Unverkäufliche Leseprobe

S. FISCHER

BARTON GELLMAN

DER DUNKLE SPIEGEL

Edward Snowden und die globale Überwachungsindustrie

Aus dem Englischen
von Martina Wiese

S. FISCHER

Aus Verantwortung für die Umwelt hat sich der S. Fischer Verlag zu einer nachhaltigen Buchproduktion verpflichtet. Der bewusste Umgang mit unseren Ressourcen, der Schutz unseres Klimas und der Natur gehören zu unseren obersten Unternehmenszielen.

Gemeinsam mit unseren Partnern und Lieferanten setzen wir uns für eine klimaneutrale Buchproduktion ein, die den Erwerb von Klimazertifikaten zur Kompensation des CO_2-Ausstoßes einschließt.

Weitere Informationen finden Sie unter: www.klimaneutralerverlag.de

Deutsche Erstausgabe
Erschienen bei S. FISCHER
Die amerikanische Originalausgabe erschien 2020
unter dem Titel »Dark Mirror: Edward Snowden
and the Surveillance State« im Verlag Penguin Press

Satz: Dörlemann Satz, Lemförde
Druck und Bindung: CPI books GmbH, Leck
Printed in Germany
ISBN 978-3-10-397046-3

1
PANDORA

Während ich schlief, traf eine Nachricht auf meiner Mailbox ein. Viele Stunden verstrichen, bis ich sie entdeckte. Vermutlich hätte ich mich von ihr fernhalten sollen, aber die Macht der Gewohnheit war stärker. Letzte Nacht hatten wir keine Verbindung zueinander aufgenommen. Nicht weil wir wussten, dass uns jemand auf die Schliche gekommen war, sondern weil wir genau das nicht wissen konnten. Unsere E-Mail-Accounts waren anonym, verschlüsselt, von unserem Internetalltag isoliert. Ich konnte bestenfalls sagen, dass sie sich nicht dichter abschotten ließen. Dieser Gedanke hatte mich früher einmal beruhigt.

Der Monat Mai des Jahres 2013 neigte sich langsam seinem Ende entgegen. Fast vier Monate waren vergangen, seit Laura Poitras, eine unabhängige Filmemacherin, mich in Bezug auf eine vertrauliche Quelle um Rat gebeten hatte. Verax – unter diesem Namen lernte ich den Informanten später kennen – hatte ihr einen rätselhaften Hinweis auf die Überwachung durch den amerikanischen Staat übermittelt.[1] Poitras und ich taten uns zusammen, um herauszufinden, was es damit auf sich hatte. Am letzten Abend waren Monate gespannter Erwartung zu Ende gegangen. Verax hatte geliefert. Die Beweise lagen auf dem Tisch. Seine Geschichte war echt, die Risiken keine bloße Mutmaßung mehr. Das FBI und die »Q Group« der NSA, die für die innere Sicherheit verantwortlich ist, würden diesem Leck garantiert ihre geballte Aufmerksamkeit schenken.[2] Zum ersten Mal in meiner Laufbahn hielt ich es nicht für undenkbar, dass die US-Behörden versuchen würden, an meine Notizen und Dateien zu gelangen. Ohne jeden Zweifel würden ausländische Geheimdienste Interesse an uns finden.

Poitras und ich beschlossen, uns in zwei Tagen wieder zu treffen.

Alles andere musste erst einmal warten. Noch in der Nacht wurde dieser Plan von der Realität eingeholt. Am nächsten Morgen loggte ich mich ein. Ich erwartete nichts Besonderes. Laut dem Zeitstempel hatte Poitras weniger als vier Stunden nach unserem Treffen eine Nachricht abgesetzt. Sie konnte nicht viel geschlafen haben. Das hatte ich auch nicht, aber meine Müdigkeit verflog, als ich die Betreffzeile las. Es war unser privates Erkennungszeichen für »dringend«. Die entschlüsselte Botschaft war kurz und bündig.

```
Ich muss Ihnen unbedingt etwas zeigen.
Das werden Sie sehen wollen.
```

