Das jüngst bekannt gewordene Internetüberwachungsprogramm Prism ist nur die Spitze des Eisbergs. Seit Ende des Zweiten Weltkriegs wird die internationale Kommunikation systematisch von spezialisierten Geheimdiensten abgehört. Mit dem technischen Fortschritt wuchs auch das Ausmaß der Überwachung rasant an. Heute betreibt wohl jedes bedeutende Land ein eigenes Abhörprogramm, gegen das die Stasi wie ein graues Relikt aus der Vorzeit wirkt. Die USA sind in Sachen Überwachung jedoch eine Klasse für sich. Der Staat, der stets so tut, als habe er einen Patent auf den Begriff „Freiheit", hat heute ein digitales Überwachungssystem, das jeder orwellschen Totalitarismusphantasie Ehre macht. Wer glaubt, es ginge dabei nur um die „Terrorismusbekämpfung", beleidigt dabei die Geschichte durch einen Mangel an Phantasie. Von **Jens Berger**.

Dieser Beitrag ist auch als Audio-Podcast verfügbar.

http://www.nachdenkseiten.de/upload/podcast/130702_Orwell_2_Punkt_0_NDS.mp3

Podcast: Play in new window | Download

Seit es möglich ist, transatlantische Telegramme zu verschicken, lesen die Geheimdienste der USA mit. Schon 1919 machten die US-Militärs Kopien von Telegrammen und ließen sie von der „Black Chamber", der ersten Vorgängerorganisation der NSA, auswerten. 1921 erzielten die Kryptoanalytiker der „Black Chamber" ihren ersten großen Erfolg, als es ihnen gelang, die verschlüsselten Telegramme der japanischen Delegation bei der Washingtoner Flottenkonferenz zu entschlüsseln. Die „Black Chamber" wurde jedoch bereits zehn Jahre nach ihrer Gründung vom damaligen US-Außenminister Stimson geschlossen. Seine bemerkenswerte Begründung: „Gentlemen do not read each other's mail". Doch die Phase der Zurückhaltung währte nicht lange. Nach dem Zweiten Weltkrieg gingen die USA in die Überwachungsoffensive und als die NSA 1952 offiziell als eigenständiger Geheimdienst gegründet wurde, konnte sie auf eine fortschrittliche Überwachungsinfrastruktur zurückgreifen, die während des Zweiten Weltkriegs von den Militärs geschaffen wurde.

Von den Anfängen zu Echelon

Seit 1945 kontrollierten die NSA und ihre Vorgänger den Kabelverkehr der großen internationalen Telekommunikationsunternehmen wie RCA Global, ITT World Communications und Western Union. Was als Sammlung von Papierkopien begann, entwickelte sich schon bald zu einer Sammlung von Magnetbändern und schließlich zu einer direkten Netzwerkverbindung zwischen den Überwachungszentren und den internationalen

Kommunikationsknoten. Da der Unterhalt eines weltweiten Überwachungssystem nicht nur teuer, sondern auch diplomatisch nicht problemlos ist, schlossen sich kurz nach dem Zweiten Weltkrieg die Geheimdienste der USA, Großbritanniens, Kanadas, Australiens und Neuseelands zu den sogenannten „five eyes“ (offiziell: UKUSA-Agreement) zusammen. Dies hatte zudem den Vorteil, dass man auch seine eigenen Bürger überwachen konnte. Auch wenn die Auslandsaufklärung zu den originären Aufgaben von Geheimdiensten gehört, ist die Arbeit im Inland doch den meisten Diensten gesetzlich verboten. Wenn nun aber die USA britische Bürger abhört und die Briten amerikanische Bürger, so ist dies auf den ersten Blick legal. Dies ändert sich jedoch, wenn die Daten systematisch ausgetauscht werden. Wo kein Kläger ist, ist jedoch auch kein Richter und es versteht sich von selbst, dass diese Operationen unter Ausschluss der Öffentlichkeit durchgeführt wurden.

