Überwachtes Netz

Arbeitstitel: »Reflexionen nach Snowden«

Hrsg. Markus Beckedahl, Andre Meister

Überwachtes Netz

Edward Snowden und der größte Überwachungsskandal der Geschichte

Überwachte Welt – Edward Snowden und der größte Überwachungsskandal der Geschichte
1. Auflage, 1.000 Stk., November 2013

Herausgeber:	Markus Beckedahl, Andre Meister
Redaktion:	Jan-Peter Kleinhans, Anna Biselli, Kilian Froitzhuber, Nicolas Fennen, Andrea, Markus Beckedahl, Andre Meister, Matthias »wetterfrosch« Mehldau
Titelbild:	Laura Poitras / Praxis Films; CC BY 3.0, Komplette Lizenz: https://creativecommons.org/licenses/by/3.0/ Montage: Jan-Peter Kleinhans, »wetterfrosch«
Satz:	»wetterfrosch«
Verlag:	newthinking communications, Berlin, in Kooperation mit epubli GmbH, Berlin
ISBN:	978-3-944622-02-6
URL:	http://netzpolitik.org/ueberwachtes-netz/

Inhaltsverzeichnis

Dank

Als erstes möchten wir uns bei Edward Snowden bedanken. Er riskiert sein Leben, um mit Mut und Zivilcourage den größten Überwachungsskandal in der Geschichte der Menschheit aufzudecken. Ebenfalls möchten wir uns bei seinen journalistischen Partnern wie Glenn Greenwald und Laura Poitras und allen anderen bedanken, die mithelfen, diesen Skandal zu dokumentieren und an die Öffentlichkeit zu bringen.

Dieses Buch wäre nicht ohne die Mithilfe zahlreicher Menschen möglich geworden. Wir möchten allen Autorinnen und Autoren dafür danken, uns bereits veröffentlichte Texte geschenkt oder sogar extra für dieses Buch geschrieben zu haben. Wir waren angenehm überrascht, dass wir so viel positives Feedback auf das Projekt erhalten haben.

Die Realisierung wäre nicht ohne ein großes Team im Hintergrund möglich gewesen. Wir möchten uns bei Jan-Peter Kleinhans für viel Unterstützung bei der Koordinierung, Übersetzung und Lektorat sowie Matthias »wetterfrosch« Mehldau für alle Fragen rund um das Design und Layout bedanken.

Zahlreiche Texte mussten vom Englischen übersetzt, andere Texte redigiert werden. Das verdanken wir vor allem Anna Biselli, Kilian Froitzhuber, Nicolas Fennen, Andrea, Caroline Kleine (Lesart), Eva und Jens. Wir danken auch allen Kommentatoren, die uns Vorschläge für einen Titel gemacht haben.

Und ohne das Team von newthinking wäre es uns auch nicht möglich gewesen, so viel Zeit in das Projekt zu stecken. Das Zusammenstellen dieses Buches war auch ein Experiment, wie man selbst ein Buch verlegen kann und ob man trotz des zeitgleichen Verschenken überhaupt Geld verdienen kann. Zuerst sollte das Buch nur digital erscheinen. Wir freuen uns, mit epubli einen Partner gefunden zu haben, , der uns ermöglicht, das Buch nach eigenen Vorstellungen und mit großer Gewinnbeteiligung zu drucken. Auch in digitalen Zeiten freuen wir uns darauf, die Arbeit von Monaten gedruckt in Händen halten zu können.

Auch wenn wir daran kein Geld verdienen sollten, um unsere Redaktion zu refinanzieren, hat sich die Erfahrung bereits ausgezahlt. Vor allem war unsere größte Motivation, die Debatte um diesen größten Überwachungsskandal der Menschheit um Analysen und Reflexionen zu erweitern und vor allem konkrete Schritte in die Debatte zu bringen, wie wir Geheimdienste besser kontrollieren und unsere Privatsphäre sowie ein offenes Netz zurück erobern können.

Zum Schluß ein großer Dank an Alle, die sich für den Erhalt und Ausbau von Grundrechten sowie die ausufernde Überwachung engagieren und/oder dagegen anschreiben. Mit diesem Buch wollen wir auch dazu motivieren, einen langen Atem zu haben, um gemeinsam die Welt verändern zu können und unsere Freiheit zu erhalten. Es ist unser Netz und unsere Freiheit.