Merkwürdig. Sehr merkwürdig. Etwas ansehen? Nach dem, was wir letzten Abend gesehen hatten? Verax hatte uns eine mehrteilige Top-Secret-Präsentation der National Security Agency geschickt; ihr jüngstes Update war einen Monat alt.[3] Nach Mitternacht hatten Poitras und ich über einen kleinen Laptop-Bildschirm gebeugt dagestanden und versucht, uns einen Reim auf die Fachbegriffe zu machen. Die zentralen Punkte waren allerdings klar. Unter dem Decknamen PRISM[4] schöpfte die NSA Daten von Zehntausenden Accounts unter anderem bei Yahoo, Google, Microsoft und Facebook ab.[5] Mit 41 Folien und 8000 Wörter umfassenden Anmerkungen wurden der rechtliche Rahmen und operative Details erläutert. Wenn diese Präsentation authentisch war – und danach sah es definitiv aus –, war sie eine ausgesprochene Rarität: die so gut wie aktuelle amtliche Darstellung von Geheimdienstoperationen auf US-amerikanischem Boden, die die öffentlich beteuerten Grenzen weit überschritt.

Beim Abschied sagte Poitras, sie verstehe vielleicht 10 Prozent von all dem. Ich konnte mir höchstens auf die Hälfte einen Reim machen. Doch darüber mussten wir uns nicht grämen. Journalisten müssen nicht sofort alle Antworten parat haben. Unsere Aufgabe war es, die Antworten zu finden, die Belege zu prüfen und weitere aufzuspüren. Aus all dem eine Story zu machen würde Zeit erfordern, aber den Grundstein hatten wir schon.

So hatte ich zumindest gedacht. Doch nun hatte etwas Poitras aufgeschreckt – so sehr, dass sie unsere Mail-Regeln gebrochen hatte. Herumrätseln nutzte nichts. Zwischen den Zeilen konnte ich nichts Aufschlussreiches entdecken. Gute oder schlechte Nachrichten waren gleichermaßen denkbar, doch in diesem Stadium war jede Überraschung beunruhigend. Eine Überraschung bedeutete, dass ich nicht wusste, wo wir standen. Wochenlang hatte ich alle Eventualitäten durchgespielt und die wahrscheinlichen Wege und Hemmnisse in der nächsten Phase der Berichterstattung überdacht. Ich musste weitere Quellen finden, mit ihnen Kontakt aufnehmen, ohne sie in Gefahr zu bringen, das Dokument authentifizieren und nach Zusammenhängen suchen. Es gab jede Menge Chancen, die Sache zu vermasseln – wir konnten Verax auffliegen lassen, auf einen Betrüger reinfallen, den Text falsch interpretieren, etwas enthüllen, das versehentlich Schaden anrichtete. Falls mein Strategieplan Fehler aufwies, würde ich möglicherweise nahende Gefahren übersehen.

Nun war keine Zeit mehr zum Planen. Verax hatte den Startschuss abgefeuert. Wir hatten das Dokument in Händen und kein festes Publikationsdatum. Das Zwischenspiel barg Risiken. Verax verriet uns nicht, wo er sich aufhielt, aber wir wussten, dass er nicht mehr zur Arbeit ging. Sobald sein Arbeitnehmer nach ihm suchen würde, wäre er nicht mehr sicher. Die Behörden würden entdecken, was er entwendet hatte, und vielleicht versuchen, unserer Story zuvorzukommen. Zweifellos würde sich das Zeitfenster für ungehindertes Arbeiten dann schließen.

Wir versuchten, dem Blick eines Überwachungsriesen zu entgehen, während wir durch seine Tore spähten. Wir konnten nicht darauf hoffen, lange unentdeckt zu bleiben, aber wir kämpften um jede Minute. Die dringende E-Mail von Poitras hatte von Tribeca bis Upper Manhattan nur knapp 10 Kilometer Luftlinie zu überwinden,[6] aber sie sandte sie über anonyme Zwischenstationen um die ganze Welt, um ihren Aufenthaltsort mit Tausenden Kilometern Umweg zu verschleiern.[7] Als ich mich einloggte, tat ich das Gleiche. Wir hatten billige Laptops bar gekauft und nutzten Datenschutz-Tools, um ihre Hardware und

Netzwerkadressen zu spoofen.[8] Poitras, Verax und ich verschlüsselten jedes Wort. Wir benutzten nie ein Telefon. Jeder Kontakt hinterließ eine Spur – das ließ sich nicht vermeiden –, doch wir sorgten für falsche Fußabdrücke.

