Information Imperialism : Wissen ist Macht : Wie steht es um den Schutz unseres Wissens?

Autor(en): **Bischof, Jörg A.**

Objekttyp: **Article**

Zeitschrift: **ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift**

Band (Jahr): **171 (2005)**

Heft 12

PDF erstellt am: **29.03.2024**

Persistenter Link: https://doi.org/10.5169/seals-69956

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

INFORMATION IMPERIALISM

Wissen ist Macht[1] – Wie steht es um den Schutz unseres Wissens?

Im vorliegenden Artikel befasst sich der Autor mit der Frage, wie offen unsere Daten in jeglicher Telekommunikation übermittelt werden, und stellt anschaulich dar, welche Systeme verdeckt und weltweit daran arbeiten, Zugang zu diesen Daten zu erhalten, um ihren Betreibern einen Informationsvorsprung zu verschaffen. Wissen ist Macht – Macht ist aber auch Geld wert. Es geht also nicht nur um militärische Macht, sondern auch um wirtschaftliche. Im Schlussteil zeigt der Autor mögliche Schutzmassnahmen auf.

Jörg A. Bischof *

Ausgangslage

Bis in die 80er- und 90er-Jahre des letzten Jahrhunderts lag der Wert eines Unternehmens hauptsächlich im Forschungs-, Entwicklungs-, Produktionswissen, im Potenzial der Infrastruktur und in den verfügbaren Kapazitäten begründet. Informationen wurden vor allem lokal benötigt, gelagert und ausgetauscht. Wenig bis nichts wurde elektronisch übermittelt. Der Austausch von Informationen erfolgte in der Regel per Briefverkehr, später auf postversandten elektronischen Datenträgern allenfalls manuell oder per Analog-Fax oder Telex. Das Telefon wurde nur zur Sprachübertragung eingesetzt und – bedingt durch die hohen Kosten – um das operative Geschäft zu steuern, aber praktisch nie, um Schlüsselwissen zu übermitteln. Telefon- und Videokonferenzen waren seltene Ausnahmen und wurden hauptsächlich zur Steuerung operativer Aufgaben eingesetzt.

Seit der Digitalisierung der Sprache fällt die Unterscheidung in Sprache und Daten weg.[2] Die Informatiklösungen von Unternehmen und Organisationen sind von Beginn weg uneinheitlich gewachsen. Selbst innerhalb von Organisationen sind Verfahrenslandschaften verschieden, das heisst

> Seit der Digitalisierung der Sprache fällt die Unterscheidung in Sprache und Daten weg.

meist unter Anwendung verschiedener Softwaresprachen und Protokollen, insgesamt ohne ein Gesamtkonzept. So verfügten beispielsweise Entwicklungs-, Finanz-, Verkaufsabteilungen derselben Organisation über unkompatible Softwareapplikationen. Komplexe Schnittstellen wurden jedoch rasch notwendig, um bereichsübergreifend arbeiten zu können. Das führte zu Sicherheitslücken, die allmählich erkannt und so gut wie möglich behoben wurden.

Die Entwicklung der letzten zehn Jahre hat dazu geführt, dass der Wert einer Organisation sich heute viel mehr über das elektronisch gespeicherte und schnell verfügbare Wissen definiert. Die meisten Organisationen haben sich aus einem abgeschotteten Inseldasein mit tiefer Wertschöpfungskette in vernetzte Firmengruppen gewandelt, die exorbitante Mengen an Daten national, kontinental und interkontinental austauschen.

Betrachtet man den Informationsfaktor, so ist erkennbar, dass Inhalte und Daten den Grossteil der schützenswerten Information ausmachen *(Abbildung 1)*. Diese Inhalte und Daten werden heute über bestehende Netzwerke ausgetauscht. Aber nur ein kleiner Teil dieser Daten ist zum Beispiel mittels Chiffrierung genügend vor fremdem Zugriff gesichert. Der Absender von Daten weiss nur in den wenigsten Fällen, über welche Übertragungsmedien die Datenübertragung erfolgt. Breitbandige Punkt-Punkt-Leitungen sind zwar verfügbar, aber sehr teuer. Dazu kommt, dass in den wenigsten Fällen die gesamte Leitungslänge überwacht werden kann.

> Inhalte und Daten werden heute über bestehende Netzwerke ausgetauscht. Aber nur ein kleiner Teil dieser Daten ist zum Beispiel mittels Chiffrierung genügend vor fremdem Zugriff gesichert.

Die Entwicklung hin zur Mobilität hat in den letzten Jahren in ungeahnte Dimensionen geführt. Hauptsächlich hat der Mobilfunk für die Sprache im Sinne digitaler Daten eklatant zugenommen und verdrängt je länger je mehr den Festnetzverkehr. Dies ist hinsichtlich der Datensicherheit relevant, weil der Mobilfunk den Übermittlungsinhalt über zwei verschiedene Medien transportiert: zunächst wie ein Funkgerät bis zum nächsten Sende-, Empfangsmasten durch die Luft; vom Masten an werden die Daten per Draht, Glasfaser oder Richtstrahl weiterübermittelt. Mit höheren Bandbreiten, neuen Standards und Technologien wie UMTS und WLAN haben sich die frei abgestrahlten Datenmengen drastisch vervielfacht. Schützenswerte Daten werden nun ausserhalb drahtgebundener Netze durch die Luft zu Basisstationen übertragen, entweder in geschützten oder in ungeschützten Netzwerken.