Echelon – Lauschangriff auf den Freund

Das erste weltumspannende Abhörsystem nach modernen Kriterien wurde von den UKUSA-Staaten unter dem Namen „Echelon“ ins Leben gerufen. Über dieses System mit seinen rund zweihundert Funkstationen wurde seit den 1970ern vor allem die weltweite Satellitenkommunikation abgehört – und dies betraf in der Zeit vor dem Glasfaserkabel einen Großteil der internationalen Telefongespräche und Telefax- sowie Internetverbindungen. Wer meint, dass das Internet das erste globale Computernetzwerk sei, irrt. Als erstes weltweites TCP/IP-Netzwerk ging das Kommunikationsnetzwerk der UKUSA-Staaten in Betrieb, um die Daten der überseeischen Abhörstationen sicher und schnell in die NSA-Zentrale zu befördern und den Informationsaustausch der beteiligten Geheimdienste zu gewährleisten. Schließlich wussten die Dienste bereits damals ganz genau, dass jeder Kommunikationsweg, den man nicht selbst lückenlos kontrolliert, unsicher ist.

In Zeiten des Kalten Krieges war die Hauptaufgabe des Echelon-Systems das Abhören „feindlicher“ Kommunikationswege. Da die Technik für eine umfassende Speicherung und Auswertung der abgehörten Daten damals noch nicht zur Verfügung stand, arbeitete man mit Listen, auf denen bestimmte Schlüsselwörter geführt wurden. Besonders interessante Personen, Unternehmen und Einrichtungen wurden ebenfalls auf einer speziellen Liste geführt. Ihre Kommunikation wurde dann von den Diensten lückenlos protokolliert und gespeichert. Wer „Freund“ und wer „Feind“ ist, verschwamm jedoch auch damals schon. So wurden beispielsweise bereits in den1970ern Kritiker des Vietnam-Kriegs, wie die Schauspielerin Jane Fonda, und Bürgerrechtsaktivisten der Black-Power-Bewegung systematisch durch die NSA bespitzelt, obgleich die Kommunikationsüberwachung von Inländern eigentlich verboten ist.

Mit dem Ende des Kalten Krieges war Echelon eigentlich überflüssig, schließlich gab es ja keinen „Feind“ mehr. Die Büchse der Pandora war jedoch längst geöffnet und ein derart verlockendes Angebot generiert stets auch eine Nachfrage. 1992 erklärte George Bush in der Nationalen Sicherheitsdirektive 67 auch die Wirtschaftsspionage zu den Operationsbereichen, denen geheimdienstliche Priorität zugewiesen wurde. Fortan drehte man die Antennen sinnbildlich einfach um und lauschte nicht mehr nur im Osten, sondern vor allem in den verbündeten Industriestaaten. Davon waren lediglich die UKUSA-Staaten selbst ausgenommen, sämtliche andere Staaten, wie auch Deutschland, zählten abhörtechnisch nicht zu den Verbündeten sondern zu den Zielen. Daran hat sich bis heute nichts geändert, wie die aktuellen Veröffentlichungen des NSA-Whistleblowers Edward Snowden belegen.

Ein solches Ziel „war“ beispielsweise die japanische Autoindustrie. Wie bei der Washingtoner Flottenkonferenz wusste die amerikanische Delegation auch bei den 1995 stattfindenden Genfer Verhandlungen über Autoexporte genau über die Anweisungen der japanischen Delegation Bescheid – Echelon sei Dank. Welch´ glückliche Fügung, dass die NSA auch im bayerischen Bad Aibling eine der größten Abhörstationen außerhalb der USA betrieb.

Es ist unbekannt, ob die NSA in diesen Zeiten Drogen- oder Waffenhändler zur Strecke gebracht hat. Fest steht jedoch, dass sie in mindestens drei Fällen aktiv Wirtschaftsspionage gegen kontinentaleuropäische Unternehmen betrieben hat. Aber auch dies ist sicher nur die sehr kleine Spitze eines sehr großen Eisbergs. Für die Weitergabe der gesammelten Informationen an US-Konzerne sorgt ein speziell eingerichtetes Verbindungsbüro (Office of Intelligence Liaison) im US-Wirtschaftsministerium. So wurden beispielsweise dem ostfriesischen Windkraftunternehmen Enercon mit Hilfe abgehörter Telefonate Details zu dessen Turbinentechnik entwendet und in einem Patentrechtsstreit an den US-Konzern Kenetech Windpower weitergegeben. Dem belgischen Unternehmen Lernout & Hauspie stahl die NSA kurzer Hand selbst die von Belgieren entwickelten Spracherkennungsalgorithmen, um sie für die eigene Überwachungstechnik nutzbar zu machen. Den größten wirtschaftlichen Schaden musste dabei der europäische EADS-Konzern einstecken. Die NSA fing die Kommunikation zwischen dem Airbus-Hersteller EADS und Saudi Arabien ab – inklusive Bestechungsgeldangeboten und Preisvorstellungen. Der US-Konzern Boeing freute sich über die weitergebenen Daten und holte den Auftrag im Volumen von sechs Milliarden US$ mit tatkräftiger NSA-Unterstützung. Boeing zählt nebenbei auch zu den umsatzstärksten technischen Partnern der NSA. Da ist es mehr als ein Scherz am Rande, dass die NSA ihre syntaxgestützten Erkennungssysteme gerne mit dem Beispiel testet, aus einer Datenbank Mails und Telefonate herauszufiltern, in denen es

