# Inside Echelon

*Duncan Campbell* *24.07.2000*

## Zur Geschichte, Technik und Funktion des unter dem Namen Echelon bekannten globalen Abhör- und Filtersystems

download

**Seit 1998 wurde viel über das so genannte Echelon-System zur Überwachung internationaler Kommunikation geschrieben und gesprochen. Davon wurde das meiste von US-amerikanischen und europäischen Behörden abgestritten oder ignoriert. Allerdings war vieles von dem, was geschrieben wurde, ebenfalls übertrieben oder falsch. Angesichts der Dementi, Ungenauigkeiten und Fehler herrschte Verwirrung. Diese Übersicht von Duncan Campbell, Autor des Berichts "Abhörmöglichkeiten 2000"[1] soll die Verwirrung beseitigen und klären, was Echelon ist und nicht ist, woher es stammt und was es tut. Denn Echelon oder ähnliche Systeme werden uns noch eine lange Zeit begleiten.**

Menwith Hill, Foto: Duncan Campbell

*Echelon* (millitärisches Englisch: Staffelung ist ein System, das von der US-amerikanischen National Security Agency (NSA) benutzt wird, um internationale Kommunikation abzuhören und zu verarbeiten, die über Kommunikations-Satelliten geleitet wird. Es ist Teil eines globalen Überwachungssystems, das bereits über 50 Jahre alt ist. Andere Teile desselben Systems fangen Nachrichten aus dem Internet, von Unterseekabeln und Funkübermittlungen ab. Sie nutzen die innerhalb von Botschaften installierten geheimen Lauschausrüstungen oder

Satelliten in der Erdumlaufbahn, um Signale irgendwo auf der Erdoberfläche abzuhören. Zu dem System gehören Stationen, die von Großbritannien, Kanada, Australien und Neuseeland unterhalten werden - zusätzlich zu solchen, die von den Vereinigten Staaten betrieben werden. Obwohl die australischen und britischen Stationen dasselbe wie die Echelon-Stationen der USA tun, werden sie nicht notwendigerweise als Echelon-Stationen bezeichnet. Aber sie alle sind Teil desselben integrierten globalen Netzwerks, das dieselbe Ausrüstung und dieselben Methoden benutzt, um täglich verbotenerweise an Informationen und Aufklärungsmaterial aus Millionen von Nachrichten aus aller Welt zu gelangen.

Die ersten Berichte über Echelon in Europa[2] sprachen dem System die Fähigkeit zu, "innerhalb von Europa jede E-Mail-, Telefon- und Fax-Kommunikation" abzuhören. Dies hat sich als falsch herausgestellt. Weder Echelon, noch das elektronische Spionagesystem, von dem es ein Teil ist, sind dazu in der Lage. Das Equipment ist auch gar vorhanden, das die Kapazität hätte, um den Inhalt jeder Sprachnachricht oder jedes Telefonanrufs zu verarbeiten und zu erkennen. Aber das von den Amerikanern und Briten betriebene Netzwerk hat gemeinsam mit seinen Schwesternstationen Zugang zu den meisten Kommunikationssatelliten der Welt, kann die Informationen verarbeiten, automatisch analysieren und seinen Kunden, die sich möglicherweise auf anderen Kontinenten aufhalten, zur Verfügung stellen.

## Die Anfänge

Das geheimste elektronische Überwachungssystem der Welt hat seinen Ursprung hauptsächlich in den Konflikten des Zweiten Weltkriegs. Eigentlich ist es eine Folge der Erfindung des Radios und des grundliegenden Charakters von Telekommunikation. Die Erfindung des Radios erlaubte es Regierungen und anderen Kommunikationsteilnehmern Nachrichten über transkontinentale Entfernungen zu übermitteln. Aber es gab einen Nachteil: Jeder konnte mithören. Zuvor waren geschriebene Nachrichten körperlich sicher - außer der Kurier geriet in einen Hinterhalt oder ein Spion kompromittierte die Kommunikation. Durch die Erfindung des Radios erhielt die Kryptografie, die Kunst und die Wissenschaft der Verschlüsselung, neue Bedeutung. Es entstand das Geschäft der Nachrichtenaufklärung, die heute industrielle Ausmaße angenommen hat. Obgleich das größte Überwachungsnetzwerk von der US-amerikanischen NSA betrieben wird, ist es bei weitem nicht das einzige. Russland, China, Frankreich und andere Nationen unterhalten weltweite Netzwerke. Mehrere dutzend fortschrittliche Nationen betreiben elektronische Fernmeldeaufklärung als Hauptquelle ihrer Aufklärung. Sogar kleine europäische Nationen wie Dänemark, die Niederlande oder die Schweiz haben kürzlich kleine, Echelon-ähnliche Stationen errichtet, um Aufklärungsmaterial durch das Abhören ziviler Satellitenkommunikation zu erhalten und zu verarbeiten.

Während des 20. Jahrhunderts erkannten die Regierungen die Bedeutung wirksamer Geheimschlüssel. Dennoch waren sie oft alles andere als erfolgreich. Während des Zweiten Weltkriegs analysierten große gemeinsame Codebrecher-Einrichtungen in Großbritannien und Amerika hunderttausende von deutschen und japanischen Nachrichten. Was sie taten und wie sie es taten blieb für Jahrzehnte ein streng gehütetes Geheimnis. Während dieser Zeit richteten die NSA und das Government Communications Headquarters (GCHQ), die US-amerikanischen und britischen Behörden, die für elektronische Fernmeldeaufklärung zuständig waren und sind, ein weltweites Abhörnetzwerk ein.

Das System basiert auf der "UKUSA-Vereinbarung" von 1947, die britische und US-amerikanische Systeme, Personal und Stationen vereinte. Schon bald schlossen sich die Netzwerke der drei britischen Commonwealth-Länder Kanada, Australien und Neuseeland an. Später unterzeichneten andere Länder, darunter Norwegen, Dänemark, Deutschland und die Türkei geheime Abhörabkommen mit den USA und wurden so zu Drittländer-Beteiligten im UKUSA-Netzwerk.

Ihre Stationen wurden in das Netzwerk integriert, jedes Land ernannte höhere Beamte, um als Verbindungsbeamte in den Hauptquartieren der anderen zu arbeiten. Die USA unterhalten ein spezielles US-Verbindungsbüro (SUSLO) in London und Cheltenham, während ein Vertreter des speziellen britischen Verbindungsbüros (SUKLO) des GCHQ seine Büros innerhalb des NSA-Hauptquartiers in Fort Meade, zwischen Washington und Baltimore, unterhält.

Entsprechend der UKUSA-Vereinbarung teilten die fünf englischsprachigen Länder die Verantwortung für die Überwachung auf verschiedene Teile des Globus auf[3] . Großbritanniens Überwachungszone erstreckte sich auf Afrika und Europa sowie Richtung Osten bis zum Ural; Kanada deckte die nördlichen Breitengrade und Polarregionen ab; Australien kümmerte sich um Ozeanien. Die Vereinbarung schrieb gemeinsame Vorgehensweisen, Ziele, Ausrüstung und Methoden vor, die die Abhöreinrichtungen nutzen sollten. Dazu gehörten auch internationale Regeln für die Sicherheit der elektronischen Fernmeldeaufklärung. Sie sahen vor, dass, bevor irgend jemand mit dem Wissen um die Vorgehensweisen bei der elektronischen Fernmeldeaufklärung betraut wurde, dieser zuvor einer lebenslangen Geheimhaltungsvereinbarung zustimmen musste. Jede Person, die in eine UKUSA-Aufklärungsorganisation eintrat, musste indoktriniert und re-indoktriniert werden, sobald sie Wissen über ein spezielles Projekt erlangten. Ihr wurde jedoch nur gesagt, "was sie wissen musste", und dass die Notwendigkeit für eine totale Geheimhaltung ihrer Arbeit "nie ende".

Alles, was in den Aufklärungsorganisationen produziert wurde, wurde mit Hunderten von speziellen Codewörtern bezeichnet, die das Wissen über die abgehörte Kommunikation und die dafür benutzten Systeme aufsplitterte. Das unterste Geheimhaltungsniveau, das tatsächlich eine höhere Klassifizierung als "Top Secret" darstellt, ist "Top Secret Umbra". Höher klassifizierte Dokumente werden als "Umbra Gamma" bezeichnet; andere Codewörter können hinzugefügt werden, um die Verbreitung weiter einzuschränken. Weniger sensitive Informationen, wie die Analysen des Telekommunikationsverkehrs, wurden beispielsweise als "Secret Spoke" klassifiziert.

## Vernetzung

Dänische Satellitenüberwachungsstation, Foto:Ekstrabladet

Das Ausmaß und die Bedeutung des globalen Überwachungssystems hat sich seit 1980 verändert. Die Einführung kostengünstiger, breitbandiger, internationaler Kommunikation führte zu einer vernetzten Welt. Aber nur wenige Leute sind sich bewusst, dass das erste globale Wide Area Network (WAN) nicht das Internet, sondern das internationale Netzwerk war, das die Aufklärungsstationen mit den Verabeitungszentren verband. Das Netzwerk wird über Unterseekabel und Satelliten verbunden. Der größere Teil der Kapazität der amerikanischen und britischen Militärkommunikationssatelliten Milstar und Skynet ist für die Weiterleitung von Fernmelde-Aufklärungsinformation vorgesehen. Erst Mitte der 90er Jahre wurde das öffentliche Internet größer als das geheime Internet, das die Überwachungsstationen verband. Die britische Spionagebehörde GCHQ gibt nun auf ihrer Website öffentlich damit an, dass es "eines der größten WANs der Welt" betreibt und dass "alle GCHQ-Systeme miteinander im größten LAN in Europa verbunden sind, mit Verbindungen zu anderen Anlagen in der ganzen Welt". Auf derselben Website behauptet sie, dass "die beachtliche Größe und die bloße Macht der GCHQ-Supercomputer-Architektur schwer vorzustellen" sei.

Das WAN der Ukusa-Allianz ist nach denselben Prinzipien wie das Internet (TCP/IP) angelegt und ermöglicht allen Feld-Abhörstationen den Zugang zum zentralen Computersystem der

NSA, bekannt als (eng.) "Platform". Andere Teile des Systems sind bekannt als "Embroidery", "Tideway" und "Oceanfront". Das Spionagenachrichtennetzwerk heißt "Newsdealer". Ein TV-Konferenzsystem, das wie jedes andere Teil des Netzwerks sehr stark verschlüsselt ist, wird als "Gigster" bezeichnet. Diese Systeme werden von Anwendungen wie "Preppy" und "Droopy" unterstützt. Das Email-System der NSA sieht aus wie jedes andere Email-System, aber es arbeitet vom öffentlichen Netzwerk völlig losgelöst. Nachrichten, die an seine geheime interne Internetadresse, die ganz einfach "NSA" lautet, adressiert sind, kommen nicht durch.

Auch die Übermittlungf des NSA-Aufklärungsmaterials sieht aus und fühlt sich an wie das Internet. Autorisierte Nutzer mit entsprechender Erlaubnis für den Zugang zur SCI[4] benutzen Standard-Web-Browser, um sich die Ergebnisse der NSA-Operationsabteilung aus der Ferne anzusehen. Das System, bekannt als Intelink, wird vom Hauptquartier der NSA in Fort Meade aus betrieben. Fertiggestellt wurde es 1996 und verbindet 13 unterschiedliche US-Geheimdienstbehörden und einige alliierte Behörden mit dem Ziel, unmittelbaren Zugang zu allen Arten von Aufklärungsinformation zu ermöglichen. Geheimdienstanalysten und Militärpersonal können, gerade wie beim Einwählen in das World Wide Web, einen Atlas auf der Homepage von Intelink sehen und dann auf irgendein Land ihrer Wahl klicken, um Zugang zu Spionageberichten, Videoclips, Satellitenfotos, Datenbanken und Zustandsberichten zu erhalten[5] .