Die wachsende Anzahl an entscheidrelevanten Informations- und Datenmengen sind für die Empfänger nur noch gezielt und zeitgerecht verfüg- und brauchbar, wenn Führungssysteme verwendet werden. In zivilen Anwendungen werden Führungssysteme mit Hilfe von Softwarelösungen verwendet. Diese Software ist aber im Vergleich zu militärischen Führungssystemen wenig komplex. Sie generieren und integrieren zwar viele Informationen, kennen aber weder komplexe Interpretationshilfen wie Lagebeurteilung und Entscheidungsvorschläge noch verfügen sie zur Führung von Operationen über eine *real-time-world*. Im zivilen Umfeld kommen solche Führungssysteme nur in internen und drahtgebundenen Netzwer-

[1] Sir Francis Bacon (1561–1626), aus: Novum Organum, 1620.

[2] Nachfolgend wird nicht zwischen Daten und Sprache unterschieden.

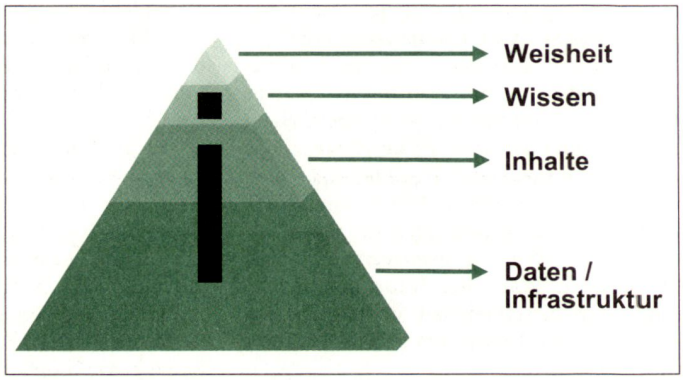


Abbildung 1: Information und ihre Faktoren.

*Jörg A. Bischof, CEO der GOFORIT Management Services, 6300 Zug.

ken zum Einsatz und kennen keine mobilen Elemente. Militärische Führungssysteme, vor allem in multinationalen und/oder interkontinentalen Operationen, verfügen über mobile Elemente und Übertragungsstrecken der verschiedensten Art.

Nebst militärischen Anwendern verfügen vor allem Finanzdienstleister über die nötige Sensibilität und notabene auch über die nötigen Budgets, um ihre Systeme und Netzwerke so wirkungsvoll wie möglich zu schützen.

Nebst militärischen Anwendern verfügen vor allem Finanzdienstleister über die nötige Sensibilität und notabene auch über die nötigen Budgets, um ihre Systeme und Netzwerke so wirkungsvoll wie möglich zu schützen.

Gefährdet sind konkurrierende Industrieunternehmen mit hohem informationsbasiertem *Know-how,* aber geringen Mitteln oder Sensibilität, was die Datensicherheit anbelangt. Dazu kommt, dass sie aus Kostengründen oft Leistungen, die für ihr Kerngeschäft von essenzieller Bedeutung sind, durch organisationsfremde Anbieter erledigen lassen *(outsourcing).* Dabei werden weder die Sicherheit der Übertragungswege noch die Sicherheit des Anbieters entsprechend beachtet. Ausgesprochen gefährdet sind Universitäten und Forschungsinstitute. Sie stehen naturgemäss bezüglich ihrer Forschungsresultate, ihres Wissens, ihrer Kapazitäten oder ihres *Know-how* vor dem Dilemma «Geheimhaltung versus Öffentlichkeit». Zudem haben sie Schwierigkeiten, wenn es um die wirkungsvolle Durchsetzung ihrer Sicherheitsvorschriften geht: Die am Institut Tätigen sind grösstenteils nicht per Arbeitsverträge gebunden, wie in anderen Organisationen, sondern temporär immatrikulierte Studenten oder Angestellte.

Information wird immer mehr auch zur zeitlich beschränkt gültigen und schützenswerten Momentinformation. Es gilt, sie nicht nur umfangmässig zu handhaben, sondern auch bezüglich ihres Wertes zum Schutze zu klassifizieren. Und weil Information zur Momentinformation geworden ist, muss sie häufig lediglich für einen bestimmten Zeitraum klassifiziert werden, das heisst, der Inhalt ist nach kurzer Zeit nicht mehr schützenswert. Aus diesem Grund müssen Aufwand und Ertrag bezüglich eines möglichen Schadens in angemessenem Verhältnis stehen. Der Begriff *end of security* (EoS) definiert den Zeitpunkt, nach dem der Schutzaufwand gemessen am Informationswert unverhältnismässig wird.

Bekannte Bedrohungsformen

Unternehmen und Organisationen sind mittlerweile zumeist gegen das unstrukturierte Vorgehen von so genannten Hackern und Cyberhooligans mehr oder weniger gewappnet. Demgegenüber gehen Cyberterroristen oder staatliche Akteure weit strukturierter vor. Eine ernst zu nehmende Bedrohung (und wenig ernst genommene) stellen so genannte Insider dar. Das können frustrierte und demotivierte Mitarbeiter sein oder solche, die sich in den Sold anderer stellen (Konkurrenz, Spionage). Untersuchungen belegen, dass der Schaden durch Insider wesentlich höher ist als derjenige durch externe Akteure. Die gleichen Untersuchungen zeigen auch, dass in mehr als einem Drittel der Fälle die Verursacher nie ermittelt werden konnten.

Eine ernst zu nehmende Bedrohung (und wenig ernst genommene) stellen so genannte Insider dar. Das können frustrierte und demotivierte Mitarbeiter sein oder solche, die sich in den Sold anderer stellen.

