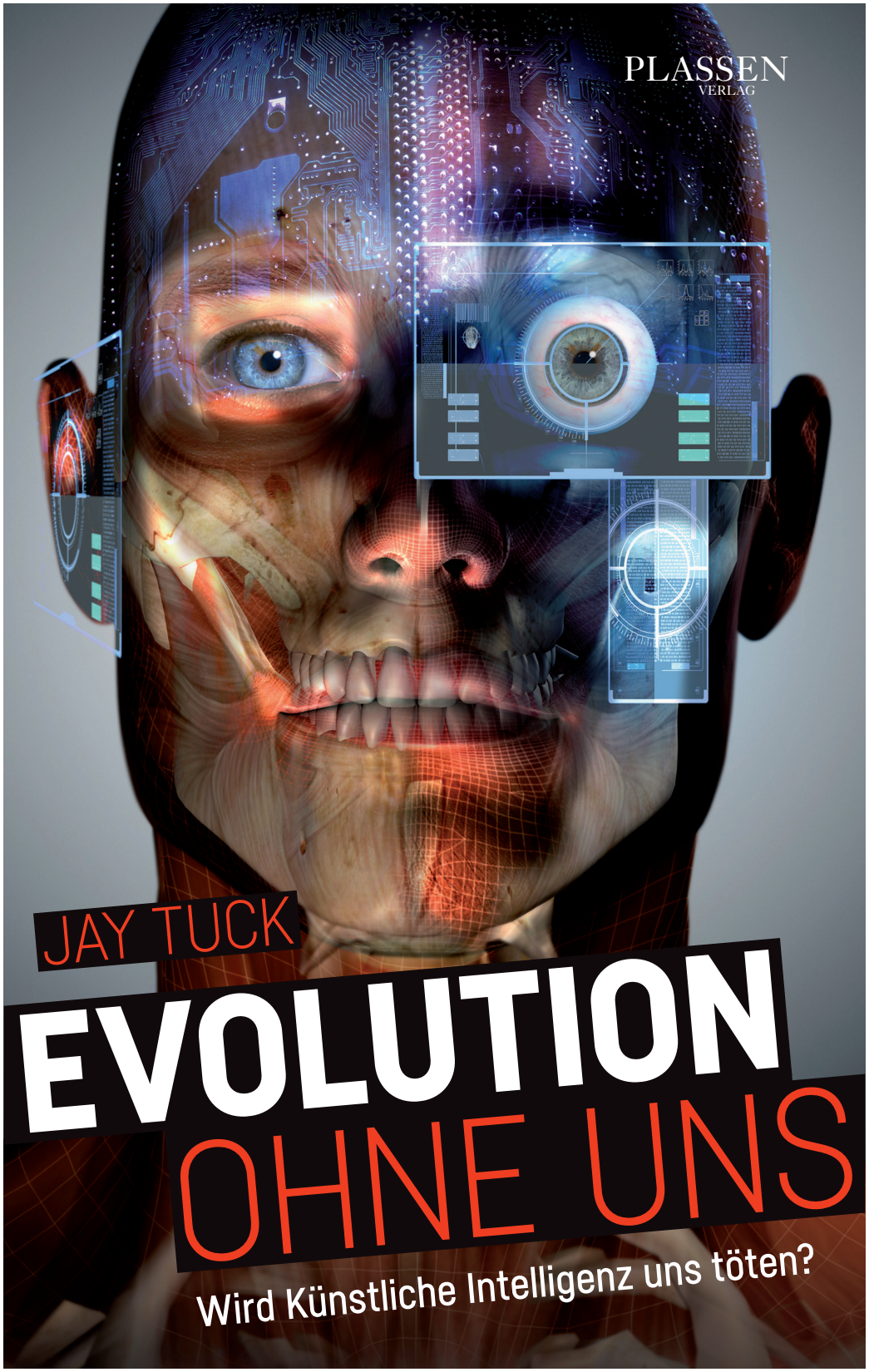
PLASSEN
VERLAG
JAY TUCK
EVOLUTION
OHNE UNS
Wird Künstliche Intelligenz uns töten?

JAY TUCK

EVOLUTION OHNE UNS

Wird Künstliche Intelligenz uns töten?

PLASSEN
VERLAG

Covergestaltung: Johanna Wack
Gestaltung und Satz: Bernd Sabat, VBS-Verlagsservice
Herstellung: Daniela Freitag
Lektorat: Hildegard Brendel
Korrektorat: Egbert Neumüller
Druck: GGP Media GmbH, Pößneck

ISBN 978-3-86470- 401-7

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

BÖRSEN MEDIEN
AKTIENGESELLSCHAFT

Postfach 1449 ▪ 95305 Kulmbach
Tel: +49 9221 9051-0 ▪ Fax: +49 9221 9051-4444
E-Mail: buecher@boersenmedien.de
www.boersenbuchverlag.de
www.facebook.com/boersenbuchverlag

Ein solches Buch ist nie allein eine Eigenleistung.
An dieser Stelle möchte ich mich bei meinem Mitautor,
dem Berliner Journalisten Armin Fuhrer, herzlichst bedanken.
Ohne seine hilfreichen Texte und Entwürfe, Anregungen und
Korrekturen, vor allem ohne seine Motivation, wäre das Buch
nie so gut geworden. Mein Dank gilt außerdem Hildegard
Brendel mit ihrer unvernichtbaren Geduld und guten Laune
sowie meiner geliebten Ehefrau Heidi, die mir mit unermüdlicher
Kraft, geduldigem Durchhaltevermögen und professionellem
Schreibgefühl von Anfang bis Ende beigestanden hat.

Jay Tuck

„Künstliche Intelligenz kann die großartigste Errungenschaft der Menschheit werden. Bedauerlicherweise kann sie auch die letzte sein."

Stephen Hawking, Astrophysiker

„Künstliche Intelligenz ist die größte existenzielle Bedrohung für die Menschheit. Wir beschwören den Teufel."

Elon Musk, Tesla

„Künstliche Intelligenz kann für die Menschheit gefährlicher werden als Atomwaffen. Sie ist das größte Risiko dieses Jahrhunderts."

Shane Legg, DeepMind

„In wenigen Jahrzehnten wird sie uns überholen. Haben wir sie bis dahin nicht im Griff, wird unsere Zukunft sehr aufregend. Und sehr kurz."

Eric Drexler, Pionier der Nanotechnologie

„Die Zukunft ist sehr beängstigend und für die Menschheit schlecht."

Steve Wozniak, Apple-Gründer

„Eine starke KI wäre wie eine Invasion Außerirdischer. Wir würden sie nicht fragen, ob sie uns mit der Wirtschaft hilft. Wir würden sie fragen, ob sie uns umbringt."[1]

Peter Thiel, Mitbegründer von Paypal

„Am Ende wird sich die Robotik durchsetzen. Es ist ganz klar, dass die Menschheit aussterben wird."

Hans Moravic, Carnegie Mellon University

„Ich verstehe nicht, warum nicht mehr Menschen beunruhigt sind."

Bill Gates, Microsoft-Gründer

Inhalt

EINLEITUNG

„Künstliche Intelligenz kann die großartigste Errungenschaft der Menschheit werden. Bedauerlicherweise kann sie auch die letzte sein.“

Stephen Hawking, Astrophysiker

Wir sind zu doof dafür.

Und deswegen werden wir die Bedrohung durch Künstliche Intelligenz wahrscheinlich erst erkennen, wenn es zu spät ist. Künstliche Intelligenz wächst nämlich mit exponentieller Geschwindigkeit. Ein menschliches Hirn kann exponentielles Wachstum nicht begreifen. Nicht wirklich. Lineares Wachstum, also x Prozent im Jahr, können wir nachvollziehen. Aber Größen, die sich ständig vervielfachen, sind schnell jenseits unserer Vorstellungskraft.

Exponentielles Wachstum kennt man in der Mathematik. So wollte Sissa ibn Dahir, Erfinder des Schachspiels, wissen, wie viel Reis auf ein Schachbrett passt, wenn man die Zahl der Körner mit jedem Feld verdoppelt. Auf das erste Feld sollte ein Korn gelegt werden, auf das zweite Feld zwei Körner, dann vier, dann acht, und bis zum 64. Feld immer wieder das Doppelte.

Auf dem letzten Feld – so sein Rechenexempel – würden $9{,}22 \times 10^{18}$ Körner liegen. Das sind mehr als 9 Trillionen Körner (9.220.000.000.000.000) mit einem Gesamtgewicht von 270 Millionen Tonnen. Diese Reismenge würde ganz Deutschland 2 cm dick abdecken. Auf dem 65. Feld würde sich der Reis nochmals verdoppeln, auf dem 66. Feld nochmals.

Exponentielles Wachstum erzeugt Größenordnungen, die für den Intellekt eines normalen Menschen kaum begreiflich sind. Deswegen verstanden wir es nicht, als sich die IT-Industrie mit exponentieller Geschwindigkeit entwickelte. Die Tragweite solchen Wachstums sprengt unsere Vorstellungskraft. Unbemerkt ist der verfügbare Speicherplatz der Menschheit faktisch ins Unermessliche gewachsen. Wir verstehen nur, dass die Entwicklung schnell geht. Wie schnell, haben wir nicht begriffen.

Mit jedem Schritt hat sich die Speicherkapazität von Heimcomputern vertausendfacht – von Kilobyte-Floppy auf Megabyte-Diskette, von Gigabyte-Speicherkarte auf Terabyte-Festplatte. Heute wird sie in den Serverparks von Nachrichtendiensten und Wirtschaftsunternehmen schon in Petabytes gemessen. Die mathematischen Fachbegriffe, die auf uns noch zukommen, stellen weitere Quantensprünge

um das Tausendfache dar: Exobytes, Zettabytes, Yottabytes, Brontobytes und Geopbytes – Größenordnungen, die unser Gehirn nicht erfassen kann.

Kilobyte (KB) 103 Byte = 1.000 Bytes
Megabyte (MB) 106 Byte = 1.000.000 Bytes
Gigabyte (GB) 10^9 Byte = 1.000.000.000 Bytes
Terabyte (TB) 10^{12} Byte = 1.000.000.000.000 Bytes
Petabyte (PB) 10^{15} Byte = 1.000.000.000.000.000 Bytes
Exobyte (EB) 10^{18} Byte = 1.000.000.000.000.000.000 Bytes
Zettabyte (ZB) 10^{21} Byte = 1.000.000.000 .000.000.000.000 Bytes
Yottabyte (YB) 10^{24} Byte = 1.000.000.000.000.000. 000.000.000 Bytes

Das heißt nichts anderes als die Möglichkeit, unbegrenzt menschliche Informationen aller Art zu speichern – Big Data. Wir haben sie nicht kommen sehen und die Folgen für unsere Demokratie nicht verstanden. Erst Medienberichte über Julian Assange und Edward Snowden versetzten die Gesellschaft in Schock. Plötzlich wurde uns klar, dass staatliche Überwachung allgegenwärtig ist, dass unsere Telefonate, E-Mails und SMS-Texte flächendeckend mitgeschnitten und für ewige Zeiten festgehalten werden. Unser demokratischer Staat wurde von den Folgen von Big Data überrumpelt. Datenschutz wird ignoriert, Grundrechte außer Kraft gesetzt, Völkerrecht umgangen.

Überwachung ist aber keineswegs auf Geheimdienste beschränkt. Facebook sammelt unsere Gesichter, Apple unsere Fingerabdrücke, Amazon unsere Vorlieben. Und Google eigentlich alles. Überwachung ist Alltag. Und wächst exponentiell.

Von der Entstehung des Homo sapiens vor zwei Millionen Jahren bis zum Jahr 2003 hat die gesamte Menschheit geschätzte fünf Exobyte an Information produziert.

Heute wird diese Datenmenge alle zwei Tage erzeugt.

Solche Datenmassen sind nur durch Maschinen beherrschbar. Eine Erfassung, Verwaltung oder Auswertung durch Menschen ist

undenkbar. Auch die Software, die Menschen schreiben, kann dies nicht bewältigen. Supercomputer mit Supersoftware sind die einzige Lösung. Sie müssen auch lernfähig sein, ihre Updates und Erweiterungen selber schreiben.

In ihrer Geschichte haben Menschen immer Maschinen erfunden, um schwere Aufgaben zu meistern, um die Reisekutsche zu ziehen oder den Dachbalken zu heben. Heute schauen wir mit unseren Erfindungen Milliarden von Lichtjahre ins Weltall auf ferne Galaxien oder tief in die Bruchteile einer atomaren Mikrowelt. Nur mithilfe unserer Maschinen wird es uns gelingen, die Dimensionen unserer Datenbanken zu begreifen und beherrschen. Es bedarf einer Künstlichen Intelligenz, die dem menschlichen Intellekt in vielfacher Hinsicht überlegen ist.