## Nachkriegsjahre

In den frühen Nachkriegsjahren und für das folgende Vierteljahrhundert gab es nur wenig Anzeichen für diese Automatisierung, beziehungsweise diesen hohen Entwicklungsstandard. In jenen Jahren wurde der Großteil der Fernkommunikation, sei sie ziviler, militärischer oder diplomatischer Natur, über Hochfrequenzfunk übermittelt. Die NSA und ihre Kollaborateure betrieben Hunderte von Fernabhörstationen, die die Sowjetunion und China umgaben und überall in der Welt verteilt waren. Im Inneren von fensterlosen Gebäuden arbeiteten Abhörteams in langen Schichten, um in die Stille zu lauschen, die von kurzen Perioden rasender Aktivität unterbrochen wurde. Für die Lauschbasen an den Grenzlinien des Kalten Krieges bedeutete die Überwachung des militärischen Funkverkehrs während des Kalten Krieges ziemlichen Stress. Mitarbeiter auf solchen Basen erinnern sich oft daran, dass Kollegen unter dem Druck zusammenbrachen und sich zum Beispiel in einem Schrank versteckten, da sie glaubten, dass sie gerade eine Nachricht abgehört hatten, die den Beginn des globalen thermonuklearen Krieges ankündigte.

Nach dem Zweiten Weltkrieg verfügte Großbritanniens GCHQ über ein weitreichendes Netzwerk von Außenposten für die elektronische Fernmeldeaufklärung. Viele waren in Großbritannien positioniert, während andere im ganzen damaligen Empire verteilt waren. Von den Stationen aus, darunter Bermuda, die Ascension-Inseln, Zypern, Gibraltar, Irak, Singapur und Hongkong, verfolgten die Funkbetreiber die politischen und militärischen Entwicklungen in der Sowjetunion und bald in China. Diese Stationen ergänzten ein US-amerikanisches Netzwerk, das 1960 Tausende von ständig betriebenen Abhör-Standorten beinhaltete. Die anderen Mitglieder der UKUSA-Allianz, Australien, Kanada und Neuseeland, steuerten Stationen im Südpazifik und der Arktis bei.

Nachdem der UKUSA-Vertrag unterzeichnet war, nahm eine neue Kette von Stationen ihren Betrieb entlang der Grenzen der westlichen Einflusssphäre auf, um den Funkverkehr auf sowjetischem Boden sowie der sowjetischen Luftwaffe zu überwachen. Die britischen Abhörposten wurden in Deutschland sowie im Geheimen in Österreich und im Iran errichtet. Die US-Abhörposten wurden in Mittel- und Süddeutschland und später in der Türkei, Italien und Spanien errichtet. Eine wichtige US-Abhörstation, die Kagnew Station in Asmara in Eritrea, übernahmen die USA 1941 von den Briten. Sie war zu ihrer Schließung 1970 eine der größten Abhörstationen der Welt. Zu ihren eher spektakulären Eigenschaften gehörte ein bewegliche Antennenschüssel, mit der Nachrichten in die USA versandt wurden, indem sie auf der Oberfläche des Mondes reflektiert wurden.

Mitte der 60er-Jahre wurden viele Stationen mit gigantischen Antennensystemen zur Überwachung des Hochfrequenzfunkverkehrs errichtet. Sie waren auch in der Lage, die

Position eines Senders zu lokalisieren. Sowohl die US-Navy, als auch die US-Air-Force unterhielten solche globalen Netzwerke. Die US-Air-Force installierte 500-Meter-große Felder, bekannt als FLR-9, unter anderem im englischen Chicksands, im italienischen San Vito dei Normanni, im türkischen Karamursel, auf den Philippinen und im japanischen Misawa. Unter dem Codenamen "Iron Horse" wurden die ersten FLR-9-Stationen in Betrieb genommen. Die US-Navy errichtete ähnliche Basen in den USA, im spanischen Rota, im deutschen Bremerhaven, im schottischen Edzell, auf Guam und später in Puerto Rico, welche auf Kuba ausgerichtet war.

Als die Vereinigten Staaten gegen Vietnam Krieg führten, arbeiteten australische und neuseeländische Betreiber in Singapur, Australien und anderswo in direkter Unterstützung des Krieges. Großbritannien als neutrales Land sollte nicht einbezogen werden. In der Praxis jedoch überwachten britische Betreiber in der GCHQ-Abhörstation UKC-201 in Little Sai Wan in Hongkong die nordvietnamesischen Luftabwehrnetzwerke und gaben Berichte darüber weiter, während US-amerikanische B52-Bomber Hanoi und andere nordvietnamesische Ziele angriffen.

Seit Ende des Kalten Krieges wurde die Geschichte einiger Abhöroperationen des Kalten Krieges deklassifiziert. Im Nationalen Kryptologie-Museum, das von der NSA in ihrem Hauptquartier unterhalten wird, gibt die Behörde nun offen viele ihrer Abhörstationen des Kalten Krieges zu. Es beschreibt auch den umstrittenen Gebrauch von Schiffen und Flugzeugen, um die militärische Verteidigung zu durchdringen oder herauszufordern, was das Leben von mehr als hundert Besatzungsmitgliedern kostete. Aber ein anderer langwieriger Aspekt der Abhöroperationen bleibt ungewürdigt: Während des Zweiten Weltkrieges, aber auch während des Kalten Krieges und seither, überwachten britische und US-amerikanische Geheimdienstbehörden den Funkverkehr und brachen die Codes von Alliierten und befreundeten Staaten ebenso wie die zivile und kommerzielle Kommunikation weltweit. Die diplomatische Kommunikation jedes Landes wurde und wird angegriffen.

Die Stationen und Methoden sind dieselben wie für militärische Ziele. Innerhalb von Geheimdienstbehörden war das zivile Ziel als ILC bekannt. ILC steht für International Leased Carrier und bezieht sich auf private Firmen oder Telekommunikationsbetreiber von Unterseekabeln oder Funkstationen. Manche ILC-Schaltungen wurden als ständige Verbindungen an Regierungen oder große Firmen vermietet. Die meisten wurden für öffentliche Telegrafie, Telex oder Telefondienste eingesetzt.

Viele Details über Operationen der englisch-sprachigen Aufklärungspraxis wurden von zwei NSA-Abtrünnigen während einer Pressekonferenz in Moskau am 6. September 1960 enthüllt. Damals erzählten die zwei NSA-Analytiker Bernon Mitchell und William Martin der Welt, was die NSA tat:

---

> Von unserer Arbeit in der NSA wissen wir, dass die Vereinigten Staaten die geheime Kommunikation von mehr als 40 Ländern mitlesen, eingeschlossen die ihrer eigenen Alliierten... Die NSA unterhält mehr als 2000 manuelle Abhör-Arbeitsplätze... sowohl verschlüsselte als auch Kommunikation im Klartext werden von fast jeder Nation in der Welt abgehört, darunter die Staaten, auf deren Boden die Abhörstationen stehen.
> *New York Times vom 7. September 1960.*

Über die Enthüllungen wurde in den USA in aller Ausführlichkeit berichtet, aber ihr Einfluss wurde bald von Gegenbeschuldigungen und Anklagen begraben. Martin und Mitchell enthüllten, dass die NSA-Operationsabteilungen zwei Hauptgruppen enthielten. Eine Gruppe deckte die Sowjetunion und ihre Alliierten ab. Die zweite Analyseneinheit war bekannt als ALLO, was für "alle anderen [Länder]" stand. Dieser Teil der NSA-Organisation wurde später in ROW umbenannt - "Rest Of the World".

Während 1965 Abhörbetreiber der NSA-Station im englischen Chicksands sich auf die Funknachrichten des Warschauerpaktes konzentrierten, deckten ihre Kollegen 200 Kilometer

nördlich des schottischen Kirknewton den ILC-Verkehr ab, einschließlich kommerziell betriebener Funkstrecken zwischen den großen europäischen Städten. Diese Netzwerke konnten alles mögliche enthalten, von Geburtstagstelegrammen bis hin zu detaillierten ökonomischen oder kommerziellen Informationen, die von Firmen ausgetauscht wurden, bis hin zu verschlüsselten diplomatischen Nachrichten. In den Abhörräumen druckten Maschinen, die auf die Übertragungskanäle ausgerichtet waren, kontinuierlich achtlagiges Papier aus, das von Aufklärungsanalysten gelesen und bearbeitet werden musste.

Rund um die Welt beschäftigten sich Tausende von Analysten mit diesen in der Regel unverschlüsselten Nachrichten, wobei sie NSA-Beobachtungslisten benutzten. Bei diesen Listen handelte es sich um wöchentliche Schlüsselwortlisten von Leuten, Firmen und Angelegenheiten von Interesse für die NSA-Beobachter, mit denen sie den "klaren" Verkehr sortierten. Kodierte Nachrichten wurde sofort weitergereicht. Unter den regelmäßigen Namen auf den Beobachtungslisten waren die Führer der afrikanischen Guerilla-Bewegungen, die später zu den Staatsoberhäuptern ihrer Länder wurden. Mit der Zeit wurden viele prominente Amerikaner dieser Liste hinzugefügt. Unter Überwachung stand die internationale Kommunikation der Schauspielerin Jane Fonda, Dr. Benjamin Spock und Hunderter anderer, da sie gegen den Krieg in Vietnam waren. Auch Eldridge Cleaver, Führer der schwarzen Bürgerrechtsbewegung Black Power und seine Kollegen wurden aufgrund ihrer Bürgerrechts-Aktivitäten in den USA auf die Liste gesetzt.

In der Nähe des schottischen Cupar wurde eine andere Abhörstation von der britischen Post unterhalten, die als Station für Langstreckenfunk getarnt war. Tatsächlich handelte es sich um eine weitere GCHQ-Abhörstation, die die Kommunikation europäischer Länder abhörte, anstatt sie weiterzuvermitteln.

Mit der Zeit wurden diese Operationen integriert. 1976 richtete die NSA ein spezielle neue zivile Einheit auf ihrer Basis in Chicksands zum Abhören der diplomatischen und zivilen Kommunikation ein. Diese Einheit, genannt "DODJOCC" (Department of Defense Joint Operations Centre Chicksands) wurde auf nicht-US-amerikanische diplomatische Kommunikation ausgerichtet, bekannt als NDC. Ein spezielles Ziel, bekannt als FRD, stand für den französischen diplomatischen Verkehr. Der italienische diplomatische Funkverkehr, als ITD bezeichnet, wurde vom Gegenpart der NSA, dem GCHQ in seinem Zentrum in Cheltingham gesammelt und entschlüsselt.

Ein Besucher würde beim Betreten des Gebäudes 600 in Chicksands durch doppelte Sicherheitszäune und ein Drehkreuz gehen, an denen grüne und pinkfarbene Abfertigungsschildchen überprüft werden. Danach würde er einem Insider-Witz der elektronischen Fernmeldeaufklärung begegnen: Einer Kopie des internationalen Telekommunikationsabkommens - das auf eine Wand tapeziert ist. Artikel 22 des Abkommens, das sowohl Großbritannien, als auch die USA ratifiziert haben, verspricht, dass die Mitgliedsstaaten "damit einverstanden sind, alle möglichen Maßnahmen zu ergreifen, die kompatibel mit dem genutzten Telekommunikationssystem sind, um die Geheimhaltung der internationalen Korrespondenz zu sichern."

