Echelon & EU

Dirk Schmidt

Inhaltsverzeichnis

Einleitung

Diese Hausarbeit ist vom Seminar „Ausgewählte Probleme der europäischen Integration“ an der Ruhr-Unversität Bochum im Wintersemester 1999/2000 bei Dr. Hubert Zimmermann inspiriert worden. Sie versucht, beispielhaft anhand des Themenkomplexes Echelon die Schwierigkeiten der Integration in Hinsicht auf nachrichten- und geheimdienstliche Tätigkeiten der EU-Mitgliedsstaaten gegeneinander darzustellen.

Geheimdienstlichen Aktivitäten ist es zu eigen, daß diese meist im Verborgenen stattfinden, so daß die Quellenzahl hierzu meist gering ist. In bezug auf den Echelon-Komplex ist es nicht zuletzt aufgrund der Befassung des Europäischen Parlamentes hiermit in der jüngsten Zeit zu einigen verwertbaren Veröffentlichungen gekommen.

Die Verwertbarkeit, die Vertrauenswürdigkeit, stellt bei der Untersuchung geheimdienstlicher Aktivitäten ein besonderes Problem dar, da hier Fakten von Gerüchten, sogar Hirngespinsten, getrennt werden müssen. Zum Echelon-Komplex und dem eigentlichen Echelon-System existieren eine Menge falscher Annahmen, beispielhaft sei die Filterung von Telefongesprächen nach inhaltlichen Kriterien genannt, die bisher technisch gar nicht realisierbar ist.
Beschränkt wurde sich dabei vor allem auf die Publikationen des Europäischen Parlamentes und des online-Magazins Telepolis des Heise-Verlags .

Weiterhin beschränkt sich diese Arbeit weitgehend auf die Analyse des Umgangs des Europäischen Parlaments mit dem Echelon-Komplex, das seine Aktivität hierzu seit 1998 kontinuierlich erhöht hat. Dennoch wird versucht herauszuarbeiten, welche Verquickungen zwischen Akteuren innerhalb und außerhalb der EU besteht (UKUSA).

Um die Brisanz des Echelon-Komplexes zu verdeutlichen, wurde der eigentlichen politikwissenschaftlichen Arbeit der Abschnitt „Abhörmöglichkeiten“ vorangestellt.[1] Dieser wurde nicht in den Anhang gestellt, da er nach Meinung des Autors vielfach zum technischen Verständnis der folgenden Teile notwendig ist.

1 Der Abschnitt „Abhörmöglichkeiten“ schildert ausschließlich die Arten der Zugangsgewinnung zu unterschiedlichen Übertragungswegen, die daran anschließende Extrahierung der übertragenen Inhalte, die Trennung von Inhalten, spielt weiter keine Rolle. Hierfür sei auf den Bericht von Duncan Campell verwiesen (siehe [9]).

Inwiefern die bestehenden technischen Möglichkeiten im Rahmen von Echelon benutzt werden klärt, der darauf folgende Abschnitt, dem sich eine Darstellung von Rechtsprinzipien bzgl. des Abhörens und des Datenschutzes anschließt.

In separaten Abschnitten werden die Interessen der Akteure, die verschiedene Akteure verfolgen, und Lösungsansätze dargestellt. Drauf folgt die Erläuterung von Handlungsoptionen und ein Abriß der bisherigen, aktuellen Entwicklung der europäischen Politik in Bezug auf den Echelon-Komplex.

Im Abschnitt „Schlußfolgerungen“ wird eine Handlungsempfehlung an das Europäische Parlament gegeben und formuliert, welches Verhalten der Autor von ihm erwartet. Er schließt mit einem Ausblick auf weitere Untersuchungen zu Fragen, die sich im Rahmen der Befassung mit dem Echelon-Komplex stellen.

Mit dieser Gliederung beschreitet diese Arbeit einen funktionalistischen Ansatz, bei dem die Forderungen und Einflüsse auf das politische System untersucht werden. Das politische System der Europäischen Union wird dabei nicht als „black box“ behandelt, sondern seine Strukturen fließen auch mit ein, so daß eine Prognose für das Verhalten eines Akteurs, des Europäischen Parlaments, abgegeben werden kann.

Zum Zwecke der bessern Lesbarkeit wurden die Quellenangaben möglichst kurz gehalten, sie lassen sich anhand der Nummern im Literaturverzeichnis identifizieren.

Abhörmöglichkeiten

Die moderene, westliche Gesellschaft zeichnet sich durch ihre vielfältigen Möglichkeiten zur Kommunikation über kurze und weite Distanzen aus. Zur Überbrückung großer Distanzen stand lange Zeit nur die mündliche Überlieferung Reisender, Boten oder der organisierte Briefverkehr zur Verfügung.

Seit jeher ist mit Briefen auch das Problem verbunden, daß diese von Fremden auf ihrem Weg zum Empfänger gelesen werden könnten. Das Postgeheimnis versuchte man zum Beispiel durch das Versiegeln von Briefen zu sichern. Der Siegelbruch, das Öffnen und Lesen eines Briefes, ließ sich so zwar nicht verhindern, aber es konnte entdeckt werden und war bei Strafe verboten.

Die Antwort der „Lauscher“ beim Briefverkehr bestand dann darin, einen Brief derart kunstgerecht zu öffnen, daß das Siegel nicht gebrochen wurde oder eine Fälschung zum erneuten Versiegeln erstellt werden mußte.

Dieser Wettbewerb zwischen Sicherung von vertraulichen, nicht abgehörten, Kommunikationswegen und den Möglichkeiten der Lauscher hat sich auch bei modernen Kommunikationsmitteln fortgesetzt.

Im 19. Jahrhundert wurde das Telefon erfunden, im 20. Jahrhunderten folgten Funkübertragung, schließlich die Satellitentechnik. Nicht nur Texte und Sprache werden heute über dieses Übertragungswege transportiert, sondern auch Bilder, Telefaxe, und Daten aller Art, all die Informationseinheiten, die die elektronische Datenverarbeitung (EDV), der Einsatz von Computern, liefert.

Um zunächst die Möglichkeiten und Wege moderner Abhörtechnologien darzustellen, wird hier zwischen Übertragungsweg, Übertragungsinhalt und Botschaft unterschieden; Übertragungsinhalt bezeichnet dabei nicht den Inhalt der eigentlichen Nachricht, die Botschaft, sondern die Form, wie dieser übermittelt wird, zum Beispiel in Gestalt einer E-Mail, eines Telefaxes oder Telefongespräches. Die heutige Digitaltechnik, aber auch in Ansätzen die bis in die 70er Jahre verwandte Analogtechnik, gestattet es, sämtliche Formen von Übertragungsinhalten über die heute zur Verfügung stehende Übertragungswege, zum Beispiel Satellitenverbindungen oder Tiefseekabel, zu transportieren.

Übertragungswege

Übertragungswege abzuhören ist für Lauschangriffe sehr interessant, da das Abhören auf diesem Wege meist unentdeckt bleibt und einfacher zu realisieren ist, als zum Beispiel eine sogenannte Wanze, ein winziges Mikrofon mit einem Sender, in ein Telefon einzubauen. Der Zugang zu einem Übertragungsweg eröffnet auch stets die Möglichkeit, eine Vielzahl von Sendern und Empfängern von Botschaften abzuhören.

Zugang zu einem Übertragungsweg zu erhalten, ist auf unterschiedliche Art möglich. Unterschieden werden muß grundsätzlich, ob dies mit oder ohne Wissen und Hilfe des Betreibers eines Übertragungsweges geschieht.

In den USA war es bisher zur Watergate-Affäre des Präsidenten Nixon üblich, daß die nationalen Geheimdienste Zugang zu den Zentralen der Netzbetreiber hatten; die gesuchten Telefonate wurden direkt von den Netzbetreibern geliefert. Eine derartige Zusammenarbeit zwischen Betreibern und Geheimdiensten ist auch heute noch, vor allem in den USA, üblich; für einige Übertragungswege ist es der einzige praktikable Weg.

Unentdeckt bleiben hingegen die Abhörmöglichkeiten, die ohne Zustimmung und Wissen der Betreiber eines Übertragungsweges erfolgen. Die Möglichkeiten dieses Vorgehens werden stark durch technische Merkmale eines Übertragungsweges bestimmt. Während bei Kabelverbindungen die Möglichkeit bestehen muß, Zugang zu diesem Kabel zu haben, entfällt dies Problem bei den meisten Funk und Satellitenverbindungen.

Kabel

Seit der Erfindung des Telegraphen und später des Telefons sind Kabelverbindungen weit verbreitet. Ein dichtes Kabelnetz, das für Sprach- und Datenverbindungen genutzt wird, durchzieht mit wenigen weißen Flecken auf der Karte die gesamte Erde.

Um die Kommunikation über Kabel abhören zu können, ist es nötig, Zugang zu diesem Kabel zu haben. Dies kann mit Hilfe des Betreibers geschehen, welcher sämtliche darüber geführten Verbindungen an den entsprechenden Geheimdienst weiterleitet oder auch nur ausgesuchte, zum Beispiel die Verbindungen eines bestimmten Empfängers oder Senders.

Ohne die Mitwisserschaft des Betreibers einer Kabelverbindung besteht aber auch die Möglichkeit, diese abzuhören, in dem die

Verbindung an einer Stelle „angezapft“ wird; anzapfen bedeutet dabei, daß der entsprechende Geheimdienst selber die Vorrichtungen unbemerkt unterhalten und einrichten muß, die ihm Zugang zu den gewünschten Verbindungen liefern.

Tiefseekabel

Tiefseekabel werden ungern betrieben und werden möglichst kurz gehalten, da sie die Betreiber bei der Wartung vor große Probleme stellen. Kabel, die mehrere tausend Meter auf den Meeresgrund gesenkt werden, sind fast gar nicht zu reparieren, falls es zu Störungen, zum Beispiel Leitungsunterbrechungen kommt. Manche Arten an Kabelverbindungen erfordern auch eine Signalverstärkung in bestimmten Abständen. Die hierfür nötigen technischen Installationen müssen mit auf den Meeresgrund versenkt werden; für die Wartung gilt das gleiche wie für das eigentliche Kabel selber.

Die Schwierigkeiten der Wartung stellen auch die Geheimdienste vor Probleme, wenn ihnen ein Zugang mit Zustimmung des Betreibers nicht gestattet ist.

Kabelverbindungen, die über elektrische Ströme, welche durch metallene Drähte fließen, realisiert werden, bieten für Lauschangriffe die Möglichkeiten sogenannte Induktionen einzufangen. Strom, der in einem Draht fließt, erzeugt elektromagnetische Schwingungen, Wellen, welche sie in andere Drähte oder metallene Gegenstände, im allgemeinen als Antennen bezeichnet, übertragen. Die Funktechnik basiert auf diesem Effekt der Induktion.
Um eine derartige Kabelverbindung abzuhören, muß das Tiefseekabel an einer Stelle mit Kabeln umwickelt werden, die die Induktionen einfangen. An den Kabeln muß eine Apparatur angebracht werden, die dies Signal aufbereitet und an eine Abhörstation des betreibenden Geheimdienstes weiterleitet.

Der us-amerikanische Geheimdienst NSA (National Security Agency) hat diese Technik in Zusammenarbeit mit der U-Boot-Flotte der US-Marine während des kalten Krieges gegen die Sowjetunion angewandt. Eine entsprechender Sender konnte aufgrund des Verrats eines übergelaufenen Mitarbeiters des NSA durch den sowjetischen KGB geborgen werden; die Apparatur kann im KGB-Museum in Moskau besichtigt werden.

Die USA betreiben in Kooperation mit Großbritannien eine Abhörstation in Menwith Hill, England; über Menwith Hill ver-

laufen die transatlantischen Kabelverbindungen zwischen Europa und den USA.

Glasfaserkabel

Glasfaserkabel, erst recht in der Ausführung als Tiefseekabel, sind sehr schwer abzuhören, da die über sie übertragenen Lichtwellen keine Induktion aufweisen. Eine Unterbrechung, um die Kommunikation anzuzapfen, kann aufgrund technischer Aspekte nur sehr schwer unentdeckt bleiben, bei Tiefseekabeln aus Glasfasern ist sie faktisch unmöglich.

Den einzigen Angriffspunkt bieten Glasfaserkabel an den Verstärkungsstellen, den sogenannten Repeatern. Das Signal eines Glasfaserkabels muß alle 40 Kilometer verstärkt werden. Hierfür sind alle 40 Kilometer technische Apparaturen anzubringen, die das Signal eines Kabelendes auffangen und verstärkt in das andere abgeben.
Bei Glasfaserkabeln in Tiefseeausführung werden die Repeater mit auf den Meeresgrund versenkt. Ihre wartungsfreie Lebensdauer ist zur Zeit auf 25 Jahre begrenzt, was somit auch die Lebensdauer eines Tiefsee-Glasfaserkabel auf 25 Jahre begrenzt.

Die für das Abhören eines Glasfaserkabels nötigen Einrichtungen, die an einem Repeater oder einer Vermittlungsstelle an Land angebracht werden müssen, um eine Kopie des Signals zu erhalten, sind auch nicht so klein, als daß sie unentdeckt bleiben könnten. Das Abhören von Glasfaserverbindungen ist daher nur mit Zustimmung und Hilfe des Betreibers praktikabel.

Funk

Funkübertragung benutzt den Effekt der Induktion. Eine Sendeeinrichtung läßt hierbei in einer Antenne, einem länglichen metallenen Gegenstand einen Strom mit einer bestimmten Frequenz fließen, der gleichzeitig Träger von Informationen, der Kommunikation ist. Von der Antenne werden elektromagnetische Wellen ausgesendet, die abhängig von der Frequenz bestimmte Eigenschaften besitzen. Diese elektromagnetischen Wellen werden vom Empfänger mit Hilfe einer Antenne aufgefangen und die Informationen, die daran gekoppelte Kommunikation, kann sichtbar bzw. hörbar gemacht werden.

Die Technik der Ausstrahlung der elektromagnetischen Wellen bedingt, daß es mehr als einen Empfänger geben kann. Je nach den Eigenschaften, die die ausgestrahlten Wellen besitzen, je

nach dem verwandten Frequenzbereich, ist der Standort abhängig, an dem ein Lauscher seine Antennen aufstellen muß, um die Kommunikation dieses Übertragungsweges abhören zu können.

Langwellen (high frequency radio)

HF-Radiowellen werden an der Erdoberfläche und der Ionosphäre, die die Erde umgibt, gespiegelt. Dies ermöglicht Empfang und Abhörung mit erdgebundenen Antennen über Tausende von Meilen.

HF-Radiowellen abzuhören ist einfach, da nur eine geeignete, große Antennenanlage in einer Gegend mit wenig Störfunk benötigt wird. (vgl. [9], S. 5)

Kurzwellen (microwave radio relay)

Kurzwellen werden im Vegleich zu Langwellen mit leistungsschwächeren Sendern gesendet und mit Parabolspiegelantennen mit einem Durchmesser von 1-3 Metern empfangen. Sie werden im Gegensatz zu HF-Radiowellen nicht an der Erdoberfläche oder Ionosphäre gespiegelt, so daß aufgrund der Erdkrümmung alle 30-50 Kilometer Relaisstationen benötigt werden, die das Signal weitergeben.

Zum Abhören wird eine zweite Antenne in dem Bereich benötigt, in dem die Kurzwellen empfangen werden können. Da zu diesen über Kurzwellen realisierten Richtfunkstrecken aber kein (legaler) Zugang für fremde Geheimdienste besteht, werden Satelitten benötigt, die ihren Standort 80 Längengrade entfernt, auf der Tangente an die Erde durch die Positionen von Sende- und Empfangseinrichtung.

Satelliten

Satelliten sind Sende- und Empfangseinrichtungen, die sich im Weltraum auf einer Umlaufbahn um die Erde befinden.

Zum Abhören muß zwischen Satelliten, die sich auf geostationären Umlaufbahnen befinden und somit von der Erde aus gesehen stillzustehen scheinen, und solchen, die es nicht tun, unterschieden werden.

Geostationäre Satelliten

Mit Hilfe von Satelliten lassen sich die Problem im Zusammenhang mit Kurzwellenübertragungen im Kurzwellenbereich umgehen. Muß bei Kurzwellenübertragungen aufgrund der

Erdkrümmung alle 30-50 Kilometer eine Relaisstation aufgestellt werden, so wird bei Satellitenverbindungen meist nur eine Relaisstation, der Satellit, benötigt. Der Satellit empfängt das Singal vom Sender und schickt es zur Erdoberfläche, zum eigentlichen Empfänger weiter. Sender und Empfänger dürfen bei dieser Technik theoretisch maximal 180 Längen- oder Breitengrade entfernt sein, ansonsten werden mindestens zwei Satelliten benötigt, um die Erdkrümmung zu überwinden.