um EU-Subventionen für das Airbus-Konsortium geht.

Es war vor allem der Vorwurf der Wirtschaftsspionage, der im Jahre 2001 dazu führte, dass das Europäische Parlament eine Untersuchung gegen das damals nur Insidern bekannte Überwachungssystem einzuleiten. Auch wenn die Untersuchung zu dem klaren Ergebnis [PDF – 1.3 MB] kam, dass die UKUSA-Staaten die Kommunikation europäischer Bürger und Unternehmen systematisch abhören, kam es nie zu einer wie auch immer gearteten Sanktion gegen die beteiligten Dienste und deren Regierungen. Die Europaparlamentarier erkannten vielmehr, dass ihnen die Hände gebunden sind und die Überwachung bereits ein Ausmaß angenommen hat, gegen das man sich mit einfachen Mitteln nicht mehr wehren kann. Sieben Tage nachdem der Sonderausschuss des Europäischen Parlaments seinen Bericht vorlegte, flogen zwei Passagierflugzeuge ins World Trade Center und die Abhörbefürworter hatten ein schlagendes Argument, um „Bedenken" hinwegzufegen und die informelle Freiheit mit neuen Gesetzen und milliardenschweren Überwachungsprogrammen endgültig zu Grabe zu getragen.

Prism ist nur die Spitze des Eisbergs

Echelon und das dazugehörige Datenverarbeitungsbackbone konnten zu ihrem technischen Höhepunkt zwei Millionen „Inputs" (also z.B. Mails oder Telefonanrufe) pro Stunde verarbeiten. Das aktuelle Abhörsystem mit dem Codenamen „Stellar Wind" kann nach Angaben des NSA-Whistleblowers William Binney 1,25 Millionen Mails mit jeweils 1.000 Buchstaben pro Sekunde verarbeiten. Bereits als das System in Betrieb ging, speicherte es laut Binney bereits 320 Millionen Telefonanrufe pro Tag. Und selbst das ist erst der Beginn für ein totalitäres Überwachungssystem, das sämtliche Vorstellungen sprengt. Das mittelfristige Ziel der NSA ist, zwanzig Terabyte Datenverkehr pro Minute abzuhören und zu verarbeiten – das entspricht über 300 Millionen Mails mit jeweils 1.000 Buchstaben pro Sekunde.

Woher kommen diese unvorstellbaren Datenmengen? Zum Beispiel von einem der angeblich rund zwanzig NSA-Rechenzentren, die direkt an die Backbones der großen Netzbetreiber angekoppelt sind und von denen unterhalten werden. Eines dieser Rechenzentren wurde vom Whistleblower Mark Klein offenbart und machte als „Room 641A" im Jahre 2006 Schlagzeilen in den einschlägigen Medien. Zusätzlich werden von der NSA auch noch die großen Glasfaserleitungen, über die der internationale Datenverkehr läuft, systematisch angezapft, wobei die abgefangenen nationalen und internationalen Telefongespräche automatisiert gespeichert werden. Welche Abhöreinrichtungen die NSA zusätzlich in „befreundeten" und nicht befreundeten Staaten unterhält, ist – wie so vieles – unbekannt. Dass überhaupt etwas über diese Programme bekannt ist, ist einzig und alleine einigen

wenigen mutigen Whistleblowern zu verdanken – zum Beispiel Männern wie William Binney, Kirk Wiebe und Thomas Drake, die allesamt Jahrzehnte in leitenden Funktionen für die NSA tätig waren, die Arbeit aber irgendwann nicht mehr mit ihrem Gewissen vereinbaren konnten und dafür von den US-Behörden massiv bekämpft werden.