Bevor ich mich auf den Weg nach Downtown machen konnte, trudelte eine weitere E-Mail ein. Die gleiche harmlos aussehende Betreffzeile, die »dringend« signalisierte. Der Chiffretext ihrer verschlüsselten Botschaft sah folgendermaßen aus:[9]

```
-----BEGIN PGP MESSAGE-----
hQIOA7RnVIVebwveEAgA7OBO1qtnQ1mdDTZwU4eI1ZbfF57dLNI
bOUxeunqK8q9Zoo9aOiHGjVreqoOYKip/1pX7rohHmA/TO38jjgns
F9E6hNahg1ZWcBRabfOxGUxu8Gzxk5H9m+kOdHCqg6jG2p/seNFNCR36v
jgCy2BuF47JcOoKgc[…]
-----END PGP MESSAGE-----
```

Ich schloss einen USB-Stick an den Computer an. Darauf befand sich mein privater Schlüssel, eine kleine digitale Datei, um ihre Nachricht entschlüsseln zu können. Ich tippte zwei Passphrasen ein – eine, um den USB-Stick in Betrieb zu nehmen, und eine weitere, um den Schlüssel verwenden zu können. Die neue entschlüsselte Nachricht von Poitras war nur wenige Wörter lang.

```
Machen Sie sich auf etwas gefasst. Jesus.
```

Was zur *Hölle* ging hier vor? Ich sagte einen Flug nach Washington ab, hetzte zur U-Bahn und im Laufschritt die Treppe hinunter. Kaum in der Bahn Richtung Downtown, zog ich die Batterie aus meinem Handy. Ein Smartphone ist ein vorzüglicher Spurenleger. Außerdem eignet es sich hervorragend als ferngesteuertes Mikrophon, wenn jemand weiß, wie es einzuschalten ist.

Als ich Laura Poitras drei Tage vor Weihnachten 2010 zum ersten Mal begegnete, tauchte sie unangemeldet in meinem Büro ganz in der

Nähe vom Washington Square auf. Karen Greenberg, eine gemeinsame Freundin, die an der juristischen Fakultät der New York University einen lebhaften politischen Salon organisierte, lag uns schon lange damit in den Ohren, dass wir uns einmal treffen sollten. Als ich die *Washington Post* verließ, hatte mir Greenberg eine Fellowship angeboten. In meinem neuen Büro empfing mich ein Kaffeebecher, den mir der frühere und künftige Pentagon-Beamte Michael Sheehan hinterlassen hatte. Darauf prangte ein lächelnder Soldat aus dem Zweiten Weltkrieg mit kantigem Kinn und einem Kaffee in der Hand. »Wie wär's mit 'ner ordentlichen Ladung Schnauze halten?«, sagte der GI. Geheimhaltungskultur anno 1944, stets brandaktuell.

Ich dachte nicht daran, Poitras zu fragen, wie sie in mein Büro gelangt war, ohne dass ein Anruf vom Sicherheitspersonal oder von der übereifrigen Vorzimmerdame ein Stockwerk höher mich gewarnt hatte. An jenem Abend ließ sie mich wissen, dass ich eine ziemliche Szene verpasst hatte. »Ich hab ein schlechtes Gewissen, weil ich Karens Leute ein wenig zusammenfalten musste, um zu Ihnen durchzukommen«, schrieb sie mir.[10]

Nicht weiter überraschend, wenn man ihren Presseausschnitten Glauben schenken durfte. Mit ihren 46 Jahren war sie eine für den Oscar nominierte und mit dem Peabody-Award ausgezeichnete Naturgewalt, die gerne mal eine Kamera schulterte und damit ohne Crew durch ein Kriegsgebiet zog. Politik mit Hang zum Radikalen.[11] Sie wurde als »intensiv« und »erbarmungslos« beschrieben. Aufgewachsen in der Nähe von Boston, absolvierte sie eine Ausbildung zur Chefköchin und wandte sich dann der Filmerei zu.[12] Ihren Durchbruch erzielte sie mit *My Country, My Country* (dt. *Irak – Mein fremdes Land*);[13] der Film spürte dem gescheiterten Versuch nach, im Irak unter US-Besatzung eine Demokratie zu errichten.[14] Auf PBS war gerade ihr neuestes Werk *The Oath* gelaufen, das abwechselnd die Geschichte von Osama bin Ladens früherem Bodyguard, mittlerweile Taxifahrer im Jemen, und seinem Schwager, einem Häftling im Gefangenenlager in Guantánamo, erzählte.[15]