Zum Abhören dieses Übertragungsweges genügt es, eine zweite Empfangsstation für einen Satelliten zu bauen, die die elektromagnetischen Wellen, welche der Satellit an den Empfänger schickt, abhört.

Der größte Betreiber von geostationären Satelliten ist die internationale Intelsat-Organisation. Ihre Satelliten bieten Übertragung für Telefon-, Fernseh- und Datenübertragung.

Nicht-geostationäre Satelliten

Nicht-geostationäre Satelliten ändern permanent, aber je nach Position mit unterschiedlicher Geschwindigkeit, ihre Position. Einzelne Satelliten sind zur Gewährleistung eines Übertragungsweges weniger geeignet, da diese sich bezüglich der Standorte des erdgebundenen Senders und Empfängers, die wiederum weniger als 180 Längen- oder Breitengrade von einander entfernt sein müssen, nicht immer oberhalb des Horizontes befinden, was für eine Verbindung zwingend erforderlich ist.

Ein Verbund von mehreren Satelliten, die nach einem bestimmten System ihre Positionen verändern, kann aber benutzt werden, um die gesamte Erdoberfläche oder auch nur Teilgebiete davon mit permanenten Übertragungswegen bei wechselnden Satelliten zu versehen. Das Abhören eines einzelnen Satelliten gestaltet sich dabei sehr schwierig, da dies immer nur von bestimmten Standorten zu bestimmten Zeiten möglich ist. Ein ganze Flotte solcher Satelliten abzuhören, scheint dann nur wieder in Zusammenarbeit mit dem Betreiber möglich zu sein.

Das satellitengestützte Mobiltelefonnetz Iridium nutzt(e) diese Technik. Weiterhin sind von Microsoft Inc. und anderen Firmen derartige Satellitenflotten geplant, die permanente Datenverbindungen mit hohen Kapazitäten, u.a. für Internetverbindungen, gewährleisten sollen.

Post

Der Postweg, das Öffnen von Briefen, spielt in dieser Arbeit keine Rolle. Auf dem Postweg versandte Datenträger können, wenn die entsprechende Versandeinheit geöffnet wird, unbemerkt vervielfältigt werden.
Verschlüsselungstechniken, wie weiter unten aufgeführt, können die Auswertung der so gewonnen Daten be- oder sogar verhindern.

Übertragungsinhalte

Die Inhalte, die über einen Übertragungsweg gesendet werden, können in zwei Kategorien sortiert werden: Öffentliche und vertrauliche bzw. private Inhalte.

Öffentliche Inhalte sind alle Übertragungsinhalte, die allen zugänglich sind. Hierzu zählen Fernseh- oder Radioübertragungen. Häufig kommt es vor, daß die Übertragungsinhalte sich aber aus öffentlichen und vertraulichen Teilen zusammensetzen.

Telefon

Bereits bei Kabelverbindungen analoger Technik konnten mehrere Gespräche auf unterschiedlichen Frequenzen übertragen werden. Mit Hilfe digitaler Übertragungstechnik läßt sich dieses noch vervielfachen. Telefongespräche werden hierbei digitalisiert, die digitalen Daten dann in Paketen gesendet, empfangen und wieder in Töne, ins Gespräch, umgewandelt. Die Datenpakete verschiedener Gespräche können so auf allen Übertragungswegen gebündelt übertragen werden.

Telefongespräche umfassen bei der Übertragung nicht nur die Informationen über das Gespräch, die Botschaft, sondern auch die Telefonnummer des Empfängers, ggf. sogar des Senders. Dies ermöglicht die gezielte Zuordnung von Gesprächen zu bestimmten Telefonapparaten und somit Personen.

Telefax

Telefaxgeräte benutzen zur Datenübertragung das Telefonnetz. Im Abschnitt Telefon (siehe Seite 11) behandeltes gilt somit auch für das Abhören von Telefaxübertragungen.

Telex

Telex ist der Vorläufer des Telefaxes. Hierbei werden über Telefonverbindungen Zeichen, also Buchstaben und Zahlen, übertragen.
Im Abschnitt Telefon (siehe Seite 11) behandeltes gilt somit auch für das Abhören von Telexübertragungen.

Daten & E-Mail

Datenverbindungen können über Telefonverbindungen realisiert werden oder selbständige Verbindungen über alle bekannten Übertragungswege darstellen. Verbindung für Intranets oder das Internet übertragen hierbei die Daten zwischen verschiedenen Teilen des jeweiligen Netzwerks. Die übertragenen Datenpakete können zu Daten unterschiedlicher Inhalte gehören. Es kann sich wiederum um digitalisierte Sprache, Töne, Bilder oder Programme und sonstige Daten handeln; insbesondere werden über derartige Verbindungen auch E-Mails gesendet.

Im Rahmen des Internets werden auf allen Übertragungswegen Datenverbindungen unterhalten. Über diese Verbindungen gehen öffentliche Inhalte, wie WWW-Seiten oder Beiträge des Usenets, aber auch private Inhalte wie E-Mails oder Chats.
Von Interesse in dieser Arbeit sind nur die privaten, vertraulichen Inhalte; für die Auswertung öffentlich zugänglicher Quellen, deren Inhalte über die gleichen Datenverbindungen übertragen werden, unterhalten die Geheim- und Nachrichtendienste oder andere staatliche Organisationen jeweils eigene Abteilungen.

Übertragungen im Rahmen des Internets enthalten ebenso wie zum Beispiel Telefongespräche nicht nur die Daten, sondern auch Informationen über Sender und Empfänger, z.B. IP-Adressen (u.U. ähnlich einer Telefonnummer auszuwerten) oder sogenannte Cookies.

Verschlüsselung

Verschlüsselung bezeichnet den Vorgang, lesbare Daten auf geheime, vorher verabredete Weise derart in informationslose Daten zu verwandeln, daß dieser Vorgang wieder rückgängig gemacht werden kann (Entschlüsselung). Werden die Übertragungsinhalte eines Übertragungsweges oder einzelne Inhalte vor der Übermittlung verschlüsselt, dann sind sie für Lauscher nicht

nutzbar, solange diese die „geheime, vorher verabredete Weise“, die als Schlüssel bezeichnet wird, nicht kennen.
Diese Technik wird auch als Kryptographie bezeichnet.

Verschlüsselungstechniken und –apparate stehen für unterschiedliche Anwendungen, für Telefax-, Telefon- und Datenverbindungen zur Verfügung, werden aber unterschiedlich stark, teilweise fast gar nicht, genutzt.

Anstatt die einzelnen Botschaften oder einzelnen Übertragungsinhalte zu verschlüsseln, besteht auch die Möglichkeit, ganze Übertragungswege mit Hilfe von Verschlüsselungsverfahren zu sichern. Es können auch alle Verfahren gekoppelt werden, das heißt, Daten können auch mehrfach verschlüsselt werden.

Verschlüsselungsmethoden

Die Kryptographie kennt zwei unterschiedliche Methoden der Verschlüsselung: Die symmetrische und die asymmetrische.
Beide haben Vor- und Nachteile, sie werden für die Anwendung häufig kombiniert.

Symmetrische Verschlüsselung

Bei der symmetrischen Verschlüsselung werden zum Verschlüsseln und Entschlüsseln die selben Schlüssel verwandt. Symmetrische Verfahren zeichnen sich durch ihr Schnelligkeit aus. Sie benötigen nicht viel weniger Rechenleistung als asymmetrische Verfahren.

Ein Problem bei der symmetrischen Verschlüsselung besteht darin, dem Empfänger der Botschaft auf sicherem Weg den Schüssel zu übermitteln. Wird dieser Vorgang bereits belauscht, dann kann der abgehörte Schlüssel benutzt werden, um die gesamte mit dem Schlüssel verschlüsselte Kommunikation abzuhören; die Verschlüsselung ist damit wirkungslos.

Ein anderes Problem ist, daß für jede mögliche Kombination aus Sender und Empfänger ein eigener Schlüssel erstellt werden muß, für den sich dann wieder das Problem der Schlüsselverteilung aus dem vorherigen Absatze stellt.

Asymmetrische Verschlüsselung

Bei der asymmetrischen Verschlüsselung werden zum Verschlüsseln und Entschlüsseln verschiedene Schlüssel benötigt. Der Schlüssel zum Verschlüsseln kann vollkommen ungesichert über alle Übertragungswege gesendet werden, da er nicht zum

entschlüsseln verwandt werden kann, sondern nur zum verschlüssen. Zum Entschlüsseln wird aber unbedingt der andere Schlüssel benötigt, welcher geheim bleiben muß. Daher heißt dieser Schlüssel auch geheimer Schlüssel (secret key), der andere öffentlicher Schlüssel (public key)

Ein Problem bei der asymmetrischen Verschlüsselung besteht darin, daß jeder Sender im Besitz des öffentlichen Schlüssels des Empfängers sein muß. Angenehm ist jedoch, daß die Veröffentlichung des öffentlichen Schlüssels unproblematisch ist, da mit ihm nur verschlüsselt werden kann, was die Schlüsselverteilung vereinfacht.
Potentiellen Lauschern bleibt die Möglichkeit, Sender und Empfänger zu täuschen, in dem der getauschte öffentliche Schlüssel abgefangen und durch den des Lauschers ersetzt wird. Dieser muß dann aber jede gesendete Nachricht abfangen, entschlüsseln und mit dem originalen öffentlichen Schlüssel wieder verschlüsseln. Vorkehrungen dagegen sind sehr einfach, Verfahren wie das Programm PGP sie vorsieht, lassen dies nicht unentdeckt; Zertifizierungsstellen mit einem ersten sicher übermittelten Schlüssel lösen dieses Problem.

Ein anderes Problem ist, daß asymmetrische Verschlüsselung sehr rechenintensiv ist.

Die Technik der Verschlüsselung mit öffentlichem und geheimem Schlüssel findet noch einen anderen Einsatz: Die digitale Unterschrift. Bei der digitalen Unterschrift oder Signatur werden die bei einigen Verfahren, zum Beispiel RSA (siehe S. 18), gleichen Techniken benutzt, um zu gewährleisten, daß die Daten nicht verändert wurden, das heißt, daß die Daten zwar für alle lesbar bleiben, eine Veränderung dieser aber auffällt. Zum Unterschreiben wird dabei der geheime Schlüssel benutzt, zum Überprüfen der Unterschrift der öffentliche.
Die digitale Unterschrift spielt hier keine Rolle, da sie nur die Authentizität, die Echtheit, einer Botschaft gewährleistet, nicht aber das „Mitlesen“ anderer verhindert.

Hybride Verschlüsselung

Symmetrische und asymmetrische Verschlüsselung werden gerne kombiniert, um die Vorteile beider Verfahren nutzen zu können. Diese heißen dann hybride Verfahren.

Die asymmetrische Verschlüsselung wird benutzt, um mit Hilfe eines Paares aus öffentlichem und geheimen Schlüssel einen dritten Schlüssel, den für das symmetrische Verfahren, zu

übermitteln. Mit Hilfe des asymmetrischen wird dabei gewährleistet, daß der symmetrische Schlüssel geheim bleibt. Der symmetrische Schlüssel kann dann benutzt werden, um die Daten schnell zu ver- und entschlüsseln.

Mit Hilfe eines derartig kombinierten Verfahrens ist es auch möglich, den symmetrischen Schlüssel häufig zu wechseln, was Angriffe ihn zu brechen, also herauszufinden, bekämpft.

Verschlüsselung mit dem Programm PGP sendet sogar mit jeder verschlüsselten E-Mail einen neuen symmetrischen Schlüssel. Jede E-Mail wird dabei mit einem neuen, frisch generierten, symmetrischen Schlüssel (Session-Schlüssel) verschlüsselt, welcher mit dem öffentlichen Schlüssel des E-Mail-Empfängers (asymmetrisch) verschlüsselt wird; der verschlüsselte Schlüssel wird dann einfach an die E-Mail angehängt. Somit bekommt jede E-Mail einen eigenen Schlüssel für den Inhalt. Es genügt natürlich einen der beiden Schlüssel zu brechen, um an die Botschaft zu gelangen.

Schlüssellänge

Die mathematischen Verfahren zur Verschlüsselung beruhen auf Eigenschaften sehr großer Primzahlen. Die zu verschlüsselnden Daten werden bei diesen Verfahren mit sehr großen Primzahlen kombiniert, zum Entschlüsseln werden die selben Zahlen benötigt. Wird versuchsweise eine andere sehr große Primzahl verwandt, die in der Nähe der richtigen liegt, kommt auch nur Datenmüll heraus; die Kombination der sehr großen Primzahl muß also direkt gefunden werden.

Natürlich kann ein Computerprogramm geschrieben werden, das entweder alle möglichen Schlüssel ausprobiert (brute force attack) oder versucht, den Schlüssel aus den Daten zu errechnen. Bei beiden Ansätzen, den Attacken den Schlüssel zu brechen, müssen eine Vielzahl an sehr großen Primzahlen erzeugt werden oder sehr große Zahlen in ihre Primfaktoren (Faktorisierung) zerlegt werden. Die Sicherheit der krypthographischen Verfahren beruht darauf, daß das Ermitteln von Primzahlen oder die Faktorisierung großer Zahlen sehr lange dauert. Die benötigte Zeit steht dabei nicht in einem linearen, sondern einem exponentiellen Verhältnis zur Größe der verwandten Zahlen. Die Größe dieser Zahlen findet sich in der Länge der zur Verschlüsselung verwandten Schlüssel wieder. Es gilt: Je länger der Schlüssel, desto mehr mögliche Kombinationen existieren, die berechnet werden müssen, um den Schlüssel zu brechen. Die

Sicherheit der Verschlüsselung beruht nun darauf, daß das Brechen eines Schlüssels - für einen Computer heutiger Bauart - theoretisch nur eine endlich lange Zeit dauert, diese für Menschenverhältnisse aber unendlich erscheint.

Schlüssellängen werden in Bit angegeben, der kleinsten Zahleneinheit eines Rechners; ein Bit repräsentiert dabei eine Potenz von 2. Ein Schlüssel von 10 Bit repräsentiert also $2^{10} = 1024$ mögliche Schlüssel, 20 Bit repräsentieren dann $2^{20} = 1048576$ mögliche Schlüssel etc.
Anfang 1999 wurde die Dauer, die ein Hochleistungsrechner benötigt, um einen 56 Bit langen Schlüssel zu brechen, noch auf 5 Jahre geschätzt. Mit einem Schlüssel von 128 Bit kann man daher davon ausgehen, daß das Finden des passenden Schlüssels für menschliche Verhältnisse unendlich lang dauern würde..

56 Bit beträgt die Länge des DES-Verfahrens zur Verschlüsselung (siehe Seite 19). Mit Hilfe verbesserter Verfahren einen Schlüssel zu attackieren und einem Hochleistungsrechner bzw. einem Rechnerverbund gelang es 1998 einen 56 Bit langen Schlüssel zunächst in weniger als 40 Tagen, schließlich in weniger als 3 Tagen zu brechen (brute force attack). Seit dem können Schlüssel mit einer Länge von 56 Bit oder weniger nicht mehr als sicher gelten.

Es könnte unterstellt werden, daß zwischen „Kodemachern“ und „Kodeknackern“ ein Wettbewerb besteht, wer die leistungsfähigeren Verfahren und Rechner zum Verschlüsseln und zum Schlüsselbrechen baut. Da Schlüssellänge und Zeitaufwand zum Brechen (brute force attack) aber in einem exponentiellen Verhältnis stehen, ist ab einer bestimmten Schlüssellänge eine Zeitdauer, eine Vielzahl an Operationen, nötig, die empirischen Überlegungen nach (siehe Seite 17) ein Rechner heutiger Bauart nie in für menschliche Verhältnisse endlicher Zeit berechnen kann, selbst wenn mehrere dieser Rechner parallel geschaltet würden.
Neue, schnellere, Verfahren zum Brechen von Schlüsseln könnten dies aber ändern (siehe Seite 19).

Verschlüsselungsverfahren

Im folgenden ist eine Auswahl wichtiger Verschlüsselungsverfahren dargestellt, die die wichtigsten Verfahren umfaßt. Bis auf RSA handelt es sich um symmetrische Verfahren.
Weitere Verfahren sind zum Beispiel Diffie-Hellmann, El Gamal oder Schoof-Elkies-Atkin, welche auch die Probleme der

Faktorisierung großer Zahlen oder ähnliche mathematische Probleme benutzen.

Hash-Verfahren, die einen sogenannten Fingerabdruck (fingerprint) von Daten erzeugen, werden hier nicht behandelt; diese werden u.a. für digitale Signaturen verwandt.

IDEA

IDEA (International Data Encryption Algorithm) ist ein symmetrisches Verschlüsselungsverfahren, das einen 128 Bit langen Schlüssel benutzt. Das Programm PGP benutzt dieses Verfahren um Daten zu verschlüsseln, der Schlüssel selber wird dann mit einem asymmetrischen Schlüssel kodiert und an den Empfänger der Nachricht gesandt.