Die NSA, GCHQ und ihre Gegenspieler sammeln neben dem Abhören von ILC-Kommunikation bei Funkstationen auch gedruckte Abzüge aller internationalen Telegramme von öffentlichen und kommerziellen Betreibern in London, New York und anderen Zentren. Sie werden zu Fernmelde-Analysten gebracht und auf dieselbe Art und Weise behandelt wie ausländische Telegramme, die von Stationen wie Chicksands und Kirknewton aus der Luft abgefangen werden. Großbritannien tut dies bereits seit 1920, die Vereinigten Staaten seit 1945. Das gemeinsame Programm war bekannt als Operation Shamrock und wurde fortgeführt, bis es unter dem Einfluss der Watergate-Affäre von den Untersuchungen des US-Kongresses aufgedeckt wurde.

Am 8. August 1995 gab der NSA-Direktor Lew Allen gegenüber dem Pike-Komitee des US-Repräsentantenhauses zu, dass "die NSA systematisch internationale Sprach- und Kabelkommunikation abhört". Er gab auch zu, dass Nachrichten von und für amerikanische Bürger im Laufe der ausländischen Nachrichtenauklärung abgefangen wurden. In einer späteren Anhörung beschrieb er, wie die NSA "Beobachtungslisten" als Hilfe benutzte, um ausländische Aktivitäten von berichtenswertem Aufklärungsinteresse zu beobachten[6] .

Die amerikanischen Gesetzgeber kamen zu dem Schluss, dass diese Operationen möglicherweise nicht verfassungsgemäß waren. 1996 untersuchte ein Team des Justizministeriums mögliche Gesetzesbrüche der NSA. Ein Teil seines Berichts wurde 1998 veröffentlicht. Er beschreibt, wie Aufklärungsmaterial über US-Bürger, bekannt als Minaret, "*zufällig* beim Abhören durch die NSA von gehörter und nicht-gehörter (beispielsweise Telex) internationaler Kommunikation sowie Telex- und ILC-Kabelverkehr (Shamrock) durch das GCHQ erlangt" wurde (Betonung im Original).

Wie in Großbritannien hatten die NSA und ihre Vorgänger seit 1945 systematisch den Kabelverkehr von den Büros der großen Kabelfirmen wie RCA Global, ITT World Communications und Western Union abgefangen. Mit der Zeit wurde die Sammlung der Kopien der Papiertelegramme durch die Lieferung von Magnetbändern und schließlich durch die direkte Verbindung von Überwachungszentren zu internationalen Kommunikationsschaltungen ersetzt. In Großbritannien wurden und werden alle internationalen Telex-Verbindungen und Telegramm-Schaltungen in, aus oder durch das Land von einer GCHQ-Überwachungsanlage im Zentrum Londons verbunden, bekannt als UKC-1000.

## Filterprozesse

Holländische Überwachungsstation, Foto: Netherlands Military Intelligence Service

In den frühen 70er-Jahren wurde der aufwendige Prozess, der darin bestand, die Papierausdrucke nach Namen und Begriffen, die auf den Beobachtungslisten auftauchten, zu durchsuchen, allmählich durch automatisierte Computersysteme ersetzt. Diese Computer erledigten die Arbeit ähnlich wie die Suchmaschinen im Internet. Ausgehend von einem Wort, einem Satzteil oder einer Wortkombination identifizieren sie die Nachrichten mit den gewünschten Wörtern oder Satzteilen. Ihre Aufgabe, die heute große Ausmaße angenommen hat, ist es, die Schlüsselwörter oder Satzteile, die für die Geheimdienstbehörden von Interesse sind, mit dem riesigen Volumen internationaler Kommunikation zusammenzubringen, sie zu extrahieren und sie zu den Bedarfsträgern weiterzuleiten. Während der 80er Jahre entwickelte die NSA den schnellen Datenfinder-Mikroprozessor - der nur für diesen Zweck entworfen wurde. Später wurde er mit der Behauptung kommerziell vermarktet, dass er "weltweit die umfangreichsten zeichenbezogenen Vergleichsfunktionen eines Textgewinnungssystems" habe.

> Eine einzelne Einheit könnte mit "Billionen von Bytes aus Textarchiven und Tausenden von Online-Nutzern oder Gigabytes von Live-Data-Stream pro Tag umgehen, die gegen zehntausende von komplexen Interessenprofilen gefiltert werden."[7]

Obwohl unterschiedliche Systeme im Gebrauch sind, ist das sogenannte "Dictionary" das computergestützte Schlüsselsystem im Herzen der Rechenvorgänge einer modernen elektronischen Fernmeldeaufklärungsanlage. Jede Echelon- oder Echelon-ähnliche-Station enthält ein "Dictionary". Es gibt sogar tragbare Versionen, die in brieftaschengroße Einheiten namens Oratory[8] geladen werden können. Die Dictionary-Computer untersuchen den Kommunikations-Input und extrahieren, was den Interessenprofilen entspricht, für Berichte und weitere Analysen. In einem gewissen Sinn besteht die Hauptaufgabe der Dictionary-Computer darin, den größten Teil der abgehörten Informationen wegzuwerfen.

1992 beschrieb der ehemalige NSA-Direktor William Studeman in einer Rede über Informationsmanagement die Art und Weise, wie in Systemen wie Echelon gefiltert wird:

> "Ein [nicht näher bezeichnetes] Spionagesammelsystem kann allein in einer halben Stunde eine Million Inputs generieren; Filter sortieren bis auf 6.500 Inputs alles aus; nur tausend Inputs entsprechen den Auswahlkriterien; zehn Inputs werden normalerweise von Analysten aussortiert und nur ein Bericht wird produziert. Das ist die Routine-Statistik für eine Reihe von Spionageauffang- und Analysensystemen, die technisches Aufklärungsmaterial sammeln."[9]

Anders gesagt, führt von einer Million Kommunikationsverbindungen nur eine einzige möglicherweise zu einer Aktion durch eine Geheimdienstbehörde. Nur eine von tausend wird jemals von menschlichen Augen gesehen.

Gigantische Spionagedatenbanken unterstützen die Operationen jedes Dictionary. Sie enthalten Tabellen mit Informationen zu jedem Ziel. In der einfachsten Ausführung bestehen diese aus einer Liste von Telefon-, Handy-, Fax- oder Pager-Nummern, die mit den Zielen in jeder Gruppe verbunden sind. Sie können Postanschriften oder E-Mail-Adressen enthalten sowie Namen, Satzteile oder Konzepte, die unter den normalen Regeln der Informationsgewinnung formuliert werden können.

Obwohl die Dictionary-Methoden und Schlüsselwort-Suchmaschinen effektiv arbeiten, werden sie möglicherweise gemeinsam mit den gigantischen Spionagedatenbanken bald durch die Themenanalyse ersetzt. Dabei handelt es sich um eine mächtigere und intuitive Technik, deren Entwicklung die NSA stark vorantreibt. Themenanalyse ermöglicht den Kunden der Kommunikationsspionage ihre Computer zum Beispiel nach "suche mir Dokumente über Thema X" abzufragen. X könnte "Shakespeare in Love" oder "Waffen für Iran" sein.

In einem US-amerikanischen Standardtest zur Evaluierung von Themenanalyse-Systemen wird dem Analysenprogramm die Aufgabe erteilt, Informationen über Airbus-Subventionen zu finden. Zur herkömmlichen Herangehensweise gehört es, Computer mit Schlüsselbegriffen oder anderen relevanten Daten sowie Synonymen zu versorgen. In diesem Beispiel könnten die Bezeichnungen A-300 oder A-320 synonym mit Airbus sein. Der Nachteil dieser Vorgehensweise ist, dass man auch irrelevantes Aufklärungsmaterial finden könnte, wie beispielsweise Berichte über Exportsubventionen für die Güter, die mit einem Airbus transportiert werden, und relevantes Material übersehen könnte, wie beispielsweise eine Finanzanalyse für eine Firma in dem Konsortium, die das Airbus-Produkt nicht mit dem Namen nennt. Die Themenanalyse wird mit solchen Problemen fertig und ähnelt eher der menschlichen Aufklärungsarbeit.

1991 berichtete ein britisches Fernsehprogramm über die Arbeitsweise eines Dictionary-Computer in der Londoner Niederlassung GCHQ in der Palmer Street, Westminster (Station UK10000). Die Sendung zitierte Angestellte des GCHQ, die nicht auf Band gesprochen hatten:

"Oben im vierten Stock hat [die GCHQ] eine Gruppe von sorgfältig überprüften Leuten der British Telecom angestellt. [Zitat eines ehemaligen GCHQ-Angestellten:] Es hat mit nationaler Sicherheit nichts zu tun. Denn es ist nicht legal, jedes einzelne Telex abzugreifen. Und sie greifen alles ab: Die Botschaften, alle Geschäftsabkommen, sogar Geburtstagsgrüße. Sie füttern es in das Dictionary."

Zu den Zielen dieser Station gehörten Politiker, Diplomaten, Geschäftsleute, Gewerkschaftsführer, Nicht-Regierungsorganisationen wie Amnesty International und sogar die Hierarchie der katholischen Kirche.

## Weltraumaufklärung

Das Echelon-System scheint seit den frühen 70er-Jahren zu bestehen und seither eine ausgedehnte Entwicklung zu durchlaufen. Der Bedarf für effiziente Verarbeitungssysteme zur Ersetzung menschliche Operatoren, die Beobachtungslisten durchsuchten, war zum ersten Mal in den späten 60er-Jahren eingeplant, als die NSA und das GCHQ die ersten großen Satellitenabhörstationen planten. Die erste dieser Stationen wurde in Morwenstow in Cornwall gebaut und hörte mit zwei großen Antennenschüsseln die Kommunikation über dem Atlantik und dem Indischen Ozean ab. Die zweite wurde in Yakima, im nordwestlichen US-Staat Washington gebaut. Yakima hörte die Satellitenkommunikation über dem Pazifischen Ozean ab.

Ebenfalls in den frühen 70er Jahren entdeckten die NSA und die CIA, dass die elektronische Fernmeldeaufklärung im Weltraum weit effektiver und produktiver war als erwartet. Dies führte zu einer raschen Anhäufung von Magnetbändern, die schnell den verfügbaren Nachschub an sowjetischen Linguisten und Analysten übertraf. Ende der 70er Jahre war Menwith Hill in Mittelengland eine der Hauptstationen für die Verarbeitung von abgehörter Weltraum-Kommunikation. Ein Dokument von 1981 identifizierte die in Menwith Hill benutzten Spionagedatenbanken als Echelon II. Daraus lässt sich folgern, dass sich das Echelon-Netzwerk 1981 bereits in der zweiten Generation befand.

Mitte der 80er Jahre wurde der Telekommunikationsverkehr, der von den Dictionary-Computern rund um die Welt erfasst wurde, mit einer großen Bandbreite von Spezifikationen für den nonverbalen Verkehr durchsiebt. Im Rahmen von zwei Top-Secret-Projekten der NSA, P-377 und P-415, war Mitte der 80er Jahre eine weitreichende Automatisierung in Planung. Mit der Implementierung dieser Projekte wurde die Automatisierung der Beobachtungslisten aus den vorangegangenen Jahrzehnten perfektioniert. Die Computer ersetzten die Analytiker, die Papierstapel mit Abhörprotokollen mit Namen und Themen auf der Beobachtungsliste verglichen. In den späten 80er Jahren nahm die Belegschaft von Behörden für die elektronische Fernmeldeaufklärung von Ländern wie Großbritannien, Neuseeland und China an Trainingskursen für die neuen Echelon-Computersysteme teil.