Nach Big Data rollt die Künstliche Intelligenz wie ein Tsunami auf uns zu. Sie wächst exponentiell. Täglich wird sie unabhängiger und unübersichtlicher. Und über die Folgen hat unsere Gesellschaft nicht einmal im Ansatz nachgedacht.

Stein um Stein kreieren wir die Bauteile eines neuen Wesens. Auf den Servern von Big Data ist ein Gedächtnis entstanden, so groß wie das menschliche Wissen. Mit der internationalen Vernetzung von Überwachungskameras haben wir Augen kreiert, die alles sehen. Armbanduhren und Automobile, Barbie-Puppen und Baumaschinen, Smartphones und Schlachtfelder lassen wir mit Künstlicher Intelligenz genauso ausstatten wie die intelligenten Waffen der Supermächte.

Die Künstliche Intelligenz, die diese Systeme steuert, ist autark – aber noch allein. Aus Effizienzgründen gibt es aber viele Gründe, die Information und Steuerung zu koordinieren, die Intelligenzen zu fusionieren. Sie wird sich verselbstständigen.

Heute sind die einzelnen Inseln der KI noch voneinander getrennt. Sie wachsen aber täglich näher aufeinander zu. Die Keime von Künstlicher Intelligenz werden wie Quecksilber-Tropfen zueinander finden. KI wird eine Intelligenz bilden, die unserer um ein Tausendfaches überlegen ist. Ihre Waffen zählen zu den gefährlichsten auf diesem Planeten. Es ist nur eine Frage der Zeit.

Wir haben wenig Spielraum, diese Entwicklung in den Griff zu bekommen. Die größten Denker des Silicon Valley sind überzeugt: Die Menschheit befindet sich in einem Endspiel.

„Der Fortschritt bei Künstlicher Intelligenz ist unglaublich schnell. Es besteht das Risiko, dass binnen fünf Jahren etwas ernsthaft Gefährliches passiert. Die Künstliche Intelligenz ist die vermutlich größte Gefahr für unsere Existenz."

Elon Musk, Gründer von Tesla und SpaceX, im November 2014

Heute erleichtert die Künstliche Intelligenz unser Leben. Lernfähige Software, die eigene Updates schreibt, existiert im Ansatz schon in Autos und Armbanduhren, in der Pharmaforschung und im Versicherungswesen, in Smart Homes und Smart Cities. Sie fliegt den Airbus und sortiert Amazon-Bestellungen, analysiert Vorlieben und Vorhaben bei Facebook und sortiert Menschen für Google und Geheimdienste. Auf den Finanzmärkten der Welt wickelt sie Milliardengeschäfte ab. In Operationssälen führt sie schon Skalpelle.

Künstliche Intelligenz ist heute in der Lage, viele hochkomplexe Aufgaben, die früher Spitzenpersonal anvertraut waren, zu übernehmen. Mit jedem Tag übernimmt sie immer mehr Verantwortung in unserer Gesellschaft.

„Sie wird anders als ein Mensch sein. Sie wird sich mit einer Geschwindigkeit entwickeln, die für einen Menschen nicht begreiflich ist."

Robert Finkelstein, CEO von Robotic Technology

Wir kreieren etwas, das wir nicht verstehen, ein Wesen, das uns in vielfacher Hinsicht überlegen ist. Es kommt mit der Geschwindigkeit eines Tsunamis auf uns zu. Es vollzieht schon heute Dinge, die wir nicht nachvollziehen können.

Ist es ein Frankenstein-Monster, das hier entsteht – von der Wissenschaft ins Leben gerufen, aber demnächst jenseits unserer Kontrolle?

Wird Künstliche Intelligenz bald eigene unerklärliche Ziele verfolgen? Und könnte Künstliche Intelligenz – im Gegensatz zum Filmmonster – leicht die Oberhand gewinnen, wie der britische Astrophysiker Stephen Hawking warnt?

„Sobald es die Menschen schaffen, Künstliche Intelligenz zu entwickeln, wird diese von sich selbst aus starten. Sich neu erfinden, und dies mit einer immer schneller werdenden Geschwindigkeit. Menschen, die durch ihre langsame biologische Entwicklung begrenzt sind, könnten damit nicht mehr konkurrieren und würden abgelöst werden."

Stephen Hawking, Astrophysiker

Dabei sind die Programme, die von Künstlicher Intelligenz in Mikrosekunden hergestellt werden, häufig für die eigenen Erfinder nicht ganz nachvollziehbar, womöglich auch nicht ganz kontrollierbar. Eines nicht so fernen Tages werden wir es mit einem Wesen zu tun haben, das das Wissen der gesamten Menschheit speichern kann und über die Intelligenz verfügt, es blitzschnell auszuwerten.

Die klügsten Köpfe des Silicon Valley schlagen Alarm. Visionäre wie Elon Musk und Bill Gates, Steve Wozniak und Stephen Hawking sowie Tausende von anderen IT-Forschern weltweit sind überzeugt, Künstliche Intelligenz wird uns bald überholen und bald beherrschen.

Viele glauben, sie könnte uns töten.

Einige glauben, sie wird uns töten.

Jay Tuck
Armin Fuhrer

„Ich verstehe nicht, warum nicht mehr Menschen beunruhigt sind."

Bill Gates, Microsoft-Gründer

GEDÄCHTNIS

Die Speicher-Explosion

Chelsea

Die weltweite Panik um Big Data haben zwei Amerikaner ausgelöst. Einer von ihnen war Chelsea.

Sie sieht nicht aus wie ein Weltverbesserer. Sie ist blass und blond, schüchtern und verstört. Sie spricht leise mit wenig Augenkontakt, achselzuckend und unsicher. Aber sie hat Geschichte gemacht, daran besteht kein Zweifel. Sie brachte die Spione einer Supermacht zum Zittern.

Chelsea bürstet das blonde Haar zurück. Ihre Akne-Narben hat sie ganz gut mit dem Abdeckstift kaschiert, der Lidstrich betont ihre Augen. Mit Lidschatten wäre das Ergebnis besser geworden. Das wurde ihr aber nicht gestattet.

Chelsea sitzt nämlich in einem Männergefängnis – im US-Militärgefängnis Fort Leavenworth, um genau zu sein. Der Knast ist für sie ein täglicher Spießrutenlauf zwischen Schwerstkriminellen, Männern ohne Manieren. Sie pfeifen und pöbeln, brüllen und beleidigen. Ihre Häme kann erbarmungslos sein. Aber Häme ist Chelsea immerhin lieber als Härte. Sie sehnt sich nach Weiblichkeit.

Held oder Hassfigur?

Verurteilt wurde Chelsea noch als Mann, Private First Class Bradley Manning, Geheimnisträger der US-Armee. Unter dem Namen war er noch bei der Einweisung registriert, als Gefangener Nr. 89289. Manning ist der prominenteste Gefangene in Leavenworth, ein Held für viele Kriegsgegner, ein Hassobjekt für viele Militärs. Nach dem Gesetz ist er ein verurteilter Straftäter, schuldig in zwanzig Anklagepunkten, inklusive Spionage gegen die USA. Voraussichtlich wird Leavenworth sein Aufenthaltsort für die kommenden 35 Jahren bleiben.

Seine Tat: der Diebstahl von Hunderttausenden von Geheimdokumenten der US-Army, die er in enger Zusammenarbeit mit Julian Assange in dem Untergrund-Enthüllungsblog *WikiLeaks* veröffentlichte.

Einige Dokumente waren hochbrisant, wie zum Bespiel das Bordvideo eines B-1-Bombers. Es zeigte einen US-Angriff auf das afghanische

Dorf Granai, bei dem über einhundert Zivilisten ums Leben kamen, darunter Frauen und Kinder.[2] Die Aufzeichnungen lösten große Diskussionen über mögliche amerikanische Kriegsverbrechen in Afghanistan aus.

Undiplomatische Depeschen

Andere Dokumente belegten geheime Vorgänge im Krieg, die offiziell abgestritten wurden. Noch andere zitierten aus vertraulichen Depeschen, wo Politiker und Diplomaten im vermeintlich vertraulichen Austausch ihre – oft wenig schmeichelhaften – Einschätzungen und Kommentare über die Führungsspitze anderer Länder austauschten. In vielen Fällen hatte die Veröffentlichung peinliche Folgen für die US-Außenpolitik.

Die Massendaten von Manning bildeten den Kern für die Enthüllungen von Julian Assange – und für das Renommee seiner Enthüllungsplattform *WikiLeaks*.

Dass ein einfacher Soldat unbemerkt an derartig viele Geheimdokumente herankommen konnte, lag nicht nur an der Arglosigkeit der Sicherheitsbehörden. Die Zeiten hatten sich geändert. Die Digitalisierung von diplomatischen Depeschen war in vollem Gang. Big Data hatte hohe Priorität. Für die Führung des Pentagons hatte sie viele Vorteile. Große Mengen an Informationen könnte man schnell speichern, sortieren und in kürzester Zeit auswerten. Katalogisierung war automatisch, Zugriff blitzschnell.

Aber Big Data war auch Neuland. Es änderte die Spielregeln der Spionage. In früheren Zeiten brauchte ein Spion für eine solche Aufgabe eine Sonderausrüstung – Minikamera, Fotolabor für die Filmentwicklung und ein gutes Versteck für die Mikrofiche-Aufnahmen, vielleicht unter einer Briefmarke. Längst vorbei waren die Zeiten, als man einzelne Dokumente ablichten musste. Mit einem kleinen USB-Stick konnte ein Spion jetzt im Handumdrehen Hunderttausende von Geheimdaten stehlen. Für Bradley Manning war das ein leichtes Spiel.

Er war Pionier. Und er führte den Mächtigen die neue Verwundbarkeit ihrer Geheimnisse vor. Sie würden lernen müssen, dass sich die Welt der Hochleistungscomputer verändert hatte.

18 GEDÄCHTNIS – DIE SPEICHER-EXPLOSION

Bradley Edward Manning hatte eine schwierige Kindheit. Er wurde am 17. Dezember 1987 in Crescent im US-Bundesstaat Oklahoma geboren. Sein Vater, damals Analytiker beim Militärischen Abschirmdienst, war ein sehr dominanter Mann, ein Trinker. Seine Mutter trank auch. In den Akten steht ein Selbstmordversuch. Für Freunde und Nachbarn war unübersehbar, dass die Familie gestört war.

Alkoholprobleme hatte Manning schon vor der Geburt. Wie spätere Untersuchungen zeigten, hat er bereits als Embryo Schäden aus der Sucht seiner Mutter mitbekommen.

In seiner frühen Kindheit ließen sich seine Eltern scheiden. Danach wurde er zwischen Elternteilen und Stiefeltern, Nachbarn und Verwandten hin und her geschoben. Als durch die Zweitheirat seines Vaters eine neue Halbschwester in sein Leben kam, klagte er: „Jetzt bin ich ein Niemand!"

Danach bedrohte er im Streit seine neue Stiefmutter mit einem Messer. Die Polizei kam.

Mit 13 Jahren erzählte er erstmals Freunden von seiner Homosexualität.

Nach einem kurzen Job als Software-Entwickler meldete sich Manning freiwillig zur Armee. Es war September 2007. Er hoffte, dort sein Studium zu finanzieren. Er hoffte auch, dass ein männliches Umfeld ihm womöglich mit seiner Geschlechtsidentität helfen könnte.

Doch es kam anders.

Er wurde Prügelknabe. „Er war kleinwüchsig. Er war schwul. Er hat's von allen Seiten bekommen", erinnert sich ein Kumpel aus seiner Armee-Zeit. „Nirgendwo hatte er Freunde."

Manning war ein schwieriger Kandidat. Wenn er – wie bei der Militärausbildung üblich – aus nächster Nähe von seinem Sergeant angeschrien wurde, brüllte er zurück. Er wurde mehrfach dafür diszipliniert. Vorgesetzte nannten ihn spöttisch „General Manning".

Nach sechs Wochen war bereits absehbar, dass er sich schlecht an die Militärdisziplin gewöhnen konnte. Es kam die Empfehlung, ihn aus der Armee zu entlassen. Es war aber die Zeit der Digitalisierung. Seine Einheit war überlastet. Manning war Software-Fachmann und

Geheimnisträger (Top Secret/Sensitive Compartmented Information). Der Militärische Abschirmdienst brauchte ihn.

Manning durfte bleiben.

Er war aber immer noch ein schwieriger Soldat.