Zum Ver- und Entschlüsseln wird bei IDEA der selbe 128 Bit Schlüssel bennötigt. Die Länge von 128 Bit gewährleistet, daß es eine riesige Menge an Schlüsseln gibt, genau 2^{128} Stück, also 340 282 366 920 938 463 463 374 607 431 768 211 456, so daß das Erraten eines Schlüssels durch systematisches Probieren (brute force attack) nicht praktikabel ist.

Daß Computer - zumindest heutiger Bauart - nicht eine unendliche Leistungsfähigkeit unterstellt werden kann, belegen folgende beiden Exkurse (aus [20]):

„**Warum soll ein Computer in der nahen Zukunft nicht fix mal alle IDEA-Schlüssel durchprobieren können**?

Weil ein Computer aus prinzipiellen Gründen diese Leistungsfähigkeit nicht haben wird.

Nach dem heutigen Stand der physikalischen Forschung, der sich natürlich ändern kann, ist die Signalübertragung in jedem denkbaren Computersystem durch die Lichtgeschwindigkeit begrenzt.

Dem widersprechen auch nicht die bisherigen "Überlichtgeschwindigkeitsexperimente".

Angenommen das Hochleistungscomputersystem zum Schlüsseltest hat eine maximale Ausdehnung von 0,3 mm, in der die elektronische oder lichtgeleitete Informationsübertragung erfolgt, dann kann es maximal 1 000 000 000 000 Operationen (10^{12}) in jeder Sekunde ausführen, weil es sonst kleiner sein müsste. In 317 Jahren, also 10 003 759 200 Sekunden ist dieses System in der Lage 10 003 759 200 000 000 000 000 Operationen auszuführen. Diese bescheidenen Leistungsfähigkeit von immerhin 10^{22}

Operationen, die in diesen 317 Jahren ausführbar sind, ermöglicht natürlich nicht die Überprüfung von 10^{22} verschiedenen IDEA-Schlüsseln, weil ein Schlüsseltest sich nicht in einem Taktzyklus erledigen lässt. Aber selbst wenn dies möglich wäre, ist die große Anzahl der möglichen IDEA-Schlüssel von 10^{38} dann nur zu 0,000 000 000 000 000 029 Prozent durchsucht. Also wird ein einzelner IDEA-Schlüssel auch dann nicht gefunden werden, wenn man "viele" solcher Computersysteme parallel an die Arbeit setzt..“

„Die bisherige Geschichte der Faktorisierung

70-stellige Zahlen werden heute (1998) in 10 Stunden auf einer Workstation faktorisiert.

100-stellige Zahlen werden in 1 Jahr auf einer Workstation faktorisiert.

129-stellige Zahlen : Im August 1977 stellte Martin Gardner den Lesern der Zeitschrift "Scientific American" die Aufgabe die Zahl
114 381 625 757 888 867 669 235 779 967 146 612 010 218 296 721 242 362 562 561 842 935 706 935 245 733 897 830 597 123 563 958 705 058 989 075 147 599 290 026 879 543 541
zu faktorisieren!

16 Jahre später im April 1994 präsentierten Paul Leyland (Uni Oxford), Michael Graff (Uni Iowa) und Derek Atkins (MIT) die Faktoren. Dabei wurden etwa 600 freiwillige Internet-Benutzer mitbeschäftigt, die nachts auf Ihren Workstations ein Faktorisierungsprogramm laufen ließen, das von K. Lenstra (Bell Labs, Morristown, New Jersey) stammte.

140-stellige Zahl: ist 1996 die kleinste noch nicht faktorisierte Zahl

140-stellige Zahlen werden in einem großen Rechnernetz in 5 Jahren faktorisiert

160-stellige Zahlen: Experten erwarten 1996 eine Faktorisierung in etwa fünf Jahren unter Verwendung der Methode der Zahlkörpersiebe.

200-stellige Zahlen: Die Faktorisierungszeit wird 1998 auf 52 000 000 Jahre geschätzt.“

RSA

RSA ist das bekannteste asymmetrische Verschlüsselungsverfahren; das weitverbreitete Programm PGP nutzt dieses, um

symmetrische Schlüssel nach IDEA zu verschlüsseln und sicher zu versenden.

Das Verfahren trägt den Namen seiner Erfinder Rivest, Shamir und Adleman (1978) und ist 1983 als US-Patent angemeldet worden. Er beruht auf der Primfaktorzerlegung sehr großer Zahlen und kann sowohl für Verschlüsselung als auch für digitale Signaturen benutzt werden.

Bisher sind keine erfolgreichen Versuche RSA zu brechen bekannt. Nachteilig an RSA ist, wie bei allen asymmetrischen Verfahren, der hohe Rechenbedarf zum Ver- und Entschlüsseln. Der symmetrische DES-Algorithmus ist z.B. um den Faktor 1000 schneller.

DES

DES (Data Encryption Standard) ist ein Verschlüsselungsverfahren, das in den 70er Jahren von IBM-Mitarbeitern entwickelt wurde. Es handelt sich um ein symmetrisches Verfahren, das einen 56 Bit langen Schlüssel verwendet. Wie auf Seite 16 geschildert, kann dieses inzwischen in auch für menschliche Verhältnis endlicher Zeit und zu ggf. vertretbaren Kosten gebrochen werden.

Daher werden inzwischen auch Derivate des DES-Verfahrens benutzt, die einen doppelt (112 Bit) oder dreifach (169 Bit) so langen Schlüssel für das gleiche Verfahren benutzen.
Mit dem gleichen Verfahren doppelt verschlüsselte Daten benötigen zum Brechen durch Ausprobieren (brute force attack) die Zeit des einfachen Verfahrens versehen mit der Potenz 2.

AES

Im Rahmen des Projektes C**AES**AR (**C**andidate **AES** for **A**nalysis and **R**esearch) werden seit 1998 verschiedene Verfahren, Kandidaten, für den AES (Adavanced Encryption Standard) getestet. AES wird voraussichtlich ab 2001 verfügbar sein. Gegenüber DES wird es flexibler sein, u.a. verschiedene Schlüssellängen verwenden, zum Beispiel 128 oder 256 Bit.

Quanten-Kryptographie

Quantencomputer und Quantenkryptographie[2] befinden sich zur Zeit noch im Stadium der Entwicklung. In der politischen Diskussion spielen sie noch keine Rolle. Dennoch werden beide der

2 Eine ausführliche Darstellung findet sich in [21], S. 383fff.

Vollständigkeit halber hier kurz dargestellt, da ihre Anwendung eines Tages die gesamten Probleme der Verschlüsselung und damit der sicheren Kommunikation verändern würde. Die Entwicklung eines Quantencomputers würde sämtliche bekannten Verschlüsselungsverfahren brechen können. Nur die Quantenkryptographie wäre ein Verfahren, das dann noch Vertraulichkeit gewährleisten könnte, da es sogar den Akt des Lauschens selbst erkennen läßt.[3]

Parallelrechner

Der Physiker Richard Feynmann entwickelte 1982 die Idee vom Rechner, der mit Hilfe der Quantenmechanik Informationen verarbeiten könne. Das Besondere an solchen Computern ist, daß sie mehrere Operationen gleichzeitig durchführen können, allerdings nur für bestimmte, speziell entwickelte Algorithmen. Das Problem bei Quantenrechner liegt darin, diese Algorithmen zu entwickeln und die Ergebnisse hierüber zu ermitteln.

„Peter Shor von den Bell Labs gelang es als erstem, einen solchen Algorithmus zu finden. Er erfand 1994 ein Verfahren, mit dem sich eine Zahl schneller in ihre Primfaktoren zerlegen läßt als mit jedem klassischen Computer. Das schlug ein, denn wichtige Kryptoverfahren begründen ihre Sicherheit damit, daß es einfach ist, durch Multiplikation große Zahlen zu produzieren, jedoch mit endlicher Rechenkapazität nahezu undenkbar, diese wieder in ihre Faktoren zu zerlegen.“ ([16])

Sollte also die Entwicklung von Quantenrechnern erfolgreich sein, dann stellt das Faktorisieren großer Zahlen kein Problem mehr dar, wodurch die zur Zeit verwandten Verschlüsselungsverfahren leicht zu brechen wären. Mit funktionierenden Quantenrechnern ist aber frühestens in einigen Jahren zu rechnen.

Quantenkommunikation

Lange existieren bereits Konzepte für die Quantenkrypthographie, die sich inzwischen zur Quantenkommunikation erweitert hat. Gegenüber dem Quantencomputer ist sie ein viel ausgereifteres Gebiet der Quanteninformationsverarbeitung. Bei der Quantenkommunikation werden zwei Übertragungswege benötigt, ein herkömmlicher für die übliche Kommunikation und ein

3 Von besonderem Interesse ist, ob die Entwicklung der Quantenkryptographie oder die des Quantencomputers zuerst zur Anwendungsreife gelangt. Sollte letzterer zuerst einsatzfähig sein, wird bis zur Funktionsfähigkeit der Quantenkryptograhie und der hierfür benötigten Infrastruktur keine Möglichkeit sicherer, verschlüsselter, Kommunikation bestehen; es sei denn, neue mathematische Verfahren werden entdeckt.

Quantenkanal, ein Glasfaserkabel über das die Lichtteilchen gesendet werden können.

„Die Quantenkryptographie nutzt den sonst unerwünschten Effekt, daß jede Messung und jede Störung ein Quantensystem stört.“([16], S.150f) Bewußt wird hier die sonst störende Heisenbergsche Unschärferelation genutzt, daß Größen wie Ort und Impuls oder Energie und Zeit gleichzeitig beliebig genau gemessen werden können. Erfolgt eine Messung, hat dies Einfluß auf das System. Dies wird bei der Quantenkryptographie genutzt, um Lauscher zu entdecken.

Die Quantenkommunikation liefert damit eine Möglichkeit, einen Lauschangriff zu entdecken. Im kombinierten Einsatz mit hybriden Verschlüsselungsverfahren und digitalen Signaturen (siehe Seite 14) würde dies dazu führen, daß

1. Lauscher entdeckt würden,
2. abgehörte Daten nicht lesbar und die verwendeten Schlüssel sicher wären und
3. die Integrität der Daten gesichert wären, daß sie also unverändert sind.

Anwendungen

Grundsätzlich können alle Verschlüsselungsverfahren auf alle Übertragungsinhalte (digitaler Art) angewandt werden, dies ist aber aufgrund technischer Eigenschaft nicht immer praktikabel. RSA für die sichere Übertragung von Telefongesprächen anzuwenden wäre nicht effizient, das 1000mal schnellere, symmetrische DES ist hier aufgrund der großen Datenmengen besser geeignet.

Nicht nur die einzelnen Arten an Übertragungsinhalten können mit Hilfe der Kryptographie gesichert werden, sondern auch die Übertragungswege selber, indem schnelle Verschlüsselungshardware das gesammte Signal in Blöcken vor und nach der Übertragung, zum Beispiel über einen Satelliten, ver- bzw. entschlüsselt.

Nachfolgend werden einige Anwendungen dargestellt, um Möglichkeiten des Einsatzes von Kryptographie aufzuzeigen.

Telefon & Telefax

Telefon- und Telefaxgeräte zur sicheren, verschlüsselten, Übertragung existieren, sind aber nicht weit verbreitet. Sicher ist bei

diesen Geräten allerdings ein relativer Begriff, da abhängig von der Gesetzgebung im Land der Herstellung, nur bedingt sichere Verschlüsselungstechnik verwandt werden darf.

GSM-Mobil-Telefone, die heute Verwendung finden, benutzten Verschlüsselungsverfahren. Seit Jahresbeginn 2000 existiert jedoch ein Verfahren, daß aus der Aufzeichnung eines Gesprächs den hierfür verwandten Schlüssel für dies Verfahren errechnen kann ([2] ,[17]).

E-Mail

E-Mails werden in der Mehrzahl unverschlüsselt übertragen. Populär ist für die Verschlüsselung von E-Mails das Programm PGP von Phil Zimmermann, welches symmetrische Verschlüsselung nach IDEA zum kodieren der Daten, asymmetrische Verschlüsselung zum sicheren Übermitteln des IDEA-Schlüssels verwendet. Der Austausch der öffentlichen Schlüssel kann auf jede erdenkliche Weise geschehen, zum Beispiel Abdruck in Telefonbüchern, Versand per E-Mail oder Weitergabe auf Diskette. Es existieren auch Internet-Server, die - so ähnlich wie Telefonbücher - eine Datenbank mit öffentlichen Schlüssel bereitstellen. Durch die Verwendung dieser Server kann der Austausch eines öffentlichen Schlüssels vor Beginn jeder Kommunikation automatisiert werden, da der entsprechende, zusätzlich durch den Server noch zertifizierte Schlüssel einfach dem Telefonbuch entnommen wird. Durch diese Server wird auch das auf Seite 14 geschilderte Problem des Austauschens von Schlüsseln durch Lauscher weitgehend gelöst[4].

Die E-Mail-Programme Lotus Notes, Microsoft Outlook, Microsoft Outlook Express und Netscape Messenger nutzen ebenfalls ein hybrides Verschlüsselungsverfahren wie PGP. Schlüssel werden im Gegensatz zu PGP dabei nicht selbst, sondern durch eine Zertifizierungsstelle erstellt, deren Schlüssel Sender und Empfänger ebenfalls benötigen. Dadurch wird das Problem des Schlüsselvertauschens durch Lauscher ebenfalls weitgehend gelöst.

Subversion

Subversion ist die Unterminierung der Sicherheit eines Verschlüsselungsverfahrens, indem der ganze Schlüssel oder zu-

4 „weitgehend gelöst“ heißt nichts anderes, als daß zumindest einmal eine Verifizierung der Schlüssel auf nicht-elektronischem Wege erfolgen sollte. Dies geschieht meist einfach dadurch, daß mit der auf einem Datenträger gelieferten Software gleich mindestens ein erster Schlüssel mitgeliefert wird.

mindest Teile davon ausgespäht werden. Bereits Teile eines Schlüssels zu kennen, verringert die Sicherheit dieser Verschlüsselung, da die Anzahl der möglichen Schlüssel kleiner wird, die für einen Angriff (brute force attack) ausprobiert werden müssen. Dies wäre mit einem Lottospiel 6 aus 49 zu vergleichen, bei dem bereits eine, mehrere oder alle gezogenen Zahlen bekannt sind.

Ein Schlüssel, zumindest einen Teil davon, zu erspähen, kann einfach dadurch gelingen, daß er gestohlen wird. Bei asymmetrischen Verschlüsselungsverfahren wird der geheime Schlüssel unbedingt zum Entschlüsseln benötigt. Da dieser unter Verschluß bleiben und in keiner Form übertragen werden sollte, bleibt hier nur der Diebstahl des Datenträgers, auf dem er gespeichert ist.

Symmetrische und Asymmetrische Schlüssel bieten aber auch noch den Ansatz, daß sie zwar prinzipiell die angegebenen Schlüssellängen benutzen, die erzeugten Schlüssel in einem Teilbereich aber immer gleich sind. Wer um diese Teile weiß, hat es einfacher den gesamten Schlüssel zu brechen.
Hierfür ist ein Eingriff in den Programmcode der Verschlüsselungssoftware nötig.

Insbesondere hybride Verschlüsselungsverfahren bieten einen weiteren Angriffspunkt. Bei hybriden Verfahren werden die Daten mit einem symmetrischen Schlüssel kodiert, welcher selber asymmetrisch kodiert versandt wird. Der Angriff besteht nun darin, daß das Verschlüsselungsprogramm mit dem öffentlichen Schlüssel eines Dritten, zum Beispiel eines Geheimdienstes wie der NSA, den symmetrischen Schlüssel oder Teile davon kodiert und an diesen überträgt. Dabei muß keine Datenübertragung im eigentlichen Sinne zu dem ausspähenden Geheimdienst erfolgen, da in der Regel kodierte Daten und kodierte Schlüssel als ein Datenpaket, eine E-Mail, versandt werden. Wird ein derartig kodiertes Datenpaket abgehört, kann der entsprechende Geheimdienst anhand seines geheimen Schlüssels die für ihn bestimmten Schlüsselteile entschlüsseln und die Daten (einfacher) lesbar machen

Eine andere Möglichkeit bilden Verschlüsselungsverfahren, die mit einer zentralen Zertifizierungsstelle oder einem Treuhänder (key escrow/key recovery) arbeiten. Die Subversion besteht dann einfach darin, daß es Möglichkeiten – bekannte, aber vor allem unbekannte - gibt, an die verwandten Schlüssel zu kommen.

