Sendedatum Sender Freies Berlin: Juni 2000
Autorin: Gabi Wuttke

Vor fast 20 Jahren veröffentlichte der Amerikaner James Bamford seine jahrelangen Recherchen über ein globales Abhörsystem. Der Name des Programms: ECHELON. Schirmherr: der US-Geheimdienst 'National Security Agency', NSA.
Unterstützung fand der Amerikaner für seine aufsehenerregenden und gleichzeitig mißtrauisch beäugten Nachforschungen in Neuseeland und Großbritannien. Was bis heute über diesen weltweit operierenden fernmelde-technischen Datenstaubsauger herausgefunden wurde, mündete 1999 in einen Bericht, den das Komitee für bürgerliche Freiheiten und Innere Angelegenheiten des Europäischen Parlaments in Auftrag gegeben hatte. Fünf Länder (unter der Führung der Vereinigten Staaten außerdem: Großbritannien, Kanada, Neuseeland und Australien) schlossen im Kalten-Kriegs-Jahr 1948 das sogenannte UK-USA-Abkommen. Jahrzehntelang waren die Lauscher von ECHELON großräumig vor allem auf den Ostblock gerichtet. Doch mit dem Fall des Eisernen Vorhangs hörte ECHELON keineswegs auf zu arbeiten:
Das ist das Resümee der Experten der vom Komitee beauftragen STOA (einer Organisation für wissenschaftliche und technologische Belange im Europäischen Parlament). In dem Bericht wurde nicht nur die Entwicklung von Informations-Technologien unter die Lupe genommen, sondern auch der Mißbrauch, den besonders ECHELON heutzutage ermöglicht.
Denn anders als viele Spionage-Systeme, die während des Kalten Krieges aufgebaut wurden -so die Untersuchung -, war ECHELON nie vorrangig auf militärische Ziele ausgerichtet, sondern auf das Abhören von Regierungen, Hilfs- und Menschenrechtsorganisationen. Inzwischen soll ECHELON zwar auch helfen, Terroristen, Geldwäschern, Drogenhändlern und Organisierten Kriminellen auf die Spur zu kommen. Doch ein Drittel, möglicherweise sogar die Hälfte, der abgeschöpften Informationen dienen nun der Wirtschaftsspionage; belauscht werden Unternehmen (in fast allen) Ländern.

Ein Beispiel aus dem STOA-Bericht:
Im Januar 1994 flog der französische Premierminister Edouard Balladur nach Riad, um europäische Airbusse an die Saudis zu verkaufen. Wider Erwarten ging der Auftrag aber an den Rivalen: das amerikanische Unternehmen McDonnell-

Douglas. Die Franzosen vermuteten, daß ihr Angebot dank ECHELON von den Amerikanern unterboten werden konnte.

Wie immer, wenn es um dieses Abhörsystem geht, dementieren die amerikanischen Geheimdienste - so auch in diesem Fall. In der Studie werden zwar keine konkreten Zahlen genannt, aber Schätzungen gehen davon aus, daß weltweit täglich bis zu 50 Millionen Nachrichten von ECHELON registriert werden. Jährliche Kosten: 27 Milliarden Dollar.

Wie funktioniert das globale Abhör-Netz? Horchstationen von Waihopia in Neuseeland bis Menwith Hill in Großbritannien fangen rund um die Uhr Nachrichten über unterschiedliche Kanäle auf. Was in den ersten Jahrzehnten von Menschen akribisch seziert werden mußte, haben inzwischen Computer übernommen. Die durchforsten im Informations-Zeitalter die täglich zunehmenden Massen von schriftlichen Nachrichten, die per Fax, Telex oder e-mail über Telekommunikations-Satelliten rund um den Erdball geschickt werden: nach Schlüsselwörtern, Namen, Orten, Stimmen und ganzen Themenkomplexen. Was für den Seniorpartner USA interessant sein könnte, wird an das NSA-Hauptquartier Fort Meade in Maryland weitergeleitet.
Einer der europäischen Horchposten wurde im bayerischen Alpenvorland lokalisiert: Der amerikanische Aufklärungs-Stützpunkt in Bad Aibling.
Der große Verbündete hört also auch seinen kleinen Bündnispartner Deutschland, vor allem dessen Wirtschafts-Unternehmen ab? Und das auch noch im eigenen Land?
Landes-Datenschutzbeauftragten und mittelständischen Betrieben stehen bei diesem Thema längst die Haare zu Berge. Alfred Büllesbach, der Datenschutzbeauftragte des deutsch-amerikanischen Groß-Konzerns Daimler-Chrysler bringt auf den Punkt, worum andere immer noch wie um den bekannten heißen Brei herumreden:

"Zunächst muß man sagen, daß Wirtschaftsspionage in der modernen Welt - glaub ich - zum Alltag geworden ist. Ich erinnere an ein Zitat, daß Henry Kissinger einmal formuliert hat, als er sagte: Mit der Beseitigung des Kalten Krieges sind nicht nur Mauern gefallen, sondern es sind neue Wirtschafts - wie er es nannte- Wirtschaftskriege zu erwarten. Weil sich große, bisher befreundete Macht- und Wirtschaftsblöcke plötzlich im Wettbewerb befinden und deshalb ein großes Interesse daran haben auch gegenseitig zu entdecken und zu erkennen, was denn gegenseitig wirtschaftlich, in der Entwicklung, in der Forschung und in den Marktstrategien gemacht wird.. Deshalb ist natürlich Wirtschaftsspionage ein breites Feld. Und ich denke, wenn man heute sozusagen sich in den wirtschaftlichen Bedingungen die Thematik ansieht, und wenn man sieht, wie der internationale Wettbewerb härter wird, dann ist sonnenklar, daß

das Thema zum zentralen Wettbewerbsbestandteil der Unternehmen geworden ist. Und es gibt durchaus auch Staaten - der Eindruck verstärkt sich - die sozusagen in ihren Abteilungen solche private Wirtschaftsspionage-Möglichkeiten aus Sicht deren jeweiliger Nachrichtendienste mit unterstützen."

"Humbug" nannte der Geheimdienstkoordinator der rot-grünen Bundesregierung, Ernst Uhrlau, solche Einschätzungen noch im August 1999. Wobei er allerdings eine kleine, aber feine Unterscheidung traf: Er trennte "unlautere" Wirtschaftsspionage von:

"....staatlichen Versuchen, Informationen über die Technologiepolitik eines anderen Staates zu sammeln"

...und brachte in einem Zeitungs-Interview dabei das Gespräch selbst auf den deutschen Bundesnachrichtendienst:

"Uns interessieren bestimmte Kontakte von und zu deutschen Firmen, nicht zuletzt um zu verhindern, daß Firmen unwissend in illegale Proliferation hineingeraten. Keine dabei gewonnene Information würde der BND an Konkurrenten weitergeben."

Auch der Bundesnachrichtendienst verfolgt hier also aktiv seine Interessen, die er als Schutzmaßnahmen deklariert. Erich Schmidt-Eenboom, Leiter des Weilheimer Instituts für Friedenspolitik und Geheimdienst-Experte schätzt den Grund für die Unterscheidung des Geheimdienstkoordinators allerdings ganz anders ein:

„ ...um im Einzelfall, wenn man erwischt wird, auch sich zu entschuldigen, zu sagen: das gehört zum generellen Auftrag eines Nachrichtendienstes auch über wirtschaftliche makroökonomische Daten Informationen zu gewinnen; aber konkret hört der Bundesnachrichtendienst natürlich nicht nur offizielle Organe, Ministerien oder Behörden ab, sondern er geht auch in die Telekommunikation ausländischer Großkonzerne: und da treibt er dann direkte Wirtschaftsspionage."

Was aber geschieht mit den Informationen, die der BND bei seiner eigenen Aufklärungsarbeit im Dienste Deutschlands im Ausland abschöpft? Duncan Campbell, einer der Pioniere bei der Enttarnung von ECHELON, der auch für den STOA-Bericht recherchierte, der vor wenigen Tagen im Europäischen Parlament vorgestellt wurde, sagte in einem Interview:

„Soviel ich weiß, gibt es nirgendwo die Möglichkeit für Groß-Unternehmen, direkt nach bestimmten Informationen zu fragen oder eine Art Geheimdienst-Abonnement zu bekommen. In der Regel werden die Wirtschaftsministerien der jeweiligen Länder über relevante Erkenntnisse informiert und können dann von Fall zu Fall entscheiden, ob sie diese weiterleiten wollen."

