des Königs durchsucht werden darf; geschweige denn darf in seinen Papieren herumgeschnüffelt werden.«¹¹

John Wilkes Klageverfahren waren in wichtigen Punkten Geburtshelfer des modernen Rechts auf Privatsphäre. Um diese Rechte wurden die Engländer von den anderen freien Völkern beneidet, darunter auch die britischen Kolonialisten in Nordamerika. Erst zwei Jahre zuvor hatten sie einen ähnlich heiß umkämpften Streit in New England ausgefochten – aber verloren. John Adams, der vehemente Verfechter der Unabhängigkeitserklärung von 1776 und spätere US-Präsident, hatte (noch bevor er Rechtsanwalt wurde) in einem Bostoner Gerichtssaal ein Verfahren verfolgt, das sich in den 1760er-Jahren zu einer bedeutenden Machtprobe zwischen dem britischen Mutterland und den amerikanischen Kolonisten entwickeln sollte. James Otis Jr., einer der feurigsten Anwälte in Massachusetts, hatte dagegen protestiert, dass britische Soldaten Machtbefugnisse ausnutzten, die denen ähnelten, gegen die Wilkes sich gewehrt hatte. Weil die Bostoner Kaufleute Waren importierten, ohne Steuern zu zahlen (denn die empfanden sie als ungerecht), hatten die Briten mit sogenannten Generalvoll-

machten reagiert, die es ihnen erlaubten, ohne konkrete Beweise von Haus zu Haus zu ziehen und nach Beweisen für Zollverstöße zu suchen.¹²

Otis argumentierte, dies sei ein massiver Verstoß gegen die bürgerliche Freiheit und nannte es »den schlimmsten Fall willkürlichen Machtgebrauchs.«¹³ Obwohl Otis seinen Fall verlor, stellten seine Worte den ersten Schritt der Kolonialisten in Richtung Rebellion dar. Gegen Ende seines Lebens sollte sich Adams immer noch an Otis Argumente erinnern und erklären, dass »sie dieser Nation den Odem des Lebens eingehaucht«¹⁴ hätten. Bis zu seinem Todestag sagte er, dass dies der Tag, der Fall, der Gerichtssaal und die Angelegenheit gewesen seien, die die Vereinigten Staaten auf den Weg in Richtung Unabhängigkeit geschickt hätten.¹⁵

Nach der Unabhängigkeitserklärung sollte es noch 13 Jahre dauern, bis das Prinzip, für das sich Otis so leidenschaftlich ausgesprochen hatte, umgesetzt wurde. Inzwischen war die Angelegenheit in New York angekommen, wo 1789 der erste US-Kongress zusammentrat. James Madison stellte vor dem Repräsentantenhaus seine Zusatzartikel zur amerikanischen Verfassung, die »Bill of Rights«, vor.¹⁶ Dazu gehörte auch der spätere Vierte Zusatzartikel (»Fourth Amendment«), der garantierte, dass Amerikaner, beziehungsweise ihre »Person, Wohnung, Papiere und Eigentum« vor »willkürlicher Durchsuchung, Festnahme und Beschlagnahmung« durch die Regierung und ihre Institutionen geschützt seien. Dies schloss die Anwendung von allgemeinen Durchsuchungsbeschlüssen mit ein.¹⁷ Seitdem wird von den Behörden verlangt, einem unabhängigen Richter einen hinreichenden Verdacht vorzulegen, um einen Durchsuchungsbeschluss für eine Wohnstatt oder ein Büro zu erwirken. Das bedeutet letztendlich, dass die Regierung einem Richter beweisen muss, dass es Fakten gibt, die »eine Person mit einem angemessenen Maß an Intelligenz« davon überzeugen, dass ein Verbrechen verübt worden sein könnte.¹⁸

Aber wie weit erstreckt sich dieser Schutz auf Informationen, die Ihr Haus verlassen? Der Vierte Zusatzartikel wurde einer Bewährungsprobe unterzogen, als Benjamin Franklin das Postamt erfand. Man versiegelt einen Briefumschlag und überlässt ihn einer Institution, die Teil der Regierung ist. Der Oberste Gerichtshof hatte im 19. Jahrhundert keinerlei Schwierigkeiten damit, festzustellen, dass der Schutz der Privatsphäre sich auch auf versiegelte Briefe erstreckte: das Briefgeheimnis.¹⁹ Infolgedessen

greift auch hier der Vierte Zusatzartikel. Die Regierung darf einen Umschlag also ohne einen auf einen hinreichenden Verdacht hin ausgestellten Durchsuchungsbeschluss nicht einfach öffnen und hineinschauen, obwohl die staatliche Postagentur aktuell im Besitz dieses Briefes ist.