Computergestützte Auswertung

Nachdem Zugang zu einem Übertragungsweg besteht und die Signale empfangen werden können, müssen diese nach Kanälen, den unterschiedlichen Übertragungsinhalten und Arten der Botschaften, öffentliche oder vertrauliche, getrennt werden[5]. Kanäle für Radio- und Fernsehübertragungen brauchen, nachdem sie identifiziert worden sind, nicht weiter erforscht zu werden. Bei vertraulichen Telefongesprächen, Telefaxsendung und Datenverbindungen sind diese weiter auszuwerten. (vgl. [9], „technical annexe“)
Die gänzlich manuelle Auswertung aller abgehörten Übertragungsinhalte ist angesichts der heutzutage übertragenen und abgehörten Datenmengen aufgrund des großen Personalbedarfs nicht mehr praktikabel.

Grundsätzlich gibt es zwei unterschiedliche Filtertechniken, die Ausbeute eines oder mehrerer Übertragungswege auszuwerten:

1. Es werden gezielt die Übertragungsinhalte eines bestimmten Senders und/oder Empfängers herausgefiltert und untersucht, oder
2. es werden sämtliche Übertragungsinhalte mit einem oder mehreren bestimmten Merkmalen, meist inhaltlicher Natur, herausgefiltert und untersucht.

Bei einem Angriff nach 1. wird gezielte ein natürliche oder juristische Person ausgeforscht. Die von ihr oder an sie gesendeten Inhalte werden dabei zum Beispiel anhand der Telefonnummer, E-Mail- oder IP-Adresse herausgefiltert und ausgewertet.
Selbst wenn die Inhalte nicht verwertbar sind, bleibt immer noch die Möglichkeit der Verkehrsanalyse, also der Auswertung, wer mit wem kommuniziert. Da bereits die Verkehrsanalyse genügt, um die Vertraulichkeit von Kommunikation zu stören, wird hier nicht weiter zwischen den Inhalten, den diese Filtertechnik liefert und der Verkehrsanalyse unterschieden.

Bei einem Angriff nach 2. werden sämtliche empfangenen Übertragungsinhalte nach dem Inhalt ihrer Botschaft gefiltert. Nur Übertragungsinhalte mit bestimmten Botschaften werden herausgefiltert und zur Auswertung weitergeleitet.
Die Anwendung dieser Filtertechnik hängt von der Art der Übertragungsinhalte ab und hat Vor- und Nachteile, die im Fol-

5 Die Analyse abgehörter Signale und die Umsetzung in verwertbare Kommunikation ist aufwendig, rein technischer Natur und spielt für diese Arbeit keine Rolle. Sieh hierzu [9], Technical annexe, Wideband extraction and signal analysis

genden untersucht werden.

Nachfolgend wird vereinfacht von unverschlüsselten Übertragungsinhalten ausgegangen. Verschlüsselte Inhalte erschweren die nachrichtendienstliche Auswertung, hierauf wird weiter unten eingegangen (s. S. 54).

Telefon

Telefongespräche können zur Zeit nur nach der Filtertechnik 1 ausgewertet werden. Es existieren keine Verfahren, um Sprache schlechter Qualität und ohne vorherige Anpassung der Software an den Sprecher verläßlich in Text umzusetzen, um es anschließend mit Filtertechnik 2 auszuwerten.

Telefax

Telefaxgeräte nutzen die Technik des Telefons zur Datenübertragung und können daher genauso nach Filtertechnik 1 herausgefiltert und zur Auswertung sichtbar gemacht werden.

Eine Auswertung von Telefaxen nach Filtertechnik 2 ist bedingt möglich. Telefaxe sind digitalisierte Bilder. Zumeist werden Bilder von Texten gefaxt. Sofern diese Texte mit der Schreibmaschine oder einem Computer erstellt worden sind, weisen sie ein derart gleichmäßiges Schriftbild auf, daß sie mit OCR-Software (Optical Charakter Recognition) automatisch in Text umgewandelt werden können, der mit Filtertechnik 2 ausgewertet werden kann.
Handschriftlich erfaßte Texte lassen sich mit einer OCR-Software nicht verläßlich in maschinenlesbaren Text umwandeln; die durch Faxgeräte gelieferte geringe Auflösung des Originals erschwert dies weiter.

Gefaxte Bilder entziehen sich einer automatisierten Filterung.

Telexübertragungen sind ihrer Natur nach ohne Probleme auszuwerten, da eine Umwandlung nicht nötig ist.

Daten

Um Daten nach Filtertechnik 1 auswerten zu können, muß ihr Format, die Art und Weise, wie sie dargestellt werden können, bekannt sein oder ausgeforscht werden. Daten bestimmter Empfänger oder Sender können anhand von Merkmalen wie IP- oder E-Mail-Adresse herausgefiltert werden.

Für die Filtertechnik 2 entziehen sich bestimmte Daten der automatisierten Auswertung, Bilder und Töne (Gespräche) lassen sich nicht nach inhaltlichen Kriterien filtern. Gefiltert werden können auch nur Daten, deren Format bekannt ist. Ebenso wie für Filtertechnik 1 ist aber hier die große Standardisierung der Datenformate hilfreich. Alle Übertragungsinhalte, die auf Texten basieren, verwenden als Grundlage eine Kodierung für Buchstaben und Zeichen nach dem ASCII-Code (American Standard Coder for Information Interchange). Dies genügt für eine erste Filterung. Per E-Mail übers Internet - auch mit Hilfe der Internetübertragungsprotokolle HTTP (HyperText Transport Protocoll) und FTP (File Transport Protocoll) - versandte Dateien können, sofern es sich um gängige Formate handelt, ihren Inhalten nach gezielt ausgewertet werden.

Filter

Die zur automatisierten Auswertung verwendete Filtertechnik 2 bietet den Vorteil, daß sie sehr schnell, sehr viele Übertragungsinhalte auswerten kann. Die inhaltliche Auswertung, die Filterung nach vorkommenden Zeichenfolgen, geschieht anhand von Wortlisten. Kommt entweder eine Wort oder eine Kombination von Worten in einem Übertragungsinhalt vor, so wird dieser herausgefiltert und einer weiteren Auswertung zugeführt.

Das hauptsächliche Problem besteht darin, daß die Filtersoftware die nötige „Intelligenz“ besitzt, die gewünschten Übertragungsinhalte anhand ihrer Botschaften herauszufiltern. Ein Beispiel soll dies verdeutlichen:

Alle E-Mails, die das Wort Tornado umfassen, können kaum von Interesse sein. Das Wort Tornado kommt in diesem Text vor, aber auch in zahlreichen E-Mails des mittleren Westens der USA, wo Tornados ein Wetterphänomen darstellen. Wiederum handelt es sich bei Tornados um einen europäischen Kampfjet. Taucht Tornado in Verbindung mit dem Wort „Saudi-Arabien“ auf, könnte es sich durchaus um eine geheimdienstlich interessante Botschaft handeln, wenn es sich um die Lieferung von Kampfjets des Typs Tornado an Saudi-Arabien handelt. Es kann aber auch sein, daß die E-Mail schlicht von einem Segelturn nach Saudi-Arabien mit einem Schiff namens „Tornado“ handelt.

Software, die Filtertechnik 2 anwendet, hilft vor allem, die Menge der auszuwertenden Daten zu reduzieren, die durch Personal ausgewertet werden muß. Angesichts der Datenflut, die

über die Vielzahl der Übertragungswege zur Verfügung stehen kann, ermöglicht sie aber überhaupt erst wieder die effektive Arbeit des Abhörens jenseits der Möglichkeiten von Filtertechnik 1.

„One [unidentified] intelligence collection system alone can generate a million inputs per half hour; filters throw away all but 6500 inputs; only 1000 inputs meet forwarding criteria; 10 inputs are normally selected by analysts and only one report is produced. These are routine statistics for a number of intelligence collection and analysis systems which collect technical intelligence.“ (William Studemann, ehemaliger NSA-Direktor, zitiert nach [9], S. (v))

Echelon

Echelon bezeichnet einen seit den 1970ern existierenden geheimen Verbund an Abhöranlagen, der am UKUSA-Abkommen beteiligten Staaten zur automatisierten Auswertung nicht-militärischer Übertragungen. Von Forschern wurde es bereits in den 1970ern entdeckt, ein 1996 erschienenes Buch ([12]) lieferte umfassende Details dazu. Seit einer Studie im Auftrag des Europäischen Parlamentes ([23]) wurde das Thema im Parlament und der europäischen Öffentlichkeit behandelt, als Folge entstanden weitere Studien zum Echelon-Komplex ([11]).

UKUSA

Die UKUSA-Allianz geht auf einen über mehr als 40 Jahre geheimen Vertrag aus dem Jahre 1947 zurück. In diesem Vertrag kommen die USA und Großbritannien überein, sich gegenseitig die Nutzung ihrer Anlage zur Signalaufklärung freizugeben. Aus der zunächst gegen die Sowjetunion gerichteten Überwachung von Signalen, wie sie bei der Radaraufklärung dieser anfallen, wurde schließlich ein Vertrag zur Kommunikationsüberwachung. Erweitert wurde diese Allianz um die Staaten Australien, Kanada und Neuseeland.

Die am UKUSA-Abkommen partizipierenden Staaten können die von den teilnehmenden Abhöranlagen jedes Mitgliedslandes gewonnen Daten zur eigenen Auswertung anfordern; es gehört zur Vereinbarung, daß die Ausspähung nicht gegen juristische und natürliche Personen eines Mitgliedslandes gerichtet sein darf, Ausnahmen gibt es nur im Rahmen der Strafverfolgung.

Die Existenz der UKUSA-Allianz wurde erst im März 1999 bestätigt, nachdem die neuseeländische Regierung offiziell zugab, daß ihr Nachrichtendienst im Rahmen des UKUSA-Abkommens mit anderen Nachrichtendiensten kooperiert.(vgl. [9], S. 1)

Einrichtungen

„Das ECHELON-System gehört zum UKUSA-System, aber im Gegensatz zu vielen elektronischen Spionagesystemen, die während des zweiten Weltkrieges entwickelt wurden, wurde ECHELON hauptsächlich für nichtmilitärische Zielgruppen entworfen: Regierungen, Organisationen und Unternehmen in praktisch allen Ländern. Das ECHELON-System zapft wahllos sehr große Menge von Verbindungen an und wertet dann durch

künstliche Intelligenz wie Memex zum Auffinden von Schlüsselwörtern die wertvollen Informationen aus. Fünf Staaten können die Ergebnisse nutzen, wobei gemäß dem UK/USA-Abkommen von 1948 die USA der Hauptpartner sind und Großbritannien, Kanada, Neuseeland und Australien eine untergeordnete Position einnehmen.

Alle fünf Zentren stellen den anderen vier Partnern „Wörterbücher" der Schlüsselworte, Sätze und Personen und anzuzapfende Anschlüsse zur Verfügung, und die angezapfte Verbindung wird sofort an das Land weitergeleitet[6], daß den entsprechenden Antrag gestellt hat." ([24], S. 8)

Welche Übertragungswege abgehört und durch Echelon ausgewertet werden, hängt von den Möglichkeiten und der gerade getroffenen Auswahl ab. Es sind nicht ausreichend Kapazitäten vorhanden, alle anzapfbaren Übertragungswege gleichzeitig abzuhören. Dies scheint auch nie möglich zu werden, da der Aufwand hierfür ökonomisch und politisch nicht zu rechtfertigen sein wird. Angesichts der Kosten der Ausspähung ist davon auszugehen, daß sich der gezielte Einsatz von Abhöranlagen an den wichtigsten nationalen Zielen orientiert, was aber Nebenprodukte, Zufallserkenntnisse, zweitrangiger Ziele nicht ausschließt.

Nachfolgend eine Aufstellung der Abhöranlagen, die von den Staaten der UKUSA-Allianz unterhalten werden (vgl [9], S. 5ff):

Seit 1945 erhielten die NSA und ihrer Vorläuferorganisationen Zugang zu Gesprächen von den großen amerikanischen Telefongesellschaften. Die mit dem Codewort SHAMROCK bezeichneten Aktivitäten wurden 1975 durch die Watergate-Affäre offengelegt.(vgl. [9], S. 5)
Inwieweit Zugang zu den transatlantischen Tiefseekabeln besteht, die über Menwith Hill (England) laufen, wo sich auch eine große Abhöranlage der NSA befindet, die in Kooperation mit dem britischen GCHQ betrieben wird, konnte nicht geklärt werden.

Antennenanlagen mit einem Durchmesser von 400 Metern betrieben Großbritannien und die USA in Schottland von 1945 bis in die 1980er, um europäische HF-Radiowellen-Kommunikation abzuhören. Derartige Antennenanlagen wurden installiert in San Vito dei Normanni (Italien), Chicksands (England), Kirknetown (Schottland), Menwith Hill

6 Zur Weiterleitung der hierbei anfallenden großen Datenmengen wird im Rahmen der UKUSA-Allianz ein Netzwerk mit den benötigten Übertragungskapazitäten unterhalten. (vgl. u.a.[9], S. 10)

(England), Ayios Nikolaos (Zypern) und Karamursel (Türkei); die Anlage in Vint Hill Farms (Virginia, USA) wurde von den USA zusätzlich genutzt, um Ziele in Großbritannien abzuhören.(vgl. [9], S. 5f)

Die USA unterhalten seit 1968 Satelliten zum Abören von Kurzwellenfrequenzen, insgesamt 11, 7 der CANYON-Klasse, 4 der VORTEX/MERCURY-Klasse. (siehe [9], S. 6)
Weitere Satellitenflotten existieren, um schwächere Signale abzuhören, zum Beispiel CB-Funk oder Mobiltelefone (siehe [9], S. 7); Satelitten für letztere Ziele unterhält ausschließlich die USA, Kapazitäten werden aber auch an Großbritannien vermietet.
Die wichtigste Bodenstation der Satelliten ist Menwith Hill (England), weitere Bodenstationen für einige Satellitenflotten sind Buckley Field, Denver (beide in Colorado, USA), Pine Gap (Australien) und Bad Aiblingen (Deutschland).

„It follows that, within contraints imposed by budgetary limitation and tasking priorities, the United States can if it chooses direct space collection systems to intercept mobile communications signals and microwave city-to-city traffic anywhere on the planet. The geographical and processing difficulties of collecting messages simultaneously from all parts of the globe suggest strongly that the tasking of these satellites will be directed towards the highest priority national and military targets. Thus, although European communications passing on inter-city microwave routes can be collected, it is likely that they are normally ignored. But it is very highly probable that communications to or from Europe and which pass through microwave communications networks of Middle Eastern states are collected and processed.“(Hervorhebung im Original, [9], S. 7)

Zum Abhören von Satelliten unterhält die UKUSA-Allianz zur Zeit circa 120 Systeme, 40 sind auf westliche Kommunikationssatelliten gerichtet, 50 dienten der Ausspähung sowjetischer Kommunikationssatelliten und dienen inzwischen ggf. anderen Zwecken und weitere 30 sind für weitere Zwecke der Signalaufklärung vorgesehen.
Standorte für diese Anlagen sind Morwenstow (Cornwall, England), Yakima (Washington, USA), Sugar Grove (West Virgina, USA), Sabana Sece (Puerto Rico, USA), Leitrim (Ontario, Kanada), Kojarena (Australien) und Waihopai (Neuseeland); kleinere Standorte sind Misawa (Japan), Cheltenham (England) und Shoal Bay (Australien). (vgl. [9], S. 8)
Zahlreiche Einrichtungen des Echelon-Komplexes speziell zum Abhören von Kommunikationssatelliten sind von Dun-

can Campell als solche indentifiziert worden. Die größten Anlagen hierzu sind (nach [8], vgl. auch [13], S. 44):

Menwith Hill, Yorkshire (Großbritannine)

Bad Aiblingen, Bayern (Deutschland)

Denver, Colorado (USA)

Pine Gap, Alice Springs (Australien)

In den achtziger Jahren, nachdem endgültigen Beitritt aller UKUSA-Staaten zum Echelon-Verbund, wurden diese um Anlagen in Perth (Australien) und Waihopai (Neuseeland) erweitert.[7]

Sowjetische Tiefseekabel wurden durch us-amerikanische U-Boote mit der oben beschriebenen Technik (siehe Seite 7) erfolgreich abgehört; eine enttarnte Anlage läßt sich im Moskauer KGB-Museum besichtigten.
In den 80ern haben die USA ihre diesbezüglichen Aktivitäten in den Mittelmeerraum verlagert, wo Kabel zwischen Europa und Westafrika verlaufen. Weitere Ziele werden im Nahen Osten, in Ostasien und Südamerika vermutet. Die USA ist die einzige Seemacht von der bekannt ist, daß sie über die nötige Technik zum Abhören von Tiefseekabeln verfügt. (vgl. [9], S. 9f)

Für das Abhören von Daten, insbesondere den geheimdienstlich interessanten, prozentmäßig geringen Anteilen, die über das Internet übertragen werden, gibt es wieder zwei Möglichkeiten: Zum einen können die Übertragungswege abgehört werden, zum anderen - wesentlich einfacher - in Zusammenarbeit mit den Betreibern. Für letzteres setzt die NSA sogenannte Sniffer-Software an 9 wichtigen Internetaustauschpunkten, an denen die unterschiedlichen Netzwerkteile miteinander verbunden sind, ein.
Technisch bedingt und ökonomisch sinnvoll laufen durch diese Punkte auch große Menge an Daten, deren Ursprung und Ziel in Europa liegt. (vgl. [9], S. 10f)

7 Auch andere Staaten unterhalten derartigen Einrichtungen. Außerhalb der UKUSA-Allianz unterhalten Deutschland (BND) und Frankreich (DGSE) Anlagen zum gleichen Zweck in Kourou (Guyana), Frankreich allein in Dordogne (Frankreich), in Neukaledonien und in den Vereinigten Arbaischen Emiraten. Der Schweizer Geheimdienst plant den Bau zweier Anlagen. (vgl.[9], S. 8)

Austauschpunkt	*Ort*	*Betreiber*
FIX East	College Park, Maryland	US Regierung
FIX West	Mountain View, California	US Regierung
MAE East	Washington, D.C.	MCI
New York NAP	Pennsauken, New Jersy	Sprintlink
SWAB	Washington, D.C.	PSInet / Bell Atlantic
Chicago NAP	Chicago, Illinois	Ameritech / Bellcorp
San Francisco NAP	San Francisco, California	Pacific Bell
MAE West	San Jose, California	MCI
CIX	San Jose, California	CIX

Tabelle 1 NSA Internetzugangspunkte (1995) (nach [9], S. 11)

Mißbrauch

Alle am UKUSA-Abkommen partizipierenden Staaten gestatten es ihren Geheimdiensten oder bestimmten Ministerien Aufträge zum Sammeln wirtschaftlicher Informationen zu erteilen, die im Rahmen von Echelon verarbeitet werden können.

