V. GLOBALE SICHERHEIT

Wenige Begriffe haben in den letzten Jahren eine derartige Konjunktur erlebt wie jener der „Sicherheit". Debatten über internationale oder öffentliche Sicherheit sind nichts Neues. Doch die neuen Informations- und Kommunikationstechnologien haben ambivalente Handlungsräume eröffnet, die den herkömmlichen Sicherheitsfragen eine neue Dimension verleihen, bisher unbekannte Sicherheitsrisiken in Erscheinung treten lassen und ein neues „Unsicherheits"-Empfinden erzeugen. Sie stellen aber auch das Reden über Sicherheit selbst unter neue Voraussetzungen: so wird es immer deutlicher, dass der Begriff Sicherheit wenig aussagekräftig ist, solange er nicht mit konkreten Situationen in Bezug gesetzt wird und die Sicherheitsinteressen und deren Vertreter benannt werden. Doch gerade wenn die jeweiligen historischen, gesellschaftlichen und politischen Rahmenbedingungen, innerhalb derer von Sicherheit gesprochen wird, ausgeblendet werden, gewinnt der Begriff jene Mobilität und universale Einsetzbarkeit, die ihn heute auszeichnet. Sicherheit ist auch unter diesem Gesichtspunkt ein wahrhaft globaler Begriff geworden, der mit einer Selbstverständlichkeit eingesetzt wird, die die Frage nach der Legitimität von Sicherheitsmaßnahmen- und Technologien häufig in den Hintergrund treten lässt. In diesem Kapitel werden daher Technologien und Einrichtungen, die im Zusammenhang mit dem globalen Streben nach „Sicherheit" eingesetzt werden bzw. operieren, in ihrer politischen und gesellschaftlichen Dimension besprochen. Der Begriff Sicherheit ist nur dann sinnvoll, wenn eine Gefahr angenommen wird, die abgewendet werden soll. Auf gesellschaftlicher und politischer Ebene bedeutet dies, dass Personen, Gruppen, Organisationen oder Länder als potenzielle Gefahrenquellen verstanden und in ihrer Freiheit eingeschränkt werden müssen, um Sicherheit zu gewährleisten. Im Zuge der Informatisierung und globalen Vernetzung sind immer mehr Menschen von derartigen Eingriffen in Grund- und Freiheitsrechte betroffen. In den folgenden Abschnitten wird das Thema Sicherheit an den konkreten Beispielen von Überwachung, Kryptografie und Biometrie behandelt. Abschließend wird das globale Überwachungssystem ECHELON vorgestellt.

5.1 Überwachung

Mit der Entwicklung der Informations- und Kommunikationstechnologien sind der Überwachung ungeahnte neue Möglichkeiten geöffnet worden. Immer weniger Lebensbereiche sind von Überwachung frei: von der Allgegenwart von Überwachungskameras bis zur Satellitenaufklärung steht die Überwachung im Dienste der „Sicherheit". Aber auch Wirtschaftsunternehmen greifen immer häufiger zu Überwachungstechnologien, um zum Beispiel die Tätigkeit von Mitarbeitern oder das Verhalten von Kunden zu kontrollieren. Überwachungspraktiken stehen in direktem Konflikt mit der Wahrung der Privatsphäre. Die Frage der Überwachung ist daher mittlerweile zu einem zentralen Thema aktueller politischer Debatten geworden und von ausschlaggebender Bedeutung im Streben nach informationeller Selbstbestimmung.

Sticker der Surveillance Camera Players
© Surveillance Camera Players

Geschichte der Überwachungsmethoden

Das Interesse am unbemerkten Beobachten anderer oder am Belauschen von Gesprächen lässt sich bis auf die Antike zurückverfolgen. Zu einer ersten Blüte entsprechender Praktiken und technischer Geräte kam es während der Renaissance in Europa, einer Zeit, in der Geheimschriften, kryptographische Techniken, Gebäude mit verborgenen Tunnels und versteckten Türen und dergleichen große Beliebtheit genossen und das Geheimnis einen ebenso hohen kulturellen Wert hatte wie die Versuche, es zu lüften. Was zunächst als eine Art Gesellschaftsspiel stattfand, wurde bald auch mit handfesten politischen Zielsetzungen betrieben. Dokumentiert sind u. a. die Aktivitäten des Grafen Walsingham (1531–1590), Secretary of State und Spion Elisabeths I. von England.[103] In Frankreich machte sich etwa zur selben Zeit Kardinal Richelieu als überwachungsfreudiger Geheimnisverwalter einen Namen, der sich durch seine ausgeklügelten Überwachungstechniken einen Informationsvorsprung erwarb, der nachhaltige Auswirkungen auf die Geschichte Frankreichs hatte.

Während die Überwachung im Zuge der Herausbildung des modernen Staatensystems in Europa also eine Funktion der internationalen Beziehungen war, wurde sie ab dem 18. Jahrhundert vermehrt auf gesellschaftlicher Ebene eingesetzt, etwa zur Bekämpfung von Schmuggel, aber auch in der Arbeit der Polizei. In den USA kam es im Verlauf der Kolonisierung des Westens zu einer Zunahme des Gangsterwesens und der Kriminalität, vor allem der Geldfälscherei. Allan Pinkerton (1819–1884) erwarb sich im Aufdecken von Fälscherwerkstätten einen Ruf und wurde von Präsident Lincoln 1861 zum ersten offiziellen Geheimdienstagenten gemacht.

Die rasche technische Entwicklung im 19. Jahrhundert führte – auch durch die damit einhergehende erhöhte Effizienz – zu einer Intensivierung der Überwachung und stellte diese auf die Grundlage, die wir heute kennen. Die systematische Zusammenarbeit der Polizei mit der Wissenschaft hat daher ihren Ursprung in dieser Zeit, wobei die Initiative zunächst von der 1863 gegründeten amerikanischen National Academy of Science ausging: Politiker fühlten sich durch den technischen Fortschritt eher bedroht

103 Zur Geschichte der Spionage vgl. Peterson (2001), S. 1–20 ff.

als unterstützt und waren daher schwer davon zu überzeugen, dass sich die moderne Technik im Sinne der Regierungsgewalt einsetzen ließe.

Bis zum Ersten Weltkrieg blieben Überwachungstechnologien daher Nebenprodukte einer von Einzelwissenschaftlern beherrschten Forschung und Entwicklung, wie zum Beispiel das 1904 von Christian Hülsmeyer patentierte Telemobiloskop, ein Vorläufer des Radars. Dies änderte sich grundlegend während des Ersten Weltkrieges, wo praktisch die gesamte Bandbreite in Frage kommender moderner Technologien zu Überwachungszwecken eingesetzt wurde. Von vorrangiger Bedeutung war das Abhören von Telefon- und Telegrafenverbindungen. Der Kriegseintritt der USA 1917 geht auf eine abgefangene Botschaft der deutschen Regierung an ihre Botschaft in Mexiko zurück, in der dem Land in Aussicht gestellt wurde, es im Falle einer Allianz bei der Rückgewinnung von Territorien zu unterstützen, die es an die USA verloren hatte.

In der Zwischenkriegszeit erlebte die staatliche Überwachung erneut im Zusammenhang mit Wirtschaftsverbrechen, besonders Alkoholschmuggel während der Prohibition in den USA, einen Aufschwung. In Großbritannien führten die Kommunikationsanforderungen des über die ganze Welt verstreuten Kolonialreiches zu einem Vorsprung in der Entwicklung von Kommunikationstechnologien, der die Entwicklung des Computers während des Zweiten Weltkrieges erleichterte und sich bis in die Gegenwart in einer britischen Marktführung bei Überwachungstechnologien auswirkt.

Nach dem Zweiten Weltkrieg wurde Überwachung maßgeblich von den Ambitionen der am Kalten Krieg beteiligten Staaten beeinflusst. Dadurch wurde sie grenzüberschreitend und dehnte sich so auf die ganze Welt aus; internationale Politik wurde dementsprechend zur „Geopolitik". Ermöglicht wurde diese durch Satellitentechnologie und neue drahtlose Abhörtechnologien, vor allem aber durch die Informatisierung: die durch Überwachung gewonnene Information wurde speicherbar. Staatliche Souveränität, sowohl im Inneren als auch in den Internationalen Beziehungen, stützt sich immer mehr auf systematisch durch Überwachung gesammelte und ausgewertete Informationen. Droht das von dem französischen Philosophen Michel Foucault thematisierte Modell einer Überwachungsgesellschaft Wirklichkeit zu werden?

Überwachungsgesellschaft

In „Überwachen und Strafen" legt Foucault (1994) diesem Gesellschaftsmodell das von Jeremy Bentham im 18. Jahrhundert entworfene Gefängnismodell des Panopticons zu Grunde. Im panoptischen System werden die Gefangenen von einer für sie unsichtbaren Aufsichtsperson überwacht und wissen daher nie, ob sie gerade unter Beobachtung stehen oder nicht. Bentham schloss daraus, dass die Gefangenen aufgrund der Möglichkeit der Beobachtung von unerlaubten Aktivitäten Abstand nehmen und sich der Gefängnisautorität unterwerfen und diszipliniert verhalten würden.

Überwachung

Jeremy Bentham (1748 - 1832),
Erfinder des Panoptikons
© *Sonoma State University*

Dem klassischen Souveränitätsmodell, das auf Gesetzen und Sanktionsandrohungen und einer punktuellen Machtausübung beruht, stellt Foucault das Modell der Überwachung gegenüber, das ohne einen physisch greifbaren Souverän auskommt, weil das Verhalten der Menschen durch eine ständig vorhandene Möglichkeit des Überwachtwerdens diszipliniert würde. Die entsprechenden Technologien, von Überwachungskameras bis zu Tracking-Technologien im Internet, vom Abhören von Telekommunikation bis zum Keyboard-Monitoring (der Aufzeichnung der Tastaturanschläge) am Arbeitsplatz, sind mittlerweile in den informationsbasierten Gesellschaften weit verbreitet. Polizei, Wachpersonal und ähnliche Vertreter der Autorität werden von Kameras und Überwachungssoftware ersetzt, ihre sichtbare Präsenz weicht der Omnipräsenz der Überwachungstechnologien. Deren öffentliche Wahrnehmung und Kritik scheint dabei weit hinter ihrer Präsenz zurückzuliegen. Denn einerseits werden Überwachungstechnologien als neutrale Instrumente der Verbrechensbekämpfung missverstanden und willkommen geheißen, andererseits stoßen sie auf resigniertes Schulterzucken. Letzteres kann jedoch bereits als typische und notwendige Auswirkung der Überwachung selbst verstanden werden: Sich in jedem Augenblick und in jeder Lage der Möglichkeit der Überwachung bewusst zu sein und auf sie zu achten, scheint unweigerlich zur Übermüdung und zum kommentarlosen Hinnehmen des Status quo zu führen.

Überwachung des öffentlichen Raumes

Immer häufiger wird versucht, die Sicherheit von öffentlichen Bereichen wie Straßen, Unterführungen, Bahnhöfen, Flughäfen, Schulen und Bürogebäuden mit Hilfe von Kameraüberwachung zu gewährleisten. Der Anblick dieser Geräte, die während des Kalten Krieges noch gerne als Lieblingstechnologien von überwachungseifrigen Sicherheitsdiensten kommunistischer Staaten gehandelt wurden, ist mittlerweile überall selbstverständlich. An Kreuzungen und in U-Bahntunnels, in Banken und Kaufhäusern, in Schulen und Spitälern ist die Kameraüberwachung mit sogenannten *CCTV* (closed circuit television-Systemen) gang und gäbe.

Die Entwicklung reicht dabei von statischen, niedrig auflösenden und leicht sichtbaren Kameras bis hin zu miniaturisierten, nachtsichtfähigen Zoom-Kameras, die an vielen Orten auch noch mit Gesichts- oder Gangerkennungssystemen verbunden sind. Ein besonders markantes Beispiel einer derartigen Überwachungstechnologie ist der Londoner Stadtteil Newham. Dort sind seit 1998 flächendeckend hunderte Überwachungskameras installiert worden, um die Straßenkriminalität zu bekämpfen. Die Kameras sind mit dem Gesichtserkennungssystem Mandrake ausgestattet, das es ermöglicht, die Gesichter aller Passanten mit einer Datenbank von 100 bis 150 gesuchten Straftätern zu vergleichen. Im Finanzbezirk Londons sowie an zahlreichen Autobahnen sind Kamerasysteme angebracht, die die Kennzeichen vorbeifahrender Autos in Datenbanken einlesen. Auch hier geht es darum, gesuchte Personen anhand ihrer Fahrzeuge aufzuspüren. Großbritannien weist die höchste Kameradichte der Welt auf, die Gesamtzahl der Überwachungskameras wird auf ca. 300.000 geschätzt. [104] Ausführlich dokumentiert wurde das Thema von Privacy International. [105]

Überwachungskamerabilder, Newham, London

© Der Spiegel

Auch wenn Großbritannien einen überwachungstechnischen Vorsprung hat – neben geschichtlichen Faktoren hat auch die Terrorismusbekämpfung zu vermehrter Forschung und Entwicklung in diesem Bereich geführt –, so werden doch in den meisten hochtechnisierten Ländern bereits derartige Technologien eingesetzt. Seit in Hannover 1976 die ersten schwenkbaren Überwachungskameras installiert wurden, hat es auch in Deutschland eine entsprechende Entwicklung gegeben, die sich zuletzt besonders in den neuen Bundesländern – Modellversuch Leipzig 1997 – beschleunigt hat. Argumentiert wird dabei im Allgemeinen damit, dass durch die Überwachung die Sicherheit der öffentlichen Plätze steige, was wiederum zu ihrer Belebung und wirtschaftlichen Aufwertung beitrage. Allerdings neigt die Kriminalität dazu, in angrenzende Bezirke abzuwandern, sodass sich wie bei jeder vernetzten Technologie ein Drang zur Expansion feststellen lässt. Darüber hinaus wurde in einer Studie fest-

104 http://koeln.ccc.de/projekte/cctv
105 http://www.privacy.org/pi/issues/cctv/

gestellt, dass Überwachungskameras durchaus auch Zwecken dienen, die mit Verbrechensbekämpfung nichts zu tun haben: 10 Prozent der beobachteten Frauen werden demnach aus voyeuristischen Gründen auf die Bildschirme der Beobachter gezoomt (Buse 1999: 122).

Das Prinzip dieser Überwachungstechnologien ist dabei jedoch, dass nicht nur Verdächtige beobachtet werden, sondern alle, die sich in den überwachten Bereichen aufhalten; letztendlich bedeutet das, dass jeder, der Grundrechte wie freie Wahl des Aufenthaltsortes, Versammlungsfreiheit, Reisefreiheit etc. in Anspruch nimmt, grundsätzlich verdächtig ist – womit der „freie Bürger" von einer Neuauflage des „disziplinierten Untertans" abgelöst wird. Der Grundsatz der Unschuldsannahme wird aufgeweicht und technisch unterlaufen. Gleichzeitig wird die Disziplinierung durch Überwachung nicht immer und nicht von allen als solche wahrgenommen und von vielen nicht als störend empfunden. Ähnlich wie in Huxleys „Schöner neuer Welt" gehen Herrschaft und individuelles künstliches Glück eine neue totalitäre Verbindung ein.

Interface von IAA für Überwachungskameras in Manhattan
© *Institute for Applied Autonomy*

Freilich sind von dieser Entwicklung hin zur Foucaultschen Überwachungsgesellschaft nicht nur die klassischen öffentlichen Bereiche betroffen. Auch in der Arbeitswelt werden immer mehr Überwachungstechnologien eingesetzt, um Mitarbeiter zu kontrollieren und Leistungsausfälle zu minimieren.

Arbeitsplatzüberwachung

Nahezu in allen Bereichen der Arbeitswelt wird der Druck auf die Arbeitnehmer verschärft. Telefongespräche, Online-Verhalten, E-Mails, Fahrten mit dem Dienstwagen, selbst Zigaretten- und WC-Pausen werden immer häufiger digital erfasst und analysiert. Je mehr Arbeit informatisiert und digitalisiert wird, um so leichter und weitreichender funktioniert die Überwachung.

In vollständig digitalisierten Arbeitsumgebungen, wie etwa Call-Centers oder E-Commerce-Betrieben, ist daher das ständige Monitoring der Leistung von Mitarbeitern und Mitarbeiterinnen weit verbreitet. Arbeitstempo, Effizienz und Pünktlichkeit, aber auch Pausendauer- und Häufigkeit, Online-Verhalten und Telefongespräche werden in Echtzeit überwacht und die Mitarbeiter damit in eine Leistungshierarchie gegliedert, die aufgrund ihrer technischen Präzision und Objektivität kaum mehr angezweifelt werden kann. In vielen Betrieben übernehmen Systemadministratoren die Aufgabe, E-Mail- und Internetverkehr von Angestellten zu überprüfen. All das ist in Firmennetzwerken recht einfach zu bewerkstelligen.

