„Yes we scan!“

Was Edward Snowden zu erwähnen vergaß

Grazyna Fosar und Franz Bludorf

Skyline von Salt Lake City bei Nacht.

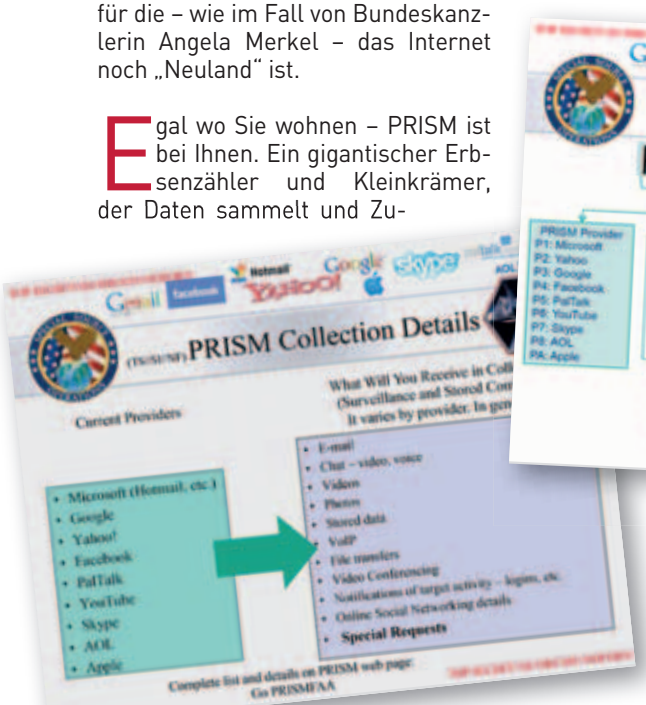
Ein Sommer neigt sich dem Ende zu. Für viele Menschen war er sehr aufregend. Ein Mann hatte dafür gesorgt. Edward Snowden. Seine mehrteilige Sitcom sorgte auf der ganzen Welt für Empörung. „Von meinem Schreibtisch aus hätte ich Dich, Deinen Steuerberater, einen Bundesrichter und sogar den Präsidenten der Vereinigten Staaten abhören können, wenn ich nur seine private E-Mail kennen würde." So die Aussage des Ex-IT-Spezialisten der NSA, dessen Enthüllungen während seiner Flucht rund um den Globus wochenlang die Medien beherrschte. Politiker empörten sich. Diplomaten empörten sich. Journalisten empörten sich. Die Bevölkerung empörte sich – über Fakten, die man im Grunde seit Jahren kannte. Matrix3000 etwa berichtete bereits 2008 – und schon damals nicht zum ersten Mal – über die weltweiten Abhörpraktiken des größten amerikanischen Geheimdienstes.

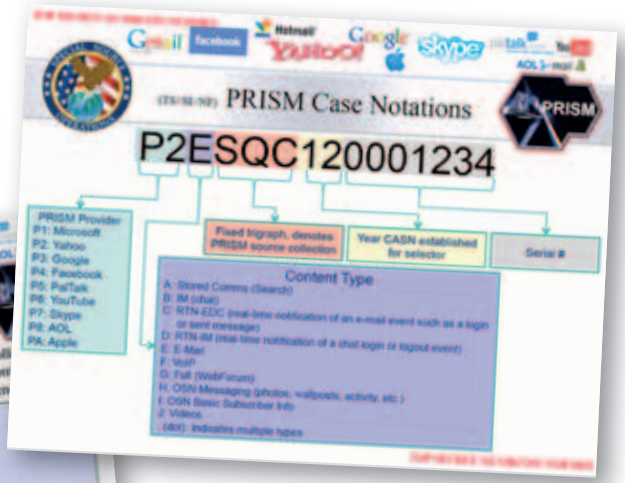
Datenschnüffler PRISM

Bei PRISM, so erfuhr die erschrockene Öffentlichkeit, handelt es sich nicht um ein Prisma, sondern um ein *"Planning Tool for Resource Integration, Synchronization, and Management"*, ein komplexes Computerprogramm, mit dessen Hilfe die NSA seit Jahren die ganze Welt überwacht und dabei unvorstellbare Datenmengen speichert. Ohne Kontrolle durch Parlament oder Justiz. Ganz einfach so, weil sie es können. Und die Regierungen der Welt behaupteten, nichts von alledem gewusst zu haben, was kaum glaubhaft erscheint, selbst bei denen, für die – wie im Fall von Bundeskanzlerin Angela Merkel – das Internet noch „Neuland" ist.