Diese Aufträge, wirtschaftliche Daten zu sammeln, können dafür bestimmt sein

- die Verhandlungspositionen anderer Staaten bei Handelsvereinbarungen ausfindig zu machen,
- zukünftige Entwicklungen und Preise abzuschätzen,
- den illegalen Handel mit kritischen Gütern, zum Beispiel Kriegsgerät, aufzudecken, oder
- die wirtschaftliche Situation anderer Staaten zu untersuchen.

Aufträge dieser Art, aber nicht nur diese, produzieren Informationen von direktem wirtschaftlichen Belang (vgl. [3] S. iv). Die Entscheidung, ob derartige Informationen, zum Beispiel Angebote in Ausschreibungen, verwendet, also weitergegeben werden, obliegt allein den verantwortlichen Auftraggebern, politischen Entscheidungsträgern.

Im Rahmen des Echelon-Systems oder des UKUSA-Abkommens scheint es nicht möglich zu sein, daß Firmen die Geheimdienste beauftragen, Informationen mit direktem wirtschaftlichen Belang für sie zu sammeln. (vgl. [3], Technical File S. iv)

Seit 1993 ist für die USA und für Großbritannien ab 1994 die Einrichtung von Komitees nachweisbar, die die Verwertung von Informationen wirtschaftlichen Belanges koordinieren. (vgl. [9] S.17f., [19], [3], Technical File S. iv f.)[8]

Zusammenfassung

Mit Echelon ist ohne wirksame Verschlüsselung in Bezug auf die Staaten der Europäischen Union grundsätzlich folgendes möglich, was aber nicht zu jeder Zeit stattfindet:

jede Satellitenübertragung von, nach oder innerhalb der EU abzuhören,

jede Funkverbindung von, nach oder innerhalb der EU abzuhören,

jedes Tiefseekabel von und nach Europa anzuzapfen,
(bezüglich Glasfaserkabel ist dies ohne Kooperation der Betreiber weniger wahrscheinlich)

Kabelverbindungen innerhalb der EU, zumindest insofern sie nicht über britisches Territorium führen, scheinen sicher zu sein.

Bezüglich folgender Übertragungsinhalte bedeutet dies:

Kein Telefonat mit Ziel und/oder Start in der Europäischen Union ist sicher vor Abhörung, da

die von Mobiltelefonen emittierten Radiowellen abgehört werden können (siehe S. 9),

Telefongespräche, vor allem Ferngespräche, teilweise über Satelliten laufen, da dies billiger ist, preiswertere Leitungen gerade belegt sind oder diese als Datenverbindungen realisiert wurden, also per Internet übertragen werden.[9]

Kein Telefax ist sicher vor Abhörung, da hierfür das gleiche wie für Telefonate gilt.

Keine E-Mail, keine Übertragung des Internets, ist sicher, da hier die Wahrscheinlichkeit sehr hoch liegt, daß sämtliche Daten oder Teile davon Übertragungswege über die USA oder abhörbare Übertragungswege wie für Telefonate und Telefaxe aufgeführt nehmen.

8 Verwiesen sei hier auch bereits auf die aus Seite 48 wiedergegeben Aussage des ehemaligen CIA-Direktors Woolsey.

9 Dies Internetrouting von Telefongesprächen wird derzeit nur von wenigen Privatleuten, Firmen mit Standleitungen verwendet; die Deutsche Post AG testet zur Zeit in einem Pilotprojekt das Routing von „normalen“ Gesprächen via Internet.

Insbesondere besteht also mit Echelon potentiell die Möglichkeit unverschlüsselte, innereuropäische Übertragungsinhalte abzuhören, wenn diese nicht ausschließlich über erdgebundene Kabelverbindungen übertragen werden.
Es stellt sich daran anschließend die Frage nach durch die Betreiber definierten Zielen von Echelon, welche Erkenntnisse gesammelt werden und was mit sogenannten Zufallserkenntnissen geschieht.

Rechtslage

Privatsphäre

Die Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) hat in allen Staaten der Europäischen Union Gesetzeskraft. Artikel 8 lautet:

[Gebot der Achtung der Privatsphäre]

(1)Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs.

(2)Der Eingriff einer öffentlichen Behörde in die Ausübung dieses Rechts ist nur statthaft, insoweit dieser Eingriff gesetzlich vorgesehen ist und eine Maßnahme darstellt, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutze der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist.

Im Einklang mit der universellen Erklärung der Menschenrechte und der verbindlichen UN-Konvention der Bürger- und politischen Rechte schützt die EMRK natürliche Personen vor ungesetzmäßigem Abhören; inwieweit dies auch für juristische Personen gilt, ist umstritten. (vgl. [10])

Weiterhin ist in der Konvention des Europarates zum Datenschutz festgesetzt, daß angemessene Maßnahmen zum Schutz persönlicher Daten gegen unbefugten Zugriff getroffen werden müssen.[10]

Direktive 95/46/EG - Präambel (2)

(2) Die Datenverarbeitungssysteme stehen im Dienste des Menschen; sie haben ungeachtet der Staatsangehörigkeit oder des Wohnortes der natürlichen Personen, deren Grundrechte und Freiheiten und insbesondere deren Privatsphäre zu achten und zum wirtschaftlichen und sozialen Fortschritt, zur Entwicklung des Handels sowie zum Wohlergehen der

10 Zum gesamten Themenkomplex Datenschutz in der EU können im Zusammenhang mit der EMRK und der EU-Datenschutzrichtlinie noch aufgeführt werden:
Council Resolution on the lawful interception of telecommunications - Council Resolution OJ 4/11/96 C329 pages 1-6, und die Direktive 97/66/EC, die zweite EU-Richtlinie zum Datenschutz , im Vergleich zur Direktive 95/46/EC die Päambel und Artikel.
Nach Meinung des Autors liefern diese aber keine neuen, weiteren, Erkenntnisse.

Menschen beizutragen

Direktive 95/46/EG - Artikel 1 Gegenstand der Richtlinie

(1) Die Mitgliedsstaaten gewährleisten nach den Bestimmungen dieser Richtlinie den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten.

Es besteht in den Mitgliedsstaaten der Europäischen Union

ein Schutz vor unrechtmäßigem Abhören und

ein Gebot zum Schutz von Daten und Kommunikation vor Zugriffen Dritter, es sei denn im Interesse der Strafverfolgung,

die Pflicht, das vorgenanntes für alle Menschen „ungeachtet der Staatsangehörigkeit und des Wohnortes“ gilt, und

eine Übereinkunft, daß die Betreiber von Kommunikationsanlagen diese derartig konstruieren und betreiben sollen, daß ein unbemerktes Abhören standardisiert möglich ist[11].

Tabelle 2 gibt eine Übersicht über die unterschiedliche Gesetzgebung in den EU-Mitgliedsstaaten bzgl. des Schutzes von Daten und Kommunikation, sofern sich die einzelnen Rechte und Pflichten dieser Vorschriften vergleichen lassen
('X' bedeutet dabei, daß ein Schutz gegeben ist, '-' bedeutet, daß keine Schutz gegeben ist, ein leeres Feld bedeutet, daß kein sicherer Schutz gegeben ist, aber auch keine eindeutige Verneinung möglich ist.)

Aufgrund der EU-Richtline zum Datenschutz haben alle Staaten inzwischen zumindest einen, wenn auch geringen und nicht unbedingt strafbewährten, Schutz gegen unrechtmäßiges Abhören. Diesen Schutz persönlicher Daten, welcher nicht immer für juristische Personen gilt, bezieht sich im Beispiel Portugals fast gar nicht auf den Schutz von Kommunikation.

Rechtmäßige Abhörung ist dort, wo Abhören allgemein verboten ist, aus unterschiedlichen Gründen zulässig: zur Strafverfolgung (siehe Tabelle 2 auf Seite 39), zum Zwecke der nationalen Sicherheit (z.B: Großbritannien und Griechenland) oder der Wohlfahrt des Staates (Großbritannien).

11 Dies ist kein Resultat aus den aufgeführten Konventionen oder Richtlinien, sondern aus einer Übereinkunft des Rates. Der Punkt dient mehr der Vollständigkeit und spielt in dieser Arbeit eine untergeordnete Rolle.

	Daten-schutz	*Korres-pondenz-geheimnis*	*Schutz-maßnah-men der Betreiber*	*Abhörung für Straf-verfol-gung*	*Abhör-hilfe der Betreiber*	*Ver-schlüsse-lung*
Großbrit.	X	X	X	X	-	X
Österreich	X	X	-*	X	X	X
Belgien	X			X		X
Dänemark	X	X	X			X
Finnland	X	X		X	X	X
Frankreich	X	X		X		X**
Deutschland	X	X	X	X	X	X
Griechenland	X	X		X		X
Irland	X	-	-	-	-	X
Italien	X		-	-	-	X
Luxemburg	X	-	-	-	-	X
Niederlande	X		X			X
Portugal	X	-	-	-	-	X
Schweden	X	X		X		X
Spanien	X		X	-	-	X

Tabelle 2 Gesetzgebung der EU-Staaten (vgl. 66, S. 8f)

Vereinigte Staaten

Abhören ist in den USA generell verboten, wird von den meisten Staaten zum Zwecke der Strafverfolgung jedoch erlaubt.

Zum einen existieren Gesetze (ECPA), die das Abhören zum Zwecke der Strafverfolgung oder nationalen Sicherheit unter bestimmten Voraussetzungen, u.a. einer richterliche Genehmigung, zulassen; Betreiber von Kommunikationseinrichtungen sind gehalten, die Institution der Strafverfolgung bei ihrer Arbeit zu unterstützen. Zum anderen existiert eine Gesetzgebung (FISA), die das Abhören ausländischer Mächte und Agenten im Sinne der nationalen Sicherheit zuläßt; die abgehörten Ziele

* Österreich verpflichtet die Betreiber nicht, Schutzmaßnahmen vor unrechtmäßigem Lauschen zu treffen, sondern die Benutzer müssen vor der Benutzung ungeschützter Übertragungswege gewarnt werden.

** In Frankreich war bis Januar 1999 die Verwendung von Verschlüsselungsverfahren stark eingeschränkt.

müssen dabei in keiner Verbindung zu einem Verbrechen stehen.

Das Abhören im Rahmen letzerer ist an zwei Bedingungen geknüpft:

- Kommunikation von US-Bürgern in den USA darf nur mit richterlicher Genehmigung und
- nicht-sprachliche Kommunikation unter alleiniger Kontrolle einer ausländischen Macht darf nur mit präsidentieller Genehmigung

abgehört werden.

Zusammenfassung

Die Menschen- und Bürgerrechte, insbesondere die EMKR, schützen vor unrechtmäßigem Abhören. Rechtmäßiges Abhören wird meist im Rahmen eines vorgeschriebenen Verfahrens genehmigt. Es besteht Bedarf nach Hilfe der Betreiber von Kommunikationsanlagen bei der Strafverfolgung.

Weitgehend ist Verschlüsselung zulässig, insbesondere für den elektronischen Zahlungsverkehr. Die meisten Staaten der EU verpflichten die Betreiber von Kommunikationsanlagen, Vorkehrungen zum Schutz vor unrechtmäßigem Abhören zu treffen.

Klar sind die Regeln des Lauschens, wenn es um das Abhören von Bürgern und im Rahmen des eigenen Staates geht. Weniger klar sind die Positionen, wenn es um das Abhören durch ausländische Mächte geht.

Das Abhören von Kommunikation zweier Personen in einem Land durch eine dritte Person in einem anderen Land scheint solange eindeutig verboten zu sein, wie diese Kommunikation die Länder beider nicht verläßt. Sollte das Abhören aber im Land des Dritten rechtmäßig sein, so ist das Abhören immer noch nicht rechtmäßig im Lande der beiden Abgehörten, solange der Dritte nicht die Erlaubnis im Rahmen des dort vorgeschriebenen Verfahrens hat.

Befindet sich der vorgenannte Dritte in den USA (FISA) oder in Großbritannien (IOCA), so kann dieses Abhören dort legal sein; bei Großbrittannien muß aber wieder auf die zitierte Präambel der Direktive 95/46/EG hingewiesen werden.

Wie vorher gezeigt wurde, haben einige Staaten die technischen Fähigkeiten und Kapazitäten, um Kommunikation innerhalb

anderer Länder abzuhören. Auch benutzen Daten und Kommunikation auf ihrem Weg von einem Punkt eines Staates zu einem anderen oft Übertragungswege, die über ein drittes Land führen, ohne daß dies Sender oder Empfänger bemerken. Letzteres findet im Rahmen des Datenverkehrs im Internet technisch und ökonomisch bedingt häufig statt (vgl. [9], S. 10f).

UKUSA & EU

„Zu jeder außen- und sicherheitspolitischen Frage von allgemeiner Bedeutung findet im Rat eine gegenseitige Unterrichtung und Abstimmung zwischen den Mitgliedsstaaten statt, damit gewährleistet ist, daß ihr vereinter Einfluß durch konvergierendes Handeln möglichst wirksam zum Tragen kommt.“ (Amsterdamer Vertrag, Artikel 16[12])

Das EU-Mitgliedsland Großbritannien unterhält sogenannte „besondere Beziehungen“ (special relations) zu den USA, die geschichtlich auf Zeiten vor dem EU-Beitritt Großbritanniens zurückgehen. Im Rahmen dieser besonderen Beziehungen zu den USA ist auch das UKUSA-Abkommen einzuordnen.

Im Bereich des UKUSA-Abkommen kann Großbritannien keine offenen Anhörungen im Rat, im Kreise mit den Vertretern der anderen EU-Mitgliedsländer, durchführen. Großbritanniens Verpflichtungen im Rahmen der besonderen Beziehungen zu den USA, insbesondere die Information über die Existenz des UKUSA-Abkommens und des Echelon-System, verstoßen gegen die vertraglichen Verpflichtungen des Maastrichter und Amsterdamer Vertrages.

Großbritannien ist zwei gegensätzliche Verpflichtungen eingegangen: Über die Informationspflicht bzgl. der Existenz des UKUSA-Abommens und Echelon können diese Vertragsverletzungen weitergehend sein. So stehen sie zum Beispiel auch im Widerspruch zum Schutz der persönlichen Daten im Sinne der Datenschutzrichtlinien der EU (siehe S. 37, vgl. auch [18]).[13]

Der ehemalige deutsche EU-Kommisar Martin Bangemann erklärte hierzu am 14. September 1998 vor dem EU-Parlament:

„Denn wenn das System bestünde, wäre das natürlich eine flagrante Verletzung von Rechten, Individualrechten der Bürger und selbstverständlich auch ein Angriff auf die Sicherheit der Mitgliedsländer. Das ist

12 Ex-Artikel J.6 des Maastrichter Vertrages

13 Die Beteiligung oder Beihilfe zu verbotener Industrie- und Wirtschaftsspionage stellt einen weiteren Aspekt dar.

vollkommen klar. In dem Moment, in dem sich so etwas offiziell bestätigt, müßten der Rat und natürlich auch die Kommission und das Parlament darauf reagieren.“

Es ist offensichtlich, daß sich das Vereinigte Königreich in einem Loyalitätskonflikt zwischen der EU und den USA (UKUSA) befindet.