Etwas mehr Aufwand ist erforderlich, wenn einzelne Mitarbeiter oder Mitarbeiterinnen gezielt überwacht werden sollen, etwa weil im Zuge von Routine-Überwachungen der Verdacht entstand, der oder die Betreffende könnte Interesse an einem Firmenwechsel haben und daher möglicherweise Firmeninterna ausplaudern. Dann kommen gerne Keyboard Monitoring Systems zum Einsatz, die den getippten Text direkt von der Tastatur drahtlos an die Kontrollstelle senden – eine Überwachungstechnologie, gegen die auch Verschlüsselung nichts ausrichtet. Hergestellt werden derartige Systeme beispielsweise vom britischen Produzenten Vascom.

Ebenso zur Werkzeugkiste der Arbeitsplatzüberwacher gehören Geheimkameras und -mikrofone, die in Teeküchen, Garderoben und ähnlichen Orten des „informellen Informationsaustausches“ angebracht werden. Denn wenn es um die Besetzung verantwortungsvoller Positionen geht, will so mancher Chef genau wissen, wer von den Angestellten wirklich vertrauenswürdig ist.

Privatausflüge mit dem Firmenwagen lassen sich anhand des GPS-Navigationssystems und einer speziellen Software aufdecken, die analysiert, wo sich ein Fahrzeug an einem bestimmten Zeitpunkt aufgehalten hat. Noch leichter wird derartiges Tracking, wenn Autos mit Internet-Anschluss ausgestattet sind – aber nicht nur die firmeninterne Überwachung wird damit unkomplizierter, auch die Fahrzeughersteller lassen sich so ihre eigenen Kundendatenbanken bequem und kostenlos aktualisieren.

Überwachte Telefonleitungen gehören zum Standardrepertoire der meisten Überwachungssituationen. Digitale Verbindungen lassen sich aber nicht nur abhören, sondern auch in allen Einzelheiten analysieren und mittels Data-Mining auswerten. Telefonsoftware wie etwa die von Harlequin hergestellte WatCall machen es Unternehmen leicht, genaue Profile des Telefonierverhaltens der Angestellten anzufertigen. Das WatCall-Analysesystem wird auch von der britischen Polizei eingesetzt, um Freundschaftsnetzwerke zu identifizieren und die so gewonnenen Daten mit bestehenden Datenbanken zu verknüpfen, womit ein automatischer Überwachungsprozess in Gang gesetzt wird, der abseits von richterlichen Beschlüssen abläuft, ja von dem die Justizbehörden

nicht einmal Kenntnis haben. Harlequin erhielt dafür 1998 den britischen Big-Brother Award. [106] Das berüchtigte Überwachungsgesetz Regulation of Investigatory Powers *(RIP)* hat in Großbritannien zu einem Boom in der Branche geführt: Der Umsatz in Schnüffeltechnologien, mittlerweile unter „RIP-Technologien" bekannt, stieg 2001 um 53 Prozent. [107]

Lauschangriffe

Das umstrittene britische RIP-Gesetz [108] ist in den letzten Jahren zum Inbegriff der staatlichen Abhörwut geworden. Das Gesetz, das bereits im Zuge seiner Entstehung zu heftigen Kontroversen Anlass gab, räumt der Polizei und dem Geheimdienst MI5 sehr weitgehende Befugnisse ein. Internet-Provider werden verpflichtet, den gesamten Datenfluss einer eigens dafür geschaffenen Abhörbehörde zugänglich zu machen, ohne dass dafür ein richterlicher Beschluss notwendig wäre. Vom Direktor der britischen Bürgerrechtsbewegung Charta 88 wurde das Abhörgesetz als „schlimmste Beeinträchtigung der Privatsphäre, die es je in einem demokratischen Staat gab" bezeichnet. Doch nicht nur Bürgerrechtsbewegungen kritisieren das Gesetz; auch Unternehmen, haben dagegen mobil gemacht, weil in vielen Fällen die Vertraulichkeit der Online-Kommunikation, wie sie zum Beispiel für den E-Commerce und die Finanzwirtschaft Voraussetzung ist, nicht gewährleistet ist.

Für Simon Davies, Direktor der britischen Cyberrechte-Initiative Privacy International, besteht die Gefahr des RIP-Gesetzes in der Vorbildwirkung für andere Regierungen, die durch die Marktführung Großbritanniens im Bereich der Überwachungstechnologien noch verstärkt werden könnte.

Tatsächlich hat sich der Trend zur flächendeckenden Überwachung von elektronischer Kommunikation massiv verstärkt. In praktisch allen hochtechnisierten Ländern wurden Vorkehrungen getroffen, um die Kommunikationstechnologien der „dritten Generation" in Echtzeit zu überwachen. „Die Überwachung ist zu einer festen Mehrwertkomponente der Architektur von Informations- und Kommunikationstechnologien geworden. Alle Kommunikationssysteme und Netzwerke beinhalten heute irgendeine Form von fester Überwachungskomponente", so die Diagnose Simon Davies'. [109]

Auf europäischer Ebene wurde vom Europarat 2001 die Cybercrime Convention verabschiedet, die für alle Mitgliedsländer gemeinsame technische Überwachungsstandards einführt und eine Behördenstruktur schafft, welche die grenzüberschreitende Überwa-

106 www.privacyinternational.org/bigbrother/uk-awards.html
107 www.newmonday.co.uk
108 http://www.fipr.org/rip
109 http://world-information.org/program/events

chung und den Austausch von Daten ermöglicht. [110] Auch hier werden Polizei und Geheimdiensten Rechte für Überwachungsaktivitäten eingeräumt, für die bisher in den meisten Fällen eine richterliche Genehmigung erforderlich war. Die Konvention unterläuft aber auch Normen zum Schutz der Menschenrechte wie etwa die Europäische Menschenrechtskonvention, indem sie die Möglichkeit bietet, an Staaten, die letztere nicht unterzeichnet und niedrige Datenschutzstandards haben, etwa die USA, Überwachungsdaten zu übermitteln. Schon ein paar unbedachte Mausklicks genügen, um Anlass zur Verfolgung zu geben.

Generell lässt sich eine starke Präsenz der USA in der globalen Überwachung feststellen. Mit einem System, das unter dem Namen Carnivore („Fleischfresser") bekannt und mittlerweile offiziell auf DCS1000 umgetauft wurde, sind die USA im Überwachen des E-Mail-Verkehrs federführend. [111] Auch das globale Überwachungssystem ECHELON wird weitgehend von den USA kontrolliert, die auch Einfluss auf die Entwicklung von Überwachungsstandards innerhalb der Europäischen Union ausüben. Die vom European Telecom Standards Institute *(ETSI,* www.etsi.org*)* unter dem Titel *ENFOPOL* entwickelten gemeinsamen Standards für Überwachungsschnittstellen innerhalb der EU erfolgte in Abstimmung mit dem FBI. [112] Dabei nehmen diese Standards praktisch ausschließlich auf die Wünsche von Strafverfolgern, Produzenten von Überwachungstechnologien und großen Netzbetreibern Rücksicht. Parlamentarische Anhörungen und ähnliche demokratische Prozesse werden um der „Sicherheit" willen umgangen.

Im Zuge der Reaktionen auf die Ereignisse des 11. September 2001 hat sich der Drang nach Überwachung nochmals verstärkt. Vorbehalte und Zweifel an der Sinnhaftigkeit und Grundrechtsverträglichkeit allgemeiner und omnipräsenter Überwachung wurden von der lautstarken und kaum differenzierten Forderung nach einer wirksamen Bekämpfung „des Terrorismus" niedergewalzt. Der US-Patriot Act (Provide Appropriate Tools Required to Intercept and Obstruct Terrorism), der bereits wenige Wochen nach den Anschlägen beschlossen wurde, gibt der Exekutive weitreichende neue Rechte zum Abhören von Kommunikation und Sammeln von Daten. [113] In so gut wie allen europäischen Ländern wurden ähnliche Gesetze zur Erleichterung von Lauschangriffen verabschiedet.

Wie weit sich die innere Legitimität von Demokratien, die sich auf diese Weise rasch in Überwachungsstaaten verwandeln, noch aufrecht erhalten lässt, ist für viele Anlass zur Beunruhigung. Bekanntlich läuft die Absicht terroristischer Aktivität ja auf eine eben-

110 http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm
111 www.epic.org/privacy/carnivore/foia_documents.html
112 www.heise.de/tp/deutsch/special/enfo/11818/1.html
113 www.epic.org/privacy/terrorism/hr3162.html

solche Aushöhlung der Legitimität hinaus. Die Frage nach dem Umgang mit Überwachungstechnologien ist daher mit der Grundfrage von demokratischer Verfasstheit im Allgemeinen verknüpft, die darüber entscheidet, ob Information ihre liberale oder ihre autoritäre Dimension verwirklichen wird.

Steven Wright, Direktor der britischen OMEGA-Foundation, ist Verfasser des Berichtes über Technologien zur politischen Kontrolle für das Science and Technology Assessment Office *(STOA)* des EU-Parlaments. [115] In diesem Bericht stellt Wright vor allem einen Mangel an demokratischer Kontrolle fest, der in einem auffälligen Missverhältnis zur raschen Verbreitung und zunehmenden Leistungsfähigkeit der Technologien steht. Überwachungstechnologien, die von Systemen für Kameraüberwachung, Abhören, Fahrzeugerkennung bis hin zum globalen Überwachungssystem ECHELON reichen, werden laut Bericht kaum öffentlich problematisiert, obwohl sie in der Lage sind, demokratische Verfahren schrittweise auszuhöhlen. Dabei stellen diese Technologien nur einen, wenn auch bedeutenden, Bestandteil eines Spektrums miteinander verflochtener politischer Kontrolltechnologien dar, die auch neue Polizei-Tools wie nichttödliche Waffen sowie Hinrichtungs- und Foltertechnologien umfassen. Wright: „Wir befinden uns in der wichtigsten globalen Debatte über die akzeptablen Grenzen der großflächigen elektronischen Überwachung seit zwanzig Jahren. Diese Debatte wird das Verhältnis zwischen Informationsfreiheit und Informationskontrolle bestimmen. Sie ist vielleicht eine der letzten wirklichen Möglichkeiten, Widerstand gegen dominante Durchsetzung von Konsens durch elektronische Medien im 21. Jahrhundert zu mobilisieren.“ [116]

Satellitenansicht des Pentagon
© *spaceimaging.com*

115 www.heise.de/tp/deutsch/inhalt/te/1393/s1.html#exec
116 http://world-information.org/wio/news/992006886/992009002

5.2 Kryptografie

Jemand, der ein Geheimnis auf irgendeine andere Weise niederschreibt als auf eine, die es vor der Öffentlichkeit verbirgt, ist verrückt.

Roger Bacon (ca. 1250)

Bei der Kommunikation zwischen Menschen geht es nicht nur um Inhalte, sondern auch darum, wie Botschaften gesendet und empfangen werden und welche Technologien dabei zum Einsatz kommen. Jeder Akt der Kommunikation basiert auf einem Muster der Einbeziehung und des Ausschlusses: sobald eine Nachricht allein an einen bestimmten Empfänger gerichtet ist, bedeutet das, dass andere ausgeschlossen sind. Botschaften können zwischen nur zwei Individuen ausgetauscht werden (eins zu eins), während alle anderen von der Kommunikation ausgeschlossen werden. Botschaften können auch an größere Gruppen gerichtet sein, wie bei Vorlesungen und Vorträgen, oder an die breite Öffentlichkeit wie bei Nachrichtensendungen. In elektronischen Kommunikationsnetzwerken wie Online-Diskussionsgruppen überwiegt zunehmend die Kommunikationsform many-to-many, „von vielen an viele" Teilnehmerinnen und Teilnehmer.

Bei der mündlichen Kommunikation von Angesicht zu Angesicht ist es immer noch relativ einfach zu kontrollieren, wer auf den Informationsaustausch zugreifen kann. Je mehr aber Kommunikation von der physischen Anwesenheit losgelöst und technologisiert wird, desto mehr Personen haben die Möglichkeit, auf Informationen zuzugreifen, die nicht für sie bestimmt sind. Um sicherzugehen, dass bei der Kommunikation von Angesicht zu Angesicht die Information den ausgewählten Rahmen nicht verlässt, genügt es zu flüstern oder sich in einen geschützten Raum zurückzuziehen. Bei der schriftlichen Kommunikation ist das bereits schwieriger, und daher ist es nicht weiter überraschend, dass sich die Kryptografie parallel zur Entwicklung der Schrift entfaltet hat. Bei den heutigen elektronischen Kommunikationsformen hat die Weiterentwicklung der Technologien auch zu einer Vervielfachung der Möglichkeiten geführt, die den nicht autorisierten Zugriff auf Informationen ermöglichen.

Die Demokratie ist an der Durchsetzung des öffentlichen Interesses genauso zu messen wie an der Wahrung der Privatsphäre des Einzelnen. Aus diesem Grund ist die Kryptografie, das Ver- und Entschlüsseln durch Codes und/oder Chiffren, eines der führenden Themen in der Auseinandersetzung mit den Möglichkeiten einer demokratischen Informationsgesellschaft.

Geschichte der Kryptografie

Ca. 1900 v. Chr.: Ägyptische Schriftgelehrte verwenden bei den Inschriften eines königlichen Grabes außergewöhnliche Hieroglyphen: vielleicht nicht das erste, aber zumindest das erste dokumentierte Beispiel schriftlicher Kryptografie.

Kryptografie

405 v. Chr.: Dem griechischen General Lysander von Sparta wird eine verschlüsselte Botschaft geschickt, die auf der Innenseite des Gürtels eines Dieners befestigt ist. Der Text wird lesbar, wenn der Gürtel um einen Holzsstab, eine so genannte Skytale, gewickelt wird.

170 v. Chr.: Polybius entwickelt ein System, mit dem Buchstaben in numerische Zeichen umgewandelt werden können, die sogenannte Polybius-Tafel.

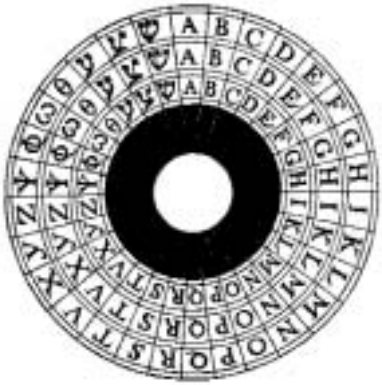
50–60 n. Chr.: Julius Cäsar entwickelt eine Verschlüsselungsmethode, die später die Cäsar-Verschlüsselung genannt wird. Dabei wird jeder Buchstabe des Alphabets um einen bestimmten Abstand verschoben. Wie bei Atbasch, einer traditionellen Form der hebräischen Substitutions-Geheimschrift, handelt es sich hier um eine monoalphabetische Substitution.

3. Jh.: Im Leiden-Papyrus werden alchemistische und magische Verfahren des antiken Ägyptens in griechischer Sprache verschlüsselt aufgezeichnet.

1250: Der englische Mönch Roger Bacon schreibt Verschlüsselungsanleitungen. Zu dieser Zeit ist die Kunst der Verschlüsselung in Klöstern ein beliebtes Spiel.

Ca. 1467: Erfindung der ersten polyalphabetischen Verschlüsselungsscheibe. Der Erfinder, Leon Battista Alberti, auch Vater der westlichen Kryptografie genannt, verwendet seine Scheibe zum Ver- und Entschlüsseln.

15./16. Jh.: Nahezu jede Regierung, insbesondere England und Frankreich, beschäftigt Leute zur Ver- und Entschlüsselung.



Verschlüsselungsscheibe von Giordano Bruno (1548–1600)

1585: Auf der Grundlage von Vorarbeiten von Leon Battista Alberti entwickelt Blaise de Vigenère ein neues Verschlüsselungsverfahren, bei dem jede einzelne Buchstabensubstitution auf der Grundlage eines anderen Geheimtextalphabets erfolgt, was die Entschlüsselung von der Kenntnis eines Schlüsselwortes abhängig macht. Die dabei verwendete Buchstabentabelle wird als Vigenère-Quadrat bezeichnet.

17. Jh.: Kardinal Richelieu erfindet ein Verschlüsselungswerkzeug namens grille, eine Karte mit Löchern, in denen Nachrichten auf Papier geschrieben werden können. Anschließend wird die Karte entfernt und die Leerstellen aufgefüllt, damit die Nachricht wie ein gewöhnlicher Brief aussieht. Der Empfänger muss im Besitz der gleichen Karte sein.
Der Englische Wissenschaftler, Magier und Astrologe John Dee arbeitet am antiken Alphabet von Enoch; er erarbeitet eine verschlüsselte Schrift, die bis heute noch nicht entschlüsselt werden konnte.