Das Projekt P-415 ermöglichte es fernen Spionagekunden mit Hilfe des globalen Internets der NSA und des GCHQ die Computer jeder Auffangstation mit bestimmten Aufgaben zu programmieren und dann die Resultate automatisch zu erhalten. Ausgesuchte Eingangsnachrichten wurden mit Kriterien zur Weiterleitung im Dictionary verglichen. Wenn eine Übereinstimmung gefunden wurde, wurde das rohe Aufklärungsmaterial automatisch zu den bestimmten Empfängern weitergeleitet. Nach Angaben des neuseeländischen Autors Nicky Hager[10] wurden die Dictionary-Computer mit vielen tausend verschiedenen Sammelanforderungen gefüttert, die als Nummern (vierstellige Codes) beschrieben wurden.

1988 wurden Details des Projektes P-415 und der Pläne für eine massive globale Erweiterung des Echelon-Systems von Margaret "Peg" Newsham enthüllt. Margaret Newsham, eine ehemalige Computersystem-Managerin, arbeitete bis Mitte der 80er Jahre an klassifizierten Projekten für Auftragnehmer der NSA. Seit August 1978 arbeitete sie in der Menwith Hill-Basis der NSA als Software-Koordinatorin. In dieser Funktion kümmerte sie sich um eine Reihe von Computer-Datenbanken zur elektronischen Fernmeldeaufklärung, darunter auch Echelon II. Sie und andere halfen beim Aufbau von Silkworth mit, einem System zur

Verarbeitung von Informationen, die von den Nachrichtenaufklärungssatelliten Chalet, Vortex und Mercury gesendet wurden. Ihre Enthüllungen führten zu dem ersten Bericht zu Echelon, der 1988 veröffentlicht wurde[11] .

Peg Newsham arbeitete in Sunnyvale, Kalifornien für die Lockheed Space and Missiles Corporation. In dieser Funktion war sie an der Planung für eine massive Erweiterung des Echelon-Netzwerks beteiligt, einem Projekt, das intern als P-415 bezeichnet wurde. Während ihrer Beschäftigung bei Lockheed wuchsen ihre Bedenken aufgrund von Korruption, Betrug und Missbrauch innerhalb derjenigen Organisationen, die die elektronischen Überwachungssysteme planten und betrieben. Sie berichtete dem ständigen Sonderausschuss für Geheimdienste im US-Kongress darüber Anfang 1988. Sie sagte auch dem Ausschuss, wie sie Zeuge wurde, wie ein Telefongespräch des US-Senators Strom Thurmond abgehört wurde, als sie in Menwith Hill arbeitete.

Vermutlich hätten die ganzen Details von Echelon nie wirklich öffentliche Aufmerksamkeit erhalten, bis schließlich der neuseeländische Autor Nicky Hager in sechs weiteren Forschungsjahren die neue Echelon-Station, die ihren Betrieb in Waihopai auf der neuseeländischen Südinsel 1989 aufgenommen hatte, gewissenhaft untersuchte. Sein Buch "Secret Power" von 1996[12] basiert auf ausführlichen Interviews mit Mitgliedern der neuseeländischen Nachrichtenauklärungsorganisation. Es bleibt bis heute der bestinformierte und detaillierteste Bericht über die Funktionsweisen von Echelon. (siehe auch: Nicky Hager: Wie ich Echelon erforscht habe)

Anfang 2000 sickerten Informationen und Dokumente an einen US-Forscher durch, die viele Details darüber lieferten, wie Echelon für den weltweiten Gebrauch entwickelt wurde[13] . Ingenieure und Wissenschaftler arbeiteten an dem Projekt P-377, ebenfalls bekannt als Carboy II, das Teil eines NSA-Plans von 1982 war, der Lockheed Space and Missiles Systems zugeteilt worden war. Dieses Projekt erforderte die Entwicklung eines Standardkits von ADPE-Teilen (ADPE - Automated Data Processing Equipment), um damit Echelon-Basen auszurüsten. Zu den "üblichen Charakteristika" von ADPE im Echelon-System gehörten folgende Elemente:

- ein lokales Management-Subsystem
- ein Remote-Management-Subsystem
- das Senden von Funkfrequenzen
- ein Subsystem zur Verarbeitung von Kommunikation
- ein Subsystem zur Verarbeitung von telegrafischen Nachrichten
- ein Subsystem zur Verarbeitung von Frequency-Division-Multiplex-Telegrafie
- ein Subsystem zur Verarbeitung von Time-Division-Multiplex-Telegrafie
- ein Subsystem zur Sprachverarbeitung
- ein Modul zur Sprachaufnahme
- ein Subsystem zur Faxverarbeitung
- eine Anlage zur Produktion von [Sprach-] Bändern

Das Carboy-II-Projekt sah ebenfalls Software-Systeme vor, um Dictionary-Datenbanken zu laden und neue Versionen einzuspielen. Zu dieser Zeit basierte die Hardware für das Subsystem zur Verarbeitung des Dictionary auf einem Cluster von DEC-VAX-Minicomputern zusammen mit Spezialeinheiten zur Verarbeitung und Trennung verschiedener Typen von Satellitenkommunikation.

1998 und 1999 erhielt der Geheimdienstspezialist Jeff Richelson des Archivs für nationale Sicherheit[14] in Washington D.C. mit Hilfe des Informationsfreiheitsgesetzes eine Reihe moderner offizieller Dokumente der US-Navy und der US-Air-Force, die die fortgesetzte Existenz, das Ausmaß und die Erweiterung des Echelon-Systems bestätigten. Die Dokumente der US-Air-Force und der US-Navy identifizierten Echelon-Einheiten auf vier Basen und ließen vermuten, dass eine fünfte Basis ebenfalls Informationen von Kommunikationssatelliten als Teil des Echelon auffängt.

Zu diesen Basen gehört Sugar Grove in West Virginia, das in einer abgelegenen Gegend der Shenandoah-Berge, 250 Meilen südwestlich von Washington liegt. Es wird von einer US-Truppe der Marinesicherheit und der Luftwaffenaufklärung betrieben. Ein verbessertes System zur elektronischen Fernmeldeaufklärung namens Timberline II wurde in Sugar Grove im Sommer 1990 errichtet. Zur selben Zeit wurde laut der offiziellen US-Dokumente eine Echelon-Trainingsabteilung eingerichtet. Nachdem das Training beendet war, erhielt die Station 1991 die Aufgabe "eine Echelon-Basis zu unterhalten und zu betreiben"[15] .

Die US-Luftwaffe hatte öffentlich die Geheimdienstaktivitäten in Sugar Grove folgendermaßen bezeichnet:

> "... die Leitung von Satellitenkommunikationseinrichtungen [zur Unterstützung von] Nutzern von Comsat-Informationen ... dies wird durch die Bereithaltung eines ausgebildeten Kaders von Betreibern, Analytikern und Managern von Auffang-Systemen erreicht."

Der Almanach des Luftwaffengeheimdienstes von 1998/99 beschrieb die Mission der Einheit in Sugar Grove als Bereithaltung "erweiterter Aufklärungsunterstützung für Befehlshaber der Luftwaffe und andere Nutzer von Comsat-Information."[16] 1990 zeigten Satellitenaufnahmen vier Satellitenschüsseln in Sugar Grove. Eine Untersuchung vom Boden aus ergab im November 1998, dass diese inzwischen auf neun erweitert worden waren.

Weitere von der US-Luftwaffe veröffentlichte Informationen identifizierten die Station der US-Marinesicherheit in Sabana Seco in Puerto Rico als Comsat-Abhörbasis (Comsat=Kommunikationsatelliten). Ihre Mission ist es "die größte Station für die Verarbeitung und Analyse von Satellitenkommunikation zu werden". Diese und weitere Dokumente zu Echelon- und Comsat-Abhörstationen in Yakima, Sabana Seco (Puerto Rico), Misawa (Japan) und Guam wurden bereits im World Wide Web veröffentlicht.

Seit 1984 schlossen sich Australien, Kanada und Neuseeland den USA und Großbritannien beim Betreiben von Comsat-Abhörstationen an. Zur australischen Basis in Kojarena/Geraldton bei Perth in Westaustralien gehören vier Abhörschüsseln. Zu den Topzielen der Station gehören japanische diplomatische und kommerzielle Nachrichten, alle Art von Nachrichten aus und nach Nordkorea sowie Informationen über indische und pakistanische Nuklearwaffenentwicklungen. Eine zweite australische Comsat-Abhörstation in Shoal Bay im australischen Norden ist hauptsächlich auf Australiens nördlichen Nachbar, Indonesien, ausgerichtet. Laut australischen Quellen ist Shoal Bay nicht Teil des Echelon-Systems, da Australien den USA und Großbritannien den Zugang zu rohen Abhörprotokollen untersagt.

Die neuseeländische Basis in Waihopai verfügt heute über zwei Schüsseln, die auf Intelsat-Satelliten im Südpazifik ausgerichtet sind. Kurz nach der Veröffentlichung von "Secret Power" 1996 gelangte eine neuseeländische Fernsehstation an Bilder, die das Innere des Betreiberzentrums der Station zeigten. Diese Bilder wurden heimlich aufgenommen, indem man in der Nacht durch ein nur teilweise durch Vorhänge verdecktes Fenster filmte. Der Fernsehreporter konnte Nahaufnahmen von technischen Handbüchern machen, die im Kontrollzentrum herumlagen. Dabei handelte es sich um technische Handbücher für Intelsat, die bestätigten, dass die Station auf diese Satelliten angesetzt war. Verblüffenderweise schien die Station praktisch leer zu sein und vollautomatisch zu arbeiten.

Vor der Einführung von Echelon wussten die verschiedenen Länder und Stationen, was abgehört wurde und wem etwas weiter gegeben wurde. Nun werden bis auf einen Bruchteil die Nachrichten von Dictionary-Computern in entfernten Stationen aussortiert und an Kunden in Übersee, normalerweise die NSA, ohne das örtliche Wissen über das erhaltene Aufklärungsmaterial weitergeleitet.

## Ausblick

Die Informationen, die über das Echelon-Netzwerk und andere Teile des globalen Überwachungssystems abgefangen werden, werden von den USA und ihren Verbündeten für diplomatische, militärische und kommerzielle Zwecke genutzt. In den Jahren nach dem Kalten

Krieg wurde Personal sowohl in der NSA als auch dem GCHQ abgebaut. Viele der überseeischen Abhöreinrichtungen wurden geschlossen oder durch Einrichtungen ersetzt, die von einer Handvoll großer Feldstationen aus der Ferne kontrolliert werden. Obwohl dies routinemäßig abgestritten wird, spielt die kommerzielle und ökonomische Aufklärung eine große Rolle bei der internationalen elektronischen Fernmeldeaufklärung. Die US-Regierung unter Präsident Clinton richtete unter einer politischen Richtlinie von 1993, die umgangssprachlich unter dem Motto "das Spielfeld einebnen" bekannt wurde, neue Handels- und Wirtschaftskomitees ein. Die NSA und die CIA sollten für US-Geschäfte bei ausländischen Vertragsverhandlungen unterstützend tätig sein. In Großbritannien gab das GCHQ-Ermächtigungsgesetz von 1994 öffentlich als eines seiner Zwecke an, "das ökonomische Wohlergehen des Vereinigten Königreichs in Beziehung zu Aktionen oder Absichten von Personen außerhalb der britischen Inseln" zu fördern.