Egal wo Sie wohnen – PRISM ist bei Ihnen. Ein gigantischer Erbsenzähler und Kleinkrämer, der Daten sammelt und Zusammenhänge erkennt, die scheinbar nichts miteinander zu tun haben. Sophie stöbert im Internet und sieht sich ein paar Seiten an, sie simst an ein paar Freunde, bezahlt etwas mit ihrer Kreditkarte, und in diesem Moment weiß PRISM bereits, dass sie im dritten Monat schwanger ist, ohne verheiratet zu sein, dass sie über ein Kreditkartenlimit von 5000 Euro verfügt und vor einem Jahr mit einem Freund telefoniert hatte, der ein paar Wochen in Pakistan war und dort mit einem Mann über Musik gesprochen hatte, dessen Bruder in Verdacht steht, mit dem Fernsehsender Al Jazeera in Verbindung zu stehen. Sophie hat bei der NSA den Status „Rot".

Hat PRISM etwa die Aufgabe, harmlose Bürger auszuspionieren? Das Problem ist viel größer. Die Überwachung der Bürger ist nur eine kleine Nebenbeschäftigung – und natürlich ein dankbarer Aufhänger für eine Pressekampagne im Sommerloch.



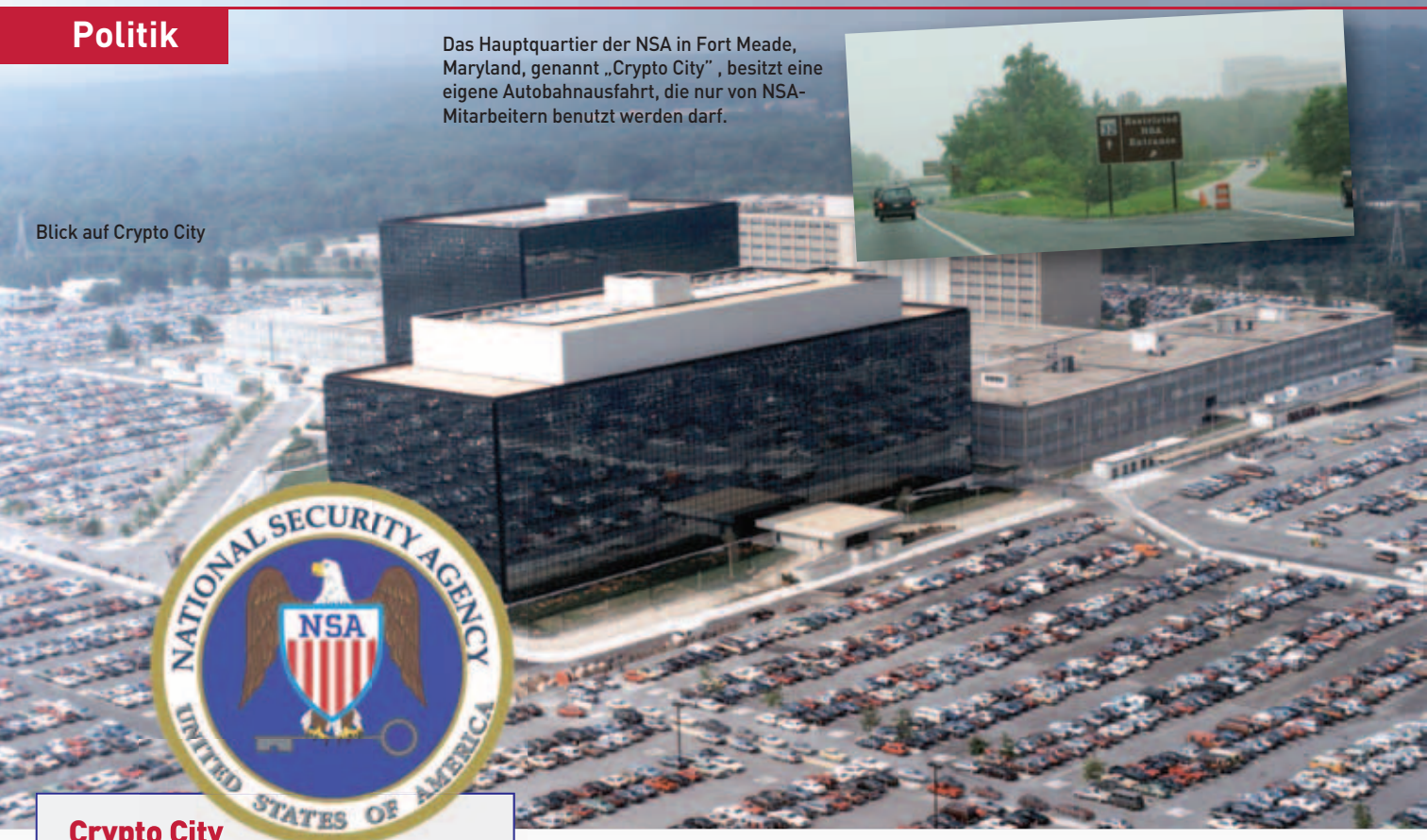


Diese Bilder entstammen einer Powerpoint-Präsentation zum PRISM-Projekt, die Edward Snowden veröffentlichte. Sie zeigen, welche Dienstleistungen welcher Internet-Anbieter von der NSA angezapft werden und wie man sie anhand der Fallaktennummer schnell identifizieren kann.

Going Dark – Aufbruch ins Dunkle

Aber bleiben wir erst einmal bei der Nebenbeschäftigung. Bereits unmittelbar nach dem 11. September 2001 startete die Bush-Administration mit geradezu hektischen Maßnahmen zur Überwachung der Bevölkerung, selbst im eigenen Lande. *Total Information Awareness* hieß das Projekt, das schließlich 2003 vom Kongress gekippt wurde (siehe Matrix3000 Band 18). Diese Form der staatlichen Paranoia ging selbst den Senatoren zu weit.