1605/1623: Sir Francis Bacon schreibt mehrere Bücher, die Ideen zur Kryptografie enthalten. Einer seiner wichtigsten Ratschläge ist es, die Verschlüsselung so durchzuführen, dass kein Verdacht geschöpft werden kann. Die Steganogramm-Methode, bei der dem eigentlichen Text ein anderer gewissermaßen übergestreift wird, sodass nicht erkennbar ist, dass es sich um eine verschlüsselte Nachricht handelt, eignet sich dazu am besten. Sie wurde oft in Gedichten angewendet. Im 20. Jahrhundert ist bei dem Versuch, die Sonette von Shakespeare zu entschlüsseln, der Verdacht aufgekommen, dass diese Texte ursprünglich von Francis Bacon verfasst worden sein könnten.

1671: Leibniz erfindet eine Rechenmaschine, die eine binäre Skala verwendet. Diese Skala ist heute die Basis für den *ASCII-Code*.

1844: Die Erfindung des Telegraphen stellt neue Ansprüche an die Kryptografie und macht sie wegen der Möglichkeit unbemerkten Abhörens auch immer notwendiger.

1861: Friedrich W. Kasiski führt eine Kryptoanalyse der Vigenère-Codes durch, die lange Zeit als nicht zu knacken galten.

1895: Die Erfindung des Radios verändert erneut die Aufgaben der Kryptografie und macht sie noch wichtiger.
Ein Mitarbeiter von AT&T, Gilbert S. Vernam, erfindet eine polyalphabetische Verschlüsselungsmaschine, die mit zufällig ausgewählten Schlüsseln arbeitet.
Arthur Scherbius patentiert eine Verschlüsselungsmaschine und versucht, sie an das deutsche Militär zu verkaufen, wird aber abgewiesen.

1923: Arthur Scherbius gründet eine Firma, um seine Enigma-Maschine zu bauen und an das deutsche Militär zu verkaufen.

Kryptografie

Späte 20er/30er Jahre: Kryptografie wird zunehmend von Kriminellen für ihre Tätigkeiten verwendet (beispielsweise beim Schmuggeln). Elizabeth Smith Friedman entschlüsselt regelmäßig die Codes von Rum-Schmugglern.

1933–1945: Die Deutschen setzen Enigma als wichtigste Krypto-Technologie ein. Der Enigmacode wird von Bill Tutte, Max Newmann und Alan Turings, Codebreakers in Bletchley Park, England, geknackt. [117]

Dechiffriermaschine Kolossus in Betchley Park, UK (1943)
© Andrew Hodges

Ca. 1930: Die Sigaba-Maschine wird in den USA erfunden, entweder von W. F. Friedman oder seinem Kollegen Frank Rowlett.
Gleichzeitig entwickeln die Briten die Typek-Maschine, die der deutschen Enigma-Maschine sehr ähnlich ist.

1943: Colossus, ein Entschlüsselungs-Computer und der weltweit erste programmierbare Computer, kommt in Bletchley Park zum Einsatz
1943–1980: Das Venona-Projekt der National Security Agency (NSA) der USA ist das am längsten andauernde Projekt seiner Art, das es jemals gegeben hat.

Späte 1960er Jahre: Das IBM Watson Research Lab entwickelt den Luzifer-Code.

1969: James Ellis entwickelt ein System mit getrennten öffentlichen und privaten Schlüsseln.

1971: Die Arbeit von IBM am Luzifer-Code und die Arbeit der NSA führen zum US Data Encryption Standard (DES).

117 Online-Dokumentationen: www.iwm.org.uk/online/enigma/eni-intro.htm, www.codesandciphers. org.uk/lorenz/fish.htm

1977/78: Der RSA-Algorithmus wird von Ron Rivest, Adi Shamir und Leonard M. Adleman entwickelt und veröffentlicht.

1991: PGP (Pretty Good Privacy) wird als Freeware im Internet veröffentlicht und definiert bald weltweit den neuesten Stand der Technik; sein Erfinder ist Phil Zimmermann.

1994: Bruce Schneider entwirft den Blowfish-Verschlüsselungsalgorithmus, ein 64-Bit-Blockcode mit einem bis zu 448 Bits langen Schlüssel.

90er Jahre: Arbeit an Quantencomputer und Quantenkryptografie.

1996: Frankreich lockert sein Kryptografiegesetz: zur Verwendung von Kryptografie ist eine Registrierung notwendig, sie kann aber von allen eingesetzt werden.
Die OECD veröffentlicht die Cryptography Policy Guidelines; ein Dokument, das Exportstandards für Verschlüsselung und uneingeschränkten Zugang zu Verschlüsselungsprodukten verlangt.

April 1997: Die Europäische Kommission erlässt eine Electronic Commerce Initiative, die sich für starke Verschlüsselung ausspricht.

Juni 1997: PGP 5.0 Freeware ist für die nichtkommerzielle Verwendung weitgehend verfügbar.

Juni 1997: Der 56-Bit-DES-Code wird von einem Netzwerk mit 14.000 Computern geknackt.

August 1997: Ein amerikanischer Richter bewertet die Exportrichtlinien für die Verschlüsselung als eine Verletzung der Redefreiheit.

März 1998: PGP kündigt seinen Plan an, Kryptografie-Produkte außerhalb der USA zu verkaufen.

April 1998: Die NSA erlässt einen Report über die Risiken von Key-Recovery-Systemen.

Juli 1998: Der DES-Code wurde binnen 56 Stunden von Forschern im Silicon Valley geknackt.

Oktober 1998: Die finnische Regierung stimmt der unbeschränkten Ausfuhr von starken Verschlüsselungssystemen zu.

Januar 1999: RSA Data Security etabliert weltweit den Vertrieb von Verschlüsselungsprodukten außerhalb der USA.

September 1999: Die USA verlautbaren, dass sie die Einschränkungen im Kryptografie-Export aufheben werden.

2000: Das Vorhaben der deutschen Regierung, die Freiheit der Kryptografie zu beschränken, trifft auf Widerstand.

2001: PGP wird von Network Associates gekauft. Der Kauf wird von dem Verdacht überschattet, dass das Unternehmen in die US-Geheimdienste involviert ist.

2001: Network Associates kündigt den Verkauf von PGP an.[118]

Begriffe und Hintergrund der Kryptografie

Die gesamte Natur ist nichts anderes als ein Code und eine Geheimschrift.

Blaise de Vigenère

Obwohl die Beschaffung und der Schutz von Informationen im (Des-)Informationszeitalter stark mit den gesellschaftlichen Machtstrukturen verwoben sind, ist meist nur von „Sicherheits"-Fragen die Rede. In Artikeln, Nachrichten und politischen Reden wird der Begriff Sicherheit mit einer unglaublichen Häufigkeit verwendet. Heute spielt er – der früher nur von und für Militär und Polizei verwendet wurde – bei jedem politischen Thema eine wichtige Rolle. Sogar Entwicklungshilfe und Welternährungsprogramme sehen „Sicherheit" als Teil ihrer Arbeit.

Das Thema Informationssicherheit betrifft alle, ob jemand Informationstechnologien verwendet oder nicht. Informationen über Einzelpersonen zirkulieren weltweit; meistens handelt es sich dabei um sensible Informationen wie Bankunterlagen, Versicherungs- und medizinische Daten, Kreditkarten-Transaktionen und vieles mehr. Jede Form der persönlichen oder geschäftlichen Kommunikation ist davon betroffen, darunter Telefongespräche, Fax-Nachrichten und natürlich E-Mail, nicht zu vergessen Finanztransaktionen und Business-Informationen.

Während der Markt bereits vom elektronischen Informationsfluss abhängig ist und die digitalen Werkzeuge immer leistungsfähiger und ausgeklügelter werden, wächst auch die Sorge über eine Gefährdung der Privatsphäre. Mit der fortschreitenden Verbreitung digitaler Kommunikation steigt gleichzeitig auch ihre Anfälligkeit für Missbrauch. Es

118 Für weitere Informationen zur Geschichte der Kryptografie vgl. http://cryptome.org/ukpk-alt.htm

existieren zwei konkurrierende Elemente, die dem Begriff digitale Sicherheit einen bitteren Beigeschmack verleihen: das sind auf der einen Seite die wachsenden Möglichkeiten, moderne Technologien für kriminelle Zwecke zu verwenden – nicht nur, um Taten geheim zu halten, sondern auch um beispielsweise Finanztransfers zu manipulieren. Auf der anderen Seite stehen die Regierungen vieler Staaten, die bestrebt sind, sich mit der Rechtfertigung der Verbrechensbekämpfung Zugang zu allen Daten der Bevölkerung zu verschaffen.

Für diese problematische Situation wurde bis jetzt noch keine definitive Lösung gefunden, aber zumindest wurden einige Werkzeuge zur Verbesserung der Situation entwickelt: mit Hilfe von Kryptografie gibt es die Möglichkeit, all jene Daten zu verschlüsseln, die nicht allen zugänglich sein sollen, und den ausgewählten Personen zur Dechiffrierung einen Schlüssel zur Verfügung zu stellen.

Während der vergangenen 80 Jahre hat sich die Rolle der Kryptografie von einem rein politischen Werkzeug zu einem privaten und wirtschaftlichen Nutzwert mit bedeutender politischer Dimension gewandelt. Gleichzeitig war es notwendig, die Werkzeuge zu verbessern, die ursprünglich aus der Mathematik kamen, weswegen Kryptografie zunächst sehr kompliziert wirkt.

Nach einer relativ stetigen viertausend Jahre langen Entwicklung der Kryptografie hatten folgende Erfindungen großen Einfluss auf die Geschwindigkeit der weiteren Entwicklungen: der Telegraph, das Radio und der Computer. Es sind vorwiegend wirtschaftliche, politische und militärische Gründe, die hinter der Notwendigkeit der Kryptografie stehen. Dennoch wird die Kryptografie auch für private und persönliche Interessen eingesetzt.

Verschlüsseltes Telegramm an die deutsche Botschaft in Mexico (1917)

© US National Archives and Records Administration

Schlüsselsysteme

Wenige falsche Ideen haben die Gedanken so vieler intelligenter Menschen beeinflusst wie die Überzeugung, dass sie eine unknackbare Chiffriermöglichkeit erfinden könnten, wenn sie es nur versuchten.

David Kahn

Kryptosysteme mit symmetrischem Schlüssel

Es wird immer derselbe Schlüssel für die Ver- und Entschlüsselung verwendet. In diesem Fall müssen sich der Absender und der Empfänger der Nachricht vor der Verschlüsselung auf einen gemeinsamen Schlüssel einigen. Das wichtigste dabei ist, dass sich die beiden vertrauen. Genau das ist aber auch das größte Problem bei diesem System: Wie kann der Schlüssel ausgetauscht werden, ohne dass er in falsche Hände gelangen kann? In früheren Zeiten haben Boten oder Brieftauben diesen Schlüsselaustausch vollzogen.

Symmetrische Schlüsselsysteme sind in kleinen Bereichen sinnvoll. Wenn jedoch viele Leute über ein großes Gebiet verstreut sind und dem gleichen Netzwerk angehören, wird die Verteilung des Schlüssels kompliziert. Heute werden diese Kryptosysteme von anderen Schlüsseln kontrolliert, die auf höchst komplizierten mathematischen Algorithmen beruhen.

Einige symmetrische Schlüsselsysteme sind:

- DES (Data Encryption Standard), der Standard bei Kreditkarten;
- Triple-DES, eine Variation des DES, die den Klartext dreifach verschlüsselt;
- IDEA (International Data Encryption Standard);
- Blowfish.

DES und seine Nachfolger wurden viele Jahre hindurch und von vielen Menschen erfolgreich eingesetzt, ohne dass es je zu einem Einbruch kam, und sind entsprechend weit verbreitet.

Kryptosysteme mit öffentlichem oder asymmetrischem Schlüssel

Das Beste ist es, einen einfachen, gut verständlichen Algorithmus zu verwenden, der auf der Sicherheit eines Schlüssels und nicht auf der eines Algorithmus basiert. Falls nun irgendjemand den Schlüssel stiehlt, kann einfach ein anderer hergestellt werden, und die Datendiebe müssen von vorne anfangen.

Andrew Carol

Bei Verschlüsselungssystemen mit asymmetrischem Schlüssel wird für die Ver- und Entschlüsselung jeweils ein anderer Schlüssel verwendet. Ein privater Schlüssel ist not-

wendig, der nur der betreffenden Person bekannt ist, und ein öffentlicher Schlüssel, der öffentlich zugänglich ist. Jede Person hat ihren persönlichen Schlüssel, der nie veröffentlicht wird. Er kommt nur bei der Entschlüsselung zum Einsatz. Die beiden Schlüssel sind mathematisch miteinander verbunden. Es ist aber trotzdem nahezu unmöglich, den privaten Schlüssel aus dem öffentlichen abzuleiten.
Um jemandem eine Nachricht zu senden, muss der öffentliche Schlüssel des anderen nachgeschlagen und die Nachricht damit verschlüsselt werden. Der Empfänger verwendet seinen privaten Schlüssel zur Entschlüsselung. Während es allen möglich ist, eine Nachricht mit dem öffentlichen Schlüssel zu verschicken, muss der private Schlüssel absolut geheim bleiben. Beispiele der Systeme mit öffentlichem Schlüssel sind RSA und PGP.

RSA (Rivest, Shamir and Adleman)
RSA ist wahrscheinlich eines der beliebtesten Krypto-Systeme, die einen öffentlichem Schlüssel verwenden. Mit Hilfe von RSA werden Botschaften verschlüsselt und digitale Signaturen bereitgestellt.
http://www.rsa.com

PGP (Pretty Good Privacy)
PGP ist ein Verschlüsselungsprogramm mit öffentlichem Schlüssel. Es wird vorwiegend zur Verschlüsselung von E-Mails verwendet.
http://www.pgpi.org
http://www.burks.de/krypto.html

Steganographie
Chiffren und Codes werden offen übermittelt. Alle können sehen, dass sie existieren. Bei Steganogrammen ist das nicht so. Steganographie ist die Wissenschaft, so zu kommunizieren, dass die Existenz des Geheimnisses, das ein Teil der Kommunikation ist, verborgen bleibt. Während der italienischen Renaissance und des Zeitalters Elisabeths I. in England war die Steganographie in der Politik und zu Unterhaltungszwecken sehr beliebt.

In der Literatur spielte die Steganographie eine bedeutende Rolle. Viele Steganographien aus dieser Zeit wurden erst vor kurzem entschlüsselt. Unter ihnen befinden sich einige Sonette von Shakespeare, die nun scheinbar belegen, dass der Schauspieler William Shakespeare nicht der Autor der berühmten Gedichte und Dramen war, sondern dass die Werke von Francis Bacon oder sogar Francis Tudor stammen könnten (s. „Geschichte der Kryptografie“). [119]

119 Mehr Informationen zu Steganographie: http://home.att.net/~tleary/

Digitale Wasserzeichen

Digitale Wasserzeichen sind eine Form der Steganographie: sie schützen digitale Multimediaprodukte. Sie setzen sich aus digitalen Codes zusammen, die in die Ursprungsdaten eingebettet sind. Sie versuchen, auf den ersten Blick unsichtbar zu sein, und es sollte praktisch unmöglich sein, sie zu entfernen. Bei der Erstellung eines Wasserzeichens wird eine Art Identifizierungsbild über das Originalbild gelegt (nichtdigitale Wasserzeichen wie auf Geldscheinen können gesehen werden, wenn das Papier gegen das Licht gehalten wird).

Obwohl Wasserzeichen primär dazu da sind, die großen Content-Besitzer beim „Schutz" ihres geistigen Eigentums zu unterstützen und vermeintlichem Kopiermissbrauch zu unterbinden, werden sie als etwas für die Allgemeinheit Notwendiges propagiert. Zunehmend werden Datensätze mit einem Wasserzeichen versehen, um sie auch im Internet einfach auffinden zu können und Nutzungsrechte geltend zu machen.

Digitale Signaturen, Zeitstempel etc.

Die meisten Computersysteme sind weit davon entfernt, sicher zu sein. Ein Mangel an Sicherheit könnte die Entwicklung neuer Informationstechnologien behindern. Es ist allseits bekannt, dass elektronische Transaktionen ein mehr oder weniger kalkulierbares Risiko in sich tragen. Viele Konsumenten bezweifeln, ob die Annehmlichkeiten des E-Commerce tatsächlich größer sind als seine Risiken.
Der Markt ist vom Konsumentenvertrauen abhängig. Um dieses zu gewinnen, wird eine weitere Anwendung der Kryptografie mit öffentlichem Schlüssel wichtig: die digitale Signatur, die verwendet wird, um die Authentizität des Versenders von Daten zu prüfen.
Dabei kommen ein spezieller privater und ein öffentlicher Schlüssel zum Einsatz, die die Signatur überprüfen. Das ist besonders wichtig, wenn sich die beteiligten Parteien nicht kennen. DSA (Digital Signature Algorithm) ist ein System mit öffentlichem Schlüssel, mit dem ausschließlich digitale Signaturen vorgenommen werden können, aber keine Nachrichtenverschlüsselung. Die digitale Signatur ist im privaten Sektor in der Tat das wesentlichste Werkzeug der Kryptografie.