Bei einem Beratungsgespräch im Dezember 2009 flippte er aus. Er schrie seine Vorgesetzten an und schmiss ihre Schreibtische samt Computer auf den Boden. Ein Militärpolizist musste eingreifen. Manning wurde entwaffnet und im Würgegriff aus dem Raum geschleppt.

Wenige Monate später wurde er von einem Offizier auf dem Fußboden einer Vorratskammer entdeckt, gekrümmt in Embryoposition liegend. Neben ihm lag ein Messer. In einen Stuhl hatte er die Worte „Ich will" (*I want*) eingeritzt. Einige Stunden danach schlug er grundlos auf eine Soldatin ein. Der diensthabende Psychiater empfahl die Entlassung aus der Armee. Manning wurde degradiert.

Aber nicht entlassen.

Drei Tage später wurde er von der Military Police verhaftet.

Wegen Spionage.

Die Spur zurück

Die Dokumente, die er zu Hunderttausenden kopiert und an Julian Assange weitergeleitet hatte, enthielten Hinweise, die bis an die Quelle zurückverfolgt werden konnten. Die Spur führte zu Manning. Er wurde identifiziert, verhaftet und verurteilt.

Seitdem sitzt er in Haft.

Begonnen hat Manning mit dem Diebstahl im Januar 2010, zunächst mit 400.000 Geheimdokumenten. Die wurden später als die „Iraq War Logs" weltweit in der Presse bekannt.

Es war der erste große Datenklau im Zeitalter von Big Data – erleichtert durch schnelle, kleine und leicht zu bedienende Speichertechnik. Der Datenklau wurde auch durch den sorglosen Umgang mit elektronischen Geheimdaten begünstigt.

Im Jahr 2010 befand sich das US-Militär in der Anfangszeit von Big Data. Es besaß große Mengen von diplomatischen Depeschen und Geheimdienstberichten, die noch nicht in digitaler Form waren.

Die Digitalisierung war Eilsache, denn erst elektronische Files können schnell gespeichert, detailliert analysiert und über große Netzwerke verschickt werden. Verschlüsselte Dateien seien auch sicherer.

Dachte die Army.

Tatsächlich eröffnete die magische Welt der Massendaten Hackern und Dieben Tür und Tor. Mit einem kleinen Speicherstift konnte ein einfacher Soldat seine umfangreiche Beute unauffällig, schnell und vollständig sichern.

Manning hatte die neue Technologie auf seiner Seite. Nur drei Tage nach seinem Irak-Download machte er sich wieder an die Arbeit. Diesmal schnappte er sich 91.000 vertrauliche Depeschen aus Afghanistan. Technisch – berichtete er später – war es ein Kinderspiel. An seinem Arbeitsplatz gab es so gut wie keine Aufsicht.

Manning kam mit einem USB-Stick aus. Mit einem paar Mausklicks konnte er ganze Archive kopieren. In der Hosentasche konnte er sie unbemerkt von seinem Arbeitsplatz beim Geheimdienst herausschmuggeln. Zurück in der Kaserne brannte er seine Beute auf CD und beschriftete sie als „Lady Gaga Songs“. Niemand wurde misstrauisch. Als er später die Heimreise nach Amerika antreten sollte, übertrug er die hochbrisanten Daten auf einen winzigen SD-Chip und steckte ihn in seinen Fotoapparat.

Es war so einfach.

Niemandem fiel das auf.

Bis die ersten Dokumente in *WikiLeaks* erschienen.

Die Veröffentlichungen – Tausende von internen Militärberichten und vertraulichen Depeschen von Diplomaten – lösten eine weltweite Welle von Presseberichten aus. Die Schockwellen reichten bis tief ins US-Außenministerium und in die obersten Ebenen der Nachrichtendienste. Hektisch begann die Spionageabwehr mit Nachforschungen. Mithilfe der vielzähligen Details in den Depeschen konnte die Quelle schnell ausgemacht werden.

Prozess

Der Prozess fand am 3. Juni 2013 vor einem Militärgericht in Quantico statt.

Seine Verteidiger wollten Manning als „Gewissenstäter" darstellen. Doch sein Status als Soldat, dazu als vereidigter Geheimnisträger der US-Streitkräfte, erschwerte diese Strategie. Anzuwenden waren Militärgesetze. Er stand vor einem Militärgericht und die Richter zeigten wenig Neigung, mildernde Umstände anzuerkennen oder Nachahmer durch eine leichte Strafe zu ermutigen.

Von dem schwersten Vorwurf wurde der junge Soldat freigesprochen. Landesverrat habe er nicht begangen, denn die Geheimunterlagen wurden nicht an Feinde verraten. Empfänger war die Weltöffentlichkeit.

Doch seine Handlung galt durchaus als Verrat von Militärgeheimnissen, keine Kleinigkeit für einen Mann in Uniform. Manning erfüllte damit den Tatbestand der Spionage.

Am 21. August 2013 wurde Bradley Edward Manning zu 35 Jahren Gefängnis verurteilt, schuldig in insgesamt 20 Anklagepunkten. Am Tag nach der Urteilsverkündung trat sein Verteidiger in der beliebten US-Talkshow mit David Letterman auf. Sein Mandant, erklärte er dem TV-Publikum, möchte nun als Frau gesehen werden. Ein halbes Jahr später wurde die Namensänderung anerkannt.

Aber im Knast wird Chelsea nach wie vor als Mann behandelt. Ein Antrag auf Verlegung in ein Frauengefängnis wurde ebenso abgelehnt wie der Wunsch auf eine Hormonbehandlung und eine Geschlechtsoperation. Er darf lediglich Frauenunterwäsche tragen.

Auf der Flucht

Am Ende konnte Julian Assange seinen Informanten nicht schützen. Er hatte keine Erfahrung mit dem Schutz von Quellen. Er selbst war kein Journalist. Außerdem hatte er eigene Probleme.

Er verfolgte das Verfahren und die Verurteilung seines Informanten aus der Botschaft Ecuadors in London. Dort hält er sich seit dem 20. Juni 2012 als Flüchtling auf.

Schweden sucht den *WikiLeaks*-Gründer mit Haftbefehl wegen sexueller Nötigung. Nur auf dem exterritorialen Boden der Botschaft kann er unbehelligt bleiben. Vor der Tür warten ein britischer Bobby, seine sichere Verhaftung und die Auslieferung nach Schweden. Von dort – so fürchtet Assange – könnte er womöglich in die USA ausgeliefert werden.

Ursprünglich wollte Julian Assange sechs bis zwölf Monate unter dem diplomatischen Schutz Ecuadors ausharren. Daraus sind mehrere Jahre geworden. „Ich sehe weniger Sonnenlicht als Gefängnisinsassen", klagt er.

Hin und wieder empfängt er Journalisten und spricht Kommentare in die Kameras. Häufig lässt er durchblicken, dass er – nach nunmehr fast drei Jahren auf der Flucht – gern nach Hause reisen würde.

Julian Assange weiß jedoch: So schnell wird das nicht passieren.

Star oder Staatsfeind

Ob als Star gefeiert oder als Staatsfeind verflucht, Bradley Manning ist sein Platz in der Geschichte der Informationsgesellschaft sicher. Durch seine Enthüllungen wurde deutlich, dass im Zeitalter von Big Data auch die Spionagedienste der Supermächte verwundbar sind. Mit relativ schlichten technischen Mitteln können sich Einzelpersonen wie Manning oder Assange Hunderttausende von geheimen Dokumenten unter den Nagel reißen und in die Weltöffentlichkeit zerren.

Sie brauchen dazu nicht – wie früher – die Mitwirkung einer großen Zeitung.

Das geht auch so.

Über das Internet.

Manning hat der Weltöffentlichkeit gezeigt, wie das geht.

Er war aber nicht der Einzige.

Edward

Es geht um die NATIONALE SICHERHEIT!“, empört sich der junge Blogger und hämmert seinen Text mit Versalien und Ausrufungszeichen in die Tastatur.

„So einen Mist schreibt man nicht in der Zeitung!!“

Gemeint waren Enthüllungen der *New York Times*, dass US-Geheimdienste das Atomprogramm Irans heimlich sabotieren wollten. Die Veröffentlichung war – aus der Sicht des Bloggers – ein Riesenskandal.

„Oder soll die *New York Times* in Zukunft unsere Außenpolitik bestimmen“, resümierte der Blogger, der im Chat unter dem Namen *TheTrueHoohah* auftrat.

„Ich hoffe, sie gehen bald pleite.“[3]

Das war im Januar 2009.

Wenige Jahre später würde der junge Mann, der sich so empörte, selber US-Geheimdokumente an die *New York Times* leiten – und zwar tausendfach. Ein Regierungssprecher würde seine Person später als „Desaster für die nationale Sicherheit“ beschimpfen, die National Security Agency NSA seine Taten als „zweites Pearl Harbor“ werten.

Genauso wie bei Bradley „Chelsea“ Manning würde er mit den Mitteln von Big Data gegen die Mächtigen im Staat vorgehen. Und die Weltöffentlichkeit erschrecken. Bei ihm war der Schock erheblich größer. Seine Taten machten klar, dass Big Data zu einer Bedrohung für die freie Gesellschaft geworden war.

Sein Name war Edward Snowden.

Kind der Küstenwache

Geboren wurde Snowden am 21. Juni 1983 in einer Kleinstadt an der Küste von North Carolina. Sein Vater war Marineoffizier bei der Küstenwache, seine Mutter Gerichtsdienerin. Seine Eltern ließen sich scheiden, als Edward noch ein Kind war. In der Schule hatte er Probleme. Unter anderem fehlte er häufig wegen Krankheit. Den regulären High-School-Abschluss schaffte er nicht.

Mit achtzehn verließ er die Schule – ohne Abitur, ohne Studienplatz, ohne Job. Der schlaksige Teenager mit dem aschblonden Haar hatte aber ehrgeizige Pläne. Er wollte etwas Besonderes werden. In Fernkursen schaffte er einen Ersatzabschluss, der ihn für Seminare an der Universität von Liverpool qualifizierte. Die Kurse, die er belegte, beendete er jedoch nicht.

Genauso verlief sein Militärdienst.

Der Schulabbrecher träumte von einer Karriere bei der US-Elitetruppe *Special Forces*. Er lernte Kung-Fu, meldete sich 2004 bei der Army und hoffte, bald das prestigeträchtige Green Beret zu tragen.

Doch kaum hatte er die Grundausbildung angefangen, musste er sie abbrechen. Er selbst erklärt seinen frühzeitigen Ausstieg mit einem „Trainingsunfall", bei dem er sich beide Beine brach. Journalistische Recherchen konnten den Vorfall nie bestätigen. Die Pressestelle des Pentagon beschränkt sich auf die Aussage, dass Snowden beim Militär keine Ausbildung abgeschlossen und keine Auszeichnungen erhalten habe.

Auch wenn aus seinen Plänen, als Elitekämpfer für die Streitkräfte zu wirken, nichts wurde, bewahrte sich Snowden seinen Sinn für Dramatik. Gern ließ er sich von seiner damaligen Freundin, einer Erotik-Tänzerin namens Lindsay Mills, als „Man of Mystery" betiteln. Er hegte immer noch den Wunsch, eines Tages zur Elite zu gehören.

Nach einer Zwischenstation als Wachmann an der University of Maryland begann Edward Snowden im Jahr 2009 eine Ausbildung bei der CIA. Er wurde als IT-Techniker der US-Mission in Genf zugeteilt. Er hatte einen Job mit verschiedenen Aufgaben: Einerseits war er für die Computersicherheit zuständig, andererseits aber auch für die Wartung der Klimaanlage.

Frust in Fernost

In dieser Zeit war er fleißig.
Er war verlässlich.

Er war ein Patriot.

Er war allerdings nicht beliebt. Edward Snowden hatte häufiger mit Vorgesetzten Ärger. Er entdeckte vermeintliche Sicherheitslücken im

IT-System, niemand teilte jedoch seine Bedenken. Er beantragte eine Gehaltserhöhung, die aber abgelehnt wurde. Er beschwerte sich über Arbeitskollegen, was zur Folge hatte, dass ein unvorteilhafter Vermerk in seiner eigenen Personalakte notiert wurde.

Snowden ärgerte sich. Er sah sich in einem Umfeld wachsender Ablehnung. In Genf blieb er weniger als ein Jahr. Schon im Februar schied er aus der CIA aus.

Er bewarb sich bei Dell Inc. Das US-Computerunternehmen war seinerzeit Auftragsfirma für ein geheimes NSA-Outpost in der Nähe von Tokio. Snowden wollte nach Japan. Er wollte nun Cyberkrieg-Spezialist werden.

In späteren Presseberichten über den Whistleblower wurden die IT-Qualifikationen von Edward Snowden hochstilisiert. Vor allem Glen Greenwald, der seine journalistische Karriere an das Schicksal von Snowden band, beschrieb ihn als „Top-Experte für Cybersicherheit."