Dieses Buch erscheint unter einer freien Lizenz und kann gerne weiterkopiert werden. Wir freuen uns immer über finanzielle Unterstützung, um weiterhin unabhängig Projekte wie netzpolitik.org oder dieses Buch auf die Beine zu stellen und über Grundrechte in der digitalen Gesellschaft aufklären zu können. Unser gemeinnütziger Verein netzpolitik.org e.V. nimmt gerne Spenden entgegen:

Inhaber:	netzpolitik.org e. V. (gemeinnützig)
Konto:	1149278400
BLZ:	43060967 (GLS Bank)
IBAN:	DE62430609671149278400
BIC:	GENODEM1GLS
Zweck:	Spende netzpolitik.org

Vorwort

> *»Ich möchte nicht in einer Welt leben, in der alles, was ich sage, alles, was ich tue, aufgezeichnet wird. Das ist nichts, was ich bereit bin zu unterstützen. Das ist nichts, unter dem ich zu leben bereit bin.«*
>
> *– Edward Snowden im Interview mit dem Guardian, 10. Juni 2013*

Edward Snowden hat die größte Überwachungsmaschinerie der Menschheitsgeschichte enthüllt. Und täglich kommen neue Puzzlestücke ans Licht. Die Geheimdienste der westlichen Welt, allen voran die amerikanische NSA und das britische GCHQ, »versuchen sämtliche Formen der menschlichen Kommunikation zu sammeln, zu überwachen und zu speichern«, so der investigative Journalist Glenn Greenwald. Full Take.

Dabei geht es nicht um Terrorismus, womit dieser Überwachungs-Koloss in der Öffentlichkeit immer wieder gerechtfertigt wird. Die Dienste geben ganz offiziell selbst zu, dass die damit klassische Spionage betreiben – für Politik und Wirtschaft. Anders sind Wanzen in EU-Einrichtungen, das abgehörte Merkel-Telefon und gehackte Firmen-Netze auch nicht zu erklären. Schließlich nutzen die mächtigen, intransparenten und demokratisch nicht kontrollierbaren Geheimdienste ihren Datenschatz auch zum Erhalt der eigenen Macht. Der »Staat im Staat« existiert nicht nur in der Türkei, die Dienste führen ein Eigenleben.

Dabei kann eine Demokratie ohne Privatsphäre nicht funktionieren. Menschen brauchen einen »Kernbereich privater Lebensführung« zum Rückzug, zur Entwicklung und zur Reflexion. Stattdessen gibt es keine unbeobachtete Kommunikation mehr. Durch die Digitalisierung wird jede kleine Handlung von Computern verarbeitet – und damit von den Geheimdiensten abgeschnorchelt: Einkäufe, Reisen, Zahlungen, bald auch Zähneputzen und Autofahren. Und natürlich sämtliche Kommunikation und Interaktion. Das bedroht die Demokratie im Kern.

Vor zehn Jahren wurde netzpolitik.org gestartet, unter anderem als Reaktion auf den Geheimdienst-Skandal der damaligen Zeit: das weltweite Spionagenetz Echelon. Alle unsere Befürchtungen wurden 2001 ganz offiziell vom Europaparlament bestätigt. Das war zwei Monate vor 9-11. Heute ist Echelon »ein Kinderspiel im Vergleich zur aktuellen Überwachung«.

Wir wollen das nicht akzeptieren. Wir wollen den Kopf nicht in den Sand stecken und akzeptieren, dass wir mit dieser Überwachung leben müssen. Wie es unsere Regierungen wollen. Wir wollen unser Verhalten nicht umstellen, um damit umzugehen. Wir müssen die Überwachungsmaschinerie zurückdrängen und sehen Ansatzpunkte in einer Kombination aus technischen und politischen Mitteln.

Wir wissen, dass es vielen so geht. Wir haben in den vergangenen Monaten eine Vielzahl an Autorinnen und Autoren eingeladen, ihre Sicht auf die durch Edward Snowden ausgelösten Entwicklungen zu reflektieren und zu überlegen, welche Schlüsse aus den enthüllten Fakten zu ziehen sind.

Die Debatte darum darf nicht verstummen. Auf dem Spiel stehen Freiheit und Demokratie. Deswegen gibt es dieses Buch.

– Markus Beckedahl und Andre Meister

»Die gute Nachricht ist: Wir sind nicht paranoid.
Die schlechte Nachricht ist: Wir werden alle überwacht.
Jederzeit und überall.«

Politische und gesellschaftliche Auswirkungen

Snowdens Rede zum Whistleblower-Award

Edward J. Snowden

Auf der Verleihung des Whistleblower-Awards am 30.08.2013 in Berlin, hielt Jacob Appelbaum stellvertretend für den leider abwesenden Edward Snowden eine Dankesrede[1]*. Mit freundlicher Unterstützung von Jacob Appelbaum können wir die Dankesrede von Edward Snowden abdrucken.*

Es ist eine große Ehre, dass mein Whistleblowing als Beitrag zum Allgemeinwohl wahrgenommen wird. Doch die größere Anerkennung und Aufmerksamkeit gebührt jenen Einzelpersonen und Organisationen in unzähligen Ländern auf der ganzen Welt, die sprachliche und geografische Grenzen gesprengt haben, um gemeinsam das öffentliche Recht auf Information und den Wert der Privatsphäre zu verteidigen.