Digitale Signaturen sind für die sichere elektronische Bezahlung notwendig. Dies ist eine von mehreren Möglichkeiten der Kryptografie, um die Daten beim Versenden zu schützen. Weitere Sicherheitsmethoden stecken diesbezüglich noch in der Entwicklungsphase, wie beispielsweise das digitale Geld (ähnlich wie Kreditkarten oder Schecks) oder digitales Bargeld, das den gleichen Grad an Anonymität bieten soll wie richtiges Bargeld und das bei den staatlichen Stellen nicht sehr beliebt ist, weil es viele Möglichkeiten für Geldwäscher und illegale Transaktionen bietet.

Grenzen der Kryptografie

Selbst mit den besten Methoden ist es unmöglich, ein absolut unknackbares kryptografisches System zu entwickeln. Zur Entschlüsselung eines Texts sind extrem viele Versuche notwendig. Die heutigen Computer würden mehrere hundert Jahre oder noch länger brauchen, um alle Möglichkeiten eines Codes auszuprobieren – und trotzdem kann der Code letztendlich geknackt werden, wie uns eines Tages die viel schnelleren Quantencomputer beweisen werden. Daher ist die Entscheidung für eine bestimmte kryptografische Methode letztlich eine Vertrauensfrage.

Für den durchschnittlichen Computernutzer ist es eher kompliziert, die Gefahren und technischen Hintergründe der elektronischen Datenübertragung zu verstehen oder sich darüber auch nur Gedanken zu machen. Die meisten Menschen, die über den eigenen Bedarf an Verschlüsselung nachdenken, sind darauf angewiesen, Spezialisten und den von ihnen verbreiteten Informationen zu vertrauen. Die Websites (und auch die Artikel und Bücher), die sich mit den Hintergrundproblemen des Themas beschäftigen, sind ebenfalls von Experten geschrieben, oftmals in der für sie so typischen wissenschaftlichen Sprache, die für Laien größtenteils unverständlich ist.

Die Tatsache, dass es schwierig ist, Gefahren zu erkennen und dass der Bedarf an Sicherheitsmaßnahmen etwas ist, was die meisten Menschen nur aus Medienberichten kennen, führt uns direkt zum Problem der unterentwickelten Demokratie im Bereich der Kryptografie.

Offensichtlich ist die Verbindung zwischen Kryptografie und Demokratie für viele Menschen nicht sichtbar. Die bereits erwähnten Medienberichte spezialisieren sich häufig auf die Berichterstattung über die Arbeit der Computer-Hacker (die mal als Verbrecher, mal als Helden präsentiert werden) und unterstreichen die Gefahr, dass es – wenn eine Kreditkarte oder andere wichtige Finanzdaten gestohlen werden – unter Umständen am eigenen Bankkonto zu missbräuchlichen Abbuchungen kommen kann.

Der Begriff Sicherheit spielt natürlich eine Rolle bei diesen Fragestellungen, unterscheidet sich aber hier wesentlich von seiner Bedeutung im Zusammenhang mit der Privatsphäre. Speziell diese zweite Bedeutung bezieht sich auf grundlegende Elemente der Demokratie.

Kryptografie und das Gesetz

Die fundamentalen Rechte des Einzelnen auf Privatsphäre, inklusive Geheimhaltung der Kommunikation und Schutz der persönlichen Daten, sollten in den nationalen Richtlinien zur Kryptografie und in der Implementierung und Verwendung kryptografischer Methoden respektiert werden.

OECD-Richtlinien [120]

120 http://www.epic.org/crypto/OECD/

Key-Recovery-Systeme

Der Sinn der Kryptografie liegt also darin, ein System zu schaffen, in dem es unmöglich ist, die verschlüsselten Daten ohne den verwendeten Schlüssel wiederherzustellen. Das Problem verlorener Schlüssel und unzugänglicher eigener Daten war der Anlass zur Entwicklung von Key-Recovery-Systemen, mit denen Schlüssel wiederhergestellt werden können. Jedoch steigen mit der Möglichkeit, einen Schlüssel wiederzubeschaffen, auch die Möglichkeit des Missbrauchs, vor allem durch Geheimdienste und Polizei, die auf die Hinterlegung von Schlüsseln bei den Behörden drängen. In den letzten zwanzig Jahren haben endlose Diskussionen über das staatliche Verbotsrecht der privaten Kryptografie und dessen Notwendigkeit stattgefunden, da die Regierungen sich selten über die Vorteile der privaten Anwender Gedanken gemacht haben. Sie selbst sind davon überzeugt, dass sie essenzielle Daten über jede Art von Feind einfangen können, und streben daher den uneingeschränkten Zugang zu allen Schlüsseln an.

Die Liste der Verschlüsselungsanforderungen mit Key Recovery, Schlüsselhinterlegung bei Behörden oder Dritten (beispielsweise Firmen), die von Regierungsstellen vorgeschlagen werden, deckt sämtliche brandneue Entwicklungen und Erfindungen im Bereich der digitalen Technologie ab. Gleichzeitig hat die National Security Agency (NSA) hart an der Durchsetzung von Gesetzen gearbeitet, um die private Verwendung starker Verschlüsselung zu verbieten. Trotzdem muss selbst eine Organisation dieser Art zur Kenntnis nehmen, dass Key-Recovery-Systeme Schwachstellen haben. Dies zeigt sich im Zusammenhang mit dem US Escrowed Encryption Standard, ein Standard zur Hinterlegung von Verschlüsselung, der die Grundlage des Clipper-Chips war (s. unten). Der Grund für solche Schwachstellen ist die hohe Komplexität solcher Systeme.

In diesem Zusammenhang muss der strenge rechtliche Rahmen zur Verwendung von Kryptografie verstanden werden, der in großem Widerspruch zum globalisierten Kommunikationsfluss steht.

Regierungseinfluss

Organisationen wie die National Security Agency (NSA) sind derzeit mit nur geringen Einschränkungen in der Lage, jedes einzelne Individuum abzuhören – auch wenn sich die NSA bemüht, ein weniger furchterregendes Bild von sich zu verbreiten. Die Kryptografie kann diese Lauschzugänge theoretisch erschweren. Daher fordern geheimdienstliche und polizeiliche Organisationen so genannte backdoors in den Codes, die ihnen den Zugriff auf verschlüsselte Daten ermöglichen. Ein flächendeckendes Projekt, alle Kommunikationstechnologien mit einer Abhörschnittstelle, einem sogenannten Clipper Chip zu versehen, ist in den USA gescheitert. [121]

121 vgl. dazu: www.epic.org/crypto/clipper

Die Verschlüsselung gewährleistet bei der Datenübertragung die Privatsphäre, die notwendig ist, wenn Nachrichten ausschließlich vom Empfänger gelesen werden sollen. Wenn Regierungen um ihre Kontrollmöglichkeiten fürchten, führt das normalerweise zu strengeren Gesetzen. Die oft gehörte Vermutung, das Internet sei ein rechtsfreier Raum, wurde bereits als falsch widerlegt. Einige Bereiche werden vom Gesetz sehr klar kontrolliert. Einer davon ist die Kryptografie. Das Verbot der Kryptografie oder zumindest ihre Einschränkung wird als angemessene Maßnahme gegen das Verbrechen betrachtet beziehungsweise galt in der Vergangenheit uneingeschränkt als solche. Mittlerweile müssen auch staatliche Einrichtungen zugeben, dass sich diese Einschränkungen vorwiegend gegen die Bevölkerung statt gegen illegale Akteure wenden. Daher wurden in den letzten fünf Jahren die Gesetze in vielen Ländern geändert. Sogar die USA, ein Land mit sehr restriktiven Kryptografie-Regelungen, haben ihre Gesetze im Jahr 2000 liberalisiert. [122]

Staatliche Regulierungen

Die neuen amerikanischen Regulierungen basieren auf der Überarbeitung des Wassenaar-Abkommens (www.wasenaar.org) aus dem Jahr 1998, wonach der lizenzfreie Export des 56-Bit-DES und ähnlichen Produkten nach einer technischen Überprüfung erlaubt ist. Dies gilt ebenso für Verschlüsselungsgüter und Software mit einer Schlüssellänge von bis zu maximal 64 Bits, die den Anforderungen des Massenmarktes entsprechen. Zu den Staaten, die von dieser neuen Regelung ausgenommen sind, gehören Libyen, Irak, Iran, Nordkorea und Kuba – Länder also, denen von der USA Förderung des Terrorismus vorgeworfen wird.

Dies ist der aktuelle Stand der Dinge in den USA, während in Deutschland das Thema Kryptografiegesetz noch auf der Tagesordnung steht. Bisher war es in Deutschland jedem selbst überlassen, eine elektronische Nachricht zu verschlüsseln oder darauf zu verzichten. Manche Organisationen befürchten aber, dass sich das bald ändern könnte. Im Februar 2000 wurde daher mit einer Aktion für die Entscheidungsfreiheit hinsichtlich Kryptografie demonstriert. Ein Argument der Regierung ist, dass Kryptografie nur von wenigen Menschen auch tatsächlich verwendet wird. Den Organisatoren der Aktion wurde daher vorgeworfen, letztendlich für einen massiveren Einsatz von Kryptografie zu werben.

Andere europäische Länder, wie z. B. Frankreich, haben liberalere Kryptografiegesetze. Österreich hat überhaupt keine Einschränkungen, was vermutlich aber eher auf ein Desinteresse der Regierung als auf eine Akzeptanz der Entscheidungsfreiheit zurückzuführen ist. Die (ehemaligen) Einschränkungen in den größeren Ländern haben die Entwicklung von noch sichereren Schlüsselsystemen beeinflusst und behindert. Unter anderem wurde dadurch die Schlüssellänge außergewöhnlich klein gehalten.

---

122 Weitere Informationen dazu unter: www.cdt.org/crypto/new2crypto/3.shtml. Die letzte Textversion der neuen amerikanischen Verschlüsselungsregulierung: www.cdt.org/crypto/admin/000110cryptoregs.shtml

Die chinesische State Encryption Management Commission (SEMC) verkündete im März 2000, dass künftig nur die starken Verschlüsselungswerkzeuge registriert werden müssen. Was auf den ersten Blick sehr entgegenkommend wirkt, entpuppt sich auf den zweiten als Makulatur, denn damit bleibt weiterhin jede brauchbare Verschlüsselungsmethode wie PGP unter staatlicher Kontrolle.

Die Einschränkungen und Verbote von Kryptografie sind Teil des staatlichen Strebens nach Kontrolle, das sich mit großer Wahrscheinlichkeit im Namen der Verbrechensbekämpfung noch weiter ausbreiten wird.

Unter dem Vorwand, so besser gegen organisierte Kriminalität vorgehen zu können, versuchen Regierungen, immer mehr Kontrolle über ihre Bürger zu erlangen. Organisationen wie die NSA treten als wichtigste Verfechter derartiger Forderungen auf. Je mehr so genannte Sicherheitsmaßnahmen getroffen werden, desto mehr Kontrolle und weniger Freiheit ist damit für die Bürger gegeben. Doch Kriminelle sind in ihrer Verwendung von Computern und in ihrer digitalen Existenz flexibel. Die meisten Bürger sind dies jedoch nicht, und damit ist es die breite Bevölkerung, die unter den negativen Konsequenzen von Überwachungstechnologien zu leiden hat.

Natürlich kann Sicherheit auch in den Dienst der Bevölkerung gestellt werden, wenn beispielsweise die Kryptografie legalisiert und damit allen zugänglich gemacht wird. Es gibt einen eindeutigen Bedarf für sichere Verschlüsselung in den Bereichen E-Commerce, Zahlungsverkehr und Übertragung privater Daten, wobei es bei hierbei vorwiegend um den Zugang zu E-Mails oder passwortgeschützen Webseiten geht. E-Mails sind nichts anderes als elektronische Postkarten. Unverschlüsselt sind sie ebenso leicht zugänglich wie Briefe ohne Umschlag, und ihr Weg kann zurückverfolgt werden, ohne dass das Passwort bekannt ist. Das Überwachungssystem ECHELON etwa durchforstet den weltweiten E-Mailverkehr nach bestimmten Stichwörtern.

Regierungen, denen an der Bekämpfung der Cyberkriminalität gelegen ist, sind daher gut beraten, die Arbeit an den neuesten Verschlüsselungstechnologien zu unterstützen statt den Zugang einzuschränken. [123]

Kryptografie und Demokratie

Die vielfältigen menschlichen Bedürfnisse und Wünsche, die zwischen zwei oder mehreren Menschen nach einer Privatsphäre inmitten des Soziallebens verlangen, müssen überall dort, wo Menschen leben und schreiben, zwangsläufig zur Kryptografie führen.

David Kahn, The Codebreakers

123 Mehr dazu: http://www.cdt.org/crypto/risks98/

Im Zeitalter des „gläsernen Menschen“, dessen Daten nicht nur von verschiedensten Institutionen gesammelt, sondern auch unter Verschluss gehalten werden und dabei unerreichbar, unkontrollierbar und für den Einzelnen nicht steuerbar sind, erlangt die Privatsphäre eine neue Bedeutung. Die Ironie hierbei ist, dass genau diejenigen, die Kryptografie zum Schutz der Privatsphäre fordern, denselben Forschern und Institutionen vertrauen müssen, die auch die Methoden zur Erschaffung des gläsernen Menschen entwickelt haben.

Beim Thema Teledemokratie wird klar, dass Kryptografie und Demokratie einen engen Bezug zueinander haben. Die Bevölkerung kann ihre Reaktionen auf bestimmte staatliche Institutionen und Entscheidungen bereits vielfach im Internet abgeben. Viele bürokratische Pflichten können ebenfalls über das Internet erfüllt werden. Am 8. Februar 2000 wurden die weltweit ersten Wahlen via Internet durchgeführt, die Wahlen des Studentenausschusses an der Universität Osnabrück.[124] Das Projekt namens i-vote (www.internetwahlen.de), das eine Vorlaufzeit von 10 Monaten hatte, schrieb Geschichte. Um ein korrektes Ergebnis zu erzielen, wurden – ähnlich wie bei der digitalen Signatur – mehrere verschiedene Verschlüsselungsprozesse gleichzeitig eingesetzt. Des weiteren wurden eine Blende zur Anonymisierung der Stimme und ein virtueller Stimmzettel verwendet, der ebenfalls verschlüsselt werden musste, da einfache E-Mails zurückverfolgt werden können. Die Verwendung von Kryptografie in einer Teledemokratie hat sich als unumgänglich erwiesen. Aber wird dadurch im Gegenzug auch die Entwicklung der Kryptografie geöffnet und demokratisiert werden? Oder ist eher zu erwarten, dass staatliche Einschränkungen und Kontrollen dann noch weiter verschärft werden?

Der Algorithmus als Code nimmt die Verschlüsselung vorweg. Als Alan Turing an seiner als Turing-Maschine bekannt gewordenen Variation des Perpetuum mobile arbeitete, schwebte ihm ein Computer vor, dessen Konstruktion nicht unabhängig von den mit ihm durchgeführten Arbeitsprozessen sein sollte, sondern von diesen ständig beeinflusst und neu gestaltet wurde. Die Maschine wurde so gewissermaßen zu ihrem eigenen Algorithmus – was eine Neuinterpretation von Dialektik erforderlich machte. Nicht zuletzt deswegen hat die Turing-Maschine das philosophische Denken inspiriert.

Genau hier berührt die theoretische Arbeit zu Verschlüsselungssystemen die Frage nach der modernen Demokratie, die Unterscheidung zwischen privat und öffentlich, indem der Anwender immer Teil des technischen Arrangements wird: Die lange verwendeten Begriffe rund um Demokratie sind im Zusammenhang mit Kryptographie nicht mehr brauchbar. Man könnte sagen, das Internet sei eine private Angelegenheit. Mit demselben Anspruch auf Richtigkeit ließe sich das Gegenteil behaupten. Dennoch

124 www.politik-digital.de/e-demokratie/forschung/wahlen.shtml

sind beide Sätze falsch. Niemals kann man im Internet gänzlich privat sein; ebenso wenig öffentlich im klassischen Sinne. Der virtuelle Raum lässt beides nicht mehr zu. Die ursprünglich gängigen Begriffe und deren ursprüngliche Bedeutungen lösen sich im virtuellen Raum bis zur Unkenntlichkeit auf.