Das war sicherlich übertrieben.

Sein Gehalt war für Geheimdienstverhältnisse eher bescheiden. Mit einem Jahresgehalt von 55.000 Euro (bei der CIA) und 95.000 Euro (bei Booz Allen Hamilton)[4] zählte er kaum zu den Spitzenverdienern. Als Geheimnisträger befand er sich auch nicht auf Eliteebene. Etwa 400.000 andere US-Staatsbedienstete besaßen eine gleichrangige Freigabe für Top-Secret-Regierungsdokumente.[5]

Er war aber mitten im Geschehen. Als Geheimnisträger von NSA und CIA gehörte er zum inneren Kreis der Sicherheitswächter. Als Systemadministrator erhielt er Zugang bis hinein in alle Ecken der Systeme, über die er wachte. Zusätzlich verfügte er über eine Genehmigung als sogenannter „Ghost-User". Das heißt, er konnte die Geheimdienst-Netzwerke kreuz und quer durchforschen – ohne Spuren zu hinterlassen.

Weniger bekannt ist der Schwerpunkt von Snowdens NSA-Arbeit, der Schutz strategischer Rechensysteme vor chinesischen Hackerangriffen. Wie kaum ein anderer war Snowden mit der geheimdienstlichen Struktur der Chinesen vertraut. Er kannte die Methodik und die Häufigkeit, die Verbreitung und vor allem die Gefahr, die von solchen Attacken ausgeht.

Chinesische Cyber-Krieger

Snowden war außerdem Spezialist für die Cyberkrieg-Strategien des chinesischen Militärs, mit denen unsere Stromnetze, Flugverkehr, Wasserversorgung und Mobiltelefone lahmgelegt werden können. Auf dem US-Luftwaffenstützpunkt Yokota nahe Tokio instruierte er japanische Sicherheitsstellen und Militär in Cyber-Abwehr gegen China.

Die Bedeutung von Edward Snowdens Spezialgebiet muss man im Zusammenhang sehen. Im Juni 2014 warnte James Clapper, Nationaler Geheimdienstdirektor der USA und Snowdens Boss*, dass Terrorismus nicht mehr die größte Gefahr für den Westen darstelle. In allen seinen Facetten sei der Cyberkrieg erheblich bedrohlicher.

An oberster Stelle nannte Clapper die Chinesen.

Flucht

Snowden war auf Hawaii, als er den Entschluss fasste, die Geheimoperationen seines Arbeitgebers dutzendfach zu enttarnen und US-Geheimdokumente millionenfach zu entwenden. Seinen Coup hatte er monatelang im Verborgenen vorbereitet. Das Werkzeug seiner Wahl waren – wie bei Bradley Manning – externe Datenspeicher.

Doch Snowdens Daten passten keineswegs auf einen gewöhnlichen USB-Stick, auch nicht auf Dutzende von Sticks. Sie füllten Terabyte-Platten.

Als Edward Snowden seine voll beladenen Harddisks in den Koffer packte, wollte er für eine bessere Welt kämpfen, sagt er. Er wollte geheimdienstliche Aktivitäten aufdecken, mit denen er nicht einverstanden war. Edward Snowden wollte eine moralische Instanz werden.

Seltsam, dass er dabei ausgerechnet China als Reiseziel wählte.

Am 20. Mai 2013 war Abreise.

---

* Als Director of National Intelligence beaufsichtigt James Clapper u. a. Central Intelligence Agency (CIA), Defense Intelligence Agency (DIA), Federal Bureau of Investigation (FBI), National Geospacial-Intelligence Agency (NGA), National Reconnaissance Office (NRO), National Security Agency (NSA), Drug Enforcement Agency (DEA), Department of Energy (DOE) und das Department of Homeland Security (DHS).

Hinter chinesischen Mauern

Snowden hätte Holland, Skandinavien oder ein liberales Land anderswo wählen können, wo er Verständnis für seine Protestaktion erwarten konnte. Er hätte ein Land wählen können, dessen Politik für ein freies Internet steht. Er hätte jedes freies Land der Welt anfliegen können.

Er wählte China.

Seine erste Station war Hongkong, eine Stadt, die bekannt ist für die Verfolgung der freien Presse und die brutale Unterdrückung von Demonstranten. Für die Überwachung des Internets hat China eines der aufwendigsten technischen Systeme der Welt. Seine Zensur ist weltbekannt. Blogger mit unliebsamen politischen Texten werden verhaftet, vorgeführt und im Schnellverfahren verurteilt.

SMS-Texte, Chats, auch Fotos werden von einem staatlichen „Büro für Internetinformationen" in Peking genau überwacht. Strafbar sind politische Texte und Meinungen, die ohne Genehmigung verbreitet werden. Bei Verstoß ist in China mit drakonischen Strafen zu rechnen – von Geldstrafen und Gefängnis bis hin zur Internierung in einem sogenannten „Reha-Camp für Internet-Süchtige". So heißen die Zwangslager für unliebsame Anwender in China, die in Chatrooms und Foren über demokratischen Protest diskutieren.

Die feindselige Haltung der chinesischen Regierung gegenüber dem Internet dürfte Edward Snowden nicht verborgen geblieben sein. Chinesische Geheimdienste standen im Mittelpunkt seiner beruflichen Arbeit bei der NSA. Sein Job war es, westliche Banken, das Militär und japanische Regierungsstellen vor deren Hacker-Attacken zu schützen.

Das Pekinger Ministerium für Staatssicherheit *GUOJIA ANQUAN BU* (中華人民共和國國家安全部) und der militärische Nachrichtendienst *ZHONG CHAN ER BU* (中华人民共和国国家安全部) standen jahrelang im Brennpunkt der nachrichtendienstlichen Arbeit der NSA.

Snowden kannte sie gut. Es ist zudem auch davon auszugehen, dass sie ihn ebenfalls gut kannten.

Und dass sie sehr neugierig waren auf die geheimen NSA-Daten, die auf den Terabyte-Disks in seinem Reisekoffer gespeichert

waren.[6] Vier Stück trug er bei sich. Zum Vergleich: alle bislang veröffentlichen Daten von Edward Snowden entsprechen nur wenigen Gigabyte.

Welche sensiblen Daten der Amerikaner tatsächlich an den chinesischen Geheimdienst verraten hat, ist nicht bekannt. Wir wissen, dass Edward Snowden über chinesische Cyber-Aktivitäten so viel wusste wie kaum ein anderer. Seltsamerweise hat er darüber nie berichtet.

Es hätte seine Pekinger Gastgeber womöglich verärgert.

Flüchtling in Transit

Sein Aufenthalt in China dauerte knapp einen Monat. Peking genehmigte keinen längeren Aufenthalt. Snowden musste weiter. In Hongkong traf er mit russischen Regierungsvertretern zusammen, die ihm halfen, seine Weiterreise zu organisieren.[7]

Als zweites Fluchtziel wählte Snowden Putins Russland – ein Land, das ebenso wenig wie China für seine freiheitliche Informationspolitik bekannt ist. Er landete am 23. Juni 2013 in Moskau. Danach wollte er offenbar weiterfliegen.

Es gab dabei aber ein Problem.

Das US-Außenministerium hatte dem flüchtigen Spion den Reisepass entzogen. Ohne Papiere war seine einzige Reiseoption die Heimreise nach Amerika, wo eine sichere Festnahme und langjährige Haftstrafe auf ihn warteten – bei einer Verurteilung wegen Landesverrat womöglich sogar die Todesstrafe.

Ohne Papiere war ein Weiterflug in ein Drittland auch nicht möglich. Von den Russen hatte er weder Einreiseerlaubnis noch Aufenthaltsgenehmigung. So saß Snowden im Transitbereich des Moskauer Flughafens Scheremetjewo fest – faktisch staatenlos, gejagt von einer Meute von Pressevertretern.

Er war in einem diplomatischen Schwebezustand. Die Putin-Regierung ließ ihn über einen Monat lang schmoren. Bis heute ist nicht genau bekannt, wo oder wie er diese Wochen verbracht hat. Man kann nur annehmen, dass er heilfroh war, als die Russen ihn endlich ins Land ließen.

Sicherlich wusste Edward Snowden, dass jede Bewegung von den unermüdlichen Augen des russischen Nachrichtendienstes FSB verfolgt wird. Der flüchtige Amerikaner war auf den guten Willen des Kremls angewiesen.

Den hatte er.

Spione unter sich

Für Wladimir Wladimirowitsch Putin war Edward Snowden ganz großes Kino. Das hat der Präsident der Russischen Föderation sofort erkannt. Snowden war amerikanischer Spion mit Unmengen an hochrangigen Cyberkrieg-Geheimnissen im Gepäck – eine wahre Fundgrube für die russischen Dienste. Snowden war außerdem ein wertvolles PR-Instrument. Mit ihm konnte Putin weltweites Misstrauen gegen die US-Supermacht säen.

Und seinen Erzfeind Barack Obama maßlos ärgern.

Eine solche Trophäe wollte Putin nicht unbeachtet in eine Vitrine schließen. Die Welt sollte ihn sehen. Journalisten, Fotografen und Kamerateams aus aller Welt durften ihn in Moskau aufsuchen. Ebenso hatte der deutsche Grünen-Abgeordnete Christian Ströbele dort seinen fernsehträchtigen Auftritt. Die konspirativen Umstände machten die Berichterstattung nur noch spannender. Damit es sich für sie lohnt, versuchte Snowden seine Enthüllungen zu portionieren. Jeder Reporter sollte seine eigene Exklusivgeschichte mit nach Hause nehmen.

Putin wollte auch persönlich von Snowdens Scheinwerferglanz profitieren. So kam es zu einem seltsamen Auftritt des Amerikaners bei der jährlichen Pressekonferenz des russischen Staatschefs. Snowden, der von einem geheimen Ort zugeschaltet war, war als „Special Guest" eingeladen. Es störte Putin wohl wenig, dass er kein Journalist war.[8]

Die beiden Männer hatten eine andere Ebene.

Von Geheimdienstler zu Geheimdienstler.

Snowden: Glauben Sie, dass es angemessen ist, statt nur Einzelpersonen eine ganze Gesellschaft unter Beobachtung zu stellen?

Putin: Mr. Snowden, Sie sind ehemaliger Agent und Spion. Ich habe früher auch für einen Geheimdienst gearbeitet. Wir sprechen dieselbe Sprache. Zunächst unterliegen nachrichtendienstliche Methoden in Russland einer strengen gesetzlichen Regelung. Unsere Dienste dürfen Überwachungstechniken für Telefon oder Online-Aktivitäten nur anwenden, wenn eine richterliche Anordnung vorliegt. Ein Programm zur Massenüberwachung haben wir nicht.[9]

Unter wachsamen Augen

Die Enthüllungen, die die Welt schockierten, wurden alle aus seinem Moskauer Versteck gesteuert, einem konspirativem Safe House, das von Geheimdienst-Gorillas des FSB überwacht wird. Auswärtige Besuche fanden immer unter ihren wachsamen Augen statt. Koordiniert wurden sie von einem Mann, den Snowden „mein Anwalt" nennt.

Die Rede ist von Anatoli Kutscherena, profilierter Putin-Freund und Mitglied im Aufsichtsorgan des russischen Geheimdienstes FSB. Ohne seinen Segen, so berichten Besucher, läuft mit Snowden nichts.

In seiner Flüchtlingszeit bewies Snowden immer wieder einen ausgeprägten Sinn für Dramatik. Wenn er am Laptop tippte, zog er eine rote Kapuze über den Kopf, damit Überwachungskameras seine Passwörter nicht erfassen, wie er erklärte. Unter die Tür schob er ein Kissen, um Abhörmaßnahmen zu blockieren. Die Mobiltelefone von Besuchern packte er in den Kühlschrank, damit sie keine Signale abstrahlten.

Sicherheitsmaßnahmen waren auf jeden Fall erforderlich.

Der flüchtige amerikanische Spion war in akuter Gefahr.

Die Jagd nach Edward

Die US-Regierung wollte ihn haben.

Daran besteht kein Zweifel.

„Snowden hat mehr Schaden angerichtet als jeder andere Spion in der Geschichte unseres Landes", so die Einschätzung des damaligen NSA-Chefs Keith Alexander. „Das wird unsere Arbeit die nächsten zwanzig bis dreißig Jahre beeinträchtigen."[10/11]

Ein solcher Täter darf nicht unbehelligt davonkommen. Nicht aus Sicht der US-Dienste, die ihn im Verborgenen verfolgen. Und bereit sind, erhebliche Risiken einzugehen. Deutlich wurde das am 2. Juli 2013, als eine gewagte CIA-Operation fehlschlug.