Riesige neue Speicher- und Verarbeitungssysteme werden erstellt, um die Online-Verarbeitung von Internet- und neuen internationalen Kommunikationsnetzwerken zu ermöglichen. In den frühen 90er-Jahren setzten sowohl das GCHQ als auch die NSA "Nearline- Speichersysteme" ein, die mehr als ein Terabyte speichern konnten. In der nahen Zukunft werden sie vermutlich Systeme einsetzen, die tausendmal größer sind. Das Entdecken von Schlüsselwörtern im gigantischem Umfang der täglich abgehörten schriftlichen Kommunikation - Telex, E-Mail und Daten - ist eine Routineaufgabe. Das Herausfiltern von Wörtern in gesprochener Kommunikation ist nicht effektiv, aber Techniken zur Identifizierung einzelner Sprecher sind bereits seit zehn Jahren in Gebrauch. Neue Methoden, die während der 90er-Jahre entwickelt wurden, werden bald zur Verfügung stehen, um Themen von Telefongesprächen zu erkennen. Sie werden es der NSA und ihren Kollaborateuren ermöglichen, den Inhalt von Telefonnachrichten automatisch zu verarbeiten - ein Ziel, das sich ihnen seit 30 Jahren entzogen hat.

Unter der Rubrik der Informationskriegsführung hoffen die Spionagebehörden den zunehmend üblichen Gebrauch von Verschlüsselung zu überwinden, indem sie Zielcomputer direkt stören oder angreifen. Diese Methoden bleiben umstritten, beinhalten aber Viren, Audiosoftware, Video und Datenfehler sowie präventive Manipulationen an Software oder Hardware (Hintertüren), um Informationen zu stehlen.

Im Informationszeitalter müssen wir eine Lehre neu lernen, die bereits ein Jahrhundert alt ist. Trotz der Weiterentwicklung der Technologie des 21. Jahrhunderts sind Emails für die Augen von Spionen und Eindringlingen so offen wie die ersten telegrafischen Nachrichten. Zu den Gründen gehört, dass die NSA und ihre Alliierten über Jahrzehnte hinweg entschlossen daran gearbeitet haben, die Privatsphäre in der internationalen Telekommunikation zu begrenzen und zu behindern. Ihr Ziel war es, Kommunikation unverschlüsselt zu halten und so Systemen wie Echelon einfachen Zugang und Verarbeitung zu gewähren. Sie wissen, dass die Privatsphäre und Sicherheit wie bereits ein Jahrhundert zuvor von geheimen Codes oder Verschlüsselung gewährleistet werden kann. Bis solche Schutzmassnahmen effektiv und allgegenwärtig sind, werden Echelon oder ähnliche Systeme unser ständiger Begleiter sein.

Duncan Campbell ist Autor des von dem Europäischen Parlament 1999 veröffentlichten Berichts "Abhörmöglichkeiten 2000".

forum
add message

top



heise online
redaktion

aktuell
special
kolumnen
netzraum
archiv
Echelon
Bio-Technik
Expo 2000
Games
Aufmerksamkeit
Infowar
Weltraum
Evolution der Kreativität
Globales Gehirn
english version

# Echelon in Holland

*Jelle van Buuren* *11.04.2000*

## Niederländischer Geheimdienst erhält Genehmigung zum Abhören von Satellitenkommunikation.

download

**Der niederländische Geheimdienst BVD erhält neue Vollmachten. Unter anderem werden die Abhörbefugnisse erweitert. Wenn es nach dem Willen der Regierung geht, wird der Dienst wahllos Satellitenkommunikation abhören und das Internet nach Schlüsselwörtern durchsuchen können. Der BVD erhält auch eine neue nachrichtendienstliche Aufgabe: das Sammeln wirtschaftlicher Informationen. Wie es scheint, bekommt auch Holland sein Echelon.**

Das neue "Gesetz über Nachrichten- und Sicherheitsdienste" (WIV), das derzeit im niederländischen Parlament debattiert wird, gibt den Befugnissen des BVD eine neue gesetzliche Basis. Konkret bedeutet das eine Erweiterung der Ermittlungsbefugnisse. Mit jedem Zusatz zum Originalentwurf werden neue Befugnisse verliehen. Im ersten Entwurf des neuen Gesetzes zum Beispiel stand, dass der BVD Telekommunikation abhören, aufzeichnen und belauschen darf. Im neuesten Zusatz von Anfang dieses Jahres wurde die Erlaubnis des "Empfangens" hinzugefügt. Das bedeutet, dass der BVD nun ermächtigt ist, Telekommunikation direkt anzuzapfen, zum Beispiel den gesamten GSM-Traffic im Äther. Damit ist der BVD nicht mehr auf die Willigkeit von Telekom-Unternehmen zum Abhören angewiesen, sondern kann sein eigenes Netzwerk von Empfangsstationen aufbauen, um den gesamten GSM-Traffic abzuhören. Damit ist auch die Möglichkeit ausgeschlossen, dass Provider etwas über die feine Tätigkeit des BVD nach außen durchsickern lassen.

Die größte Erweiterung aber ist der neu hinzugefügte Artikel 25a. Mit diesem Artikel wird der BVD ermächtigt, jegliche internationale

Telekommunikation, die nicht über Kabel läuft, flächendeckend abzufangen und nach verschiedenen Dingen von Interesse zu durchforsten (Personen, Gruppen, Schlüsselworte). Laut den zusätzlichen Erläuterungen zu diesem Gesetzesentwurf ist diese Form flächendeckenden Abhörens nötig, um festzustellen, ob irgendwelche interessanten Botschaften Teil der internationalen Kommunikation sind.

Die Regierung gibt nonchalant zu verstehen, dass es nicht verhindert werden könne, dass der BVD so Kenntnis von den Inhalten der übermittelten Botschaften bekomme, obwohl das, so die niederländische Regierung, nicht der Hauptzweck des ziellosen Abhörens sei.

> "Die Suche ist in erster Linie ein Werkzeug der Aufklärung über die Kommunikation, um die Art der Unterhaltung oder die Identität der Person oder Gruppe feststellen zu können. Dass die Agentur damit teilweise Kenntnis vom Inhalt der Kommunikation erhält, ist unvermeidbar, wenn man herausfinden will, wer kommuniziert und ob diese Person oder Gruppe von Interesse für die Agentur ist. Dennoch geht es bei der Suche nicht eigentlich darum, den gesamten Inhalt der Kommunikation zu erfahren. In gewisser Weise ist diese Aktivität mit dem Hineinhören in ein Telefongespräch vergleichbar, um herauszufinden, ob die Verbindung in Ordnung ist".

Das klingt nach einer sehr kreativen Art zu sagen, dass Abhören nicht wirklich Abhören ist, sondern nur ein technischer Test der Verbindung. Und dafür ist kein eigener Durchsuchungsbefehl vonnöten...

## Schlüsselworte

Da große Teile internationaler Telekommunikation über Satelliten und Funkstrecken übertragen werden, ist es klar, dass Artikel 25a den niederländischen BVD ermächtigt, alle diese Verbindungen abzuhören. Das heißt also es wird eine unkontrollierbare Befugnis verliehen, alle diese Kommunikationsformen abzuhören, die nicht an Kabel gebunden sind. Das kann auch von großen Konsequenzen für den Internetverkehr sein. Da Botschaften im Internet die günstigste Verbindung wählen und das Herz des Internet in den USA schlägt, gibt es eine gute Chance, dass Emails, die von einem Punkt in den Niederlanden zu einem anderen Punkt in den Niederlanden eine Route über die USA wählen. In der Zukunft könnte das auch bei Telefongesprächen der Fall sein. Alle diese Botschaften könen abgefangen und durchsucht werden. Bereits jetzt werden die Telefongespräche zwischen zwei großen Städten in Holland, zwischen Amsterdam und Rotterdam über Funkwege übertragen.

Im ersten Entwurf des WIV musste der Innenminister noch die Erlaubnis für die Schlüsselwörter erteilen, mit denen der Nachrichtendienst die abgehörte Telekommunikation durchsucht. Nach den letzten Veränderungen erhält der Innenminister nur noch einmal im Jahr eine Liste der verwendeten Schlüsselwörter zur Kenntnisnahme, während der BVD ermächtigt wurde, neue Schlüsselwörter nach eigenem Gutdünken

hinzuzufügen.

Abgesehen davon erhält der BVD nun auch die Befugnis, abgehörte Kommunikation aufzuzeichnen. Während die erste Fassung des WIV noch verlangte, dass der BVD alle abgehörte Kommunikation, die für ihn nicht von Interesse ist, sofort zu löschen, erhält er nun das Recht, diese für ein Jahr zu speichern.

Auf diese Art schafft die niederländische Regierung ihr eigenes Mini-Echelon. Der BVD benutzt für seine Abhörmaßnahmen das technische Informationsverarbeitungszentrum (TIVC) des Marine-Geheimdienstes. Dieses auf dem Marine-Stützpunkt Kattenberg bei Amsterdam gelegene Zentrum verarbeitet Satellitenkommunikation, die von verschiedenen Bodenstationen aufgefangen wird. Das TIVC arbeitet auf dieselbe Art und Weise wie sein großer Bruder, die NSA, wie durch die Publikation interner Dokumente in der niederländischen Tageszeitung *De Haagse Courant* 1985 gezeigt wurde. Satellitenkommunikation wurde abgehört, aufgezeichnet und nach Schlüsselwörtern zur weiteren Analyse durchkämmt. Die daraus gewonnenen Informationen schickte das TIVC an den Auslandsnachrichtendienst (IDB), bevor dieser 1994 nach einer Serie von Skandalen geschlossen wurde. Seither befindet sich die gesamte *Signal Intelligence* in den Händen der Marine-Aufklärung.

Laut einer Studie der zweier niederländischer Geheimdienstexperten (Bob de Graaff and Cees Wiebes, *Villa Maarheeze*, 1998), ist das TIVC Teil eines größeren internationalen Netzwerks und arbeitet eng mit anderen westlichen Diensten zusammen. So berichtete TIVC zum Beispiel 1972 dem israelischen Geheimdienst Mossad, dass Ägypten und Lybien eine Unterwasserverbindung für Telefongespräche und Telexe aufgebaut hatten. Israelische Sondereinheiten zerstörten diese Leitung, so dass Ägypten und Lybie wieder auf Satellitenkommunikation zurückgreifen mussten, ein leichtes Ziel für das Abhören. Nach Aussagen der Autoren protestierte die amerikanische CIA 1992 heftig gegen die bevorstehende Auflösung des IDB, da sie fürchteten, dass dadurch niederländische Sigint-Kapazitäten vermindert werden würden.

## Vitale ökonomische Interessen

Die neuen Befugnisse zum flächendeckenden und ziellosen Abhören von Satellitenkommunikation werden zweifellos auch zur Wirtschaftsspionage benutzt werden. Schon in der Vergangenheit wurden Sigint-Kapazitäten für wirtschaftliche Zwecke benutzt. Die Autoren des oben erwähnten Berichts sprechen von "inzestuösen Beziehungen" zwischen niederländischen Nachrichtendiensten und der Industrie und nennen dafür einige Beispiele. Führende Persönlichkeiten holländischer Unternehmen mit großem Auslandsengagement arbeiteten zugleich für den IDB. Zum Ausgleich bekamen sie wirtschaftsbezogenes Geheimdienstmaterial vom IDB. Der holländische multinationale Konzern Philips hat laut dieser

Studie enge Beziehungen mit heimischen Nachrichtendiensten. Das Unternehmen baute angeblich Abhör-Einrichtungen in Telefonschaltanlagen ein, die an ausländische Unternehmen und Regierungen verkauft wurden.