Die Kryptografie, die zum Schutz der Privatsphäre eingesetzt wird, kann keine absolute Privatsphäre gewährleisten, da ihre Entwicklung beständig von der großen Gefahr eines Entschlüsselungsversuchs überschattet wird. Spätestens mit dem bereits entstehenden Quantencomputer werden die Muster der verschlüsselten Information nicht mehr sichtbar sein. Gleichzeitig scheinen die genauen Bedeutungen von sozialen Beziehungen zu verschwimmen. Die Demokratie braucht etwas, worauf sie sich stützen kann, einen Bezugsrahmen, genau wie sie das Private und das Öffentliche braucht. Dennoch entspringt der Bedarf an Kryptografie, Information und Entschlüsselung unserem Bedürfnis nach Privatsphäre einerseits und unserer Neugierde andererseits. Dabei gibt es einen wesentlichen Unterschied zwischen dem Schutz der Privatsphäre und der Geheimhaltung: „Die Privatsphäre ist für eine offene Gesellschaft im elektronischen Zeitalter notwendig. Privatsphäre ist nicht gleichzusetzen mit Geheimhaltung. Eine Privatangelegenheit ist etwas, bei dem man nicht will, dass es die ganze Welt weiß, aber eine geheime Angelegenheit ist etwas, von dem man nicht will, dass es irgendjemand weiß. Privatsphäre ist die Macht, sich der Welt selbstbestimmt und selektiv zu öffnen.“ [125]

Zukunftsaussichten

Wissenschaftler arbeiten intensiv an der Entwicklung des Quantencomputers und an der Quanten-Kryptografie. Gleichzeitig ist es vorstellbar, dass in den nächsten Jahren auch eine Revolution in der Kryptografie auf uns zukommen wird. Wenn diese Meilensteine erreicht sind, werden unsere jetzigen Hardware- und Software-Werkzeuge im wahrsten Sinne des Wortes alt aussehen. Die Auswirkungen der neuen Werkzeuge auf die Kryptografie und auf demokratische Entwicklungen sind derzeit noch nicht absehbar; wir sollten uns gleichzeitig auf das Beste und das Schlimmste gefasst machen. Eine gewisse Portion Pessimismus und Verfolgungswahn sind wahrscheinlich die richtige emotionale Mischung, um diesen Entwicklungen zu begegnen, besonders seit den Ereignissen des 11. September 2001, die einer Politik Vorschub geleistet haben, die die Überwachung favorisiert. Dennoch ist noch offen, ob die Wissenschaft im Dienste der demokratischen Freiheiten arbeitet oder nicht. Die zunehmende Geschwindigkeit in der Datenübertragung wird eine ebenso zunehmende Geschwindigkeit der Entwicklung von Verschlüsselungsmethoden erfordern. Wir leben in einer Gesellschaft, in der Arbeit und Privates immer stärker zusammenwachsen. Gegen diesen Prozess kann auch die Kryptografie nichts ausrichten. Die Fragen zum Schutz der Privatsphäre gehen

125 Cypherpunk's Manifesto, http://www.activism.net/cypherpunk/manifesto.html

über den technologischen Bereich hinaus und sind eng verbunden mit Menschenrechtsfragen, die letztlich den Kern wahrhaft demokratischer Politik ausmachen.

5.3 Biometrie

Absolute Identifizierung ist eine verlockende Idee, unglücklicherweise hat sie einen fundamentalen Fehler: Diese Methoden identifizieren nicht Menschen, sondern Körper. [126]

Simson Garfinkel, Autor von „Database Nation"

Mittel zur Identifizierung

Auf Grund der zunehmenden Beschleunigung der Gesellschaft werden die Prozesse zur Identifizierung des Individuums zunehmend technisiert. Denn einerseits kann den traditionellen bürokratischen Identifikationstechnologien ausgewichen werden – Reisepässe und Unterschriften können gefälscht und Daten können manipuliert werden. Zum anderen sind die bürokratischen Identifikationstechnologien auch sehr langsam und können mit der Informatisierung nicht Schritt halten. Die Lösung dieses Problems wird heute von Industrie und Regierungen bevorzugt in der Biometrie gesehen: die automatische Identifizierung durch die digitale Vermessung von Körpermerkmalen, die bei jeder Person anders ausgebildet sind: etwa die Iris oder Fingerabdrücke.

Identifizierungsmittel in der Geschichte

In den biometrischen Technologien wird das Subjekt auf seine physischen, unveräußerlichen Eigenschaften reduziert. Das Subjekt ist nur mehr insofern ein Subjekt, als es zum Objekt der Vermessung gemacht werden kann. Sobald es diesem Prozess, der sich aus dem Bestreben nach Messbarkeit ergibt, Widerstand leistet, sind persönliche Nachteile in Kauf zu nehmen. Die Biometrie stellt den Traum der vollkommen sicheren Identitätskontrolle in Aussicht.

Die Frage der Identifizierung ist nicht auf den modernen Staat beschränkt. Die Babylonier und Chinesen verwendeten Fingerabdrücke in Ton, um die Verfasser von Schriftstücken zu identifizieren, während die Römer bereits Handschriften systematisch verglichen.

Besonders bedeutsam ist die Identifizierung im Militär. Zu den ersten Maßnahmen, denen die Soldaten beim Eintritt in das Militär unterzogen werden, zählen Identifizierungsprozesse und die Erhebung der Körpermaße. Diese Maße werden katalogisiert, mit anderen Daten verbunden und ergeben den sogenannten Datenkörper der Soldaten. Wenn die Datenkörper in Besitz der Staatsgewalt sind, so sind die Soldaten nicht mehr in der Lage, sich frei in ihrem sozialen Gefüge zu bewegen, sondern abhängig von

126 http://www.zeit.de/2001/46/Wissen/print_200146_biometrie.html

der Disziplinärstruktur der militärischen Institutionen. Die soziale Existenz der Soldaten wird so von den militärischen Institutionen definiert.
Dabei gilt es zu berücksichtigen, dass in modernen Gesellschaftsformen die militärischen und zivilen Bereiche ineinander übergreifen. Die Ambivalenz der hochentwickelten Technologien führt dazu, dass häufig nicht mehr eindeutig unterschieden werden kann, ob eine Technologie für demokratische oder autoritäre Zweck eingesetzt wird. Die Vermessung körperlicher Eigenschaften und die Erschaffung von Datenkörpern kommen in allen Bereichen der modernen Gesellschaften zur Anwendung.

Biometrische Technologien

Im folgenden Abschnitt werden die wichtigsten biometrischen Technologien kurz beschrieben. Eine gängige Definition des Begriffes Biometrie ist die „automatisierte Identifizierung einer Person auf Basis ihrer physiologischen Eigenschaften oder Verhaltensweisen“. [127]

Im Kontext von IT-Umgebungen kommt die Biometrie für Sicherheitstechnologien zum Einsatz, deren Aufgabe es ist, den Zugang zu Informationen, Orten und anderen Ressourcen einzuschränken und nur einer bestimmten Personengruppe zugänglich zu machen.

Alle biometrischen Technologien basieren auf den gleichen Prozesskomponenten. Ausgangspunkt ist eine biometrische Messung, die anschließend in digitale Information umgewandelt und als biometrische Vorlage der betreffenden Person gespeichert wird. Bei jeder erneuten Identifizierung wird eine weitere Messung vorgenommen und die Übereinstimmung mit dem vorliegenden Muster überprüft. Wenn die beiden Messungen identisch sind, so ist die Identität der Person bestätigt, und das System weiß, wer die Person ist. So kann zum Beispiel der Zutritt zu Gebäuden oder zu Informationsressourcen gestattet oder verweigert werden.

Es bedeutet aber auch, dass gleichzeitig Informationen über das Verhalten oder die Bewegungen der betreffenden Person gesammelt wurden. Das System weiß, wer zu welchem Zeitpunkt und mit welchen Zeitabständen auf welchen Identifizierungs-Checkpoint zugegriffen hat. Das System kann diese Daten mit anderen Daten verbinden und sich damit den Datenkörper eines Individuums aneignen.

Gesichtserkennung

Um eine andere Person zu erkennen, blicken wir ihr zumeist ins Gesicht, da die sichtbaren Unterscheidungsmerkmale im Gesicht konzentriert auftreten. Insbesondere die

127 http://biometrics.cse.msu.edu/info.html

Augen scheinen nicht nur darüber Auskunft zu geben, wer jemand ist, sondern auch wie sich diese Person fühlt, worauf ihre Aufmerksamkeit gerichtet ist usw. Will jemand seine Identität oder die Sichtbarkeit innerer Vorgänge verbergen, so muss er sich maskieren. Daher kann die Gesichtserkennung als eine Art elektronischer Demaskierung bezeichnet werden.

Die Kommunikation von Angesicht zu Angesicht ist ein Austauschprozess, der in zwei Richtungen funktioniert. Jemanden anzusehen, bedeutet das eigene Gesicht zu exponieren und es dem anderen zu ermöglichen, einen selbst anzusehen. Jemanden zu beobachten, ohne selbst von der Person gesehen zu werden, versetzt die exponierte Person gegenüber dem Zuseher in eine angreifbare Position.

Muster für Gesichtserkennung
© *MIT*

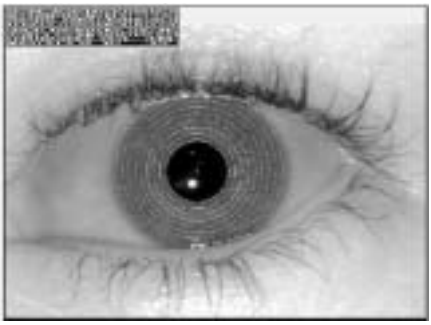
Iriserkennung

Iriserkennung stützt sich auf die Tatsache, dass die Retina jedes Individuums eine individuelle Struktur besitzt. Die Oberfläche der Iris setzt sich aus einem Kranz, Vertiefungen, Fäden, Flecken, Gruben, ringförmig angeordneten Rillen und Wellen zusammen, die in unendlich vielen verschiedenen Variationen erscheinen und in ebenso vielen Arten miteinander kombiniert sind. Iris-Scanning gilt als ganz besonders genaue Identifizierungstechnologie, da sich die Eigenschaften der Iris im Leben eines Menschen nicht verändern und weil eine Iris mehrere hundert messbare Variablen aufweist. Überdies ist es ein schnelles Verfahren, das nicht länger als ein bis zwei Sekunden dauert.

All diese Eigenschaften haben die Iriserkennung zu einer attraktiven Technologie im Einsatz für Sicherheitsanwendungen gemacht, wie beispielsweise für die Gefängnisüberwachung. Die Iristechnologie wird aber auch für Onlineanwendungen eingesetzt, wo sie die Identifizierung via Passwort ersetzen kann. Wie auch im Fall der anderen

biometrischen Technologien ist die Verwendung von Iris-Scanning zum Schutz privater Bereiche eine zweischneidige Angelegenheit. Denn der Schutz gegen den Identitätsdiebstahl funktioniert nur horizontal, nicht vertikal, also etwa im Falle der Dateneignung durch Behörden: die Datenbeschaffung, die während der Identifizierung geschieht, wird auch nicht als Diebstahl der Identität einer Person durch das biometrische System bezeichnet.

Im Prozess der Iriserkennung trifft die biometrische Technologie beinahe buchstäblich ins „Schwarze des Auges". In einer Welt, die mit sich verändernden und manipulierten Bildern übersättigt ist, setzt man auf die Iris, um an die „letzte Wahrheit" in Form einer digital artikulierten Identität heranzukommen.



Iris-Vermessung
© Telecommunications Software and Multimedia Laboratory

Fingerabdruckerkennung

Während dem Fingerabdruck mit Papier und Stempelkissen der Ruch vordigitaler Polizeitechniken anhaftet, scheint sich sein digitaler Nachfolger als weit verbreitete biometrische Technologie zu etablieren. Die Fingerabdruckerkennung beruht auf der Tatsache, dass die Einzigartigkeit eines Fingerabdruckes durch die Analyse winziger Merkmale wie Schweißdrüsen, Rillenabstände und Verzweigungen definiert werden kann. Die Wahrscheinlichkeit, dass zwei Individuen den gleichen Fingerabdruck haben, wird auf weniger als eins zu einer Milliarde geschätzt.

Als Zugangskontrolle ist der digitale Fingerabdruck vorwiegend bei militärischen Einrichtungen wie dem Pentagon und Forschungszentren der Rüstungsindustrie verbreitet. Auch bei Banken kommt diese Technologie stark zum Einsatz, und große Kreditkarten-Unternehmen wie Visa und MasterCard streben eine breite Integration dieser Fingerabdruckmethoden im Bankkartenbereich an.

Ein großes Hindernis stellen Ungenauigkeiten dar, die durch fettige, verschmutze oder rissige Haut auftreten. Dieses Problem wurde vor kurzem durch die Entwicklung einer Vorrichtung gelöst, die in der Lage ist, die spezifischen Eigenschaften eines Fingerab-

drucks ohne direkten Hautkontakt aufzuzeichnen, zu digitalisieren und in ein digitales Bild umzuwandeln. [128]

Wie auch bei anderen biometrischen Technologien treffen bei der Fingerabdruckerkennung der staatlich kontrollierte Polizei- und der zivile Sicherheitsmarkt aufeinander – was einmal mehr bestätigt, dass im Hightechmarkt das Zivile und das Militärische nicht eindeutig zu trennen sind. So scheint die Utopie einer gefängnisfreien Gesellschaft in die Reichweite einer Technologie zu kommen, die von einer sich rasch drehenden Spirale aus Identifikationserfordernissen und Identifikationstechnologien zügig weiterentwickelt wird und letztlich die freie Bewegung durch eine Simulation derselben zu ersetzen im Stande ist: dies ist zum Beispiel bei den von Digital Angel entwickelten elektronischen Fußfesseln der Fall, die die jeweilige Position von auf Bewährung freigelassenen Gefangenen an die Polizei übermitteln.

Handerkennung

Bei der Handerkennung wird ein dreidimensionales Bild der Hand erstellt und mit einem entsprechenden gespeicherten Bild verglichen. Die dazu nötigen Geräte sind im Gegensatz zu den Geräten zur Vermessung von Fingerabdrücken oder der Iris recht sperrig. Sie sind aber in der Lage, umfassende Identifizierungsvorgänge in kürzester Zeit durchzuführen. Sie kommen daher vorwiegend an Orten wie Flughäfen zum Einsatz, wo es darauf ankommt, viele Menschen in kurzer Zeit zu identifizieren.

Stimmerkennung

Stimmerkennung ist die einzige biometrische Technologie, die nichtvisuelle Eigenschaften des menschlichen Körpers vermisst. Hier werden die Tonvibrationen in der Stimme einer Person gemessen und mit bestehenden Mustern verglichen. Normalerweise muss dazu die zu identifizierende Person ein bestimmtes Erkennungswort oder einen ganzen Erkennungssatz aussprechen, die den Verifizierungsprozess zusätzlich unterstützen. Diese Methode kann selbst am Telefon angewendet werden, hat aber einen großen Schwachpunkt, nämlich die Empfindlichkeit gegen Interferenzen und Hintergrundgeräusche.

Gangerkennung

Es ist eine relativ neue Erkenntnis der Biometrie, dass die Identität einer Person nicht ausschließlich anhand äußerlicher Merkmale oder der Stimme festgelegt werden kann, sondern auch anhand der Gangart.

Anders als die bereits besser ausgereiften biometrischen Technologien, bei denen Körperteile untersucht werden, unterliegt die Erkennung der Gangart der zusätzlichen

128 www.ddsi-cpc.com

Schwierigkeit, Bewegungen als Muster aufzuzeichnen und zu identifizieren. Wissenschaftler der Universität Southampton haben ein Modell entwickelt, das die Beinbewegungen als Pendelbewegungen wahrnimmt und die Hüftneigung als Variable definiert. [129]

Bei einem anderen Modell werden Form und Länge der Beine zusätzlich zur Geschwindigkeit der Gelenksbewegungen gemessen. Ziel der Forscher ist es, beide Modelle zusammenzuführen. Damit würde die Identifizierung anhand der Gangart zu einer voll einsatzfähigen biometrischen Technologie werden.

Die Anwendung dieser Technologie auf bewegliche Subjekte macht sie als Überwachungstechnologie besonders interessant. So wird an der University of Leeds an Computermodellen gearbeitet, die es ermöglichen, auffällige Bewegungsabläufe von Menschen zu erkennen: etwa die eines potenziellen Autodiebs auf einem Parkplatz oder eines Menschen auf einem Bahnsteig, der im Begriff ist, sich vor den Zug zu stürzen. [130] Weibliche Ladendiebe, die sich als Schwangere tarnen und so die Beute verstecken, können aufgedeckt werden, da tatsächlich Schwangere anhand ihres Ganges vom System erkannt werden können.

Personenerfassung mit feststehender Kamera
© University of Leeds

Andere biometrische Technologien

Andere biometrische Technologien, die hier nicht im Detail besprochen werden, beruhen auf besonderen Merkmalen von Ohr, Unterschrift, Tastaturanschlag, Venenmuster, Retina, Körpergerüchen oder DNA. Diese Technologien stecken entweder noch in frühen Entwicklungsstadien oder werden in hoch spezialisierten und daher eingeschränkten Bereichen eingesetzt.