Das Abhörprogramm Prism, mit dem die NSA sich automatisierten Zugang zu den Daten bestimmter amerikanischer Internetdienstleister verschafft, ist nur ein kleines Prisma in einem unvorstellbar großen Überwachungssystem. Die sprichwörtliche Spitze des Eisbergs. Doch wohin fließen die ganzen Daten? In Utah wird in diesem Jahr ein neues NSA-Rechenzentrum eröffnet, das fähig ist, Daten im „Yottabytebereich" zu verarbeiten – ein Yottabyte sind eine Billion Terabyte. Damit hätte das Rechenzentrum die Kapazität, dass Eintausendfache[*] des gesamten Datenvolumens zu verarbeiten, das jährlich über das Internet transferiert wird.

Doch der größte Speicher nutzt wenig, wenn man die gesammelten Daten nicht sinnvoll auswerten kann. Aber auch an diesem Problem arbeitet die NSA bereits fieberhaft. In Oak Ridge, Tennessee entsteht momentan ein gigantisches geheimes Rechenzentrum, in dem bis 2018 einen neuer Superrechner untergebracht werden soll, der alle bekannten zivilen Superrechner in den Schatten stellen soll. Dieser Rechner hat den Stromverbrauch von 200.000 Haushalten und soll dann auch in der Lage sein, Daten und Mails, die mit aktuellen AES-Verschlüsselungsalgorithmen verschlüsselt wurden, in vertretbarer Zeit zu knacken. Zusätzlich hat die NSA im Februar dieses Jahres den Bau eines weiteren „Hochleistungsrechenzentrum" in Ft. Meade, Maryland angekündigt, das ebenfalls zum „Codebreaking" genutzt werden soll. Die Verschlüsselung stellt heute – neben den Gesetzten – das einzig nennenswerte Problem für die NSA dar. Im Datenpool der Schlapphüte dürften noch zigtausende Mails und Dokumente schlummern, die noch darauf warten, entschlüsselt zu werden.

Orwell 2.0

Ein Nachrichtendienst hat natürlich die Aufgabe, bestimmte Formen der Kommunikation von „bösen Buben" abzuhören und die daraus gewonnen Erkenntnisse weiterzugeben. Dagegen ist auch prinzipiell nichts einzuwenden, doch was die NSA macht, hat mit diesem naiven Bild eines Nachrichtendienstes so gar nichts mehr zu tun. Auf Basis der wenigen öffentlich bekannten Informationen sieht es vielmehr so aus, als würde die NSA bestrebt sein, jedes Bit, das durch die Netzwerke rauscht und jedes Telefonat, das weltweit geführt wird, zu erfassen, abzuspeichern und auszuwerten. Ein leitender NSA-Angestellter fasste dies gegenüber Wired mit dem griffigen Satz „Jeder ist ein Ziel; jeder, der kommuniziert ist ein Ziel" ("Everybody's a target; everybody with communication is a target.)" zusammen.

Und dabei geht es keineswegs nur um die Terrorabwehr. Eine aktuelle Studie des niederländischen Geheimdienstes stellt nicht umsonst fest, dass die wirklich „bösen Buben" für ihre konspirative Kommunikation verschlüsselte Foren im sogenannten „Deep Web" nutzen, die Google und Co. überhaupt nicht bekannt sind. Die Idee, dass Terroristen sich über Facebook oder Skype zum nächsten Anschlag verabreden, ist derart albern, dass es schon peinlich ist, wenn beispielsweise das Prism-Programm mit dem Argument der Terrorismusabwehr und –bekämpfung begründet wird. Bereits das technisch wesentlich schwächere Echelon-System wurde auch zur Bespitzelung von Regierungskritikern und zur umfassenden Wirtschaftsspionage genutzt und es gibt keinen einzigen Grund anzunehmen, dass sich darin bis heute etwas geändert haben soll.