Die andere Bedrohung

Der ehemalige amerikanische Präsident Bill Clinton hat als Erster wiederholt den Begriff *INFORMATION IMPERIALISM* verwendet. Er bezeichnete damit den fehlenden Informationsfluss zwischen den westlichen und den afrikanischen Staaten. Das sei, so Clinton, entscheidender Vorteil der *more developed countries* gegenüber den *lesser developed*. Clinton spielte mit dem Begriff allerdings auch auf die diesbezügliche Überlegenheit der USA an. Wie meinte er das? – Die USA sind der übrigen Welt[3] in vielen Sachen immer einen Schritt voraus. Seit dem Zweiten Weltkrieg sind Innovationen in Forschung und Technik mehrheitlich von den USA ausgegangen. Zu diesen Bereichen gehört auch der Vorsprung in der Informationstechnologie. Der damit implizierte Informationsvorsprung wird beispielsweise dazu genutzt, im Ringen um Grossaufträge, sei es bei der Beschaffung von Rüstungs- oder zivilen Gütern, die Nase vorn zu haben.

Den meisten Ländern der Europäischen Union (EU) und insbesondere deren Zentrale in Brüssel war bis zum Ende der 90er-Jahre des vorigen Jahrzehntes nicht bewusst, um was es ging. Dies obwohl zehn Jahre zuvor, im August 1988, der englische Journalist Duncan Campbell in der Zeitschrift *New Statesman* den Artikel *Somebody's listening*[4] veröffentlichte, der zumindest einige Fragen hätte aufwerfen müssen. Duncan beschrieb in seinem Artikel das Projekt P415: Ein globales elektronisches Überwachungssystem, im Investitionswert von Milliarden von US-Dollar. Weitere Artikel zum Thema folgten zwischen 1988 und 1998. Darin taucht auch erstmals der Begriff ECHELON auf. Die Fragen waren gestellt – wenige Reaktionen folgten.

Duncan beschrieb in seinem Artikel das Projekt P415: Ein globales elektronisches Überwachungssystem, im Investitionswert von Milliarden von US-Dollars. Weitere Artikel zum Thema folgten zwischen 1988 und 1998. Darin taucht auch erstmals der Begriff ECHELON auf.

Anfang 1998 veröffentlichte das Europäische Parlament ein Arbeitspapier des Autors Steve Wright zuhanden des Ausschusses *Scientific Technology Options Assessment* (STOA) unter dem Titel *An Appraisal Of Technologies of Political Control.*[5] Der Autor behauptete darin, dass alle E-Mails, Telefongespräche und Faxübermittlungen in Europa durch den amerikanischen Nachrichtendienst *National Security Agency* (NSA) routinemässig aufgezeichnet würden.[6] Das Arbeitspapier machte in Europa die bisher bloss vermutete Existenz eines umfassenden globalen Abhörsystems, genannt ECHELON, zum breiten Thema.

1998 liess sich der damalige EU-Kommissar Martin Bangemann zu Fragen bezüglich ECHELON verlauten, dass die EU nichts darüber wisse und auch nicht ausreichend Beweise für dessen Existenz vor-

[3] *rest of the world;* ein in den USA geprägter Begriff, der alle Länder ausserhalb der Vereinigten Staaten von Amerika bezeichnet.

[4] http://duncan.gn.apc.org/echelon-de.htm *«They've got it taped»* und http://duncan.gn.apc.org/stoa.htm

[5] http://www.europarl.eu.int/stoa/default_en.htm, http://www.europarl.eu.int/dg4/stoa/en/publi/publi.htm siehe auch: http://www.heise.de/tp/r4/artikel/6/6280/1.html#s1

[6] Kapitel 4.4, *National & International Communications Interceptions Networks*

lägen.[7] 1999 hat dann ausgerechnet ein Amerikaner, der republikanische Kongressabgeordnete Bob Barr, die Sache ins Rollen gebracht und vom Direktor der *Central Intelligence Agency* (CIA), Direktor der NSA und dem Generalstaatsanwalt innerhalb 60 Tagen einen Bericht verlangt. Darin sollte die Frage beantwortet werden, wie die Privatsphäre der amerikanischen Bürger gegenüber dem Projekt ECHELON geschützt werde.

1999 erschien ein zweiter STOA-Bericht: *(...) in order to find out more about this subject, STOA commissioned a five-part study of the 'development of surveillance technology and risk of abuse of economic information'. Part 2/5, by Duncan Campbell, concerned the existing intelligence capacities and particulary the mode of operation ECHELON (...)*

Dieser Bericht hat im Wesentlichen zur Erkenntnis geführt, dass das ursprünglich zur Überwachung der Aktivitäten der ehemaligen Ostblockstaaten konzipierte System ECHELON nun schwergewichtig zur Wirtschaftsspionage diene. Als Beweis wurden einige Grossaufträge angeführt, die Firmen wie Airbus und Thomsen CSF wegen ECHELON an amerikanische Konkurrenzfirmen verloren hätten. Als Resultat des zweiten STOA-Berichtes wurde über ECHELON im Europäischen Parlament debattiert. Frankreich und Belgien verfassten in der Folge eigene Berichte. Im Juli 2000 beschloss das Europäische Parlament, eine temporäre Arbeitsgruppe zum Thema *ECHELON Interception System* zu bilden.

Der Bericht kam zum Schluss *(...) that a global system for intercepting communications exists, operating by means of cooperation proportionate to their capabilities among the USA, the UK, Canada, Australia and New Zealand under the UK-USA agreement, is no longer in doubt.*

Anfang Juli 2001 verabschiedete die Arbeitsgruppe den Entwurf zu ihrem knapp 140 Seiten umfassenden ECHELON-Bericht. Der Bericht kam zum Schluss (...) *that a global system for intercepting communications exists, operating by means of cooperation proportionate to their capabilities among the USA, the UK, Canada, Australia and New Zealand under the UK-USA agreement, is no longer in doubt.* Das Europäische Parlament behandelte den Bericht Mitte Juli 2001.[8]

[7] http://cryptome.org/echelon-fi.htm#leprevost
[8] http://cryptome.org/echelon-ep-fin.htm

Was ist ECHELON?