An diesem Tag war Boliviens Präsident Evo Morales zu einem Staatsbesuch in Moskau. Es gab einen Geheimtipp: Snowden sollte an Bord des Präsidialjets heimlich aus dem Land geschmuggelt werden. So die Informationen. Daraufhin verweigerten mehrere EU-Länder den Überflug. Das Flugzeug des Präsidenten wurde zur unplanmäßigen Landung in Wien gezwungen.

Der Tipp entpuppte sich als Ente, die Aktion als Flop. Snowden war nicht an Bord. Diplomatisch war es ein Desaster. Aus ganz Europa folgte Kritik. Der österreichische Außenminister sah sich gezwungen, sich öffentlich zu entschuldigen.[12]

Für die ganze Welt wurde sichtbar, wie weit die Amerikaner gehen würden, um den abtrünnigen NSA-Spion zu schnappen.

Snowdens Schockwellen

Die Enthüllungen von Edward Snowden machten Schlagzeilen.
Rund um die Welt.
Monatelang.
Mit dramatischen Folgen.

Bürger waren schockiert, Politiker empört, Nachrichtendienste verunsichert. Die Washingtoner Regierung wollte Snowden schnellstmöglich ins Gefängnis befördern. Deutsche Datenschützer feierten ihn als Helden. Einige wollten ihm Asyl gewähren, andere sogar für den Friedensnobelpreis nominieren.

Wie auch immer man die Taten von Edward Snowden wertet, eines steht fest: Seine Veröffentlichungen haben für große Verunsicherung in der Bevölkerung gesorgt. Der Umfang der gespeicherten Informationen, das merkten alle, hat unsere Gesellschaft unwiderruflich verändert.

Die Debatte um Big Data hat begonnen.

Und da Big Data nur von Künstlicher Intelligenz gesteuert werden kann, wird die Debatte um Künstliche Intelligenz sehr bald folgen.

Big Data, Big Danger

Big Data haben wir nicht kommen sehen. Mit einem Schlag war sie da, eine fast grenzenlose Speicherkapazität, fast grenzenlose Datenbestände, fast grenzenloses Überwachungspotenzial. Big Data ist das Ergebnis eines exponentiellen Wachstums in der Hardware-Industrie.

Wir sind heute erst dabei, die Konsequenzen zu verstehen.

Und das Wachstum setzt sich unaufhörlich fort.

Exponentiell.

Nach den Veröffentlichungen von Bradley „Chelsea" Manning bei *WikiLeaks* und Edward Snowden in der Weltpresse wurde klar, dass die Menschheit am Ufer eines gigantischen Datenmeers steht. Wir schauen in die Ferne, können aber weder Weite noch Tiefe begreifen. Wir haben keine Übersicht, geschweige denn Kontrolle.

Der Speicherplatz, der hier entsteht, ist das Gedächtnis eines neuen Wesens, das der Menschheit bei Weitem überlegen sein wird. Das Gehirn kommt noch.

Solche Datenmassen sind nur durch Maschinen beherrschbar. Eine Erfassung, Verwaltung oder Auswertung durch Menschen ist undenkbar. Auch die Software, die Menschen schreiben, kann es nicht schaffen. Supercomputer mit Supersoftware sind die einzige Lösung. Big Data wird eines Tages das Gedächtnis einer neuen weltumspannenden Künstlichen Intelligenz (KI) werden.

Big Data hat das Potenzial, das Wissen der gesamten Menschheit zu erfassen, Informationsmassen, die unsere Vorstellungskraft sprengen. Es könnte Bücher, Brockhaus-Enzyklopädien und sogar sämtliche Bibliotheken der Welt zur Makulatur machen.

In den ersten vierzehn Jahren seiner Existenz ist der Datenumfang von Wikipedia allein in englischer Sprache auf über fünf Millionen Beiträge gewachsen. Weltweit enthält das Werk heute 19 Milliarden Wörter in 287 Sprachen. Zwischen dem Schreiben dieses Manuskripts und der Veröffentlichung als Buch ist davon auszugehen, dass Wikipedia sich schon wieder verdoppeln wird.

Manning und Snowden haben geholfen, die Folgen von Big Data für die Weltöffentlichkeit anschaulich zu machen. Schockierende Schlagzeilen, düstere Leitartikel und polemisierende Politiker taten den Rest.

Die öffentliche Beunruhigung richtet sich fast ausschließlich auf staatliche Daten, insbesondere auf die US-Abhörbehörde National Security Agency, NSA. Sie ist keineswegs der einzige Datensammler, der unsere Intimsphäre verletzt, vielleicht auch nicht der gefährlichste.

Interessanterweise waren einige der sogenannten Enthüllungen von Edward Snowden inhaltlich nicht neu. Einige Presseberichte wurden aufgebauscht, einiges an Empörung geheuchelt.

Aber die Bevölkerung hat eines verstanden:

Big Data bedeutet Big Danger.

Mutti abgehört

Es war vor allem das Abhören des Handys von Bundeskanzlerin Angela Merkel, das Deutschland wachgerüttelt hat. Es war eine persönliche Attacke gegen seine Bundeskanzlerin. Wenn die Privatsphäre von „Mutti" Merkel für die alliierten Freunde in Amerika nicht heilig ist, wie steht es mit dir und mir? Bundesbürger begannen zu begreifen, was Big Data in der Spionagewelt von heute bedeutet: Die Öffentlichkeit wird komplett beobachtet.

Die Öffentlichkeit war erschüttert.

Das Vertrauen in den transatlantischen Bündnispartner ebenso.

„Einen Angriff auf die Souveränität eines demokratischen Staates" nannte das Thomas Oppermann (SPD), Vorsitzender der Parlamentarischen Kontrollkommission im deutschen Bundestag. „Wer so dreist ist, der hat auch keine Hemmung, die Mobiltelefone der Bürger abzuhören und ihre E-Mails zu lesen."

Über „einen schweren Vertrauensbruch" beschwerte sich der damalige Bundesinnenminister Hans-Peter Friedrich (CSU). „Nicht hinnehmbar", schimpfte Belgiens Regierungschef Elio Di Rupo. Der damalige EU-Kommissionschef José Manuel Barroso warnte gar vor „Totalitarismus". In der Presse gab es zahlreiche Vergleiche mit den Abhörpraktiken der DDR-Staatssicherheit.

Das persönliche Mobiltelefon der Bundeskanzlerin anzapfen, fragten viele, wie geht das technisch?

In der Presse kursierten die schrillsten Erklärungen. *Stern-TV* machte „den Abhörtest“[13]. In einer Sendung vom 30. Oktober 2013 stellten sich Redakteure auf dem Rasen vor dem Reichstag auf die Lauer. Aus einem geparkten Minibus demonstrierten sie, wie man mithilfe eines sogenannten IMSI-Catchers in der Nähe befindliche Mobiltelefone orten und identifizieren, abhören und die Daten abspeichern kann.

Witzbuch-Autor und „IT-Sicherheitsexperte“ Tobias Schrödel ergänzte: „Eine räumliche Nähe zu dem Abhörobjekt macht deswegen Sinn, weil ich mit entsprechenden Richtfunk-Antennen Daten abfangen und dann mit einem Rechner entschlüsseln könnte.“

Das Publikum war beeindruckt.

Beifall.

Absurdistan.

Tatsächlich ist ein IMSI-Catcher ein recht simples Gerät, das Amateur-Hacker für rund 150 Euro im Versandhandel erwerben können. Die Abhörmethodik, die *Stern-TV* als NSA-Enthüllung präsentierte, ist in Wirklichkeit nicht viel mehr als ein Wald-und-Wiesen-Trick für eine Dorf-Detektei. Die Vorstellung, dass amerikanische Hightech-Spezialisten in einem Kastenwagen vor dem Kanzleramt parken und Frau Merkel belauschen, ist abstrus. Westliche Geheimdienste – und zwar nicht nur die NSA – greifen ihre Daten von Unterwasserkabeln, Satellitenstationen, Mobilfunkmasten und zentralen Knotenpunkten ab. Lauernde Lauscher mit Kopfhörer im Kastenwagen oder Trenchcoat-Täter in dunklen Gassen gehören in die Geschichtsbücher des Kalten Krieges oder in Kinofilme über die DDR („Das Leben der Anderen“).

Der moderne Spion arbeitet mit Großrechnern.

Andere Redaktionen schickten Reporter zur US-Botschaft am Brandenburger Tor. Der Standort liegt knapp 800 Meter vom Bundeskanzleramt entfernt. Fotografen knipsten Infrarot-Bilder von dem Gebäude. Heiße Stellen unter dem Dach des Diplomaten-Hauses sollten als Beweis für die Abstrahlung von Abhöranlagen herhalten.

Tatsächlich verfügt jede größere Botschaft in Berlin über Sendemasten und Satellitenschüsseln für diplomatische Depeschen. Bei der US-Botschaft stehen diese unter dem Dach. Sie strahlen Wärme ab.

Viele Enthüllungen von Edward Snowden, die in der deutschen Presse ein großes Echo auslösten, werden niemanden in deutschen Sicherheitskreisen wirklich schockiert haben. Unter informierten Politikern und sachkundigen Journalisten waren sie längst bekannt. Der Datenaustausch zwischen NSA und BND ist alltäglich. Und eng, sehr eng. Gemeinsam mit anderen befreundeten Diensten werten BND und NSA Lauschangriffe zusammen aus – Namen und Nummern, Staatsangehörigkeit und SMS-Texte, Mails und Mitschnitte.

Sie werden durchsucht und gefiltert, identifiziert und ausgewertet. Technisch geht das mit der Stimmerkennung. Die Stimmbänder eines jeden Menschen besitzen Merkmale, die genauso einmalig sind wie ein Fingerabdruck. Hinzu kommen Aussprache und Dialekt, Redewendungen und Rhythmus. Abhörspezialisten können daraus das Sprachprofil einer verdächtigen Person erstellen und es wieder in die Datenbestände einfüttern.

Diese riesigen Datenmassen bilden den Heuhaufen.

Sicherheitsbehörden suchen die Nadel.

Und manchmal finden sie die.

NSA auf dem Kanzlerschreibtisch

Das Ergebnis dieser Lauschangriffe wird an höchste Regierungsstellen weitergeleitet. Auf den Schreibtisch der Kanzlerin zum Beispiel werden jeden Morgen Geheimberichte gelegt, die Infos aus den weltweiten Abhöranlagen der NSA enthalten. Die Kooperation zwischen CIA und BND, FBI und Verfassungsschutz, NSA und dem Militärischen Abschirmdienst der Bundeswehr (MAD) ist selbstverständlich und – wie BND-Mitarbeiter unter der Hand berichten – unverzichtbar.

Dass ein Mobiltelefon der Kanzlerin darunterfällt, durfte niemanden sonderlich überraschen. Handy-Gespräche in der Bundesrepublik – wie anderswo in Europa auch – werden flächendeckend und lückenlos angezapft. Faktisch muss man davon ausgehen, dass alles,

was dort gesprochen, getextet oder gesurft wird, von NSA-Lauschern in Fort Meade verfolgt werden kann.

Nach der großen Empörungswelle in der deutschen Öffentlichkeit sah sich US-Präsident Barack Obama genötigt, öffentlich zu versprechen, dass Angela Merkels Handy nicht mehr belauscht wird. Dies signalisierte allerdings keine grundlegende Veränderung der Abhörtaktik der USA. Das wissen Eingeweihte, auch im Kanzleramt. Die US-Lauschbehörde verfügt nach wie vor über die nötige Technologie. Sie kann jederzeit per Knopfdruck aktiviert werden. Es ist nur eine Frage von Zeit und Zweckmäßigkeit.

Obamas Versprechen, das Gerät der Kanzlerin nicht mehr anzuzapfen, war eine diplomatische Geste. Wogen sollten geglättet, lädierte Beziehungen gekittet werden.

Die öffentlichen Wogen wurden aber nicht gleich geglättet, die lädierten Beziehungen nicht gekittet.

Kurz darauf platzte die nächste Bombe.

Diesmal kam die Enthüllung nicht von Edward Snowden. Sie wurde von der deutschen Spionageabwehr aufgedeckt. Am 2. Juli 2014 marschierten Beamte des Bundeskriminalamts in die neue Nachrichtendienstzentrale des BND in Berlin und verhafteten einen Mitarbeiter. Der 31-jährige Markus R. war Analytiker aus dem Stab EA („Einsatzgebiete/Auslandsbeziehungen"), zuständig für technische Unterstützung. Er war auch – wie er kurz nach der Verhaftung gestand – Spion für die CIA. Der nächste Skandal um amerikanische Geheimdienste in Deutschland war perfekt.