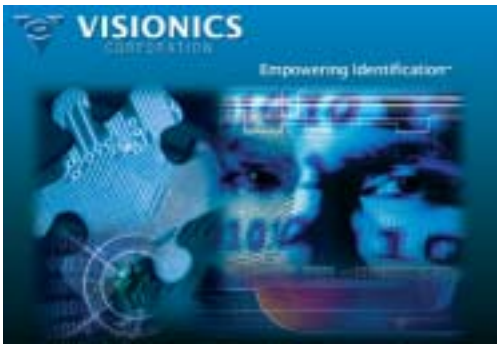
129 www.isis.ecs.soton.ac.uk/image/gait/
130 www.comp.leeds.ac.uk/vision/imv/index.html

Einsatzgebiete von biometrischen Technologien

Bewachung

Identität hat etwas mit Verortbarkeit zu tun. In weniger mobilen Gesellschaftsformen ist der Ort ein aussagekräftiges Kriterium für die Identität einer Person. Vor dem industriellen Zeitalter wurde der Zugang zu bestimmten Orten durch Wachpersonal reguliert. Diese identifizierten die ankommenden Personen und entschieden dann, ob der Person tatsächlich der physische Zugang zu einem bestimmten Ort wie einer Stadt, einem Gebäude oder einem Fortbewegungsmittel genehmigt wurde.

In den modernen Gesellschaften wurde die Eindeutigkeit des Ortes geschwächt, die körperliche Mobilität hat enorm zugenommen. Die Virtualisierung von Orten findet speziell seit der Verbreitung von elektronischen Kommunikationstechnologien statt, wo der Raum zum virtuellen Raum wird. Die Frage nach der eigenen Identität ist nicht mehr an einen physischen Ort gebunden. Die in höchstem Maße mobilen und virtualisierten sozialen Kontexte erfordern daher neue Technologien der Identifikation im Hinblick auf die Zugangskontrolle, welche man sich von der Biometrie erhofft.



Web-Seite von Visionics

© Visionics, Inc.

Körperliche Zugangskontrolle

Dies ist der größte Anwendungsbereich von biometrischen Technologien und auch der Bereich, bei dem der Vergleich mit dem feudalen Wachpostensystem am passendsten ist. Die körperliche Zugangskontrolle mittels biometrischer Technologien kam ursprünglich vorwiegend beim Militär und anderen Hochsicherheitsanlagen zum Einsatz, mittlerweile hat sich der Anwendungsbereich allerdings stark verbreitert. Biometrische Technologien für die Zugangskontrolle werden bereits in Schulen, Supermärkten, Spitälern und Einkaufszentren verwendet, wo sie den Zutritt des Personals regeln.

Aber auch der Zugang zu politischen Territorien wird durch biometrische Technologien kontrolliert. Beispielsweise wird der Immigrantenfluss an Flughäfen und an den stark frequentierten Grenzen, wie zwischen den USA und Mexiko, auf diese Weise

kontrolliert. In diesem Fall werden die biometrischen Technologien mit Kameraüberwachungssystemen und Entwicklungen aus der künstlichen Intelligenz gekoppelt, um potenziell verdächtige Personen an unbewachten Grenzübergängen zu identifizieren. [131]

Eine elektronische Variante des feudalistischen Bewachungssystems ist in den USA bereits an mehreren Grenzübergängen im Einsatz, um „riskante" Reisende aus der Menge herauszufiltern. Als Nebeneffekt hat die Effizienz dieser Inspektionssysteme dazu geführt, dass die Anzahl der Drogenbeschlagnahmungen gestiegen ist, da den Inspektoren mehr Zeit zur Verfügung steht, Fahrzeuge zu untersuchen, die mit einem hohen Risikofaktor eingestuft sind.

Biometrische Kontrollsysteme verhindern aber nicht nur, dass Personen in bestimmte Bereiche oder Orte eindringen können, sondern auch, dass sie aus bestimmten Gebäuden, wie beispielsweise aus Gefängnissen, herauskönnen.

Zugang zu Rechten

In manchen Ländern, wie unter anderem in Mexiko und Spanien, werden Identifizierungskarten mit digitalisierten Fingerabdrücken bei Wahlen verwendet.
Biometrische Identifizierungstechnologien halten aber auch im Gesundheitswesen vieler Staaten Einzug, mit der Begründung, ungerechtfertigte Inanspruchnahme von Leistungen zu verhindern, wie etwa in der kanadischen Provinz Ontario.

Zugang zum virtuellen Raum

Dieser Bereich beinhaltet Zugang zu Computerinformationen, wie beispielsweise den Zugriff auf Datenbanken. Statt ein Passwort einzutippen, könnten die Anwender beispielsweise ihren Fingerabdruck, ihre Iris oder ihr ganzes Gesicht von einem in den Computermonitor integrierten Gerät lesen lassen.

Biometrie und Überwachung

Biometrische Technologien sind nicht automatisch Überwachungstechnologien. Als Technologien, die zu Identifizierungszwecken verwendet werden, liefern sie aber einen wichtigen Beitrag zur Überwachung. Mit Hilfe von Kombinationen aus Gesichtserkennungssystemen, Kamerasystemen und Polizei-Datenbanken werden öffentliche Plätze überwacht und einzelne Personen herausgefiltert. Diese Art von biometrisch verstärkter Kameraüberwachung ist insbesondere in Großbritannien im Einsatz; der Londoner Stadtteil Newham ist bereits flächendeckend mit Kameraüberwachung ausgestattet [132] (s. oben, Überwachung des öffentlichen Raumes).

131 Beispiele: www.ins.usdoj.gov/graphics/lawenfor/bmgmt/inspect/rvis.htm
132 www.spy.org.uk/n-mandrake.htm

Bei biometrischen Anwendungen im Bereich der Zugangskontrolle ist der Dateneingabeprozess den Anwendern bewusst. Im Unterschied dazu wirft die laufende Datenentnahme bei den biometrischen Anwendungen in der Überwachung kritische Fragen auf, da die Datenentnahme von den betreffenden Personen nicht wahrgenommen wird.

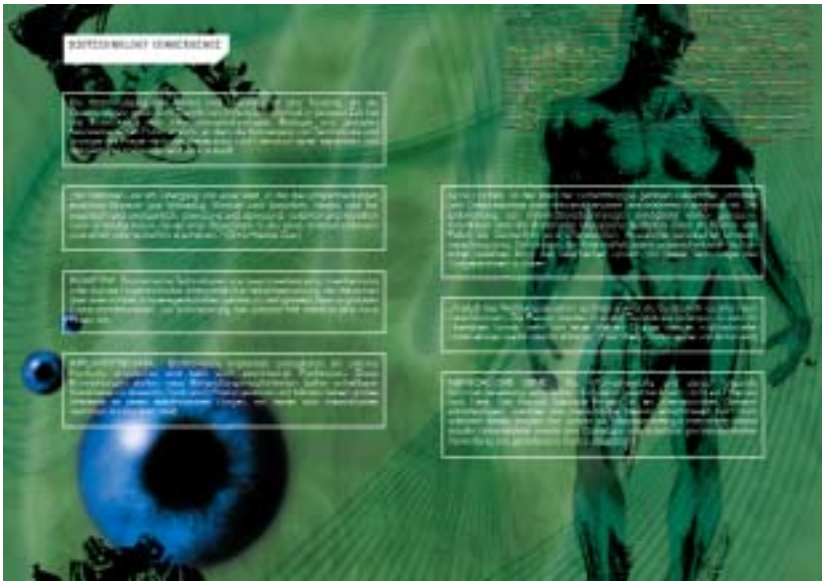
Bedrohte Privatsphäre

Alle biometrischen Technologien sammeln biometrische Personendaten. Sind diese Daten einmal vom System erfasst, können sie im Grunde jeder beliebigen anderen Stelle zugänglich gemacht werden, ohne dass dies der betroffenen Person bekannt wird. Diese Daten können vielen unterschiedlichen Verwendungszwecken zugeführt werden, die möglicherweise die Privatsphäre einer Person verletzen.

Aus technischer Sicht ist es einfach, biometrische Daten mit anderen Personendaten aus Behörden- oder Firmendokumenten abzugleichen. Damit wären wir dem transparenten Bürger und dem Kunden, dessen Datenkörper außerhalb seiner eigenen Kontrolle liegt, einen Schritt näher. Auch wenn biometrische Technologien oft als Beschützer der persönlichen Daten und als Sicherheitstechnologie gegen den „Identitätenraub" vorgestellt werden, können sie auch zum Fortschritt der Big-Brother-Technologien beitragen.

Die Kombination aus personalisierten Akten und biometrischen Daten bietet ein enormes Kontrollpotenzial. Auch wenn sich niemand in der Regierung oder der Industrie zu solchen Intentionen bekennt, ist es interessant, dass führende Firmen wie EDS (Electronic Data Systems, www.eds.com), die auf Datenmanagement spezialisiert sind, auch biometrische Systeme an die Geheimdienste der Regierung und der Industrie liefern.

Biometrische Technologien werden zu Identifizierungszwecken verwendet. Die Geschichte zeigt, dass Identifizierungsmechanismen eine notwendige Voraussetzung für Machtausübung sind. Dabei werden jeweils nur die Personen geschützt, die nicht in Konflikt mit dieser Macht stehen. Sollte die Digitalisierung des Körpers mittels biometrischer Technologien tatsächlich so weite Verbreitung finden, wie es sich ihre Befürworter erhoffen, so könnte sich ein neues, elektronisches feudales System entwickeln. In diesem System würden die Menschen als Datenkörper erfasst. Die Freiheit, sich zu bewegen, zu handeln, zu kommunizieren wird dadurch begrenzt, dass es Kontrollinstanzen gibt, die über jede Bewegung, über jeden Austausch Bescheid wissen. Die Bürger würden zu „digitalen Untertanen", die Macht selbst bleibt dabei unsichtbar: während die Wachposten der mittelalterlichen Städte durch ihre Uniformen identifizierbar waren, sind biometrische Technologien nur mehr reine Masken, hinter denen sich kein wahres Gesicht verbirgt. Eine Situation, die manche an Kafkas Roman „Das Schloss" erinnern mag: auch hier ist die Autorität durch ihre Abwesenheit auf besondere Weise präsent.



Größere Abbildung auf Seite 262

5.4 ECHELON

In ECHELON liegt ein riesiges Potential zu Verletzungen der Privatsphäre und zum Missbrauch der Demokratie. Weil es so machtvoll ist und seine Operationen so verborgen bleiben, erlegt es Geheimdiensten keine wirklichen Einschränkungen auf, sodass sie es gegen jegliches Ziel einsetzen können, das die Regierung wählt. Der übertriebene Geheimhaltungsapparat, der während des Kalten Krieges aufgebaut wurde, beseitigt schon die bloße Androhung einer Rechenschaftspflicht.

Nicky Hager, Autor von „Secret Powers“

ECHELON ist ein hochautomatisiertes, gestaffeltes System und Überwachungsnetzwerk, um Daten auszuwerten, die man durch das Abhören von Kommunikationsverkehr aus der ganzen Welt erhalten hat. Es wird von den wichtigsten Nachrichten- und Geheimdiensten aus fünf Nationen betrieben, die auf der Grundlage verschiedener Abkommen zusammenarbeiten: die Vereinigten Staaten, Großbritannien, Kanada, Australien und Neuseeland. Offiziell wird behauptet, ECHELON diene dazu, den Terrorismus, den illegalen Waffenhandel und andere Verbrechen zu bekämpfen. Aber in den letzten Jahren wurde offenkundig, dass das System auch auf die wirtschaftliche, diplomatische und private Kommunikation in den teilnehmenden Ländern ausgerichtet ist.

Das UKUSA-Abkommen

Die angeführten Länder koordinieren ihre Aktionen unter der Führung der National Security Agency (NSA) der USA auf der Grundlage des UKUSA-Abkommens, das im März 1946 geschlossen wurde. Die Vereinigten Staaten und Großbritannien hatten damals durch die Entschlüsselung der im Zweiten Weltkrieg eingesetzten Chiffriermaschinen „Enigma“, „Fish“ und „Purple“ bereits eine Art Tradition in kryptoanalytischen Verfahren. Das in diesem Zusammenhang entstandene Bündnis von USA, Großbritannien, Kanada, Australien und Neuseeland wurde in die Form des UKUSA-Signal- und Aufklärungs-Abkommens überführt, welches in erster Linie gegen die UdSSR und andere kommunistisch regierte Staaten gerichtet war. Obwohl das Abkommen anscheinend nur von den Vereinigten Staaten und Großbritannien unterzeichnet ist – genaue Informationen sind aufgrund des geheimen Charakters des Dokuments nicht zugänglich – gehören auch die Geheimdienste einer Anzahl anderer Länder der UKUSA-Gemeinschaft an, wie etwa Deutschland, Österreich, Japan, Norwegen, Südkorea und die Türkei.

Größere Abbildung auf Seite 264

Diese Länder werden manchmal als „Drittbeteiligte“ des Abkommens bezeichnet, denn ihr Zugang zu den abgehörten Daten und deren Analyse ist eingeschränkt. Zusätzlich beherbergen einige Länder wie z. B. China Stationen der UKUSA-Signalaufklärung (Signals Intelligence, SIGINT) oder nehmen in anderen begrenzten Formen an der SIGINT der UKUSA-Länder teil. Die UKUSA-Mitglieder verständigten sich darauf, Terminologie,

Codewörter, Methoden des Abhörens und die Geheimhaltungsabkommen, denen jede mit Aufgaben der UKUSA betraute Person zustimmen muss, aus Gründen von Effizienz und Sicherheit zu standardisieren. Über die Jahre entwickelte sich die UKUSA-Partnerschaft zu einer einzigartigen überstaatlichen Körperschaft, die dem Blick der Öffentlichkeit vollkommen verborgen blieb. Das Hauptquartier dieser virtuellen Nation war und ist Crypto City, die Gebäude der NSA in Fort Meade im US-Bundesstaat Maryland.

Das globale System

Vor 1971 wurde noch ein Großteil der eingehenden Information manuell ausgewertet. Zu jener Zeit baute die NSA unter dem Codenamen PLATFORM ein gewaltiges Computer-Netzwerk auf, das 52 Systeme, die sich im Besitz der um den Erdball verstreuten Mitglieder befanden, miteinander verknüpfte. Das Software-Paket, das die SIGINT-Operationen der einzelnen Partner zusammenführte, trug den Codenamen ECHELON. Die Ressourcen und die Prioritäten haben sich seit seiner Einrichtung stark erweitert. In den späten 80er Jahren, während des Siegeszuges relativ billiger Kommunikations-Satelliten, gab es kaum einen Winkel auf der Erde, der nicht durch eine Abhöranlage oder eine Satellitenüberwachungsstation aus dem Besitz eines der UKUSA-Mitglieder kontrolliert war. Damit ist es ECHELON möglich, jegliche Art von unverschlüsselter und einige Arten von verschlüsselter Kommunikation, insbesondere solche, die in standardisierten Verfahren verschlüsselt wird, auf der ganzen Welt abzuhören und zu verarbeiten. ECHELON soll täglich bis zu 3 Milliarden Kommunikationsverbindungen abhören und dabei sowohl Telefon- und Faxverbindungen, E-Mail-Verkehr, Internet-Chats, Newsgroups und ähnliches erfassen.

Das ECHELON-System erfasst all diese Verbindungen wahllos über verschiedene „Schnüffel"-Einrichtungen. Diese „Schnüffler" (ähnlich wie das berüchtigte CARNIVORE, das vom FBI speziell für das Abhören von Kommunikation über E-Mail verwendet wird) sammeln Informationen über Datenpakete, wenn sie das Internet über verschiedene Knotenpunkte durchwandern. Dann filtert das System mit Hilfe von Spracherkennungstechnologie und künstlicher Intelligenz die Information heraus, die von Interesse ist – ähnlich wie es Suchmaschinen wie Google oder Altavista tun, aber auf wesentlich höherem Niveau. Die NSA hält in diesem Technologie-Bereich mehrere Patente, wie z. B. das berühmte „Semantic-Forest"-Patent zur Themenanalyse (US-Patent-Nummer: 5937422). Einige Stimmen behaupten, dass ECHELON ca. 90 Prozent der täglichen Kommunikation im Internet durchsiebt.
Das ECHELON-System kann Daten über eine Reihe verschiedener Schnittstellen sammeln. Es gibt riesige landgestützte Empfangsstationen, um Satellitenübermittlungen abzufangen. Zusätzlich können angeblich an einigen Orten Hoch- oder Höchstfrequenz-Fernmeldeübermittlungen, die via Kabel über Land erfolgen, angezapft werden. Die Stationen dienen als Bodenstationen für Spionagesatelliten, die „Überlauf"-Daten von Übermittlungen zwischen Städten abfangen. Diese Satelliten übertragen die Infor-

mation dann zu geheimen Auswertungszentren am Boden. Die Hauptzentren liegen in den Vereinigten Staaten, in England, Australien, Japan und Deutschland.