Heute gilt als gesichert, dass im Jahre 1948, kurz nach Ende des Zweiten Weltkrieges, die Länder USA, Kanada, Grossbritannien, Australien und Neuseeland einen geheimen Vertrag abgeschlossen haben, der der Grundstein für das Projekt ECHELON war. Zweck des Vertrages war es, ein weltumspannendes System von Horchposten aufzubauen, um den gesamten internationalen elektronischen Verkehr und den grössten Teil des lokalen elektronischen Verkehrs in allen Ländern der Welt auszuhorchen. Die wichtigsten heutigen Standorte des Systems sind in Grossbritannien *(Morwenstow/Cornwall, Menwith Hill/Yorkshire)*, in der Bundesrepublik Deutschland *(Bad Aibling)*, in Australien *(Shoal Bay, Geraldton)* und Neuseeland *(Waihopai)*, in Kanada *(Leitrim)*, sowie in den USA *(Yakima Firing Centre/Washington State, Sugar Grove/West Virginia)*.

Zweck des Vertrages war es, ein weltumspannendes System von Horchposten aufzubauen, um den gesamten internationalen elektronischen Verkehr und den grössten Teil des lokalen elektronischen Verkehrs in allen Ländern der Welt auszuhorchen.

Alle diese Basen haben Rechner, die in der Lage sind, Telefongespräche (Mobil und Festnetz), E-Mails und Fax nach Suchbegriffen zu filtern. Die entscheidende Priorisierung der Suchbegriffe erfolgt auf nationaler Ebene. Alle fünf ECHELON-Mitglieder verfügen über eigene Suchwörterbücher. Werden Suchbegriffe durch ECHELON aufgefangen, wird zuerst eine Grobanalyse mit Hilfe einer Software durchgeführt, die Feinfilterung erfolgt danach durch Mitarbeiter. Um länderspezifische gesetzliche Grundlagen zu umgehen, ist es üblich, die Partnerorganisationen anzufragen, die Überwachungen selber durchzuführen. Der EU-Bericht listet Beispiele auf, wie die britische Regierung unter Margaret Thatcher ihr unbequeme englische Politiker durch die NSA und der amerikanische Präsident Ronald Reagan seinerseits unangenehme amerikanische Politiker durch das britische *Government Communication Headquarters* (GCHQ) abhorchen liessen. ECHELON beschäftigte zu dieser Zeit rund 15000 Mitarbeiter mit einem jährlichen Budget von rund 500 Millionen US-Dollar.

Neben den vielen Horchposten in den Äther, die sich in Form riesiger Antennenanlagen rund um den Globus erstrecken,

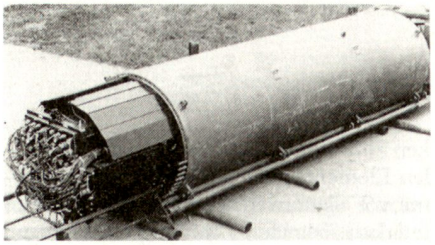


Abb. 2: Unterwasser-Abhorchkanister.

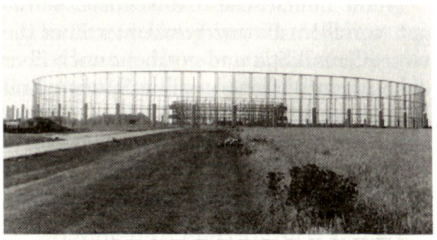


Abbildung 3: Horchposten in den Äther.

hat ECHELON ab 1950 systematisch auch sämtliche Unterwasser-Kommunikationskabel angezapft. Diese geheime Aktivität wurde erst publik, als die Russen in der Barentssee in den 80er- und 90er-Jahren einen Abhorchkanister bargen, der neben einem, unter Wasser verlegten, Telekommunikationskabel auf russischem Hoheitsgebiet lag. Sie stellten das *corpus delicti* kurzerhand in einem Moskauer Museum aus *(Abbildung 2,3)*. Bedingt durch die Länge der unterwasserverlegten Kupferkabel mussten Zwischenverstärker geschaltet werden. In der Umgebung dieser Zwischenverstärker waren die Signale am stärksten und somit der ideale Ort, um die auf induktiver Basis arbeitenden Abhorchkanister zu positionieren. Dies war allerdings nur dann nötig, wenn die Kopfstationen der Unterwasserverbindungen auf beiden Seiten der Ufer nicht direkt angezapft und somit ins ECHELON-System eingebunden werden konnten. Zufällig enden die meisten transatlantisch verlegten Kabel auch heute noch in *Cornwall*/Grossbritannien. Zufällig ist auf der Klippe bei *Sharpnose Point* die Anfang der Siebzigerjahre

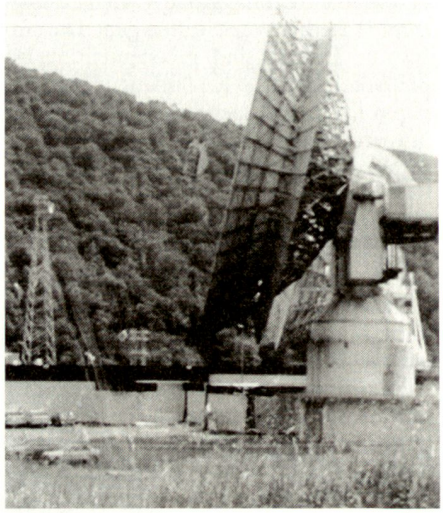


Abbildung 4a: Sharpnose Point, Morwenstow.