Sogar in der damaligen aufgeheizten Atmosphäre gab es NSA-Insider, die sich von der allgemeinen Überwachungs-Hysterie nicht anstecken ließen. Zu ihnen gehörten der Pilot und IT-Spezialist Thomas Drake und der Mathematiker William Binney, ein altgedienter Kryptographie-Spezialist. Die beiden Insider schlugen ihren Chefs vor, man könne sich zur Terrorabwehr auf das Anzapfen der Glasfaserkabel des internationalen Datenverkehrs beschränken, sobald sie das amerikanische Festland erreichten, oder auch auf hoher See mit Hilfe von Atom-U-Booten. Das würde eine überschaubare Anzahl zu überwachender Knotenpunkte bedeuten. Drake und Binney entwickelten sogar eine passende Software, die diese Aufgabe preisgünstig erledigen konnte. Man schenkte ihnen kein Gehör



Das Hauptquartier der NSA in Fort Meade, Maryland, genannt „Crypto City" , besitzt eine eigene Autobahnausfahrt, die nur von NSA-Mitarbeitern benutzt werden darf.

Blick auf Crypto City

Crypto City

Das Hauptquartier der National Security Agency in Fort Meade, Maryland, trägt auch den Spitznamen „Crypto City". Die schwarze Glasfassade des Hauptgebäudes bildet nur die äußerste Schale. Darunter befindet sich das wahre Gebäude, dessen Außenhaut aus Kupfer besteht. Die Fenster sind mehrschichtig aufgebaut: Zunächst eine Schicht Panzerglas, darunter 12,5 cm geräuschdämpfender Raum, eine dünne Kupferabschirmung und eine innere Scheibe. Diese spezielle Abschirmungstechnik mit Kupfer trägt den Codenamen TEMPEST. Sie bildet eine ausgeklügelte Schutzmaßnahme und bewirkt, dass keine Geräusche oder elektromagnetischen Signale das Gebäude verlassen können.