Es bin nicht nur ich, sondern die Allgemeinheit, die von dieser mächtigen Wandlung hin zu der Abschaffung unserer Grundrechte betroffen ist. Es bin nicht nur ich, sondern Zeitungen aus aller Welt, die Gründe haben, unsere Regierungen dafür verantwortlich zu machen, wenn mächtige öffentliche Vertreter versuchen, solche Themen durch Gerüchte und Anschuldigungen kleinzureden. Und es bin nicht nur ich, sondern ganz gewiss auch mutige Regierungsvertreter in der ganzen Welt, die neue Schutzmaßnahmen und Limitierungen vorschlagen, um zukünftige Angriffe auf unser aller Rechte und unser Privatleben zu verhindern.

Ich danke all jenen, die sich an ihre Freunde und Familien gewandt haben, um ihnen zu erklären, warum sie anlasslose Überwachung etwas angeht. Sie trifft den Mann, der an einem heißen Tag eine Sturmmaske trägt, sie trifft die Frau mit einem Schild und einem Schirm im Regen, sie trifft den jungen Studenten, auf dessen Laptop sich Sticker zu Freiheitsrechten befinden und den Gymnasiasten, der sich in der letzten Reihe des Klassenraums Internet-Memes ausdenkt.

1 *Original-Rede; The WikiLeaks Supporters Forum; http://www.wikileaks-forum.com/news-and-supporters/335/snowden-wins-whistleblower-award-in-germany/22431/*

All diese Menschen verstehen, dass eine Veränderung mit einer einzelnen Äußerung beginnt und sie haben der Welt eine Botschaft überbracht. Regierungen müssen sich uns gegenüber für ihre Entscheidungen rechtfertigen – denn es sind Entscheidungen über die Welt, in der wir alle leben. Die Entscheidungen über Rechte und Freiheiten von Menschen sind Sache der Allgemeinheit und dürfen nicht der Geheimhaltung durch Regierungen unterliegen.

Diese Freude wird für mich jedoch von dem Bewusstsein überschattet, was uns heute hier zusammengebracht hat. Im Amerika der heutigen Zeit hat die Kombination aus schwachem Rechtsschutz von Whistleblowern, schlechten Gesetzen zur Verteidigung öffentlicher Interessen und zweifelhafter Immunität derjenigen, die sich abseits von Gesetzen bewegt haben, zur Pervertierung des Systems aus Anreizen geführt, das Geheimhaltung und Regierung reguliert. Ergebnis dessen ist eine Situation, die einen unzumutbaren Preis für die Bewahrung der Grundpfeiler einer freiheitlichen Demokratie – informierte Bürger – fordert.

Den Mächtigen gegenüber die Wahrheit auszusprechen, haben Whistleblower mit ihren Freiheiten, Familien und ihrer Heimat bezahlt.

Von diesem Zustand profitieren weder Amerika noch der Rest der Welt. Es braucht keine besondere Expertise, um zu verstehen, dass es zu Unwissenheit und Verunsicherung führt, wenn notwendige Warnrufe mit der Bedrohung nationaler Sicherheit gleichgesetzt werden. Eine Gesellschaft, die dem Irrtum einer Volksweisheit erliegt, man müsse »den Überbringer schlechter Nachrichten erschießen«, wird schnell merken, dass bald nicht nur die Überbringer, sondern auch alle anderen Nachrichten ausbleiben. Es ist richtig, den Sinn einer solchen Politik und ihre unbeabsichtigten Konsequenzen in Frage zu stellen.

Wenn die Strafe für die böswillige Übergabe von Geheiminformationen an fremde Regierungen geringer ist, als wenn diese Informationen mit guten Absichten an die Öffentlichkeit gegeben werden, ermutigen wir damit nicht Spione viel mehr als Whistleblower? Was bedeutet es für die Allgemeinheit, wenn Anti-Terror-Gesetze auf den Journalismus angewendet werden?

Können wir in einer offenen Gesellschaft leben, wenn wir Einschüchterung und Vergeltung über Recherche und die Suche nach Wahrheit stellen?

Wo ziehen wir die Grenze zwischen nationaler Sicherheit und öffentlichem Interesse?

Wie können wir auf die Angemessenheit dieser Grenze vertrauen, wenn diejenigen, die sie festlegen, ausschließlich aus Reihen der Regierung stammen?

Fragen wie diese können nur durch eine öffentliche Diskussion wie die heutige beantwortet werden. Wir dürfen niemals vergessen, was die Geschichte uns über die Konsequenzen übermächtiger Überwachung gelehrt hat. Aber genauso wenig dürfen wir unsere Macht aus den Augen verlieren, diese Systeme in unser aller Interesse zu verändern.

Unser Weg war und ist steinig, aber er führt uns zu besseren Zeiten. Zusammen können wir die Sicherheit und die Rechte der kommenden Generationen sichern.

All jenen, die an dieser Diskussion teilhatten, vom höchsten offiziellen Repräsentanten bis zum kleinen Bürger, sage ich: Danke.