Interessenlagen

Drei Interessen lassen sich identifizieren, die die politische Diskussion um die Zulässigkeit und Schwierigkeit von Abhöraktivitäten bestimmen, die im Folgenden behandelt werden. Alle drei Interessen haben unterschiedliche Forderungen bezüglich Abhörmöglichkeiten, die untereinander kollidieren. Welche Interessen wichtiger sind und wo Kompromisse geschlossen werden müssen, ist eine politische Entscheidung.

Die Debatte innerhalb der Europäischen Union ist wesentlich von der Art der Beziehungen zu den Vereinigten Staaten geprägt.

Privatsphäre

Der Schutz der Privatsphäre gehört zu den Menschen- und Bürgerechten. Die rechtlichen Probleme bzgl. Korrespondenz, dem Überwachen dieser und teilweise inwieweit das Abhören bzgl. der EU-Mitgliedsstaaten sanktioniert ist, wurde bereits geschildert (siehe S. 37ff).

Der Schutz der eigenen Korrespondenzen, von Übertragungsinhalten jeglicher Art, erfordert es, daß die Übertragungsinhalte nicht abgehört werden können. Daß dies für die meisten Übertragungsinhalte nicht zu erkennen und abhängig vom verwandten Übertragungsweg ist, dessen genaue Wahl aber nicht einer bewußten Entscheidung des Sender liegt, wurde ebenfalls dargelegt.

Wenn also nicht garantiert ist, daß ein Übertragungsinhalt nicht abgehört werden kann, dann hilft nur Verschlüsselung. Hiermit besteht die Möglichkeit, daß die abgehörten Daten keinerlei Nutzen haben.

Verschlüsselung kann dabei an zwei Stellen ansetzen:

- Die Übertragungsinhalte können direkt vom Sender verschlüsselt werden, der Empfänger muß sie dann wieder entschlüsseln.
- Die Übertragungsinhalte werden vor der Übertragung durch die Betreiber vermeintlich unsicherer Übertragungswege verschlüsselt.

Der erste Weg besticht durch die Möglichkeit, daß der Urheber einer Botschaft die volle Kontrolle über die Verschlüsselung hat,

sofern das von ihm verwandte Verschlüsselungsverfahren sicher oder nicht durch Subversion unbrauchbar ist (siehe S. 22).

Der zweite Weg besticht durch seine Einfachheit für die Urheber von Übertragungsinhalten, da diese auf jeden Fall durch die Betreiber von Übertragungswegen gesichert werden. Dies gewährt aber dann keinen Schutz gegen Abhören, wenn dies in Kooperation mit dem Betreiber - für geheimdienstliche Zwecke oder im Interesse der Strafverfolgung - geschieht. Fraglich ist auch die Überprüfung dieser Verschlüsselung für den Benutzer, da sie den unterschiedlichen nationalen Gesetzgebungen der Betreiber unterliegen. Ein schwaches Glied in der Kette der Übertragungswege genügt, um die Übertragungsinhalte abzuhören.

Der letztgenannte Weg der Verschlüsselung von gesamten Übertragungswegen besticht aber zusätzlich durch den Umstand, daß er mehr leistet als der erste: Ersterer ermöglicht trotz Verschlüsselung die Anwendung von Filtertechnik 1 (siehe S. 24), was zweiterer durch die Verschlüsselung sämtlicher übertragenen Daten verhindert, da die nötigen Meta-Informationen (Telefonnummer, IP-Adresse, E-Mail-Adresse etc.) mitverschlüsselt werden.

Sollte die für den ersten Weg verwendete Verschlüsselung - wenn auch nur mit großem Aufwand - zu brechen sein, dann bietet diese Art der Verschlüsselung keinerlei Schutz gegen die gezielte Ausspähung einzelner.

Letztgenannter Weg erfordert einen vermehrten finanziellen und technischen Aufwand von den Betreibern von Übertragungswegen, da zusätzliche Verschlüsselungshardware benötigt wird, während dies bei ersterem auf die Nutzer abgewälzt wird.

Strafverfolgung

Es muß zwischen geheimdienstlichen Abhöraktivitäten und Abhörmaßnahmen im Interesse der Strafverfolgung unterschieden werden. Geheimdienstliche Abhöraktivitäten richten sich - meist mit Ausnahme der eigenen Bürger - gezielt gegen einzelne Gruppen und ganze Nationen, ohne daß eine Verbindung mit einer Straftat vorliegt oder eine richterliche Genehmigung einzuholen ist; allein das Potential einer möglichen Gefährdung reicht aus, geheimdienstliche Aktivitäten zu rechtfertigen. Verschlüsselung erschwert diese Aktivitäten, wenn es sie nicht sogar vollständig unmöglich macht.

Effektive Verschlüsselungsverfahren, die den Institutionen der Strafverfolgung keine Möglichkeit des Abhörens lassen, können nicht im Interesse der Strafverfolgung sein. Im Interesse der Strafverfolgung sind daher Verfahren, die in Kooperation mit den Betreibern von Übertragungswegen umgangen werden können oder bei denen ein Zweitschlüssel vorliegt, zudem die Organe der Strafverfolgung (unbemerkt) Zugang erhalten können. (siehe S.22)

Im Interesse der Strafverfolgung liegt es daher nahe zu fordern,

daß Verschlüsselung generell verboten wird,

daß Verschlüsselung nicht zu stark sein darf,
also die Schlüssellänge (siehe S. 15) beschränkt werden muß,
oder

daß Verschlüsselungsverfahren einen Zweitschlüssel für Zwecke der Strafverfolgung liefern müssen.

Strafverfolgung ist eine Sache, die Bürger vor Straftaten zu schützen eine andere. Jegliche Beschränkung in der Verwendung von Verschlüsselung führt dazu, daß für wenige Fälle der Strafverfolgung alle Bürger gefährdet werden. Eine Beschränkung von Verschlüsselung macht die Urheber von Botschaften zu potentiellen Opfern.

Eingeschränkt wirksame Verschlüsselungsverfahren mögen für Privatpersonen in der Regel nicht zu brechen sein, da dies je nach Stärke des Verfahrens den Einsatz von immer größeren Ressourcen, also Geld, Zeit und Rechnerkapazität, bedeutet. Organisierte Kriminalität, Geheimdienste und selbstverständliche die Organe der Strafverfolgung, in deren Sinne eine derartige Beschränkung wäre, wären aber als gleichstark beim Schlüsselbrechen einzuschätzen.

Gleiche Einschätzungen treffen auf unterschiedliche Konzepte für den Umgang mit Zweitschlüsseln zu. Genügt es, einen einzigen Generalschlüssel zu brechen oder zu erhalten, ist kein wirklicher Schutz gegeben (vgl. auch 22f.).

Zuletzt muß dringend davor gewarnt werden, Kalküle zu verwenden, die darauf beruhen, daß Straftäter Gesetze in bezug auf Verschlüsselung beachten würden. Potentielle Straftäter sind durchaus in der Lage

sichere Verschlüsselungsverfahren illegal aus dem Ausland oder einfach dem Internet zu besorgen,

einfach Daten doppelt zu verschlüsseln,

sicher verschlüsselte Daten mit einer weiteren unsicheren Verschlüsselung zu tarnen, und/oder

Steganographie[14] zu verwenden.

Mit diesen vier Punkten erweist sich eine Diskussion um Verschlüsselungsbeschränkungen im Interesse der Strafverfolgung als ein Scheingefecht, da es viel einfachere Wege gibt, Übertragungsinhalte den Augen der Strafverfolgung zu entziehen.
Weiterhin gibt es für die Strafverfolger noch andere technische Möglichkeiten, an die Inhalte von Kommunikation zu gelagen. Beispielhaft seien der Einsatz von sogenannten Wanzen, Trojanischen Pferden und Geräten, die die Induktionen von Computern auswerten, genannt.

In seinem Bericht für das Europäische Parlament führt Duncan Campell Hinweise für einen Täuschungsversuch der USA gegenüber den EU-Staaten an, wo diese überredet werden sollten, im Interesse der Strafverfolgung ein Treuhänderverfahren zur Schlüsselverwaltung und –wiederbeschaffung (key recovery), das eigentliche Interesse habe laut Campbell aber nicht bei den us-amerikanischen Strafverfolgungsbehörden sondern der NSA gelegen ([9], S.15); ähnliche Ziele verfolgte auch eine Initiative zur legalen Beschränkung der maximalen Schlüssellänge.

Mit dem Kurswechsel Frankreichs in Richtung Freigabe der Verschlüsselung scheint sich die Entwicklung aber unumkehrbar gegen die schwache Argumentation zugungsten der Strafverfolung gewandt zu haben. Tabelle 2 auf Seite 39 zeigt hierzu deutlich, daß die Verwendung von Verschlüsselungsverfahren in keinem Mitgliedsland der EU mehr beschränkt ist.

e-commerce

Elektronischer Handel und elektronischer Zahlungsverkehr, hier einfach unter e-commerce zusammengefaßt, benötigen ebenso wie der Schutz der Privatsphäre sichere Übertragungswege und Verschlüsselung. Zum einen sind hier Inhalte vor Lauschangriffen zu schützen, noch wichtiger ist aber die Garantie der Authentizität der empfangenen Daten, die Gewißheit, daß diese nicht manipuliert wurden und der angegebene Absender wirklich der Absender ist.

14 Steganographische Verfahren verstecken Daten in anderen Daten. Steganographie ist die Kunst vom Verbergen von Botschaften.

Im Interesse der Entwicklung des e-commerce und des elektronischen Zahlungsverkehrs sind von der EU und den USA bereits früh Zugeständnisse gemacht worden, so daß hierfür bereits länger legale, sichere Verschlüsselungstechniken zur Verfügung stehen. Beispielhaft sei hier die Diskussion über die Schlüssellänge der in Browsern verwandten Verfahren, über die in der Regel im Rahmen des Internets schützenswerte Daten für den Zahlungsverkehr, insbesondere Kreditkartennummern, übermittelt werden.

Da sowohl die USA, als auch die EU an einer Entwicklung des e-commerce interessiert zu sein scheinen, war dies nötig, um die elektronischen Instrumente mit der nötigen Sicherheit, und damit dem von den Kunden verlangten Vertrauen, auszustatten.
Gestützt wird dieser Politik durch eine starke Lobby der handelnden Wirtschaftszweige.

Transatlantische Beziehungen

Die Beziehungen zu den USA als Handelspartner der EU-Mitgliedsstaaten, aber auch als militärischer Alliierter im Rahmen der NATO, spielen auch in Bezug auf den Echelon-Komplex eine Rolle.

Die Verwendung von Verschlüsselungsverfahren behindert die Aktivitäten des US-Geheimdienstes. Die Unterbindung seiner Tätigkeiten im Interesse der einzelnen Staaten, zum Beispiel die Ermittlungen der französischen Staatsanwaltschaft, drohen sogar die Beziehungen aktiv zu belasten. Daß diplomatische Initiativen der USA in Bezug auf die Kontrolle von Verschlüsselungstechniken nicht erfolgreich waren, war vielleicht nicht schädlich, aber bestimmt nicht förderlich.

Kompliziert wird das Verhältnis noch durch die besonders engen Beziehungen zwischen Großbritannien und den USA, so daß nicht immer mit einem geschlossenen Verhalten aller nationalen Regierungen der EU gegenüber den USA zu rechnen ist; im Rahmen des UKUSA-Abkommens tauschen beide Regierungen ihre Informationen und Erkenntnisse aus, so daß ein Verstoß gegen EU-Recht nicht nur von außerhalb der Union kommt, sondern zugleich auch von innen.
Problematisch sind auch teilweise Regelungen militärischer Art, so ist zum Beispiel im Zusammenhang mit dem Echelon-Komplex die Tätigkeiten der USA auch nach dem NATO-Truppenstatut zu betrachten (vgl. z.B. [19]).

Beispielhaft für diese Problematik und das Bewußtsein dieser für das Europäische Parlament sei die Resolution des EU-Parlaments vom 16. September 1998 genannt („Resolution on transatlantic relations/Echelon system“, wiedergegeben auch im Anhang von [1]). In den ersten Abschnitten der Resolution, die bereits im Titel die Beziehungen mit den USA und den Echelon-Komplex aufgreift, betont das EU-Parlament die Bedeutung der Beziehungen zu den USA, die gemeinsamen Werte und Ziele, bevor es die eigentlichen Forderungen an die Vereinigten Staaten stellt.

Politikziele der USA

Auch in den Vereinigten Staaten existieren Organisationen, zum Beispiel Bürgerrechtsbewegungen, und politische Gruppen, die das Potential des Echelon-Komplexes kritisch bewerten oder offen dagegen sind, die jegliche Beschränkung von Verschlüsselungstechniken bekämpfen.
Deren Politikziele sollen hier nicht behandelt werden, vielmehr wird sich auf diejenigen beschränkt, die Konfliktpotential mit der EU bieten.

Das große Problem des Echelon-Komplexes besteht im Mißbrauch für Zwecke der Wirtschafts- und Industriespionage. Der ehemalige CIA-Direktor Woolsey erklärte im März 2000 (hier wiedergegeben nach der Übersetzung von [22]):

„Würde man eine technologische Analyse von etwas aus einem befreundeten 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.“

Zusammen mit der von Duncan Campbell angeführten Einrichtung von Stellen zur Koordination der Weitergabe von Erkenntnissen wirtschaftlichen Belanges, so läßt sich ein Interesse der USA identifizieren, daß darin besteht, befreundete Nationen wie die Mitgliedsstaaten der EU auch zu kommerziellen Zwecken auszuspionieren. (s. S. 33).

Da sichere Verschlüsselungstechniken und unterschiedliche technische Standards Abhöraktivitäten, wie sie die NSA betreibt, erschweren, wird von Seiten der USA - anscheinend unter Einflußnahme von Mitarbeitern der NSA – versucht, durch ent-

sprechende Maßnahmen oder Übereinkommen, das Abhören zumindest für die NSA zu vereinfachen bzw. nicht zu erschweren.
Duncan Campell identifiziert hierfür in seinem Bericht für das Europäische Parlament eine von den USA initiierte Zusammenarbeit auf Beamtenebene, die ILETS (International Law Enforcement Telecommunications Seminar, s. [9], S. 15), die diese Politik verfolgt haben soll. Auch zeigt er das Einwirken der NSA auf Firmen wie Lotus zum Zwecke der Subversion von Schlüsseln auf.

Zusammenfassung

Zusammenfassend läßt sich sagen, daß

- sichere Verschlüsselungsverfahren vorhanden sind, zu denen sich jedermann leicht Zugang verschaffen kann, so daß deren Verbreitung nur mit immensem Aufwand zu kontrollieren wäre,
- vor den Argumenten des Schutzes der Privatsphäre, die Argumente der Strafverfolgung im Sinne einer Beschränkung von Verschlüsselung inzwischen nicht mehr zurückstehen,
- die politische Absicht, Vertrauen in die neuen Kommunikationswege zu schaffen, insbesondere im Interesse des sicheren elektronischen Handels und Zahlungsverkehrs, dazu geführt hat, daß bereits sichere Verfahren - zumindest in den betroffenen Bereichen - Anwendung finden,
- den Beziehungen der EU zu den USA, aber auch den Beziehungen der Einzelstaaten - insbesondere die des Vereinigten Königreichs -, eine besondere Bedeutung in Hinblick auf den Echelon-Komplex zukommt.

Lösungen

Lösungen, um das Abhören von Kommunikation zu unterbinden, sollen hier aus zwei unterschiedlichen Perspektiven dargestellt werden: Die eine sei die Mikroperspektive, bei der der Fokus auf dem einzelnen Übertragungsinhalt oder Datenpaket liegt, die andere sei die Makroperspektive, bei der der Fokus auf der Gesamtheit aller Übertragungsinhalte liegt.

Beide Perspektiven erlauben unterschiedliche Lösungen und Bewertungen von Lösungen, das Abhören wirkungsvoll zu ver- oder behindern.

Mikroperspektive

Bei der Mikroperspektive kommt es allein darauf an, daß ein Übertragungsinhalt, als Beispiel sei eine E-Mail genannt, sicher vom Sender zum Empfänger kommt, d.h., daß ihr Inhalt nicht abgehört werden kann oder daß dieser aufgrund von Verschlüsselungstechniken zumindest für einen Dritten keinen Sinn ergibt.

Bereits das Potential, daß ein Übertragungsinhalt abgehört werden könnte, genügt bereits, daß kein hundertprozentiger Schutz mehr gegeben ist. Da sich das Abhören bei den heutigen Techniken nicht nachweisen läßt und da die Wege eines Inhaltes über die unterschiedlichen Übertragungswege nicht einfach und für den Sender und Empfänger eindeutig nachvollziehbar sind, kann die Übertragung von unverschlüsselten Inhalten nicht als sicher erachtet werden.