und installierte statt dessen für Milliarden von Dollars in jedem größeren Telekommunikationsknotenpunkt der USA geheime fensterlose elektronische Monitoring Rooms, sogenannte Switches. Codename: Stellar Wind (Sternenwind). Damit war von Anfang an klar – es ging nicht nur darum, äußere Bedrohungen abzuwehren, sondern die Maßnahmen richteten sich gegen die normale Bevölkerung, sogar im eigenen Land. Da dies natürlich illegal war – die NSA darf laut Gesetz nur im Ausland tätig werden, ebenso wie die CIA -, erarbeitete man auch von Anfang an die notwendigen Grundlagen, um die Rechtsprechung des Foreign Intelligence Surveillance Court (US-Gerichtshof zur Überwachung der Geheimdienste) zu umschiffen.

Der Widerstand der Politik währte nicht lange. Noch vor Ende der Bush-Administration verabschiedete der Senat 2008 den FISA Amendments Act, ein Gesetz, das diese Praktiken im Nachhinein de facto legalisierte und den Verantwortlichen, sowohl auf seiten der Geheimdienste als auch auf seiten der Telekom-Anbieter, rückwirkend Immunität garantierte. Wer immer sich hingegen der allgemeinen Überwachungswut entgegenstellte, wurde „gekreuzigt", wie es der NSA-Experte James Bamford ausdrückte. William Binney wurde von einem Rollkommando des FBI mit vorgehaltener Waffe unter der häuslichen Dusche verhaftet. Auch Thomas Drakes Appartement wurde durchsucht, und da man Geheimdokumente bei ihm fand, wurde er wegen Spionage angeklagt. Er hatte noch Glück, dass er anstelle der angedrohten 35 Jahre nur ein Jahr auf Bewährung erhielt und heute wieder ein freier Mann ist. Beide, Binney und Drake, erklärten in diesem abenteuerlichen Sommer die Aussagen Edward Snowdens für zutreffend und authentisch.

Anfang 2013 dann ein erneuter Versuch der NSA, Unterstützung für ihre sinistren Überwachungspläne zu erhalten. Unter dem Titel „Going Dark" wandte man sich erneut an den Kongress mit der Befürchtung, die existierenden Abhörmethoden würden der zunehmenden Datenflut nicht mehr standhalten. Daher müsse man die Daten unmittelbar und direkt an der Quelle abgreifen, also bei den wichtigsten Internet-Dienstanbietern wie Google, Apple, Microsoft oder Facebook. Der Kongress, so der Wunsch der NSA, solle den Geheimdiensten einen Blanko-Scheck ausstellen, diese Daten ohne gerichtliche Kontrolle in Realzeit bei den genannten Anbietern abgreifen zu können. Derartige Bestrebungen gehen übrigens über die Grenzen der USA weit hinaus. „Big Data" stand auf der Tagesordnung der Bilderberg-Konferenz im Juni 2013 in Watford, England (siehe auch Matrix3000, Band 76), und sinnigerweise waren Vertreter großer Internetkonzerne wie Google, Amazon und Microsoft als Teilnehmer geladen.

Sobald die Kommunikationsdaten eines Telefonats oder eine E-Mail eines x-beliebigen Bürgers erst einmal gespeichert sind, beginnt das *data mining*, also auf gut Deutsch das

Buddeln nach Informationen im Datensumpf. Neben Verbindungsdaten, E-Mail-Texten und Gesprächsinhalten werden auch finanzielle Transaktionen, Reisedaten, Bankauszüge, Zollbescheinigungen, ja sogar Kassenquittungen von Buchhandlungen gespeichert und zueinander in Beziehung gesetzt. Auf diese Weise kann die NSA ein mehr und mehr detailliertes Bild vom Leben jedes Menschen zeichnen. Jeder ist ein Target.