Asyl für Snowden

Markus Beckedahl

»Es ist gefährlich, Recht zu haben, wenn die Regierung Unrecht hat.« Was dem politisch verfolgten NSA-Whistleblower Edward Snowden derzeit widerfährt, wusste schon Voltaire in Worte zu packen. Der 30-jährige Systemadministrator hat der Weltöffentlichkeit einen Dienst erwiesen, in dem er mit einer Serie interner Dokumente bewiesen hat, was bisher oft als Verschwörungstheorie abgetan wurde. Täglich kommen neue Details des größten Überwachungsskandals in der Geschichte der Menschheit an die Öffentlichkeit, ein Ende ist noch nicht absehbar. Mehrere Geheimdienste der Welt, in diesem Fall vor allem die der USA und Großbritannien, überwachen und speichern große Teile der weltweiten Kommunikation - unrechtmäßig auch in unserem Land. Verbindungsdaten und Inhalte aller Internet- und Telefon-Nutzer werden in riesigen Datenzentren für unbestimmte Zeit gespeichert und mit Algorithmen gerastert. Keine Datenschutzbehörde kontrolliert dies. Unsere Spitzenpolitiker erfahren davon aus der Zeitung. Dass auch diplomatische Vertretungen, Unternehmen und unsere Spitzenpolitiker betroffen sind, beweist, dass der Kampf gegen den Terror dabei nur eine Ausrede ist.

Edward Snowden ist damit ein klassischer Whistleblower: er hat Missstände an die Öffentlichkeit gebracht, die diese wissen sollte. Denn ohne informiert zu sein, können Gesellschaften auch nicht zustimmen oder kontrollieren, was in ihrem Namen mit ihren Daten gemacht wird. Spätestens durch die Berichte über das Ausspionieren diplomatischer Vertretungen und des Telefons von Angela Merkel wahrt Snowden damit auch die »politischen Interessen der Bundesrepublik Deutschland«. Das im Übrigen die Formulierung des Aufenthaltsgesetzes ist, wann eine Aufnahme von Asylsuchenden aus dem Ausland geboten ist.

Innen- und Außenpolitiker der Volksparteien begründen die mögliche Ablehnung eines Asylantrages von Edward Snowden in Deutschland damit, dass die USA ein Rechtsstaat sind. Die Behandlung von Chelsea Manning, inklusive Folter und drohender Todesstrafe für das Aufdecken von Kriegsverbrechen, konterkarieren dieses Argument. Edward Snowden hätte momentan keine Chance auf einen fairen Prozess in den USA und würde im Gefängnis ruhig gestellt. Aber auch wenn es keinen Asylantrag gibt, hätte die Bundesregierung die Chance, Edward Snowden in ein Zeugenschutzprogramm zu stecken. Er ist der wichtigste Zeuge bei der Aufklärung dieses Überwachungsskandals.

Es ist unvorstellbar, dass ein chinesischer Geheimdienstler mit Informationen über die Hacking-Programme der Volksrepublik oder ein iranischer Wissenschaftler mit Informationen über das Atomprogramm der Islamischen Republik von den USA in sein Heimatland ausgeliefert würde. Die Ablehnung der Bundesregierung beweist damit bestenfalls ihre Doppelmoral, aber noch wahrscheinlich ihr Einverständnis mit dem umfangreichsten Überwachungsprogramm der Menschheitsgeschichte. Die Frage nach Snowdens Asylantrag ist eine politische Frage, die eine politische Antwort verlangt. Und die kann nur lauten: Asyl für Snowden!

Leben im Überwachungsstaat

Oder warum wir das dunkle Monster in unserer Mitte nicht länger ignorieren dürfen

Kai Biermann

Ich komme aus einem Land, das heute als der Inbegriff des Überwachungsstaates gilt. Für die Überwacher hatten wir damals viele Namen. Sie wurden »Horch und Guck« genannt, oder »die Firma«, meistens aber mit der Abkürzung bezeichnet, die bis heute jedem ein Begriff ist: »Stasi«. Das Ministerium für Staatssicherheit hatte so viele Angestellte, dass pro 180 Einwohner ein hauptamtlicher Mitarbeiter existierte. In keinem Land davor und in keinem danach kamen so viele Bewacher auf so wenige Überwachte, es war der größte Geheimdienstapparat der Weltgeschichte.

Die Stasi gehörte zum Alltag in der DDR. Niemand redete offen über sie, aber jeder wusste von ihr und jeder fürchtete sie. Die Warnung meiner Eltern, »das darfst du aber niemandem erzählen«, war in meiner Kindheit ein ständiger Begleiter. Meine Eltern hatten Angst, also hatte ich sie auch.

Trotzdem lebten alle irgendwie vor sich hin und versuchten, dieses Monstrum zu ignorieren, so gut es eben ging. Möglich war das durchaus, kaum jemand kannte Opfer des Terrors persönlich. Entweder waren die in den Westen abgeschoben worden, oder sie hielten wohlweislich die Klappe, um nicht wieder abgeholt zu werden. Das Dunkle ließ sich ganz gut verdrängen.