Verschlüsselt übertragene Inhalte bieten aber nur dann eine hundertprozentige Sicherheit, falls die Verschlüsselung nicht zu brechen ist. Ein Verschlüsselungsverfahren ist dann zu brechen, wenn es grundsätzlich vom Verfahren her gebrochen werden kann oder weil das verwandte Verfahren unterwandert worden ist, wie es im Abschnitt „Subversion“ beschrieben wird (siehe S. 22).

Verfahren, die grundsätzliche Mängel, zum Beispiel durch begrenzte Schlüssellängen, aufweisen, können bei entsprechendem Aufwand von jedem entschlüsselt werden.

Verfahren, die in ihrer Implementation mit einem Zweitschlüssel arbeiten, können auch nicht als sicher eingestuft werden, da nicht gewährleistet werden kann, daß dieser Schlüssel nicht in die Hände weiterer als die der hinterlegten Stelle gelangt oder

mißbraucht wird. Letzteres ist vor allem ein Problem, da eine Übertragung auf ihrem Weg meist häufig den Hoheitsrechten einer Vielzahl an unterschiedlicher Gesetzgebern unterliegt, die unterschiedliche Erlaubnisse zum Abhören erteilen. Eine Stelle zur Schlüsselaufbewahrung in den USA kann für Europäer, natürliche oder juristische Personen, keinen Schutz bieten, solange zum Beispiel die NSA Zugang zu diesen Daten hat. Nach dem bisherigen Gebahren der NSA geurteilt, kann dies nicht mit letzter Sicherheit, die für ein hinlängliches Vertrauen notwendig wäre, verhindert werden. Es sei vor der Marktmacht eines etablierten Schlüsselaufbewahrungs- oder –rettungssystems gewarnt, das nicht mehr schnell verändert werden kann, wenn es zum Mißbrauch - sei es auch durch legale, einseitige Ermächtigung der US-Regierung - kommt.

Gleichgelagert sind die Probleme bei jeglicher Art an Verschlüsselung, die nicht durch den Urheber eines Übertragungsinhaltes selber vollständig kontrolliert und durchgeführt wird.

Die sichere Verschlüsselung durch die Urheber selber erfordert

- die freie Verfügbarkeit von sicheren Verschlüsselungsverfahren und
- die uneingeschränkte zulässige Nutzung dieser.

Erstgenannter Punkt erfordert, daß dem Urheber des Übertragungsinhaltes bzw. dem Nutzer von Verschlüsselung klar ist, ob und wie sicher das Verfahren ist, insbesondere, daß es nicht technisch bedingt in irgendeiner Form der Subversion unterliegt, und daß er zwischen verschiedenen Verfahren wählen kann.

Die uneingeschränkte Nutzung bedeutet, daß er mit einem beliebigen Verfahren alle Inhalte seiner Wahl verschlüsseln darf und daß die Übertragung verschlüsselter Übertragungsinhalte für den gesamten Übertragungsweg, insbesondere auch für den Empfänger gilt. Die Wahl eines Verschlüsselungsverfahren hat, um für den Nutzer praktikabel zu sein, auch unabhängig von der Art des Übertragungsinhalts und vom Aufenthaltsort zu sein. Letzteres kann vor allem dann ein Problem sein, wenn unterschiedliche Verfahren mit unterschiedlichen Graden an Sicherheit, zum Beispiel bedingt durch unterschiedliche erlaubte Schlüssellängen, unterschiedlichen nationalen Verboten unterliegen.

Bezüglich des gewählten Verschlüsselungsverfahrens sollte es dem Nutzer aber auch möglich sein, bewußt - zum Beispiel aufgrund technischer Bedingungen - weniger sicherere Verfah-

ren wählen zu dürfen.

Die Schwachstelle der Verschlüsselung durch den Urheber eines Übertragungsinhaltes bildet der Umstand, daß zwar die eigentliche Botschaft nicht abgehört werden kann, aber dennoch Profile, wer mit wem kommuniziert, erstellt werden können.

Makroperspektive

Die Makroperspektive legt nicht Wert auf die Sicherheit eines einzelnen Übertragungsinhaltes, sondern auf die Sicherheit aller übertragenen Inhalte. Während bei der Mikroperspektive angeraten wurde, daß die Wahl des Verfahren durch den Nutzer in puncto Sicherheit bestimmt wird, kommt es bei der Makroperspektive auf eine generelle Lösung an, die entweder alle Urheber von Übertragungsinhalten betrifft oder alle Betreiber von Übertragungswegen. In der Makroperspektive besteht die Wahl des Grades der Sicherheit. Hier stehen sich die Pole „keine Nachricht kann abgehört werden“ und „alle können abgehört werden gegenüber“.

Der höchste Grad der Sicherheit kann in der Makroperspektive erreicht werden, wenn alle Urheber von Übertragungsinhalten und alle Anbieter von Übertragungswegen sicherere Verschlüsselungstechniken anwenden. Hierdurch wäre es weder möglich an einzelne übertragene Botschaften zu kommen, noch Kommunikationsprofile zu erstellen. Das Echelon-System hätte in diesem Idealfall keine Daten, die es verwerten könnte.

Dieser Idealfall ist aus einer Vielzahl von Gründen - zumindest zur Zeit - nicht erreichbar, als da wären:

- Aufwand zur sicheren Verschlüsselung insbesondere bei großen Datenmengen,
- Kooperation der Betreiber von Übertragungswegen mit Geheimdiensten,
- Durchsetzung der obligatorischen allgemeinen Verwendung von sicheren Verschlüsselungsverfahren durch alle Nutzer.

Im Rahmen der Makroperspektive können aber auch geringere Ziele, geringere Grade an Sicherheit, definiert werden. Bezogen auf das Echelon-System könnte es genügen, dessen Einsatz oder den ähnlicher Systeme zu behindern, was sie unrentabel in Hinsicht auf Aufwand und Kosten werden läßt.

Für die Verwertung abgehörter Übertragungsinhalte durch das Echelon-System müssen die Botschaften erst einmal im Klartext vorliegen. Sind die Übertragungsinhalte verschlüsselt, so müssen sie erst einmal mit entsprechendem Aufwand entschlüsselt werden, falls möglich. Werden für die Übertragungswege auch Verschlüsselungsverfahren verwandt, so muß auch hier durch den Lauscher entsprechender Aufwand betrieben werden.

Es existieren derzeit marktreife technische Lösungen (siehe DES, S. 19), die das schnelle Ver- und Entschlüsseln bei relativer Sicherheit erlauben. Relative Sicherheit soll hierbei deuten, daß der Schlüssel einer verschlüsselte Übertragung mit entsprechendem Aufwand gebrochen werden kann. Eine absolute Sicherheit ist nicht möglich.

Bedenkt man aber, daß das Brechen eines einzigen DES-Schlüssels zur Zeit ca. 24 Stunden in Anspruch nimmt, dann ist es, sofern der Schlüssel häufig genug unter Verwendung aufwendigerer, sicherer, Verfahren gewechselt wird, nur mit einem Vielfachen des Aufwandes für das Verwerten unverschlüsselter Übertragungen möglich, an die Übertragungsinhalte zu gelangen.

Hiermit läßt sich die Forderung nach der generellen - ggf. zusätzlichen - Verschlüsselung der über einen Übertragungsweg transportierten Daten begründen. Die Betreiber von Übertragungswegen müßten hierfür verpflichtet werden, für jeden einzelnen Übertragungsweg - per Kabel, Satellit oder Funk -, die Daten noch einmal zu verschlüsseln. Erst in der Gesamtheit macht dies Sinn, da die Sicherheit der Kette der Übertragungswege bzgl. eines Übertragungsinhaltes vom schwächsten Glied abhängt.

Für eine Annäherung an den Idealfall der Makroperspektive in puncto Sicherheit ist eine politische Entscheidung des zuständigen Gesetzgebers nötig, die den Grad der Annäherung, der Sicherheit, wovon letztlich die Kosten abhängen, bestimmt, aber auch die Entscheidung, daß dieser Aufwand für alle Betreiber von Übertragungswegen verpflichtend ist, denn nur dann ist überhaupt eine Annäherung an den Idealfall denkbar.

Eine Annäherung an den Idealfall liefert auch - im Gegensatz zu dem in Bezug auf die Mikroperspektive geschilderten - einen Schutz vor der Erstellung von Kommunikationsprofilen (Verkehrsanalyse), wenn diese Daten von den Betreibern mitverschlüsselt werden.

Subversion

Subversion ist grundsätzlich nur in Kooperation mit den Herstellern von Verschlüsselungssoftware oder den Betreibern von Zertifizierungsstellen machbar. Von Verschlüsselungstechniken ist nicht immer bekannt, daß ihre Schlüssel unterwandert werden. Gesetzgeberische Maßnahmen können die Betreiber oder Hersteller dazu bewegen, von ihnen gewährte Möglichkeiten der Subversion offenzulegen oder sogar ganz zu unterbinden.

Die Hersteller können per Gesetz verpflichtet werden, die Möglichkeiten der Subversion ihres angebotenen Produktes offenzulegen, so daß die Subversion einen schweren Mangel darstellt, ohne dessen Kenntnis ein Verkauf nichtig wäre. Entsprechend wäre die Haftung für Fälle der Subversion zu regeln. Für Schäden könnten die Hersteller oder Betreiber unterwanderter Techniken haftbar gemacht werden. Dies ist aber nur sinnvoll, wenn die Beweislast beim Hersteller beziehungsweise Betreiber läge, so daß schon eine potentielle Gefahr für die Beweisführung ausreiche. Da „Lauschen“ generell von geheimdienstlicher Natur ist, wird es nur in wenigen Fällen, Zufällen, möglich sein, entsprechende Beweise für kausale Zusammenhänge zwischen einem Schaden und der Subversion eines Schlüssels zu finden, was eine Umkehr der Beweislast ändern würde.

Strafverfolgung

Wie auf Seite 44ff dargelegt, sind die Kosten finanzieller und nicht-finanzieller Art bei Beschränkung von Verschlüsselungstechniken gegenüber dem zu erwartenden Nutzen zu hoch. Jegliche Beschränkung ist daher auch entgegen den Interessen der Strafverfolgung nur eine Scheinlösung, die weitere Probleme aufwirft. Bezüglich der technischen Einrichtungen zum Abhören von Kommunikation kann der Gesetzgeber, was eine politische Entscheidung ist, Vorschriften erlassen, ob und in welcher Ausführung diese existieren sollen. Dies macht dann Sinn, wenn es über die Art der Einrichtungen multi-nationale oder sogar weltweite Standards gibt. Unterschiedliche Standards würden ansonsten den Wettbewerb der Anbieter von Kommunikationseinrichtungen erheblich behindern. Ein weltweiter Standard hätte Vorteile für die Hersteller dieser Einrichtungen und für die Institute der Strafverfolgung.

Zusammenfassung

Das Europäische Parlament (EU-Parlament), der Europäische Rat und die Europäische Kommission sind in der Lage, Politiken zu betreiben, die zu Beschlüssen führen, die

1. die Verwendung von Verschlüsselungstechniken verpflichtend in allen Lebensbereichen oder auch nur in Teilen verpflichtend machen
2. die Offenlegung von Einschränkungen bei der Sicherheit von Verschlüsselungstechniken und –einrichtungen erzwingen, zum Beispiel im Falle der Subversion,
3. die Haftungs- und Schuldfragen bezüglich Verschlüsselungseinrichtungen und –techniken regeln,
4. Standards in bezug auf die verwandten Techniken setzen.

Optionen und Entwicklung

Das EU-Parlament hat seine entsprechenden Gegner in den Verfahren, die zu Beschlüssen bzgl. der geschilderten Lösungsansätze führen, in den anderen beiden beteiligten Institutionen, dem Rat und der Kommission. Es ist benachteiligt, da es kein eigenes Initiativrecht für eigenständige Rechtsakte der Europäischen Union besitzt.

Begreift das EU-Parlament Sicherheit bei der Kommunikation als Querschnittsaufgabe, so ist es in der Lage, dies derartig umzusetzen, daß es in alle Beschlußvorlagen entsprechende Bestimmungen, zum Beispiel zur verpflichtenden Nutzung von Verschlüsselungsverfahren, aufnehmen läßt, ohne die es seine Zustimmung verweigern würde.

Alle drei Institutionen sind sich der besonderen Bedeutung der Beziehungen zu den USA bewußt. Der verstärkte Einsatz von Verschlüsselungstechniken behinderte die geheimdienstliche Tätigkeit der Vereinigten Staaten, sind somit einem guten Verhältnis zumindest so lange nicht dienlich, wie die USA oder Teile ihres politischen Systems eine Politik verfolgen, Zugang zur Kommunikation anderer Nationen zu haben.
Dennoch hat das EU-Parlament sich das Anliegen sicherer, „unbelauschter“, Kommunikation zu eigen gemacht, aber war auch stets bemüht, das Verhältnis zu den USA dadurch nicht zu sehr zu belasten. Die bisher stärkste Belastung wird die Einsetzung eines Ausschusses zum Echelon-Komplex durch das EU-Parlament am 5.7.2000 sein. Es ist zu erwarten, daß durch die Arbeit des Ausschusses ggf. neue Fakten veröffentlicht werden, insbesondere aber durch die Berichterstattung eine Öffentlichkeit geschaffen wird, die Echelon ablehnt, was sich auf die betreibenden Staaten, u.a. die USA, auswirken wird. Die Existenz des Ausschusses allein stellt somit bereits ein Problem dar.

Da diplomatisch mit den USA hauptsächlich die Regierungen der Mitgliedsstaaten der EU verkehren, ist der Rat mehr von den Auswirkungen auf die Beziehungen betroffen als das EU-Parlament. Auf der Ebene der nationalen Regierungen fließen auch die Argumente der Strafverfolgung aus den Mitgliedsländern selber oder aufgrund diplomatischer Initiativen der USA in den Politikfindungsprozeß ein.

Initiativen für den Einsatz von Verschlüsselungstechniken sind in Bezug auf die Beziehungen zu den USA für die Einzelstaaten und den Rat daher nicht dienlich. Desgleichen gilt für Initiativen

der EU-Kommission hierzu. Beide Institutionen haben aber auch ein Interesse an sicherer Kommunikation, wie eben das EU-Parlament. Es existiert ein Interessenskonflikt:

Anschuldigungen gegen die USA in Bezug auf das Abhören von Kommunikation und der Verwendung der dadurch gewonnen Informationen, wie in einigen Fällen geschildert (zum Beispiel in [3], Technical File S. iv f.), sind in Hinsicht der Beschaffenheit des Themenkomplexes Echelon nicht zu vermeiden. Eine Befassung mit dem Echelon-Komplex und die damit verbundenen Anschuldigungen belasten mit Sicherheit das Verhältnis zu den USA. Dies ist ganz besonders nicht im Interesse von Rat und Kommission, aber auch nicht des EU-Parlaments.

Potential, die Beziehungen zu den USA zu belasten, haben in Hinsicht auf den Echelon-Komplex folgende Ereignisse des ersten Halbjahres 2000:

> Am 30. März 2000 erklärte EU-Kommissar Erkki Liikanen, zuständig für Unternehmen und Informationsgesellschaft, nachdem er feststellte, daß allein die Mitgliedsstaaten der EU Kompetenzen auf dem Gebiet geheimdienstlicher Tätigkeiten besitzen, daß die technischen Gegebenheiten für ein System wie Echelon nach dem STOA-Bericht ([9]) gegeben seien. In der Natur der Sache läge es laut Liikanen, daß die Existenz von Echelon weder bestätigt noch geleugnet werden könne. Er fügte hinzu: „Es gibt keinen Grund zur Behauptung, daß vorhandene technische Möglichkeiten nicht genutzt würden.“ Auch bestätigte Liikanen, daß der Einsatz von Kryptographie für die EU-Kommission hohe Priorität hat. (vgl. [5])
>
> Am 29. Mai 2000 setzte der Europäische Rat für Justiz und Inneres eine technische Arbeitsgruppe ein, die klären soll, inwieweit „technische Maßnahmen“, wie starke Verschlüsselungsverfahren, den Mißbrauch von abgehörtem Material verhindern kann. Diese Arbeitsgruppe ist dabei das Ergebnis einer Diskussion über das anglo-amerikanische Spionagenetzwerk Echelon.(vgl. [6])
>
> Im Juni 2000 befaßte sich das niederländische Parlamente mit dem Echelon-Komplex, nachdem die niederländische Regierung aufgrund der Sitzung des Europäischen Rats für Justiz und Inneres zwar immer noch keine Beweise und Antworten betreffend einiger Anfragen von Parlamentariern vorlegen kann, aber dennoch präventiv tätig werden will. (vgl. [4])

In einer nicht-öffentlichen Sitzung befaßte sich der Ausschuß für europäische Angelegenheiten des Deutschen Bundestages zum ersten mal mit dem Themenkomplex Echelon. Ausgesagt hat dabei unter anderen Duncan Campbell, Verfasser eines Teils des für das EU-Parlament erarbeiteten sogenannten STOA-Berichts ([9]).
Im Rahmen der Ausschußsitzung wurde auch die Rechtsgrundlage in Frage gestellt, nach der die USA und Großbritannien Anlagen des Echelon-Komplexes in Deutschland, vor allem in Bad Aiblingen, betreiben.