Der BND-Techniker hatte seine Dienste der US-Botschaft in Berlin per E-Mail angeboten und über einen Zeitraum von zwei Jahren Geheimpapiere an die Amerikaner geliefert. Für seine Dienste zahlten sie ihm rund 25.000 Euro.

Die Vorwürfe waren brisant.

Das Timing hätte nicht schlechter sein können.

Empörung kam aus ganz Europa.

Alliierte abhören

„Befreundete Länder kann man nicht einfach abhören, Daten absaugen, verarbeiten," ärgerte sich Österreichs Vizekanzler Michael Spindelegger. Er war eine von vielen Stimmen im In- und Ausland.

Dabei ist es die Aufgabe von Nachrichtendiensten, Politiker in befreundeten Ländern auszukundschaften. Das gilt für Skeptiker der US-Allianz wie auch für begeisterte US-Freunde wie Angela Merkel.

Für die USA ist die Bundesrepublik ein Partnerland, das Wirtschaftsbeziehungen zur aufstrebenden Atommacht Iran pflegt, enge Kontakte zu Russland unterhält und einen Ex-Kanzler hat, der auf der Gehaltsliste von Wladimir Putins *Gazprom* steht.

„Es gibt zwischen Staaten keine Freundschaften", erklärte mir ein ehemaliger Präsident des Bundesnachrichtendienstes am Rande einer Sicherheitskonferenz. „Es gibt nur Interessen."[14]

Da kann es niemanden ernsthaft überraschen, dass NSA und CIA ihre langen Ohren in Richtung Berlin ausstrecken. Spioniert wird überall und immer, auch unter Freunden. Das ist bekannt. Und wird abgestritten. Es ist der Beruf des Geheimdienstlers – lauschen, leugnen und – wenn es sein muss – lügen.

Die Empörung war scheinheilig.

Deutsche Dienste spionieren fleißig mit – auch gegen Freunde, auch gegen Amerika. Knapp einen Monat nach der Verhaftung des US-Spions flatterten Belege in die Redaktionen deutscher Zeitungen. Aufgetaucht – wahrscheinlich nicht zufällig – war das BND-Protokoll eines abgehörten Telefonats mit US-Außenministerin Hillary Clinton. Im Oktober 2011 hatte sie mit ihrem Handy aus einer amerikanischen Militärmaschine telefoniert. Dem BND liegt ein vollständiges Protokoll im Wortlaut vor.

Die Pressestellen der Regierung hatten gerade angefangen, die Dementi-Maschinen anzuwerfen, als kurz darauf ein weiteres Abhörprotokoll auftauchte. Clintons Nachfolger im Amt, John Kerry, wurde bei einem vertraulichen Nahost-Gespräch mit dem ehemaligen UN-Generalsekretär Kofi Annan belauscht.

Wie die Mitschnitte auf Festplatten des BND landeten, wurde nie geklärt. Der Regierungssprecher erklärte kleinlaut, es habe keine gezielten

Abhörmaßnahmen gegen die amerikanischen Amtsträger gegeben. Die vertraulichen Mitschnitte waren im Rahmen anderer Operationen entstanden. „Beifang" nannte man das beim BND.

„Idiotisch" nannte es ein Regierungsbeamter. Eigentlich hätten alle Aufnahmen mit US-Politikern sofort gelöscht werden müssen. Sagte er. Dabei ist eines klar:

BND und CIA hatten beide die goldene Regel der Spionage gebrochen:

„Lass dich niemals erwischen."[15]

Kurz nachdem die BND-Abhörprotokolle von Clinton und Kerry an die Öffentlichkeit gelangt waren, folgten Belege, dass die Bundesrepublik Deutschland auch andere NATO-Freunde belauscht. Ganz offiziell gehörte der NATO-Partner Türkei zu den erklärten Zielen der BND-Spionage. Seit vielen Jahren.

In einem geheimdienstlichen Grundsatzpapier aus dem Jahr 2009 wurde der Türkei eine hohe Priorität für den BND eingeräumt. Einige Tage später folgte die Enthüllung, dass der NATO-Partner Albanien ebenfalls langjähriges Spionageziel des BND war. Auch Maßnahmen gegen befreundete Länder wie Frankreich und Italien wurden ausdrücklich erwähnt.

Ja, Freunde spioniert man aus.

Das ist einfach so.

Enthüllungen, die keine waren

Edward Snowden hat seine Dokumente nicht gleichzeitig veröffentlicht. Wie ein guter PR-Manager wusste er, dass die Wirkung damit verpufft wäre. Er hat seine Pressemitteilungen in Paketen portioniert. Jeder Journalist sollte eine eigene Enthüllungsgeschichte bekommen – exklusiv für sein Heimatland, maßgeschneidert für seine Leserschaft. Die Veröffentlichungen erfolgten nach strengem strategischen Zeitplan, den Snowden mit seinem vertrauten Journalistenkumpel Glen Greenwald ausgearbeitet hat – mit Unterstützung der WikiLeaks-Anwältin Jesselyn Radack. Ungeklärt ist die Mitwirkung von russischen Ratgebern.

Auf jeden Fall hat Radack gern NSA-kritische Kommentare der russischen Presse angeboten. In einem Interview für *Voice of Russia* kritisierte sie massiv die Arbeit der US-Dienste. Russische Spionage erwähnte sie nicht.

Viele Dokumente, die Snowden groß ankündigte, waren kaum Enthüllungen. Aber Dokumente mit der Aufschrift „Top Secret" kommen bei Journalisten immer gut an. Ihnen wird ein prominenter Platz und eine fette Schlagzeile eingeräumt. Dazu zählten PowerPoint-Präsentationen zur Orientierung von neuen Mitarbeitern. Sie trugen zwar die Überschrift *Top Secret/NoForn* (Geheim/für Ausländer gesperrt), beschrieben aber NSA-Programme nur in groben Zügen – ohne vertrauliche Namen, Gesprächsinhalte oder sensible Quellen.

Sie hatten die Brisanz eines Organogramms.

Mehrere Programme waren längst eingestellt.

Mauscheleien am Meeresboden

Für viele Bundesbürger waren die groß angelegten Lauschangriffe der NSA auf Unterseekabel schockierend. Für Eingeweihte nicht. Seit Jahrzehnten stehen sie in der Presse. Im Parlament und in der Politik hat man ausgiebig, langjährig und in aller Öffentlichkeit über die enge Zusammenarbeit zwischen NSA und der britischen Lauschbehörde *Government Communications Headquarters (GCHQ)* debattiert.

Bereits 1992 wurden Details der gemeinsamen Lauschangriffe in Anhörungen des US-Senats öffentlich. Seitdem ist bekannt, dass die gesamte Telekommunikation zwischen Nordamerika und Europa auf dem riesigen NSA-Stützpunkt Manwith Hill in North Yorkshire routinemäßig mitgeschnitten wird. Die Ergebnisse werten London und Washington gemeinsam aus. Supercomputer der NSA durchsuchen alle Gespräche nach Anschlüssen und Identitäten, Schlüsselwörtern und Stimmabdrücken, die aus Sicht der Spionagebehörde interessant sind.

Inzwischen sollen NSA und GCHQ über uneingeschränkten Zugang zu über 200 Unterseekabeln weltweit verfügen. Allein das NSA-Teilprogramm Tempora verdaut rund 21 Millionen Gigabyte

am Tag. Rund 550 Analytiker von NSA und GCHQ sind mit der Auswertung beschäftigt.

Die größte Leistung bringt dabei Kollege Computer, der mit Künstlicher Intelligenz ihre Such- und Sortiersysteme immer weiter verfeinert.

Auch in deutschen Medien sind die groß angelegten Lauschprogramme der NSA seit Langem Thema. Im Jahr 2000 veröffentlichte zum Beispiel *Der Spiegel* geheime Details über das NSA-Programm *Echelon*:

„Dass die Vereinigten Staaten und Großbritannien mit ihrem Abhörsystem Echelon die eigenen Verbündeten ausschnüffeln, war ein offenes Geheimnis. Jetzt ist es keines mehr."[16]

Lauschen in der UNO

Für große Empörung sorgte auch die Snowden-Enthüllung, dass die NSA geheime Beratungen der UNO in New York belauscht. Dabei gehören Abhöraktionen in den Vereinten Nationen seit eh und je zum Alltag. Mit dem Bau des Gebäudes begannen Spione aller Couleur, mit Schleifgerät und Bohrmaschine die Wände zu durchsieben. Im Jahr 1960 präsentierte der US-Botschafter Henry Cabet Lodge einen Holzschnitt des US-Staatswappens, das ihm von einer russischen Schulklasse geschenkt wurde. Versteckt im hübschen Wandschmuck war eine Wanze des russischen Geheimdienstes KGB.

Manche Diplomaten witzeln darüber, dass es an ein Wunder grenzt, dass das UN-Hochhaus an der New Yorker First Avenue noch steht. Eigentlich müsste die Statik durch Wanzenlöcher längst zusammengebrochen sein.

Diplomaten-Treffs bieten eine einmalige Gelegenheit, an die Verhandlungstaktik fremder Staaten heranzukommen. So überrascht es nicht, dass Snowdens Dokumente Abhöraktivitäten von NSA und GCHQ beim G20-Treffen 2009 in London belegten. Angezapft wurden – so Snowden – Mobiltelefone, E-Mails und Laptops. Mit Keyloggern wurden alle Tastatureingaben festgehalten.[17]

Die Beobachtung solcher Gipfel ist keine Einbahnstraße. Auch für den ehemaligen Geheimdienstler Wladimir Putin sind sie interessant. Als sich die Staatschefs am 5. September 2013 in St. Petersburg

versammelten, war das für seine Dienste ein Heimspiel. Unter den Giveaway-Geschenken, die Besucher vom Gastgeber erhielten, war ein hübscher USB-Stick mit buntem G20-Logo. Darauf – wie der BND später in Brüssel entdeckte – war ein Trojaner, der Laptops und heimische PCs für die Russen ausspionieren sollte.

Es ist eigentlich selbstverständlich für Spione.

Ausspähen ist ihr Beruf.

Der bessere BND

Im August 2014 wurde ein hochgeheimes Strategiepapier des Bundesinnenministeriums im Bundeskanzleramt vorgelegt. Spezialisten sollten die elektronischen Fähigkeiten der deutschen Dienste kritisch unter die Lupe nehmen und Schwachstellen ausloten. Trauriges Resümee: Elektronisch sind die deutschen Dienste so gut wie blind und taub.

Lange war der BND für seine exzellenten Agenten-Quellen im Bereich HUMINT („Human Intelligence") bekannt. Traditionsgemäß verfügte er über verlässliche Informanten-Netzwerke im ehemaligen Ostblock, im Iran und in der arabischen Welt. Technisch waren seine Horchposten in Pakistan und – versteckt auf Containerschiffen – im arabischen Raum sehr ergiebig.

Aber die Zeiten haben sich geändert. Im elektronischen Bereich (SIGINT) hatte der BND – so die Studie – den Anschluss ans Zeitalter von Big Data verschlafen. Ursache war vor allem, dass viele deutsche Technologiefirmen ihre globale Spitzenposition verloren hatten. Ohne Unterstützung der US-Partnerdienste sei der BND – nach eigener Einschätzung – nicht voll handlungsfähig. Kurz- und mittelfristig seien deutschen Spione auf das Wohlwollen der Amerikaner angewiesen.

Der Bundesnachrichtendienst – so das Strategiepaper weiter – besitzt weder die Technik noch das Personal, um globale Datennetze umfassend anzuzapfen oder sinnvoll auszuwerten. Hacker-Angriffe ausländischer Mächte könne er orten, aber nicht verhindern.

Ein BND-Insider zog den Vergleich: „Wir sitzen auf dem Berg und zählen die Blitze".[18]

„Ohne US-Hilfe", lamentiert ein anderer, „würden wir von hundert Dschihadisten in Deutschland maximal fünf selber finden."

Ähnlich sieht es bei der Verschlüsselung von Daten und deren sicherer Aufbewahrung aus. Die stärksten Unternehmen befinden sich im Silicon Valley*. Dort ist seit Langem bekannt, dass internationale Verschlüsselungsfirmen vertragliche Beziehungen zur NSA unterhalten. Sie sollen dafür sorgen, dass die Exportversionen ihrer Produkte leichter zu knacken sind.

Die NSA ist auch durch Strohmänner an den entscheidenden Gremien beteiligt, die technische Standards für die internationale Übertragung von Daten festlegen. Zusammen mit ihrem britischen Partner GCHQ hat sie Vereinbarungen mit den Betreibern von Unterseekabeln, die Abhörpraktiken ausdrücklich erleichtern.