Selbst im Herbst 1989 ging das noch. Dabei wurden bei den Montagsdemos nicht mehr nur Einzelne abgeholt. Zu Hunderten verhaftete die Stasi nun Demonstranten, jede Woche, wahllos. Und die, die anschließend wieder freikamen, wollten nicht mehr schweigen, sie fertigten Gedächtnisprotokolle über ihre Erlebnisse, sie redeten. Plötzlich bekam die Stasi ein hässliches Gesicht, plötzlich war sie keine vage Ahnung mehr, kein Gerücht, keine Verschwörungstheorie – sie wurde real, ihre Verhöre, ihre Drohungen, die Bedrohung, die von ihr ausging, wurde auf einmal jenen Menschen bewusst, die sie sehen wollten.

Noch immer aber konnte, wer wollte, das Monster beiseite schieben. Schließlich traf es nur die, die sich gegen den Staat auflehnten, die demonstrierten, Flugblätter druckten. Wer nicht aufmuckte, der hatte doch nichts zu befürch-

ten, oder? Wie die Punkband Feeling B so richtig sang: »Wir woll'n immer artig sein, denn nur so hat man uns gerne.«

Der wahre Schrecken folgte erst später. Im Dezember 1991 trat das Stasi-Unterlagen-Gesetz in Kraft, die Opfer konnten nun nachlesen, was die Täter über sie gesammelt hatten. Meine Eltern beantragten sofort Einsicht in ihre Stasi-Akten. Es war ein Schock. In der kalten Sprache von Bürokraten wurde dort über Menschen geschrieben, die bereits verurteilt waren, obwohl noch nicht einmal eine Anklage existierte, geschweige denn irgendwelche Beweise.

Es war ein Schock, den wohl alle erlebten, die ihre Akten lasen. Denn plötzlich zeigte sich, dass jeder ein Staatsfeind gewesen sein konnte, auch wenn er selbst geglaubt hatte, dass er immer artig war. Ein Gerücht genügte, eine Bemerkung eines neidischen Nachbarn, eine Verdächtigung eines Bekannten – für die Stasi war jeder ein Feind. Und alles war ihr Recht, um mehr über die vielen Feinde zu erfahren, die sie überall sah.

In den Stasi-Akten standen Freunde und Kollegen als Zuträger, Männer, die ihre Frauen bespitzelten und Kinder, die ihre Eltern verrieten. Die Gründe dafür waren so banal wie niedrig: Geld, Eitelkeit, Missgunst. Jeder konnte zum Opfer werden, einfach so, ohne die Chance, es zu verhindern oder seine Unschuld zu beweisen.

Warum erzähle ich das alles? Der Gedanke, dass die allgegenwärtige Technik in unserem Leben dazu benutzt werden kann, uns auszuspähen, ist den meisten von uns schon lange gewärtig. Der Chaos Computer Club warnt seit vielen Jahren davor, dass Handys »Ortungswanzen« sind, die alles über ihren Besitzer verraten. Spätestens seit den Anschlägen vom 11. September werden immer mehr Gesetze verabschiedet, die Bürgerrechte einschränken und die Macht des Staates ausdehnen, die Überwachung zulassen, auch auf einen vagen Verdacht hin.

Trotzdem ließ sich das Monster bis zum Juni 2013 noch gut verdrängen. Der so verführerische wie gefährliche Satz, dass wer nichts zu verbergen hat, auch nichts zu befürchten habe, wurde von allzu vielen allzu gern geglaubt. Diejenigen, die vor allwissenden Geheimdiensten und einem misstrauischen, allmächtigen Staat warnten, wurden als Alu-Hüte verspottet, als Verschwörungstheoretiker und Sonderlinge.

Edward Snowden hat das geändert. Edward Snowden hat uns dank seiner mutigen Tat unsere Akten zugänglich gemacht. Und sie sind – selbst für jene, die es schon länger ahnten – ein Schock.

Wir wissen noch gar nicht so viel darüber, wie genau die ganzen Spionageprogramme von NSA, GCHQ, BND und wie sie alle heißen funktionieren. Dazu sind die von Snowden veröffentlichten Unterlagen zu vage und zu überblicksartig. Es sind fast ausschließlich Powerpoint-Folien, in denen stichpunkthaft über diese Projekte informiert wird. Nirgends finden sich bislang technische Beschreibungen, Organigramme oder konkrete Zahlen.

Doch das, was wir dank Edward Snowden wissen, genügt, um eigentlich auch dem Letzten klar zu machen, dass die Regierungen der Welt die Technik des Internets und des Mobilfunks missbrauchen, um ihre Bürger – uns – nahezu vollständig zu überwachen. Es braucht nicht einmal mehr ein Gerücht oder einen Verdacht, jeder ist das Ziel dieser Ausspähung. Mit der Begründung, wer eine Nadel finden wolle, müsse eben den ganzen Heuhaufen durchsuchen, wird inzwischen alles gefiltert und gespeichert, was es an elektronischer Kommunikation gibt.