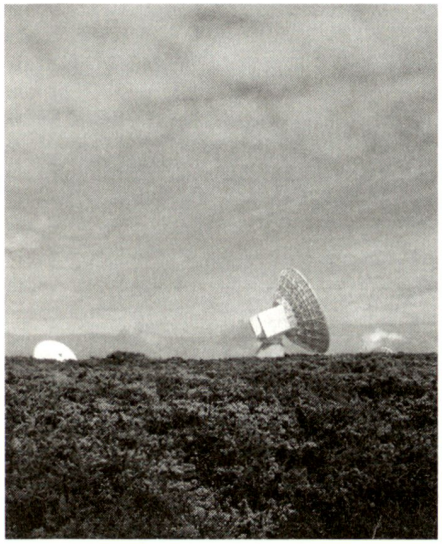


Abbildung 4b: Teilsystem zu ECHELON.

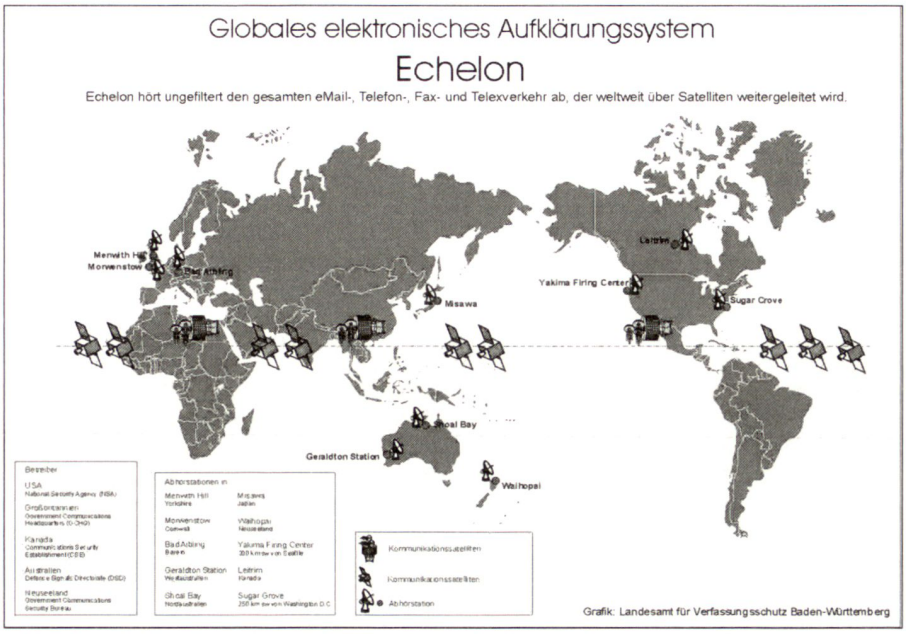


Abbildung 5: Das bekannte ECHELON-Stationierungskonzept.

gebaute und ins ECHELON-System eingebundene Station von *Morwenstow* gelegen *(Abbildung 4)*. Zufällig liegt diese nur 110 km nördlich der *satellite up and down link station* der *British Telecom* in *Goonhilly,* die wiederum für die Satelliten über dem Atlantischen und Indischen Ozean gebaut wurde. Zusätzlich zu *Morwenstow* ist eine zweite Station für die Satelliten über dem Pazifischen Ozean notwendig. Sie befindet sich auf einem Tafelberg in *Yakima Firing Centre,* Bundesstaat Washington, 200 km südlich von *Seattle.*

In den 70er- und 80er-Jahren wurde ein grosser Teil des Fernmeldeverkehrs nicht mehr über die langsamen Unterwasser-Kupferkabel, sondern neu über Satellitenverbindungen geführt. Diese über dem Äquator geostationär positionierten Satelliten der ersten Generation (sog. Intelsat) hatten zwar nur wenige tausend Kanäle, aber lediglich drei Satelliten mit breiter Abstrahlcharakteristik waren notwendig, um die Welt zu umspannen. Anfänglich genügten die zwei Stationen in *Morwenstow* und *Yakima* zur Überwachung des gesamten Intelsat-Verkehrs. ECHELON wurde indes Schritt für Schritt erweitert.[9] Der Ausbau des Intelsat-Netzes von wenigen Satelliten der ersten bis dritten Generation bis zu 20 Satelliten der siebten Generation bis Mitte der Neunzigerjahre führte zum Bau neuer Stationen, die ins ECHELON-Netz eingebunden werden konnten *(Abbildung 6)*. Heute sind 200 Länder über das Intelsat-Satellitennetz erschlossen *(Abbildung 5)*. Intelsat-Satelliten sind aber nur einige von vielen interessanten Zielobjekten. Aufgrund der immer dichteren Erschliessung mit Fernmeldeanschlüssen und der immer grösser werdenden Datenmenge wurden zusätzliche Satelliten für regionale oder landesspezifische Bedürfnisse in Betrieb genommen.[10] Neben den mindestens sechs Stationen, mit denen Intelsat abgehorcht wird, wurden in der Folge mindestens fünf weitere Stationen gebaut, um den regionalen Satellitenverkehr überwachen zu können.

Von der Schweiz aus gesehen ist die nächstgelegene Station des ECHELON-Systems die Feldstation F-81 in Mietraching bei Bad Aibling, zwischen München und Salzburg gelegen.[11] Bad Aibling kam mehrmals in die Schlagzeilen der deutschen Presse. Mehr als 1000 amerikanische Staatsangehörige arbeiten dort, ohne dass die Bundesrepublik selber Zutritt zu den Anlagen hätte. Letztes Jahr hätte diese Station für den ECHELON-Betrieb geschlossen und nach Griesheim bei Darmstadt verlegt werden sollen. Auf dem ehemaligen August-Euler-Flughafen stehen seit 2004 mindestens fünf neue so genannte Radarkuppeln (sog. Radome) mit Antennen. Ob die Verlegung wirklich vollzogen worden ist, weiss man allerdings nicht.