Im Lauf der Jahrhunderte wogen Gerichte immer wieder ab, ob die Bürger eine »berechtigte Erwartung an die Privatsphäre« hatten, und überlegten, was es bedeutete, wenn man seine Informationen bei jemand anderem lagerte. Einfach ausgedrückt: Wenn es um so etwas wie einen verschlossenen Behälter ging und der Schlüssel anderen nicht zugänglich war, dann, so die Richter, lag eine solche Erwartung vor und der Vierte Zusatzartikel kam zur Anwendung. Bewahrte man seine Dokumente jedoch in einer Kiste voller Akten auf, die neben Kisten anderer Leute an einem Ort lagerten, wo jeder nach Belieben kommen und gehen konnte, brauchte auch die Polizei keinen Durchsuchungsbeschluss. Das lag daran, dass die Gerichte geschlussfolgert hatten, dass man dadurch seine berechtigte Erwartung an den Schutz der Privatsphäre nach dem Vierten Zusatzartikel aufgegeben habe.²⁰

Die Rechenzentren von heute, mit ihren redundanten physischen und digitalen Ebenen, können wohl mit Fug und Recht als verschlossene Lagerbehälter bezeichnet werden.

Im Sommer 2013 wurden wir regelmäßig von verschiedenen Reportern angesprochen, die alle an der Snowden-Story dran waren. Immer wieder gerieten neue vertrauliche Dokumente an die Öffentlichkeit. Es entwickelte sich eine gewisse Routine. Wenn ich Dominic mit John zusammengedrängt in dessen Büro sah, wusste ich, dass bald wieder ein neuer Artikel veröffentlicht werden sollte. »In diesen ersten Wochen führte ich fast täglich dasselbe Gespräch, allerdings mit unterschiedlichen Reportern«, erinnerte sich Dominic. »Die sagten dann immer: >Gut und schön, Dominic, aber einer von euch beiden lügt doch, entweder Microsoft oder Edward Snowden.<<

Die Berichterstattung des *Guardian* über PRISM spiegelte nur einen Teil einer längeren Geschichte über die Anstrengungen der NSA wider, an Daten aus dem privaten Wirtschaftssektor zu kommen. Inzwischen freigegebene Berichte haben ausführlich gezeigt,²¹ dass die Agentur in der Zeit nach dem 11. September 2001 freiwillige Partnerschaften mit der

Privatwirtschaft anstrebte, um den Rechtsweg mit seinen Vorladungsverfahren und Durchsuchungsbeschlüssen zu umgehen und so Nutzerdaten zu sammeln.

Wie jedes andere führende Technologieunternehmen musste auch Microsoft überlegen, ob man den Behörden freiwillig solche Daten zur Verfügung stellen sollte. Bei unseren internen Gesprächen über diese Fragen bezogen wir auch das geopolitische Klima mit ein. Der lange Schatten der Angriffe vom 11. September lag über unserem Land. Gemeinsam mit ihren Verbündeten hatten die USA die »Operation Enduring Freedom« in Afghanistan ausgerufen, der Kongress unterstützte die Invasion im Irak und die verängstigte amerikanische Öffentlichkeit schrie nach weitreichenderen Antiterrormaßnahmen. Es war eine außergewöhnliche Zeit, weshalb viele nach außerordentlichen Maßnahmen verlangten.

Doch die Aufforderung an Unternehmen, freiwillig die Art von Daten preiszugeben, wie sie in den inzwischen freigegebenen Berichten beschrieben werden, barg ein ganz grundlegendes Problem: Diese Daten gehörten nicht den Unternehmen, sondern den Nutzern, den Kunden, und beinhalteten mitunter vertrauliche Informationen.