Die Schockwellen nach dem Irak-Film brachten sie zu mir. Nach

der Erstausstrahlung im Jahr 2006 hatte man sie vier Jahre lang jedes Mal, wenn sie eine amerikanische Grenze überquerte, verhört und durchsucht.[16] Meistens hielten Beamte der Customs and Border Patrol sie ohne Angabe von Gründen stundenlang fest.[17] Sie blätterten durch ihre Notebooks, kopierten Videomaterial aus ihren Speicherkarten und manchmal nahmen sie ihre elektronischen Geräte »in Verwahrung« (so der juristische Euphemismus). Wie Poitras später erzählte, hatten sie am John F. Kennedy Airport in New York in jenem Sommer »Laptop, Videokamera, Filmmaterial und Handy konfisziert« und sie 41 Tage lang festgehalten.[18] Sie gaben zu, mindestens einmal eine vollständige forensische Aufnahme ihres Laptops angefertigt zu haben, eine Kopie aus vielen Einzelteilen, die sie für alle Zeit behalten und unter anderem dazu verwenden konnten, gelöschte Dateien wiederherzustellen.

Ich fand all das erschreckend – angefangen damit, dass die US-Regierung so tat, als seien Computer und Handys simple »Behälter«, genau wie eine Handtasche oder Reisetasche.[19] Nach dieser grotesken Logik war das Beschlagnahmen, Kopieren und Einbehalten von Hunderttausenden persönlichen und professionellen Dateien kein schwerwiegenderer Eingriff als das Durchsuchen eines Koffers nach unverzollten Whiskyflaschen. Es war seit langem gängige Praxis, dass die Forderung des 4. Zusatzartikels zur Verfassung nach einem begründeten Verdacht nicht für Durchsuchungen beim Grenzübertritt galt, wo die Behörden Spielraum brauchten, um Bedrohungen der Sicherheit abzuwehren und die Zollgesetze durchzusetzen. Nun machte die Regierung einen weiter gefassten Anspruch geltend, der den gesunden Menschenverstand und das grundlegende Recht eines Bürgers, unbehelligt zu bleiben, sehr viel aggressiver herausforderte.[20] Wie die Regierung argumentierte, gab es so etwas wie eine »unbegründete« Durchsuchung an der Grenze überhaupt nicht, weil Zollbeamte frei darüber bestimmen dürften, was sie inspizieren und beschlagnahmen würden. Dafür bräuchten sie überhaupt keine Begründung. König Georg hätte dem in allen Punkten sicher zugestimmt. Die Bundesrichter hatten gerade erst begonnen, es in Frage zu stellen.[21]

Poitras hatte gehört, dass ich bei meinen alten Reporterkollegen als exzentrisch galt, was Datenschutz betraf – ich war der Typ, der seine Notizen verschlüsselte und befremdliche Accounts anlegte. Vermutlich trug ich eine Nachtmütze aus Alufolie, um feindliche Funkstrahlen abzuwehren. Für mich lag die Notwendigkeit von Vorsichtsmaßnahmen auf der Hand. Genau wie alle anderen hatten Journalisten die Gaben des Internets freudig angenommen, ohne über ihren Preis nachzudenken. Handys, Browsen im Netz, E-Mails und SMS hinterließen lange Datenspuren – sie verrieten, mit wem wir wann redeten, wo wir uns trafen und worüber wir uns unterhielten. Neue Gesetze und Technologien gewährten dem Staat einen leichteren und weniger kontrollierten Zugang zu dieser Datenfundgrube. Große Privatunternehmer installierten vergleichbare Tools auf Unternehmensebene, um ihren Arbeitnehmern nach Belieben über die Schulter blicken zu können. Einige Personen im Fokus von Investigativjournalisten versuchten, Datenlecks zu stopfen, indem sie Privatdetektive damit beauftragten, die Aufzeichnungen unserer Kommunikation an sich zu bringen.[22] Wir Journalisten gelobten zwar, unsere vertraulichen Quellen nicht preiszugeben, erlaubten unseren Gegnern jedoch, sie aus unseren digitalen Spuren herauszulesen.[23] Seit Jahren hatte ich meine Notizen nicht mehr so aufbewahrt, dass irgendwer, auch Vorgesetzte, denen ich vertraute, sie lesen konnten. Die »Cloud«, so drückte es der Sicherheitsanalyst Graham Cluley aus, sei nur ein anderes Wort für »den Computer von jemand anderem«.[24] Wenn man dort Informationen hinterlegte, verlor man die Kontrolle darüber.