Deep Web – Jenseits des Internet

Diese ganze Überwachungs- und Datensammelwut der Geheimdienste hat Dimensionen angenommen, die für den Normalbürger unvorstellbar sind. Und doch ist und bleibt dies nur eine kleine Nebenbeschäftigung. Denn im Grunde gibt es noch etwas, was die Geheimdienste viel mehr interessiert, und das ist „Deep Web" – die ganze Welt der gespeicherten Computerdaten und internen Netzwerke außerhalb des öffentlich zugänglichen Internet. Dort befinden sich die eigentlichen Schatzkammern: Passwortgeschützte Dateien, Regierungskommunikationen, nichtkommerzieller Datenaustausch zwischen vertrauenswürdigen Partnern, Regierungsberichte, Datenbanken, eben die wirklichen „Big Data", deren Volumen das des Internets um Größenordnungen übersteigen.

Und das war die Geburtsstunde von etwas wirklich Großem, das sogar den beängstigenden Datenschnüffler PRISM klein und harmlos aussehen lässt. Ein Datencenter, das eine Datenspeicherkapazität in der Größenordnung von Yottabytes benötigt, eine Zahl, die für die meisten Menschen nicht mehr vorstellbar ist. Für die nächsthöhere Größenordnung gibt es noch nicht einmal einen Namen. Ein Yottabyte, das ist eine Billion Terabyte, also eine Billion von solchen Festplatten, wie Sie vermutlich auch eine in Ihrem PC haben.

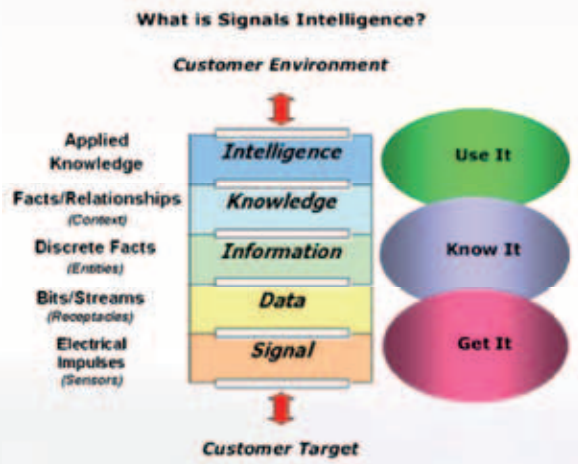
Zum Vergleich: Das gesamte Wissen, das die Menschheit seit ihren Anfängen bis zum heutigen Tage angesammelt hat, beläuft sich nach Schätzungen auf etwa 5 Millionen Terabyte. Die NSA glaubt das 200.000fache an Speicherkapazität zu benötigen. Das heißt, die Jungs haben etwas vor, das sich näher zu betrachten lohnt. Das Ganze spielt sich im Nirgendwo der amerikanischen Provinz ab, am südlichen Stadtrand von Salt Lake City im Bundesstaat Utah.

„Yes we scan!"

Bluffdale. Vom Großen Salzsee weht eine sanfte, trockene Brise hinüber in den kleinen Vorort der Mormonenstadt Salt Lake City. Hierher kamen vor 160 Jahren die ersten Siedler dieser Religionsgemeinschaft, um in der Abgeschiedenheit die Glaubenslehren zu entschlüsseln, die ihnen ihr Gott durch den Religionsstifter Joseph Smith offenbart hatte.

> **„Amerika hat derzeit keine funktionierende Demokratie".**
>
> Jimmy Carter, US-Präsident 1977-1981, Friedensnobelpreisträger

Heute kommen wieder geheimnisvolle Newcomer in diese Gegend. Auch sie suchen die Abgeschiedenheit, und auch sie wollen etwas entschlüsseln. Aber damit sind die Gemeinsamkeiten auch schon erschöpft. In Bluffdale wurde in den letzten Jahren ein gewaltiges Computerzentrum für die NSA errichtet, das Utah Data Center. Im September 2013 soll es in Betrieb gehen. Für den Gebäudekomplex, der fünf Mal größer als der Kongress in Washington ist, mussten eigens die Stadtgrenzen erweitert werden.



Oben: Informationsgewinnung bei SIGINT-Operationen (Quelle: NSA). Siehe dazu auch den Insert "Empfangen - Erkennen - Benutzen" auf Seite 12.