Die Debatte um Lausch-Angriffe aller Art ist auch in Deutschland facettenreich: Sie hat sich vor dem Hintergrund der wachsenden Digitalisierung der Kommunikation, also dem weltweiten Aufbruch ins Internet, verschärft.
Wie weit darf die Kontrolle des Staates über seine Bürger reichen? Andererseits: Wo muß der Staat sich selbst und seine Interessen schützen? Ist die Wirtschaft ein schützenswertes nationales Gut? Und welche Rolle spielen dabei die Nachrichtendienste? Fragen, die auch der STOA-Bericht für das Europäische Parlament aufgeworfen hat.
Besonderes Augenmerk legten die Experten dabei auf den Daten-Austausch, der für global operierende Unternehmen zwingend ist. Sich an diesen Informationen, wenn sie ungeschützt (also im Klartext) übermittelt werden zu vergreifen, ist ziemlich einfach. Schwieriger wird es, wenn die Informationen mit digitalen 'Echtheitszertifikaten' versehen und überdies mit speziellen Programmen verschlüsselt sind.
Die NSA und ihre ausführenden ECHELON-Schlapphüte werben auf ihrer Homepage mit dem markanten Satz, sie seien die Nummer 1 im Code-Erstellen und im Code-Knacken.
Darüberhinaus schmücken sie sich mit einem Ausspruch ihres obersten Dienstherren Bill Clinton: Die Leistungen der US-Nachrichtendienste seien integraler Bestandteil nationaler Sicherheitsstrategien. In Deutschland dagegen schieden sich genau am Punkt 'nationale Sicherheit' über viele Jahre die Geister: Der frühere Innenminister Manfred Kanther war ein standhafter Gegner der freien Verschlüsselung von Daten-Informationen durch sogenannte 'kryptographische Programme': Wenn immer weniger Daten offenlägen, wie sollte der große Lauschangriff dann funktionieren? Wie der Bundes-Nachrichten-Dienst seine Arbeit tun?
Eine ungewöhnliche Allianz, zu der der damalige Wirtschaftsminister Günter Rexrodt ebenso gehörte wie der Bundesverband der Deutschen Banken, die Stiftung Warentest und der Chaos Computer Club, stellten die Gegenfrage: Wie anders als mit starken Verschlüsselungs-Programmen sollten Firmen und Bürger sich vor Datenmißbrauch und Wirtschaftsspionage schützen?
Auch Kanthers Nachfolger, der Sozialdemokrat Otto Schily mußte zum expliziten Schutz globaler Kommunikation überredet werden: Nach langem Hin und Her verabschiedete das Bundeskabinett im Juni 1999 ein Eckwerte-Papier zur deutschen Kryptopolitik. Darin wird - wenn auch nur indirekt - die Notwendigkeit zum Schutz deutscher Unternehmen vor Wirtschaftsspionage

anerkannt. Zentrales Anliegen der Kabinettsentscheidung ist der verbesserte Schutz deutscher Nutzer in den weltweiten Informationsnetzen durch Einsatz sicherer kryptographischer Verfahren.
Experten schätzen die Schäden durch das illegale Ausspähen, Manipulieren oder Zerstören von Daten jährlich auf Milliardenbeträge. Datensicherheit ist also ein ernstzunehmender Faktor im globalen Wettbewerb und tangiert damit auch Arbeitsplätze der betroffenen Unternehmen und Wirtschaftsbereiche. Ein weiteres wichtiges Ziel besteht in der Stärkung der internationalen Wettbewerbsfähigkeit deutscher Kryptohersteller.

Doch mit dem Beschluß der rot-grünen Regierung hat sich das Problem elektronischer Wirtschaftsspionage in der Bundesrepublik nicht erledigt. Diese Technologie hat nämlich einen kleinen Schönheitsfehler: Wo es Schlüssel gibt, können Schlüssel auch hinterlegt oder nachgemacht werden. Außerdem sind Schlösser für Bartschlüssel leichter zu knacken als Sicherheitsschlösser. Dieses alte Prinzip gilt auch im digitalen Zeitalter.
Diesen 'Schönheitsfehler' versucht die US-Regierung sich zunutze zu machen. Sie hat vehement an die Tür der Europäischen Union gepocht und gefordert, sich auf eine einzige, einheitliche Verschlüsselungsmethode festzulegen oder zumindest die entsprechenden Nachschlüssel bei ihr zu hinterlegen. Sich auf ein gemeinsames Programm zu einigen, vereinfacht vielleicht die gemeinsame Strafverfolgung. Aber ein einziger Nachschlüssel - das liegt nahe - würde den amerikanischen Geheimdiensten auch erheblich die Arbeit erleichtern, wenn es ums Ausschnüffeln dessen geht, was der STOA-Bericht als maßgeblichen Arbeitsauftrag von ECHELON beschreibt: Das Abhören fremder Regierungen und ausländischer Unternehmen. Genau deshalb, so Geheimdienst-Experte Erich Schmidt-Eenboom, ist die Vielfalt der Verschlüsselungsprogramme so wichtig:

„Die NSA ist natürlich von ihrem technologischen Standard her in der Lage, in diesem Wettlauf zwischen Verschlüsselern und Entschlüsselern im Entschlüsseln immer fast jeden Code zu knacken. Auf der anderen Seite gibt es Fortschritte in der Kryptologie, die heißen: wenn jeder mit verschiedenen Methoden möglichst sicher verschlüsselt, dann scheitert das Entschlüsseln nicht im Einzelfall, aber in der Summe an den Kapazitätsgrenzen. Das heißt: Die NSA könnte zwar in einem gewichtigen Einzelfall einen Schlüssel durch massiven Rechnereinsatz knacken, aber wenn es eine Vielzahl von geschützten Schlüsselsystemen gibt, ist selbst die NSA überfordert, alles, was man jetzt so aus dem Äther raussaugen kann, zu knacken."

Ulrich Sandl, Regierungsdirektor in der Abteilung 'Technologie- und Informationspolitik" im Bundeswirtschaftsministerium, hat den Entwurf zur deutschen Kryptopolitik maßgeblich erarbeitet. Sandls Antwort auf die Frage,

warum der Kabinettsbeschluß eine verbesserte technische Ausstattung der deutschen Strafverfolgungs- und Sicherheitsbehörden vorsieht, macht deutlich: Die Bedenken gegen Verschlüsselungsprogramme im Bundesinnenministerium sind - über den Regierungs-Wechsel hinweg - geblieben. Und erinnern zudem an die Forderung der US-Regierung gegenüber Europa:

„Es hat sich auch erwiesen, daß das, was ursprünglich das Bundesinnenministerium gefordert hat, nämlich die Schlüsselhinterlegung, die Einrichtung einer Sollbruchstelle, der schlechteste Weg ist, um auch den Strafverfolgungsinteressen zu helfen. Also von daher: Es wird einen Bericht geben, innerhalb der nächsten zwei Jahre von den zuständigen Behörden, und in diesem Bericht werden wir uns mit der Thematik, nämlich Auswirkung der Nutzung von Verschlüsselungstechniken auf die Strafverfolgungsbehörden dann auseinandersetzen - und auch entsprechende Schlußfolgerungen ziehen."

Das Bundesinnenministerium selbst fordert also Nachschlüssel für kryptographische Programme?
Der Blick in die USA zeigt die Dimensionen staatlicher Zugriffsmöglichkeiten, denn dort sind die Gesetze noch immer besonders rigide: Um eine Verschlüsselungsmethode überhaupt verkaufen (also auch exportieren) zu dürfen, brauchen die Hersteller die Zustimmung der amerikanischen Regierung. Das gilt für relativ einfach zu entschlüsselnde Massenprodukte ebenso wie für hochgradig komplizierte, deren potentielle Käufer vor allem ausländische Regierungen und große Unternehmen sind. Besonders bei solchen Programmen ist der Krypto-Hersteller sogar verpflichtet, wichtige Zugangs-Informationen bei der amerikanischen Regierung zu deponieren. Eine weitere Vereinfachung für die Arbeit der Geheimdienstler.
Und in der Bundesrepublik? Erich Schmidt-Eenbooms Erfahrungen:

„Wir kennen aus dem Bereich der Kryptohersteller sehr viele Einflußversuche des BND. Und wenn da Exportgenehmigungen erteilt worden sind, dann in der Regel dann, wenn sich diese Kryptohersteller verpflichtet hatten, dem Bundesnachrichtendienst ihre Nachschlüssel, Zugang zu den Systemen, mindestens für den Einzelfall einzuräumen.
Und wer sich einigermaßen im nachrichtendienstlichen Metier auskennt, weiß natürlich, daß der Bundesnachrichtendienst keine sehr dichte nachrichtendienstliche Behörde ist, daß man an solche Nachschlüssel nachrichtendienstlich auch rankommen kann und das damit wieder ein paar mehr Mithörer als geplant im Äther sind."