Geheimnisse im Kabinett

Trotz enger Zusammenarbeit zwischen den Nachrichtendiensten hat jede Regierung Geheimnisse, die geheim bleiben sollen. Aus Sicherheitsgründen lagert der BND einige empfindliche Daten auf israelischen Servern in der Negev-Wüste. Von der Parlamentarischen Kontrollkommission des Bundestags wurde ein Panzerschrank für die Mobiltelefone der Parlamentarier angeschafft.

Besonders sensibel sind die Tagungen des Bundeskabinetts. Wenn die Kanzlerin im abhörsicheren Kabinettsaal mit gusseiserner Glocke die Sitzung einläutet, sollen sich die Teilnehmer sicher fühlen. Minister wollen ungestört Meinungen und Maßnahmen austauschen. Geheimhaltung ist zwingend.

Deswegen wird hier das Protokoll in Steno angefertigt.

Mit Bleistift.

Auf Papier.

Ganz ohne Elektronik.

Zur Sicherung des Protokolls wird auf eine Technologie aus dem 19. Jahrhundert zurückgegriffen, die gute alte Rohrpost. Die sensiblen

* Eine Ausnahme ist Kaspersky, ein Moskauer Unternehmen mit engen Verbindungen in den Kreml.

Papierprotokolle werden in kleinen, zylindrischen Behältern in den Keller des Kanzleramts befördert und dort in einem Panzerraum gelagert. Das System ist nicht gerade Hightech.

Es ist aber abhörsicher.[19]

Nach dem Snowden-Sturm

Auch wenn einige Enthüllungen von Edward Snowden im Einzelfall nicht wirklich neu sind, in der Wirkung lösten sie einen großen Schock aus. Menschen in der ganzen Welt wurde bewusst, wie viel Informationen Geheimdienste sammeln. Sie überlegten, was sie dagegen machen könnten. Gegenmaßnahmen werden in einem späteren Kapitel abgehandelt.

Viele bedrohliche Aspekte von Big Data wurden von Manning und Snowden nicht thematisiert.

Schmelztiegel für Daten

Kurz nach der Jahrtausendwende hat der Hardware-Hersteller Seagate die erste Terabyte-Harddrive auf den Markt gebracht – eine Entwicklung mit weitreichenden Folgen. Speicherkapazität hatte damit Preise und Größen erreicht, die kaum einen Kostenfaktor darstellten. Die alte Prognose, „niemand braucht mehr als 640 kB RAM“[20], wurde zu Makulatur. Explodierende Speicherkapazität hat die Welt endgültig verändert. Wenn es früher sinnvoll war, Informationen erst zu filtern, dann zu speichern, war es nunmehr sinnvoll, alles erst einmal zu speichern. Filtern kann man später, wenn die Technologie dazu erfunden wird.

2001 war auch das Jahr der Geheimdienste. Am 11. September wurden die US-Städte New York und Washington von einem kriegerischen Überraschungsangriff heimgesucht. Einer kleinen Gruppe fanatischer Islamisten war es gelungen, knapp 3.000 Amerikaner in ihrem eigenen Land zu ermorden.

Ohne Sprengstoff.

Ohne Schusswaffen.

Und ohne Vorwarnung.

Die Spionagedienste der Supermacht waren ahnungslos. Die Tätergruppe Al Kaida war ihnen bekannt, auch Anführer Osama Bin Laden. Aber niemand hatte ihnen eine derartige Aktion zugetraut. Die Attentäter waren unerkannt ins Land gereist und mit Teppichmessern und Tränengas an Bord gestiegen.

Das Frühwarnsystem hatte versagt, für die Spionagedienste Totalschaden. Man stellte fest, dass menschliche Quellen (*HUMINT*, „human intelligence“) unzureichend waren. Künftig wollte man mehr Gewicht auf elektronische Ausspähung (*SIGINT*, „signal intelligence“) legen. Rückblickend hätte man dort verdächtige Personen aufspüren können. Nötig waren eine vollkommene Renovierung und ein Relaunch. Man brauchte Systeme, die Flugbewegungen, Grenzübertritte, Ferngespräche und Internetkommunikation wirksam überwachen.

Man wollte wissen, wer ins Land reist. Und weshalb. Jedes Detail.

Gefragt war Big Data.

Die National Security Agency NSA sollte ihre Datenmassen und die Erkenntnisse daraus in einem lückenlosen Informationsaustausch mit anderen Nachrichtendiensten teilen. Und auch mit der Polizei.

Eine weitere Priorität war die Grenzüberwachung, in den USA eine ziemlich lange Strecke. Die Landgrenzen zu Kanada und Mexiko, kombiniert mit Küstenstreifen entlang zweier Ozeane, addieren sich zu einem knapp 32.000 Kilometer langen Kontrollbereich. Mit Grenzbeamten und Küstenwache ist das kaum zu bewältigen. Menschliche Kontrollen sollten durch vollautomatische maschinelle Überwachung ergänzt beziehungsweise gänzlich ersetzt werden.

Die heutige Grenzsicherung beginnt mit der Reisebuchung. Wer ins Land will, wird schon lange vor dem Abflug erfasst. Über Personenmerkmale, die in umfangreichen Fragebögen abgefragt werden: Ehestatus und Einreisetermin, Bankauskunft und Berufsausbildung, Krankengeschichte und Kreditkarten, Finanzverhältnisse und Führungszeugnis gehören alle dazu. Alle Angaben werden mit Vergleichsinformationen aus einer Vielzahl anderer Quellen abgeglichen. Auf Amerikas Gäste, die es ins Land schaffen, wartet ein biometrisches Vollprogramm.

„Smile!“ Das Gesicht wird fotografiert, Fingerabdrücke eingelesen, Augen gescannt. Womöglich wird auch der Unterleib mit den Röntgenaugen eines Ganzkörper-Scanners kurz unter die Lupe genommen.

Bei Letzterem gab es Ärger. Passagiere empörten sich über die Verletzung ihrer Intimsphäre. Aktivisten schrieben Proteste in Metallic-Farbe auf Intimstellen, damit sie bei der Durchleuchtung deutlich zu lesen waren. Außerdem stellten diverse Studien die Leistungsfähigkeit der Ganzkörper-Scanner infrage. Auf vielen Flughäfen wurden sie wieder abgebaut.

Die Daten von Anreisenden haben natürlich nur einen Sinn, wenn sie mit den Speichern der Spionagedienste verglichen werden. Das werden sie. Jede Antwort auf jedem Fragebogen von jedem Besucher, jedes freundlich lächelnde Touristengesicht, kommt hinzu.

Big Data wächst täglich weiter.

Grenzfälle

Bei der bisherigen Debatte in Deutschland konzentrierte sich die Kritik auf mitgeschnittene Telefongespräche und E-Mail-Texte. Faktisch ist dies nur ein kleiner Ausschnitt aus dem Repertoire der Geheimdienste. Personenmerkmale sind vielfältig. Erkennungswissenschaftliche Technologien zu deren Erfassung auch.

Jeder Mensch wurde von der Natur anders erschaffen. Er besitzt Eigenschaften, die genauso einmalig für seine Person sind wie der Fingerabdruck. Einige liegen auf der Hand.

Nicht nur Fingerkuppen haben Papillarleisten und Minutien, die ringförmige Abdrücke hinterlassen können. Auch die Fläche der Hand, der Hacken am Fuß oder sogar das Ohr kann von Kriminalisten zur Personenidentifizierung herangezogen werden. Nachrichtendienste entwerfen sogar Profile für die Geometrie von Fingern oder die Venen am Handrücken.

Die Firma Palm Secure zum Beispiel vermarktet einen Sensor, der eine Handfläche mittels Nah-Infrarot-Kamera abtastet. Weil das sauerstoffreduzierte Blut in Venen die Infrarotstrahlung absorbiert, wird ein detailliertes Muster der Venenstruktur mit fünf Millionen Punkten sichtbar. Nach Herstellerangaben kann das System einen Menschen mit einer Fehlerquote von eins zu zehn Millionen identifizieren.[21]

In der Akustik ist der Stimmabdruck einer Person ein wichtiges Merkmal. Es besteht zum einen aus den biometrischen Schwankungen der Stimmbänder, zum anderen aus dem unverwechselbaren Rhythmus der gesprochenen Wörter. Wenn nötig, können Sprachwissenschaftler mit weitergehenden Untersuchungen Dialekt, Betonung und Wortwahl identifizieren. Früher war diese Technologie ein Monopol des Staates, ein Werkzeug von Polizei und Nachrichtendiensten. Heute kann das jedes Smartphone.

Das Gesicht ist ein vertrautes Merkmal von Menschen. Jedes ist anders. Wir erkennen das meistens. Maschinen erkennen das immer. Die Entfernungen zwischen Nase und Oberlippe, Augenbraue und Haaransatz, Ohrläppchen und Kragenweite sind zu einer fein getunten Wissenschaft verfeinert worden. Die Software dazu heißt Gesichtserkennung.

Für sie wird das biometrische Passbild angefertigt – Mund zu, Augen auf, Kopf gerade. Besonders wichtig dabei: der blöde Gesichtsausdruck.

Einheitsnormen erleichtern maschinelle Erkennung.

Heute ist Biometrik überall. Wir gewöhnen uns an die kleinen Webcams, die bei Passkontrolle, Hotelempfang oder Autovermietung auf uns warten.

Mund zu, Augen auf, Kopf gerade.

Weltweit füllen wir die Datenbanken mit unserer Abbildung.

Mit Fingerabdrücken von uns.

Mit Iris-Scans von uns.

Die Überwachung ist allgegenwärtig. Und ziemlich unheimlich.

Wer in die Vereinigten Arabischen Emirate einreist, wird gleich am Flughafen mit der Technik konfrontiert. Bei der Passkontrolle warten die üblichen Webcams und Lesegeräte für Fingerabdrücke. Wer aber denkt, dass die Personenidentifizierung hier beginnt, täuscht sich.

Auf dem Weg vom Flugzeug zur Passkontrolle laufen Fluggäste an acht bis zehn weiteren Kameras vorbei. Durch die Gesichtserkennung werden Identität und Klassifizierung automatisch ermittelt und an die Passkontrolle weitergeleitet. Foto und Fingerabdruck an der Theke sind Formalitäten. Die Einreisebehörden wissen längst, wen sie vor sich haben.

Je wichtiger eine Zielperson ist, umso aufwendiger die Verfahren, die angewandt werden, um sie zu finden. Je größer die Datenbanken mit Personenmerkmalen, umso besser die Chancen.

Die Technologie der Gesichtserkennung ist nur ein Teil einer globalen Vernetzung, die uns mit Webcams, CCTV-Video und versteckten Kameras ständig observiert. Nationale Nachrichtendienste, Polizei und Privatfirmen arbeiten dabei oft Hand in Hand.

Mit der Hochleistungs-Gesichtserkennung kann man sogar Einzelpersonen auf einer Großdemonstration identifizieren, oder den Verdächtigen in der Menschenmenge einer Bahnhofshalle. Man kann sogar die Personen auf ihrem Weg durch das Gedränge weiterverfolgen. Einzelne Kameras können miteinander synchronisiert werden und eine Zielperson von Kamera zu Kamera über mehrere CCTV-Systeme hinweg

verfolgen. Mit sogenannter *Fusion-Software* kann eine Video-Überwachung sogar medienübergreifend mit anderen Systemen wie Auto-GPS oder Smartphone-Ortung synchronisiert werden.

Es wäre ein verhängnisvoller Fehler, wenn unsere Gesellschaft nur die Folgen einzelner Überwachungsprogramme betrachten würde. In der Vernetzung liegt die Gefahr.

Wenn wir die gesellschaftlichen Folgen einer bevorstehenden Überwachungsgesellschaft betrachten, wäre es ein grober Fehler, jede Maßnahme einzeln zu betrachten. Es ist nicht die einzelne Kamera am Straßenrand, der Sensor in einem RFID-Chip oder die Abhöranlagen in einer Barbie-Puppe, die eine Bedrohung darstellen. Es ist die geballte Kraft eines neuen Wesens, das alles überwachen – und kontrollieren – kann. Solange die Systeme getrennt bleiben, sind sie halb so gefährlich.

Die Entstehung gigantischer Datenmassen, die Geburt von Big Data, war eine gewaltige Entwicklung. Bis heute haben wir sie nicht verdaut. Und dennoch ist sie nur ein erster Schritt in der Entstehung eines gefährlichen neues Wesens, das uns vollkommen überlegen sein wird.

Sensorik und Software

Mit dem rasanten technologischen Ausbau der Grenzüberwachung sind ganze Wissenschaftszweige neu entstanden. Die Biometrik, die mit Stimmabdruck und Gesichtserkennung begann, ist heute ein vielseitiges Forschungsfeld.