Heute beherbergt das NSA-Hauptquartier in Ford Meade, Maryland, insgesamt drei Dienststellen: Die National Security Agency, den Central Security Service und das US Cyber Command

Rechts: Das weltweite Spionagenetzwerk der NSA. Alle Rohdaten von Außenstellen, Satelliten etc. laufen zunächst im Utah Data Center zusammen und werden bei Bedarf an die Multiprogram Research Facility in Oak Ridge, Tennessee, weitergeleitet. Die Endresultate liefert das UDC dann an das NSA-Hauptquartier in Fort Meade, Maryland, von wo aus sie an die ursprünglichen Auftraggeber, z. B. Weißes Haus, CIA, Pentagon, weitergegeben werden.

Das Utah Data Center ist der letzte und ultimative Stein in einem gewaltigen Puzzle, das dazu dient, die gesamte Kommunikation der Welt abzugreifen, zu speichern und auszuwerten, und zwar in Realzeit. Der Gebäudekomplex hat die Kleinigkeit von 2 Milliarden Dollar gekostet. Das UDC kann sich selbst unterhalten, es besitzt ein eigenes Kraftwerk und Treibstofftanks, die die Stromversorgung im Krisenfall drei Tage aufrechterhalten können. Und das, obwohl die gigantischen Computeranlagen einen gewaltigen Energiehunger haben – 65 Megawatt! Der Unterhalt des Data Center wird pro Jahr etwa 40 Millionen Dollar verschlingen.

Es ist mehr als nur ein Datencenter, wie ein hoher Geheimdienstoffizier betonte, denn die Hauptaufgabe des UDC wird es sein, Codes zu knakken. Und zwar solche, die bislang als nicht zu knacken galten. Als vor einigen Jahren die Daten bei der NSA stetig zu fließen begannen, machte man eine erschreckende Feststellung. Die Geheimdienstler waren in der gleichen Situation, wie sie einst Jorge Luis Borges in seiner „Bibliothek von Babel" beschrieb. Sie hatten praktisch das gesamte Wissen der Welt gespeichert, konnten aber das meiste davon nicht lesen, weil es verschlüsselt war. Moderne Verschlüsselungsalgorithmen mit 128 oder gar 256 Bit, wie sie die NSA als Standard für ihre eigenen Geheimdokumente verwendet, sind mittlerweile allgemein zugänglich und stehen nicht nur Regierungen anderer Staaten zur Verfügung, sondern auch dem einzelnen privaten Computerbenutzer, so er will.

Einen 128-Bit- oder 256-Bit-Codierschlüssel mit Hilfe der alten Hackertechnik „Brute Force" zu knacken (d. h. den Computer so lange alle Zeichenkombinationen ausprobieren zu lassen, bis der Schlüssel erraten ist), dazu würden selbst modernste Supercomputer mehr Zeit benötigen, als das Universum alt ist. In ihrer Verzweiflung taten die NSA-Strategen das, was sie eigentlich immer tun – sie forderten mehr Geld vom Kongress, um neue Computer und neue Analyseverfahren zu entwickeln. Und sie bekamen es natürlich.

Zwei Wege können aus dem Dilemma herausführen, eine gewaltige Datensammlung zu besitzen, die man nicht lesen kann. Der eine ist es, ganz einfach einen so schnellen Computer zu bauen, dass er mit Hilfe von „Brute Force" die Schlüsselworte eben doch etwas schneller knacken kann. Prinzipiell sicher nicht unmöglich, aber nicht von heute auf morgen zu schaffen. Der zweite Weg ist etwas knniffliger und spricht eher die kreativen Talente von Geheimdienstlern an. Um die verschlüsselten Daten einer Person leichter dechiffrieren zu können, versucht man einfach, noch mehr davon zu sammeln. Das klingt absurd, ist aber durchaus plausibel. Wenn man davon ausgeht, dass in den Daten Texte aus der menschlichen Sprache verschlüsselt sind, so lassen sich auch in dem unlesbaren verschlüsselten Kauderwelsch Sprachmuster entdecken, und zwar um so leichter, je mehr Material man zur Verfügung hat. Auf diese Weise kann man nach und nach versuchen, die Texte zu dechiffrieren. Dazu braucht man nur viele, viele Computer, viele Experten und viel Zeit. Das alles bietet das neue Superzentrum von Bluffdale zur Genüge.