ECHELON-Abhörstation
Menwith Hill, UK
© Federation of American Scientists

Des weiteren gehören zu ECHELON spezielle Unterwasser-Vorrichtungen, die die Kabel anzapfen, die transkontinentale Telefongespräche übermitteln. In der Ära der Kupferkabel begannen die Vereinigten Staaten mit speziell ausgerüsteten U-Booten, etwa Halibut und Parche, diese Kabel abzuhören. Spulen und Hochleistungs-Verstärker wurden neben den Kabeln platziert, sodass man auf elektromagnetischem Wege die gewünschten Daten erhielt. Durch die modernen Glasfaserkabel dringen hingegen keine Fernmeldesignale nach außen; sie können deshalb nur schwer angezapft werden. Es wird berichtet, dass die USA bereits mit optoelektronischen Verstärkern, einer neuen Fasertechnologie, Experimente durchführen, deren Verwendung als Abhöranlage offiziell noch nicht möglich ist.

Die Hauptmethoden zur Übermittlung von großen Mengen öffentlicher, Geschäfts- und Regierungs-Kommunikation bestehen immer noch aus der Kombination von Unterseekabeln im Bereich der Ozeane und Höchstfrequenz-Netzwerken über Land. Da Unterseekabel im Wasser leicht sichtbar sind, sind sie besonders anfällig für Abhöroperationen.

Falls die oben genannten Methoden zur Erfassung der gewünschten Daten nicht ausreichen sollten, kann auf die Alternativen der Human Intelligence *(HUMINT)* zurükkgegriffen werden. Eines der vielen Systeme, die das klassische Spionage-Business elektronisch aufrüsten, heißt TEMPEST (Transient Electromagnetic Pulse Emanation Standard) und ist in der Lage, durch Wände hindurch von benachbarten Gebäuden aus die von Computern ausgehenden elektromagnetischen Strahlungen abzufangen, etwa Tastenanschläge oder Monitorstrahlung. Auf diese Weise können Daten von Rechnern aufgefangen werden, ohne dass in deren Netzwerk eingedrungen werden müsste.

Eine weitere Methode zur Datenkontrolle besteht darin, das Abhörsystem entweder direkt in die Hardware oder in die Normen und Protokolle der Kommunikationstech-

nologien einzubinden, was aber nur mit der Unterstützung der lokalen Regierungen möglich ist. Tatsächlich vollzieht sich dies gerade in der Europäischen Union unter dem Codenamen Lawful Interception („rechtmäßiges Abhören") oder ENFOPOL. In den USA laufen diese Maßnahmen unter dem Gesetz Communications Assistance for Law Enforcement Act (CALEA), das Telekommunikationsgesellschaften dazu verpflichtet, ihre bestehenden Netzwerke so zu modifizieren, dass die Abhörtätigkeit der Behörden ermöglicht bzw. erleichtert wird. Insbesondere seit dem Terroranschlag vom 11. September 2001 kann man solche Bestrebungen überall auf der Welt beobachten, die die ECHELON-Idee nun auf eine regionale Ebene übertragen. Entsprechende nationale Gesetzesentwürfe werden verabschiedet, und überstaatliche Kräfte kooperieren, um nebulöse Feinde, Terroristen und Cyberkriminalität zu bekämpfen.

Die Aufdeckung von ECHELON

Das Überwachungssystem ECHELON war, wie Geheimendienstaktivitäten im Allgemeinen, nicht Bestandteil der öffentlich zugänglichen Infosphäre. Als in den 1980er Jahren die ersten klaren Hinweise auf die Existenz eines derartigen Systems auftauchten, wurde dieses von den betroffenen Regierungen stets bestritten. In dieser Zeit waren es hauptsächlich Basisorganisationen, die den Bruch der Privatsphäre und der freien, geheimen Kommunikation verstärkt ins gesellschaftliche Bewusstsein rückten. Im Jahr 1988 konzentrierte sich der Journalist Duncan Campbell [133] in einem Bericht auf die Existenz des ECHELON-Systems und forderte eine Untersuchung der Aktivitäten der NSA in Europa. Die bekannteste ECHELON-Basis ist immer noch die amerikanische Satellitenüberwachungsstation in Menwith Hill im englischen Yorkshire. So haben die Bemühungen der britischen Gemeinde auch eine maßgebliche Rolle dabei gespielt, dass eine offizielle Untersuchung in Gang gesetzt wurde. Ein offizieller Sprecher und eine treibende Kraft hinter dieser Bewegung war Glyn Ford, Labour-Mitglied des Europäischen Parlaments für den Wahlkreis Manchester. Mit seinem Buch „Secret Powers", das 1996 in Neuseeland veröffentlicht wurde, hat Nicky Hager den bisher detailliertesten Bericht über die Organisation und die Aktionen des neuseeländischen Nachrichtenaufklärungsdienstes Government Communications Security Bureau (GCSB) und seine Rolle in der UKUSA-Allianz wie auch über die Operationen von ECHELON abgegeben. Schließlich wurde die Angelegenheit auch im Europäischen Parlament behandelt, was 1995 zu einem Bericht des STOA-Referats (Scientific and Technological Options Assessment) führte, der 1998 abgeschlossen wurde. Der Bericht, an dem auch Duncan Campbell als Autor beteiligt war, bestätigte die Existenz von ECHELON und führte im September 2000 zur Einsetzung einer provisorischen Kommission im Europäischen Parlament zur Untersuchung dieses Abhörsystems. [134]

133 http://duncan.gn.apc.org/

134 STOA-Report: Development of surveillance technology and risk of abuse of economic information. www.europarl.eu.int/stoa/publi/default_en.htm

Abgesehen von der Anschuldigung, dass ECHELON in erster Linie zur Überwachung der Zivilbevölkerung eingesetzt werde, war eine der Hauptbefürchtungen, dass die US-Nachrichtendienste das System leicht zur Wirtschaftsspionage nutzen könnten. Die Regierungen in Europa fürchteten, dass die Vereinigten Staaten die durch ECHELON erhaltenen Daten verwenden würden, um amerikanischen Unternehmen gegenüber rivalisierenden europäischen Firmen einen Vorteil zu verschaffen. Diese Befürchtung wurde von R. James Woolsey, dem ehemaligen Kopf der Central Intelligence Agency (CIA), umgehend bekräftigt. Er bestätigte, dass die Vereinigten Staaten das System gegen „eine in Europa herrschende Kultur der Bestechung" einsetzen würden, um so „das Spielfeld einzuebnen". [135]

Mitglieder des EU-Ausschusses besuchten im Mai 2001 die USA mit einer langen Liste von Gesprächsterminen, um mehr über ECHELON herauszufinden. Aber kurz nach ihrer Ankunft wurden zuvor vereinbarte Treffen mit Funktionären verschiedener US-Nachrichtendienste in letzter Minute abgesagt. Der Vorsitzende der Kommission, Carlos Coelho, gab an, dass die Gruppe sehr enttäuscht über diese offensichtliche Abfuhr sei; aus Protest kehrten die Parlamentsabgeordneten einen Tag früher als geplant nach Hause zurück.

In Europa veröffentlichte die Kommission einen Bericht, der feststellte, dass ECHELON tatsächlich existiert. Das Gremium blieb aber im Unklaren darüber, ob der Verdacht bestätigt werden kann, dass ECHELON zur Industriespionage genutzt wird. Es wurde erklärt, dass es Beweise bzw. Indizien dafür gebe, dass ECHELON zu bedeutsamen Übergriffen auf die Privatsphäre verwendet wurde. Diese vermeintlichen Verletzungen schließen die heimliche Überwachung von politischen Organisationen wie Amnesty International ein. Es wurde weiterhin festgestellt, dass ECHELON in Industriespionage gegenüber mehreren privaten Unternehmen wie Airbus Industries und Panavia verwickelt war; die erhaltenen Informationen waren an deren amerikanische Konkurrenten weitergeleitet worden. Aber Funktionäre des Nachrichtendienstes erklärten, dass solche Vorfälle nur durch Bestechung bedingt sein könnten. Es herrscht weiterhin Unklarheit darüber, inwieweit die ECHELON-Aktivitäten Privatpersonen geschädigt haben.

Im Bericht der Kommission findet sich eine nachdrückliche Empfehlung zur Verschlüsselung von Kommunikation. Ironischerweise favorisiert der Bericht auch die Idee, Agenten der europäischen Regierungen mit weiter reichenden Vollmachten zur Entschlüsselung elektronischer Kommunikation auszustatten, was später jedoch von einigen Beobachtern und mehreren Mitgliedern derselben Kommission als eine weitere Unterstützungsmaßnahme für ein europaweites Überwachungssystem kritisiert wurde. Das Europäische Parlament nahm den Bericht an, der parlamentarische Aus-

135 http://www.heise.de/tp/deutsch/special/ech/6679/1.html

schuss wurde jedoch trotz des offensichtlichen Bedarfs an weiteren Untersuchungen im September 2001, wenige Tage vor dem terroristischen Anschlag in den USA, aufgelöst.

Viele Staaten, die keine Hauptverbündeten des UKUSA-Systems sind, betreiben eine ECHELON-ähnliche Politik der Informationsbeschaffung, so etwa Russland, Frankreich, Israel, China, Indien, Pakistan und einige andere. Tatsächlich gibt es Gerüchte, dass diese Operationen mit denen ihrer amerikanischen Gegenparte vergleichbar sind, denn auch sie schließen das Beschaffen von Wirtschaftsinformationen für Privatunternehmen ein, um ihre Positionierung auf dem internationalen Markt zu verbessern. Jedoch scheint keine dieser Aktivitäten hinsichtlich Ausmaß und Machtkonzentration mit ECHELON vergleichbar zu sein.

Mit der Sensibilisierung der Öffentlichkeit für das Thema ECHELON sah sich die Regierung der USA mit einer ständig wachsenden Anzahl von Fragen zum rechtlichen Status ihrer Überwachungsaktivitäten konfrontiert. Doch Institutionen wie die NSA verweigerten jegliche Auskunft über Gerüchte sowie inzwischen aufgetauchte Beweise zur zivilen Überwachung in den Vereinigten Staaten. Dies ist besonders interessant, da das US-Recht die Aktivitäten der Nachrichtendienste im Bereich der zivilen Überwachung stark einschränkt.

Bereits im Jahr 1999 unterzeichnete Präsident Clinton einen Finanzierungsentwurf, der von der NSA verlangte, einen Bericht über die rechtliche Grundlage von ECHELON und ähnlichen Aktivitäten abzulegen. Der darauf folgende Bericht (mit dem Titel „Legal Standards for the Intelligence Community in Conducting Electronic Surveillance“) enthielt jedoch nur wenige Details zu den Tätigkeiten und zur Rechtmäßigkeit von ECHELON. Und heute immer noch ist es ein simples Faktum, dass niemand außer den Beteiligten genau weiß, wie ECHELON arbeitet und auf wen bzw. welche Informationen es abzielt. Wenn es hauptsächlich Kriminelle und Terroristen ins Visier nimmt, ist es in der Tat erstaunlich, dass der Terroranschlag vom 11. September die USA so überraschend traf. Viele Leute aus den Kreisen der Nachrichtenaufklärung ließen verlauten, dass ein Terroranschlag geplant war, jedoch nichts über die Ziele und über das Ausmaß des Anschlags bekannt war. Die richtigen Strukturen seien nicht ermittelt worden. Trotz der Tatsache, dass nach der Katastrophe die Beschränkungen eines omnipräsenten automatischen elektronischen Überwachungssystems allen klar sein sollten, erhöhten viele westliche Regierungen sofort das Budget für ähnliche Überwachungsaktivitäten und veränderten ihre Gesetze zugunsten staatlicher Überwachung. Das Bewusstsein der Öffentlichkeit in Bezug auf die Gefahren und den möglichen Missbrauch allgegenwärtiger Überwachungssysteme ist in den letzten Jahren stetig gewachsen. All dies scheint nun von der Angst vor Anschlägen, die überall in den Medien und in der Politik geschürt wird, ausradiert zu werden. Präsident Bush hat einen neuen Jahresfinanzierungsentwurf unterzeichnet, der den Geheimdiensten neben einem Minimal-Bud-

get von 30 Milliarden US-Dollar weitere Extra-Milliarden zuteilt, damit die land- und raumgestützte Nachrichtenaufklärung verstärkt und wiederbelebt werden kann. Länder wie Großbritannien, Deutschland und Österreich verabschiedeten neue Gesetze und statteten Geheimdienste und Polizei mit mehr Rechten aus, um Kommunikationsdaten aus Telefongesprächen und Zugang zu Internetkonten von Verdächtigen zu erhalten – manchmal sogar ohne gerichtliches Urteil.

Aber es ist nicht das Sammeln der Daten, das den Experten der Nachrichtenaufklärung Schwierigkeiten macht. Es ist die Auswertung der Daten, die keine befriedigenden Resultate ergibt. Einige Mitglieder aus den Zirkeln der Nachrichtenaufklärung führen an, dass es möglich gewesen wäre, den Anschlag vom 11. September abzuwehren, wenn die automatische Themenanalyse besser funktionieren würde. Sie meinen, dass die Indizien für den bevorstehenden Anschlag alle vorhanden waren, aber nicht in die richtige Ordnung gebracht wurden. Experten empfehlen, Nachrichtenaufklärung nicht vollautomatisch ablaufen zu lassen. Was fehlt, sei der menschliche Aspekt. HUMINT (human intelligence) solle sowohl in den Prozess der Informationsbeschaffung wie auch in den der Auswertung weiter integriert werden. Alle Kräfte in den Zirkeln der Nachrichtenaufklärung sollten enger zusammenarbeiten und ihre Daten miteinander verbinden (zumindest innerhalb der Vereinigten Staaten oder innerhalb von EUROPOL in Europa). Anstelle von geheimer automatischer Datensammlung sollte die Betonung auf einer Auswertung aller erhältlichen Quellen liegen sowie auf einer Verbesserung der menschlichen Analyse, auf geheimer Informationsbeschaffung durch Menschen und auf einem Zugang zur vollen Bandbreite multi-lingualer offener Quellen für Information. Davon ist die Verteidigungsindustrie natürlich nicht begeistert, und so wird es also in den nächsten Jahren wahrscheinlich einen Kampf zwischen den unterschiedlichen Interessenvertretern geben: technokratischen Industrieangehörigen, die raumgestützte Überwachung und ähnliche Technologien absetzen und weiterentwickeln wollen, und den Befürwortern der traditionellen Spion- und Agenten-Ideologie, die hauptsächlich von der Computerindustrie unterstützt wird (aus der Sprach-, Speicher- und Krypto-Technologie).

Aber eine äußerst wichtige Problematik sollte neben der Diskussion um Maßnahmen gegen den Terror nicht vergessen werden. Wie verändert sich die Situation der Bürgerrechte, wenn ECHELON nicht nur ein mächtiges Überwachungssystem ist, sondern ständig und überall ins tägliche Leben eingreifen kann? Wie ist es überhaupt möglich, dass derartige Überwachungssysteme innerhalb eines Rahmens bestehender Gesetze zur Privatsphäre existieren? Die Zeichen der Zeit stehen sicherlich ungünstig für die Beantwortung dieser unbequemen Fragen, aber es ist dennoch notwendig, die Regierungsverantwortlichen sowie Initiativen zur Gesetzesverschärfung oder ausgedehnteren Nachrichtenaufklärung sorgsam im Auge zu behalten, um möglichen Missbrauch von Überwachungssystemen aufzuzeigen und zu beseitigen. Der 11. September 2001 hat jedenfalls eine Reihe von beunruhigenden Fragen im Zusammenhang mit globalen

Überwachungsambitionen aufgeworfen. Steven Aftergood von der Federation of American Scientists:
„Nach dem 11. September sollten die Grenzen des so genannten ECHELON-Überwachungsnetzwerkes allen klar sein. ECHELON ist weit davon entfernt, ein allwissendes globales Überwachungssystem zu sein, und war nicht einmal in der Lage, einen direkten Angriff auf die USA abzuwenden. Bei der Auseinandersetzung zwischen jenen, die behaupten, die globalen Überwachungsaktivitäten der NSA seien omnipräsent und unausweichlich, und jenen, die behaupten, dass die NSA die neuere Technikentwicklung verschlafe und langsam „taub" würde, scheinen die Ereignisse die letztere Position zu stärken." [136]

Hauptstationen des ECHELON-Systems

Ort	Staat	Hauptziel, Hauptaufgabe	Beziehungen
Morwenstow	GB	INTELSAT, Atlantik, Europa, Indischer Ozean	NSA, GCHQ
Sugar Grove	USA	INTELSAT, Atlantik, Nord- and Süd-Amerika	NSA
Yakima Firing Center	USA	INTELSAT, Pazifik	NSA
Waihopai	Neuseeland	INTELSAT, Pazifik	NSA, GCSB
Geraldton	Australien	INTELSAT, Pazifik	NSA, DSD
Menwith Hill	GB	Sat, Bodenstation, Höchstfrequenz-Übermittlungen	NSA, GCHQ
Shoal Bay	Australien	Indonesien (Satelliten)	NSA, DSD
Leitrim	Kanada	Lateinamerika (Satelliten)	NSA, CSE
Bad Aibling	Deutschland	Satelliten, Bodenstation	NSA
Misawa	Japan	Satelliten	NSA
Pine Gap	Australien	Bodenstation	CIA
Fort Meade	USA	Datenauswertung	NSA Headquarters
Washington	USA	Datenauswertung	NSA
Ottawa	Kanada	Datenauswertung	CSE
Cheltenham	GB	Datenauswertung	GCHQ
Canberra	Australien	Datenauswertung	DSD
Wellington	Neuseeland	Datenauswertung	GCSB Headquarters