Und ein lukratives.

Der Staat, so scheint es, kann nicht genug speichern. Täglich werden neue Eigenschaften des menschlichen Körpers entdeckt und katalogisiert – Körperbau und Kopfhaltung, Muttermal und Muskelbau, hübsche Tattoos und hässliche Narben. Alles wird protokolliert und in Big Data eingefüttert. Es gibt sogar orthopädische Fachleute, die die Gangart studieren und Personen an einem hinkenden Bein oder einer hängenden Schulter erkennen können. Es ist ein neues Fach in der Verhaltensforschung („gait recognition“) und gilt als ziemlich sichere Methode, um Personen zu identifizieren. Andere Forschungsbereiche vergleichen Proben von Körpergeruch, Mundgeruch und Fußschweiß.

Psychologen suchen Hinweise im Verhalten, bei Hobbys etwa, oder im Lebensstil. Ist man Schlipsträger oder Sportfan, Fernfahrer oder Frauenheld, Linkshänder oder Langstreckenläufer?

Es geht aber auch genauer.

Menschen haben ziemlich eindeutige Merkmale, von denen sie meist überhaupt nichts wissen. Ob man mit Zehn-Finger-System in eine Tastatur tippt oder mit Zwei-Daumen-Methodik in ein Smartphone, jeder hat seinen eigenen Stil. Und seinen eigenen Rhythmus. Experten können das heraushören. Und zuordnen. Die US-Firma Apple hat entdeckt, dass sie ihre User am Tipp-Rhythmus und an der Handhabung ihres iPhones erkennen kann.

Verhaltensbedingte Identifizierung ist ein weiteres Neugebiet in der Wissenschaft. Forscher nennen es „Behaviometrics".

Profile, die früher mit dem Eintrag in das Notizbuch eines Kripobeamten begannen – und meistens auch endeten –, werden heute in den endlosen Annalen von Big Data verewigt.

Augen und Ohren der Künstlichen Intelligenz

Automatische Sensoren sind heute die Augen und Ohren der modernen Überwachung. Sie sind erheblich leistungsfähiger als ihr menschlicher Gegenpart. Sensoren können weiter und besser sehen als Augen, auch bei Nacht. Sie können Infrarot und Radioaktivität erkennen, leiseste Geräusche hören und chemische Substanzen riechen.

Biometrik zieht Großunternehmen an. Damit ist viel Geld zu verdienen. Der Staat ist bereit, große Teile davon gern outzusourcen, zum Beispiel bei der Überwachung von Staatsgrenzen.

Heute ist sie hauptsächlich eine Sache der modernen Sensorik. Zunehmend wird sie vom Staat in die Hände von Privatunternehmen gegeben. IBM, spezialisiert auf Biometrik, Personenerkennung und Datenverwaltung, ist enger Partner des Department of Homeland Security, DHS. Die Firma Accenture leitet die *Smart Border Alliance* in den USA, einen Zusammenschluss diverser Spezialfirmen.

Fachgebiet: die Sammlung und Auswertung von Daten.

Gesamtetat: knapp 10 Milliarden Dollar.

In solchen Kreisen sind Daten nicht nur ein Thema für Fachsimpelei. Sie sind Ware. Es wird damit gehandelt, fleißig gehandelt – mal im Tausch, mal gegen Bares. Besonders wertvoll sind sie, wenn sie miteinander verschmelzen.

Eine der Lehren aus dem Attentat vom 11. September war die mangelnde Kooperation zwischen den US-Nachrichtendiensten. Viele Informationen, die zu einer Früherkennung der Attentäter und ihrer Absichten hätten führen können, lagerten in den Karteien einzelner Behörden – abgeschirmt, abgelegt, unzugänglich. Nicht mal der Auslandsdienst CIA war mit dem Inlandsdienst FBI datentechnisch vernetzt. Niemand hatte Zugang zu allen nötigen Informationen. Niemand war in der Lage, „The Big Picture" zu sehen, den wachsenden Zusammenhang, das bedrohliche Gesamtbild.

Datenbestände aus den diversen Bundesbehörden sollten schleunigst zusammengelegt werden, und – soweit es die Geheimhaltung zulässt – gemeinsam genutzt werden. Der Inlandsdienst FBI, der Auslandsdienst CIA, der militärische Nachrichtendienst DIA und andere relevante Bundesbehörden sollten teilen lernen.

Schmelztiegel für Spione

Fusion Centers wurden eingerichtet, wo vertrauliche Daten zusammenliefen. Unter dem umstrittenen „Freedom of Information Act" wurde ein undurchsichtiges Gebilde von Vollmachten und Sondergenehmigungen errichtet. Dazu zählen die berüchtigten „National Security Letters", die dem FBI Festnahmen und Durchsuchungen erlauben – ohne Haftbefehl, ohne Durchsuchungsbefehl, ohne Richter.

Bürgerrechtsorganisationen waren über die neuen Vollmachten für Strafverfolgungsbehörden entsetzt. Sie warnten vor der Vielzahl von neuen Behörden, die sich mit dem Kampf gegen Terror befassten. Allein im Bundesstaat Illinois waren es 91. Und sie warnten vor dem, was sie „Kriegsrecht in einem nicht erklärten Krieg" nannten.

Noch wichtiger – und bedenklicher – war das Verschmelzen staatlicher Datenbanken. Ein Informations-Smörgåsbord wurde aufgetischt. Alle Dienste wurden zum Festessen eingeladen.

Es waren aber keineswegs nur die großen Spionagebehörden, die von den neuen Anti-Terror-Gesetzen profitierten. Auch viele Dienststellen in der Provinz genossen neue Privilegien.

Im Bundesstaat Illinois erreichte die Zahl der Landesdienststellen, die sich mit Anti-Terror-Aufgaben befassten, eine Rekordhöhe. Und manch ein US-Dorfpolizist freute sich plötzlich über Hightech-Wunderwaffen, die sonst ausschließlich in den Arsenalen von CIA und NSA zu finden waren.

NSA-Technologie für die Dorfpolizei

Kleinstadt-Cops wurden plötzlich in der Lage versetzt, mit raffinierten Infrarotkameras die Marihuana-Farmen in Großstadtsiedlungen aufzuspüren, mit leistungsstarken Lauschgeräten die Handy-Gespräche von Kleinkriminellen mitzuschneiden und die Strafregister von Millionen von Menschen mühelos zu durchforsten.

Das bietet viele Vorteile in der Kriminalitätsbekämpfung.

Und verbirgt viele Gefahren für Bürgerrechte.

Es folgen ein paar Beispiele aus der Praxis.

Das Werkzeug der Wächter

WatchHound

Zu den neuen polizeilichen Wunderwaffen von heute zählt der kleine *WatchHound* („Wachhund") von Berkeley Veritronics in New Jersey. Als Funkempfänger im Taschenformat, der als Buch oder Wasserflasche getarnt werden kann, entdeckt das Gerät verbotene Funksignale jeder Art. Ob bei einer Klausurarbeit an der Uni oder dem Konzert eines Rockstars, im Gefängnis oder im Gerichtssaal, der kleine Hund spürt jede drahtlose Aktivität in Echtzeit auf. Er ortet Stimme, SMS-Text, sogar Handys im Standby-Modus. Er erfasst eingehende sowie ausgehende Kommunikation und protokolliert alles samt Mobil-Nummer und Uhrzeit.

Während der WatchHound für legitime Überwachungsaufgaben entwickelt wurde, könnte er auch für die Verfolgung von demokratischen Demonstranten und Dissidenten eingesetzt werden.

Stingray

Etwas ominöser ist der IMSI-Catcher *Stingray* der Harris Corporation. Seine Aufgabe ist es, einen Sendemast zu simulieren. Damit kann er alle Handys in der Umgebung zum Andocken locken, ihre Gespräche mitschneiden, ihre SMS-Texte speichern und womöglich den gesamten Speicherinhalt eines Smartphones ohne Wissen des Inhabers downloaden. Das Gerät kann Tausende von Mobilphones gleichzeitig anzapfen.

„Mit dem Gerät kann der Staat", so die Bürgerrechtsorganisation ACLU, „Signale durch Wände und Kleidungsstücke empfangen, um vielfältige Informationen über unbescholtene Menschen zu sammeln."

- In Florida hat eine Polizeidienststelle den *Stingray* über zweihundert Mal innerhalb eines Jahres eingesetzt – ohne einen einzigen Gerichtsbeschluss.

- Bei der Suche nach einem entführten Mädchen hat die Polizei in Colorado die Daten von mehreren Tausend Männern angezapft. Fünfhundert von ihnen wurden zu DNA-Proben aufgefordert.[22]
- Mit einem *Stingray* sammelte ein Sheriff in South Carolina sämtliche Daten aus vier mobilen Sendemasten. Es ging um die Aufklärung einer Serie von Autodiebstählen. „Wir brauchten so viele Informationen wie möglich", erklärte der Sheriff.
- In Miami begründete die Polizei den Kauf eines *Stingrays* damit, dass sie Demonstranten beim Welthandelstag überwachen wollte.[23]

Cellebrite

Cellebrite ist ein Gerät zur Sicherstellung von forensischen Beweismitteln. Der gesamte Inhalt eines Smartphones kann damit innerhalb von zwei Minuten kopiert werden. Die Profi-Version kann auch gelöschte, verschlüsselte und versteckte Daten lesen. Sie wird von Militär, Strafverfolgung und Nachrichtendiensten in über sechzig Ländern verwendet.

Cellebrite funktioniert so:
Gerät infiltrieren,
Sperre umgehen,
Code starten, um Flash zu lesen,
Datentransfer zu USB aktivieren,
Keine Spuren hinterlassen.

FinFischer/FinSpy

Überwachungssoftware der Trojaner-Produktfamilie *FinFischer/FinSpy* aus dem Hause Gamma wird häufig von staatlichen Institutionen verwendet. Sie ist ein offensives Spionage-System, vom Bundeskriminalamt getestet, und wird unter anderem gegen „Schurkenstaaten" wie Iran und Nordkorea eingesetzt. Billig ist es nicht. Allein die *Remote-Monitoring-Lösung* von FinSpy kostet um die 1,5 Millionen Euro. Dafür kann sie Gespräche abhören, Kontakte kopieren, Mikrofone aktivieren, Standorte verfolgen und sicherlich vieles mehr, was die Hersteller nicht öffentlich erzählen.

Natürlich werden solche Geräte in der Privatwirtschaft eingesetzt, sogar bei der katholischen Kirche. In Neapel war Priester Don Michele Madonna vom Texten und Telefonieren während des Gottesdienstes mächtig genervt. Mehrfach hatte er die Gemeinde aufgefordert, den Gebrauch von Handys in der Kirche zu unterlassen. Auf der Suche nach himmlischer Ruhe hat der genervte Geistliche in der Kirche einen Störsender installiert. Es funktionierte. Allerdings beschwerten sich Ladenbesitzer aus der Nachbarschaft, dass auch bei ihnen Laptops, Smartphones und Tablets gestört wurden.[24][25]

Google für Geheimdienstler

Das US-Unternehmen Raytheon ist für exotische Rüstungsgüter bekannt. Neben Sensorpaketen für Killerdrohnen, Exoskeletten für US-Infanteristen und Überwachungszeppelinen für die US-Marine hat Raytheon für die NSA eine besondere Software im Angebot – eine Suchmaschine für Spione. Das Programm heißt *RIOT* („Rapid Information Overlay Technology") und wird ausschließlich an Militärs, Nachrichtendienste und andere Sicherheitsbehörden verkauft. Die Leistung stellt Google in den Schatten.

Die Algorithmen sind für ihre enormen Informationsmassen ausgelegt – in der Fachsprache „Extreme-Scale Analytics". Die Geschwindigkeit ist atemberaubend.[26]

Tippt man den Namen einer Zielperson ein, spuckt die Software sofort eine vollständige Liste aller Telefonate – komplett mit gelben Landkarten-Pins – aus. In Sekundenschnelle werden alle Orte mit Datum und Uhrzeit angezeigt, an denen die Zielperson telefonisch eingeloggt war – komplett. Jedes Mal, wenn dieser Teilnehmer sein Telefon aktiviert, legt er eine Spur auf der Landkarte. Wie Brotkrümel im Märchenwald kann ein Nachrichtendienstler den Weg einer Zielperson nachverfolgen – nicht nur aktuell, sondern auch für Jahre, oder Jahrzehnte, rekonstruieren.

Die RIOT-Software kann mehr, viel mehr, wie zum Beispiel komplexe Eventketten. Geht Person A in das Café mit Person B, die sich mit Person C im Chat austauscht, die Bargeld an Person D übergibt, können