Mit dem neuen Gesetz für Geheimdienste erhält der BVD offiziell die Aufgabe zur Wirtschaftsspionage. Der BVD muss "vitale ökonimische Interessen schützen", was als Teil der nationalen Sicherheit gesehen wird.

> "Die niederländische Wirtschaft ist äußerst abhängig von ökonomischen Entwicklungen überall auf der Welt. Diese Entwicklungen sind von zunehmender Internationalisierung und Globalisierung gekennzeichnet. Anderswo getroffene Entscheidungen können von tiefem Einfluss auf die niederländische Wirtschaft sein. Es ist möglich, Informationen über diese Entwicklungen auf verschiedene Arten zu erhalten, zum Beispiel durch Zusammenarbeit mit Geheimdiensten anderer Länder. Diese Dienste werden allerdings zuerst ihre eigenen Interessen berücksichtigen. Um nicht von Informationen von Dritten abhängig zu sein, denkt die Regierung, dass es notwendig ist, die Position der eigenen Information auszubauen und zu stärken".

Was genau die "vitalen ökonomischen Interessen" sind, bleibt jedoch von einer Wolke des Geheimnisses verdeckt.

> "Deshalb möchten wir mit der Bemerkung schließen, dass mit der Erklärung der "vitalen ökonomischen Interessen" in Bezug zur Arbeit des BVD auch die Möglichkeit geschaffen wird - wenn es angemessen erscheint - Ermittlungen in diesem Bereich zu führen, auch wenn die nationale Sicherheit direkt nicht betroffen ist oder das schwierig zu argumentieren wäre".

## Verschlüsselung

Die neuen Befugnisse des BVD sind auch hinsichtlich mehrerer Paragraphen interessant, die Verschlüsselung und Informationstechnologie betreffen. Der BVD darf in Wohnungen und Büros einbrechen, um Wanzen in Computer-Keyboards einzubauen. Darüberhinaus darf der BVD auch in Computer eindringen, um Informationen, die auf diesem Computer gespeichert sind, zu stehlen, zu verändern oder zu löschen. Mit anderen Worten, der BVD erhält die Erlaubnis zum Hacking. Der Nachrichtendienst kann damit Daten von Rechnern stehlen, Software manipulieren, Passwörter korrumpieren oder trojanische Pferde installieren, so dass der Zugang sichergestellt und Kryptographie umgangen werden kann.

Kryptographie ist ein Thema von besonderem Interesse für den BVD. Im Gesetzesentwurf werden die Befugnisse zur Entschlüsselung erweitert. Im ersten Entwurf wurde dem BVD zugestanden, verschlüsselte Kommunikation und Daten mit "technischen Mitteln" zu entschlüsseln. In der letzten Fassung wurde das dahingehend erweitert, dass

Entschlüsselung "mit allen möglichen Mitteln" zugelassen ist. Laut den erklärenden Zusätzen "hat die Praxis gezeigt, dass Entschlüsselung auch mit anderen als technischen Mitteln möglich ist".

Diese kryptische Beschreibung scheint auf Infiltratoren hinzuweisen, die anderen Passwörter entlocken, oder ihnen über die Schulter spähen, wenn Botschaften verschlüsselt werden, oder auf Agententeams, die in Wohnungen und Büros einbrechen, auf der Suche nach dem Stück Papier auf dem das Passwort notiert ist.

Auch die Artikel über das Abhören von Telekommunikation enthalten Abschnitte über Kryptographie. Verschlüsselte Botschaften dürfen solange aufbewahrt werden, wie der BVD zur Entschlüsselung braucht. In den Erklärungen heißt es:

> "Was Telekommunikation angeht, die nicht entschlüsselt wurde und wobei allein die Tatsache, dass Kryptographie benutzt wurde, diese Kommunikation für den Dienst interessant macht, so ist es wünschenswert, dass diese Kommunikation so lange gespeichert wird, bis die Kapazität zur Entschlüsselung vorhanden ist oder entwickelt wurde".

Die Benutzung einer ganz normalen Technik zum Schutz der Privatsphäre, von Handelsgeheimnissen oder sensibler politischer Information ist in den Augen der niederländischen Regierung also bereits ein höchst verdächtiger Akt. Der Entwurf macht es auch zur Verpflichtung für jeden, von dem die Behörden annehmen, dass er Zugang zu den Schlüsseln hat, mit dem Geheimdienst bei der Entschlüsselung zu kooperieren. Die Weigerung kann mit bis zu zwei Jahren Haft bestraft werden. Das Parlament hat die Regierung bereits gefragt, ob das auch bedeutet, dass Verdächtige gezwungen sind, Schlüssel zu übergeben.

Bis jetzt gab es dazu noch keine Antwort. Falls die Regierung aber bestätigt, dass diese Verpflichtung auch für Verdächtige gilt, dann wäre das eine deutliche Verletzung grundlegender Menschenrechte, so wie zum Beispiel im Vertrag über den Schutz der Menschenrechte und grundlegenden Freiheiten festgelegt. Es würde bedeuten, zur eigenen Verurteilung beitragen zu müssen und wäre auch eine Umkehrung der Beweislast.

Übersetzung: Armin Medosch

paranoia *by anonymous coward, 16.4.2000*

Echelon. Machen wir uns nichts vor *by Echelon-praktischer-Betrachter, 25.8.2000* new

Spannende Ähnlichkeit bzgl. Kryptographie zum RIP in England *by Uwe W. Fiedler, 12.4.2000*

Yahoo wegen Nazi-Auktionen verklagt *by lwxcjmich, 12.4.2000*

Spartip *by gHack, 12.4.2000*

Sehr explizit, aber nicht neu. Wie sieht die Entwicklung aus *by Werner Lehmann, 11.4.2000*

schöne, neue welt... *by john dow, 11.4.2000*

top



heise online redaktion

aktuell
special
kolumnen
netzraum
archiv
Echelon
Bio-Technik
Expo 2000
Games
Aufmerksamkeit
Infowar
Weltraum
Evolution der Kreativität
Globales Gehirn

weitere artikel
STOA-Bericht von 1997

# Abhören im Jahr 2000

*Christiane Schulzki-Haddouti, Armin Medosch* *10.05.1999*

## Ein neuer STOA-Bericht zu technischen Abhörfähigkeiten, ECHELON, Wirtschaftsspionage und Internetüberwachung ist erschienen.

download

**Vor wenigen Tagen nahm das Science and Technology Options Assessment Panel (STOA) des Europäischen Parlaments den Bericht "Interception Capabilities 2000" als Arbeitspapier an. Der Bericht untersucht den Stand der Dinge bezüglich des Abhörens und Überwachens von elektronischer Kommunikation für Geheimdienstzwecke ("communications intelligence") und kommt zu Ergebnissen, welche die schlimmsten Befürchtungen nähren.**

- 30 Meter Antenne in Morwenstow, England, zum Abhören regionaler Satelliten über dem atlantischen und indischen Ozean. Foto D.Campbell

Weltweit seien umfassende Systeme implementiert, die jede wichtige Form moderner Kommunikation abfangen und verarbeiten können. Im STOA-Bericht von 1997 war erstmals das System zum Abhören kommerzieller Telekommunikationssatelliten (ECHELON) in einem offiziellen EU-Papier erwähnt worden. Bei den darauf folgenden Diskussionen im Europa-Parlament hatte Martin Bangemann noch blauäugig behaupten können, von der Existenz von ECHELON nichts gewußt zu haben. Der neue Bericht legt nun umfassende Materialien vor, in denen Geschichte und Arbeitsweise des ECHELON-Systems aufgezeigt werden.

*Routinemäßiges Abhören für Wirtschaftsspionage*

Rund 120 Abhörstationen sammeln im Simultanbetrieb Aufklärungsmaterial. U-Boote werden routinemäßig benutzt, um Kontinente verbindende Telefonkabel anzuzapfen. Der Bericht kommt zu der Schlußfolgerung, daß das Abhören internationaler Kommunikation seit langer Zeit routinemäßig benutzt wird, um heikle Daten über Individuen, Regierungen, Handelsorganisationen und internationale Institutionen zu sammeln. Europäische Wirtschaftsunternehmen seien demnach das Ziel von Abhöraktionen und Regierungen führender westlicher Nationen würden das von Geheimdiensten gewonnene Material benutzen, um eigenen Spitzenunternehmen Wettbewerbsvorteile zu verschaffen.

Auch für das Abhören des Internets seien die US-Geheimdienste, allen voran die NSA, bestens gerüstet. So würden die sogenannten UKUSA-Staaten (die traditionellen West-Alliierten USA, UK, Kandada, Australien) schon seit den achtziger Jahren ein auf dem Internet Protokoll beruhendes, geschlossenes Netz betreiben, das größer war als der gesamte Rest des Internets in dieser Phase. Seit 1995 habe die NSA "Sniffer-Software" an den neun wichtigsten Internetknoten in den USA installiert, allen voran an den von US-Regierungsbehörden betriebenen Knoten FIX East und Fix West, die wiederum mit den kommerziellen Knoten MAE East und MAE West eng verbunden sind. Da der Internet-Backbone immer noch US-dominiert ist, werden auch viele ausländische Datenpackete über diese Knoten geroutet.

## Grenzen der Abhörmöglichkeiten

Der Bericht weist aber auch zugleich auf die Grenzen des grenzenlosen Abhörens hin. Entgegen anderslautenden Presseberichten und trotz 30 Jahren Forschung gäbe es noch keine effektiven Methoden, um Sprachtelefonie elektronisch und in Echtzeit nach Stichwörtern zu durchforsten. Allerdings sei es möglich, sogenannte Stimmprofile ("voiceprints") zu erstellen, diese in Datenbanken abzuspeichern und sie mit geführten Telefongesprächen abzugleichen, so daß Zielpersonen anhand ihrer Sprachcharakteristik erkannt werden können. Obwohl global jährlich 15 bis 20 Milliarden Euro für nachrichtendienstliches Abhören und verwandte Aktivitäten ausgegeben werden, stoßen die entsprechenden Behörden an ihre Kapazitätsgrenzen.

Der ehemalige NSA Direktor William Studeman bestätigt dies mit folgenden, im Bericht zitierten Aussagen:

"Informationsmanagement wird zum größten, singulären Problem für die US-Geheimdienste. [...] Ein technisches System zur Informationssammlung allein generiert 1 Million Inputs pro halber Stunde. Filter reduzieren das auf 6500 Inputs, nur 1000 Inputs entsprechen den Kriterien zur Weiterleitung; 10 Inputs davon werden von Mitarbeitern analysiert und nur ein Bericht wird schließlich verfaßt".

Auch verschlüsselte Internetkommunikation macht den Geheimdiensten zu schaffen, da immer aufwendigeres Equipment beschafft werden muß, um noch an die Nachrichten im Klartext zu kommen. Laut dem Bericht sind die jüngsten Bemühungen der US-Diplomatie, eine obligatorische Schlüsselhinterlegung (Key Escrow) in Europa durchzusetzen, ein Täuschungsmanöver. Für die Öffentlichkeit werden Argumente wie organisiertes Verbrechen, Drogenhandel und Kinderpornographie in die Waagschale geworfen. Das eigentliche Motiv der US-Regierung sei aber das flächendeckende Sammeln von nachrichtendienstlichem Aufklärungsmaterial.