Tabelle 13 *Quelle: MSNBC Robert Windrem, „Spy Satellites Enter New Dimension," MSNBC und NBC News, 8. August 1998*

136 http://www.space.com/businesstechnology/technology/echelon_011121-2.html

Die Partner der UKUSA-Abkommen

UKUSA-Nation	Ziel-Regionen	Beteiligte Dienste	Abkürzung für	Abkommen
USA	Lateinamerika, fast ganzAsien, Russland und Nord-China	NSA (- CIA, USAF, NSG)	National Security Agency (- Central Intelligence Agency, US AirForce, Naval Security Group)	BRUSA-Abkommen 1943
UK	Die Länder der ehem. Sowjetunion westlich des Urals, Afrika	GCHQ	Government Communication Head Quarters	BRUSA-Abkommen 1943
Australien	Nachbarländer, Südchina, Indochina	DSD	Defense Signals Directorate	UKUSA-Allianz seit 1946
Kanada	Polarregionen Russlands	CSE	Communications Security Establishment	UKUSA-Allianz seit 1946, CANUS Abkommen 1950
Neuseeland	Westpazifik	GCSB	Government Communications Security Bureau	UKUSA-Allianz seit 1977

Tabelle 14 *Quelle: MSNBC Robert Windrem, „Spy Satellites Enter New Dimension," MSNBC und NBC News, 8. August 1998*

Satellit	Hersteller	Anzahl	Zweck	Umlaufbahn
Advanced KH-11	Lockheed Martin	3	Spionagefotos mit 12–cm-Auflösung	320 km
LaCrosse Radar Imaging	Lockheed Martin	2	Spionagefotos mit 1- bis 3–m-Auflösung	320 – 640 km
Orion/Vortex	TRW	3	Überwachung von Telekommunikation	36.000 km
Trumpet	Boeing	2	Überwachung von Mobiltelefonen	320 – 36.000 km
Parsae	TRW	3	Überwachung der Ozeane	960 km
Satellite Data Systems	Hughes	2	Datenrelais	320 – 36.000 km
Defense Support Program	TRW/ Aerojet	4+	Missile-Frühwarnsystem	36.000 km
Defense Meteo-rological Support Program	Lockheed Martin	2	Meteorologie, Erfassung von nuklearen Explosionen	800 km

Tabelle 15 *Quelle: MSNBC Robert Windrem, „Spy Satellites Enter New Dimension," MSNBC und NBC News, 8. August 1998*

Anti-ECHELON-Aktivismus

Initiativen zur Aufklärung der ECHELON–Aktivitäten und zur Öffentlichmachung und Bekämpfung von großflächigen Abhörvorgängen sind von Anfang an von zivilgesellschaftlichen Gruppen und investigativen Journalisten ausgegangen, während Regierungen sich jahrelang im Beschwichtigen und Ableugnen übten bzw. zum Teil über die Aktivitäten von Geheimdiensten im eigenen Land gar nicht informiert waren. Der Anti-ECHELON-Aktivismus der frühen Tage, bei dem es darum ging, die Existenz des Systems erst einmal zum Thema eines breiteren Diskurses zu machen, ist zum Teil in die Institutionen abgewandert. Er hat aber auch eine Reihe von Aktionen hervorgebracht, die darauf abzielen, das Überwachungssystem anzugreifen oder zumindest immer wieder ins Bewusstsein der Öffentlichkeit zu rücken. Eine solche Initiative ist der Jam-ECHELON-Day, der 21. Oktober, an dem das System mit Stichwörtern überfüttert und so in seiner Funktion beeinträchtigt werden soll. Die Stichwörter werden dabei als Signatur an möglichst viele E-Mails angehängt. Inwieweit derartige Aktionen ECHELON tatsächlich beeinträchtigen können, ist natürlich sehr fraglich; immerhin dürfte damit aber ein Beitrag zur Bewusstseinsbildung geleistet werden.

Auszug aus einer Liste vermuteter ECHELON-Stichwörter des Jam-ECHELON-Days (www.jamechelon.org):

SUAEWICS, Juiliett Class Submarine, Locks, qrss, loch, 64 Vauxhall Cross, Ingram Mac-10, wwics, sigvoice, ssa, E.O.D., SEMTEX, penrep, racal, OTP, OSS, Siemens, RPC, Met, CIA-DST, INI, watchers, keebler, contacts, Blowpipe, BTM, CCS, GSA, Kilo Class, squib, primacord, RSP, Z7, Nerd, fangs, Austin, no|d, Comirex, GPMG, Speakeasy, humint,GEODSS, SORO, M5, BROMURE, ANC, zone, SBI, DSS, S.A.I.C., Minox, Keyhole, SAR, Rand Corporation, Starr, Wackenhutt, EO, burhop, Wackendude, mol, Shelton, 2E781, F-22, 2010, JCET, cocaine, Vale, IG, Kosovo, Dake, 36,800, Hillal, Pesec, Hindawi, GGL, NAICC, CTU, botux, Virii, CCC, ISPE, CCSC, Scud, SecDef, Magdeyev, VOA, Kosiura, Small Pox, Tajik, +=, Blacklisted 411, TRDL, Internet Underground, BX, XS4ALL, wetsu, muezzin, Retinal Fetish, WIR, Fetish, FCA, Yobie, forschun g, emm, ANZUS, Reprieve, NZC-332, edition, cards, mania, 701, CTP, CATO, Phon-e, Chicago Posse, NSDM, l0ck, beanpole, spook, keywords, QRR, PLA, TDYC, W3, CUD, CdC, Weekly World News, Zen, World Domination, Dead, GRU, M72750, Salsa, 7, Blowfish, Gorelick,Glock, Ft. Meade, NSWT, press-release, WISDIM, burned, Indigo, wire transfer, e-cash, Bubba the Love Sponge, Enforcers, Digicash, zip, SWAT, Ortega, PPP, NACSE, crypto-anarchy, AT&T, SGI, SUN, MCI, Blacknet, ISM, JCE, Middleman, KLM, Blackbird, NSV, GQ360, X400, Texas, jihad, SDI, BRIGAND, Uzi, Fort Meade, *&, gchq.gov.uk, supercomputer, bullion, 3, NTTC, Blackmednet, :, Propaganda, ABC, Satellite phones, IWIS,

Planet-1, ISTA, rs9512c, Jiang Zemin, South Africa, Sergeyev, Montenegro, Toeffler, Rebollo, sorot, Yucca Mountain, FARC, Toth, Xu Yongyue, Bach, Razor, AC, cryptanalysis, nuclear, 52 52 N – 03 03 W, Morgan, Canine, GEBA, INSCOM, MEMEX, Stanley, FBI, Panama, fissionable, Sears Tower, NORAD, Delta Force, SEAL, virtual, WASS, WID, Dolch, secure shell, s crews, Black-Ops, O/S, Area51, SABC, basement, ISWG, $@, data-haven, NSDD, black-bag, rack, TEMPEST, Goodwin, rebels, ID, MD5, IDEA, garbage, market, beef, Stego, ISAF, unclassified, Sayeret Tzanhanim, PARASAR, Gripan, pirg, curly, Taiwan, guest, utopia, NSG, orthodox, CCSQ, Alica, SHA, Global, gorilla, Bob, UNSCOM, Fukuyama, Manfurov, Kvashnin, Marx, Abdurahmon, snullen, Pseudonyms, MITM, NARF, Gray Data, VLSI, mega, Leitrim, Yakima, NSES, Sugar Grove, WAS, Cowboy, Gist, 8182, Gatt, Platform, 1911, Geraldton, UKUSA, veggie, XM, Parvus, NAVSVS, 3848, Morwenstow, Consul, Oratory, Pine Gap, Menwith, Mantis, DSD, BVD, 1984, blow out, BUDS, WQC, Flintlock, PABX, Electron, Chicago Crust, e95, DDR&E, 3M, KEDO, iButton, R1, erco, Toffler, FAS, RHL, K3, Visa/BCC, SNT, Ceridian, STE, condor, CipherTAC-2000, Etacs, Shipiro, ssor, piz, fritz, KY, 32, Edens, Kiwis, Kamumaruha, DODIG, Firefly, HRM, Albright, Bellcore, rail, csim, NMS, 2c, FIPS140-1, CAVE, E-Bomb, CDMA, Fortezza, 355ml, ISSC, cybercash, NAWAS, government, NSY, hate, speedbump, joe, illuminati, BOSS, Kourou, Misawa, Morse, HF, P415, ladylove, filofax, Gulf, lamma, Unit 5707, Sayeret Mat'Kal, Unit 669, Sayeret Golani, Lanceros, Summercon, NSADS, president, ISFR, freedom, ISSO, walburn, Defcon VI, DC6, Larson, P99, HERF pipe-bomb, 2.3 Oz., cocaine, $, imapct, Roswell, ESN, COS, E.T., credit card, b9, fraud, ST1, assasinate, virus, ISCS, ISPR, anarchy, rogue, mailbomb, 888, Chelsea, 1997, Whitewater, MOD, York, plutonium, William Gates, clone, BATF, SGDN, Nike, WWSV, Atlas, IWWSVCS, Delta, TWA, Kiwi, PGP 2.6.2., PGP 5.0i, PGP 5.1, siliconpimp, SASSTIXS, IWG, Lynch, 414, Face, Pixar, IRIDF, NSRB, eternity server, Skytel, Yukon, Templeton, Johohonbu, LUK, Cohiba, Soros, Standford, niche, ISEP, ISEC, 51, H&K, USP, ^, sardine, bank, EUB, USP, PCS, NRO, Red Cell, NSOF, DC7, Glock 26, snuffle, Patel, package, ISI, INR, INS, GRU, RUOP, GSS, NSP, SRI, Ronco, Armani, BOSS, Chobetsu, FBIS, BND, SISDE, FSB, BfV, IB, froglegs, JITEM, SADF, advise, TUSA, LITE, PKK, HoHoCon, SI SMI, ISG, FIS, MSW, Spyderco, UOP, SSCI, NIMA, HAMASMOIS, SVR, SIN, advisors, SAP, Monica, OAU, PFS, Aladdin, AG, chameleon man, Hutsul, CESID, Bess, rail gun, .375, Peering, CSC, Tangimoana Beach, Commecen, Vanuatu, Kwajalein, LHI, DRM, GSGI, DST, MITI, JERTO, SDF, Koancho, Blenheim, Rivera, Kyudanki, varon, 310, 17, 312, NB, CBM, CTP, Sardine SBIRS, jaws, SGDN, ADIU, DEADBEEF, IDP, IDF,Halibut, SONANGOL, Flu, &, Loin, PGP 5.53, meta, Faber, SFPD, EG&G, ISEP, blackjack, Fox, Aum, AIEWS, AMW, RHL, Baranyi, WORM, MP5K-SD, 1071, WINGS, cdi, VIA, DynCorp, UXO, Ti, WWSP, WID, osco, Mary, honor, Templar, THAAD, package, CISD, ISG, BIOLWPN, JRA, ISB, ISDS, chosen, LBSD, van, schloss, secops, DCSS, DPSD, LIF, J-Star, PRIME, SURVIAC, telex, Analyzer, embassy, Golf, B61-7, Maple, Tokyo, ERR, SBU, Threat,

JPL, Tess, SE, Alex, EPL, SPINTCOM, FOUO, ISS-ADP, Merv, Mexico, SUR, blocks, SO13, Rojdykarna, RSOC, USS Banner, S511, 20755, airframe, jya.com, Furby, PEC-SENC, football, Agfa, 3210, Crowell, moore, 510, OADR, Smit h, toffee, FIS, N5P6, EuroFed, SP4, shelter, Crypto, 3, 7, 17, 20, 51, 69, 312, 414, 707, 737, 747, 757, 767, 777, 868, 888, 1071, 1911, 1984, 1997, 2600, 3848, 8182, $, &, ^, ^?, ~, 1*, 1080H, 15kg, 3B2,50BMG, a, ABC, ACC, ActiveX, advise, advisors, afsatcom, AFSPC, AHPCRC, AIMSX, Aladdin, Alica, Alouette,AMEMB, Amherst, AMW, anarchy, ANC, AOL, AOLTOS, ARC, Archives, Area51, argus, Armani, ARPA, Artichoke, ASIO, ASIS, ASIS, ASLET, assasinate, Asset, AT, AT&T, Atlas, Austin, AVN, b, B.D.M., b9, Badger, bank, basement, BATF, BBE, BECCA, beef, Bess, bet, BeyondHope, BfV, BITNET, black-bag, Blackbird, Blacklisted411, Blackmednet, Blacknet, Black-Ops, BletchleyPark, Blowfish, BMDO, BND, Bob, BOP, BOSS, botux, BRLO, Broadside, Bubba, BubbatheLoveSponge, bullion, BVD, BZ, c, Cable&Wireless, CANSLO, Capricorn, Cap-Stun, CATO, CBM, CBNRC, CBOT, CCC, CCS, CDA, CdC, CDC, cdi, CESID, CFC, chaining, chameleonman, Chan, Chelsea, ChicagoPosse, Chobetsu, chosen, CIA, CID, CIDA, CIM, CIO, CIS, CISE, Clandestine, clone, cocaine, COCOT, Coderpunks, codes, Cohiba, Colonel, Competitor, Compsec, Compsec97, ComputerTerrorism, Consul, CONUS, Cornflower, CorporateSecurity, COS, COSMOS, CounterTerrorism, counterintelligence, Cowboy, CovertVideo, CQB, CQB, CRA, creditcard, cryptanalysis, crypto-anarchy, CSE, csystems, CTP, CTP, CTU, CTU, CUD, cybercash, Cypherpunks, d, D-11, Daisy, datahavens, DATTA, DCJFTF, Dead, DEADBEEF, debugging, Defcon, DefConV, DefenseInformationWarfare, Delta, Delta, DERA, DES, DEVGRP, DF, DIA, Dictionary, Digicash, DITSA, DJC, DOE, DOE, Dolch, domesticdisruption, DRA, DSD, DSD, DSS, Duress, DynCorp, E.O.D., E.T.

Zusammenfassung

Wie kaum ein anderer Bereich sind Sicherheitsfragen von einem Spannungsverhältnis zwischen staatlichen und gesellschaftlichen Ordnungsansprüchen und individuellen Freiheitsansprüchen gekennzeichnet. Dieser Konflikt prägt wesentlich Forschung und Entwicklung sowie die Gesetzgebung und insgesamt den gesellschaftlichen Umgang mit Sicherheitstechnologien. Dabei zeigt sich, dass Sicherheitstechnologien sich einerseits sehr rasch ausbreiten, weil sie angesichts der komplexen Risiken einer sich immer schneller informatisierenden Gesellschaft mit einem Anspruch auftreten können, der keiner gesonderten Begründung zu bedürfen scheint. Gerade dies scheint aber auch eine kritische Auseinandersetzung mit derartigen Technologien bzw. deren transparente Gestaltung zu erschweren. Denn einerseits wirkt Sicherheit als Ausschlussmechanismus, der von vornherein auf Geheimhaltung abzielt und daher nur begrenzt öffentlich diskutiert werden kann. Der Sicherheitsdiskurs sowie die Technikentwicklung werden daher in krasser Weise von staatlichen Einrichtungen wie Polizei und Geheimdienst sowie von großen Firmen dominiert. Die Standardphrase „aus Sicherheitsgründen“ bedeutet daher oft genug, dass bestimmte Themen einer breiteren Öffentlichkeit nicht zugänglich gemacht werden sollen. Die Handhabung etwa von Verschlüsselungstechniken, die oft als militärische Technologie klassifiziert werden, illustriert dies sehr deutlich. Noch bedrohlichere Ausmaße nimmt dieser hermetische Charakter des Sicherheitsdiskurses im Bereich der Überwachungstechnologien an, wo er eine autoritäre Gesellschaftsstruktur bewirkt und die Idee des „freien öffentlichen Raumes“ als eines Ortes der autonomen Individuen ad absurdum führt.

Zivilgesellschaftliche Aneignungen von Sicherheitstechnologien können einerseits den Diskurs öffnen, andererseits aber auch das Sicherheits- und Autoritätsdenken fester etablieren. Ersteres war zum Beispiel in der Auseinandersetzung um die Verschlüsselungstechnologie festzustellen, letzteres zeigt sich immer mehr im Ausspionieren von Arbeitsplatz und Privatleben. Notwendig scheinen daher sowohl ein höheres Maß an demokratischer Mitsprache bei den entsprechenden gesetzlichen Regelungen als auch die Infragestellung eines oft undifferenzierten Sicherheitsdiskurses.