Das wirtschaftliche Gipfeltreffen des *World Economic Forum* (WEF) hat nach einer kurzzeitigen Verlegung nach New York im Jahre 2002 umgehend wieder im Talkessel von Davos in den Bündner Bergen stattgefunden. Obwohl nahe bei Bad Aibling gelegen, bedingt es technisch einen wesentlich höheren Aufwand, die lokal geführten Gespräche abhorchen zu können, als in New York.

In einsehbaren Geländen werden Radome nicht nur zum Schutz der Antennen vor Umwelteinflüssen eingesetzt, sondern hauptsächlich, um Bauart und Ausrichtung der Antenne verdeckt halten zu können. Seit im Internet Satellitenaufnahmen auch von ECHELON-Abhorchstationen einsehbar sind, hat die Verwendung von Radomen stark zugenommen.

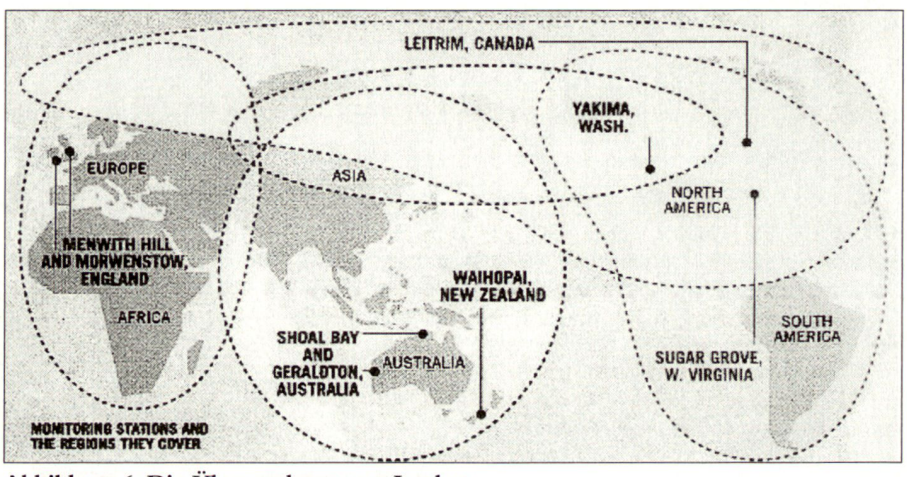


Abbildung 6: Die Überwachung von Intelsat.

[9] http://www.fas.org/irp/eprint/sp/sp_c2.htm

[10] http://de.wikipedia.org/wiki/Echelon. In Europa zum Beispiel Eutelsat oder für Italien Italsat.

[11] http://kai.iks-jena.de/miniwahr/badaibling.html

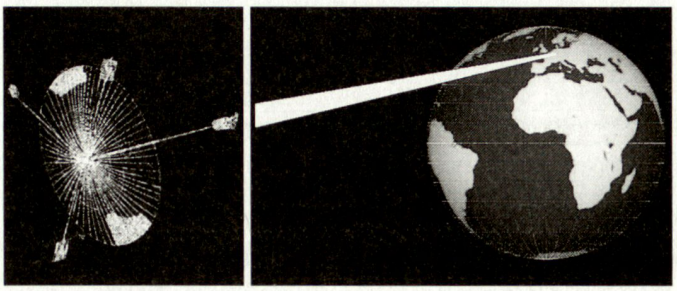


Abbildung 7: Vortex-Satellit.

Eine weitere Ebene im ECHELON-System sind Spionagesatelliten. Da inzwischen weltweit mehr als 1000 für Kommunikationssatelliten um die Erde kreisen, musste ECHELON nebst terrestrischen Abhörstationen auch Satelliten einsetzen. Diese horchen sowohl die Kommunikation per Satellit direkt im Weltall ab als auch diejenige auf der Erde aus dem Weltall.

Die mit dem Codenamen versehenen Orion- und Vortex-Satelliten werden von der amerikanischen Firma TRW konstruiert. Sie dienen der *telecom surveillance* und sind auf einer mittleren Höhe von 35700 Kilometer über der Erde positioniert *(Abbildung 7)*. Mit der sich ausbreitenden Verwendung des Mobilfunks wurden Satelliten mit dem Codenamen *Trumpet* der Herstellerfirma Boeing im Weltraum stationiert. Diese Satelliten haben eine Einsatzhöhe von 320 bis 35700 Kilometer.

Das Internet bedingte eine weitere ECHELON-Ebene. Die meisten Internetknoten stehen vor allem in den USA auf dem Gelände der Armee und können somit einfach «angezapft» und direkt dem ECHOLON-System zugeführt werden. Experten gingen vor dem 11. September 2001 davon aus, dass über 90% des gesamten Internetverkehrs durch ECHELON überwacht wird. Nach der Terrorattacke sind es nahezu 100%. Dabei hat diese Überwachung auch seine nützlichen Seiten, wie beispielsweise erfolgreiche internationale Operationen gegen die Kinderpornografie zeigen. Sie stützten sich auf US-Daten ab. Oder: Dass zur Ausführung der Terrorattacke in New York für Mobiltelefone Schweizer Prepaid-Karten verwendet wurden und Al-Kaida-Anführer Khalid Sheikh Mohammed deswegen verhaftet wurde, ist bekannt.[12] Weniger bekannt ist, dass die nachträgliche Eingabe der entsprechenden Suchbegriffe ins ECHELON-System diesen Fahndungserfolg ermöglicht hat.