Am 5. Juli berichtet die englische Tageszeitung The Guardian, daß die französische Staatsanwaltschaft die französische Spionageabwehr mit einer Untersuchung zu Echelon beauftragt hat. Eine solche strafrechtliche Untersuchung richtet sich in der Regel gegen Einzelpersonen, hier wahrscheinlich gegen Mitarbeiter der amerikanischen National Security Agency (NSA), die in Frankreich tätig sind. Hieraus werden sich voraussichtlich Spannungen zwischen den USA und Frankreich - und der EU - ergeben.(vgl. [15])

Auf der Plenumssitzung des Europäischen Parlamentes am 5. Juli 2000 hat dieses einen Ausschuß eingesetzt, der die STOA-Berichte verifizieren soll (vgl. [7]). Hinter dem Antrag, einen Untersuchungsausschuß einzusetzen, ist es dabei zurückgeblieben. Als Gründe können dabei angesehen werden, daß nicht zu erwarten ist, daß vor einem solchen Untersuchungsausschuß Vertreter der Regierung der USA und Großbritannien aussagen würden, und daß nach Vermutungen einiger Parlamentarier, andere nicht gegen die Interessen bestimmter EU-Regierungen, also der des Vereinigten Königreichs, stimmen wollten; vor diesem Hintergrund scheint der Ausschuß nur bedingt arbeitsfähig zu sein.
Die Diskussion über den Antrag zur Einrichtungen eines Ausschusses hatte seit der Sitzung des Plenums am 30. März 2000 angedauert.

Begonnen mit einem ersten Bericht 1998 ([11]), in dem der Echelon-Komplex Erwähnung fand, über einen kompletten fünfbändigen Bericht zu Echelon 1999 ([1],[3],[9],[10],[14]) ist es dem EU-Parlament über seine weitergehende Arbeit im ersten Halbjahr 2000 gelungen, eine breitere Öffentlichkeit für das Thema Echelon zu interessieren, als dies jemals der Fall war; insbesondere die Befassung nationaler Parlamente zum gleichen Thema, beispielhaft seien die Niederlande und Deutschland an-

geführt, ist als ein Erfolg des EU-Parlaments anzusehen.

Schlußfolgerungen

Die Behandlung des Themenkomplexes Echelon führt viele unterschiedliche Akteure zusammen. Die Vertreter der Interessen der Privatsphäre, der Strafverfolgung, des e-commerce und der Geheimdienste stellen dabei nur eine Möglichkeit der Kategorisierung dieser dar, wichtig ist es auch die Politikziele der einzelnen EU-Institutionen und nationalen Regierungen zu bedenken. In Bezug auf Echelon stellt sich dabei als erschwerend für die Findung einer einheitlichen Politik aller EU-Mitglieder dar, daß als Nutznießer der Ergebnisse des Echelon-Komplexes nicht nur externe, hauptsächlich die USA, sondern auch interne Akteure, Großbritannien, auftreten; dies erschwert auch die Politikfindung im EU-Parlament (vgl. [7]).

Als treibende Kraft im Kampf gegen die durch die Existenz des Echelon-Systems existierende Gefahr von Wirtschafts- und Industriespionage stellt sich das EU-Parlament dar. Seine Arbeit vergrößert die Öffentlichkeit, die um Echelon weiß und sich damit befaßt. Es hat die Möglichkeit Schutzmaßnahmen zu ergreifen, indem es sie als Querschnittsaufgabe begreift und in vorgelegte Beschlußentwürfe einarbeitet.
Auch wenn dem EU-Parlament das nötige Initiativrecht für eigenständige Rechtsakte fehlt, kann es auf die übrigen Institutionen der EU, Rat und Kommission, über seine Befaßung mit dem Thema und Ausschüsse Druck via die Bedeutung der transatlantischen Beziehungen ausüben, den diese mit einer Änderung ihrer Politik und entsprechender Vorlagen an das EU-Parlament entgegnen können.

„Doch für politischen Unmut im amerikanisch-europäischen Verhältnis wird Coelho[15] allemal sorgen, dann nämlich, wenn er zusammenträgt, was auf der politischen EU-Ebene niemand hören mag: Es gibt ein satellitengestütztes amerikanisches Abhörsystem „Echelon“, das systematisch die weltweite Kommunikation auf bestimmte Schlüsselbegriffe hin durchscannt.“([22])

Es stellt sich dar, als ob das EU-Parlament den nötigen Druck erzeugt, um innerhalb des Europäischen Rats eine einheitliche Politik gegen das Echelon-Systems zu finden, was diesem aufgrund der Beteiligung Großbritanniens schwer fällt.

15 Der portugiesische Europa-Abgeordnete Carlos Coleho ist Vorsitzender des ab September für ein Jahr tagenden, nicht ständigen Ausschusses des EU-Parlaments, der sich mit dem Echelon-Komplex befaßt.

Empfehlung

Das EU-Parlament sollte in alle ihm vorgelegten Beschlußvorlagen, zum Beispiel EU-Richtlinien, die verbindliche Nutzung von Verschlüsselungsverfahren aufnehmen, solange es keine ausreichenden Regelungen aufgrund einer eigenständigen Richtlinie gibt. *(Erfolg vor allem im Bereich der Makroperspektive)*

Das EU-Parlament sollte sich weiter mit dem Thema befassen, um die schwer zu erreichende europäische Öffentlichkeit über den Echelon-Komplex zu informieren und damit Druck für entsprechende Initiativen der übrigen Akteure zu erzeugen. *(Initiativen im Sinne der Makro, aber auch der Mikroperspektive)*

In Hinsicht auf dem in seiner Sitzung am 5.7.2000 eingesetzten Ausschuß hat es die Möglichkeit, durch dessen Arbeit die Öffentlichkeit über die Berichterstattung der Medien zu erreichen. Diesen Druck kann es noch weiter erhöhen, wenn es zum Echelon-Komplex nicht nur einen Ausschuß, sondern einen Untersuchungsausschuß einsetzt, wovon es in der Sitzung am 5.7.2000 abgesehen hat.

Erwartung

Der vom EU-Parlament eingesetzte Ausschuß wird daran kranken, daß er keine richtigen Untersuchungsmöglichkeiten in Bezug auf die am Echelon-System Beteiligten hat. Es ist unwahrscheinlich, daß Vertreter der USA oder des Vereinigten Königreichs vor diesem aussagen werden, erst recht nicht in einer öffentlichen Sitzung.

Es ist vielmehr eine Prüfung der vom STOA-Komitee abgegebene Berichte ([1],[3],[9],[10],[14]) zu erwarten. Hierdurch wird es voraussichtlich zu einer verstärkten Berichterstattung der Medien kommen..

Sollte es innerhalb der 12 Monate nach der Einsetzung des Ausschusses zu keiner nennenswerten Initiative von Seiten der EU-Kommission oder des Rates kommen, so wird das Europäische Parlament versuchen, den Druck zu erhöhen, zum Beispiel in der Form der Einsetzung eines Untersuchungsausschusses, dem mehr Kompetenzen zukommen, wovon es auf seiner Sitzung am 5.7.2000 abgesehen hat.
Außerdem ist zu erwarten, daß einige Parlamentarier dann bei jeder Vorlage zu Themengebieten, in denen Verschlüsselungs-

verfahren eine Rolle spielen können, das Thema Echelon und sichere Verschlüsselungsverfahren in der parlamentarischen Debatte aufgreifen werden. *(Dies führt ggf. zu Erfolgen im Sinner der Makroperspektive.)*

Sollte der Einsatz von Verschlüsselungsverfahren weitgehend verpflichtend werden, ist davon auszugehen, daß die Bedeutung des Echelon-Komplexes rasch verschwindet. Bei der verpflichtenden Benutzung von Verschlüsselungsverfahren für Übertragungswege kann damit gerechnet werden, daß innerhalb von fünf Jahren Lauschangriffe weitgehend unmöglich werden.

Dies würde dann auch den Loyalitätskonflikt des Vereinigten Königreichs lösen. So kann erwartet werden, daß Großbritannien sämtliche Ermittlungen und Prozesse der Politikfindung, sowie Gesetzgebung solange verzögern wird, bis aufgrund des technischen Fortschritts und veränderter Kommunikationseinrichtungen die Ausbeute von Echelon allgemein nur noch als marginal eingeschätzt wird.

Ausblick

Der Echelon-Komplex stellt nur eine Gefahr für Wirtschafts- und Industriespionage dar. Neben dem Echelon-Komplex existieren noch andere Systeme, die ein ähnliches Gefährdungspotential aufweisen. Beispielhaft, seien französische, schweizerische, russische und chinesische Einrichtungen gleicher Art angeführt.

Insbesondere die deutsch-französische Zusammenarbeit der Nachrichtendienste auf diesem Gebiet ist von Untersuchungsinteresse in bezug auf die Politikfindung der EU zum Echelon-Komplex. Dies ist dabei nur ein Punkt in Hinsicht auf die geheimdienstlichen Tätigkeiten der EU-Mitgliedsstaaten gegeneinander, die es nach Artikel 16 des Amsterdamer Vertrages (s. S. 41) abgeleitet eigentlich nicht geben sollte und brächte, offensichtlich aber doch gibt. Das Problem mag darin vermutet werden, daß keiner EU-Institution irgendwelche Kompetenzen auf dem Gebiet der Geheimdienste zustehen, es existiert ausschließlich das Informationsgebot aus Artikel 16 des Amsterdamer Vertrages.

Weiteren Untersuchungswert haben die Auswirkungen einer Zusammenarbeit zwischen EU-Organen und den USA auf dem Gebiet der Strafverfolgung. Durch die Übernahme des Schen-

gener-Abkommens in den Amsterdamer Vertrag, der damit einhergehenden Erweiterung des Schengen-Informations-Systems (SIS) zu einem europäischen und über das Rechtshilfeabkommen mit den USA wird das SIS zu einem internationalen Instrument der Strafverfolgung, das auch Mißbrauchsmöglichkeiten, zum Beispiel durch die Standardisierung von Abhöreinrichtungen, eröffnet. Auch hier stellt sich wieder das Problem der Wirtschafts- und Industriespionage.

Allgemeiner besteht auch Bedarf nach einer Untersuchung des unterschiedlichen Umgangs mit und der unterschiedlichen Wahrnehmung schützenswerter Kommunikation und Information. Markant tritt dieser Unterschied bei der Behandlung des Datenschutzes auf. Während im europäischen Kontext Datenschutz aus dem garantierten Schutz der Privatsphäre resultiert, somit staatliche Regelung und Kontrolle begründet, besteht die us-amerikanische Position aus einer privatrechtlichen Regelungsverantwortung des Datenschutzes.

Literaturverzeichnis

Bei den zitierten, nur online existierenden Dokumenten wurde neben der eindeutigen Adresse, dem Uniform Resource Locator (URL), auch jeweils die E-Mail-Adresse des Autors oder Herausgebers mit angegeben, um es – wie inzwischen allgemein akzeptiert – für den wissenschaftlichen Diskurs doppelt zu referenzieren; bei den Publikationen des Heise-Verlags wurde darauf verzichtet, da eine Zuordnung über Verlag, Erscheinungsort und -jahr, sowie Telepolis über http://www.heise.de/tp/ eindeutig gewährleistet ist.

[1] Becker, Peggy: Présentation et analyse 1) Présentation des quatre études 2) Analyse: protection des données et Droit de l'Homme dans l'Union et rôle du Parlement Européen (Englische Übersetzung), Luxemburg, Dezember 1999, Teil 1/5 in Europäsiches Parlament, „Development of Surveillance Technology and Risk of Abuse of Economic Information“

[2] Biryukov, Alex und Shamir, Adi: Real Time Cryptanalysis of the Alleged A5/1 on a PC (preliminary draft), New York, 1999
http://cryptome.org/a5.ps
http://cryptome.org/a51-bsw.htm , jy@cryptome.org

[3] Bogolikos, Nikos: The perception of economic risks arising from the potential vulnerability of electronic commercial media to interception, Luxemburg, Oktober 1999
Teil 5/5 in Europäisches Parlament: „Development of Surveillance Technology and Risk of Abuse of Economic Information

[4] Buuren, Jelle van: Anhörung zu Echelon im holländischen Parlament, Telepolis, München, 27.6.2000
http://www.heise.de/tp/deutsch/special/ech/6871/1.html

[5] Buuren, Jelle van: Europäische Kommission gibt verwaschene Stellungnahme zu Echelon ab, Telepolis, München, 30.3.2000
http://www.heise.de/tp/deutsch/special/ech/6701/1.html

[6] Buuren, Jelle van: Europäischer Rat für Justiz- und Inneres erwägt Schutzmaßnahmen gegen Echelon, Telepolis, München, 30.5.2000
http://www.heise.de/tp/deutsch/special/ech/6815/1.html

[7] Buuren, Jelle van: Kein Untersuchungsausschuss über Echelon im Europäischen Parlament, Telepolis, München, 5.7.2000
http://www.heise.de/tp/deutsch/special/ech/6890/1.html

[8] Campbell, Duncan: Enthüllt: Die größten Abhörzentren,
http://www.zdnet.de/news/report/echelon/abhoerzentren_00-wc.html
in: ZDNet News Report „Das Abhörsystem Echelon“,
http://www.zdnet.de/news/report/echelon/echelon-wc.html

ZDNetDE@zdnet.com

[9] Campbell, Duncan: The state of the art in communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband ultu-language leased or common carrier systems, and its appicability to COMINT targetting and selection, includingspeech recognition, Luxemburg 1999
Teil 2/5 in Europäisches Parlament: „Development of Surveillance Technology and Risk of Abuse of Economic Information“

[10] Elliot, Chris (Prof.): The legality of the interception of electronic communications: A concise survey of the principal legal issues and instruments under international, European and national law, Luxemburg, Oktober 1999
Teil 4/5 in Europäisches Parlament: „Development of Surveillance Technology and Risk of Abuse of Economic Information“

[11] Europäisches Parlament (Hrsg.): „Development of Surveillance Technology and Risk of Abuse of Economic Information“, Hrsg.: Europäisches Parlament, Generaldirektorat für Forschung, Direktorat A, STOA Programm, Luxemburg, 1999 (PE 168.184)

[12] Hager, Nicky: Secret Power: New Zealands's Role in the International Spy Network“, Nelson (Neuseeland), 1996

[13] Landesamt für Verfassungsschutz Baden-Württemberg: Wirtschaftsspionage, Die gewerbliche Wirtschaft im Visier fremder Nachrichtendienste, Stuttgart, 1998
http://www.baden-wuerttemberg.de/verfassungsschutz/wi-spio.pdf

[14] Leprevost, Franck (Dr.): Encryption and cryptosystems in electronic surveillance: a survey of the technology assessment issues, Luxemburg, November 1999
Teil 3/5 in Europäisches Parlament: „Development of Surveillance Technology and Risk of Abuse of Economic Information“

[15] Medosch, Armin: Frankreich leitet Untersuchung über Echelon ein, Telepolis, München, 5.7.2000
http://www.heise.de/tp/deutsch/special/ech/6889/1.html

[16] Rink, Dr. Jürgen: Quäntchen für Quäntchen, c't-Magazin 16/98, S.150, Garbsen, 1998

[17] Schöne, Bernd: Kleiner Lauschangriff, Handys sind nicht mehr abhörsicher - Verschlüsselungs-Algorithmus gebrochen, Die Welt, Berlin, 3.1.2000

[18] Schulzki-Haddouti, Christian: 5. Juli ist Echelon-Tag, Telepolis, München, 30.6.2000
http://www.heise.de/tp/deutsch/special/ech/6879/1.html

[19] Schulzki-Haddouti, Christiane: Echelon im Bundestag: Abgeordnete drängen auf Spionageverbot, Telepolis, München, 6.7.2000
http://www.heise.de/tp/deutsch/special/ech/6895/1.html

[20] Senderek, Ralf: Die Sicherheit des geheimen Schlüssels, 1998

http://senderek.de/security/schutz.html , ralf@senderek.de

[21] Singh, Simon: Geheime Botschaften, Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internets, München, 2000

[22] Ulfkotte, Udo: Undankbare Aufgabe, Ein EU-Ausschuss soll Licht in die Schattenwelt amerikanischer Geheimdienste bringen, FAZ, 22.7.2000

[23] Wright, Steve: An Appraisal of Technologies of Political Control, Interim Study, Hrsg. Europäisches Parlament, Luxemburg, Januar 1998 (PE 166.499)

[24]Wright, Steve: Eine Bewertung der Technologien für eine politische Kontrolle, Zwischenstudien, Aktualisierte Zusammenfassung, Luxemburg, September 1998 (PE 167.499)