- Die Geheimdienste schneiden große Teil der Daten mit, die über die internationalen Seekabel laufen, nach Angaben der NSA sind das 29 Petabyte am Tag, 1,6 Prozent des gesamten Netztraffics[2], eine sicher geschönte Zahl.
- Die Geheimdienste kopieren Metadaten von Telekommunikationsverbindungen bei den Anbietern in unbekannter Menge und aggregieren daraus Bewegungsprofile und Analysen der privaten Netzwerke der Abgehörten.
- Die Geheimdienste filtern und speichern E-Mails in unbekannter Menge und für eine unbekannte Zeit, wenn die E-Mails verschlüsselt sind wahrscheinlich für ewig.
- Die Geheimdienste überwachen via Internet geführte Gespräche mit Skype und anderen Messengerdiensten und speichern auch SMS in unbekanntem Umfang.
- Die Geheimdienste hacken die Computer von Telefonbetreibern, um die eigentlich verschlüsselt übertragenen Gespräche von Mobiltelefonen abhören zu können.
- Die Geheimdienste kopieren Daten von Finanztransaktionen, um Kontobewegungen verfolgen zu können.
- Die Geheimdienste beobachten Kommunikation in sozialen Netzwerken wie Facebook und sammeln die dort öffentlich zugänglichen Informationen aus den Accounts, um Profile von den Vorlieben und Vorstellungen

2 http://www.zdnet.com/nsa-hunger-demands-29-petabytes-of-data-a-day-7000019255/

der Überwachten zu erstellen und um zu erfahren, mit wem diejenigen Kontakt haben.
- Die Geheimdienste lesen Blogs und was sonst noch so in Newsgroups und Foren öffentlich im Netz verfügbar ist und werten diese Informationen aus.
- Die Geheimdienste geben Milliarden von Dollar aus, um Verschlüsselungsverfahren zu knacken oder zu unterwandern.

Mit anderen Worten: Unsere Geheimdienste tun alles dafür, dass wir keine Geheimnisse mehr haben, gar keine.

Und wer jetzt glaubt, dass davon ja nur andere betroffen sind und nicht er selbst – immerhin dürfen Geheimdienste wie NSA, GCHQ oder BND laut den Gesetzen ihrer Länder nur Ausländer überwachen und nicht die eigenen Bürger –, der darf nicht vergessen, dass eben diese Geheimdienste ihre Erkenntnisse gern und oft miteinander tauschen. Was der eine offiziell nicht erfahren darf, das darf der andere ganz problemlos. Denn, wie der Spontispruch sagt, jeder ist Ausländer, fast überall.

Und wer jetzt glaubt, dass davon ja nur Terroristen betroffen sind und andere Bösewichter, der darf nicht vergessen, dass bereits ein Gerücht, eine böse Bemerkung, eine Verdächtigung oder auch ein Zufall genügen, um diesen riesigen Spähapparat auf Touren zu bringen. Und dass die Betroffenen keine Chance haben, ihre Unschuld zu beteuern, weil sie im Zweifel gar nicht erfahren, dass sie minutiös überwacht werden und weil jede Bewegung, jede Handlung ihnen zum Schlechten ausgelegt wird und ganz bestimmt nicht zum Guten und zu ihrer Entlastung.

Die Stasi ließ sich ignorieren, zumindest bis ihre Akten zugänglich wurden. Die Bedrohung durch den technischen Überwachungsstaat ließ sich ignorieren, bis Edward Snowden uns die Akten der Überwacher zugänglich gemacht hat.

Die Stasi hat sich erledigt, weil viele Tausende mutige Menschen monatelang auf die Straße gingen und letztlich den Staat zu Fall brachten, der das Ministerium für Staatssicherheit geschaffen hatte. Zu glauben, dass nun überall auf der Welt Menschen demonstrieren und die Regierungen der halben Welt stürzen, ist eine Illusion. Aber zu glauben, dass überall auf der Welt mutige Menschen auf die Straße gehen und mehr Bürgerrechte fordern, mehr staatliche Transparenz, engere Grenzen für Geheimdienste und besseren Schutz vor ihnen, ist keine Utopie. Immerhin leben wir in Demokratien, wir wählen diejenigen, die die Gesetze machen.