*Unterscheidung zwischen Strafverfolgung und geheimdienstlichen Aktivitäten.*

Deshalb sei es, so der Bericht in seinen Schlußfolgerungen, für den Schutz der Menschen- und Grundrechte und der im guten Glauben geführten Wirtschaftstätigkeit unabdingbar, eine klare Unterscheidung zwischen inländischem Abhören zu Strafverfolgungszwecken und dem Abhören zu Zwecken der Geheimdienste zu treffen. Auch die ökonomischen Kosten würden einen Ansatzpunkt bieten, um das nicht-autorisierte Abhören von Kommunikation einzudämmen. Nicht zuletzt kann durch den Einsatz von Verschlüsselungsverfahren das Verarbeiten der Inhalte von Nachrichten ebenso wie das Analysieren von Verbindungsdaten eingeschränkt werden.

Verfaßt wurde der Bericht vom schottischen Journalisten Duncan Campbell. Dieser arbeitet seit Ende der 70er Jahre über den Themenkomplex Überwachen und Abhören, hat 1988 als erster Journalist über die Existenz von ECHELON berichtet und in jüngster Zeit die Berichterstattung in Telepolis über ENFOPOL 98 bereichert. Sein Artikel über "ILETS, die geheime Hand hinter ENFOPOL" beruht auf im Rahmen des STOA-Berichts geführten Recherchen.

Die offizielle Version des Berichts INTERCEPTION CAPABILITIES 2000 kann beim Büro des Europäischen Parlaments in Luxemburg bestellt werden und wird in kürze auch auf einer Web-site der EU abrufbar sein.

aktuell
special
kolumnen
netzraum
archiv
Echelon
Bio-Technik
Expo 2000
Games
Aufmerksamkeit
Infowar
Weltraum
Evolution der Kreativität
Globales Gehirn

# Literaturangaben

1) Der Bericht "Abhörmöglichkeiten 2000" ist Teil einer Serie von vier Berichten über "Development of surveillance technology and risk of abuse of economic information". Der Bericht enthält eine detaillierte Beschreibung über die verschiedenen Abhörmöglichkeiten von Kommunikation.

back

2) "An appraisal of technologies of political control", Bericht für das "European Parliament Scientific and Technological Options Office" (STOA), Steve Wright, Omega Foundation, Manchester, Großbritannien, Januar 1998.

back

3) Die Abkommen werden manchmal als "TEXTA Authority" bezeichnet. TEXTA steht für "Technical Extracts of Traffic Analysis" und ist eigentlich eine umfangreiche Aufzählung jeder einzelnen Kommunikationsquelle, die von einem Dienst identifiziert wurde. Sie ist nach Ländern, Nutzern, Netzwerken, Kommunikationssystemtypen und anderen Merkmalen katalogisiert und sortiert.

back

4) Special Compartmented Intelligence, bekannt als Spezialaufklärung, ist geheimes Aufklärungsmaterial, das nur mit einem Codewort einzusehen ist. Spezielle Regelungen gelten für Büros, in denen SCI untersucht wird. Sie müssen physisch sicher und elektronisch abgeschottet sein. Diese Büros sind bekannt als SCIFs (SCI Facilities - SCI-Einrichtungen).

back

5) Das Intranet der US-Geheimdienste wird beschrieben in "Top Secret Intranet: How U.S. Intelligence Built Intelink -- the world's

largest, most secure network", Frederick Martin, Prentice Hall, 1999

back

6) The National Security Agency and Fourth Amendment Rights, Anhörungen vor dem Sonderkomitee zur Untersuchung von Regierungsoperationen in Bezug auf Geheimdienstaktivitäten, US-Senat, Washington 1976

back

7) Paracel Corporation, FDF "Textfinder". Es wird behauptet, das wäre das "schnellste, anpassungsfähigste Informationsfiltersystem weltweit".

back

8) Oratory wird beschrieben in "Spyworld", Mike Frost,Michel Gratton, Doubleday Canada, 1994. Es wurde benutzt, um die von in Botschaften verborgenen Abhöranlagen abgehörten Nachrichten auszusortieren.

back

9) Anmerkungen für das Symposium zu "National Security and National Competitiveness: Open Source Solutions" von Vizeadmiral William Studeman, Deputy Director der Central Intelligence Agency und ehemaliger Direktor der NSA vom 1. Dezember 1992, McLean, Virginia

back

10) Secret Power, Nicky Hager, Craig Potton Publishing, Neuseeland, 1996.

back

11) New Statesman (UK), 12. August 1988. Zu dieser Zeit war Frau Newsham eine vertrauliche Informationsquelle und wurde im Artikel nicht genannt. Im Februar 2000 teilte Frau Newsham, nachdem sie bereits in Rente lebte und mit einer ernsten Krankheit zu kämpfen hatte, mit, dass sie als Originalquelle der Informationen über Echelon identifziert werden dürfe. Sie erschien auch in einer CBS-Fernsehsendung über Echelon, Sixty Minutes vom 27. Februar 2000.

back

12) Secret Power, Nicky Hager, Craig Potton Publishing, Neuseeland, 1996.

back

13) "Echelon P-377 Work Package for CARBOY II", veröffentlicht unter cryptome.org/echelon-p377.htm

back

14) Eine unabhängige Organisation, die neben anderen Aufgaben auch US-Regierungsdokumente katalogisiert, die aufgrund der Informationsfreiheitsgesetzgebung erlangt wurden.
www.gwu.edu/~nsarchiv

back

15) Naval Security Group Command Regulation C5450.48A; siehe Fußnote 23.

back

16) "Desperately Seeking Signals", Jeff Richelson, Bulletin of the Atomic Scientists, März/April 2000.

back

top

bereits in Rente lebte und mit einer ernsten Krankheit zu kämpfen hatte, mit, dass sie als Originalquelle der Informationen über Echelon identifziert werden dürfe. Sie erschien auch in einer CBS-Fernsehsendung über Echelon, Sixty Minutes vom 27. Februar 2000.

[12]) Secret Power, Nicky Hager, Craig Potton Publishing, Neuseeland, 1996.

[13]) "Echelon P-377 Work Package for CARBOY II", veröffentlicht unter cryptome.org/echelon-p377.htm [10]

[14]) Eine unabhängige Organisation, die neben anderen Aufgaben auch US-Regierungsdokumente katalogisiert, die aufgrund der Informationsfreiheitsgesetzgebung erlangt wurden. www.gwu.edu/~nsarchiv [11]

[15]) Naval Security Group Command Regulation C5450.48A; siehe Fußnote 23.

[16]) "Desperately Seeking Signals", Jeff Richelson, Bulletin of the Atomic Scientists, März/April 2000.

**Links**

[0] http://www.heise.de/tp/deutsch/special/ech/6730/1.html
[1] http://www.gchq.gov.uk
[2] http://www.heise.de/tp/deutsch/special/ech/6728/1.html
[3] http://www.heise.de/tp/deutsch/special/ech/6638/1.html
[4] http://www.gwu.edu/~nsarchiv
[5] http://www.heise.de/tp/deutsch/special/ech/6663/1.html
[6] http://www.europarl.eu.int/dg4/stoa/en/publi/pdf/98-14-01-2en.pdf
[7] http://www.europarl.eu.int/dg4/stoa/en/publi/pdf/98-14-01-2en.pdf
[8] http://www.europarl.eu.int/dg4/stoa/en/publi/default.htm
[9] http://www.europarl.eu.int/dg4/stoa/en/publi/default.htm#up
[10] http://cryptome.org/echelon-p377.htm

---

# Wie ich Echelon erforscht habe

*Nicky Hager* *11.04.2000*

## Geheimdienste arbeiten meist nicht völlig hinter unüberwindbaren Mauern

**Nicky Hager war derjenige, der erstmals in Neuseeland das globale Lauschsystem Echelon aufgedeckt hatte. Mit seinen Berichten und seinem 1996 erschienenem Buch Secret Power hat er wesentlich die Diskussion über die Praktiken der Geheimdienste angestoßen, die zu den STOA-Berichten und schließlich der Forderung des Europäischen Parlaments nach einem Untersuchungsausschuß geführt haben. In seinem ersten Artikel berichtet er für Telepolis, wie er die Informationen über Echelon erlangt hat. In einem zweiten Artikel, den Telepolis demnächst veröffentlicht, rekapituliert er, wie sich die Informationen über Echelon verbreitet haben.**

download

Viele Menschen haben gefragt, wie ich Informationen über Echelon herausbekommen habe. Das sind Erfahrungen, von denen ich glaube, dass es wichtig ist, sie öffentlich mitzuteilen. Der Ausgangspunkt meiner Forschung war das Herausfinden der Namen und Berufszeichnungen aller Angestellten des elektronischen Geheimdienstes von Neuseeland. Der Durchbruch kam, als ich erkannte, dass alle ihre Namen in den Personallisten der Behörden versteckt und über viele Seiten von Angestellten des Militärs verstreut waren. Da kaum jemand überhaupt von der Existenz der Organisation Kenntnis hatte, dachte man wahrscheinlich, dass die Namen niemals bemerkt würden.

Nachdem ich weitere Listen über das militärische Personal, die die Spione nicht aufführten, erhalten und die eine Liste von der anderen abgezogen hatte, besaß ich schließlich eine fast perfekte Liste von Hunderten von Menschen des Geheimdienstes und von vielen weiteren, die früher für ihn gearbeitet hatten. Ein Vergleich dieser Liste mit anderen Personallisten

des öffentlichen Dienstes gewährte mir Einblick in die allgemeinen Berufsbezeichnungen all dieser Menschen. Durch die Kombination mit einigen anderen Informationen, die schon früher an die Öffentlichkeit gekommen waren, konnte ich Schritt für Schritt den gesamten, hochgeheimen Organisationsplan aus relativ öffentlich zugänglichen Quellen erschließen. Dann begann die Arbeit, die Menschen in den verschiedenen Bereichen zu finden, die zum Sprechen bereit waren.

Menschen entscheiden sich aus unterschiedlichen Gründen, Informationen weiter zu geben. Es gibt beispielsweise einfach die Erleichterung, mit jemandem zu sprechen, der über ihre Arbeit Bescheid weiß, nachdem sie jahrelang ihrem Ehemann oder ihrer Ehefrau verschweigen mussten, was sie jeden Tag gearbeitet hatten. Doch der Hauptgrund in diesem Fall war die Sorge der Angestellten, dass ein wichtiger Bereich der Regierungsaktivitäten zu lange Zeit vor dem Parlament und vor der Öffentlichkeit zu stark geheimgehalten worden war. Manche hatten eine starke Abneigung gegen Geheimdienstaktivitäten, die sie als unmoralisch oder nicht im Sinne der Interessen des Staates betrachteten. Ich suchte mir diejenigen aus, von denen ich glaubte, dass sie mit mir sprechen könnten, suchte Menschen aus allen Abteilungen, die ich untersuchen wollte, und begann dann vorsichtig mit ihnen Kontakt aufzunehmen. Ich bin noch immer erstaunt, dass die meisten bereit waren, mit mir zu sprechen, woraus viele hundert Seiten Interviewaufzeichnungen über die Hightech-Lauschsysteme entstanden, mit denen sie gearbeitet hatten.