Das Abhörprogramm der NSA ähnelt noch nicht einmal im Ansatz einem „Minority Report" und kann keine Verbrechen verhindern, bevor diese begangen werden. Es ist eine Sache, gigantische Datenbanken zu erfassen und abzuspeichern – sie auch sinnvoll auszuwerten, ist ungleich schwieriger. Was die Datenbank in puncto Terrorabwehr jedoch kann, ist, sämtliche Mails und Telefonate von Tätern auszuwerten, nachdem die Tat begangen wurde. Da die echten bösen Buben dies jedoch genau wissen, dürfte sich der praktische Nutzen eher in Grenzen halten. Diesem geringen Nutzen steht jedoch eine unverhältnismäßig große Gefahr gegenüber. Denn (siehe oben) jedes Angebot generiert automatisch auch eine Nachfrage. Und welche Regierungsbehörde könnte schon dem süßen Honigtopf mit einem derart umfassenden Datenpool auf Dauer widerstehen?

Mittels der heute entwickelten Technik ist es schon bald möglich, ein komplettes Profil einer Person anzulegen. Nahezu jede Mail, die jemals verschickt wurde, jedes Telefonat, das jemals geführt wurde, jede Finanztransaktion und jede Rechnung, die nicht in bar bezahlt wurde, wird bereits heute von der NSA direkt oder indirekt abgespeichert und ist über intelligente Datenbankanwendungen auch personalisierbar. Der „Big Brother" kann sich somit ein umfassendes Bild von jeder Person – auch von Ihnen – machen. Und dies ist keine Dystopie, kein orwellsches Schreckenszenario, sondern bereits heute technisch machbar. Nur noch die Gedanken sind frei; alles, was in irgendeiner Form digitalisiert wurde, ist nicht mehr frei. Und wir regen uns über die Stasi auf.

Was kann ich dagegen tun?

Am wichtigsten ist es, dass die Bürger endlich ein Gespür für die Bedrohung durch die alltägliche Überwachung bekommen. Erst dann wird sich auch ein politisches Bewusstsein für diese Thematik entwickeln. Für Angela Merkel ist ja bereits das Internet Neuland und die beiden großen Volksparteien scheinen überdies noch nicht einmal über rudimentäre Kenntnisse im Bereich Datenverarbeitung zu verfügen. Und wenn es – siehe

Echelon/Europäisches Parlament – doch einmal eine politische Initiative schafft, Datenschutzskandale öffentlich zu machen, zählen schlussendlich die wirtschaftlichen Interessen mehr als die informelle Freiheit der Bürger. Man muss nicht zynisch sein, um daraus zu folgern, dass die Wahrscheinlichkeit, dass von dieser Politik mittel- bis langfristig etwas gegen die Überwachungsallmacht der Geheimdienste unternommen wird, gegen null geht. Und dies gilt spiegelbildlich auch für die USA und andere Staaten mit ausgefeilten Überwachungsprogrammen.

Einstweilen bleibt uns daher nur übrig, zu hoffen, dass die Politik und die staatlichen Organe mit den Daten, die sie laut Verfassung gar nicht erheben dürfen, zumindest halbwegs verantwortungsvoll umgehen. Da das Angebot jedoch auch die Nachfrage generiert, kann man hier leider nur pessimistisch sein. Immerhin sitzen wir alle in einem Boot und es macht bekanntlich einen Unterschied, ob man in der Fußgängerzone oder am FKK-Strand die Hosen herunterlassen muss. Und wer es der NSA etwas schwerer machen will, der sollte seine Mails und Daten grundsätzlich verschlüsseln, so wenig proprietäre Software wie möglich nutzen und auch ansonsten so wenig Daten wie möglich hinterlassen. Dies gilt umso mehr für Unternehmen, Journalisten, Bürgerrechtler und ähnlich exponierte Personen. Der Satz „Gentlemen do not read each other's mail" hat nämlich heute leider keine Bedeutung mehr.

Hintergrund und Quellen (wenn nicht anders angegeben):

- James Bamford – The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)
- Duncan Campbell – Inside Echelon
- Oliver Schröm – Verrat unter Freunden
- Peter Lee – Snowden and the three wise NSA whistleblowers
- James Risen – Bush Lets U.S. Spy on Callers Without Courts
- Democracy Now! – "On a Slippery Slope to a Totalitarian State": NSA Whistleblower Rejects Gov't Defense of Spying
- Democracy Now! – National Security Agency Whistleblower William Binney on Growing State Surveillance

[«*] Basis: Schätzung von Cisco, nach der im Jahr 2015 der Internetverkehr bei 966 Exabyte pro Jahr liegen wird.