Experten gingen vor dem 11. September 2001 davon aus, dass über 90 % des gesamten Internetverkehrs durch ECHELON überwacht wird. Nach der Terrorattacke sind es nahezu 100 %.

Das zunehmende Bedürfnis an grösserer Bandbreite führte dazu, dass neben Satelliten auch neue Übertragungsmedien gefunden werden mussten. Die Glasfasertechnologie setzte sich durch. Diese Technologie hat eine hohe Abhörsicherheit, da die Leitungen nicht abstrahlen und nicht einfach «angezapft» werden können. Die Kabel verfügen über optische Verstärker. Das heisst, leistungsfähigere Unterwasserkabel kommen wieder zum Zuge. In den letzten 20 Jahren wurden zahlreiche Glasfaserkabel unter Wasser verlegt oder sind noch im Bau.[13] Schon 1998 erreichte man damit eine transatlantische Datenrate von 26 Gbit pro Sekunde; heute ist es bereits ein Vielfaches. Alle diese Kabel enden an Kopfstationen in den USA, wo der Verkehr durch ECHELON überwacht werden kann. Es ist daher von strategischem Interesse der ECHELON-Partner, Kopfstationen kontrollieren zu können, um mit verhältnismässig geringem Aufwand an Daten zu gelangen, die ins ECHELON-System eingespiesen werden können.

Die Betreiber von ECHELON

Der wichtigste und grösste Betreiber des ECHELON-Systems ist die amerikanische *National Security Agency* (NSA). 1999 beschäftigte sie mehr als 40000 Mitarbeiter. Man vermutet, dass mit den zusätzlichen Aufgaben nach dem 11. September 2001 noch wesentlich mehr Mitarbeiter dazugekommen sind. Über 35000 Personen arbeiten am Hauptsitz in *Fort Meade/ Maryland,* 16 km nördlich von *Washington (Abbildung 8)*. Auf dem Gelände gibt es 1670 Gebäude und 150 km Strassen. Die Gebäude sind aufwändig abgeschirmt, um elektromagnetische Abstrahlung zu vermeiden. 30000 Tonnen an geheimen Akten wurden jährlich von NSA-Kurieren zwischen *Fort Meade* und *Washington* hin und her transportiert. Heute scheint ein stark abgeschirmtes Intranet benützt zu werden, das von 35 Geheimdiensten mit Information versorgt wird und 3000 Nutzer umfassen soll. Es gibt für die Angestellten eine eigene Autobahnausfahrt, und Fotos zeigen rund 18000 Parkplätze. Damit ist die NSA die weltweit grösste nachrichtendienstliche Organisation. Gemäss der NSA-Webseite beläuft sich das Budget für die Elektrizität am Hauptsitz auf 21 Millionen US-$ pro Jahr. Alle übrigen Verbraucher eingerechnet und vorsichtig geschätzt, ergibt das eine Rechenleistung der dort eingesetzten Computer von rund 160000 GFLOPS[14], also 16x10 hoch 13 Operationen pro Sekunde. Die NSA ist der weltweit grösste Arbeitgeber für Mathematiker (rund 16000) und der grösste Abnehmer für Hochleistungsrechner. Man darf annehmen, dass die NSA bezüglich Verschlüsselung allen übrigen auf der Welt um Jahre voraus ist. Gemäss der *Free Congress Research & Education Foundation* in Washington kann die NSA Verschlüsselungen bis zur Menge von gegen 1000 Bit entschlüsseln.

[12] www.guardian.co.uk *«How mobile phones and an 18£ bribe trapped 9/11 mastermind»*

[13] http://www.ita.hsr.ch/vorlesungen/computernetze/Transatlantiklink.pdf

[14] http://de.wikipedia.org/wiki/NSA



Abbildung 8: Das National Security Agency (NSA)-Hauptquartier Fort Meade, Maryland, USA.

Es ist auch kein Geheimnis, dass Nachrichtendienste bevorzugt Mieter in gleichen Gebäuden wie Telecom-Gesellschaften sind. Die NSA hatte jahrelang über der deutschen Hauptpost in Frankfurt residiert. Nach einigem Verwirrspiel gab sich der Bundesnachrichtendienst (BND) als offizieller Mieter der Räume zu erkennen, die Besucher waren jedoch mehrheitlich Amerikaner.[15]

Es ist auch kein Geheimnis, dass Nachrichtendienste bevorzugt Mieter in gleichen Gebäuden wie Telecom-Gesellschaften sind.

Das letzte veröffentlichte Budget für die US-Geheimdienstaktivitäten im Jahre 1998 wies 26,7 Milliarden US-Dollar aus. Ein Gerichtsbeschluss ordnete 1999 an, dass eine weitere Offenlegung der Budgets die nationale Sicherheit nachhaltig beeinträchtigen könnte. Seit der Terrorattacke vom 11. September 2001 – so darf angenommen werden – wurden diese Budgets massiv aufgestockt.

Weitere Betreiber des ECHELON-Systems sind:
– *Government Communication Headquarters* (GCHQ) in Grossbritannien[16]
– *Communication Security Establishment* (CSE) in Kanada[17]
– *Defence Signal Directorate* (DSD) in Australien[18]
– *Government Communications Security Bureau* (GCSB) in Neuseeland[19]

Systeme vergleichbar ECHELON

Man kann davon ausgehen, dass auch andere Länder über Systeme verfügen, um an Daten zu gelangen und sie auszuwerten. Man kann aber annehmen, dass keines dieser Systeme auch nur annähernd die Grössenordnung und Effizienz wie ECHELON hat. Das hat erstens mit den fehlenden finanziellen Mitteln und zweitens mit der Verfügbarkeit von genügend Rechenleistung zu tun.