Offensichtlich ist nur noch nicht genug Menschen aufgegangen, wie wichtig es ist, dass keine solchen Monster unter uns leben. Denn das Problem ist das Misstrauen, das sie säen. Früher richtete es sich gegen den Nachbarn und die Freunde, letztlich gegen jeden, denn jeder konnte einen verraten. Es zerfraß die Gesellschaft. Das Monster ließ sich zwar verdrängen, glücklich aber wurde damit niemand, die Angst blieb. Bei jedem Witz, den man erzählte, bei jeder Kritik, die man äußerte, war die Angst mit dabei. Heute richtet sich das Misstrauen gegen die Technik. Jedes Gespräch, jede Verbindung, jeder Datenaustausch kann uns verraten und uns zu Verdächtigen machen. Das Internet, das so viel Positives ermöglicht, wird von den Geheimdiensten als Waffe gegen uns missbraucht.

Es macht keinen Unterschied, ob wir unseren Gegenüber fürchten oder das Gerät in unserer Hosentasche. Beides sind unsere Netzwerke, die uns bestimmen, in denen wir hängen und ohne die wir nicht leben können.

Das 2008 formulierte IT-Grundrecht, das eigentlich Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme heißt, beschreibt, worum es geht. Im Urteil des Bundesverfassungsgerichtes, das dieses Grundrecht schuf, heißt es: »Die Nutzung der Informationstechnik hat für die Persönlichkeit und die Entfaltung des Einzelnen eine früher nicht absehbare Bedeutung erlangt. Die moderne Informationstechnik eröffnet dem Einzelnen neue Möglichkeiten, begründet aber auch neuartige Gefährdungen der Persönlichkeit. Die jüngere Entwicklung der Informationstechnik hat dazu geführt, dass informationstechnische Systeme allgegenwärtig sind und ihre Nutzung für die Lebensführung vieler Bürger von zentraler Bedeutung ist. [...] Informationstechnische Systeme haben mittlerweile einen derart hohen Komplexitätsgrad erreicht, dass ein wirkungsvoller sozialer oder technischer Selbstschutz erhebliche Schwierigkeiten aufwerfen und zumindest den durchschnittlichen Nutzer überfordern kann. [...] Viele Selbstschutzmöglichkeiten – etwa die Verschlüsselung oder die Verschleierung sensibler Daten – werden überdies weitgehend wirkungslos, wenn Dritten die Infiltration des Systems, auf dem die Daten abgelegt worden sind, einmal gelungen ist. Schließlich kann angesichts der Geschwindigkeit der informationstechnischen Entwicklung nicht zuverlässig prognostiziert werden, welche Möglichkeiten dem Nutzer in

Zukunft verbleiben, sich technisch selbst zu schützen. Aus der Bedeutung der Nutzung informationstechnischer Systeme für die Persönlichkeitsentfaltung und aus den Persönlichkeitsgefährdungen, die mit dieser Nutzung verbunden sind, folgt ein grundrechtlich erhebliches Schutzbedürfnis. Der Einzelne ist darauf angewiesen, dass der Staat die mit Blick auf die ungehinderte Persönlichkeitsentfaltung berechtigten Erwartungen an die Integrität und Vertraulichkeit derartiger Systeme achtet.«

Doch der Staat achtet die Vertraulichkeit der Technik nicht. Es wird Zeit, dass wir etwas dagegen tun, bevor die Zahl der Opfer der Überwachung so groß ist, dass wir sie nicht mehr ignorieren können. Wir sollten uns dagegen wehren, technisch und politisch.

Verschlüsselung ist Bürgerpflicht, sagt Phil Zimmermann, der das Programm *Pretty Good Privacy* entwickelt hat. Wer seine Daten verschlüsselt, schützt nicht nur sich selbst, sondern auch viele andere, die das noch nicht können und noch nicht tun. Wer seine Kommunikation verschlüsselt, sorgt mit dafür, dass es zur Normalität wird, zum Standard. Auch wenn das keine Überwachung verhindert, macht Verschlüsselung es doch den Überwachern schwerer.

Und es wird Zeit, dass wir für unsere Rechte auf die Straße gehen und dafür demonstrieren, nicht mehr überall und jederzeit überwacht zu werden. Im Zweifel jeden Montag.

Die Welt nach PRISM: Lektionen und ein überfälliger Anfang

Georg C. F. Greve

Die Utopie des frühen Internet war die Behauptung, es fördere qua seiner naturgegebenen Eigenschaften die Demokratie und führe zu einer Gesellschaft, in der Regierungen zum Auslaufmodell gehören. Auch wenn die Mauer um diese Utopie schon eine ganze Weile bröckelte: PRISM hat sie endgültig niedergerissen. Bruce Schneier nennt das Internet daher vielmehr einen Macht-Multiplikator: Wer bereits viel Macht hatte, wird gestärkt. Wer weniger Macht hatte, gewinnt auch dazu, aber der Abstand wächst. Viel spricht dafür, dass Schneier mit seiner Einschätzung Recht hat. Auch und gerade bei der stark wachsenden »Cloud«, für die anwendbares Recht weit vor Kryptografie oder technischer Sicherheit über die wahre Kontrolle der Daten entscheidet.