Kontrolle einerseits. Schutz andererseits. Ulrich Sandl vom Bundeswirtschaftsministerium propagiert zwar die Weiterentwicklung sicherer

Verschlüsselungs-Produkte für alle. Er weiß aber auch, was international für Gepflogenheiten gelten:

„Es kommt immer darauf an, welche Werte auf dem Spiel stehen. Also Sie müssen immer davon ausgehen, daß es hier um einen Grenznutzen geht. Und wenn große Werte auf dem Spiel stehen, dann wird auch der Aufwand größer sein, der betrieben wird, um Zugriff auf den Klartext zu bekommen auf welche Weise auch immer."

Viel stand offensichtlich auch auf dem Spiel, als im November 1999 überraschend folgende Nachricht die Runde machte: Die Bundesrepublik werde von Bad Aibling aus nicht mehr ausgehorcht.
Wie das? Die NSA selbst hatte sich immer in Schweigen gehüllt - nur ab und an sickerte etwas über ECHELON durch. Und auch in der Bundesrepublik wollte kein Politiker laut eingestehen, daß von Bad Aibling aus die Lauscher der Vereinigten Staaten auch direkt in die bundesdeutschen Wohnzimmer und Konstruktions-Büros gehalten wurden.
Nun hieß es plötzlich, Washington hätte der deutschen Bundesregierung die Garantie gegeben, die NSA werde von Oberbayern aus weder deren Bürger noch Unternehmen kontrollieren. Womit für Geheimdienstkoordinator Ernst Uhrlau "die in der Öffentlichkeit entstandene Geheimniskrämerei um Bad Aibling angemessen und eindeutig beendet" sein soll. Was ist denn nun 'Humbug'? Erich Schmidt-Eenboom:

„Ich war eine Woche nach dieser Erklärung von Herrn Uhrlau in Amsterdam zu einer internationalen Konferenz über fernmeldeelektronische Aufklärung, und habe die Stellungnahme von Herrn Uhrlau mit amerikanischen Experten wie James Bamford und Mattew Aid besprochen: und die haben nur herzlich gelacht als ich ihnen erklärt habe, daß der deutsche Geheimdienstkoordinator davon ausgeht, daß amerikanische Fernmeldeaufklärung nicht mehr hinter deutschen Firmengeheimnissen her ist. Mattew Aid - als ehemaliger NSA-Analytiker und mit guten Rückbezügen in diese Behörde hinein - hat gesagt, es ist überhaupt nicht anders vorstellbar, als daß die NSA - wie immer - sich mit den wesentlichen deutschen Wirtschafts-Unternehmen nachrichtendienstlich auseinandersetzt."

Schmidt-Eenboom und andere Geheimdienst-Beobachter gehen davon aus, daß nun die ECHELON-Station Menwith Hill in Großbritannien den Teil der Lausch-Aufgaben übernommen hat, die der Bundesrepublik gelten.
Was weiß die Bundesregierung über Bad Aibling? Hinweise darauf liefert Geheimmaterial über ECHELON, das kürzlich vom "Nationalen Sicherheits-Archiv" in Washington veröffentlicht wurde. Das brisante Material stammt aus

dem Giftschrank der NSA. Herausgefischt hat es Jeffrey T. Richelson, dessen Veröffentlichungen über das Innenleben amerikanischer Geheimdienste seinen Ruf, seriös zu arbeiten, durchaus nicht geschmälert haben. Die ausgewerteten Mikrofiche-Dateien der NSA belegen erstmalig die Existenz von ECHELON und des Horchpostens in Bad Aibling.
In einem der Dokumente heißt es, daß Präsident Clinton Anfang 1995 die Geheimhaltung über Details eines Satelliten-Programms (zu dem auch Echelon gehört) aufgehoben hatte. Spätestens von diesem Zeitpunkt an müßte also die Bundesregierung ziemlich genau gewußt haben, was in Bad Aibling passiert. Denn in einer Notiz des amerikanischen Außenministeriums, die bei Richelson die Nummer 14 trägt, ist von der Sorge der Vereinigten Staaten die Rede, wie Deutschland auf das Eingeständnis reagieren werde.