Frankreich hat beispielsweise dank seinen ehemaligen Kolonien selbst eine weltumspannende Länderbasis für ein solches

Man kann davon ausgehen, dass auch andere Länder über Systeme verfügen, um an Daten zu gelangen und sie auszuwerten. Man kann aber annehmen, dass keines dieser Systeme auch nur annähernd die Grössenordnung und Effizienz wie ECHELON hat.

System. ECHELON ist offensichtlich für Frankreich kein Thema, in den Europäischen Kommissionen beispielsweise wurde ECHELON nie durch französische Vertreter thematisiert. Das Land hat eigene Satelliten und Trägerraketen sowie eine eigene Industrie zur Entwicklung und Herstellung der Infrastruktur. Der französische Nachrichtendienst *General Directorate for External Security* (DGSE), im Verteidigungsdepartement angesiedelt, ist u. a. zuständig für die strategische Informationsgewinnung *(electronic intelligence, counter intelligence)* ausserhalb des französischen Territoriums.[20] Antennenstationen sind in den meisten französischen Interessensgebieten dokumentiert, ihr genauer Zweck aber nicht bekannt.

Wie können wir uns schützen?

Oberster Grundsatz aller Benutzer im Umgang mit elektronischen Mitteln und Möglichkeiten muss die Aufmerksamkeit *(awareness)* gegenüber der täglich realen Bedrohung und gegenüber trügerischer Sicherheit sein. Ein Unterschied besteht

Oberster Grundsatz aller Benutzer im Umgang mit elektronischen Mitteln und Möglichkeiten muss die Aufmerksamkeit *(awareness)* gegenüber der täglich realen Bedrohung und gegenüber trügerischer Sicherheit sein.

zwischen dem militärischen und dem zivilen Umfeld. Zwar verfügt die Schweiz über eine ausgezeichnete Sicherheit in den militärischen Netzen. Das grösste Risiko stellt allerdings der (immer noch) geduldete Gebrauch von Mobiltelefonen in militärischer wie ziviler Umgebung dar.

Bei der Zusammenarbeit zwischen Armee und zivilen Behörden im Bereich der öffentlichen Sicherheit gibt es zudem bedenkliche Lücken. Das liegt begründet in der föderalistischen Struktur mit den 26 kantonalen Hoheiten und – fast ist man versucht zu sagen – mit 26 Lösungen. Die Sicherheitslücke rührt daher, weil es der Bund nicht schafft, das flächendeckende Sicherheitsnetz POLYCOM zu betreiben und im Sinne eines *back bone* die bestehenden kantonalen Polycom-Inseln und das Polycom-Netz der Grenzschutzorganisationen in einem einzigen Netz zu integrieren. Es bleibt zu hoffen, dass die erkannte Lücke mit Blick auf das sportliche Grossereignis UEFA EURO 2008 geschlossen werden kann.

Im zivilen Umfeld geht es in erster Linie um Industriespionage. Der EU-Bericht zu ECHELON dokumentiert einige Fälle. Beispielsweise installierte der französische Geheimdienst in den Flugzeugen der Air France in den Erstklasssitzen Mikrofone, um die Unterhaltungen der reisenden Geschäftsleute aufzuzeichnen. Dies wurde bis 1994 praktiziert, danach entschuldigte sich die Fluggesellschaft öffentlich. Der Fall des Volkswagen-Managers José I. Lòpez ist ein weiterer. Seine Videokonferenzen wurden von der NSA mitgeschnitten und der Firma *General Motors* zugespielt.

Letztlich geht es in allen Fällen um Informationssicherheit. Nachdem bewiesen ist, dass unser Wissen systematisch abgehört, gefiltert und ausgewertet wird, muss man sich einige Fragen stellen. Was bedeutet dies für unsere Behörden, Organisationen, Unternehmen und für mich als Privatperson? Wie werden wir als Bürger, Unternehmen, Mitglied oder Mitarbeiter informiert, sensibilisiert und ausgebildet, um sicherzustellen, dass das schützenswerte Wissen auch wirklich geschützt wird? Und vor allem stellt sich die Frage, wessen Aufgabe ist es zu informieren, zu sensibilisieren und auszubilden? Dies erfordert eine Analyse der Bedrohung, des Risikos und der Schwachstellen. Das muss zu Sicherheitsvorkehrungen führen, die aus infrastrukturellen, organisatorischen, technischen und personellen Massnahmen bestehen. Sie dienen dem Ziel, Vertraulichkeit, Integrität, Verlässlichkeit und Verfügbarkeit der Information wahren zu können. Der übergeordnete Rahmen dieser Vorkehrungen bildet die *security policy* einer Organisation. Die Mitarbeiter müssen nach den Richtlinien dieser *security policy* ausgebildet werden, und deren Umsetzung muss kontrolliert, nötigenfalls auch durchgesetzt, werden. Das hat letztlich mit Führung zu tun und nicht mit blossem Einsatz weiterer Technik. Ein Experte hat dies wie folgt formuliert:

If you* think *that technology can solve your security problem, then you don't understand the problem and you don't understand the technology. ●

[15] http://www.heise.de/ct/98/05/082
[16] http://www.fas.org/irp/world/uk/gchq/
[17] http://www.cse-cst.gc.ca/en/home/peer_organization-e.html
[18] http://www.dsd.gov.au/
[19] http:// www.govt.nz
[20] http://www.fas.org/irp/world/france/defense/dgse/