Der Grund für diese Eigenheiten wird offenbar, wenn man sich die Konsequenzen des selben latenten Anarchismus vor Augen führt, der auch die Argumente für die inhärente Demokratieförderung liefert. Wo jeder Akteur direkt auf Basis seiner individuellen Fähigkeiten mit jedem anderen Akteur interagiert, steht der einzelne Bürger der Staatsmacht eines jeden Landes direkt gegenüber. Die größte Konzentration von nicht-staatlicher Macht befindet sich in den großen Internet-Unternehmen. Diese sind jedoch weit weniger extraterritorial als sie uns glauben machen wollen. Vielmehr nehmen sie eine De-facto-Ausweitung des US-Rechts auf die ganze Welt vor, gestützt durch Abkommen wie Safe Harbor. Das Europäische Datenschutzrecht ist hier weitestgehend entkräftet und der Schutz, den die US-Unternehmen versprechen, wird meist nur aufgrund der nahezu bedingungslosen Offenlegung intimer Details und der Erlaubnis, diese kommerziell zu verwerten, gewährt. Der Vergleich mit Feudalherren ist daher nicht völlig abwegig, um die Beziehung zu beschreiben. Nun ist die Rückkehr ins Feudalsystem allerdings eher das Gegenteil der versprochenen Demokratisierung, unter der diese Dienste beworben wurden.

Daher gehören die Vertreter der Utopie oft auch zu den schärfsten Kritikern der Internetlords. Die oft gepredigte Antwort auf die Feudalherren ist Dezentralisierung, Föderalisierung, Selbsthosting. Es sollen also alle Menschen ihre Technologien mit Freier Software auf eigenen Servern selbst betreiben. Nur gibt es gute Gründe, diese Antwort zumindest in ihrer Absolutheit als zynisch zu betrachten. Vielen Menschen fehlen nicht nur die finanziellen Mittel, um einen eigenen Server zu unterhalten, der großen Vielzahl an Menschen fehlt

vielmehr die Kompetenz, ja sogar der Wunsch nach dieser Kompetenz. Und das wird sich trotz aller Versuche der Umerziehung auch nicht ändern. Denn für den Großteil der Menschen ist die Technologie schlicht ein Werkzeug für einen bestimmten Zweck, nicht aber Selbstzweck. Ohne dies untermauern zu können, würde ich sogar vermuten, dass eine überraschend große Zahl der Nutzer dieses Werkzeug lieber aufgeben würde, wenn die einzig verbleibende Alternative der entsprechende Aufbau von Kompetenz wäre.

Eine häufige Reaktion auf dieses Problem ist die Bereitstellung von vereinfachten, bereits vorkonfigurierten Lösungen. Nur ist die Zielgruppe für derartige Lösungen letztlich dieselbe Gruppe, die auch sonst selber eigene Infrastruktur betreiben könnte. Denn die Komplexität der Lösungen ist ein Resultat der Vielfalt der Möglichkeiten und Anwendungsfälle und nicht einer Verschwörung mit dem Ziel, die Nutzung dieser Technologien zu erschweren. Komplexität zu reduzieren, dabei nicht zu viele Annahmen und Einschränkungen zu machen, die Sicherheit nicht zu kompromittieren, all dies sind extrem schwere Aufgaben. Nahezu alle Techniker unterschätzen diesen Teil systematisch. Daher ist es auch kein Zufall, dass bisher nur in den seltensten Ausnahmen eine derartige Kombination gelang – und meines Wissens niemals ohne erhebliche Investition in die nicht-technischen Bereiche.

Das Ergebnis ist also auch hier wieder letztlich eine Form der libertären Gesellschaft, in der Einzelne dem Offensivpotential der NSA oder vergleichbarer Organisationen anderer Länder im Wesentlichen ausgeliefert sind. Zumal dieser Macht nahezu keine rechtlichen Rahmenbedingungen gesetzt sind. Geheimdienstliche Tätigkeit läuft außerhalb des sonstigen rechtlichen Rahmens. Das ist auch in Deutschland so, wo Artikel 10 des Grundgesetzes eine entsprechende Ausnahme vorsieht. Und da die Geheimdienste eng vernetzt sind, werden bestimmte Tätigkeiten dort vorgenommen, wo dies möglich ist und dann im Rahmen von geheimdienstlicher Kooperation mit anderen Diensten ausgetauscht. Dabei dienen gesammelte Daten als »Pseudowährung«, mit der Zugang zu anderen Quellen oder Erkenntnissen erkauft wird.

Aber vermutlich wird schon die reine Ökonomie diesen Schritt verhindern. Denn ohne Frage ist die Skalierung der Kosten im Rechenzentrum um Größenordnungen besser. Und auch die Frage der Betriebssicherheit ist nicht von der Hand zu weisen. Ein System ohne regelmäßige Wartung durch einen Administrator ist verwundbar. Spätestens bei der Vorstellung von hunderten von Millionen von Systemen ohne Administrator verteilt über die ganze Welt sollte