Poitras wollte wissen, wie sie sich schützen könne. Normalerweise würde ich zu Beginn eines solchen Gespräches erst einmal fragen, was sie schützen wolle und wer ihrer Meinung nach gern Zugriff darauf hätte. Poitras wusste bereits, dass sie einen Gegner von Weltrang hatte. Das war nicht unbedingt beruhigend, doch selbst die US-Regierung musste sich ihre Zeit, Geldreserven und knappen technischen Ressourcen einteilen. Sie konnte nicht alle Hebel in Bewegung setzen, um jemanden auf einer Watchlist unter Beobachtung zu halten. Bislang war Poitras ein kostengünstiges Ziel gewesen, da sie nur nackte Daten

beförderte. Mit Dateiverschlüsselungen konnte sie ihren Preis erheblich in die Höhe treiben. Kurze Zwischenfrage: Was war mit dem Laptop, den sie kopiert hatten? Hatte sie die Passwörter für ihre E-Mails und Accounts geändert? Ja, hatte sie.

In jener Nacht sandte ich ihr eine vorgeblich »kurze Notiz für weitere Lektüre«. In Wahrheit ließ ich alle Zurückhaltung fahren. Meine 1000-Wörter-Mail strotzte vor Links und Rezepten für eine Buchstabensuppe aus Software-Tools: GPG, TrueCrypt, OTR, SOCKS-Proxys, Tor.[25] In der Rückschau ist verständlich, warum mich meine Kollegen selten um diese Art von Ratschlägen baten.

Viele Techniken, die ich Poitras empfahl, stammten von den Cypherpunks der 1990er Jahre, einer libertär eingestellten (und daher führerlosen) Gemeinschaft von Visionären und Technologen.[26] Als das Internet noch in den Kinderschuhen steckte, machten es sich die Cypherpunks zur Aufgabe, es vor Zensur, Überwachung und anderen Formen unerwünschter staatlicher Kontrolle zu schützen. Einer von ihnen, John Perry Barlow, ehemaliger Songtexter von The Grateful Dead und Mitbegründer der Electronic Frontier Foundation, verfasste eine Unabhängigkeitserklärung, in der er Regierungen allgemein (»ihr müden Riesen aus Fleisch und Stahl«) davor warnte, sie seien »nicht willkommen unter uns«. In *A Cypherpunk's Manifesto* verkündete Eric Hughes einen Aktionsplan: »Wir wissen, dass jemand Software schreiben muss, um die Privatsphäre zu schützen, und da wir uns unsere Privatsphäre nur sichern können, wenn dies alle tun, werden wir sie schreiben.«

Und das taten sie. Sie schrieben die Software und die Software funktionierte und sie stellten sie allen kostenlos zur Verfügung. Selbst das US Naval Research Laboratory, das »Onion Routing« erfand, um anonyme Online-Kommunikation zu ermöglichen, veröffentlichte die Software und den zugrunde liegenden Code zur freien öffentlichen Nutzung.[27] »Der Schutz der Privatsphäre bedeutet nicht nur das Verbergen von Nachrichteninhalten, sondern auch zu verbergen, wer mit wem spricht«, schrieben die Autoren des wegweisenden Fachartikels.