Als die Information einmal zu fließen begonnen hatte, setzte ein richtiger Strom ein. Innerhalb der Geheimdienste wurde bekannt, dass ich begonnen hatte, sie zu untersuchen. Neue Angestellte wurden vor mir durch Sicherheitsmitteilungen gewarnt, obgleich sie keine Vorstellung davon hatten, was ich bereits erfahren hatte oder dass ich ein Buch schreiben wollte. Doch genau dies schien die Bereitschaft noch zu verstärken, Geheimnisse mitzuteilen. Lange Zeit war ich immer dann aufgeregt, wenn ich mit meiner Hand in meinen Briefkasten griff, falls ich dort geheime Dokumente finden sollte, die jemand anonym hineingesteckt hatte.

Einige Informationen hatte ich erhalten, weil "high security" mehr mit Schein als mit der Wirklichkeit zu tun haben kann. Beispielsweise müssen sich die Geheimdienstchefs sicher gewundert haben, warum ich wiederholt die neuesten Ausgaben der internen Newsletter des Dienstes angefordert habe, da sie diese nur freigaben, wenn jedes bedeutungsvolle Wort schwarz durchgestrichen war. Diese Menschen sind die Hauptberater unserer Regierung in Sicherheitsfragen, aber sie haben niemals erkannt, dass ich, wenn ich die fotokopierten Newsletter gegen meine Schreibtischlampe hielt, mit einiger Anstrengung praktisch alles lesen konnte: all die Details über die neuen oder umstrukturierten Abteilungen, die Personalveränderungen, die Mitteilungen ins Ausland und so weiter, die unleserlich gemacht wurden.

Auch die höchste Geheimhaltung an der Waihopai-Station, dem geheimsten Lauschposten des Geheimdienstes, war mehr Schein als Wirklichkeit. Trotz der Elektrozäune, Sensoren und Stacheldrähte ging ich dort einige Male hin, während ich mein Buch schrieb, und konnte später sogar ein Aufnahmeteam für eine Dokumentationssendung im Fernsehen mit hinein nehmen. Dort filmten sie die Echelon-Ausrüstung im zentralen Operationsraum und sogar die Titel der Intelsat-Handbücher (International Satellite Organisation) auf den Schreibtischen, die belegten, dass der Lauschposten auch normale öffentliche Telekommunikationsnetze abhörte.

Obgleich es sehr geheime Informationen gab, die ich nur von den Insidern erfahren konnte, stammte ein Großteil der Informationen aus sorgfältiger Feldarbeit (beispielsweise durch das Beobachten der Veränderungen bei unterschiedlichen Echelon-Post auf der ganzen Welt, während die Telekommunikationstechnik sich veränderte) und aus Informationsschnipseln aus nicht geheimen Dokumenten und Nachrichten. Manche der Insider waren Freunde von Freunden von Freunden, die ich einfach dadurch herausfand, dass ich viel herumfragte. Man sollte nicht von der Voraussetzung ausgehen, dass geheime Organisationen undurchdringlich sind. Es gibt eine Menge wichtiger Forschungsarbeit über viele Themen in jedem Land, die nur darauf wartet, durchgeführt zu werden.

Aus dem Englischen übersetzt von Florian Rötzer

forum
add message

:-)... *by Z, 11.4.2000*

Ein Schelm wer sich böses dabei denkt ... *by Zardoz, 12.4.2000*

Ich hab mal... *by Z, 12.4.2000*

Auf der ersten Liste *by Kassandra, 11.4.2000*

so wie ich das verstanden habe ... *by Roger, 11.4.2000*

weiter nachgehakt ... :-) *by H. Kater, 11.4.2000*

top

aktuell
special
kolumnen
netzraum
archiv
Echelon
Bio-Technik
Expo 2000
Games
Aufmerksamkeit
Infowar
Weltraum
Evolution der Kreativität
Globales Gehirn

english version

weitere artikel
Die Echelon-Debatte geht jetzt erst richtig los

# Ehemaliger CIA-Direktor sagt, die Wirtschaftsspionage der USA würde auf "Bestechungsaktionen der Europäer " zielen

*Duncan Campbell* *12.03.2000*

"Wir haben darüber schon in der Vergangenheit Spionage betrieben. Ich hoffe, ...dass die Regierung der Vereinigten Staaten fortfährt, Bestechung zum Ziel von Spionage zu machen."

download

**Der ehemalige Direktor der CIA, James Woolsey, bestätigte am 7. März in Washington, dass die USA Wirtschaftsgeheimnisse stehlen, "mit Spionage, durch Abhören, durch Aufklärungssatelliten", und dass es nun "verstärkte Anstrengungen" bezüglich Wirtschaftsspionage gäbe.**

Er behauptete, dass Wirtschaftsspionage gerechtfertigt sei, da europäische Unternehmen eine "nationale Kultur" der Bestechung hätten und dass sie "als erste im Verdacht" stünden, "wenn es darum geht, Bestechungsgelder im Zusammenhang mit großen internationalen Aufträgen zu zahlen".

In Antwort auf den Bericht an das Europaparlament bezüglich Abhörmöglichkeiten und das Überwachungssystem Echelon sagte Woolsey, dass der Bericht "Interception Capabilities 2000", der am 23. Februar dem Bürgerrechtsausschuss vorgestellt worden war, "intellektuell aufrichtig" sei. In den zwei Fällen, die in dem Bericht zitiert werden, "ist es ein Faktum, dass der Gegenstand amerikanischer Aufklärung Bestechung war."

"Das ist korrekt", sagte er einem vollem Auditorium ausländischer Presse.

"Wir haben darüber schon in der Vergangenheit Spionage betrieben. Ich hoffe, ...dass die Regierung der Vereinigten Staaten fortfährt, Bestechung zum Ziel von Spionage zu machen."

Woolsey behauptete, dass die Ergebnisse amerikanischer Wirtschaftsspionage normalerweise von der US-Regierung weiterbehandelt und nicht an US-Wirtschaftsunternehmen weitergegeben würden. Die USA hätten wenig Bedarf an High-Tech-Spionage , da "die amerikanische Industrie in vielen Bereichen technologisch weltführend ist".

Allerdings sei das "keine allgemeingültige Wahrheit. Es gibt einige technologische Bereiche, in denen die amerikanische Industrie gegenüber Unternehmen anderer Länder zurück liegt. Doch im Großen und Ganzen haben amerikanische Unternehmen keine Notwendigkeit, ausländische Technologien zu stehlen, um vorne zu bleiben".

Wenn US-Nachrichtendienste allerdings Informationen über technologische Durchbrüche ausländischer Unternehmen zusammenstellen würden, dann glaubt Woolsey, dass diese auch weitergegeben würden.

"Würde [...] man eine technologische Analyse von etwas aus einem befreundetem Land machen, was keine Bedeutung hat, außer von kommerziellem Nutzen zu sein, und das dann in der Schublade liegen lassen, weil es nicht an ein amerikanisches Unternehmen weitergegeben werden kann? Ich glaube, das wäre ein Missbrauch von Ressourcen der Nachrichtendienste. Ich denke nicht, dass man so verfahren würde."

Die meisten Daten amerikanischer Spionage, ob ökonomischer oder militärischer Natur, würden von öffentlichen Quellen stammen. Doch "fünf Prozent sind wirkliche Geheimnisse, die wir stehlen. Wir stehlen Geheimnisse mittels Spionage, mittels Abhörmaßnahmen und mit Aufklärungssatelliten".

Zur Erklärung seiner Ansicht, warum Europa das Zentrum industrieller Bestechung auf der ganzen Welt sei, fragte er: "Warum ... haben wir in der Vergangenheit von Zeit zu Zeit ausländische Unternehmen und die Hilfe, die sie von ihren Regierungen erhalten, zum Ziel gemacht?"

"Einige unserer ältesten Freunde und Alliierten haben eine nationale Kultur und Praxis, die darin besteht, dass Bestechung ein wichtiger Teil der Art und Weise ist, wie sie im internationalen Handel ihre Geschäfte abzuwickeln versuchen. ... Jener Teil der Welt, in dem es üblich ist, Aufträge durch Bestechung zu erhalten, in dem es auch wirklich sehr viel Geld gibt und der aktiv in internationalen Geschäften ist, ist mit hoher Wahrscheinlichkeit Europa".

"[...] Europa steht zuerst im Verdacht, wenn es darum geht, Bestechungsgelder zu bezahlen, um große internationale Aufträge zu erhalten. Und tatsächlich sind es auch einige bestimmte Unternehmen, und Unternehmen in bestimmten Ländern, in denen neulich am meisten Aufregung über angebliche US-amerikanische Wirtschaftsspionage entstanden ist."

Seiner Meinung nach sei das aber keine Wirtschaftsspionage. "Ich reserviere den Begriff Wirtschaftsspionage dafür, wenn einer Industrie direkte Vorteile verschafft werden sollen. Ich nenne es nicht Wirtschaftsspionage, wenn die USA ein europäisches Unternehmen ausspionieren, um herauszufinden, ob es durch Bestechung Aufträge in Asien oder Lateinamerika zu erhalten versucht, die es auf ehrlichem Weg nicht gewinnen würde".

"Einige unserer alten Freunde und Alliierten sind ebenfalls in diesem Geschäft, nicht nur indem sie Mikrophone in die Kopfstützen der Sitze in der Ersten Klasse ihrer Transatlantikflüge installieren, sondern auch auf anderen Wegen. ... Es gibt europäische Länder, wo ... wenn man als Geschäftsmann seinen Aktenkoffer zurücklässt, wenn man zum Abendessen geht, und dieser enthält sensible Informationen, dann sollte man seinen Kopf untersuchen lassen".



"Wir haben darüber schon in der Vergangenheit Spionage betrieben. Auch wenn ich keine unmittelbaren Beweise vorbringen kann, so hoffe ich jedenfalls, dass die US-Regierung fortfährt, über Bestechung zu spionieren."

"Ob das nun gemacht wird oder nicht, es erscheint mir, dass es für jeden verständlich sein sollte, der diesen Bericht an das Europaparlament liest, wer überhaupt darüber nachdenkt, ob amerikanische Unternehmen Bedarf an Diebstahl technologischer Geheimnisse ausländischer Unternehmen haben, und für alle, die ein Verständnis davon haben, wie internationaler Handel und Geschäfte ablaufen, dass Bestechung im Zentrum amerikanischer nachrichtendienstlicher Bedürfnisse bezüglich ausländischer Unternehmen und der Unterstützung durch ihre Regierungen stehet - oder stehen sollte - und das war zu meiner Zeit sicherlich so."

Yankees go home! *by BUFFEN, 22.3.2000*

Erschreckend und unglaublich dreist *by Jürgen Friedrich, 19.3.2000*

RE:Erschreckend und unglaublich dreist *by MW, 02.4.2000*

Natuerlich sind die Amerikaner weltfuehrend! *by ParappaTR, 18.3.2000*

Nicht von der Hand zu weisen, aber .... *by Noppes, 15.3.2000*

ein anderer Name fürs gleiche Kind *by Gärtner Pötschke, 16.3.2000*

Dem ist nichts hinzuzufuegen *by hunsolo, 26.7.2000*

Mal was für unsere Paranoiker ;-) *by Ser Lev Arris, 15.3.2000*

Haeh? *by DeeKay, 22.3.2000*

Was die Amis alles erfunden haben glauben: *by Gärtner Pötschke, 14.3.2000*

Wir sind mitten im Wirtschaftskrieg *by Paranoider, 14.3.2000*

Technologisch führend ?? *by Gogi, 13.3.2000*

Widerstand ist zwecklos! *by Lucky Lui, 19.3.2000*

Schmeißt die scheiss Ammis raus *by Don Bernd, 13.3.2000*

No comment *by Blueboy, 14.3.2000*

sour.....(d[h]<e>...???) *by aurum, 13.3.2000*

top