Um den ersten Weg, den Bau eines genügend schnellen Supercomputers, weiterzuverfolgen, müssen wir den Schauplatz wechseln. In Utah benutzen sie die Computer nur, gebaut werden sie woanders. Die, von denen wir reden, werden natürlich an einem

Empfangen – Erkennen – Benutzen

Wenn die NSA von einer Regierungsstelle einen Abhörauftrag erhält, dann beginnen die zuständigen Agenten damit, die Kommunikationskanäle des gewünschten Zielobjekts (Customer Target) anzuzapfen.

Dadurch bekommen sie streng genommen erst einmal nur ein physikalisches Signal herein. Im ersten Auswertungsschritt werden aus diesen elektromagnetischen Impulsen Daten gewonnen – im digitalen Zeitalter hauptsächlich Ströme von Bits.

Diese Daten repräsentieren natürlich eine gewisse Information, z. B. den Inhalt eines Gesprächs, das die Zielperson führt und dessen Inhalt die NSA ihrem Auftraggeber verfügbar machen soll.

Die Bitströme müssen also in Informationen verwandelt werden, wobei in der Regel auch kryptographische Methoden zum Einsatz kommen, da speziell Regierungskommunikationen ja oft verschlüsselt sind. Dadurch gewinnt man zunächst einmal sogenannte „diskrete Fakten"; also im Moment noch zusammenhanglos im Raum stehende Einzelinformationen. Indem die NSA-Experten zwischen diesen Einzelinformationen Verbindungen herstellen und sie in einen konkreten Kontext einbinden, wird daraus Wissen. Der letzte Schritt ist es dann, mit Hilfe dieses gewonnenen Wissens die Frage des Auftraggebers zu beantworten.

Diesen Prozess fasst die NSA zu dem werbewirksamen Slogan zusammen: „Get it – Know it – Use it", oder frei übersetzt: „Empfangen – Erkennen – Benutzen".

In der Nähe von Bluffdale, Utah, wurde das neue Utah Data Center der NSA gebaut.

Das Utah Data Center ist Tag und Nacht streng bewacht

„Wir sagen ihnen nicht alles, was wir machen oder wie wir es machen – aber jetzt wissen sie es.“

NSA-Direktor Keith B. Alexander über die Deutschen

Der größte Teil der Multiprogram Research Facility in Oak Ridge, Tennessee, ist öffentlich zugänglich. Er dient hauptsächlich dazu, die Existenz der supergeheimen Forschungsanlage der NSA (Building 5300) auf dem Gelände zu verschleiern.

Die Multiprogram Research Facility in Oak Ridge, Tennessee.

supergeheimen Ort gebaut, an einem Ort, der im Grunde nicht existiert. Er befindet sich auf historischem Grund.

Building 5300

In Oak Ridge, einem kleinen Ort bei Knoxville, Tennessee, wurde im Zuge des Manhattan-Projekts in den vierziger Jahren zum ersten Mal waffentaugliches Uran-235 für die erste Atombombe isoliert. Und ein Ort, der sich einmal zur Geheimhaltung eignete, ist wiederverwendbar. Noch heute steht am Ortsrand von Knoxville ein Schild mit der Aufschrift: *„What you see here, what you do here, what you hear here, when you leave here, let it stay here."* (Was du hier siehst, was du hier tust, was du hier hörst, wenn du hier fortgehst, lasse es hier.) Und der Satz gilt noch immer.