Mit Hilfe solcher Tools, verpackt in die elegante Mathematik der

Kryptographie, konnte jeder ohne Zensur oder Angst lesen und schreiben und sich im Internet verabreden. Jeder konnte es und kaum einer tat es. Die Muggel hielten sich vom Hexenwerk der Zauberer fern. Kaum jemand erfuhr, dass es solche geheimen Tricks gab, und noch weniger hatten Lust oder die Geduld, sie sich anzueignen. Mit einem gewissen streberhaften Vergnügen machte ich mir die Mühe; zudem war ich als Journalist, der über Geheimdiplomatie, Geheimdienste und Krieg berichtete, besonders motiviert. 2006 verwendete ich erstmals GPG, den Goldstandard der E-Mail- und Dateiverschlüsselung[28] – nicht lange nachdem sich das Magazin *Time* über die Einwände eines Reporters hinweggesetzt und seine Notizen an Staatsanwälte in der Strafsache gegen den Stabschef von Vizepräsident Dick Cheney weitergegeben hatte.[29] Für mich war Werner Koch, der die Software geschrieben hat und sie nach wie vor betreut, einer der Helden der Zivilgesellschaft.

Dennoch musste man leider sagen: Die Bedienung von GPG war so kompliziert, dass selbst Experten an seinem epischen Benutzerhandbuch scheiterten.[30] Die Anleitung übertrumpfte Robert Louis Stevensons *Dr. Jekyll and Mr. Hyde* um 2000 Wörter.[31] Damit war eigentlich schon alles gesagt, aber einen besseren Rat konnte ich Poitras nicht geben. Mein bester Tipp für sie war vielleicht: »Sie sollten sich wohl einen erfahreneren Berater suchen.«[32] Ich sollte noch erwähnen, dass es heute leichter zu bedienende Tools gibt, auch wenn sie immer noch zu kompliziert sind. Auf gellman.us/pgp finden Sie eine fortlaufend aktualisierte Liste.

Unsere Zusammenarbeit an der NSA-Story begann zwei Jahre später, am 31. Januar 2013, als Poitras mir schrieb, sie sei gerade in New York.

»Haben Sie in den nächsten Tagen Zeit für einen Kaffee?«, fragte sie. »Ich könnte einen Rat gebrauchen.«[33] Die Einladung war nicht so spontan, wie sie aussah. Es folgte eine verschlüsselte Notiz, in der ich gebeten wurde, mein Handy nicht mitzunehmen. Zwei Tage später im Joe, der Espressobar im Taschenformat, die ich ausgesucht hatte, verzog sie das Gesicht, als sie die eng beieinander stehenden Tische sah, und meinte, wir sollten lieber woanders hingehen. Nach zwei weiteren

Anläufen fanden wir schließlich ein Lokal, das ihr diskret genug war. Nun hatte sie meine ungeteilte Aufmerksamkeit.

Poitras machte ein wenig Smalltalk, bis die Bedienung uns Essen und Getränke brachte. Aus reiner Gewohnheit zog ich mein Notizbuch hervor. Sie schüttelte den Kopf, und ich steckte es wieder ein. Ein namenloser Informant habe sich an sie gewandt, erzählte sie, der sich als Angehöriger der Intelligence Community der USA ausgab. Damals verriet sie es noch nicht, aber ihre Kommunikation hatte fünf Tage zuvor begonnen.[34] Laut dem anonymen Informanten hatte die NSA einen derart umfassenden und leistungsfähigen Überwachungsapparat errichtet, dass die amerikanische Demokratie in Gefahr war. Das konnte er auch beweisen, aber noch nicht sofort.

Das klang fürs Erste nicht sehr vielversprechend. Ich glaube, es gelang mir, ein Pokerface aufzusetzen, doch aus Erfahrung wusste ich, dass kaum etwas einen solchen Reiz auf wahnhafte Informanten ausübte wie eine Story über den Geheimdienst. Nachdem es in meinem letzten Buch um Inlandsüberwachung ohne richterlichen Beschluss gegangen war, war ich von Briefen in krakeliger Schrift und Sprachnachrichten überschwemmt worden, bis meine Warteschlange aus allen Nähten platzte.[35] Poitras' Quelle klang zwar nicht wie ein Spinner, aber es gibt auch Hinweise auf eine Story, die Reporter gemeinhin unter »wichtig, falls wahr« ablegen. Der Tipp klang glaubwürdig, lohnenswert, wenn er echt war, aber die Story war für uns einfach außer Reichweite. Ich konnte mir durchaus vorstellen, wie sich ihre Glaubwürdigkeit nachweisen ließe, aber dazu brauchte man schon eine Zwangsvorladung oder, nun ja, eine Wanze. Diese Dateien konnten Gold wert sein, aber ihre Echtheit zu prüfen würde womöglich ein Leben lang dauern.

[…]