Wie reagiert die Bundesrepublik nun aber auf den Bericht für das Europäische Parlament? Und was machen die europäischen Gremien selbst mit den Studien der STOA? Angesichts der darin aufgeführten Risiken und Probleme der sich rasant weiterentwickelnden Informationstechnologien, ist schnelles Handeln geboten. Besonders, wenn man sich die Mißbrauchs-Möglichkeiten durch Abhörsysteme wie ECHELON vergegenwärtigt.
Die STOA fordert deshalb nichts Geringeres als jährliche Berichte über Wirtschaftsspionage - und zwar von jedem einzelnen Mitgliedstaat. Außerdem mahnt sie ein härtere Gangart gegenüber den Vereinigten Staaten an: Sie nennt es "kritische Prüfung" der amerikanischen Forderung nach Verbot bzw. Standardisierung von Kryptographie-Produkten.
Ulrich Sandl macht eine sehr lange Pause bevor er auf die Frage antwortet, wie der Bericht im Bundeswirtschaftsministerium aufgenommen wurde:

„Wir nehmen ihn zur Kenntnis. Aber auch das haben wir gelernt in den Diskussionen, daß nicht alles so ist, wie es zu sein scheint. Und von daher hüte ich mich jetzt hier davor mich mit einigen Äußerungen hervorzutun. Weil, so klar, wie es manchmal auch in den Medien dargestellt wird, ist es nicht. Erstens von der Zielrichtung her, von den Beteiligten her, und ich glaube, daß wir hier auch noch viel mit unseren Partnern noch zu klären haben, wie wir uns da wirklich in der Öffentlichkeit drüber unterhalten."

Auf europäischer Ebene herrschte lange ähnliche Zurückhaltung. Detlef Eckert, Leiter der Grundsatz-Abteilung der Generaldirektion 'Informationsgesellschaft' der Europäischen Kommission, betont allerdings, Wirtschaftsspionage falle in den Bereich der nationalstaatlichen Souveränität der Mitgliedstaaten:

„Die Verbrechensbekämpfung ist Aufgabe der Mitgliedstaaten und nicht Aufgabe der Kommission. Das heißt, wir sind hier nur subsidiär tätig. Im Sinne

der Kooperation der Mitgliedstaaten. Dafür gibt es bestimmte Gremien. Da wird auch dieses Thema besprochen, in den Ausschüssen. Im Übrigen ist es eine Frage der Zuständigkeiten: Wir haben ja hier auf EU-Ebene keine Polizei, die nun irgendwelche Spionagetätigkeiten verfolgen würde. Sie könnten vielleicht Europol anführen, aber das ist eine Organisation, die außerhalb der Kommission angesiedelt ist. Und in diesem Fall besitzen wir nicht die Zuständigkeit und nicht die Mittel, aktiv nun einzugreifen."

Auch Erich Schmidt-Eenboom vom Weilheimer Institut für Friedenspolitik ist der Ansicht, daß die Nachrichtendiensten offensichtlich einen letzten Hort nationalstaatlicher Interessen darstellen. Wie steht es unter dem Vorzeichen 'Wirtschaftsspionage' dann um das geeinte Europa und den immer stärker werdenden Konkurrenzkampf mit den USA? Nach der Vorlage des STOA-Berichts im Europäischen Parlament wächst der Druck auf die Kommission. Die Empörung ist groß. Australien hat längst zugegeben, daß ECHELON existiert. Aber die Vereinigten Staaten und Großbritannien weisen die Ergebnisse der Studie weiter zurück. Dabei belegen doch die geheimen Unterlagen der NSA - was nicht verwundert -, daß es nach dem Zusammenbruch der Sowjetunion nur noch zwei amerikanische Aufklärungs-Gruppen gibt: eine für den Rest der Welt und eine für Europa. Erich Schmidt-Eeenboom:

„Ich denke das Signifikanteste ist, daß im Dezember 1999 der britische Manager von British Aerospace in Marseille von französischen Nachrichtendiensten überwacht und kontrolliert wurde. Weil das deutlich macht, daß auch innerhalb der europäischen Union Wirtschaftsspionage gegeneinander betrieben wird.
Was ich zunehmend beobachte ist, daß die Amerikaner beispielsweise nachrichtendienstlich mit Österreich oder der Schweiz sehr enge gemeinsame Joint-Ventures in der fernmeldeelektronischen Aufklärung machen, d.h.: Sie nisten sich in einem Teil der Europäischen Union selbst wieder ein, damit eben kein geschlossener - in Anführungszeichen - Gegnerblock gegen die Aufklärungskapazitäten der NSA wachsen kann."

Der George Orwell gewidmete "Big-Brother-Preis" der britischen Bürgerrechts-Organisation "Privacy International" wurde übrigens unlängst an die österreichischen Europa-Parlamentarier verliehen: Sie hatten im Mai '99 geschlossen dem grenzüberschreitenden Zugriff auf Telekommunikation und Internet zugestimmt.