An diesem Ort errichtete – ganz unverdächtig – das US-Energieministerium das Oak Ridge National Laboratory, um neue Supercomputer zu entwickeln. Der größte Teil des Areals ist unklassifiziert und den Wissenschaftlern sowie der Öffentlichkeit zugänglich. Hier hat man in Zusammenarbeit mit dem Computerhersteller Cray den neuen Supercomputer XT5 entwickelt. Aufgrund seiner Geschwindigkeit haben ihm die Techniker den Spitznamen Jaguar verliehen, denn er soll 1,75 Petaflops leisten, d. h. 1,75 Billiarden Flops (Flops = Floating Point Operations, ein Maß für die Anzahl der mathematischen Berechnungen pro Sekunde). Das hört sich gewaltig an, reißt aber einen Insider nicht vom Stuhl. Der offiziell zugängliche Teil des Oak Ridge National Laboratory erfüllt im Grunde nur zwei Ziele. Zum einen soll die Daseinsberechtigung der gesamten Einrichtung glaubwürdig vermittelt werden. Zum zweiten dient es der Geldbeschaffung beim Kongress. Die Cray XT5 ist nämlich derzeit nur der drittschnellste Rechner der Welt. Japan und China haben je einen schnelleren. Grund genug, dem Zentrum weitere Millionen an Steuergeldern zuzuschanzen. Und die werden sofort weitergeleitet an Leute, die in einem Gebäude arbeiten, das im Grunde gar nicht existiert: Building 5300.

Diese Halle, die eher an einen riesigen Supermarkt erinnert, darf nur betreten, wer eine hohe Security Clearance (Sicherheitsfreigabe) hat, denn in Building 5300 bastelt die NSA an ihrem eigenen Superrechner, von dem niemand etwas wissen darf, nicht einmal der Kongress, und der eines Tages in Utah sein volles Potential entfalten soll. Bis 2018 soll der Prototyp eine Geschwindigkeit von einem Exaflop erreichen, das sind 1000 Petaflops, also das Tausendfache eines Großrechners für Normalsterbliche. Inoffiziell peilt man allerdings dann nochmals einen weiteren Faktor 1000 an, d. h. Endziel ist 1 Yottaflop, was dann der Rechenleistung von einer Million Cray-Supercomputern entsprechen würde. Mit solch einem Ding hofft man, in überschaubarer Zeit auch lange Verschlüsselungscodes knacken zu können. Keine Geheimnisse mehr!

Geld dafür wird nahezu unbegrenzt vorhanden sein. Für Barack Obama haben IT-Technologien und Cybersicherheit einen hohen Stellenwert in der Sicherheitspolitik. Während er den klassischen Verteidigungsetat immer wieder kürzt (was ihm Sympathiepunkte einbringt), macht er für diese Bereiche sogar zusätzliche Mittel locker. Cybersicherheit – das suggeriert, es würde darum gehen, Hackern und Cyberterroristen das Handwerk zu legen. Wer würde etwas dagegen haben, so etwas zu tun? Nur braucht man dafür kein Utah Data Center. Bei der Grundsteinlegung in Utah war niemand vom Department of Homeland Security anwesend, das doch eigentlich für die Cybersicherheit zuständig ist. Die NSA war dort unter sich. In Utah geht es nicht um Datenschutz, sondern um Sammeln, Analysieren und Speichern.

Edward Snowdens Auftrag

Wie kann man Edward Snowdens Odyssee im Kontext aller dieser Fakten einordnen? Für viele Menschen ist er ein Held. Für manche ist er ein Verräter. Für noch andere ein Superagent. Ein moderner Robin Hood. Höchstwahrscheinlich ist er von alledem etwas. Vor allem aber ist er ein Mensch, der eine wichtige Aufgabe erfüllt hat. Er sollte die Aufmerksamkeit der Welt auf die Nebenbeschäftigungen der NSA mit dem Programm PRISM lenken. Dazu brauchte er natürlich eine Geschichte, die sich pressewirksam vermarkten ließ.

Das weitere Schicksal Edward Snowdens ist offen. Die wahren Ziele der NSA, „Going Dark", bleiben für die Weltöffentlichkeit eher im Hintergrund und fast undurchschaubar. Irgendwann haben wir vermutlich alle den Status „Rot". ■

Die Autoren haben in mehreren ihrer Bücher die Thematik der Überwachung und Kontrolle der Bevölkerung behandelt:
Fosar/Bludorf: Welt am Limit. Peiting 2011.
Fosar/Bludorf: Der Geist hat keine Firewall. München 2009.
Fosar/Bludorf: Top Secret Umbra. Marktoberdorf 2006.