Wie das PRISM-Programm warfen auch die Anstrengungen der NSA, nach dem 11. September an Kundendaten aus dem privaten Sektor zu kommen, eine Grundsatzfrage auf: Wie können wir gleichzeitig unserer Verantwortung gegenüber unseren Kunden und dem Aufruf zum Schutz des Landes nachkommen?

Für mich ist die Antwort klar. Bei dieser Problematik sollte nach rechtsstaatlichen Prinzipien entschieden werden. Die Vereinigten Staaten sind ein Land, in dem Recht und Gesetz gelten. Wenn die Regierung der USA unsere Kundendaten verlangt, muss sie den Gesetzen unseres Landes entsprechend für deren Erhalt vor Gericht ziehen. Und wenn die Regierungsvertreter der Exekutive der Meinung sind, die Gesetze gingen nicht weit genug, können sie sich an den Kongress wenden und um weitreichendere Vollmachten bitten. So sollte zumindest eine demokratische Republik funktionieren.

Edward Snowden und seine spektakuläre Flucht waren 2002 nicht vorauszusehen, doch wir können einen Blick auf die Geschichte werfen, um etwas allgemeiner vorherzusagen, was die Zukunft wohl bringen wird.

In Zeiten von Staatskrisen wurden individuelle Freiheiten immer wieder zugunsten der nationalen Sicherheit eingeschränkt.

Die erste Staatskrise dieser Art ereignete sich etwas mehr als zehn Jahre nach der Unterzeichnung der amerikanischen Verfassung. Sie trug sich 1798 zu, als es in der Karibik quasi zum Krieg zwischen den USA und Frankreich kam. Die Franzosen, die die USA dazu zwingen wollten, vom inzwischen abgesetzten König gewährte Kredite zurückzuzahlen, beschlagnahmten über 300 amerikanische Handelsschiffe und verlangten ein Lösegeld.²² Einige wütende Amerikaner riefen nach einem offenen Krieg. Andere, wie etwa Präsident John Adams, glaubten jedoch nicht, dass die junge Nation einem Gegner wie Frankreich gewachsen wäre. Weil er befürchtete, die öffentliche Debatte könnte die in den Kinderschuhen steckende Regierung irreparabel beschädigen, versuchte Adams die Unstimmigkeiten beizulegen, indem er vier neue Gesetze unterzeichnete, die als die »Alien and Sedition Acts« bekannt wurden. Diese Gesetze erlaubten der Regierung, »gefährliche« Ausländer zu inhaftieren und auszuweisen, und erklärten Kritik an der Regierung zu einer Straftat.²³

Gute sechzig Jahre später ließen die USA während des amerikanischen Bürgerkriegs erneut einen Schlüsselgrundsatz unserer Demokratie außer Acht, als Präsident Abraham Lincoln mehrfach den »Habeas Corpus Act«, das Recht auf richterliche Haftprüfung, außer Kraft setzte, um Rebellionen vonseiten der Konföderierten zu unterdrücken. Um die Macht der Armee zu stärken, erweiterte Lincoln die Außerkraftsetzung und verweigerte landesweit das Recht auf ein ordnungsgemäßes Gerichtsverfahren. Insgesamt wurden während des Krieges 15 000 Amerikaner gefangen gehalten, ohne dass man sie je einem Richter vorgeführt hätte.²⁴

Kurz nach der Bombardierung von Pearl Harbor unterzeichnete Präsident Franklin D. Roosevelt unter dem Druck des Militärs und der öffentlichen Meinung 1942 eine Verfügung des Präsidenten. Infolge dieser Verfügung wurden 120 000 Amerikaner japanischer Herkunft in entlegene Lager deportiert und von bewaffneten Sicherheitsleuten hinter Stacheldraht gefangen gehalten. Zwei Drittel der Internierten waren in den USA geboren. Als die Verfügung drei Jahre später aufgehoben wurde, hatten die meisten ihre Häuser, Höfe, Geschäfte und den Rückhalt in ihrem sozialen Umfeld verloren.²⁵